UNODC
مكتب الأمم المتحدة المعني بالمخدرات والجريمة

كوفيد-19
الاستجابة

كوفيد-١٩: تحليل التهديدات الإلكترونية

مكتب الأمم المتحدة المعني بالمخدرات والجريمة
الشرق الأوسط وشمال إفريقيا
التقييم والإجراءات

نظرة عامة على الاتجاهات الإجرامية الحالية عبر شبكة الإنترنت ذات الصلة بالجائحة في منطقة الشرق الأوسط وشمال إفريقيا وكيفية حماية الضحايا من محاولات الخداع والتدليس

برنامج مكافحة الجرائم الإلكترونية بالمكتب الإقليمي للشرق الأوسط وشمال إفريقيا

١ مايو/ايار ٢٠٢٠

كوفيد-١٩: تحليل التهديدات الإلكترونية

مقدمة

يعتبر يوم ١٧ نوفمبر ٢٠١٩ بداية لطريق طويل لما هو معروف الآن باسم وباء COVID-19[I]. لم يكن من الممكن توقع وصول الأمر لأزمة عالمية تتحدى كافة الطبقات الاجتماعية وجميع القطاعات الصناعية والتجارية والسكنية بالعالم. وقد أنتج عن ذلك الوباء الحديث تحديات جديدة أصبحنا نتوقعها في أوقات الأزمات. يعد تسونامي ٢٠٠٤ في آسيا وزلزال ٢٠١٠ في هايتي من الأمثلة الواضحة عن كيفية تفاعل السلوك البشري مع الأزمات الشديدة[II].

كلما ظهرت أزمة جديدة، يكون المجرمون أول من ينتهزون الفرصة لاستغلال الضحايا حسني النية في أوقات الخوف، وعدم اليقين والشك. يتخذ ذلك الاستغلال أشكالاً متعددة، من النطاق المادي إلى الرقمي. وقد أثبت التاريخ أن الطريقة الأكثر فاعلية لمواجهة تلك التهديدات هي الوقاية ورفع الوعي على جميع المستويات العملية والشخصية.

وفي هذا الصدد، أسفر الوباء عن تحدي كبير نادراً ما أثير من قبل. فهو وباء عالمي ويؤثر على الجميع بغض النظر عن الموقع الجغرافي، العِرق، الدين، الأصل الاجتماعي، الجنس، الإعاقة، الدخل أو أي وضع آخر. فبالرغم من كون بعض الفئات أكثر عرضة للخطر، قد تمتد دائرة الخطر لتصل الي عائلاتنا، أصدقائنا وزملاء العمل. وفي هذا السياق، يسعى المجرمون للاستفادة من تلك المخاوف. هذا التقرير سيسلط الضوء على معالجة الجانب الرقمي لتلك التهديدات وكيفية الحد من وقوع المزيد من الضحايا نتيجة لهذا الوباء.

منظور التهديدات الرقمية[III]

في خلال ٢٤ ساعة:
١٥ – ١٦ ابريل/نيسان ٢٠٢٠

١٧٠٣٨٧ بريد إلكتروني عشوائي يحمل عنوان "كورونا" او "" كوفيد-١٩

١٦٩٦٤ عنوان بروتوكول للإنترنت (IP address) مُستخدم لإرسال تلك الرسائل الإلكترونية.

٨٣٩١ نطاق إلكتروني (domain) مُستخدم لإرسال رسائل البريد الإلكتروني.

٥٨٣ من تلك الرسائل الإلكترونية تحمل مرفقات فاسدة إذا تم الضغط عليها يستطيع المهاجم التحكم بجهاز الضحية.

كل هذا تم خلال يوم واحد وبالتركيز على نوع واحد من التهديد. يمكنك الآن تصور مدى التأثير العالمي الذي قد يحدث.

جدول المحتويات

كوفيد-١٩: تحليل التهديدات الإلكترونية

ما هي التهديدات الرئيسية؟

سيركز هذا التقرير على التهديدات المستخدمة على نطاق واسع والتي يعاني منها العالم الرقمي في ظل تلك الأزمة والتحديات الجديدة في مجال مكافحة الجرائم الإلكترونية. ولازال الوقت مبكراً لتحديد مدى فاعلية تلك الهجمات ولكن من الممكن ان تكون عواقبها مُدمرة. فلابد من الأخذ في الاعتبار بأن معظم تلك الهجمات تستهدف أي مُستخدم لتكنولوجيا الانترنت حيث يتم استغلاله والتلاعب بمشاعره للإيقاع به. نرفق أدناه نظرة عامة عن مختلف الهجمات التي شوهدت يومياً وشرح بسيط عن أسلوب تلك الهجمات وأهدافها.

