الإنتربول

الجريمة السيبرية

كوفيد - 19 تقرير تقييم

آب/أغسطس 2020

INTERPOL General Secretariat
200, quai Charles de Gaulle
69006 Lyon
France

Web: www.interpol.int
E-mail: info@INTERPOL.int

المحتويات

مقدمة

يؤثر وباء فيروس كورونا غير المسبوق تأثيرا بالغا في مشهد التهديدات السيبرية في العالم. وتفاقم الأزمة الصحية العالمية المصحوب بزيادة حادة في الأنشطة الجنائية السيبرية المرتبطة بكوفيد - 19 يفرض ضغوطا شديدة على أجهزة إنفاذ القانون في العالم أجمع. ووفقا لأحد شركاء الإنتربول من القطاع الخاص[1]، بين كانون الثاني/يناير و24 نيسان/أبريل 2020، كُشفت 907 000 رسالة احتيالية و737 حادثا على صلة ببرمجيات خبيثة و 48 000 موقع إلكتروني موبوء – جمعيها مرتبطة بكوفيد - 19.

ولإلحاق أكبر قدر من الضرر وتحقيق أقصى ما يمكن من أرباح مالية، يتحول مرتكبو الجرائم السيبرية عن استهداف الأفراد والشركات الصغيرة إلى المؤسسات الكبرى والحكومات والبنى التحتية الحساسة التي تضطلع بدور حيوي في مكافحة تفشّي الوباء. وفي موازاة ذلك، بسبب الانتقال المفاجئ والضروري على الصعيد العالمي إلى العمل عن بُعد، اضطرت المنظمات إلى أن تقيم بسرعة منظومات وشبكات وتطبيقات مخصصة لهذا الغرض. لذا، يستغل المجرمون تزايد مكامن الضعف الأمنية الناجمة عن العمل عن بُعد لسرقة البيانات وتحقيق الأرباح وزرع الفوضى.

وفي ضوء هذه الأحداث، أعدت إدارة الإنتربول لمكافحة الجريمة السيبرية تقرير التقييم العالمي هذا عن الجريمة السيبرية المرتبطة بكوفيد - 19 بفضل إمكان وصولها الفريد من نوعه إلى بيانات من البلدان الأعضاء الـ 194 ومن الشركاء في القطاع الخاص من أجل تقديم لمحة عامة شاملة عن وضع الجريمة السيبرية في خضمّ الوباء. ويستند التقرير إلى البيانات التي جُمعت من البلدان الأعضاء وشركاء المنظمة من القطاع الخاص في إطار استقصاء الإنتربول العالمي في مجال الجريمة السيبرية الذي أُجري في نيسان/أبريل وأيار/مايو 2020. وفي المجمل، أجاب 48 من أصل 194 بلدا عضوا على الاستقصاء وأسهم 4 من أصل 13 من الشركاء في القطاع الخاص ببياناته في التقرير.

الشكل 1. استقصاء الإنتربول العالمي في مجال الجريمة السيبرية:
توزيع الجهات المجيبة على الاستقصاء بحسب المناطق

1. شركة Trend Micro، جرت زيارة الموقع وأُخذت منه المعلومات في 27 أيار/مايو 2020 على العنوان التالي:
https://www.trendmicro.com/vinfo/fr/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains

وشُفعت نتائج التحليل بمعلومات وفرها شركاء من القطاع الخاص وأفرقة الإنتربول الإقليمية العاملة المعنية بمكافحة الجريمة السيبرية. ويشتمل هذا التقرير أيضا على معلومات وتحليلات أصدرتها وحدة الإنتربول لمواجهة التهديدات السيبرية والمركز المتعدد الاختصاصات التابع لها – وهو فريق من أفراد إنفاذ القانون وخبراء القطاع الخاص مقام في سنغافورة. وترد أدناه النتائج الرئيسية المتعلقة بمشهد الجريمة السيبرية المرتبط بوباء كوفيد- 19:

الاحتيال الإلكتروني ومواقع التصيّد الاحتيالي

أعادت الجهات مصدر التهديد النظر في خططها المعتادة المرتبطة بعمليات الاحتيال الإلكترونية ومواقع التصيّد الاحتيالي مستغلة الوباء كفرصة لتعزيز إمكانات نجاح اعتداءاتها. ومن خلال بثّ رسائل إلكترونية احتيالية مرتبطة بكوفيد19- ينتحلون فيها صفة السلطات الحكومية والصحية، يستدرج مرتكبو الجرائم السيبرية ضحاياهم إلى تزويدهم ببياناتهم الشخصية وإلى تنزيل محتويات خبيثة.

البرمجيات الخبيثة التخريبية (برمجيات انتزاع الفدية وهجمات تعطيل الخدمة DDoS)

يستخدم مرتكبو الجرائم السيبرية باطّراد برمجيات خبيثة لتعطيل البنى التحتية الحيوية ومؤسسات الرعاية الصحية، بسبب تأثيرها السلبي الكبير والأرباح المالية التي تدرّها. ويمكن أن تؤدي برمجيات انتزاع الفدية أو هجمات تعطيل الخدمة DDoS إلى إحداث أعطال منتظمة أو توقف كامل للأعمال وضياع معلومات بالغة الأهمية بشكل مؤقت أو دائم.

البرمجيات الخبيثة لجمع البيانات

يتزايد أيضا استخدام مرتكبي الجرائم السيبرية برمجياتٍ خبيثة لجمع البيانات مثل أحصنة طروادة للتسلل عن بُعد، وبرمجيات سرقة المعلومات، وبرمجيات التجسس، وأحصنة طروادة المصرفية. وتتغلغل الجهات مصدر التهديد في المنظومات الحاسوبية باستخدام المعلومات المرتبطة بكوفيد – 19 كطُعم لتعطيل الشبكات وسرقة البيانات واختلاس الأموال وزرع برمجيات "بوتنت" الخبيثة.

النطاقات الخبيثة

تزايد بشكل ملحوظ عدد مرتكبي الجرائم السيبرية الذين يستغلون اشتداد الطلب على الإمدادات الطبية والمعلومات المرتبطة بكوفيد – 19 لتسجيل أسماء نطاقات تحتوي على كلمات رئيسية ذات صلة بالوباء مثل "coronavirus" أو "COVID". وتُخفي هذه المواقع الاحتيالية مجموعة واسعة من الأنشطة الخبيثة، ولا سيما خواديم C2 وبرمجيات خبيثة ومواقع تصيّد احتيالي.

المعلومات المضللة

يتفشّى بين عامة الناس قدر متزايد من المعلومات المضللة والأخبار الكاذبة. وهذه المعلومات غير الموثوقة، والتهديدات المغلوط فهمها، ونظريات المؤامرة التي تذكيها أوضاع اجتماعية واقتصادية مضطربة في العالم قد أسهمت في بثّ القلق في المجتمعات السكانية وسهّلت في بعض الحالات تنفيذ هجمات سيبرية.

تغير اتجاهات الجريمة السيبرية وتهديداتها في خضم كوفيد - 19

اتجاهات الجريمة السيبرية على المستوى الإقليمي

بينما استفحلت الجريمة السيبرية في أرجاء العالم خلال وباء كوفيد - 19، تختلف الاتجاهات الجنائية باختلاف المناطق. وترد أدناه لمحة عامة عن مشهد التهديدات السيبرية المرتبطة بكوفيد - 19 على الصعيد الإقليمي.

