المقر الرئيسي في أوروبا
Cisco Systems International
BV Amsterdam,
The Netherlands

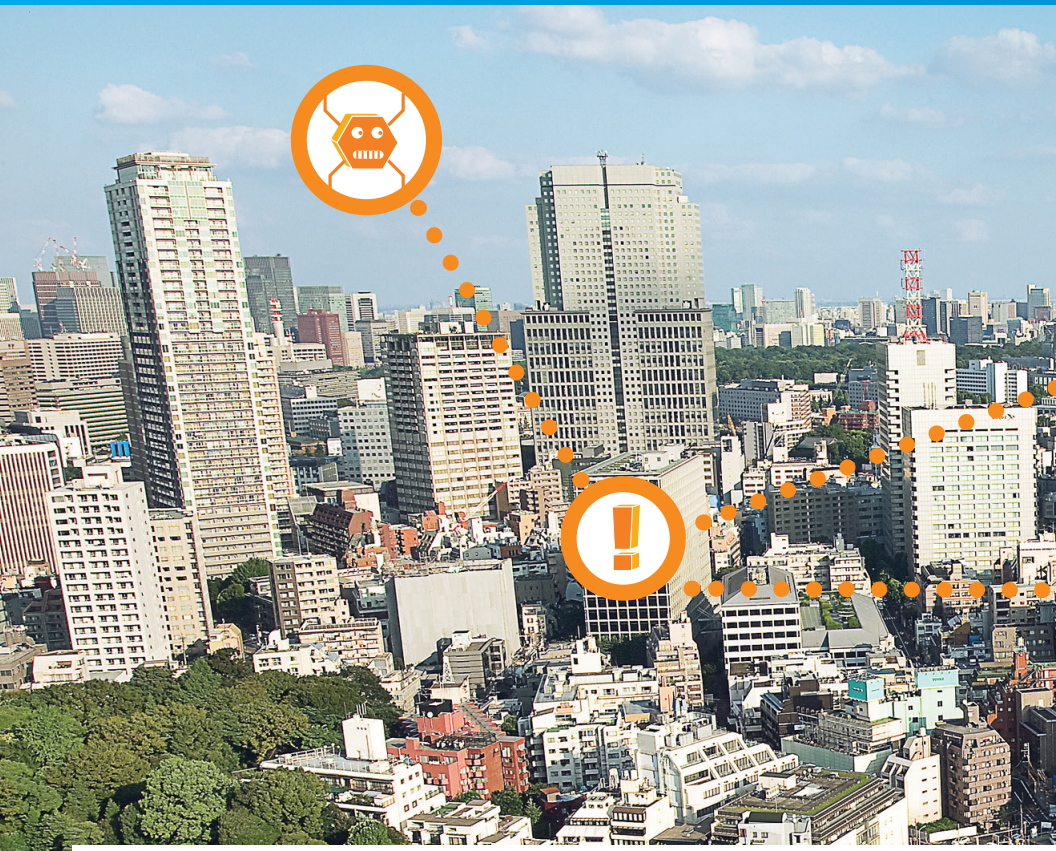
المقر الرئيسي لدول آسيا والمحيط الهادئ
Cisco Systems (USA) Pte. Ltd.
Singapore

المقر الرئيسي بأمريكا
Cisco Systems, Inc.
San Jose, CA

يوجد لدى Cisco أكثر من 200 مكتب في جميع أنحاء العالم. تتوفر قائمة بالعناوين وأرقام الهواتف وأرقام الفاكسات على موقع ويب الخاص بشركة Cisco على العنوان www.cisco.com/go/offices.

تقرير الأمان السنوي لعام 2013 من Cisco

الحياة في عالم "الاتصالات المفتوحة" السائد تلك الأيام.



يستفيد مجرمو الإنترنت من مساحة الهجوم التي تتسع دائرتها بشكل سريع في عالم "الاتصالات المفتوحة" السائد تلك الأيام، حيث يستخدم الأفراد أي جهاز للوصول إلى تطبيقات الأعمال في أي بيئة شبكات تستخدم أجهزة لامركزية تستند إلى السحابة. ويلقي تقرير الأمان السنوي لعام *2013* من *Cisco*® الضوء على اتجاهات التهديدات العالمية المستندة إلى بيانات مستقاة من العالم الحقيقي، ويوفر رؤية وتحليلاً يساعد المؤسسات التجارية والحكومات على تحسين وضعها الأمني في المستقبل. ويجمع التقرير بين أبحاث الخبراء ومعلومات الأمان التي تم تجميعها من كل أقسام Cisco، مع التركيز على البيانات التي تم تجميعها أثناء عام 2012.

المحتويات

الاتصال الوثيق بين الأجهزة والسحب والتطبيقات

إن عالم الاتصالات المفتوحة والإنترنت الشامل يعد تطورًا في الاتصال والتعاون الذي يتسم بسرعة الانتشار. حيث يعني الاتصال الوثيق بين الأجهزة والسحب والتطبيقات.

وبينما لا يعد هذا التطور غير متوقع، فإن مؤسسات اليوم قد تكون غير مستعدة للتعامل مع واقع التنقل في عالم "الاتصالات المفتوحة"؛ من ناحية الأمان على الأقل.

