السلامة الرقمية

العدد الثاني / الخميس 23 ربيع الأول 1446هـ - 26 سبتمبر 2024م

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

المبادرة الوطنيّة للسلامة الرقميّة
Digital Safety National Initiative

أجهزة البيجر
وحروب الجيل الخامس تظهر في لبنان

الثقة في جوجل
عامل جَذْب يستغله مجرمو الإنترنت لخداع مستخدمي مُحرّك البحث عبر الإعلانات

دلال العقيدي
الذكاء الاصطناعي حاضر في المبادرة الوطنية للسلامة الرقمية

المحتويات

الذكاء الاصطناعي حاضر في المبادرة الوطنية للسلامة الرقمية

عَقِب التطورات التكنولوجية المتسارعة، لا سيما في مجال الذكاء الاصطناعي، وتطوُّر التهديدات السيبرانية المعتمِدة على تقنيات تكنولوجية فائقة التقدُّم، والتي تستهدف الدول والمؤسسات والمجتمعات والأفراد، ازدادت أهمية التوعية بهذه المخاطر وبكيفية التعرُّف عليها والوقاية منها. خاصةً أن العالَم يتَّجه بخطوات حثيثة نحو زيادة الاعتماد على الذكاء الاصطناعي في مختلف المجالات الاقتصادية والعلمية والطبية، وغيرها، ما يعني مزيداً من الانتشار الأفقي والعمودي لهذه التقنيات.

هذا الواقع يؤكد على ضرورة التركيز على التوعية بمخاطر الذكاء الاصطناعي، وأخلاقيات استخدامه، وهذا ما تحرص عليه الوكالة الوطنية للأمن السيبراني في مختلف برامجها ومشاريعها، وآخرها كان "المبادرة الوطنية للسلامة الرقمية"، وذلك من خلال تضمين المحتوى التوعوي توجيهات وإرشادات حول هذه المخاطر، مثل: التزييف العميق، واستخدام الذكاء الاصطناعي في الهندسة الاجتماعية، وغيرها من التهديدات السيبرانية.

وفي هذا السياق يتم التركيز على محتوًى قريبٍ من اهتمامات ومجالات عمل مختلف الشرائح المستهدَفة بالمبادرة، بمعنى أن الأثر المنشود من المبادرة في هذا المجال يعتمد بشكلٍ رئيسٍ على مرونة عالية، تظهر من خلال التوجُّه لكلِّ شريحةٍ بمحتوًى توعويّ وبأدوات توعوية تتناسب مع الاحتياجات التوعوية الفعلية لها. فالمبادرة، وفقاً لهذا الطرح، تسعى للاهتمام بأحدث المفاهيم في مجال الأمن السيبراني والسلامة الرقمية، ما يُعزّز من قِيمتها المضافة، ويُسهم في تحقيق أهدافها، ويدعم بلوغ رؤيتها ورسالتها.

دلال العقيدي

مدير إدارة التميز السيبراني الوطني

أنشطة "الشبح"

تدفع الشرطة الأوروبية لاعتقال 51 شخصاً من عدة دول

في استهدافٍ لشبكات الجريمة المنظَّمة العالمية: تفكيك منصة "Ghost".. ومُصادَرة أكثر من مليون يورو

فـي خطوةٍ مهمةٍ لتفكيـك واحدة من أخطر منصـات الجريمة المنظَّمة علـى الإنترنت، قادت منظمة الشـرطة الأوروبية (يوروبول) ووكالات إنفاذ القانون من تسع دول عملية دولية لتفكيك منصة "الشبح" Ghost، التي تَسـتخدم ثلاثة معايير تشفير مختلفة، تسمح بتدمير جميع الرسائل بواسطة رمز محدَّد، ما جعَلها المنصة المفضَّلة لعصابات الاتجار بالمخدرات وغسيل الأموال بفضل ميزاتها الأمنية المتقدّمة.

وتُعدّ هذه العملية أحدث عملية تقوم بها وكالات دولية لتعطيل خدمات الرسائل المشفَّرة المستخدَمة مِن قِبَل المجرمين على الإنترنت، وذلك بعد إغلاق منصات مشابهة مثل EncroChat & Sky ECC.