الحملات الخبيثة

رسائل البريد الالكتروني المخادعة

يعد البريد الالكتروني وسيظل أكبر ناقل لتهديد الأفراد والمنظمات. لطالما استخدم مجرمو شبكات الانترنت الأحداث الكبرى المعلن عنها على نطاق واسع في شن حملات التصيُّد للارتقاء بفاعلية هجومهم، ولا يعد هذا الوباء استثناءً من ذلك.

تعلن عدة مواقع ضارة على مواقع الشبكة المظلمة (Dark Web) عن مجموعات كوفيد-١٩ للتصيد الاحتيالي المكونة من بريد إلكتروني مرفق به خريطة وهمية لتفشي الفيروس بأسعار مختلفة يمكن أن تتراوح من ١٥٠ دولارًا إلى ١٠٠٠ دولار. يشتري مجرمو شبكات الانترنت تلك "المجموعات " لاستخدامها في حملات البريد الإلكتروني التي تستهدف الأفراد والمنظمات واسعة النطاق. تلك الهجمات أصبحت ممكنة نتيجة لأنظمة التشغيل الغير مُؤمنة واستخدام مرفق فاسد يقوم باستغلال نقاط الضعف بالحاسب الالي ويهاجمه.

يتم استخدام مواضيع متنوعة بتلك الرسائل الالكترونية لزيادة معدل الضغط على الروابط الالكترونية المخادعة والمستخدمة في تلك الحملة. وقد تظهر تلك الفيروسات باستخدام صورة من تقرير حول الوباء أو من خلال نصائح صحية من مصادر حكومية رسمية. بمجرد الضغط على الرابط او المرفق الفاسد، تتضمن تلك الفيروسات صور مختلفة لتدمير النظام مثل طلب فدية، رصد لوحة المفاتيح وصور أخرى من جمع المعلومات الشخصية.

كما يقوم المجرمون بالإعلان عن بيع أقنعة الوجه والمنتجات الأخرى ذات الصلة بانتشار فيروس كورونا بهدف الحصول على أكبر قدر من المعلومات من نظام الكومبيوتر الذي تم اختراقه وكذلك الحصول على بيانات بطاقة الائتمان في حال قام الضحية حسن النية بشراء المستلزمات الطبية المزورة.

يرسل المجرمون موجات عديدة من تلك الحملات والتي قد تتضمن أكثر من ١٥٠٠٠٠ الى ١٧٥٠٠٠ بريد الكتروني في المرة الواحدة. ونشهد يومياً حملات عديدة يتضمن أغلبها برامج ضارة تستغل الضحايا حسني النية للحصول على بيانات شخصية يمكن استخدامها في العديد من جرائم.

الحجم الحالي لرسائل البريد الالكتروني المخادعة ذات الصلة بفيروس كورونا يمثل أعلى معدل هجوم شهده مجال مكافحة الجرائم الالكترونية.

كوفيد-١٩: تحليل التهديدات الإلكترونية

هل تعلم؟

يستخدم مجرمو شبكات الانترنت موجة كوفيد-١٩الخلق واستغلال مخاوف الإصابة.. ولا تعد تلك الظاهرة بجديدة في مجال مكافحة الجرائم الالكترونية. لطالما استغل مجرمو شبكات الانترنت نتائج مزورة لتحليل فيروس نقص المناعة البشرية (HIV) لاستهداف مجال الرعايا الصحية، وشركات التأمين والأدوية عالمياً.

جائحة فيروس نقص المناعة البشرية /الإيدز (HIV/AIDS) (في قمته ٢٠٠٤ – ٢٠١٢)
عدد الوفيات: ٣٢ مليون
السبب: فيروس نقص المناعة البشرية /الإيدز

لقد أثبت فيروس نقص المناعة البشرية /الإيدز (HIV/AIDS) أنه جائحة عالمية، حيث قتل أكثر من ٣٢ مليون شخص منذ عام ١٩٨١. وقد انخفض المعدل السنوي للوفيات عالمياً بين عامي ٢٠٠٤ و٢٠١٢ من ١,٧ مليون الى ٧٧٠٠٠٠[IV].

الهجمات عبر الانترنت ذات الصلة بفيروس نقص المناعة البشرية (HIV/AIDS) تعد ضئيلة مقارنة بحجم الحملات التي تستغل حالة الذعر الناتجة عن فيروس كورونا.

تلك الحملات هي بمثابة تذكرة ان الهجمات الشرسة التي تستغل الأوبئة العالمية لم تبدأ ولن تتوقف عند أحدث الهجمات التي نشهدها بعنوان فيروس كورونا. إن مجرمو شبكات الانترنت يعملون في إطار استراتيجية متسقة حيث يدرك المهاجمون فائدة عامل الإنذار المتعلق بالصحة.. عادةً يحاولون إضافة الطابع الشخصي للبريد الالكتروني المُرسل في حملاتهم لإثارة فضول المتلقي. قد يتوصل الى البيانات الشخصية المذكورة في البريد الالكتروني عن طريق مصدر عام او إجراء سابق غير مشروع.