يقول كريس يونج؛ نائب رئيس مجموعة شؤون الأمان والحكومات في Cisco: "يتمثل جوهر الاتصالات المفتوحة في: أننا نصل بسرعة إلى النقطة التي تقل عندها بشدة احتمالية وصول مستخدم إلى عمل من خلال شبكة الشركة".
"وبشكل متزايد، يتعلق الأمر بأي جهاز في أي مكان يأتي على أي مثيل للشبكة. تحاول الأجهزة القابلة للدخول إلى الإنترنت ـ مثل الهواتف الذكية والأجهزة اللوحية وغيرها ـ الاتصال بتطبيقات يمكنها العمل في أي مكان وتشمل سحابة البرامج العامة كخدمة (SaaS)، في سحابة خاصة أو في سحابة مختلطة".

وفي الوقت نفسه، هناك تطور آخر في الطريق وهو اتجاه بشكل مطرد نحو تكوين "إنترنت شامل". وهذا هو الاتصال الذكي بين:

- **الأشخاص:** أي الشبكات الاجتماعية والمراكز السكانية والكيانات الرقمية
- **العمليات:** أي الأنظمة وعمليات الأعمال
- **البيانات:** أي شبكة الإنترنت العالمية والمعلومات
- **الأشياء:** أي العالم المادي والأجهزة والأشياء

"وبشكل متزايد، يتعلق الأمر بأي جهاز في أي مكان يأتي من أي مثيل للشبكة. كل الأجهزة التي تدعم خدمة الإنترنت - الهواتف الذكية، والأجهزة اللوحية، وغيرها الكثير - تحاول الاتصال بالتطبيقات التي يجري تشغيلها في أي مكان".

كريس يونج، نائب رئيس مجموعة شؤون الأمان والحكومات في Cisco

"سيؤدي نمو وتجميع الأشخاص والعمليات والبيانات والأشياء على الإنترنت إلى جعل التواصل الشبكي أكثر صلة وقيمة من أي وقت مضى".

نانسي كام وينجت، مهندسة متميزة في Cisco

يستفيد الإنترنت الشامل من أساس "إنترنت الأشياء"[1] من خلال إضافة ذكاء الشبكة التي تتيح التقارب والتنسيق والرؤية في كامل الأنظمة المتباينة في السابق. ولا تتعلق الاتصالات في "الإنترنت الشامل" بالأجهزة المحمولة أو الكمبيوتر المحمول والكمبيوتر المكتبي ولكن تتعلق أيضًا بالعدد المتزايد بسرعة من اتصالات الأجهزة بالأجهزة (M2M) التي تظهر على الإنترنت كل يوم. وغالبًا ما تكون هذه "الأشياء" عبارة عن أشياء نتعامل معها على أنها مسلم بها أو نعتمد عليها كل يوم ولا نفكر فيها بشكل معتاد على أنها متصلة؛ مثل نظام التدفئة المنزلية أو محرك الرياح أو السيارة.

الإنترنت الشامل عبارة عن حالة مستقبلية ـ على سبيل التأكيد ـ ولكنه غير بعيد للغاية عند التفكير في موضوع الاتصالات المفتوحة. وعلى الرغم من أنه ستنتج عنه أيضًا تحديات أمان تواجه المؤسسات، فإنه سيجلب فرصًا جديدة أيضًا. تقول نانسي كام وينجت، مهندسة متميزة في Cisco: "ستحدث أشياء مدهشة وسيتم إنشاؤها أثناء نمو إنترنت يحوي كل شيء. سيؤدي نمو وتقارب الأشخاص والعمليات والبيانات والأشياء على الإنترنت إلى جعل الاتصالات الشبكية أكثر صلة وقيمة عن أي وقت مضى. وبالتدريج، سينشئ "الإنترنت الشامل" إمكانات جديدة وتجارب أثرى وفرصًا اقتصادية غير مسبوقة للدول والأنشطة التجارية والأفراد".

كيفية تعقيد السحابة للأمان

أصبح تحدي تأمين مجموعة كبيرة من التطبيقات والأجهزة والمستخدمين، سواءً كان ذلك في سياق من "الاتصالات المفتوحة" أو "الإنترنت الشامل"، أكثر صعوبة نتيجة لانتشار السحب كوسيلة لإدارة أنظمة المؤسسات. ووفقًا للبيانات التي جمعتها Cisco، من المتوقع زيادة نسبة استخدام شبكة مركز البيانات العالمية أربعة أضعاف خلال الخمس سنوات التالية وستكون بيانات السحابة هي المكون الأسرع نموًا. وبحلول عام 2016، ستبلغ نسبة استخدام شبكة السحابة العالمية ما يقارب ثلثي إجمالي نسبة استخدام شبكة مركز البيانات.

ولا تقدم حلول الأمان التدريجية، مثل تطبيق جدران الحماية على حافة شبكة قابلة للتغيير، تأمينًا للبيانات التي تكون في حركة مستمرة الآن بين الأجهزة والشبكات والسحابة. حتى بين مراكز البيانات ـ والتي تستضيف الآن أهم بيانات المؤسسات "البيانات الكبيرة" ـ تصبح الظاهرية هي القاعدة أكثر من كونها استثناءً. ويتطلب التعامل مع تحديات الأمان الناتجة عن الظاهرية والسحابة إعادة التفكير حيال أوضاع الأمان بحيث تعكس عناصر التحكم الجديدة القائمة على النموذج أو المحيط ويجب تغيير نماذج الوصول والاحتواء القديمة من أجل تأمين نموذج العمل الجديد.