بعد وصفها بـ"شريان حياة الجريمة المنظَّمة".. الشرطة الأوروبية تنجح في إخماد خطر منصة "الشبح"

وكجزء من التزام أوسع لمكافحة الجريمة المنظَّمة العالمية؛ تمكَّنت "اليوروبول" بمساعدة السلطات من أستراليا وكندا وفرنسا وأيسلندا وأيرلندا وإيطاليا وهولندا والسويد والولايات المتحدة، من منع عدة تهديدات من خلال اعتقال 51 شخصاً، ومصادرة أكثر من مليون يورو (بما يعادل 1.11 مليون دولار) نقداً على مستوى العالم[1].

وعن ذلك، قال نائب المدير التنفيذي لليوروبول، جان فيليب ليكوف: "انتهت اللعبة"؛ في إشارة منه إلى جهود التحقيق المشترك الذي بدأ في عام 2022م لتفكيك المنصة غير القانونية التي وُصِفَت بأنها "شريان حياة للجريمة المنظَّمة الخَطِرة".

جدير بالذكر أن تطبيق Ghost هو شبيه بتطبيق WhatsApp، وقد تم إطلاقه قبل تسع سنوات، وكان مخصصاً للمراسلات غير القانونية، كما كان لا يعمل إلا من خلال هواتف ذكية معدَّلة، وهذا التطبيق يستخدم تقنيات متقدمة للتشفير[2]، بحيث يصبح من الصعب خرقه، ما يحقّق سرية للعمل غير القانوني، ويُعزّز من العلاقة بين الهجمات السيبرانية والجريمة المنظَّمة.

1. Noemie Olive & Charlotte Van Campenhout, 'Ghost' cybercrime platform dismantled in global operation, 51 arrested, reuters, September 2024. https://2u.pw/KCuOKaIB
2. Connor Jones, Cops across the world arrest 51 in orchestrated takedown of Ghost crime platform, theregister, Sep 2024. https://2u.pw/tAUjfFyj

أجهزة البيجر وحروب الجيل الخامس تظهر في لبنان

أثار انفجار أجهزة الاتصالات اللاسلكية في لبنان مخاوف كثيرين حول العالم، رغم تراجع استخدام أجهزة الاتصال اللاسلكي (ووكي توكي) وأجهزة النداء (البيجر)، وحول هذا عرضت شبكة سي إن إن (CNN) محاكاة عملية لبيان مدى تأثير تلغيم أجهزة "بيجر" بالمتفجرات على دمية؛ حيث تم ربط جهاز نداء "بيجر" مزوّد بمادة بي إي تي إن "PETN" التفجيرية على خَصْر الدمية، وبالقرب من رأسها، ووُصِفَت التجربة بـ"الكارثية" لتسبُّبها في شطر الرأس إلى نصفين، علاوةً على قدرة تفجير مماثل على إلحاق الضرر بالآخرين المحيطين بحاملي تلك الأجهزة المُلغَّمَة[1].

حادثة "البيجر" في لبنان... العالم على أعتاب تحوُّل جديد يقوم على الدمج بين الهجمات التقليدية والسيبرانية، ما يُنْتِج جيلاً جديداً من الحروب الهجينة

وفتح تفخيخ أجهزة "البيجر" بمتفجرات شديدة الحساسية وتفجيرها عن بُعْد باب النقاش حول حروب الجيل الخامس التي أصبحت التكنولوجيا تُشكِّل عنصراً حاسماً فيها، بما تشمله من أسلحة سيبرانية وذكاء اصطناعي، وتكتيكات غير تقليدية، وما ارتبط بها من تحويل أجهزة بديلة للهواتف الذكية كانت تُعدّ آمِنَة بنسبة 100% إلى قنابل موقوتة تُستغَلّ في الصراعات المسلحة والحروب.

وتعمل حروب الجيل الخامس على تغيير طبيعة وخواص الصراع بشكلٍ كامل؛ إذ تمكَّنت من توسيع مجال الصراع ليضمّ المجال المادي المعلوماتي والسيبراني، ما يجعلها أنجح أجيال الحروب وأكثرها تأثيراً في العقود الخمسة الأخيرة.

