cisco SECURE

الحماية ضد

برامج الفدية الضارة

نموذج Zero Trust (انعدام الثقة) الخاص بالأمان من أجل قوى عاملة عصرية

الحماية ضد

برامج الفدية الضارة

نموذج Zero Trust (انعدام الثقة) الخاص بالأمان من أجل قوى عاملة عصرية

المحتويات

حقوق النشر© لعام 2021 لصالح شركة Cisco Systems و/أو جميع الشركات التابعة لها. جميع الحقوق محفوظة.

إن برامج الفدية هذه مُقدّر لها البقاء

تطورت برامج الفدية الضارة بسرعة كجزء من إحدى استراتيجيات الهجوم. بمجرد حدوث استيلاء عدائي على أجهزة الكمبيوتر المنعزلة، تزداد المخاطر المحتمل حدوثها يوميًا. تستهدف الجهات الفاعلة الخبيثة بشكل متزايد الأهداف الجغرافية-السياسية وأنظمة الأعمال الحساسة والبُنى التحتية (مثل، صيد الطرائد الكبيرة)، مما قد ينتج عنها أضرار غير مسبوقة. واليوم، تُعد برامج الفدية الضارة أحد أكبر التهديدات في مجال الأمن السيبراني، حيث ازدادت بنسبة 150% في عام 2020 نظرًا للتحول المفاجئ لنظام العمل عن بُعد.

يتم تصنيف برامج الفدية الضارة الآن على أنها إرهاب سيبراني، ويؤكد القرار التنفيذي الأخير من جانب الرئيس الأمريكي بايدن أنه يجب اتخاذ إجراء الآن للحفاظ على أمان الأنظمة. يُعد نهج Zero trust (انعدام الثقة) المعيار الذهبي للحماية ضد برامج الفدية الضارة. صرح المعهد الوطني للمعايير والتكنولوجيا (NIST)، بأن "تنفيذ بنية تحتية خاصة بنهج zero trust (انعدام الثقة) قد أصبح أمرًا ضروريًا للأمن السيبراني والأعمال."

تنص صحيفة وقائع البيت الأبيض على أن "حوادث الأمن السيبراني الأخيرة مثل التي تعرضت لها كل من SolarWinds وMicrosoft Exchange وColonial Pipeline هي رسالة تذكير واقعية بأن كيانات القطاع العام والقطاع الخاص في الولايات المتحدة تواجه بشكل متزايد نشاطًا سيبرانيًا خبيثًا ومتطورًا من الجهات الفاعلة القومية في الدولة ومجرمي الإنترنت."

> "حوادث الأمن السيبراني الأخيرة مثل التي تعرضت لها كل من SolarWinds و Microsoft Exchange وColonial Pipeline هي رسالة تذكير واقعية بأن كيانات القطاع العام والقطاع الخاص في الولايات المتحدة تواجه بشكل متزايد نشاطًا سيبرانيًا خبيثًا ومتطورًا من الجهات الفاعلة القومية في الدولة ومجرمي الإنترنت."
>
> صحيفة وقائع البيت الأبيض في الولايات المتحدة الأمريكية.

ما هي برامج الفدية الضارة؟

بعبارة بسيطة، تستخدم برامج الفدية الضارة أساليب متنوعة لاستهداف المستخدمين غالبًا من خلال إصابتهم بالبرامج الضارة، وعادةً ما تبدأ بتصيُّد المعلومات من خلال البريد الإلكتروني أو سرقة كلمة المرور أو الهجوم العنيف. يمكن تحقيق هجوم برامج الفدية الضارة من خلال تشفير الملفات أو المجلدات، ومنع وصول النظام إلى محرك القرص الثابت والتلاعب في سجل التمهيد الرئيسي لمقاطعة عملية تمهيد النظام. بمجرد تثبيت البرامج الضارة ونشرها، يمكن للمتسللين الوصول إلى البيانات الحساسة وبيانات النسخ الاحتياطي، التي يقومون بتشفيرها من أجل الاحتفاظ بالمعلومات كرهينة. يمكن للمتسللين التحرك بسرعة أو قضاء أشهر في البحث وهم متخفيين لفهم البنية التحتية للشبكة قبل شن الهجوم.

يهدف الاستيلاء على البيانات إلى إثارة الخوف والإلحاح من الضحايا. لا يمكن الوصول إلى بياناتهم قبل إتمام الدفع (بشكل أساسي بعملة البيتكوين). ورغم ذلك، قد لا تسترجع الشركات جميع بياناتها. هناك أنواع كثيرة من برامج الفدية الضارة، ولكن في أغلب الأحيان، تسيطر برامج الفدية الضارة المُشفّرة على المجال. نتيجة لتعدد الأشكال (البرامج الضارة المتغيرة باستمرار)، هناك أنواع كثيرة يمكن أن تتنجنب الكشف عنها.

تتحسن برامج الفدية الضارة المُشفّرة التي تقوم بالاحتفاظ بالبيانات بسرعة. في عام 2006، استخدمت برامج الفدية الضارة 56 وحدة بت مع تشفير محلي. يستخدم الإصدار المتقدم الحالي من برامج الفدية الضارة خوارزميات AES المتناظرة ومفتاح التشفير العام RSA أو ECC للاحتفاظ بالبيانات.

تتطور برامج الفدية الضارة في الأعمال

مع استمرار اكتساب برنامج الفدية زخمًا، قد تطورت إلى أعمال احترافية تديرها مؤسسات إجرامية (تقع أغلبها في الصين، وروسيا، وكوريا الشمالية، وشرق أوروبا) مخصصة في تحديد الأهداف عالية القيمة وزعزعتها والحصول على المال في مقابل البيانات. للقيام بذلك بشكل فعّال، قد ذهبت هذه المنظمات إلى حد إنشاء خدمة عملاء لتوجيه الجهات المُستهدفة خلال عملية شراء البيتكوين ودفع الفدية. حتى أنه قد يتم تصنيف بعضهم بامتلاك خدمة عملاء جيدة من جانب الجهات المُستهدفة لهم.

في بعض الأحيان من أجل تحفيز عملية الدفع، سيقوم المهاجمون بتقديم "تقرير أمني مُفصّل" يحدد بالضبط كيفية قيامهم بالهجوم بعد تبادل الفدية. في حين أنه سيكون من الذكاء للعصابات فك تشفير الملفات مقابل المال للحفاظ على سمعتها سليمة أمام الهدف التالي، فهذا ليس هو الحال دائمًا. توضّح *حالة برامج الفدية الضارة لعام 2021* طبقًا لشركة Sophos أن 8% فقط من الضحايا يستعيدون بياناتهم مرة أخرى وأن 29% منهم يستعيد أكثر من نصف بياناتهم. في بعض الأحيان يتم حصاد البيانات وتبادلها مع مهاجمين آخرين أو الاحتفاظ بها من أجل أي فرصة تبادل فدية تتم مستقبلاً.