فإذا استقبلت بريد الكتروني من هذا القبيل، فلا تفتحه خاصة إذا كنت لا تتوقع أن تُرسل لك أية نتائج. بل قم بالاتصال بالطبيب الخاص بك مباشراً لمناقشة النتائج أو تحديد موعد متابعة لأي اختبارات قد تكون خضعت لها.

سيضمن ذلك عدم وقوعك كضحية لأي حملات إلكترونية محتملة.

نطاق إلكتروني مخادع (Malicious Domains)

تم تسجيل مواقع جديدة لنشر المعلومات ذات الصلة بالوباء. ومع ذلك، العديد من تلك المواقع يكون فخاً للضحايا حسني النية. ففي خلال الستة أسابيع السابقة، تم تسجيل مئات النطاقات الالكترونية ذات الصلة بـكوفيد-١٩ يومياً. ورغم كون بعضهم حقيقي ويوفر بيانات صحيحة دون سوء نية، فإن عدد كبير منهم تكون طبيعته مخادعة. بنهاية مارس /آذار ٢٠٢٠، تم تسجيل أكثر من ٩٠٠٠ نطاق الكتروني عن فيروس كورونا. تملك تلك المواقع الخبيثة صور مختلفة من الهجمات منها التالي:

انتحال هوية موقع رسمي

لقد أعلن المركز الوطني للأمن الالكتروني (NCSC) بالمملكة المتحدة تمكن مجرمو شبكات الانترنت من انتحال صفة موقع المركز الأمريكي لمكافحة الأمراض (CDC) بخلق نطاق الكتروني بأسماء مماثلة للعنوان الإلكتروني لمركزو لقرصنة كلمات المرور بالإضافة الى قيامهم بطلب تبرعات "بيتكوين" لتمويل لقاح مزور[v].

نشر البرامج الخبيثة

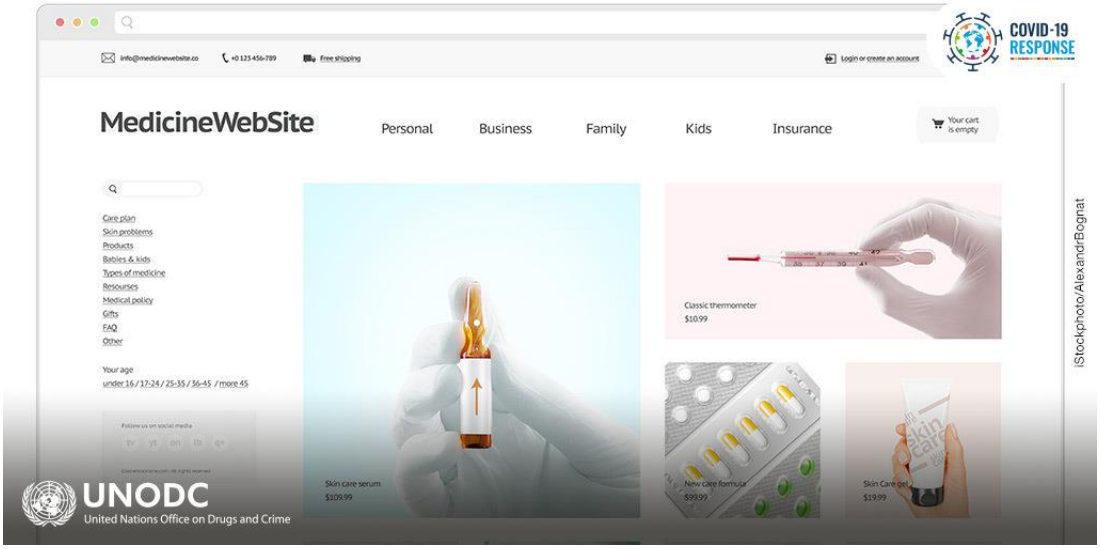
العديد من تلك العناوين الالكترونية تخلق صفحات يتم تحميلها عن طريق برامج خبيثة تم تصميمها لاستغلال نقاط الضعف بأنظمة تشغيل معينة. يمكن لتلك البرامج الخبيثة سرقة بيانات من أي نوع، بيانات بطاقات الائتمان، بيانات بنكية، بيانات حساسة للمتصفح واستخدامها لأغراض إجرامية. يمكن للبرامج الخبيثة أيضاً جمع محافظ العملات المشفرة، السيطرة على الكاميرات الالكترونية بدون تصريح، جمع البيانات المسجلة بالجهاز وتطبيق نظام رصد للوحة المفاتيح الذي يسجل كل ما يتم كتابته باستخدام لوحة مفاتيح النظام الذي تم اختراقه.

