بيان إخباري

العلاقات الإعلامية
شارون ديفان
أوك كونسلتينغ للعلاقات العامة
+971 50 8444 823
sharon@oakconsulting.biz

تقرير سيسكو نصف السنوي للأمن 2016 يتوقع جيل جديد من برمجيات طلب الفدية وظهور أساليب الجديدة تضاعف أرباح المهاجمين

إغلاق الفرص أمام المهاجمين أبرز أولويات المؤسسات، وسيسكو تقود جهود القطاع في تقليل زمن الكشف عن التهديدات لتحقق زمناً قدره 13 ساعة فقط

دبي، الإمارات العربية المتحدة – 28 يوليو 2016 – أظهر تقرير سيسكو نصف السنوي للأمن الإلكتروني 2016 أن المؤسسات غير مهيّأة لمواجهة السلالات المطورة من برمجيات طلب الفدية الأكثر تعقيداً في المستقبل. فالبنية التحتية الهشة وضعف سلامة الشبكات وبطء سرعة الكشف عن التهديدات توفر للمهاجمين فسحة من الوقت ومجالاً واسعاً للعمل. وبحسب نتائج التقرير، فإن المحاولات المضنية لتحديد مجال عمل المهاجمين هو أكبر تحدٍّ تواجهه الشركات ويهدد الأسس اللازمة للمضي قدماً في مسيرة التحول الرقمي. ومن بين النتائج الأخرى لتقرير سيسكو نصف السنوي للأمن، ظهر بأن المهاجمين يعملون على توسعة نطاق تركيزهم ليشمل الهجمات على الخوادم، فضلاً عن تطوير أساليب الهجوم وزيادة استخدام التشفير للتغطية على أنشطتهم.

وحتى تاريخ صدور التقرير للعام 2016، فقد أصبحت برمجيات طلب الفدية أكثر البرمجيات الضارة تحقيقاً للأرباح في التاريخ، وتتوقع سيسكو أن نشهد استمراراً لذلك التوجه مع ظهور برمجيات أكثر شراسة يمكنها الانتشار ذاتياً والسيطرة على شبكات بأكملها، وبالتالي السيطرة على الشركات، لتكون أشبه بالرهائن. وستتمكن السلالات الجديدة من برمجيات طلب الفدية، والمؤلفة من وحدات مترابطة، قادرة على تغيير الأساليب والتكتيك الهجومي بشكل سريع لتعزيز كفاءتها، بحيث يمكن لتلك البرمجيات مستقبلاً، على سبيل المثال، تفادي الكشف عنها من خلال قدرتها على تقييد استخدام وحدة المعالجة المركزية والإحجام عن أنشطة القيادة والتحكم. وسيكون بمقدور تلك السلالات الجديدة الانتشار بسرعة أكبر والتكاثر ذاتياً داخل المؤسسة قبل تنسيق أنشطة الفدية.

في هذا السياق قال مايك ويستون، نائب الرئيس لدى سيسكو الشرق الأوسط: "فيما تستفيد المؤسسات من نماذج الأعمال الجديدة التي يقدمها التحول الرقمي، يبقى الأمن هو الأساس الأول. فالمهاجمون أصبحوا يمرّون دون الكشف عنهم وأصبحوا يزيدون من وقت عملهم، مما يعني أن العملاء بحاجة إلى قدرات أكبر لمراقبة الشبكات إذا ما أرادوا قطع السبل على المهاجمين، كما أن عليهم تحسين أنشطتهم، كترقيع البنى التحتية القديمة وإخراج تلك التي تفتقر إلى الإمكانات الأمنية المطوّرة عن الخدمة. وفيما يواصل

المهاجمون استفادتهم من الهجمات وتحويلها إلى مكاسب مالية لهم لتصبح نموذج أعمال يدرّ عليهم الأرباح، تعمل سيسكو مع عملائنا لمساعدتهم في مضاهاة وتجاوز مستوى التطور والرؤية والتحكم لدى المهاجمين."