في الأعوام الأخيرة، قامت جهات فاعلة خبيثة بإنشاء برامج الفدية الضارة كخدمة (RaaS)، وهي حل مُبتكر متكامل يتيح لأي شخص نشر هجوم برامج الفدية الضارة بدون معرفة كيفية البرمجة. تمامًا مثل منتجات البرامج كخدمة (SaaS)، تتيح (RaaS) وصولاً سهلاً ورخيصًا نسبيًا إلى هذه الأنواع من البرامج الضارة مقابل رسوم أقل من تكلفة إنشاء برامج خاصة بك. يحصل مقدمو خدمة RaaS بشكل عام على تخفيض بنسبة 20%-30% من أرباح الفدية المحققة. الآن هناك اشتراك ونماذج تابعة للمساعدة في إتمام عمليات هجوم ناجحة. كانت المجموعة المتسللة REvil تمتلك نموذجًا تابعًا لها يحصل على نسبة من الأرباح من خلال مشاركة أي شخص يساهم في هجوم ناجح من خلال برامج الفدية الضارة. لقد أدى هذا النموذج إلى الزيادة الكبيرة في حجم عمليات الهجوم من خلال برامج الفدية الضارة.

كان يُنسب أولاً إلى عصابة Maze، هناك توجّه آخر يتمثل في الابتزاز المزدوج، حيث يأخذ المتسللون المعلومات المسروقة ويهددون بنشرها على الويب المظلم و/أو الإنترنت إذا لم تتم تلبية مطالبهم. حيث لديهم بنية تحتية مُدمجة للتعامل مع عمليات تفريغ البيانات هذه، وفقًا لـ*تقرير التحقيقات حول عمليات خرق البيانات لعام 2020* لشركة Verizon. أصبح أسلوب "تحديد الأسماء والتشهير بهم" معروفًا الآن لأغلب عصابات برامج الفدية الضارة، كما هو الوضع مع نموذج "العقوبة"، حيث يرتفع السعر مع مرور الوقت.

بما أن الشركات تعمل على تقوية الوضع الأمني لأجهزة الكمبيوتر والشبكات الخاصة بهم من هجمات برامج الفدية الضارة، يوجّه المتسللون انتباههم الآن نحو استغلال الأجهزة المحمولة. تمتلك الأجهزة المحمولة شاشات أصغر بكثير ولا تقدّم معلومات كاملة للوهلة الأولى (البريد الإلكتروني على سبيل المثال)، مما يسهل على الضحايا الضغط على الروابط الضارة. إن عمليات هجوم إنترنت الاشياء (IoT) في ازدياد هي أيضًا ويمكن أن تؤدي برامج الفدية الضارة وقلة الأمان إلى تحويل الأجهزة والجهات المستهدفة إلى نقاط إدخال لأدوات برامج الفدية الضارة. في عام 2020، ازدادت هجمات برامج الفدية الضارة التي تستهدف أجهزة إنترنت الأشياء بنسبة 109% في الولايات المتحدة.

أدت هذه العوامل، إلى جانب الدول التي تعمل كملاجيء آمنة للمهاجمين إلى زيادة جرائم برامج الفدية الضارة. كان هناك هجوم ناجح من برامج الفدية الضارة كل 10 ثواني في عام 2020، ووفقًا لاستطلاع Anomali Harris Poll فإن واحدًا من كل خمسة أمريكيين يقع ضحية لهجمات برامج الفدية. بالإضافة إلى ذلك، تفيد مجلة Infosecurity Magazine بأن الطريقة الأكثر شيوعًا للهجوم "كانت إلى حد كبير حركة مرور روبوتات الشبكة (28%)، يليها عمال تعدين العملات الرقمية (21%)، وسارقي المعلومات (16%)، والجهاز المحمول (15%) والبرامج الضارة المصرفية (14%)." وللتصدي لذلك، تسعى الشركات جاهدة لإنفاق المزيد من الأموال على الأمن (150 مليار دولار في عام 2021 وفقًا لشركة Gartner).

تتراجع الهجمات على الأفراد حيث يُركّز المتسللون على أهداف محددة مُربحة بشكل أكبر. يبلغ مقدمو الخدمات المُدارة (MSPs) عن زيادة نسبة الهجمات إلى 85% ضد الشركات الصغيرة والمتوسطة. يتم استهداف المؤسسات إلى جانب البنية التحتية والرعاية الصحية والحكومة والشركات المُصنعة أكثر من أي وقت مضى، مع بطاقات أسعار تصل إلى ملايين مقابل بياناتهم. تضاعف حجم الفدية في العام الماضي حيث ضرب المهاجمون شركات أكبر. كما زادت الهجمات على المورّدين والمقاولين وبرامج الجهات الخارجية بشكل كبير. كان على الشركات الاعتماد على أمان الجهات الخارجية هذه التي لديها إمكانية الوصول إلى أنظمتها.

نهوض عصابات برامج الفدية الضارة

جاءت أول حالة معروفة لبرامج الفدية الضارة من خلال الأقراص المرنة التي تحتوي على استطلاعات الرأي حول الإيدز والبرامج الضارة، والتي تم توزيعها في جميع أنحاء العالم في عام 1989 بواسطة الدكتور جوزيف بوب. تقوم الأقراص بتشفير الملفات الموجودة على نظام الضحية وتمنع الوصول إلى أن يرسلوا مبلغ 189 دولارًا إلى صندوق بريد في بنما. تم بعد ذلك توزيع أقراص مضغوطة كطُعم في مؤتمر الإيدز لمنظمة الصحة العالمية. كانت الأقراص المضغوطة الخاصة بالدفع والشحن مثيرة للمشاكل ومكلفة.

2006

بدأ المجرمون الإلكترونيون في استخدام شكل أكثر فعالية من تشفير المفتاح العام RSA 660 لتشفير الملفات بشكل أسرع. كانت الجهات البارزة القائمة بذلك في تلك الحقبة هما Archiveus Trojan وGPcode اللذان اعتمدا على تصيُّد المعلومات من خلال البريد الإلكتروني كنقاط إدخال لهم.

2008-2009

ظهر برنامج مكافحة فيروسات جديد مُحمّل عليه برامج الفدية الضارة، واستخدم برنامج الأمان الاحتيالي FileFix Pro للحصول على الأموال مقابل فك التشفير.

2010

غيرت عملة البيتكوين كل شيء. تم اكتشاف عشرة آلاف نوع من برامج الفدية الضارة المختلفة وظهرت لأول مرة برامج فدية ضارة على شاشة القفل.

2013

تم العثور على ربع مليون عينة من برامج الفدية الضارة، وسرعان ما أصبح كل من برنامج Cryptolocker والبيتكوين طريقة الدفع الأساسية. استخدمت برامج الفدية الضارة تشفير RSA 2048 بت للطلبات المتزايدة، مما أثبت أنه مربح للعصابات.