هذا ومن المتوقع أن تزيد نسبة استخدام شبكة مركز البيانات العالمية أربعة أضعاف خلال الخمس سنوات التالية وستكون بيانات السحابة هي المكون الأسرع نموًا. وبحلول عام 2016، ستبلغ نسبة استخدام شبكة السحابة العالمية ما يقارب ثلثي إجمالي نسبة استخدام شبكة مركز البيانات.

يعد الموظفون الشباب المتنقلون من بين العوامل المعقدة في معادلة من الاتصالات المفتوحة شيء. حيث تؤمن هذه المجموعة بأنه يجب أن تكون قادرة على القيام بالعمل من أي مكان يتواجدون فيه ومن أي أجهزة تتيسر لهم.

الموظفون المتصلون وخصوصية البيانات

يعد الموظفون الشباب المتنقلون من بين العوامل المعقدة في معادلة الاتصالات المفتوحة. حيث تؤمن هذه المجموعة بأنه يجب أن تكون قادرة على القيام بالعمل من أي مكان يتواجدون فيه ومن أي أجهزة تتيسر لهم. يشتمل تقرير الأمان السنوي لعام *2013* من *Cisco* لهذا العام على نتائج تقرير التقنية العالمية المتصلة لعام *2012* من *Cisco* والذي يستفيد من بحث تم إجراؤه عام 2011 عن الاتجاهات المتغيرة لطلاب الكليات والمتخصصين الشباب حول العالم بخصوص العمل والتقنية والأمان.

تلقي الدراسة الأخيرة مزيدًا من الضوء على اتجاهات الموظفين بخصوص الأمان مع تركيز خاص على الخصوصية وكم أو عدد المرات التي تتدخل فيه الشركة في رغبات الموظفين في التجوال الحر على الإنترنت أثناء العمل. كما تقوم دراسة تقرير التقنية العالمية المتصلة لعام *2012* من *Cisco* بالتحقق مما إذا كانت الخصوصية على الإنترنت لا تزال شيئًا يقلق جميع المستخدمين حياله دائمًا.

تحليل البيانات واتجاهات الأمان العالمية

يشتمل تقرير الأمان السنوي لعام 2013 من Cisco على تحليل مفصل للبرامج الضارة على الويب واتجاهات البريد العشوائي؛ وذلك بناءً على البحث الذي أجرته Cisco. بينما ركّز العديد ممن يعملون في "اقتصاد الظل" جهودهم في السنوات الأخيرة على تطوير أساليب معقدة بشكل متزايد، يوضح بحث Cisco أن مجرمي الإنترنت غالبًا ما يستخدمون طرقًا معروفة وأساسية لاختراق المستخدمين.

ويعد ارتفاع هجمات رفض الخدمة الموزع (DDoS) في العام الماضي مثالاً على الاتجاه ناحية "إعادة استخدام الأساليب القديمة" في الجريمة الإلكترونية. لسنوات عديدة، كانت هجمات رفض الخدمة الموزع - والتي يمكنها إحداث شلل لدى موفري خدمة الإنترنت (ISP) وقطع حركة المرور من وإلى مواقع الويب المستهدفة - تأتي متأخرة في قائمة أولويات أمان تقنية المعلومات لدى العديد من المؤسسات. ومع ذلك، تلعب الحملات الأخيرة ضد عدد من الشركات الكبرى - بما في ذلك المؤسسات المالية الأمريكية[2] - دورًا كتذكير بأن أي تهديد لأمان الإنترنت يحتمل تسببه في انقطاع كبير وتلف غير قابل للإصلاح إذا لم تكن المؤسسة مستعدة له. لذا، يجب أن تتسم المؤسسات بالحكمة بحيث تدرس كيفية التعامل مع حدث إنترنت ضار والتعافي منه؛ وذلك عند إعداد خطط إدارة استمرار نشاطها التجاري. وذلك بغض النظر عما إذا كان الحدث قد اتخذ شكل هجوم رفض الخدمة الموزع في الشركة أو أن منشأة تصنيع تستخدم الإنترنت قد أصبحت غير متصلة بشكل مفاجئ أو شيء آخر لم.

"نرى بعض التغييرات المزعجة في بيئة التهديدات التي تواجه الحكومات والشركات والمجتمعات".

جون ن. ستيوارت، نائب الرئيس ومسؤول الأمان في Cisco

"بينما نالت مناقشة أمان تقنية المعلومات أكثر من نصيبها العادل من التنبيه عبر السنوات، فإننا نرى بعض التغييرات المزعجة في بيئة التهديدات التي تواجه الحكومات والشركات والمجتمعات"، جون ن. ستيوارت، نائب الرئيس ومسؤول الأمان في Cisco. "لم تعد الجريمة الإلكترونية تمثل إزعاجًا أو تكلفة أخرى للقيام بالأعمال. ونحن بصدد نقطة تحول حيث تمثل الخسائر الاقتصادية الناتجة عن الجريمة الإلكترونية تهديدًا لإعاقة المكاسب الاقتصادية الناشئة بواسطة تقنية المعلومات. وبشكل واضح، نحن بحاجة إلى تفكير جديد وأساليب جديدة لتقليص الضرر الناتج عن تأثيرات الجريمة الإلكترونية على الصالح العام للعالم".