حملات وهمية

تروج المواقع الالكترونية ايضاً لخدمات ومنتجات عديدة وعادةً تطلب مساهمة المواطنين للقيام بذلك. مثلاً، موقع الكتروني يطلب من المستخدمين التبرع بقدرات حاسبتهم لصالح القيام ببحوث عن كوفيد-١٩لتقديم برامج خبيثة لسرقة البيانات[vi] .

بعبارات أكثر بساطة، التبرع بقدرات الحاسوب هو بمثابة السماح لشخص/كيان باستخدام القوة المعالجة لجهازك او حاسبك الالي الخاص بك للقيام ببعض العمليات الحسابية او أي مهام أخرى باستخدام جهازك. علماً بانه في السيناريو المذكور، التبرع بقدرات الحاسوب هو مجرد حجة لضمان سرقة بياناتك.

كوفيد-١٩: تحليل التهديدات الإلكترونية



التضليل

إن مفهوم المعلومات الخاطئة والتضليل ليس بجديد. وقد ساعد الوضع الحالي على انتشار تلك المعلومات المضللة من خلال جميع المنصات المجتمعية. حيث تخضع شريحة كبيرة من مستخدمي الانترنت للحجر المنزلي فزادت نسبة استخدامهم للإنترنت مما يسمح بإضافة ونشر وإعادة نشر المعلومات المضللة عبر أي وسيلة إعلام.

إن التقنيات المستخدمة معقدة جداً وقد تتخذ العديد من الصور. ففي الواقع، يمكن دمج أي من التقنيات المذكورة بالتقرير نظراً لترابطهم.
مثلاً، يستقبل موظف بمنظمة دولية كبيرة وبارزة رسالة بريد الكتروني مخادعة ويضغط على الرابط او المرفق بالبريد. أثار هذا الفعل تحريك التسلسل الذي يسمح بالارتقاء بفاعلية الحملة الالكترونية. فيصبح للمهاجم الان إمكانية الوصول للعديد من الحسابات التي يملكها الضحية غير المرتاب. فيستخدم المجرم تلك الحسابات لإرسال رسائل بريد الكتروني مخادعة او نشر معلومات خاطئة بمواقع التواصل الاجتماعي الخاصة بانتحال شخصية مسئول محترم في المجتمع الدولي مما يضيف مصداقية لتلك المعلومات المغلوطة التي تم نشرها عبر مختلف المنصات. يمكن لذلك المثال البسيط ان يتطور ويصبح معقداً إذا ما أصر المهاجم على الوصول لأهدافه.

ما هي أهداف التضليل؟

يوجد تعريفات عديدة لهذا المفهوم. عادةً، يكون الهدف هو التضليل لتدمير وكالة، كيان، شخص أو/والربح المالي أو المنفعة السياسية. كما يمكن استغلاله لزيادة عدد القراء عن طريق الإثارة، عدم الأمانة أو عناوين ملفقة صريحة. ففي زمن أصبح فيه زيادة عدد المتابعين أو القراء مصدر للربح المالي، يمكننا فهم الجهود المبذولة في التضليل خلال السنوات الأخيرة. أما فيما يخص هذا الوباء تحديداً، ونظراً لكونه مُتصدراً العناوين الرئيسية بالعالم، يطلق المضللين حملات خبيثة بخلق قصص وإرشادات خاطئة عبر كل القطاعات والمنصات المجتمعية للوصول لأهدافهم.

يوجد مواقع الكترونية تتحرى عن المعلومات الخاطئة ذات الصلة بكوفيد-١٩ ([vii], [viii]). ففي خلال فترة أكثر من شهر بقليل، تم فضح أكثر من خمسين مقالة وأثبتت أنها زائفة.. وقد أصبح من الصعب متابعة كم المعلومات الخاطئة ذات الصلة بالوضع الحالي. وهكذا أصبح من الأهمية البالغة التأكد من مصداقية مصدر المعلومات قبل اتخاذ أي إجراء ذو صلة بالخبر.

تعزيز استخدام مواقع التواصل الاجتماعي

ونظراً لاعتماد الكثير من الأشخاص على مواقع التواصل الاجتماعي للحصول على معلومات و للتواصل مع أصدقائهم وعائلاتهم، للعمل، والتسوق عبر الإنترنت والمزيد ، فقد تضاعف استخدام تلك المواقع كنتيجة لأزمة وباء كوفيد-١٩. كما هو مذكور أدناه، تُظهر الإحصائيات تلك الزيادة مما يساعدنا على فهم تأثير الحملات الخبيثة المشار اليها على الوضع الحالي. ذلك يتيح لمجرمون الانترنت الوصول لعدد كبير من الضحايا المحتملين من خلال محاولاتهم المستمرة في التحايل على الأشخاص والكيانات.