أفريقيا

- أكدت الجهات المجيبة على الاستقصاء من البلدان الأفريقية الأعضاء تزايد استخدام عمليات الدفع الإلكتروني أو غير النقدي منذ بداية الوباء، ما جعل عامة الناس أكثر عرضة للاعتداءات السيبرية.
- بالنظر إلى تطبيق معظم المنظمات والشركات سياسةً للعمل من المنزل، أسفرت هشاشة الترتيبات المتخذة في هذا الصدد عن ارتفاع حاد في مجالات إجرامية محددة مثل التصيّد الاحتيالي والابتزاز الجنسي والاحتيال في مجال الأعمال خيرية.
- تزايد تداول الأخبار الكاذبة المرتبطة بكوفيد - 19 في وسائل التواصل الاجتماعي.
- انخفضت نسبيا الأنشطة المنفذة في إطار شراكات بين القطاعين العام والخاص لمكافحة الجرائم السيبرية، ما أسهم في تزايد قضايا الجرائم السيبرية التي لم تُسوَّ بعد.

الأمريكتان

- أفادت الجهات المجيبة على الاستبيان بارتفاع حاد في حالات التصيّد الاحتيالي وحملات التضليل المرتبطة بكوفيد19- التي تستغل الأزمة الناجمة عن فيروس كورونا والحَجْر الصحي الذي أعقبها.
- بما أن الكثير من الشركات في الأمريكتين قد طبقت سياسة العمل عن بُعد، يستهدف مرتكبو الجرائم السيبرية أكثر فأكثر الموظفين بهدف دخول شبكات هذه الشركات عن بعد وسرقة معلومات حساسة.
- تُنفَّذ حاليا حملة لانتزاع الفدية عن طريق برمجية LOCKBIT بشكل رئيسي تستهدف شركات متوسطة الحجم في بعض بلدان هذه المنطقة.
- يستخدم المجرمون وسائل التواصل الاجتماعي استخداما متزايدا من أجل استغلال الأطفال جنسيا على الإنترنت. وبشكل خاص، يقوم جناة ناشطون على الشبكات الإلكترونية للاعتداء الجنسي على الأطفال بتحديد مواقع ضحاياهم ويتصلون بهم عن طريق وسائل التواصل الاجتماعي مستغلين الحَجْر الصحي المفروض عالميا. وفي الوقت نفسه، تفاقمت تجارة صور الاستغلال الجنسي للأطفال.

آسيا وجنوب المحيط الهادئ

- من الاتجاهات الإقليمية البارزة في آسيا وجنوب المحيط الهادئ حملات احتيال وتصيّد احتيالي مرتبطة بكوفيد – 19 وكذلك بيع لوازم طبية مقلدة وعقاقير ومعدات الوقاية الشخصية بطريقة غير مشروعة على الإنترنت.
- يستغل مرتكبو الجرائم السيبرية نقاط الضعف الأمنية في أدوات التداول عن بُعد.
- أفادت معظم البلدان الأعضاء في آسيا وجنوب المحيط الهادئ المشاركة في الاستقصاء بتداول أخبار ملفقة ومعلومات مضلِّلة ذات صلة بكوفيد – 19.
- أُشير إلى أن نقص التوعية بالأمن السيبري والوقاية الصحية بصفته أحد التحديات الرئيسية في هذه المنطقة.

أوروبا

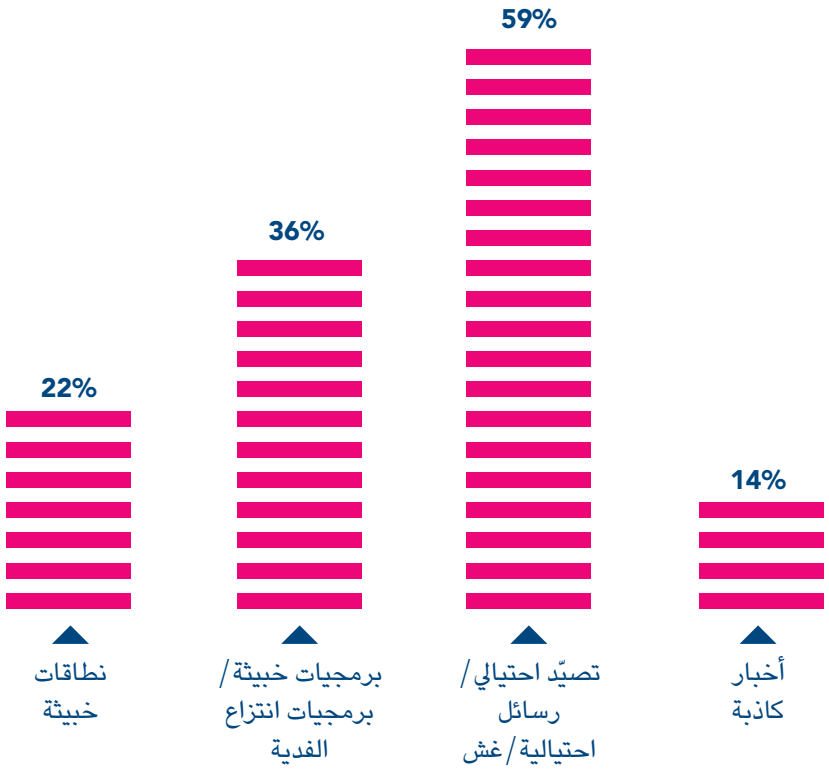
- أفاد ثلثا البلدان الأعضاء من أوروبا بزيادة ملحوظة في عدد النطاقات الخبيثة المسجلة بالكلمتين الرئيسيتين 'COVID' أو 'corona' من أجل استغلال تزايد عدد الأشخاص الباحثين عن معلومات عن كوفيد – 19 على الإنترنت.
- يستغل مرتكبو الجرائم السيبرية الوباء لبثّ برمجية انتزاع الفدية بهدف تعطيل البنى التحية الحساسة ومؤسسات الرعاية الصحية المسؤولة عن مكافحة كوفيد – 19
- يتزايد استنساخ مواقع إلكترونية حكومية رسمية من أجل سرقة بيانات حساسة لمستخدمين يمكن تسخيرها لاحقا في اعتداءات سيبرية أخرى.
- تسجل أجهزة إنفاذ القانون في أوروبا هجمات تصيّد احتيالي واسعة النطاق.

الشرق الأوسط وشمال أفريقيا

- شددت هذه المنطقة على تنامي استخدام وسائل التواصل الاجتماعي لنشر أخبار كاذبة ذات صلة بكوفيد – 19.
- يتكرر استخدام منصات التواصل الاجتماعي للبيع غير المشروع لمنتجات صيدلانية وشبه صيدلانية مرتبطة بفيروس كورونا.
- ازداد تسجيل نطاقات خبيثة تدعي أنها تقدم إحصاءات عن كوفيد – 19.
- ازداد عدد مواقع التصيّد الاحتيالي والغش الإلكتروني المرتبطة بوباء كوفيد – 19.

التهديدات السيبرية الرئيسية المرتبطة بكوفيد - 19

استنادا إلى تحليل شامل للبيانات الواردة من البلدان الأعضاء، والشركاء من القطاع الخاص، والمركز المتعدد الاختصاصات لمكافحة الجريمة السيبرية، كُشفت التهديدات السيبرية التالية باعتبارها مخاطر رئيسية مرتبطة بوباء كوفيد - 19.