ولا تزال إمكانية رؤية ومراقبة الشبكة والنقاط النهائية تحدياً بارزاً، فمتوسط الوقت الذي تستغرقه المؤسسات في الكشف عن الهجمات الجديدة يصل إلى 200 يوم. إلا أن الزمن الوسيط الذي تستغرقه سيسكو للكشف عن التهديدات يتفوق بشكل واضح على القطاع، حيث حقق زمناً جديداً قدره 13 ساعة فقط للكشف عن الهجمات غير المعروفة سابقاً، وذلك خلال الأشهر الستة المنتهية في أبريل 2016 – مقارنة مع 17.5 ساعة في الفترة المنتهية بشهر أكتوبر 2015. ويعد الكشف السريع عن التهديدات عاملاً حيوياً في تضييق الخناق على المهاجمين وتقليل الأضرار التي تنشأ عن أنشطتهم إلى أقل قدر ممكن. وتم حساب الأرقام بناء على بيانات القياس الأمني عن بعد، والتي تم جمعها من منتجات سيسكو الأمنية المستخدمة حول العالم.

وفيما يواصل المهاجمون ابتكارهم، يستمر جانب الدفاع في محاولات مضنية للحفاظ على أمن اجهزتهم وأنظمتهم، إذ أن الأنظمة التي لا تتمتع بالدعم المناسب ووجود الرقع الأمنية المطلوبة تتيح فرصاً إضافية للمهاجمين للوصول بسهولة إلى تلك الأنظمة دون الكشف عنهم، كما تزيد من الضرر الناشئ وتعزز أرباح الفريق المهاجم. يظهر تقرير سيسكو نصف السنوي للأمن الإلكتروني 2016 أن هذا التحدي مستمر على نطاق عالمي، ففي الوقت الذي شهدت فيه مؤسسات عاملة في قطاعات حيوية، كالرعاية الصحية، ارتفاعاً ملموساً في الهجمات خلال الأشهر القليلة الماضية، تشير نتائج التقرير إلى ان جميع القطاعات والمناطق حول العالم تمثل هدفاً للهجمات. فقد شهدت المؤسسات على اختلافها، من النوادي والجمعيات الخيرية والمنظمات غير الحكومية إلى شركات الإلكترونيات وغيرها ارتفاعاً في وتيرة الهجمات خلال النصف الأول من العام 2016. وعلى الساحة العالمية، تتضمن المخاوف الجيوسياسية التعقيدات التنظيمية والسياسات المتضاربة للأمن الإلكتروني في الدول. وقد تؤدي الحاجة إلى ضبط البيانات أو الوصول إليها إلى تقييد التجارة العالمية والتعارض معها في ظل المشهد المعقد والمتنامي للتهديدات.

المهاجمون يعملون دون قيود

عندما يتوفر للمهاجمين وقت أطول للعمل دون اكتشافهم فإن ذلك يعني تحقيق المزيد من الأرباح. ويشير تقرير سيسكو إلى ان أرباح المهاجمين حققت ارتفاعاً هائلاً في النصف الأول من العام 2016 بسبب العوامل التالية:

توسع نطاق التركيز: فدائرة تركيز المهاجمين اتسعت لتتجاوز استغلال الثغرات لدى العملاء إلى استغلالها في الخوادم، بحيث يتجنبون اكتشافهم ويحققون أعلى قدر من الأضرار والأرباح في آن واحد.

- لا تزال الثغرات في برنامج "أدوبي فلاش" من أهم الأهداف للإعلانات الضارة ومختلف برمجيات استغلال الثغرات. وفي مجموعة Nuclear التي تلقى رواجاً عالياً، شكّل برنامج "فلاش" نسبة 80 بالمائة من أهداف المحاولات الناجحة.
- كما شهدت سيسكو توجهات جديدة في الهجمات بواسطة برمجيات طلب الفدية التي تستغل نقاط الضعف في الخوادم، وبخاصة في خوادم JBoss، حيث وجد بأن 10 بالمائة من تلك الخوادم المتصلة بالإنترنت حول العالم عرضة للخطر.

تم التعرف على العديد من نقاط الضعف في خوادم JBoss والتي تستخدم لإضعاف تلك الأنظمة قبل خمس سنوات، مما يعني أن الإجراءات البسيطة للترقيع والتحديث كانت لتمنع وقوع الهجمات بكل سهولة.