2015

ظهر برنامج الفدية الضارة Teslacrypt trojan، وكان هناك الآن 4 ملايين نوع من برامج الفدية الضارة المختلفة، وتم تقديم برامج الفدية الضارة كخدمة (RaaS).

2016

انتشر برنامجا الفدية الضارة JavaScript وLocky، حيث كان يصيب Locky 90000 ضحية يوميًا. استهدف المهاجمون مؤسسات أكبر، مثل المستشفيات والمؤسسات الأكاديمية. وصلت أرباح برنامج الفدية الضارة إلى أكثر من مليار دولار. تسببت البرنامج الضار Petya في خسائر مالية تزيد عن 10 مليارات دولار.

2017

ظهر برنامج التشفير الضار WannaCry Cryptoworm هذا العام، وتطور إلى مجموعة متنوعة من المتغيرات يوميًا وانتشر بسرعة إلى 300000 جهاز كمبيوتر في جميع أنحاء العالم من خلال استغلال Microsoft.

2018

تم طرح Katsuya. أغلقت SamSam العديد من خدمات البلدية التي تؤثر على مدينة أتلانتا.

2019

بزغت REvil، وهي عصابة RaaS خاصة، من روسيا. يتطلب Ryuk، أحد برامج الفدية الضارة المتطورة والمكلفة المُضمنة في المرفقات الضارة ورسائل تصيُّد معلومات البريد الإلكتروني، مدفوعات أعلى مقارنةً بعمليات هجوم مماثلة وقام بإغلاق جميع الصحف الرئيسية في الولايات المتحدة بشكل فعّال.

2020

ارتفعت برامج Darkside وEgregor وSodinokibi بصفتهم لاعبين رئيسيين. انتقل Ryuk من حالة واحدة في اليوم إلى 19.9 مليون بحلول سبتمبر، أي ما يعادل ثماني حالات في الثانية.

2021

زعزعت مجموعات REvil/Sodinokibi وConti وLockbit الرعاية الصحية بشدة. قامت CryptoLocker بالحصول على 40 مليون دولار من شركة التأمين الرئيسية CNA Financial في واحدة من أكبر مدفوعات برامج الفدية الضارة حتى الآن. نجح DarkSide في مهاجمة شركة Colonial Pipeline Company، مما يمثل أكبر اختراق تم الكشف عنه علنًا للبنية التحتية الحيوية للولايات المتحدة.

المحيط يتوسع

كيف أصبحت برامج الفدية الضارة شائعة للغاية؟ في السابق، كانت المحيط عبارة عن جدار مسوّر أدار التطبيقات والبيانات المركزية عبر جدران حماية الشبكة الافتراضية الخاصة (VPN) وحلول إدارة الأجهزة المحمولة (MDM)، مثل خندق يحيط بقلعة الشبكة. وفي الوقت الحاضر، يتم العمل من أي مكان ومن أي جهاز (بما في ذلك الأجهزة المحمولة الشخصية)، وتحتاج البيانات إلى أن يصل إليها تطبيقات جهات خارجية في السحابة. فلا يوجد خندق، ولكن بالأحرى الكثير من المدخلات إلى القلعة. لقد حوّلت الزيادة المفاجئة للعمل عن بُعد أثناء الجائحة المحيط التقليدي إلى "محيط خارجي معرّف بالبرامج." وفي إطار الاندفاع للحفاظ على عمل الموظفين، كان الأمان فكرة متأخرة بالنسبة للكثيرين، مما أدى إلى ظهور برامج فدية للجهات الفاعلة السيئة.

الوصول عن بُعد

يفيد تقرير *أهم توجهات الأمان والمخاطر من شركة Gartner لعام 2021* بأن 64% من الموظفين قادرون الآن على العمل من المنزل، وأن خُمسَي القوى العاملة يعملون من المنزل. وبسبب أوامر البقاء في المنزل الإلزامية أثناء الجائحة تعيّن على أغلبية العاملين الانتقال إلى العمل عن بُعد بنسبة 100% واحتاجوا إلى القدرة على العمل على أجهزتهم الخاصة مع الوصول إلى تطبيقات SaaS في السحابة وفي موقع العمل. لم يكن لدى الكثير من الشركات البنية التحتية التي تدعم هذا التغيير. اليوم، الوصول عن بُعد هو الواقع الجديد للقوى العاملة. بينما تتكيف المؤسسات مع معيار التشغيل هذا، من المتوقع أن القوى العاملة ستكون نموذجًا هجينًا من العاملين عن بُعد وهؤلاء العاملين الذين يعودون إلى المكتب.

قال بيتر فيرستبروك، نائب رئيس المحللين في شركة Gartner، في منشور على مدونة، أنه "مع تبلور الوضع الطبيعي الجديد، ستحتاج كل المؤسسات إلى وضع دفاعي متصل دائمًا، والوضوح بشأن مخاطر الأعمال التي يرتقي لها المستخدمون عن بُعد ليظلوا آمنين."

تخلق الشركات التي لم تقوي وضعها الأمني لهذا التغيير أو تعزز تعليمها الأمني الداخلي طريقة سهلة للدخول للمهاجمين. تذكر شركة Gartner أن 57% من الاختراقات ترتبط بإهمال الموظفين/الجهة الخارجية. وفقًا لـ ZDNet، يُعد بروتوكول سطح المكتب البعيد (RDP) هو الطريقة الأولى التي تتمكّن بها الجهات القائمة بالتهديد على الوصول إلى أجهزة الكمبيوتر التي تعمل بنظام التشغيل Windows وتثبيت برامج الفدية الضارة والبرامج الضارة الأخرى، متبوعة بتصيُّد معلومات البريد الإلكتروني وعمليات استغلال أخطاء شبكة VPN.

قيود شبكات VPN

عمليات الاستغلال للتسلل في شبكات VPN هي ثالث أشهر طريقة دخول لمتسللي برامج الفدية الضارة. وكان التسلل الذي أغلق شركة Colonial Pipeline ناتجًا عن كلمة مرور مخترقة واحدة من شبكة VPN غير مستخدمة. بينما يمكن لشبكات VPN تقييد الوصول إلى تطبيقات موقع العمل، هناك تعارض بشأن الوصول إلى تطبيقات السحابة الذي يمكن أن يؤدي إلى الثغرات الأمنية. وبمجرد الاختراق، يمكن أن تؤدي شبكات VPN إلى باب خلفي للوصول إلى الشبكة حيث يمكن للمتسللين تثبيت البرامج الضارة على الأنظمة الداخلية.

> يمنع نهج جدار الحماية وشبكة VPN ذات طبقة بنهج zero trust (انعدام الثقة) مع المصادقة متعددة العوامل 100% (MFA) من الروبوتات، و99% من هجمات التصيُّد المجمّعة، و90% من الهجمات المستهدفة، وفقًا لبحث Google.