انتشار نقطة النهاية

يشتمل تطور "الاتصالات المفتوحة" على مليارات من الأجهزة المتصلة بالإنترنت؛ وقد تزايد عدد هذه الأجهزة حول العالم عام 2012 لأكثر من 9 مليارات.[3]

مع الأخذ في الاعتبار أن أقل من 1 في المائة من الأشياء في العالم الحقيقي متصلة اليوم، تظل هناك احتمالية كبيرة "لاتصال غير المتصل".[4] ومن المتوقع أنه باستخدام إنترنت يشمل حوالي 50 مليار من "الأشياء" المتصلة به الآن، سيزداد عدد الاتصالات إلى 13,311,666,640,184,600 بحلول عام 2020. وستؤدي إضافة "شيء" واحد متصل بالإنترنت (أي 50 مليار + 1) إلى زيادة عدد الاتصالات بمقدار 50 مليار أخرى.[5]

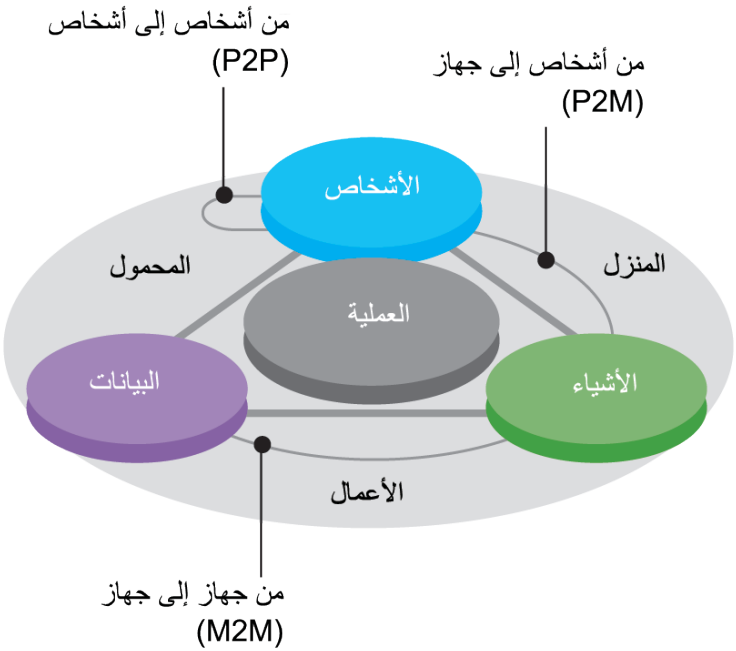
بالنسبة إلى "الأشياء" التي ستشكل "كل شيء" تدريجيًا، فإنها ستتراوح بين الهواتف الذكية إلى أنظمة التدفئة المنزلية ومن محركات الرياح إلى السيارات. يشرح دايف إفانز، مدير المستقبليات في Cisco مع مجموعة حلول الإنترنت، مفهوم تزايد نقطة النهاية فيقول: "عندما تصبح سيارتك متصلة بإنترنت شامل في المستقبل القريب، سيزيد ذلك من عدد الأشياء على الإنترنت بمقدار واحد. والآن، فكّر في العناصر العديدة الأخرى التي يمكن لسيارتك الاتصال بها؛ مثل السيارات الأخرى وإشارات المرور ومنزلك وموظفي الخدمة وتقارير الطقس واللافتات التحذيرية وحتى الطريق نفسه".[6]

في "الإنترنت الشامل"، تكون الاتصالات هي الأكثر أهمية. نوع الاتصالات وليس عددها هو الذي يؤسس قيمة بين الأشخاص والعمليات والبيانات والأشياء. وأخيرًا، سيقلص عدد الاتصالات من عدد الأشياء.[7] هذا ويتم تحفيز التزايد الكبير في الاتصالات الجديدة - والذي أصبح جزءًا من "الإنترنت الشامل" - بشكل أساسي بواسطة تطوير الكثير من الأجهزة المزودة بعنوان IP وأيضًا بواسطة الزيادة في توفر خدمة البروباند (النطاق العريض) العالمية وظهور العنونة

> "عندما تصبح سيارتك متصلة بإنترنت يحوي كل شيء في المستقبل القريب، فسيزيد ذلك من عدد الأشياء على الإنترنت بمقدار واحد. والآن، فكّر في العناصر العديدة الأخرى التي يمكن لسيارتك الاتصال بها؛ مثل السيارات الأخرى وإشارات المرور ومنزلك وموظفي الخدمة وتقارير الطقس واللافتات التحذيرية وحتى الطريق نفسه".
>
> دافيد إفانز، مدير المستقبليات في Cisco

الشكل 1: "الإنترنت الشامل"

"الإنترنت الشامل" هو الاتصال الذكي بين الأشخاص والعمليات والبيانات والأشياء.