تطور أساليب الهجوم: خلال النصف الأول من العام 2016، استمر المهاجمون في تطوير أساليبهم الهجومية للاستفادة من ضعف إمكانات الرؤية لدى أهدافهم.

- ارتفع عدد حالات استغلال برمجيات Windows Binary لتصبح الوسيلة الأولى لهجمات الويب خلال الأشهر الستة الماضية، حيث تحقق تلك الوسيلة موطئ قدم ثابت للمهاجمين في البنية التحتية للشبكة، وتزيد من صعوبة التعرف إلى الهجمات والقضاء عليها.
- وخلال تلك الفترة الزمنية، انخفض عدد حالات التلاعب للحصول على البيانات الشخصية عبر موقع فيسبوك لتصبح في المركز الثاني بعد أن كانت في المركز الأول عام 2015.

إخفاء الآثار: يزداد استخدام المهاجمين للتشفير كوسيلة للتغطية على مختلف مكونات وعناصر أعمالهم، مما يزيد من صعوبات الكشف لدى المدافعين.

- شهدت سيسكو ارتفاعاً في استخدام العملات الرقمية المشفرة وأمن طبقات النقل وبرنامج Tor، والذي يسمح بالتواصل عبر الشبكة دون إظهار الهوية.
- ومن المثير للاهتمام أن البرمجيات الضارة المشفرة عبر HTTPS والمستخدمة في برامج الإعلانات الضارة سجلت زيادة قدرها 300 بالمائة بين ديسمبر 2015 ومارس 2016، حيث تمكّن تلك البرمجيات المهاجمين من إخفاء انشطتهم على الشبكة وزيادة الوقت المتاح لهم للعمل.

<u>المدافعون يواجهون صعوبات في تخفيف نقاط الضعف وسد الثغرات</u>

يواجه المدافعون صعوبات جمّة في محاولتهم لمواكبة خطوات المهاجمين في ظل ازدياد تعقيد الهجمات ومحدودية الموارد وشيخوخة البنية التحتية. وتشير البيانات إلى أن إحتمال اهتمام المدافعين بالتعامل مع سلامة الشبكات، كاستخدام الرقع الأمنية، يقل كلما إزدادت أهمية التقنيات لعمليات الأعمال. على سبيل المثال:

- في عالم متصفحات الإنترنت، يستخدم 75 إلى 80 بالمائة من مستخدمي متصفح غوغل كروم، والذي يعمل بنظام التحديث التلقائي، أحدث إصدار من المتصفح أو متأخراً بإصدار واحد فقط.
- بالانتقال من المتصفح إلى البرمجيات، تشهد برامج جافا بطئاً في الانتقال إلى الإصدارات الأحدث، إذ تستخدم ثلث الأنظمة المشمولة بالدراسة الإصدار Java SE 6 الذي تخطط أوراكل للتوقف عن تشغيله تماماً (الإصدار الحالي هو SE 10).
- في نظام التشغيل Microsoft Office 2013، الإصدار 15x، تستخدم نسبة 10 بالمائة أو أقل من مستخدمي الإصدار أحدث نسخة من حزمة الخدمات.

وبالإضافة لما سبق، وجدت سيسكو بأن قدراً كبيراً من البنية التحتية لم يحصل على الدعم أو يعمل في ظل وجود نقاط ضعف معروفة، وهي مشكلة شائعة بين البائعين والنقاط النهائية. وقام باحثو سيسكو بدراسة 103,121 جهاز متصل بالإنترنت من سيسكو ليجدوا ما يلي:

- يبلغ متوسط نقاط الضعف 28 مشكلة معروفة يعمل الجهاز بوجودها.
- تعمل الأجهزة مع وجود نقاط الضعف المعروفة لمتوسط 5.64 سنوات.
- أكثر من 9 بالمائة من الاجهزة تعاني من نقاط ضعف أقدم من 10 سنوات.