الأجهزة الطرفية غير المحمية

وباتصال المزيد والمزيد من الأجهزة بشبكات الشركة، قد ازداد عدد الأجهزة الشخصية والأجهزة غير الرسمية. ونظرًا لأن هذه الأجهزة قد لا تتم مراقبتها أو ليست-محدّثة، من المحتمل أنه يمكن أن تؤدي إلى الاختراقات في الأجهزة الطرفية الرئيسية دون اكتشافها. وبينما يبحث المتسللون عن طريقة للدخول، يمكن أن تؤدي الأجهزة الطرفية غير المحمية ونقص الرؤى بشأن مَن وما هو متصل بشبكتك وسلامة الجهاز إلى خرق.

تصيُّد المعلومات والهجمات المستهدفة والثغرات الأمنية

ما الأساليب التي يتم استخدامها في هجمات برامج الفدية الضارة؟ إنها عملية متعددة الخطوات يمكن أن تكون قصيرة نسبيًا، أو يتم تنفيذها على مدار أشهر للوصول إلى البيانات الأكثر قيمة وتشفيرها وسيتسبب ذلك في إحداث أكبر ضرر إذا تم احتجاز رهينة. يبلغ موقع CSOonline.com عن أن 94% من البرامج الضارة مستلمة عبر البريد الإلكتروني، وحساب هجمات تصيُّد المعلومات لأكثر من 80% من حوادث المعلومات. تتضمن نقاط الدخول الأخرى التحديثات غير المصححة والثغرات الأمنية دون انتظار. تبدأ كل تلك الحوادث تقريبًا بسرقة بيانات الاعتماد.

أساليب برامج الفدية الضارة

"إرسال العديد من الرسائل الاحتيالية والاحتيال على الضحايا" أو التصيد على نطاق واسع

تستحوذ الجهات القائمة على التهديد بقوائم البريد الإلكتروني من السوق السوداء، ثم تحلل بيانات الاعتماد وتوزّع رسائل البريد الإلكتروني لتصيُّد المعلومات. تكون بعض بيانات الاعتماد فقط ضرورية ليتم الأمر بنجاح، ويتم الاستحواذ في الغالب عبر البريد الإلكتروني بمرفقات ضارة، أو مواقع ويب احتيالية تظهر على أنها مشروعة أو هوية مزيفة تستهدف الموظفين ذوي مناصب عالية.

التصيد الاحتيالي الموجه

يتم تنفيذ هذا الهجوم المستهدف المنسق على مجموعة معينة من المستخدمين بإرسال رسائل موجّهة اجتماعيًا مخصصة تستدعي الفضول أو الخوف أو المكافأة من مصدر يبدو-مشروعًا. تحتوي رسائل البريد الإلكتروني وموقع الويب على برامج ضارة مُستخدمة لسرقة بيانات الاعتماد. كما يمكن نشر البرامج الضارة خلال الوسائط الاجتماعية وتطبيقات الرسائل الفورية.

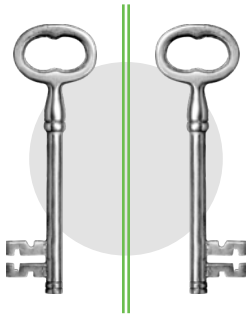
هجوم عنيف

وفقًا لاستطلاع LastPass، أقر 91% من المستجيبين بأنهم يعيدون استخدام كلمات المرور. يدرك المتسللون هذا الأمر تمامًا ويجمّعون كلمات المرور من تفريغ بيانات الاعتماد أو الويب المظلم. ويستخدمون حينئذٍ الأدوات التلقائية لاختبار كلمات المرور عبر المواقع المختلفة، والمعروفة باسم حشو بيانات الاعتماد أو القوة الغاشمة. وبمجرد الدخول، يمكن بدء الهجوم.

استغلال الثغرات الأمنية المعروفة

وبالإضافة إلى الرؤى بشأن الأجهزة المتصلة بشبكتك، تُعد معرفة سلامة الجهاز ومدى مواكبته للتصحيحات والتحديثات أمرًا مهمًا للحفاظ على ملف تعريف أمني عالي. تفيد Security Boulevard، بأن "المكونات مفتوحة المصدر "القديمة و"المُتخلى عنها" واسعة الانتشار. و91% من الرموز الأساسية احتوت على مكونات إما كانت قديمة لأكثر من أربع سنوات أو لم يكن بها نشاط تطوير في العامين الماضيين."

دليل تفصيلي حول هجوم برامج الفدية الضارة



تشفير برامج الفدية الضارة

في الحالات الأكثر شيوعًا، تشفّر هجمات برامج الفدية الضارة البيانات حول الأنظمة المستهدفة، بجعلها غير قابلة للوصول حتى يتم دفع فدية مقابل التشفير. والأسلوب الأخير هو مضاعفة التشفير، حيث يقوم المتسللون بتشفير نظام ما مرتين، أو تستهدف عصابتان مختلفتان الضحية نفسها. وباستخدام هذا النهج، يحظى المهاجمون بفرصة جمع فديتين بتلقي دفعة للطبقة الأولى من التشفير، ومن ثم يفاجئون الضحايا بطبقة أخرى بعد جمع الدفعة مقابل الأولى. التشفير الأكثر شيوعًا هو غير متماثل أو متماثل.

تنسيق الهجوم

في هذه النقطة، يدرس متسللو برامج الفدية الضارة وضع الشركات المعينة التي يستهدفونها. قد يشترون قوائم البريد الإلكتروني من الويب المظلم، ويعرّفون القادة المهمين ويقرأون التقارير المالية للشركة ويبحثون عن ملفات تعريف الوسائط الاجتماعية ويجمعون قائمة بالمساهمين الرئيسيين من المقاولين والمورّدين والشركاء. ما هي الأساليب التي يستخدمها المتسللون للدخول؟ جاءت أهم ثلاثة هجمات في عام 2020 من أجهزة RDP طرفية مؤمّنة بشكل غير جيد وهجمات تصيد معلومات البريد الإلكتروني، واستغلال الثغرات الأمنية دون انتظار لشبكة VPN. وتُعد بيانات الاعتماد المخترقة هي الطريقة الأولى التي يحصل بها المعتدون على الوصول.

الحركة العمودية

في حالة التسرب أو الإصابة، تحدث الحركة العمودية عندما تنتقل الجهات القائمة على التهديد من وضع خارجي إلى وضع داخلي. وبمجرد الدخول، يقومون بمسح الملفات وينفذون رمزًا ضارًا على الأجهزة الطرفية وأجهزة الشبكة. تنتقل البرامج الضارة عبر النظام المُصاب، وتعطّل جدران الحماية وبرامج مكافحة الفيروسات. وحتى الآن، لقد استولى المهاجمون على البيانات، ولكنها ليست مشفّرة بعد. تتضمن نقاط الدخول الشائعة للحركة العمودية حسابات البريد الإلكتروني التي تعرضت لتصيد المعلومات، وخوادم الويب منخفضة المستوى والأجهزة الطرفية المحمية بشكل سيء.