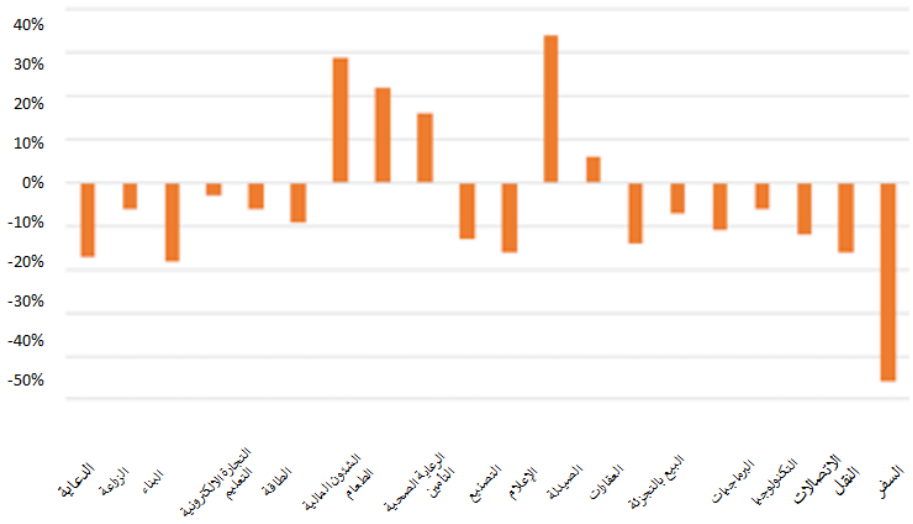
لقد تم جمع البيانات المذكورة بالإحصائيات المشار اليها أدناه عن طريق استطلاع رأي لأكثر من ٢٥٠٠٠ مستخدم في ٣٠ سوق خلال الفترة من ١٤ الى ٢٤ مارس ٢٠٢٠[ix].

شهد تطبيق واتساب (WhatsApp)زيادة في نسبة الاستخدام قدرها ٤٠٪. في بداية الأزمة زادت نسبة الاستخدام بمقدار ٢٧٪. ووصلت تلك الزيادة الى ٤١٪ في منتصف المرحلة من الوباء ووصلت نسبة استخدام تطبيق واتساب في الدول التي تعاني من مراحل متقدمة من الوباء الى ٥١٪.
في دول معينة، وصلت نسبة الاستخدام لدرجة أعلى بكثير. فقد وصلت نسبة استخدام التطبيق في إسبانيا الى ٧٦٪.

ولا تعد تلك الزيادة في نسبة الاستخدام على ذلك التطبيق فقط، فقد اثبتت دراسة ان تطبيقات "فيسبوك" (Facebook)، "إنستاجرام" (Instagram)، "وي شات" (WeChat) و "ويبو" (Weibo) قد شهدت زيادة في استخدامهم بنسبة ٤٠٪.

كوفيد-١٩: تحليل التهديدات الإلكترونية

نسبة استخدام مواقع التواصل الاجتماعي نتيجة لكوفيد-١٩



جدول ١ ([x])

وتجدر الإشارة الى انه رغم تلك الزيادة في نسبة استخدام مواقع التواصل الاجتماعي عالمياً، فقد أقر المستخدمين عدم ثقتهم في الأخبار الهامة المتعلقة بكوفيد-١٩ التي يتم نشرها عبر تلك المنصات وهو ما يتوجب الإثناء عليه حيث يظهر ان الغالبية العامة من المستخدمين على دراية بانتشار الأخبار الخاطئة عبر تلك الوسائل.
فاعتبر المجيبين على استطلاع الرأي ان قنوات البث الوطنية ومواقع الوكالات الحكومية خيارات أفضل ومصدر أخبار ومعلومات جدير بالثقة. فقط ١١٪ من المستخدمين اعتبروا مواقع التواصل الاجتماعي جديرة بالثقة[ix].

أبرز النتائج الإحصائية عن زيادة نسبة استخدام التطبيقات هي المكالمات الجماعية التي شهدت نسبة زيادة لأكثر من ١٠٠٠٪ خلال الشهر الماضي كما أعلنه تطبيق "فيسبوك ماسنجر" (Facebook Messenger) مما يثبت ان نسبة كبيرة من العالم تتبع إرشادات التباعد الاجتماعي بشكل صحيح.