الشكل 2. توزّع التهديدات السيبرية الرئيسية الناجمة عن كوفيد19-
استنادا إلى تعليقات البلدان الأعضاء

الاحتيال الإلكتروني والتصيّد الاحتيالي

أفاد ثلثا البلدان الأعضاء المجيبة على الاستقصاء باستخدام واسع النطاق لمواضيع مرتبطة بكوفيد - 19 في أعمال تصيّد احتيالي وغش على الإنترنت منذ تفشّي الوباء. ومنذ كانون الثاني/يناير 2020، كشف أحد شركاء الإنتربول من القطاع الخاص، وهو شركة Trend Micro، 907 000 رسالة مرتبطة بكوفيد - 19[2]. وحسّن مرتكبو الجرائم السيبرية أساليب الهندسة الاجتماعية التي يتبعونها باستخدام كوفيد - 19 كأساس لشن اعتداءاتهم مستغلين الركود الاقتصادي وحالة القلق لدى الناس خلال الوباء. وعلى وجه الخصوص، غيّر العديد من جماعات الجريمة المنظمة أساليبه الإجرامية لاستغلال التطورات المتعلقة بالوباء والنقص في الإمدادات وكذلك للترويج لأدوية مقلدة وحِزَم ضريبية وتحقيق مكاسب عاجلة.

2. شركة Trend Micro، جرت زيارة الموقع وأُخذت منه المعلومات في 19 نيسان/أبريل 2020 على العنوان التالي:
https://www.trendmicro.com/vinfo/fr/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains

وشملت نسبة كبيرة من الحوادث التي أُبلغت بها سلطات إنفاذ القانون جهاتٍ مصدر تهديد كانت توجّه رسائل تصيّد احتيالي مرتبطة بكوفيد - 19 تدعو المستخدمين إلى تزويدها بمعلومات تسجيل الدخول وكلمات السر. وغالبا ما كانت تُنتحل في هذه الرسائل الإلكترونية صفة موظفين حكوميين أو في الهيئات الطبية يدّعون تقديم معلومات وتوصيات تتعلق بالوباء. وبالإضافة إلى هذه الصلات المباشرة بالأخبار عن الوباء، سلّط شريك للإنتربول هو شركة Kaspersky الضوء على جهات مصدر تهديد تستخدم تخفيضات ضريبية مرتبطة بكوفيد - 19 لاستدراج المستخدمين عن طريق الخداع إلى تصفح موقع إلكتروني احتيالي يجمع معلوماتهم المالية والضريبية دون علمهم.

وتضمنت رسائل التصيّد الاحتيالي المرسلة زعماً من وزارات الصحة ومنظمة الصحة العالمية ملفات مرفَقة خبيثة تستغل نقاط الضعف الحاسوبية من أجل تشغيل رمز خبيث. وقد أفادت بلدان أعضاء وشركاء للإنتربول من القطاع الخاص بأن برمجيات مثل Emotet وTrickbot وCerberus المصممة خصيصا لسرقة المعلومات تُستخدم على نطاق واسع في رسائل إلكترونية احتيالية.

وتشير معلومات واردة من شركاء في القطاع الخاص إلى أن الاحتيال بالبريد الإلكتروني المهني يظل أسلوب الغش المفضل للكثير من الجهات مصدر التهديد. وجرى تكييف الأساليب الاحتيالية مع السياق الحالي المرتبط بكوفيد - 19 الاستيلاء على عناوين البريد الإلكتروني للمورّدين والزبائن أو استخدام عناوين شديدة الشبه بها - من أجل شن الاعتداءات. وتشكل الحاجة الملحّة إلى الإمدادات الأساسية ومنتجات الرعاية الصحية فرصة مثالية للمجرمين لجمع المعلومات أو اختلاس ملايين الدولارات من أموال المشتريات العامة وتحويلها إلى حسابات غير مشروعة.

ووفقا للمعلومات الواردة من البلدان الأعضاء والشركاء في القطاع الخاص، تشتمل أهم أساليب التصيّد الاحتيالي المرتبطة بكوفيد - 19 على ما يلي:

- رسائل إلكترونية واردة من السلطات الصحية الوطنية أو العالمية؛
- أوامر حكومية ومبادرات دعم مالي؛
- طلبات دفع مزورة وإرجاع أموال؛
- عروض لقاح وإمدادات طبية؛
- تطبيقات هواتف نقالة لتعقب كوفيد - 19؛
- عروض استثمارات وأسهم مالية؛
- طلبات هبات وصدقات مرتبطة بكوفيد - 19.

وفي المجمل، بالنظر إلى كوفيد - 19 وما استتبعه من حَجْر صحي، يكتسب التصيّد الاحتيالي المرتبط بفيروس كورونا زخما ويستغل المخاوف ويستقطب اهتمام الأشخاص المستضعفين ويستغل اضطراب مراكز العمل.

البرمجيات الخبيثة التخريبية (برمجيات انتزاع الفدية وهجمات تعطيل الخدمة DDoS)

يتزايد عدد الاعتداءات باستخدام البرمجيات الخبيثة وتتغير أهدافها بعد أن تكيّفت مع تفشّي فيروس كورونا. واستنادا إلى التحليلات التي يجريها المركز المتعدد الاختصاصات لمكافحة

الجريمة السيبرية والدعم الذي يقدمه للبلدان الأعضاء، تحوّل التركيز الرئيسي لهذه الاعتداءات من الأفراد والشركات الصغيرة إلى الأجهزة الحكومية وقطاع الرعاية الصحية التي يمكن مطالبتها بمبالغ مالية أكبر.

وأفادت عدة بلدان أعضاء باعتداءات بالبرمجيات الخبيثة على البنى التحتية الحيوية لمنظمات حكومية ومستشفيات ومراكز طبية تجاوزت الأزمة الطبية طاقاتها. وتهدف الاعتداءات بهذه البرمجيات إلى حجب البيانات أو تعطيل المنظومات، ما يسهم في استفحال وضع مأسوي أساسا.

ووفقا للمركز المتعدد الاختصاصات، سُجِّلت في الأسبوعين الأولين من نيسان/أبريل 2020 زيادة حادة في الاعتداءات ببرمجيات انتزاع الفدية التي شنتها مجموعات كانت هامدة نسبيا في الأشهر القليلة الماضية. ويشير ذلك إلى احتمال إصابة منظمات بهذه البرمجية ولكن دون تفعيلها بعد. وتشير تحقيقات أجهزة إنفاذ القانون إلى أن مرتكبي الاعتداءات، بعد أن رصدوا بتعمق شبكات المنظمات التي استهدفوها، قدّروا بدقة كبيرة أعلى مبلغ للفدية يمكنهم المطالبة به. وعند بثّ البرمجية الخبيثة في أماكن استراتيجية في الشبكة تتسبب في تعطيل سير الأعمال إلى أقصى حد، تجد المنظمات المعنية نفسها مرغمة في الغالب على دفع الفدية. ويمكن أن يرافق هذه الاعتداءات استخراج معلومات حساسة قد تُستخدم لاحقا لممارسة المزيد من الضغط من أجل دفع الفدية.

وأهم البرمجيات الخبيثة اكتشفها مؤخرا شركاء الإنتربول من القطاع الخاص هي CERBER وNetWalker وRyuk. وهي تتطور باستمرار لإلحاق أكبر ضرر ممكن بضربة واحدة وتعزيز الأرباح التي يجنيها مرتكبوها إلى أقصى حد أيضا.