نقطة انطلاق جانبية

لقد ازدادت التهديدات المتقدمة المستمرة (APTs) نظرًا للحركة الجانبية. لإنشاء نقطة انطلاق، يتعين على المجرمين تشفير أجهزة الكمبيوتر ونشر برامج الفدية الضارة على أكبر عدد ممكن من الأنظمة. وبمجرد الحصول على الوصول، يبدأ هجوم المتسلل. إنهم يبدأون بشكل جانبي، وغير مكتشف، لمدة أسابيع أو أشهر عبر الشبكة لتحديد الأهداف الرئيسية مثل مركز القيادة والتحكم (C2)، والمفاتيح غير المتماثلة وملفات النسخ الاحتياطي. وفي الوقت نفسه، يطوّرون وصولهم وأذوناتهم بإصابة حسابات مستخدمين وأنظمة إضافية وإعداد تواجد ضار دائم للاستيلاء على البيانات. تتضمن بعض الأمثلة على الحركة الجانبية استغلال الخدمات عن بُعد، والتصيُّد الاحتيالي الموجه الداخلي واستخدام كلمات المرور المسروقة، المعروفة أيضًا بـ "تمرير التجزئة."

نقل البيانات غير المصرح به

وبمجرد إكمال تقييم المخزون، يبدأ التشفير. يتم حذف النسخ الاحتياطية للنظام ويتم تشفير المجلدات والملفات المحلية، ويتم توصيل محركات الشبكة غير المعينة بالأنظمة المصابة ويتم إجراء الاتصال بمركز القيادة والتحكم لإنشاء مفاتيح التشفير المُستخدمة على النظام الحالي. يتم نسخ بيانات الشبكة محليًا، وتشفيرها ومن ثم تحميلها، واستبدالها للبيانات الأصلية. يمكن استخدام البيانات التي تم نقلها بشكل غير مصرح به لمضاعفة الابتزاز. في هذه الحالة، تتم المطالبة بفدية مقابل فك تشفير البيانات المشفرة، ومن ثم تتم المطالبة بفدية ثانية لعدم تسريب البيانات المسروقة.

الدفع والفتح

يقوم المهاجمون بعد ذلك بتنشيط البرامج الضارة وحظر البيانات وإعلان مطالبهم للفدية في مواقع مخترقة بتعليمات محددة بشأن كيفية إجراء الدفع، تمامًا ليكون الدفع بعملة البيتكوين. يؤدي نجاح برنامج الفدية الضارة إلى حدوث مشكلة تعطل مكلفة للغاية ومن الصعب للغاية حلها. يتم إجراء التهديدات، ويبدأ العد التنازلي. يجب أن تقرر الشركات ما إذا كانت تريد أن تتحمل الخسارة وتدفع، وتحاول استعادة ملفاتها بمفردها، أو تستخدم تأمين الأمن السيبراني الخاص بها، الذي سيسترد جزءًا من الفدية فقط. إنه خيار ضمن خيارات سيئة، ولهذا السبب من الضروري أن تنفذ المؤسسات البنية التحتية لنهج zero trust (انعدام الثقة) وتحظى بأفضل ممارسات الأمان المعززة في موضعها لتجنب هذا الموقف.

المجالات المعرضة للخطر

مجالات الرعاية الصحية والبلديات والحكومة بالإضافة إلى البيع بالتجزئة والتعليم والتمويل، هي المجالات الأكثر تأثرًا بهجمات برامج الفدية الضارة. لدى هذه المجالات حلول قديمة معقدة وقد لا تستفيد من أمان السحابة القوي. تُكيّف مجالات الرعاية الصحية والتعليم والحكومة وضعها الأمني ببطء مع التحديثات والتقنيات الجديدة، مما يجعلها أهدافًا سهلة ومربحة.

إيقاف عمليات اختراق برامج الفدية الضارة قبل أن تبدأ

في هجوم برنامج الفدية الضارة، يحتاج المهاجمون أولاً إلى الحصول على الوصول. ويمكنهم القيام بذلك من خلال الحصول على بيانات اعتماد مخترقة كما هو الحال في عملية خرق شركة Colonial Pipeline.

يمكن أن تساعد المصادقة متعددة العوامل (MFA) من Duo على منع برامج الفدية الضارة من الحصول على الوصول في المقام الأول. تطلب المصادقة متعددة العوامل من أحد المستخدمين تقديم مجموعة من نقطتين أو أكثر من بيانات الاعتماد للتحقق من هويته لتسجيل الدخول. على سبيل المثال، بالإضافة إلى اسم المستخدم وكلمة المرور، تطلب المصادقة متعددة العوامل من Duo شيئًا أنت تملكه — مثل رمز مميز لجهاز أو برنامج أو جهاز موثوق — قبل الحصول على الوصول إلى الموارد. ويفضل هذا المطلب الإضافي، تُصعِّب MFA على برامج الفدية الضارة الحصول على نقطة الانطلاق الأولية تلك بشكل كبير للغاية.

كما تحرص برامج الفدية الضارة على استخدام الخدمات عن بُعد، مثل RDP وشبكات VPN، للحصول على الوصول إلى شبكة ما. إن Darkside، المجموعة المزمع ارتكابها لهجوم Colonial Pipeline، يُشتبه في أنها قد استخدمت وصول شبكة VPN للشركة للحصول على مدخل إلى بيئة الضحية. فهي أكثر من مجرد مصادقة متعددة العوامل، حيث تجتمع Duo MFA، وDuo Device Trust، وDuo Network Gateway (DNG)، وDuo Trust Monitor في حل وصول موثوق واحد ويمكنها المساعدة في تأمين الوصول عن بُعد إلى البنية التحتية الداخلية ومنع برامج الفدية الضارة من الحصول على الوصول في المقام الأول.

كيف يساعد Duo على الحماية من برامج الفدية الضارة

تفيد Gartner بأن 90% من برامج الفدية الضارة يمكن منعها. يتمتع Duo بوضع فريد لمساعدة المؤسسات في ثلاث جبهات:

1. منع برامج الفدية الضارة من الحصول على نقطة انطلاق أولية في بيئة ما
2. منع أو إبطاء نشر برامج الفدية الضارة إذا تمكّنت من اختراق مؤسسة ما
3. حماية الأصول والأجزاء المهمة من المؤسسة بينما ما يزال المهاجم متواجدًا في البيئة وحتى يتم تحقيق المعالجة الكاملة

تتطلب المصادقة متعددة العوامل من Duo أكثر من مجرد اسم مستخدم وكلمة مرور للمصادقة. تتيح DNG للمستخدمين الوصول إلى مواقع الويب الداخلية وتطبيقات الويب وخوادم SSH و RDP دون الاضطرار إلى القلق إزاء بيانات اعتماد VPN. يضمن Duo Device Trust أن الجهاز الذي يصل إلى الموارد عن بُعد هو جهاز كمبيوتر موثوق وليس جهازًا مهاجمًا. وأخيرًا، يجذب Duo Trust Monitor الانتباه إلى طلبات المصادقة التي تظهر على أنها مشبوهة، مثل التي تنشأ من البلدان التي من المعروف أن الجهات القائمة على برامج الفدية الضارة نشطة بها، والبلدان حيث لا يكون لدى مؤسسة ما موظفين بها.