نسبة التغيير في الإستخدام الشهري للانترنت المنزلي عبر الأجهزة الالكترونية

مقارنة بين 2019 و 2020 - معدل إستقبال الجيجابيت

	تليفزيون متصل بالانترنت	التحكم بالألعاب	الكمبيوتر	التليفون المحمول	مكبر صوت ذكي	جهاز /عصا الارسال	جهاز تابلت	المجموع
يناير	26%	6%	-3%	21%	7%	24%	18%	16%
فبراير	22%	12%	-5%	27%	-4%	21%	15%	16%
مارس	27%	12%	-4%	34%	30%	24%	12%	16%

comscore

Source: Comscore Total Home Panel Custom Reporting.
*March compares same 17-day period for both 2019 and 2020

جدول ٢

متوسط إستخدام الانترنت المنزلي عبر الأجهزة الالكترونية

معدل إستقبال الجيجابيت

	تليفزيون متصل بالانترنت	التحكم بالألعاب	الكمبيوتر	التليفون المحمول	مكبر صوت ذكي	جهاز /عصا الارسال	جهاز تابلت	المجموع
17-19 مارس 2019	2.6	3	1.4	0.7	0.1	3.9	0.4	12
15-17 مارس 2020	3.6	4.4	1.6	1	0.1	5.4	0.6	16.6
نسبة التغيير	37%	48%	15%	53%	44%	38%	33%	38%

comscore

Source: Comscore Total Home Panel Custom Reporting.
*March compares same 17-day period for both 2019 and 2020

جدول ٣

منظور إقليمي

لم تنجو منطقة الشرق الأوسط وشمال افريقيا من الهجمات الالكترونية. يستغل مجرمو شبكات الانترنت انشغال السلطات بعدم انتشار الوباء لمرحلة يصعب التحكم فيها. فينتهز المهاجمين فرصة قيام الحكومات بإعادة تعيين موظفين رئيسيين لضمان بقاء الأزمة الصحية تحت السيطرة. ذلك القسم سيسلط الضوء على أحداث مختلفة ظهرت بالمنطقة منذ انتشار الوباء عالمياً.

المخاطر الالكترونية بمنطقة الشرق الأوسط وشمال إفريقيا

البنية التحتية المصرفية والحكومية

وقعت العديد من الأحداث خلال الأسابيع الماضية مستهدفة البنية التحتية المصرفية والحكومية بالمنطقة. ونظراً لتقييد الخدمات كنتيجة لفرض حظر التجوال في دول عديدة بالمنطقة، شن مجرمو شبكات الانترنت هجمات عديدة على البنية التحتية الحيوية.

رغم عدم نجاح كل تلك الهجمات، فإن بعضها قد أتاح الفرصة لمجرمو شبكات الانترنت بخداع الضحايا في وقت أصبحت فيه المدخرات مهمة. تمكنت السلطات في بعض تلك الحالات من تحديد المشتبه بهم وإجراء تحقيقات.

مواقع التواصل الاجتماعي

ونظراً لخضوع الأشخاص للحجر الصحي في منازلهم، أصبح استخدام مواقع التواصل الاجتماعي وسيلة للترفيه. حوّل مجرمو شبكات الانترنت انتباههم لعدة تطبيقات مستخدمة على نطاق واسع بالمنطقة لشن هجمات مختلفة. مثلاً، يوم ١٥ ابريل ٢٠٢٠ شهد تطبيق "تيك توك" (Tiktok)، والذي ارتفعت نسبة استخدامه بالمنطقة بصورة استثنائية خلال الأسابيع الماضية، العديد من نقاط الضعف التي استغلها مجرمو شبكات الانترنت حيث تم إضافة مقاطع فيديو غير معتمدة وغير مصرح بها لحسابات الضحايا دون علمهم. جدير بالذكر ان العديد من المنظمات الإقليمية تستخدم ذلك التطبيق مما قد يترتب عليه انتشار معلومات خاطئة حول كوفيد-١٩.

استغلال المؤتمرات عبر الفيديو

ونظراً لخضوع معظم الدول بالمنطقة لحظر التجوال، أتاحت عدة منظمات إمكانية العمل من المنزل لموظفيها لمساعدة السلطات في تقليل العبء على قطاع الصحة للحد من انتقال عدوى فيروس كورونا. وحتى تستمر تلك الشركات في المضي قدماً بأنشطتهم، فقد استعانت باستخدام تطبيقات عبر الانترنت لانعقاد الاجتماعات وأي أنشطة أخرى لازمة.
وبالتالي يتربص مجرمو شبكات الانترنت لأي فرصة سانحة يمكن استغلالها بمختلف الجوانب لمجتمع الانترنت. مثلاً، بما أن معظم الدول قد بدأت الالتزام بمعايير التباعد المجتمعي، أصبح استخدام احدى التطبيقات شائعاً لعقد اجتماعات، مؤتمرات تليفونية ودورات تدريبية. أتاحت نقطة ضعف بذلك التطبيق الفرصة للمهاجمين التحكم كلياً بجلسة. حيث تمكن المجرم من اعتراض الصوت والفيديو لجميع الحضور بالاجتماع وعرض مضمون غير مرغوب فيه أثناء انعقاد المؤتمر او الدورة التدريبية. ومن البديهي ان تلك الاجتماعات قد تحتوي على معلومات سرية تم تسريبها او استغلالها بصورة إجرامية أخرى.