وعلى غرار الاعتداءات ببرمجيات انتزاع الفدية، ازداد عدد هجمات تعطيل الخدمة DDoS التي أُبلغ المركز المذكور بها والتي استهدفت تعطيل عمل مختلف المنظمات والمرافق الحساسة. ويهدد مرتكبو الجرائم السيبرية بتخريب المواقع الإلكترونية التي يستهدفونها إذا لم يُحوّل المال إلى حساباتهم، وذلك من خلال تحميل بوابات الخدمات على الإنترنت تبادلاتٍ إلكترونية تفوق قدرة الخادوم أو الشبكة على المعاملة.

وتختلف في النهاية تبعات الاعتداءات ببرمجيات انتزاع الفدية أو برمجيات DDoS ويمكن أن تشمل تعطيل العمليات وإغلاق منظومات حساسة وضياع بيانات، ما يُلحق خسائر مالية ناجمة عن وقت التوقف عن العمل واسترداد المنظومات والملفات.

النطاقات الخبيثة

يرصد أكثر من ثلث البلدان الأعضاء تزايدا في عدد النطاقات المسجلة حديثا التي تُستخدَم في تسجيلهما كلمتان أساسيتان هما "COVID" أو "Corona". وعلى غرار مواقع التصيّد الاحتيالي المرتبط بكوفيد - 19، تُستخدم نسبة كبيرة من النطاقات التي تدّعي تقديم معلومات محدثة عن الوباء أو منظومات لتعقبه أو إحصاءات عنه من أجل تنفيذ عدد كبير متنوع من الأنشطة الخبيثة التي تستغل تعطش العامة للمعلومات خلال الوباء. وفي نهاية آذار/مارس 2020، كُشف 357 116 نطاقا حديث التسجيل مرتبطا بكوفيد - 19، وتبيّن أن 022 2 منها يحتوي على برمجيات خبيثة و261 40 هي نطاقات "شديدة الخطورة"[3]، وفي حزيران/يونيو 2020، كشفت

3. شركة Palo Alto Networs، جرت زيارة الموقع وأُخذت منه المعلومات في 6 تموز/يوليو 2020 على العنوان التالي: https://unit42.paloaltonetworks.com/how-cybercriminals-prey-on-the-covid-19-pandemic/

فرقة العمل العالمية المعنية بالنطاقات الخبيثة التابعة لإدارة الإنتربول لمكافحة الجريمة السيبرية 200 000 نطاق خبيث في أكثر من 80 بلدا عضوا وقامت بتحليلها.

وتؤوي النطاقات الخبيثة المسجلة حديثا برمجيات خبيثة لجمع البيانات أو هي مصممة للحصول على معلومات شخصية بالاتصال بالضحايا بوسائل احتيالية عن طريق البريد الإلكتروني أو الرسائل النصية القصيرة أو الاتصالات الهاتفية المغفَلة المباشرة. وبين شباط/فبراير وآذار/مارس 2020، كشفت شركة Palo Alto Networks، أحد شركاء الإنتربول من القطاع الخاص، زيادة بنسبة 569 في المائة لتسجيلات خبيثة مرتبطة بشكل خاص ببرمجيات خبيثة ومواقع تصيّد احتيالي، وزيادة بنسبة 788 في المائة لتسجيلات شديدة الخطورة متصلة على سبيل المثال بالاحتيال وتعدين العملات المشفرة بدون ترخيص، وتتعلق بنطاقات مقترنة بصفحات ويب خبيثة. وهذه الزيادة في التسجيلات أعقبت بلوغ اهتمام المستخدمين بمواضيع ذات صلة بكوفيد19- ذروته، وقد كشف تطبيق Google Trends هذا الاهتمام متأخرا بضعة أيام[4].

وشددت تعليقات أخرى واردة من أجهزة إنفاذ القانون على أن بعض المواقع الإلكترونية الخبيثة قد استُحدثت لمحاكاة مرافق رسمية عامة تشمل بوابات حكومية، وشركات اتصالات، ومصارف، وسلطات وطنية معنية بالضريبة والجمارك وغيرها. وعرض بلد عضو مثالا على هذا التوجه تمثل في استغلال مبادرة وطنية لتوفير دعم مالي سريع لأصحاب المهن الحرة وصغار الشركات. ولتلقّي هذه المساعدة، طُلب من الشركات تقديم طلباتها عن طريق مواقع إلكترونية حكومية رسمية. ونسخت الجهات مصدر التهديد بسرعة هذه المواقع وبثّت تطبيقا مزيفا لجمع البيانات الشخصية التي أحالها مقدمو الطلبات.

ومن مصادر القلق الأخرى تزايد عدد المواقع الإلكترونية الاحتيالية التي استغلت اشتداد الطلب مؤخرا على الكمامات الجراحية ومعدات الوقاية الشخصية ومجموعات اختبار فيروس كورونا وأجهزة التنفس الطبية للاتجار غير المشروع بهذه المواد الأساسية. وتختلف الأساليب التي يتبعها أصحاب هذه المواقع وتشمل نسخَ مواقع مشروعة أو بيع سلع غير مرخص بها أو منتجات مقلدة أو تلقّي أثمان سلع دون تسليمها. وبالإضافة إلى ذلك، تُطرَح مشكلة عندما يُحوَّل المال الذي دفعه ضحايا الاتجار غير المشروع إلى حساب مصرفي في الخارج، ما يجعل من الصعب إسناد الجريمة واسترداد الخسائر المالية كليهما.

البرمجيات الخبيثة لجمع البيانات

أظهر الاستقصاء العالمي في مجال الجريمة السيبرية تركيزا شديدا على استخدام البرمجيات الخبيثة لجمع البيانات تحت غطاء توفير معلومات متصلة بكوفيد - 19. فالجهات مصدر التهديد تضل المستخدمين وتستدرجهم لاستخدام برمجيات خبيثة مثل أحصنة طروادة للتسلل عن بُعد، وبرمجيات سرقة المعلومات، وبرمجيات التجسس[5]، وأحصنة طروادة المصرفية بهدف تعطيل الشبكات وسرقة البيانات واختلاس الأموال وزرع برمجيات "بوتنت" الخبيثة. ومواقع التصيّد الاحتيالي المرتبطة بالوباء تسهّل إلى حد بعيد نشر هذه الملفات التنفيذية الخبيثة. ولوحظ أن البرمجيات الخبيثة تُرسَل أيضا عن طريق وصلات إلكترونية مدمجة في خرائط تفاعلية عن فيروس كورونا وتطبيقات مصنفة حسب المواضيع ومواقع إلكترونية احتيالية.