وبالمقارنة، درست سيسكو البنية التحتية للبرمجيات في عينة تضم أكثر من 3 ملايين تثبيت، كانت الغالبية العظمى منها تعمل بأنظمة Apache و OpenSSH وبمتوسط 16 نقطة ضعف معروفة وزمن تشغيل قدره 5.05 سنة.

تعدّ تحديثات المتصفح التحديثات الأخفّ للنقاط النهائية، بينما من الأصعب تحديث التطبيقات المؤسسية والبنية التحتية الخاصة بالخوادم ويمكن أن تسبب مشاكل في استمرارية الأعمال. ومن الأهمية بمكان، كلما زادت أهمية التطبيق لعمليات الأعمال، قل إحتمال التعامل معه بشكل متكرر، مما يساهم في خلق الثغرات وإتاحة الفرص أمام المهاجمين.

سيسكو تنصح بخطوات بسيطة لحماية بيئات الأعمال

لاحظ باحثو منظمة تالوس التابعة لسيسكو أن المؤسسات التي تتخذ عدداً من الخطوات البسيطة والهامة يمكنها أن تعزّز أمن عملياتها بشكل كبير، بما في ذلك:

- **تعزيز سلامة الشبكة** من خلال مراقبة الشبكة واستخدام الرقع الأمنية والتحديث في الوقت المناسب، تقسيم الشبكات، واستخدام الدفاعات على الحواف، بما فيها أمن البريد الإلكتروني وأمن الويب وحلول الجيل الجديد من الجدار الناري والجيل التالي من حلول منع التطفل.
- **الدفاعات المتكاملة**، من خلال الاستفادة من منهجية هيكلية تجاه الأمن، خلافا لاستخدام المنتجات المتخصصة.
- **قياس الوقت اللازم للكشف**، التصميم على أسرع وقت ممكن للكشف عن التهديدات ومن ثم تخفيف مخاطرها فوراً. جعل تلك المقاييس جزءاً من السياسة الأمنية للمؤسسة من الآن فصاعدا.
- **حماية مستخدميك أينما كانوا** وأينما كان مكان عملهم، بحيث لا تقتصر الحماية على الأنظمة التي يتفاعلون معها أو على وقت تواجدهم على الشبكة المؤسسية.
- **دعم البيانات الحرجة**، واختبار فعاليتها بشكل دوري مع التأكد من كون نسخ الدعم غير معرّضة للهجمات.

حول التقرير

يدرس تقرير سيسكو نصف السنوي للأمن 2016 أحدث معلومات استقصاء التهديدات التي تجمعها سيسكو لاستقصاء الأمن الجماعي. ويقدم التقرير الأفكار والرؤى القائمة على البيانات وتوجهات الأمن الإلكتروني من النصف الأول من العام، إلى جانب التوصيات القابلة للتطبيق بهدف تحسين الوضع

الأمني. يقوم التقرير على البيانات التي تم جمعها على نطاق واسع، بحيث تفوق 40 مليار نقطة من القياس اليومي عن بعد. يعمل باحثو سيسكو على ترجمة البيانات الاستقصائية إلى حماية فورية لمنتجاتنا وخدماتنا التي يمكن تسليمها فوراً إلى عملاء سيسكو حول العالم.

مصادر الدعم

مقطع فيديو سيسكو مع دايفيد غوكلر، ستيف مارتينو: تقرير سيسكو نصف السنوي للأمن 2016

تقرير سيسكو نصف السنوي للأمن 2016

رسومات تقرير سيسكو نصف السنوي للأمن 2016

تابعو سيسكو على تويتر @CiscoSecurity

تابعوا سيسكو على فيسبوك

حول سيسكو

سيسكو هي الرائد العالمي في مجال التكنولوجيا والتي تمكِّن الإنترنت من العمل منذ عام 1984. الشركة مدرجة في بورصة الأوراق المالية "ناسداك" تحت الرمز (CSCO). يساعد موظفونا ومنتجاتنا وشركاؤنا المجتمع في التواصل الآمن واغتنام الفرص الرقمية المستقبلية اليوم. اكتشف المزيد عبر الرابط newsroom.cisco.com وتابعنا على تويتر @Cisco