كما أن استخدام البرامج الضارة هو أسلوب الإصابة الشهيرة ببرامج الفدية الضارة. توفر Cisco حلولاً تكميلية، مثل Secure Endpoint وEmail Gateway، حيث يمكنهما فحص برامج الفدية الضارة القائمة على البرامج الضارة واكتشافها وحظرها قبل أن تصيب الأجهزة الطرفية.

صدّ النشر

تتمتع برامج الفدية الضارة التي تؤثر على عدد صغير من الأنظمة بتأثير محدود ومن غير المحتمل أن تتسبب في إحداث تأثير كبير يجعل مؤسسة ما تتوقف عن العمل وتريد دفع فدية. هذا هو السبب في أن انتشار برامج الفدية أمر بالغ الأهمية لإسقاط جزء كبير من المؤسسة بشكل فعّال وإجبارهم على دفع الفدية للعودة بسرعة إلى العمل. وبالعودة إلى عام 2017، استخدم كل من WannaCry وNotPetya استغلال External Blue للاستفادة من الثغرات الأمنية في Microsoft ونشرها دون تدخل المستخدم.

يمكن أن يحافظ Device Health Application من Duo على الأجهزة مصححة ومحدّثة، مما يجعل نشر برامج الفدية الضارة تلقائيًا أصعب. وبالإضافة إلى ذلك، إنه يوفر إمكانية رؤية أثناء التحقق من حالة سلامة الجهاز، بما في ذلك مدى تحديث الجهاز، في كل محاولة تسجيل دخول واحدة. ومع قدرة المعالجة الذاتية من Duo، يمكن أن يحافظ المستخدمون على أجهزتهم مصححة دون مساعدة من تكنولوجيا المعلومات.

المعالجة في سلامة

لا يعني التعافي من هجوم برامج فدية ضارة وإعادة النظام عبر الإنترنت بالضرورة أن المهاجم قد غادر البيئة. قد يحاول إنشاء تواجد ثابت للعودة لاحقًا. فهناك أسلوب شائع يتمثل في اختراق حسابات موجودة أو إنشاء حسابات جديدة، غالبًا بالوصول إلى الدليل النشط أو أدلة أخرى تحتوي على حسابات المستخدمين. يمكن أن توفر المصادقة متعددة العوامل MFA من Duo راحة البال لأن المهاجم الذي ما يزال موجودًا على الشبكة لا يمكنه التمحور والانتقال جانبيًا باستخدام بيانات الاعتماد المخترقة. كما يمكنها شراء الوقت ومنع المهاجم من إحداث ضرر أكبر بينما تتم معالجة الهجوم بشكل كامل، بإزالة كل آثار وجوده الثابت.

تنفيذ نموذج الأمان بنهج Zero Trust (انعدام الثقة)

نهج zero trust (انعدام الثقة)، المُصمم على مبدأ "لا تثق أبدًا، تحقق دائمًا" هو نموذج أمني يمكنه مساعدة المؤسسات بشكل استباقي على تنفيذ أفضل الممارسات المعروفة للحماية من الهجمات الإلكترونية، بما في ذلك برامج الفدية الضارة.

إن Zero trust (انعدام الثقة) مهم للغاية حيث أصدر البيت الأبيض أمرًا تنفيذيًا تحديدًا لتحويل نهج zero trust (انعدام الثقة) وMFA (المصادقة متعددة العوامل).

يوفر Duo المصادقة متعددة العوامل (MFA) التي يسهل نشرها وتنفيذها. كما يتيح للمؤسسات منح الوصول فقط إذا كان يمكن التحقق من مستخدم وجهازه والوثوق بهما. تُعد هذه القدرة على التحكم وإدارة الوصول هي إحدى الركائز الأساسية لنهج zero trust، والمصادقة متعددة العوامل (MFA) من Duo هي إحدى أولى الخطوات لتنفيذ إطار عمل zero trust (انعدام الثقة).

الخاتمة

ستكون برامج الفدية الضارة شائعة بشكل أكبر ويجب أن تكون الشركات أكثر يقظة. إن الهندسة الاجتماعية والتصيد الاحتيالي الموجه ناجحان نظرًا لأنهما يستغلان العنصر البشري لأمان المؤسسة. ويُعد تبني فلسفة الأمان بنهج zero trust الذي يبدأ بتقنية MFA القوية ومنصة الوصول الموثوقة مهمًا للبقاء متقدمًا على هجمات برامج الفدية الضارة.

تحديث دفاعك بما يفوق المصادقة متعددة العوامل (MFA) مع Duo

يمكن أن تدافع المؤسسات ضد تأثير برامج الفدية الضارة من خلال هجمات تصيد المعلومات المستهدفة والاجتماعية بتنفيذ سياسات الوصول المشروطة التي تستفيد من العوامل السياقية، مثل الموقع وموضع الجهاز، لإنشاء الثقة في المستخدمين وأجهزتهم.

تحمي منصة الأمان القائمة على السحابة من Duo الوصول إلى كل التطبيقات، لأي مستخدم وجهاز، من أي مكان. لقد بسّطنا الوصول الآمن لمعالجة مخاطر الهوية والجهاز بست قدرات هامة:

1. تحقق من هويات المستخدمين بطرق المصادقة متعددة العوامل الآمنة والمرنة.
2. استلم تجربة تسجيل دخول متسقة مع Duo Single Sign-On، مما يوفر وصولاً مركزيًا إلى تطبيقات السحابة وموقع العمل.
3. احصل على إمكانية رؤية في كل جهاز، وحافظ على مخزون مفصل لكل الأجهزة الذي يصل إلى تطبيقات الشركة.
4. أنشئ ثقة الجهاز من خلال فحوصات السلامة والموضع للأجهزة المُدارة أو غير المُدارة قبل منح وصول التطبيق.
5. نفّذ سياسات الوصول متعددة المستويات لتقييد الوصول لهؤلاء المستخدمين والأجهزة التي تلبي مستويات تدارك المخاطر للمؤسسة.
6. راقب سلوك تسجيل الدخول الخطر واكتشفه باستخدام Duo Trust Monitor، أو استكشف السجلات إلى SIEM الخاص بك، لمعالجة الأحداث المشبوهة مثل تسجيل الجهاز للمصادقة أو تسجيل الدخول من موقع غير متوقع.