4. شركة Palo Alto Networs، جرت زيارة الموقع وأُخذت منه المعلومات في 24 نيسان/أبريل 2020 على العنوان التالي: https://unit42.paloaltonetworks.com/how-cybercriminals-prey-on-the-covid-19-pandemic/

5. جرت زيارة الموقع وأُخذت منه المعلومات في 26 نيسان/أبريل 2020 على العنوان التالي:

https://unit42.paloaltonetworks.com/how-cybercriminals-prey-on-the-covid-19-pandemic/

وأحد أبرز الأمثلة على البرمجيات الخبيثة لجمع المعلومات التي أشار إليها الشركاء من القطاع الخاص هو برمجية Emotet. وقد ازداد انتشارها بشكل كبير منذ بداية الوباء. وكشف باحثون من مركز IBM X-Force حصان طروادة Emotet في اليابان استخدمه على نطاق واسع مرتكبو جرائم سيبرية انتحلوا صفة مقدمي خدمات الرعاية الصحية للمعوقين[6]. ففي رسائلها الإلكترونية الاحتيالية، استدرجت الجهات مصدر التهديد الضحايا لفتح ملفات مرفقة زُعِم أنها تتضمن تدابير وقاية من كوفيد - 19، ولكنها كانت موبوءة ببرمجية Emotet الخبيثة. وقد وقع الكثير من الأشخاص في هذا الشرك لأن الرسائل بدت وكأنها واردة من بريد إلكتروني رسمي لمقدم الخدمات وكانت تتضمن عنوانا بريديا ورقما هاتفيا مشروعين في الظاهر. وكشف باحثون في مجال التهديدات في شركة Kaspersky كانوا يحققون في نفس الحالة عن أن حصان طروادة Emotet يُرسل في العادة بنسق .pdf و.mp4 و.docx كمرفَق برسائل إلكترونية تدعي أنها تحتوي على معلومات مفيدة عن فيروس كورونا، ولا سيما آخر المستجدات المتعلقة به، وتدابير الوقاية منه، وأساليب الكشف عنه[7]. وقد نجحت هذه الاعتداءات إلى حد بعيد لأن مرتكبي الجرائم السيبرية اختاروا اللحظة المناسبة لنشر البرمجية الخبيثة في وقت كان الناس يشعرون فيه بالقلق وعدم الأمان. ونتيجة لذلك، سُرق قدر كبير من البيانات الشخصية في الأشهر الأخيرة. وبرمجية Emotet التي خلّفت تبعات على 13 في المائة من المنظمات في العالم تصدرت في كانون الثاني/يناير 2020 قائمة أبرز البرمجيات الخبيثة لجمع البيانات[8].

وTrickbot هو مثال آخر على البرمجيات الخبيثة لجمع البيانات التي انتشرت بشكل كبير خلال الوباء. وبيّنت دراسة حديثة أجرتها شركة Microsoft أن هذه البرمجية هي الأكثر استخداما في عمليات الخداع المرتبطة بكوفيد - 19[9]. وأُفيد بأنها ارتبطت أكثر من أيّ برمجية أخرى برسائل احتيالية منذ بدء الوباء. وقد تلقاها الضحايا أيضا كملفات مرفقة برسائل إلكترونية واردة من منظمات وهمية غير ربحية تقدم مجموعات اختبار كوفيد19- بالمجان.

6. شركة IBM، جرت زيارة الموقع وأُخذت منه المعلومات في 24 نيسان/أبريل 2020 على العنوان التالي:
https://exchange.xforce.ibmcloud.com/collection/18f373debc38779065a26f1958dc260b

7. https://www.techrepublic.com/article/hackers-using-coronavirus-scare-to-spread-emotet-malware-in-japan/

8. شركة Check Point Technologies، جرت زيارة الموقع وأُخذت منه المعلومات في 6 تموز/يوليو 2020 على العنوان التالي:
https://blog.checkpoint.com/2020/02/13/january-2020s-most-wanted-malware-coronavirus-themed-spam-spreads-malicious-emotet-malware/

9. https://twitter.com/MsftSecIntel/status/1251181180281450498

المعلومات المضلِّلة

في منتصف شباط/فبراير 2020، أعلنت منظمة الصحة العالمية أن 'وباء معلوماتيا' قوامه معلومات مضللة عن كوفيد - 19. وحذرت من أن خطر هذه المعلومات البالغ لا يقل أهمية عن الوباء في حد ذاته [10].

وحددت دراسة عالمية أجراها معهد Reuters المسائل التالية المرتبطة بكوفيد - 19 والناجمة عن تفشّي المعلومات المغلوطة والمضللة[11] باعتبارها المواضيع الأكثر شيوعا:

- إجراءات السلطات العامة؛
- بثّ المعلومات بين السكان؛
- الأخبار الطبية العامة؛
- الجهات الفاعلة الرئيسية؛
- نظريات المؤامرة؛
- أسلوب انتقال الفيروس؛
- جهوزية عامة الناس؛
- تطوير لقاح.

وأكدت نسبة 27 في المائة من البلدان المشاركة في الاستقصاء العالمي تداول معلومات مغلوطة عن كوفيد - 19 بين سكانها وأعربت 21 في المائة منها عن تنامي القلق إزاء هذا التوجه. وخلال شهر واحد، أفاد بلد عضو بظهور 290 منشورا إلكترونيا احتوت في معظم الحالات على برمجيات خبيثة مخفية.

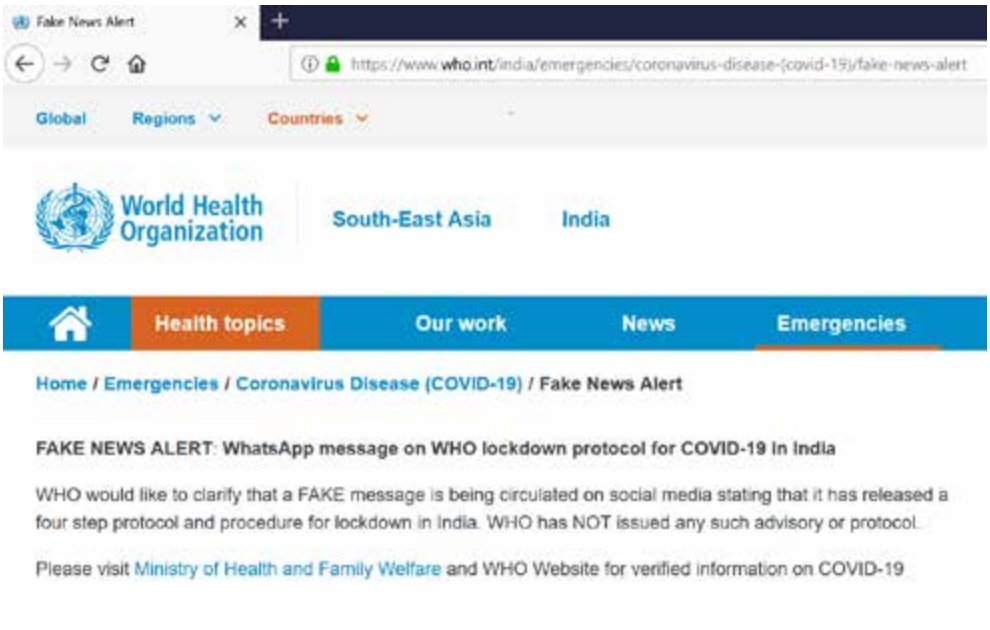
وجرى تناقل المعلومات بشكل رئيسي عن طريق وسائل التواصل الاجتماعي (واتسآب، وفايسبوك، وتويتر وغيرها) وتضمنت ادعاءات مضللة وإشاعات وافتراضات تتعلق باستمرار تطور الوضع المتعلق بالوباء. وأفادت بعض أجهزة إنفاذ القانون التي شاركت في الاستقصاء بأن المعلومات المضللة في بلدانها كانت مرتبطة باتجار غير مشروع بسلع طبية مقلدة.

وأعربت بعض البلدان الأعضاء عن قلقها من أن المعلومات المضللة كانت تبثّ الرعب بين السكان وتسبب اضطرابات اجتماعية متفاقمة أساسا بسبب الوباء. وأفادت أجهزة إنفاذ القانون بحالات تعميم معلومات مضللة على الإنترنت تتعلق بعدد الأفراد المصابين وبظهور الفيروس في مناطق خالية منه.