في "الإنترنت الشامل"، تكون الاتصالات هي الأكثر أهمية.
نوع الاتصالات وليس عددها هو الذي يؤسس قيمة بين الأشخاص والعمليات والبيانات والأشياء.

باستخدام IPv6. لا ترتبط مخاطر الأمان الناتجة عن "الإنترنت الشامل" بتزايد نقطة نهاية "الاتصالات المفتوحة" - والتي تقربنا من بعضنا يومًا بعد يوم في عالم أكثر اتصالاً بدرجة كبيرة - فقط ولكن ترتبط أيضًا بفرصة العوامل الضارة في استخدام المزيد من الهجمات لاختراق المستخدمين والشبكات والبيانات. وتتسبب الاتصالات الجديدة نفسها في مخاطر لأنها ستنتج المزيد من البيانات المتحركة التي تحتاج إلى الحماية في الوقت الفعلي؛ بما في ذلك الكميات المتنامية للبيانات الكبيرة التي ستستمر المؤسسات في تجميعها وتخزينها وتحليلها.

"يتخذ "الإنترنت الشامل" شكله بسرعة ولذا يحتاج متخصص الأمان إلى التفكير حيال كيفية تغيير اهتمامه من مجرد تأمين نقاط النهاية ومحيط الشبكة".

كريس يونج، نائب رئيس مجموعة شؤون الأمان والحكومات في Cisco

يقول كريس يونج: "يتخذ "الإنترنت الشامل" شكله بسرعة ولذا يحتاج متخصص الأمان إلى التفكير حيال كيفية تغيير اهتمامه من مجرد تأمين نقاط النهاية ومحيط الشبكة. وسيكون هناك الكثير للغاية من الأجهزة والكثير للغاية من الاتصالات وكذلك الكثير من أنواع المحتويات والتطبيقات،وسوف يبقي العدد فقط متزايدًا. وفي هذه المشهد الجديد، ستصبح الشبكة نفسها جزءًا من نموذج الأمان الذي يتيح للمؤسسات توسيع السياسية والتحكم في البيئات المختلفة".

تحديث BYOD من Cisco

انتشار نقطة النهاية عبارة عن ظاهرة تدركها Cisco جيدًا داخل مؤسستها التي تضم 70000 موظف في كل أنحاء العالم. منذ إطلاق Cisco سياستها تحت اسم "أحضر جهازك الخاص معك إلى العمل" (BYOD) منذ عامين، شهدت الشركة معدل نمو بلغ 79% في عدد أجهزة الهواتف المحمولة في المؤسسة.

اهتم *تقرير الأمان السنوي من Cisco لعام 2011*[8] أولاً باختبار نشر Cisco لرحلة BYOD، والتي تعد جزءًا من التحول المستمر والموسع داخل المؤسسة حتى تصبح "مؤسسة ظاهرية". وبمرور الوقت، تصل Cisco إلى المرحلة الأخيرة من رحلتها المخططة، والتي سوف تستغرق سنوات عديدة، وسوف تكون الشركة مستقلة بشكل متزايد من حيث الموقع والخدمات، وستظل بيانات المؤسسة آمنة.[9]

في عام 2012، أضافت Cisco حوالي 11000 هاتف ذكي وجهاز كمبيوتر لوحي في كل أنحاء الشركة - أو حوالي 1000 جهاز جديد يدعم خدمة الإنترنت في الشهر. يقول بريت بيلدينج، كبير مديري الإشراف على الخدمات المتنقلة لتقنية المعلومات في Cisco "في نهاية عام 2012، كان هناك ما يقرب من 60000 هاتف ذكي وجهاز كمبيوتر لوحي يتم استخدامهم في المؤسسة - بما في ذلك ما يقل قليلاً عن 14000 جهاز iPad—وكلهم كانوا بعد تطبيق سياسة "أحضر جهازك الخاص معك إلى العمل" (BYO). "أجهزة الهاتف المحمول تسير الآن في Cisco بسياسة BYO، فترة زمنية".

أكثر نوع من الأجهزة شوهد استخدامه بكثرة في Cisco هو جهاز Apple iPad. "إنه من الرائع أن تعود بذاكرتك وتفكر في أنه منذ ثلاث سنوات، لم يكن لهذا المنتج وجود" قال هذا بيلدينغ. "والآن، هناك ما يزيد عن 14000 جهاز iPad مستخدم في Cisco كل يوم من قِبل موظفينا لممارسة مجموعة متنوعة من الأنشطة - على الصعيدين الشخصي والعملي. ويستخدم الموظفون أجهزة iPad بالإضافة إلى هواتفهم الذكية".