التأثير الإقليمي لكوفيد-١٩ [xi]

(إعتباراً من ٢١ ابريل ٢٠٢٠)

مجموع الحالات

١٤٣٣١٧

مجموع الوفيات

٦٦٥١

مجموع التحاليل التي تمت

١٩٩٢٤٢٠

التأثير العالمي لكوفيد-١٩

(اعتبارًا من ٢١ ابريل ٢٠٢٠)

مجموع الحالات

٢٥٢٩٧٠٧

مجموع الوفيات

١٧٤٦٨٣

مجموع التحاليل التي تمت

٢٢١٣٠٦٧٦

حملات التصيُّد الاحتيالي

كما كنا قد أشرنا من قبل، أصبحت رسائل البريد الإلكتروني المخادعة جزء من حياتنا منذ أواخر التسعينات ولم تشهد الأزمة الحالية سوى تدفق لتلك الهجمات. شهدت منطقة الشرق الأوسط وشمال افريقيا العديد من تلك الهجمات في مختلف الصناعات المحلية، الإقليمية او الدولية. فزادت أهمية الالتزام بالحرص الواجب عن أي وقت مضى، فإننا جميعاً نعتمد على المعلومات التي تم نشرها عبر الانترنت وعليه يلزم علينا التأكد بأن تلك البيانات التي نستخدمها أو نراها هي الصحيحة.

الاستجابة الإقليمية لمكتب الأمم المتحدة المعني بالمخدرات والجريمة

يقدم البرنامج الإقليمي لمكافحة الجريمة الالكترونية حالياً العديد من أنشطة الدعم التقني بالمنطقة. ويستجيب خبراء المكتب المتخصصون في مكافحة الجريمة الالكترونية للطلب المتزايد من الجهات المعنية في هذا الشأن بتوفير المعدات الملائمة، دورات تدريبية واستشارات.

وكما يمثل الوضع الحالي تحدي على كافة المستويات للحكومات، فقد تم تكييف الأنشطة وتوفير المعدات لتتناسب مع الوضع الراهن ولتلبية الاحتياجات الفورية لمختلف الوزارات الإقليمية ذات الصلة بتلك الأزمة التي يهتز لها العالم.

تواجه الحكومات العديد من المخاطر من الهجمات المحددة والموضحة بالتقرير. إن سرقة البيانات، نشر معلومات مضللة للجمهور، انخفاض الثقة ومشكلات السمعة ليست سوى بعض الأمثلة لتلك المخاطر التي يمكن ان يواجها أي كيان. لذلك، فلابد من الرد على تلك الهجمات مما يضمن الحد من الآثار الناتجة عن سعي مجرمو شبكة الانترنت لزعزعة ثقة الجمهور وتحقيق منفعة مادية.

الخطط المستقبلية

خطط برنامج مكافحة الجريمة الالكترونية الإقليمي بالشرق الأوسط وشمال إفريقيا للقيام بالعديد من الأنشطة والمشتريات خلال الأشهر القادمة لتعزيز قدرات الدول على مواجهة أزمة كوفيد-١٩ بشكل أكثر فاعلية من المنظور الرقمي.

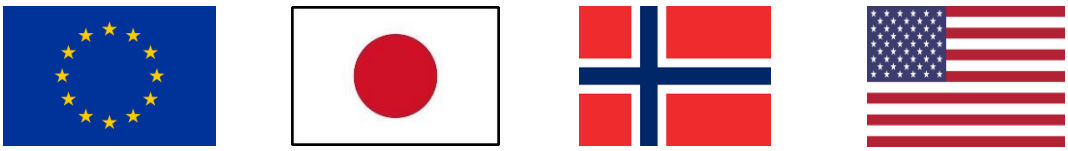
قد تتخذ تلك الاستجابة الأشكال التالية:

- الارتقاء بمستوى الأمن التكنولوجي بالبنية التحتية الحيوية على المستوى الوطني
- تطوير إجراءات التشغيل الموحدة لضمان استجابة رقمية مثلى
- توفير تدريبات معترف بها دولياً للمستجيبين الأوائل والمسئولين بالحكومات
- شراء معدات طب شرعي رقمي لضمان كفاءة التحقيق عن الهجمات الالكترونية المختلفة في السياق الحالي
- تقييم الاحتياجات والتنسيق الإقليمي لتقديم الدعم
- تحقيقات الجرائم الالكترونية المتخصصة لمنع المزيد من الهجمات
- استجابة الطب الشرعي الرقمي لمواقع الجرائم مختلفة او تتبع البيانات
- مراجعة واستشارات تشريعية
- دعم التعاون الدولي
- حملات توعية بمواقع التواصل الاجتماعي عن مشكلات محددة ذات صلة بالوباء