وشملت حالات المعلومات المضللة الأخرى رسائل احتيالية وردت عن طريق رسائل نصية قصيرة تتضمن عروضا مغرية لدرجة يصعب تصديقها مثل أغذية مجانية أو مزايا خاصة أو حسومات ضخمة في الأسواق التجارية الكبرى. وتعتقد هذه الأجهزة أن معظم هذه الرسائل قد عُمِّمت على السكان من أجل خلق تجمعات كبرى من الناس واستغلالها.

10. منظمة الصحة العالمية، جرت زيارة الموقع وأُخذت منه المعلومات في 21 أيار/مايو 2020 على العنوان التالي: https://www.who.int/docs/default-source/coronaviruse/situation-reports/20200202-sitrep-13-ncov-v3.pdf.

11. معهد Reuters، جرت زيارة الموقع وأُخذت منه المعلومات في 22 أيار/مايو 2020: https://reutersinstitute.politics.ox.ac.uk/research.



الشكل 3: تنبيه أصدرته منظمة الصحة العالمية لتحذير العامة من الأخبار المضللة عن كوفيد19- المتداولة عن طريق تطبيق واتسآب [12]

رد الإنتربول

في مواجهة بيئة الجريمة السيبرية المتسارعة التغيير خلال وباء كوفيد - 19، يضع الإنتربول ردا شرطيا عالميا على التهديدات السيبرية ذات الصلة ويتولى قيادته. وما فتئت إدارة مكافحة الجريمة السيبرية في المنظمة تعمل مع البلدان الأعضاء والشركاء من القطاع الخاص وأوساط الأمن السيبري في أنحاء العالم على عدد من المحاور.

ولمساعدة بلدانه الأعضاء على منع ومواجهة الجريمة السيبرية أثناء الوباء، قام الإنتربول ولا يزال يقوم بما يلي:

- تنظيم اجتماعات افتراضية طارئة مع جهات معنية شتى لتزويد البلدان الأعضاء بخدمات متكيفة مع احتياجاتها لمنع الجريمة السيبرية المتصلة بكوفيد - 19 وكشفها والتحقيق فيها. ويشمل هذا التدبير اجتماعات استراتيجية لرؤساء الوحدات الوطنية والإقليمية المعنية بالجريمة السيبرية ولفريق خبراء الإنتربول العالمي المعني بالجريمة السيبرية[13].

12. منظمة الصحة العالمية، جرت زيارة الموقع وأُخذت منه المعلومات في 21 أيار/مايو 2020 على العنوان التالي: https://www.who.int/india/emergencies/coronavirus-disease-(covid-19)/fake-news-alert.

13. فريق خبراء الإنتربول العالمي المعني بالجريمة السيبرية هو شبكة خبراء في الجريمة السيبرية من البلدان الأعضاء والقطاعين الخاص والعام والأوساط الأكاديمية يضعون في المتناول معلومات وممارسات جيدة ويقدمون المشورة للأمانة العامة للإنتربول في سياق وضع السياسات وتنفيذ المشاريع في مجال الجريمة السيبرية.

- المشاركة الفاعلة أيضا في مناقشات استراتيجية متعددة الأطراف يشرف عليها المنتدى الاقتصادي العالمي[14] لإقامة شراكات وتحالفات من أجل مواجهة الجريمة السيبرية. والإنتربول أيضا عضو في المجلس الاستشاري لمركز الأمن السيبري التابع للمنتدى.
- **إصدار نشرات بنفسجية** [15] لإطلاع أجهزة إنفاذ القانون على التهديدات السيبرية الجديدة الشديدة الخطر. وهذه التنبيهات العالمية التي توجَّه عبر شبكة الإنتربول المأمونة تتضمن ما يلي[16]:
  - **هجمات ببرمجيات انتزاع الفدية تستهدف البنية التحتية الأساسية والمستشفيات:** كشف مركز الإنتربول المتعدد الاختصاصات لمكافحة الجريمة السيبرية محاولات لتعطيل مؤسسات وبنى تحتية رئيسية لازمة للمساعدة على مو ا جهة كوفيد - 19ومهاجمتها ببرمجيات انتزاع الفدية.
  - **استخدام وتعميم حصان طروادة مصرفي:** استغل حصان طروادة مصرفي نقاط الضعف في أحد الأجهزة الوطنية لانتحال هوية كيان معين وتوجيه رسالة نصية باستخدام المحتوى المتصل بكوفيد - 19 لاسترعاء الانتباه وتنزيل الرابط الخبيث المدمّج في الرسالة النصية.
  - **إرسال مفاتيح USB تحتوي على برمجيات خبيثة بالبريد:** جمع المركز المتعدد الاختصاصات لمكافحة الجريمة السيبرية معلومات عن وسيلة جديدة تستخدمها مجموعات الجريمة السيبرية لارتكاب الاعتداءات، تتمثل في استخدام البريد لإرسال مفاتيح USB تحتوي على برمجيات خبيثة بمثابة 'هدايا' لدخول الشبكات الكمبيوترية في شركات وسرقة معلومات حساسة.
  - **استخدام ونشر برمجية حصان طروادة خبيثة:** تجعل البرمجية الخبيثة المعروفة باسم "Coronavirus" محتويات الأقراص غير قابلة للاستخدام عن طريق الكتابة فوق سجل إقلاعها الرئيسي (MBR).
- تشكيل **فرقة عمل عالمية معنية بالنطاقات الخبيثة**. تضم هذه الفرقة ضباط معلومات متخصصين في الجريمة السيبرية وخبراء من الشركاء في القطاع الخاص وأفراد من أجهزة إنفاذ القانون الوطنية، وترمي إلى كشف واستهداف الجهات التي يصدر عنها التهديد والبنية التحتية المشتركة التي تقف وراء النطاقات الخبيثة لتقويضها واستئصال هذا النوع من التهديدات. كانت الفرقة بحلول شهر حزيران/يونيو 2020 قد حددت وحللت حوالى 000 200 من النطاقات الخبيثة. وبالاستناد إلى النتائج التي توصلت إليها، قامت إدارة مكافحة الجريمة السيبرية بتعميم تقارير أنشطة سيبرية تضمنت بيانات مفيدة إلى أكثر من 80 من البلدان الأعضاء المتضررة.

14. المنتدى الاقتصادي العالمي، جرت زيارة الموقع وأُخذت منه المعلومات في 14 تموز/يوليو 2020 على العنوان التالي: https://www.weforum.org/agenda/2019/11/why-public-private-partnerships-are-critical-for-global-cybersecurity/; https://www.weforum.org/agenda/2020/01/partnerships-are-our-best-weapon-in-the-fight-against-cybercrime-heres-why/.

15. يعمم الإنتربول على البلدان الأعضاء نشرات بنفسجية لجمع أو توفير معلومات بشأن الأساليب الإجرامية والأغراض والأجهزة وطرائق الإخفاء التي يستخدمها المجرمون.

16. حُذفت تفاصيل النشرات البنفسجية بسبب عمليات الإنتربول الجارية لمكافحة الجريمة السيبرية.