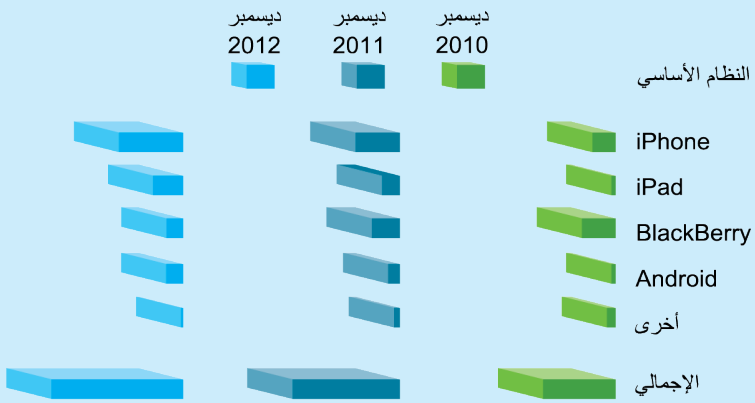
وفيما يخص الهواتف الذكية، تضاعف عدد أجهزة Apple iPhone المستخدمة داخل Cisco إلى ما يقرب من ثلاثة أضعاف العدد الموجود منذ عامين ليصل إلى 28600 جهاز تقريبًا. كما تم تضمين أجهزة RIM BlackBerry، وGoogle Android، وMicrosoft Windows في برنامج BYOD داخل مؤسسة Cisco. ويتسنى للموظفين فرصة التداول داخل المؤسسة بفضل الوصول إلى بيانات الشركة على أجهزتهم الشخصية بما يتفق مع الضوابط الأمنية. على سبيل المثال، يلزم المستخدمون الذين يريدون التحقق من بريدهم الشخصي والتقويم على أجهزتهم أن يأخذوا ملف تعريف الأمان الخاص بشركة Cisco الذي يفرض المسح عن بُعد والتشفير وعبارة مرور.

"لدينا أجهزة مدعومة أكثر من أي وقت مضى وفي الوقت نفسه، لدينا العدد الأقل من حالات الدعم. يتمثل هدفنا في أن يتمكن الموظف في يوم ما من جلب أي جهاز والإمداد الذاتي باستخدام Cisco Identity Services Engine (ISE) وإعداد أدوات تعاون WebEx الأساسية بما في ذلك Meeting Center وJabber وWebEx Social".

بريت بيلدنج، المدير الأول المشرف على خدمات تنقل تقنية المعلومات في Cisco

---

الشكل 2: نشر أجهزة المحمول من Cisco



لقد كان الدعم الاجتماعي أحد العناصر الرئيسية لبرنامج BYOD في Cisco منذ البداية. يضيف بيلدينج "إننا نعتمد بقوة على [النظام الأساسي للتعاون داخل المؤسسة] WebEx Social كنظام أساسي لدعم برنامج BYOD، وقد أدى هذا إلى تضخم الأرباح". ويضيف "لدينا الآن المزيد من الأجهزة المدعومة أكثر من أي وقت مضى وفي الوقت ذاته، كان لدينا أقل عدد من حالات الدعم.

يكمن هدفنا في أن يتمكن الموظف يومًا ما من إحضار أي جهاز وتكوين إعدادات تشغيل الخدمة ذاتيًا باستخدام محرك خدمات هوية Cisco (ISE) وإعداد أدوات تعاون WebEx الرئيسية، بما في ذلك Meeting Center، وJabber، وWebEx Social".

والخطوة التالية لبرنامج BYOD في Cisco، وفقًا لما جاء على لسان بيلدينج، هي التوسع في تحسين نظام الأمان عن طريق زيادة الرؤية والتحكم في كل أنشطة المستخدمين والأجهزة، على كل من الشبكة المادية والبنية التحتية الظاهرية، مع تحسين تجربة المستخدم. يضيف بيلدينج "إن الحرص على العناية بتجربة المستخدم هو جوهر تقنية المعلومات الاستهلاكية للاتجاه السائد لتقنية المعلومات". "إننا نحاول تطبيق هذا المفهوم على مؤسستنا. لا يسعنا سوى ذلك. إنني أعتقد أن ما نراه الآن هو "إضفاء طابع تقنية المعلومات" على المستخدمين. إننا نتجاوز الآن نقطتهم وهم يتساءلون، "هل لي أن أستخدم هذا الجهاز في محل العمل؟" فهم يقولون الآن، "إنني أفهم أنكم بحاجة إلى الحفاظ على أمان المؤسسة، ولكن بما لا يتداخل مع تجربتي كمستخدم".

الخدمات الموجودة في العديد من لسحب

نسبة استخدام شبكة مركز البيانات العالمية في ازدياد. وفقًا لمؤشر السحابة العالمية من Cisco، من المتوقع زيادة نسبة استخدام شبكة مركز البيانات العالمية أربعة أضعاف خلال الخمس سنوات التالية وستنمو بمعدل نمو سنوي مركب (CAGR) بمقدار 31 في المائة بين عامي 2011 و2016.[10]

ضمن هذا النمو الهائل، نجد أن المكون الأسرع نموًا هو بيانات السحابة. حيث ستزيد نسبة استخدام شبكة السحابة العالمية ست مرات خلال الخمس سنوات التالية وستنمو بمعدل 44 في المائة من عام 2011 إلى عام 2016. وفي الواقع، ستشكل نسبة استخدام شبكة السحابة العالمية ما يقارب ثلثي إجمالي نسبة استخدام شبكة مركز البيانات العالمية بحلول عام 2016.[11]

ويؤدي هذا التزايد الهائل في نسبة استخدام شبكة السحابة إلى طرح أسئلة حيال قدرة المؤسسات على إدارة هذه المعلومات. وفي السحابة، نجد أن حدود التحكم غير واضحة: هل يمكن لمؤسسة وضع شبكات حماية حول بياناتها في السحابة إذا كانت لا تملك و لاتشغل مركز البيانات؟ كيف يمكن تطبيق أدوات الأمان الأساسية مثل جُدر الحماية وبرامج مكافحة الفيروسات عندما لا يمكن تحديد حافة الشبكة؟