في الوقت الحالي، هناك حاجة فورية لتلك الأنشطة لدعم البلدان لضمان الارتقاء بدرجة استجابة حول العالم

وكما هو موضح في مبادرة البرنامج العالمي لمكافحة الجريمة الالكترونية التابع لمكتب الأمم المتحدة المعني بالمخدرات والجريمة، "الآن ليس الوقت المناسب لإلغاء الاستثمار في ضباط انفاذ القانون المتخصصين في مكافحة الجرائم الالكترونية. تعد القدرة على مواجهة الجريمة الالكترونية من العناصر الحيوية لحماية البنية التحتية الوطنية مهمة للغاية وذلك للحفاظ على أمن الأطفال عبر الانترنت، دعم الصناعة، تأمين المستشفيات ودعم الانتعاش الاقتصادي في اعقاب كوفيد-١٩[xii].

يتوجه فريق برنامج مكافحة الجريمة الالكترونية بالمكتب الاقليمي للأمم المتحدة المعني بالمخدرات والجريمة في الشرق الأوسط وشمال افريقيا بخالص الشكر للاتحاد الأوروبي، حكومة اليابان، مملكة النرويج والولايات المتحدة الأمريكية على دعمهم الذي جعل الجهود المذكورة أعلاه ممكنة.



المساهمين

المساهمين الرئيسين للتقرير هم فريق برنامج مكافحة الجريمة الالكترونية بمكتب الأمم المتحدة المعني بالمخدرات والجريمة للشرق الأوسط وشمال افريقيا

باتريك بوامونيو، patrick.boismenu@un.org
المستشار الإقليمي لمكافحة الجريمة الالكترونية بالمكتب ومنسق البرنامج

مصطفى البنا، mostafa.elbanna@un.org
المسئول الإقليمي لبرنامج مكافحة الجريمة الالكترونية

صادق بن رجب، sadok.benrejeb@un.org
المسئول الوطني لبرنامج مكافحة الجريمة الالكترونية بتونس

ندى فراج، nada.farrag@un.org
المساعد الإداري لبرنامج مكافحة الجريمة الالكترونية

مادة مرجعية

I. دوبيوبتي براهما، سيكيم تشاكرابورتي وأرادهيكا مينوكي، *بداية الوباء العالمي: جدول زمني لانتشار COVID-19 وتدخل الحكومات* (٢ ابريل ٢٠٢٠)
II. البرنامج الإقليمي لمكتب الأمم المتحدة المعني بالمخدرات والجريمة للشرق الأوسط وشمال افريقيا، *كيفية البقاء آمناً من COVID-19 استغلال مجرمو شبكات الانترنت للوباء* (مارس ٢٠٢٠)
III. RiskIQ، RiskIQ i3: *المستحدثات اليومية ل COVID-19* (١٥ ابريل ٢٠٢٠)
IV. برنامج الأمم المتحدة المشترك المعنى بالإيدز، *بيان حقائق – اليوم العالمي لمرضي الإيدز ٢٠١٩* (١ ديسمبر ٢٠١٩)
V. المركز الوطني للأمن الالكتروني بالمملكة المتحدة، *تدخل خبراء التكنولوجيا لمواجهة سعي المجرمون لإستغلال المخاوف الناتجة عن فيروس كورونا* (١٦ مارس ٢٠٢٠)
VI. جيرمي ه.، أكسيل ف. وفريق بروفبوينت لمراقبة التهديدات، *انتشار RedLine Stealer جديد بإستخدام حملات بريد اليكتروني عن موضوع فيروس كورونا* (١٦ مارس ٢٠٢٠)
VII. جاين ليتفينينكو، *قائمة مستحدثة عن التضليلات المنتشرة حول فيروس كورونا* (٢٤ مارس ٢٠٢٠)
VIII. جاين ليتفينينكو، *قائمة بالتضليلات التي انتشرت حول فيروس كورونا في الأسابيع الأولى* (٢ مارس ٢٠٢٠)
IX. سارة بيريز، تقرير: *شهد تطبيق WhatsApp زيادة في نسبة الإستخدام بمعدل ٤٠٪ نتيجة لوباء COVID-19* (٢٦ مارس ٢٠٢٠)
X. نايل باتيل، *ماذا يعني فيروس كورونا COVID-19 للمسوقين* (١٥ ابريل ٢٠٢٠)
XI. Worldometer، *وباء فيروس كورونا COVID-19* (٢١ ابريل ٢٠٢٠)
XII. البرنامج العالمي لمكافحة الجريمة الالكترونية التابع لمكتب بمكتب الأمم المتحدة المعني بالمخدرات والجريمة، الجريمة الالكترونية و *COVID-19: المخاطر والاستجابات* (١٤ ابريل ٢٠٢٠)