- إطلاق **حملة #WashYourCyberHands العالمية للتوعية بالتهديدات السيبرية المرتبطة بكوفيد - 19.** أُطلقت هذه الحملة في أيار/مايو 2020 بمشاركة بلدان أعضاء و23 شريكا خارجيا لتوعية عامة الناس بأبرز التهديدات السيبرية المتصلة بوباء فيروس كورونا وتشجيعهم على اتخاذ تدابير الوقاية الإلكترونية الجيدة. ولكي تدفع عن السكان خطر مرتكبي الجرائم السيبرية الساعين إلى استغلال تفشّي الوباء لسرقة البيانات وزرع الفوضى وارتكاب أعمال الاحتيال، تدعم الحملة ما تتخذه أجهزة إنفاذ القانون الوطنية من إجراءات لمكافحة التهديدات السيبرية المرتبطة بكوفيد - 19. والمواد البصرية للحملة وإعلاناتها على وسائل التواصل الاجتماعي، التي صممها الإنتربول وشركاؤه، وصلت إلى حوالي 7,5 ملايين مستخدم على الإنترنت. وعلى منصة تويتر وحدها (INTERPOL_@Cyber)، ورد هاشتاغ الحملة #WashYourCyberHands حوالي 10 000 مرة.

الأولويات والتوصيات

لكي تحافظ المساعدة والخدمات المقدمتان من الإنتربول لبلدانه الأعضاء على أكبر قدر من الفعالية في التخفيف من وطأة التهديدات السيبرية المرتبطة بكوفيد - 19، حُددت الأولويات والتوصيات التالية:

- **إتاحة تبادل المعلومات في الوقت المناسب.** إن حصول إدارة مكافحة الجريمة السيبرية على معلومات محدثة عن التهديدات السيبرية الحديثة الكشف يتيح لها توقّع الاتجاهات الجديدة بدقة وتعميم أساليب عمل إجرامية عبر شبكة الإنتربول العالمية لتشجيع التوعية والوقاية. ويتعلق ذلك بشكل خاص بشنّ الاعتداءات على الحكومات والبنية التحتية الحساسة وقطاع الرعاية الصحية ببرمجيات انتزاع الفدية، الأمر الذي قد يهدد السلامة العامة والأمن ويُلحق بهما أشد الضرر. وبفضل تلقّي المعلومات المفيدة في الوقت المناسب، يمكن للإنتربول مساعدة بلدانه الأعضاء عن طريق إعداد وتنفيذ رد فعال.
- **تعزيز التعاون الشرطي بين البلدان الأعضاء.** في ضوء التهديدات عبر الوطنية المرتبطة بكوفيد - 19، يشدد الإنتربول على أهمية التعاون بين سلطات إنفاذ القانون الوطنية والإجابة بشكل آني على طلبات المعلومات التي تردها من سائر البلدان. والتعاون وتبادل المعلومات أمر حاسم لمواجهة التهديدات السيبرية التالية:
  - الاعتداءات ببرمجيات انتزاع الفدية على بنى تحتية حيوية، مؤشر الاختراق، عناوين بيتكوين؛
  - الغش في الأتعاب المدفوعة سلفا والاحتيال بالبريد الإلكتروني المهني؛
  - البرمجيات الخبيثة المنتشرة عن طريق التطبيقات غير الحكومية لتتبع الاتصال؛
  - تفاصيل بشأن الحملات التي تستغل عددا كبيرا من النطاقات الخبيثة.

17. منصة الإنتربول للتعاون في المجال السيبري مقامة داخل قسم الجريمة السيبرية في مركز الإنتربول العالمي للمعارف الذي تغذيه تكنولوجيا منصة التعاون المأمونة.

- **استخدام منصة الإنتربول للتعاون في المجال السيبري**[17]. هذه المنصة المصممة لتبادل المعارف وتنسيق العمليات تضع في متناول البلدان الأعضاء أداة مأمونة لتشكيل فرق عمل مشتركة متعددة الجهات والاختصاصات من أجل مكافحة الجرائم المرتكبة ضد الشبكات الحاسوبية. وتسهّل هذه الأداة الاتصالات المباشرة بين الأفرقة الميدانية في البلدان الأعضاء ومع الإنتربول لتبادل المعلومات المتعلقة بالجريمة السيبرية تبادلا فاعلا من أجل إعداد تدابير مواجهة ميدانية فورية للأعطال.

- **تطبيق تدابير الوقاية والتوعية.** يُتوقَّع لتطور التهديدات السيبرية المرتبطة بكوفيد - 19 أن يستمر في طرح صعوبات قانونية وعملياتية على أجهزة إنفاذ القانون في العالم. والوقاية من خلال توعية الجمهور وتمكينه من المحافظة على سلامته على الإنترنت تكتسي أهمية حاسمة للتخفيف من حدة هذه الصعوبات. وتُشجَّع البلدان الأعضاء في الإنتربول على تعميم الرسائل الأساسية لحملة الإنتربول العالمية #WashYourCyberHands على السكان فيها من خلال شبكات التواصل الاجتماعي وعلى إطلاق حملات توعية مماثلة على الصعيد الوطني.

- **تعزيز قدرات التحقيق في الجريمة السيبرية.** مع استمرار التهديدات السيبرية في التطور في علاقة مباشرة أو غير مباشرة بالوباء، من الأهمية بمكان بالنسبة لأجهزة إنفاذ القانون امتلاك تكنولوجيا وقدرات متخصصة. وإقرارا منه بأهمية النهوض بمستوى الخبرات لدى بلدانه الأعضاء خلال الأزمة العالمية، أطلق الإنتربول أكاديميته الافتراضية العالمية لتوفير مجموعة من فرص التدريب الإلكتروني لأجهزة إنفاذ القانون. وتنظم إدارة الإنتربول لمكافحة الجريمة السيبرية دورات تدريب إلكتروني وحلقات دراسية شبكية لتعزيز قدرات البلدان الأعضاء على مواجهة التهديدات السيبرية الجديدة والتحقيق في قضايا الجريمة السيبرية إبّان الأزمة العالمية وما بعدها.

- **توطيد الشراكات بين القطاعين العام والخاص.** منذ بداية تفشّي كوفيد - 19، اضطلعت الشراكات بين القطاعين العام والخاص بدور حاسم في التخفيف من وطأة التهديدات السيبرية الجديدة. ومن خلال تبادل المعلومات والخبرات بشأن الاتجاهات الحديثة وتقديم المساعدة التقنية، يمكن لشركات القطاع الخاص أن تكون شريكا بالغ الأهمية بالنسبة لأجهزة إنفاذ القانون.

- وفي هذا الصدد، جمعت إدارة الإنتربول لمكافحة الجريمة السيبرية منذ كانون الثاني/يناير 2020 **بيانات ومعلومات عن التهديدات السيبرية** المرتبطة بكوفيد - 19 من **البلدان الأعضاء وشركاء الإنتربول من القطاع الخاص** والأفرقة الوطنية للتصدي للطوارئ الحاسوبية وهيئة الإنترنت للأسماء والأرقام المخصصة ومجموعات تبادل المعلومات على الإنترنت من قبيل مجموعة Slack. وأفضى تنوع خلفية هؤلاء الشركاء إلى إغناء مجموعة البيانات وأثبت جدواه من خلال تزويد البلدان الأعضاء بالمساعدة اللازمة في الوقت المناسب. والإنتربول، إدراكا منه لجوانب التعاون الإيجابية هذه، يهدف إلى إعداد قاعدة بيانات يمكن لجميع الجهات المعنية تغذيتها والوصول إليها لوضع أكثر التدابير فعالية لمواجهة تهديدات الجريمة السيبرية. وإقامة علاقة

قوية بين أجهزة إنفاذ القانون وشركات القطاع الخاص تولّد في نهاية المطاف شعورا بالمسؤولية المشتركة في مكافحة التهديدات السيبرية المرتبطة بكوفيد - 19 وتتيح مواجهة التهديدات الجديدة في الوقت المناسب.