1. لك أن تتخيل.. تجربة انفجار "بيجر" على دمية بفيديو لفهم مدى الضرر، سي إن إن، 21 سبتمبر 2024. https://2u.pw/G7mLFEPf

تحوُّل أجهزة اللاسلكي إلى "قنابل موقوتة" يكشف عن سوق غامضة للتكنولوجيا

وتُصنَّف مادة "بـي إي تي إن" -التي عثرت الأجهزة الأمنية اللبنانيـة عليها لدى فحـص بقايا الأجهزة المسـتهدفة- بأنهـا شـديدة الانفجـار لتَفُـوق سـرعة موجة الصدمـة التي تُولّدها عنـد الانفجار 8 كم/ثانيـة. ونتيجةً لخصائصها المميزة تُسـتخدَم في صُنع القنابل النووية لصعوبة رَصْدها من طرف أجهـزة المراقبـة؛ إذ تتحوَّل إلى بلورات شـفَّافة لا رائحة لهـا، ومُقاوِمَة للاحتـكاك والصدمات. وقد سـاعدت خصائـص "PETN" فـي تفضيـل الدول والجماعات السـرية اسـتخدامها لإمكانية تطويع شـكلها وإخفائها عن طريـق المَزْج مـع مكونات تفجيرية أخرى، ممَّا يُسهّل تهريبها عبر وسائل النقل العالميـة كالمطارات، كما حدَث فـي تفجير طائرة خطوط "بانام" فـوق بلدة لوكربي الإسـكتلندية، حيـن تم اسـتخدام تلـك المادة شـديدة الانفجار ضمن مكونات أخرى جرى إخفاؤها داخل جهاز راديو تجاري[1].

جديـر بالذكر أنه وعلى الرغم من أن هجمات لبنان لا تُعدّ هجوماً سـيبرانيّاً صريحاً؛ إلا أنها تعتمد بشـكل كبير على تقنيات التشـفير، واستخدام التكنولوجيا في تنفيذ الهجمات، ما يتقاطع بشكلٍ مباشرٍ أو غير مباشـر مع الحروب الإلكترونية والسيبرانية، خاصةً أن عملية الاسـتهداف تَعتمد على خرق شـبكات الاتصالات، وتحفيز المادة المتفجّرة من خلال رسالة مُحدَّدة ذات كـود برمجي محدَّد. وهـذا الاعتماد على التشـفير وخرق شـبكات الاتصالات يُعدّ من صُلب الهجمات السيبرانية.

وهنا يمكن القول إننا على أعتاب تحوُّل جديد يقوم على الدمج بين الهجمات التقليدية والسيبرانية، ما يُنْتِج جيلاً جديداً من الحروب الهجينة.

1. India Today Information Desk, What is PETN, the key component in Mossad's deadly operations?, Sep 2024. https://2u.pw/N835G4sY

الثقة في "جوجل"

عامل جَذْب يستغله مجرمو الإنترنت لخداع مستخدمي مُحرّك البحث عبر الإعلانات

تجنّب النقر على الإعلانات وتحديث المتصفّح ونظام التشـغيل.. نصائح خبراء الأمن السيبراني لزوار مواقع الويب

يبحـث مجرمو الإنترنت عن قنـوات إيصال للبرمجيات الخبيثـة إلى ضحاياهم للبدء في شـنّ هجماتهم السـيبرانية، ومن بينها "الإعلانـات المنبثقة" دائمة الظهور خلال عمليات البحـث الروتينية على محرّك البحث جوجل "Google".

وفي هذا السياق كشفت شركات متخصّصة في البرمجيات الضارّة ارتفاع وتيرة استغلال هذه الإعلانات خلال السـنوات الأخيرة. ومن أمثلة ذلك: ما أسفرت عنه عمليات بحث قامت بها شركة Malwarebytes وتوصلت إلى نتائج تؤكد زيادة تُقدَّر بـ 42% على أسـاس شـهري في حوادث الإعلانات الضارّة بالولايات المتحدة في عام 2023م[1].

وتُسـتخدَم الإعلانـات المنبثقـة لأغـراض خبيثة كالتصيـد الاحتيالـي أو تنزيل برمجيـات ضارّة على الأجهـزة الإلكترونية لزُوّار مُحـرّك جوجل؛ إذ يمكن إخفاء البرمجية الضارة في الإعلانات التي تظهر على مواقع الإنترنت الرئيسة التي يزورها المستخدمون يومياً.

وعن ذلـك، قال جيـروم سـيجورا، المديـر الأول للأبحـاث فـي Malwarebytes: إن موظفـي

1. Cheryl Winokur Munk, Google searches are becoming a bigger target of cybercriminals with the rise of 'malvertising', SEP 2024. https://2u.pw/kMwKYC0Z