ما سبب اختيار Duo؟

السرعة إلى الأمان

توفر Duo كتل البناء لنهج zero trust (انعدام الثقة) في حل واحد سريع ويسهل نشره على المستخدمين. ووفقًا لحالة استخدامها المعينة، يمكن تشغيل بعض الأجهزة العميلة في غضون دقائق.

سهولة الاستخدام

يمكن أن يسجّل المستخدمون ذاتيًا بمجرد تنزيل تطبيق ما من متجر التطبيقات ويسجلون الدخول. عناصر التحكم في الصيانة والسياسة سهلة للمسؤولين للتحكم في إمكانية الرؤية الواضحة والحصول عليها.

يتم تصميم منتجنا

الذي يتكامل مع كل التطبيقات ليكون غير محدد ويعمل مع الأنظمة القديمة. بغض النظر عن مورّدي تكنولوجيا المعلومات والأمن الذين تتعامل معهم، مع Duo، ما يزال بإمكانك الوصول بأمان إلى جميع تطبيقات العمل، لجميع المستخدمين، من أي مكان.

تكلفة إجمالية أقل للملكية (TCO)

لأن تطبيق Duo يتسم بالسهولة وعدم تطلبه استبدال الأنظمة، لأنه يتطلب موارد أقل بكثير في الوقت والتكلفة، مما يساعدك على العمل بسرعة وبدء الرحلة إلى نموذج Zero Trust (انعدام الثقة).

المراجع

شهد العالم الذي ضربته الجائحة نموًا بنسبة 150% في برامج الفدية، https://cisomag.eccouncil.org/growth-of-ransomware-2020/، مجلة CISO، إصدار 5 مارس 2021

حصري: ستعطي الولايات المتحدة اختراقات برامج الفدية أولوية مماثلة للإرهاب، https://www.reuters.com/technology/exclusive-us-give-ransomware-hacks-similar-priority-terrorism-official-says-2021-06-03/، نقلاً عن رويترز، 3 يونيو 2021

تعلن NIST عن المتعاونين التقنيين في مشروع NCCoE Zero Trust، https://www.hstoday.us/industry/emerging-innovation/nist-announces-tech-collaborators-on-nccoe-zero-trust-project/، طبقًا لمجلة Homeland Security Today، إصدار 24 سبتمبر 2021

ورقة حقائق: جهود الولايات المتحدة العامة المستمرة لمكافحة برامج الفدية، https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/13/fact-sheet-ongoing-public-u-s-efforts-to-counter-ransomware، البيت الأبيض، 13 أكتوبر 2021

أنواع التشفير: متماثل أم غير متماثل؟ RSA أم AES؟، https://preyproject.com/blog/en/types-of-encryption-symmetric-or-asymmetric-rsa-or-aes/، Prey Project، 15 يونيو 2021

ما نعرفه عن DarkSide، مجموعة القراصنة الروسية التي أحدثت خرابًا شاملاً على الساحل الشرقي، https://www.heritage.org/cybersecurity/commentary/what-we-know-about-darkside-the-russian-hacker-group-just-wreaked-havoc، مجمع The Heritage Foundation، لعام 20 مايو 2021

ما يمكن أن نتعلمه من القائمين على برامج الفدية "تقارير أمنية"، https://www.coveware.com/blog/2021/6/24/what-we-can-learn-from-ransomware-actor-security-reports، شركة Coveware، عام 24 يونيو 2021

حالة برامج الفدية لعام 2021، https://secure2.sophos.com/en-us/content/state-of-ransomware.aspx، Sophos، 2021

عملية التنقيب في البيانات: الفرق بين التنقيب في البيانات وجمع البيانات، https://www.import.io/post/the-difference-between-data-mining-data-harvesting، Import.io، 23 أبريل 2019

برامج الفدية: العدو على الأبواب، https://ussignal.com/blog/ransomware-enemy-at-the-gate، US Signal، 3 سبتمبر 2021

تقرير التحقيقات في خرق البيانات لعام 2020، https://enterprise.verizon.com/content/verizonenterprise/us/en/index/resources/reports/2020-data-breach-investigations-report.pdf، Verizon، 2020

تتراجع البرامج الضارة، لكن هجمات إنترنت الأشياء وبرامج الفدية آخذة في الارتفاع، https://www.techrepublic.com/article/malware-is-down-but-iot-and-ransomware-attacks-are-up/، Tech Republic، 23 يونيو 2020

ضحية واحدة لبرامج الفدية كل 10 ثوانٍ في عام 2020، https://www.infosecurity-magazine.com/news/one-ransomware-victim-every-10/، Infosecurity Magazine، 5 فبراير 2021

إحصائيات مرعبة: 1 من كل 5 أمريكيين وقع ضحية لبرامج الفدية، https://sensorstechforum.com/1-5-americans-victim-ransomware/، Sensors Tech Forum، 19 أغسطس 2019

تتوقع Gartner أن يتجاوز الإنفاق العالمي على الأمن وإدارة المخاطر 150 مليار دولار في عام 2021، https://www.gartner.com/en/newsroom/press-releases/2021-05-17-gartner-forecasts-worldwide-security-and-risk-managem، Gartner، 17 مايو 2021

لقد وقعت 1 من كل 5 من شركات صغيرة ومتوسطة ضحية لهجوم برمجيات الفدية، https://www.helpnetsecurity.com/2019/10/17/smbs-ransomware-attack/، Help Net Security، 17 أكتوبر 2019

برامج الفدية – كيفية إيقاف هذا السبب الرئيسي والمتنامي لوقت التوقف عن العمل، https://polyverse.com/blog/ransomware-how-to-stop-this-growing-major-cause-of-downtime، Polyverse.com

الماضي الغريب لبرامج الفدية، https://theworld.org/stories/2017-05-17/strange-history-ransomware، PRI The World، 17 مايو 2017

الخط الزمني لبرامج الفدية، https://www.tcdi.com/ransomware-timeline، tcdi.com، 27 ديسمبر 2017

تاريخ هجمات برامج الفدية: أكبر وأسوأ هجمات برامج الفدية في التاريخ، https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time، Digital Guardian، 2 ديسمبر 2020

دفعت إحدى أكبر شركات التأمين الأمريكية بحسب ما ورد للمتسللين فدية قدرها 40 مليون دولار بعد هجوم سيبراني، https://www.businessinsider.com/cna-financial-hackers-40-million-ransom-cyberattack-2021-5، Business Insider، 22 مايو 2021

أنفقت أتلانتا 2.6 مليون دولار للتعافي من تهديد بقيمة 52 ألف دولار من برامج الفدية، https://www.wired.com/story/atlanta-spent-26m-recover-from-ransomware-scare، Wired.com، 23 أبريل 2018