- **وضع وتنفيذ استراتيجيات وطنية في مجال الجريمة السيبرية.** أظهر استقصاء الآراء الذي أجراه الإنتربول مؤخرا غياب استراتيجية وطنية في مجال الجريمة السيبرية لمواجهة وباء كوفيد - 19 في 30 من البلدان الأعضاء. وتشير هذه النتيجة إلى ضرورة استحداث مثل هذه الاستراتيجية لترسيخ مناعة البنى التحتية والخدمات الوطنية التي يمكنها مساعدة البلدان على مجابهة التهديدات السيبرية بقدر أكبر من الفعالية وحماية السكان من اختراق البيانات خلال الأزمة العالمية وما بعدها.

التوقعات في الأجل القصير

استنادا إلى تحليل التعليقات الواردة من أجهزة إنفاذ القانون وكيانات القطاع الخاص، من المرجح أن يستمر المشهد العام للتهديدات السيبرية في التدهور. والتوقعات التالية من إدارة الإنتربول لمكافحة الجريمة السيبرية تلقي الضوء على مجالات القلق المحتملة.

- مع استمرار كوفيد - 19 عالميا، يرجَّح جدا أن تسجَّل زيادة إضافية في الجريمة السيبرية في المستقبل القريب. ويرجَّح جدا أيضا أن يكثّف مرتكبو الجرائم السيبرية أنشطتهم ويستخدموا طرائق عمل أكثر تطورا وتعقيدا، تجتذبهم إلى ذلك مواطن الضعف المتصلة بالعمل من المنزل واحتمالات زيادة المكاسب المالية.
- سيستمر مرتكبو الجرائم السيبرية على الأرجح في استغلال مواطن الضعف المتصلة بالعمل من المنزل، ساعين إلى الحصول على بيانات التعريف الخاصة بالموظفين من خلال أدوات وبرمجيات مكتبية أساسية. ويمكن أيضا استغلال البيانات الشخصية المسروقة لارتكاب المزيد من الاعتداءات السيبرية.
- أحد العوامل الأخرى المؤدية إلى اتساع نطاق الجريمة السيبرية هو تبعات الحَجْر المرتبط بكوفيد - 19 على مجالات الجريمة الأخرى، الذي حمل المجرمين على البحث عن مصادر دخل بديلة. من هذا المنطلق، قد يستغل بعض الجناة أسواق الشبكة الخفية لعرض 'الجريمة السيبرية كخدمة' لتيسير الوصول إلى هذا الشكل من أشكال الجريمة.
- يرجَّح أن تستمر الجهات التي يصدر عنها التهديد، مستغلةً حالة الهلع التي يسببها الوباء، في ارتكاب أعمال الاحتيال الإلكترونية المرتبطة بفيروس كورونا وحملات التصيّد الاحتيالي. ويرجَّح أيضا أن تسجل عمليات الاحتيال بالبريد الإلكتروني المهني ارتفاعا حادا بسبب الركود الاقتصادي والتحول في المشهد العام للشركات التجارية، الأمر الذي سيفتح آفاقا جديدة أمام الأنشطة الإجرامية.

- بالإضافة إلى ذلك، من المحتمل جدا عندما يتوفر لقاح أو دواء لكوفيد - 19 أن ترتفع حالات التصيّد الاحتيالي المتصلة بهذه المنتجات الطبية، ويتزايد اختراق الشبكات الحاسوبية والاعتداءات السيبرية لسرقة البيانات.
- يرجَّح للاعتداءات ببرمجيات انتزاع الفدية التي تستهدف قطاع الرعاية الصحية وسلاسل الإمداد المتصلة به أن تستمر في وتيرة أكثر تسارعا وأن يعجّل بها تنوع الوسائط المستخدمة لارتكابها.
- يُتوقَّع أن تستهدف الجهات التي يصدر عنها التهديد بيانات الأفراد الشخصية من خلال انتحال هوية شركات التزويد بالمحتوى الرقمي.
- حتى بعد انحسار حالات فيروس كورونا، من شبه المؤكد أن يكيّف مرتكبو الجرائم السيبرية مخططاتهم الاحتيالية لاستغلال الوضع في مرحلة ما بعد الوباء وأكبر عدد ممكن من الضحايا.

خاتمة

يطور مرتكبو الجرائم السيبرية اعتداءاتهم ويوسعون نطاقها بوتيرة مثيرة للقلق، مستغلين حالة الخوف واللايقين التي يسببها الوضع الاجتماعي والاقتصادي غير المستقر في العالم أجمع. والتعويل المتزايد على الاتصال بالإنترنت والبنية التحتية الرقمية بسبب الحَجْر العالمي يعزز في الوقت نفسه إمكانات الاختراق والاعتداءات السيبرية.

وعلى الرغم من هذا الأفق، يتخذ الإنتربول خطوات استباقية وجميع التدابير اللازمة لمساعدة بلدانه الأعضاء في أزمة هي الأولى من نوعها. كما أنه يتهيأ لمواجهة تهديدات ما بعد كوفيد - 19. فقد أتاح الوباء فرصا قيّمة للتفكير في القدرات والموارد الحالية التي ينبغي تحسينها للاستعداد بشكل أفضل لمواجهة أيّ صدمات مقبلة ومقاومتها.

أخيرا، أظهرت الأزمة أهمية اعتماد رد عالمي تعاوني ومنسق. وأولى الأولويات للتصدي لهذه التهديدات السيبرية المتفاقمة هي مواصلة تعزيز التعاون الشرطي الدولي في الأنشطة الميدانية وتحسين تبادل المعلومات بشأن الجريمة السيبرية مع مختلف الشركاء في أوساط الأمن السيبري العالمية.

ومن خلال التركيز على الأركان الأساسية لمواجهة التهديد الذي تشكله الجريمة السيبرية وعلى عمليات مكافحة هذه الجريمة وتطوير القدرات في هذا المجال، ستواصل إدارة الإنتربول لمكافحة الجريمة السيبرية سعيها إلى تخفيف التبعات العالمية لهذه الجريمة وحماية السكان منها لإقامة عالم أكثر أمانا.

الإنتربول

نبذة عن الإنتربول

الإنتربول هو أكبر منظمة دولية للشرطة في العالم. ويتمثل دوره في مد يد العون إلى أجهزة إنفاذ القانون في بلدانه الأعضاء الـ 194 لمكافحة الجريمة عبر الوطنية بجميع أشكالها. وهو يسعى إلى مساعدة أجهزة الشرطة في العالم أجمع على مواجهة التحديات المتنامية للجريمة في القرن الحادي والعشرين بتزويدها بالدعم التقني والميداني بفضل بنية تحتية متطورة. وتشمل الخدمات التي يقدمها الإنتربول تدريبا محدد الأهداف، ودعما متخصصا لعمليات التحقيق، وقواعد بيانات متخصصة، وقنوات مأمونة للاتصالات الشرطية.

رؤيتنا:

"الوصل بين أجهزة الشرطة لجعل العالم أكثر أمانا"

تتمثل رؤية الإنتربول في إقامة عالم يكون فيه كل موظف من موظفي إنفاذ القانون قادرا، من خلال المنظمة، على التواصل بشكل مأمون وعلى تبادل المعلومات الشرطية الحيوية والاطلاع عليها كلما وحيثما دعت الحاجة، من أجل ضمان سلامة المواطنين في العالم. ويقدم الإنتربول باستمرار حلولا جديدة ومتطورة لمواجهة التحديات التي تعترض عمل أجهزة الشرطة والأمن على الصعيد العالمي ويشجع على استخدامها.