الإنتربول

التهديدات السيبرية المرتبطة بكوفيد – 19 في العالم

#WashYourCyberHands

يستغل مجرمون واسعو الحيلة وانتهازيون وباء كوفيد – 19 لشن مختلف أنواع الاعتداءات السيبرية. ومنذ تفشّي الوباء، عادت إلى الظهور برمجيات خبيثة معروفة كانت مختفية نسبيا؛ واتخذت أشكالا جديدة أو استفادت من هذه الجائحة لتعزيز أساليبها القائمة على الهندسة الاجتماعية. والتطور مستمر في هذا المجال، وترد أدناه بعض أحدث التهديدات التي جرى تبيانها:

النطاقات الخبيثة

ازداد عدد النطاقات المسجلة بالكلمتين الرئيسيتين 'COVID' أو 'corona' من أجل استغلال تزايد عدد الأشخاص الباحثين عن معلومات عن كوفيد – 19 . ويُعتبر الكثير من هذه النطاقات مستحدثا لتحقيق مآرب خبيثة. فنقلا عن Palo Alto Networks، اكتُشف في نهاية شهر آذار/مارس 2020 نطاقا خبيثا و261 40 نطاقا شديد الخطورة مسجلة حديثا.

عمليات الاحتيال الإلكترونية ومواقع التصيد الاحتيالي

يستحدث مرتكبو الجرائم السيبرية مواقع إلكترونية مزورة ذات صلة بكوفيد – 19 بهدف استدراج الضحايا إلى فتح ملفات مرفقة خبيثة أو النقر على وصلات إلكترونية احتيالية من أجل انتحال الهوية أو النفاذ خلافا للقانون إلى حسابات خاصة. وأبلغت شركة Trend Micro أيضا أن حوالي مليون رسالة تطفلية موجهة منذ كانون الثاني/يناير 2020 كانت على صلة بكوفيد – 19 .

أضحى الاحتيال بالبريد الإلكتروني المهني أسلوب الغش المفضل. فهو يتيح الاستيلاء على عناوين البريد الإلكتروني للمورّدين والزبائن أو استخدام عناوين شديدة الشبه بها من أجل شن الاعتداءات. وتشكل الحاجة الملحّة إلى المنتجات الأساسية فرصة مثالية للمجرمين لجمع المعلومات أو اختلاس ملايين الدولارات من أموال المشتريات العامة وتحويلها إلى حسابات غير مشروعة.

البرمجيات الخبيثة لجمع البيانات

إن البرمجيات الخبيثة لجمع البيانات مثل أحصنة طروادة للتسلل عن بُعد، وبرمجيات سرقة المعلومات، وبرمجيات التجسس، وأحصنة طروادة المصرفية، تتغلغل في المنظومات الكمبيوترية باستخدام المعلومات المرتبطة بكوفيد – 19 كطُعم لتعطيل الشبكات وسرقة البيانات واختلاس الأموال وزرع برمجيات "بوتنت" الخبيثة.

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

يبث مرتكبو الجرائم السيبرية برمجيات تخريبية خبيثة مثل برمجية انتزاع الفدية لتعطيل بنى تحتية ومؤسسات حيوية مثل المستشفيات والمراكز الطبية التي تجاوزت الأزمة الصحية طاقاتها أصلا. والاعتداءات التي تشنها هذه البرمجيات لا تستهدف سرقة المعلومات عادة، بل منع هذه البنى التحتية من الوصول إلى البيانات الحساسة أو تعطيل منظوماتها الكمبيوترية، ما يؤدي إلى تفاقم وضع مأسوي أساسا في العالم الواقعي.

مواطن الضعف في العمل عن بُعد

تستغل الجهات التي يصدر عنها التهديد مواطن الضعف في المنظومات الكمبيوترية والشبكات والتطبيقات التي تستخدمها الشركات والحكومات والمدارس لتمكين موظفيها من العمل عن بُعد. وتزايُد عدد الأشخاص الذين يعوِّلون في عملهم على المعدات الإلكترونية يلقي عبئا كبيرا على التدابير الأمنية المتخذة قبل تفشّي الفيروس؛ ويبحث الجناة عن المزيد من الفرص لسرقة البيانات أو تحقيق الأرباح أو تعطيل المنظومات.

التطورات المتوقعة

في ضوء الظروف الاجتماعية والاقتصادية السريعة التغير، سيتواصل تفاقم التهديدات السيبرية التي يواجهها الأفراد والشركات والبنى التحتية الحيوية وستستمر في إلحاق الأضرار في العالم أجمع. وستتفاقم الجريمة السيبرية أيضا لأن المجرمين يبحثون عن مصادر إيرادات جديدة من خلال استغلال الجوانب المتصلة بالإنترنت في أنماط الجريمة الأخرى. ومن المتوقع أن نشهد ما يلي:

- ستتزايد بشدة عمليات الاحتيال الإلكترونية والتصيد الاحتيالي والاحتيال بالبريد الإلكتروني المهني بسبب الركود الاقتصادي والتحوّل الذي يشهده عالم الشركات، وسينتج عنها أنشطة إجرامية جديدة
- سيستغل المجرمون الأسواق السرية ليتحولوا إلى الجريمة السيبرية كخدمة' بسبب سهولة دخول هذه المنصات وانخفاض تكلفتها وارتفاع إيراداتها المحتملة؛
- سيزداد تعويل الحكومات والشركات والمدارس التي يواصل موظفوها العمل عن بُعد على الوصلات الإلكترونية وأدوات التواصل الافتراضي، الأمر الذي سيجعلها أكثر هشاشة ويتيح لمرتكبي الجرائم السيبرية المزيد من الفرص.

الإجراءات التي يتخذها الإنتربول

يعدّ برنامج الإنتربول العالمي لمكافحة الجريمة السيبرية ويقود الإجراءات العالمية التي تتخذها أجهزة إنفاذ القانون لمكافحة التهديدات السيبرية التي تستغل تفشّي فيروس كورونا. ونعمم نشرات بنفسجية من أجل تنبيه البلدان الأعضاء إلى التهديدات السيبرية الجديدة والشديدة الخطورة، ونعطي إرشادات تقنية للمنظمات التي تقع ضحية هذه الاعتداءات لمساعدتها في جهود التعافي التي تبذلها؛ وقد أجرينا استقصاء عالميا في مجال الجريمة السيبرية لإدراك الوضع العالمي السريع التغيّر على نحو أفضل. ونتعاون أيضا مع مجموعات خبراء في مجال الأمن السيبري عبر الإنترنت ونعقد اجتماعات افتراضية في حالات الطوارئ مع جهات معنية شتى – منها رؤساء الوحدات الوطنية والإقليمية لمكافحة الجريمة السيبرية وفريق خبراء الإنتربول العالمي لمكافحة الجريمة السيبرية وشركاؤنا من القطاع الخاص – من أجل تزويد البلدان الأعضاء بخدمات متكيفة مع احتياجاتها لمنع الجريمة السيبرية وكشفها والتحقيق فيها.

الإنتربول
INTERPOL General Secretariat
Tel: +33 4 72 44 70 00
www.interpol.int