بغض النظر عن عدد أسئلة الأمان التي تُطرح، من الواضح أن المزيد من المؤسسات تتبنى فوائد السحابة؛ وأنه ليس من المحتمل أن تعود المؤسسات التي تفعل ذلك إلى نموذج مركز البيانات الخاص. وبينما تعد فرص السحابة للمؤسسات عديدة ـ بما في ذلك توفير التكاليف والمستوى الأعلى من تعاون الموظفين والإنتاجية وتقليص آثار الكربون ـ تشتمل مخاطر الأمان المحتملة التي تواجهها المؤسسات كنتيجة لنقل بيانات العمل وعملياته إلى السحابة على:

حيث ستزيد نسبة استخدام شبكة السحابة العالمية ست مرات خلال الخمس سنوات التالية وستنمو بمعدل 44 في المائة من عام 2011 إلى عام 2016.

الأجهزة الظاهرية المتعددة

في حالة اختراقه، قد يؤدي هذا البرنامج الذي ينشئ ويشغل الأجهزة الظاهرية إلى اختراق جماعي أو اختراق البيانات في خوادم متعددة؛ مما يطبق سهولة الإدارة نفسها والوصول الذي توفرها الظاهرية لاختراق ناجح. بإمكان جهاز ظاهري متعدد مخادع (تمت السيطرة عليه بواسطة "الاختراق الإلكتروني" التحكم بالكامل في خادم.[12]

خفض تكلفة الإدخال

خفضت الظاهرية من تكلفة الإدخال لتوفر خدمات مثل الخادم الظاهري الخاص (VPS). ومقارنةً بنماذج مركز البيانات القديمة القائمة على الأجهزة، نرى نموًا في البنية الأساسية السريعة والرخيصة وسهلة التوفر للأنشطة الإجرامية. على سبيل المثال، هناك العديد من خدمات الخادم الظاهري الخاص متوفرة للبيع الفوري (مع القدرة على الشراء باستخدام Bitcoin أو أنواع دفع أخرى صعبة التعقب) والتي يتم توجيهها إلى العالم الإجرامي المتخفي. وقد قللت الظاهرية من تكلفة البنية الأساسية وجعلتها أكثر سهولة في التوفر مع القليل من الرقابة على الأنشطة أو انعدام الرقابة تمامًا.

بإمكان جهاز ظاهري متعدد مخادع (تمت السيطرة عليه بواسطة "الاختراق الإلكتروني") التحكم بالكامل في خادم.12

"فصل" التطبيقات الظاهرية

نظرًا لفصل التطبيقات الظاهرية عن الموارد المادية التي تستخدمها، يصبح تطبيق أساليب الأمان التقليدية أكثر صعوبةً على المؤسسات. لذا يسعى موفرو تقنية المعلومات إلى خفض التكلفة من خلال عرض مرن للغاية يمكنهم فيه تحريك الموارد وفقًا للحاجة؛ وهذا في مقابل مجموعة الأمان التي تسعى إلى ترتيب الخدمات المشابهة لأوضاع الأمان وإبقائها منفصلة عن الأوضاع الأخرى التي قد تكون أقل أمانًا.

يقول جو إبستن، المدير التنفيذي السابق لشركة Virtuata - وهي شركة استحوذت Cisco عليها عام 2012 وتوفر إمكانات ابتكارية لتأمين معلومات مستوى الجهاز الظاهري في مراكز البيانات وبيئات السحابة - أن: "الظاهرية والحوسبة تتسببان في مشكلات مثل مشكلات جلب الأجهزة الخاصة ولكنها أحدثت تغييرًا جذريًا. وتنتقل التطبيقات عالية القيمة والبيانات عالية القيمة في مركز البيانات الآن. ويؤدي مفهوم أحمال العمل الظاهرية إلى شعور المؤسسات بعدم الراحة. وفي البيئة الظاهرية، كيف تعرف أنه يمكنك الوثوق فيما تشغله؟ تتمثل الإجابة في أنك لم تكن قادرًا على ذلك حتى الآن وأن عدم التأكد أصبح عائقًا أساسيًا لاعتماد السحابة".

ولكن ينوه "إبستن" إلى أن صعوبة تجاهل المؤسسات للظاهرية والسحابة تزيد بشكل متزايد. ويضيف "إن العالم على وشك مشاركة كل شيء. ستتم محاكاة كل شيء افتراضيًا وستتم مشاركة كل شيء. ولن يكون من المنطقي متابعة تشغيل مراكز البيانات الخاصة فقط حيث ستكون السحب المختلطة وجهة تقنية المعلومات".

الأمان المتوائم والمتجاوب هو إجابة هذه التحديات المتنامية للسحابة والظاهرية. وفي هذه الحالة، يجب أن يكون الأمان عنصرًا قابلاً للبرمجة يتم دمجه بسلاسة في البنية الأساسية لمركز البيانات؛ وذلك وفقًا لما قاله إبستن. وبالإضافة إلى ذلك، يجب أن يكون الأمان مضمنًا في مرحلة التصميم بدلاً من إدخاله قبل التنفيذ.