هجوم سيبراني: تلقي الولايات المتحدة والمملكة المتحدة اللوم على كوريا الشمالية لهجوم WannaCry، https://www.bbc.com/news/world-us-canada-42407488، BBC.com، 19 سبتمبر 2017

برامج الفدية: الآن تصل خسائرها مليار دولار سنويًا وتتزايد، https://www.nbcnews.com/tech/security/ransomware-now-billion-dollar-year-crime-growing-n704646، NBCNews.com، 9 يناير 2017

قصة NotPetya غير المروية، الهجوم السيبراني الأكثر فتكًا في التاريخ، https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world، Wired.com، 22 أغسطس 2018

برامج الفدية في منشآت الرعاية الصحية: نحن في المستقبل، https://mds.marshall.edu/cgi/viewcontent.cgi?article=1185&context=mgmt_faculty، Marshall University Digital Scholar، خريف 2017

برنامج فدية جديد يحتجز ملفات Windows كرهينة، ويطلب 50 دولار، https://www.networkworld.com/article/2265963/new-ransomware-holds-windows-files-hostage--demands--50.html، NetworkWorld.com، 26 مارس 2009

منع الابتزاز الرقمي، https://subscription.packtpub.com/book/networking_and_servers/9781787120365/4/ch04lvl1sec24/the-advancement-of-locker-ransomware-winlock، PackIt، مايو 2017

التأثيرات التي لا يمكن التعافي منها لهجوم برامج الفدية، https://www.crowdstrike.com/blog/irreversible-effects-ransomware-attack، CrowdStrike، 20 يوليو 2016

عصر جديد من دعوات العمل عن بُعد لعقلية أمنية حديثة، نتائج استطلاع Thales العالمي لقادة تكنولوجيا المعلومات، https://www.businesswire.com/news/home/20210914005014/en/New-Era-of-Remote-Working-Calls-for-Modern-Security-Mindset-Finds-Thales-Global-Survey-of-IT-Leaders، Business Wire، 14 سبتمبر 2021

يرى مكتب التحقيقات الفيدرالي ارتفاعًا في تقارير الجرائم الإلكترونية أثناء جائحة فيروس كورونا، https://thehill.com/policy/cybersecurity/493198-fbi-sees-spike-in-cyber-crime-reports-during-coronavirus-pandemic، The Hill، 16 أبريل 2020

ملخص أمان Symantec - سبتمبر 2021، https://symantec-enterprise-blogs.security.com/blogs/feature-stories/symantec-security-summary-september-2021، Symantec Security، 27 سبتمبر 2021

تقرير INTERPOL (الإنتربول) يُظهر معدلاً ينذر بالخطر من الهجمات الإلكترونية خلال جائحة فيروس كورونا، https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19، منظمة Interpol، 4 أغسطس 2020

أفضل توجهات Gartner للأمان والمخاطر لعام 2021، https://www.gartner.com/smarterwithgartner/gartner-top-security-and-risk-trends-for-2021، شركة Gartner، 5 أبريل 2021

يكشف استطلاع Gartner عن خطة 82% من قادة الشركات للسماح للموظفين بالعمل عن بُعد لبعض الوقت، https://www.gartner.com/en/newsroom/press-releases/2020-07-14-gartner-survey-reveals-82-percent-of-company-leaders-plan-to-allow-employees-to-work-remotely-some-of-the-time، شركة Gartner، 14 يوليو 2020

تسلّط شركة Gartner الضوء على "أمان الهوية أولاً" كأحد أهم توجهات الأمان لعام 2021، https://www.attivonetworks.com/blogs/gartner-identity-first-security-in-2021، شركة Attivo، لتاريخ 27 أبريل 2021.

تقرير SonicWall للتهديدات السيبرانية لعام 2021، https://www.sonicwall.com/medialibrary/en/white-paper/2021-cyber-threat-report.pdf، شركة SonicWall، لعام 2021

أهم الثغرات التي تستخدمها عصابات برامج الفدية هي أخطاء VPN، لكن RDP ما يزال يحتل الصدارة، https://www.zdnet.com/article/top-exploits-used-by-ransomware-gangs-are-vpn-bugs-but-rdp-still-reigns-supreme، موقع ZDNet.com، 23 أغسطس 2020

ارتفع استغلال VPN في عام 2020، وتباطأت المؤسسات في معالجة العيوب الخطيرة، https://www.cybersecuritydive.com/news/trustwave-network-security-remote-access/602044/، شركة Cybersecurity Dive، 18 يونيو 2021

بحث جديد: ما مدى فعالية الأمان الأساسي للحساب في منع الاحتيال، https://security.googleblog.com/2019/05/new-research-how-effective-is-basic.html، Google Blog، 17 مايو 2019

أهم إحصائيات وتوجهات وحقائق الأمن السيبراني، https://www.csoonline.com/article/3634869/top-cybersecurity-statistics-trends-and-facts.html، CSOonline.com، 7 أكتوبر 2021

حماية الشركات من الهجمات السيبرانية، https://www.inc.com/knowbe4/protecting-companies-from-cyberattacks.html، Inc.com، 20 سبتمبر 2021

قائمة تهديدات: يعرف الناس أن إعادة استخدام كلمات المرور أمر غبي، لكنهم ما يزالون يفعلون ذلك، https://threatpost.com/threatlist-people-know-reusing-passwords-is-dumb-but-still-do-it/155996/، Threatpost، 25 مايو 2020

تُظهر دراسة Synopsys أن 91% من التطبيقات التجارية تحتوي على مكونات مفتوحة المصدر قديمة أو مهجورة، https://www.securitymagazine.com/articles/92368-synopsys-study-shows-91-of-commercial-applications-contain-outdated-or-abandoned-open-source-components، مجلة Security Magazine، 12 مايو 2020

الحيلة الجديدة الخطيرة لبرامج الفدية هي التشفير المزدوج لبياناتك، https://www.wired.com/story/ransomware-double-encryption/، Wired.com، 17 مايو 2021

مكافحة الحركة الجانبية وصعود برامج الفدية، https://www.msspalert.com/cybersecurity-guests/combating-lateral-movement-and-the-rise-of-ransomware، MSSP Alert، 24 يونيو 2021

الحركة الجانبية، https://attack.mitre.org/tactics/TA0008/، MITRE| ATT&CK، 17 أكتوبر 2019

الصناعات المتضررة من برامج الفدية، https://airgap.io/blog/industries-impacted-by-ransomware، AirGap.com

الدفاع ضد هجمات برامج الفدية والرد عليها، https://www.gartner.com/en/documents/3978727/defend-against-and-respond-to-ransomware-attacks، Gartner Research، 26 ديسمبر 2019

الأمر التنفيذي بشأن تحسين الأمن السيبراني للأمة، https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/، البيت الأبيض. 12 مايو 2021