"تتسبب الظاهرية والحوسبة السحابية في مشكلات مثل مشكلات جلب الأجهزة الخاصة ولكنها أحدثت تغييرًا جذريًا... تنتقل التطبيقات عالية القيمة والبيانات عالية القيمة في مركز البيانات".

جو إبستن، الرئيس التنفيذي السابق لشركة Virtuata

الجمع بين العمل والاستخدام لشخصي

جيل الألفية ومكان العمل

يريد الموظفون العصريون ـ وخصوصًا جيل الألفية ـ حرية استعراض الويب؛ وهذا ليس في الوقت وبالكيفية التي يريدونها فقط ولكن بالأجهزة التي يختارونها أيضًا. ومع ذلك، لا يريدون لأصحاب الأعمال مس هذه الحرية مما يشكل موقفًا مقلقًا لمتخصصي الأمان.

وفقًا لتقرير التقنية العالمية المتصلة لعام *2012* من *Cisco*، يرى ثلثا المستجيبين أن أصحاب العمل لا يجب أن يتتبعوا أنشطة الموظفين الإلكترونية على الأجهزة الصادرة من الشركة. وباختصار، لا يرون أن أصحاب العمل لهم أي حق في مراقبة مثل هذه التصرفات. وقال ثلث واحد فقط من الموظفين الذين تم استطلاع رأيهم (34 في المائة) أنهم لا يمانعون تتبع أصحاب العمل لسلوكهم عبر الإنترنت.

يقول واحد فقط من خمسة مستجيبين أن صاحب عمله يتتبع أنشطته الإلكترونية بالفعل على الأجهزة المملوكة للشركة، بينما قال 46 في المائة أن أصحاب أعمالهم لا يتتبعون نشاطهم. وتوضح نتائج أحدث دراسة من دراسة العالم المتصل *(Connected World)* أن جيل الألفية لديه مشاعر قوية حيال تتبع أصحاب العمل لأنشطة الموظفين عبر الإنترنت؛ وذلك حتى لدى الذين صرحوا بأنهم يعملون في مؤسسات لا يحدث فيها مثل هذا التتبع.

ومما يزيد من التحديات التي تواجه متخصصي الأمان، يبدو أن هناك انفصالاً بين ما يرى الموظفون أنه يمكنهم فعله باستخدام أجهزتهم الصادرة من الشركة وبين ما تمليه سياسات تقنية المعلومات بالفعل حيال الاستخدام الشخصي. يقول أربعة من بين كل 10 مستجيبين أنه من المفترض استخدامهم للأجهزة الصادرة من الشركة في أنشطة العمل فقط بينما يقول الربع أنه متاح لهم استخدام أجهزة الشركة

يقول واحد فقط من خمسة مستجيبين أن صاحب عمله يتتبع أنشطته الإلكترونية بالفعل على الأجهزة المملوكة للشركة، بينما قال 46 في المائة أن أصحاب أعمالهم لا يتتبعون نشاطهم.

في أنشطة غير متعلقة بالعمل. ومع ذلك، يقول 90% من متخصصي تقنية المعلومات الذين تم استطلاع رأيهم بأن لديهم بالفعل سياسات تحظر استخدام الأجهزة الصادرة من الشركة في الأنشطة الإلكترونية الشخصية؛ وذلك على الرغم من أن 38 في المائة يفيدون بأن الموظفين يخرقون السياسة ويستخدمون الأجهزة في أنشطة شخصية بالإضافة إلى القيام بالعمل. (يمكنك الاطلاع على معلومات عن أسلوب Cisco في التعامل مع تحديات جلب الأجهزة الشخصية في صفحة 16.)

ومما يزيد من التحديات التي تواجه متخصصي الأمان، يبدو أن هناك انفصال بين ما يرى الموظفون أنه يمكنهم فعله باستخدام أجهزتهم الصادرة من الشركة وبين ما تمليه سياسات تقنية المعلومات بالفعل حيال الاستخدام الشخصي.

الخصوصية وجيل الألفية

وفقًا لتقرير التقنية العالمية المتصلة لعام *2012* من *Cisco*، قبل جيل الألفية الحقيقة القائل بأن الخصوصية الشخصية قد أصبحت شيئًا من الماضي؛ وذلك بفضل الإنترنت. ويقول واحد وتسعون في المائة من المستهلكين الشباب الذين تم استطلاع رأيهم بأن عصر الخصوصية قد انتهى ويرون أنه لا يمكنهم التحكم في خصوصية معلوماتهم، وهذا مع قول ثلث المستجيبين أنهم غير قلقين حيال البيانات التي يتم تخزينها والتقاطها عنهم.

وبشكل عام، يرى جيل الألفية أيضًا أن هويتهم الإلكترونية مختلفة عن هويتهم في العالم الحقيقي. ويقول خمسة وأربعون في المائة أن هذه الهويات غالبًا ما تكون مختلفة وفقًا للنشاط المعنيّ بينما يرى 36 في المائة أن هذه الهويات مختلفة تمامًا. ويرى 8 في المائة فقط أن هذه الهويات متطابقة.

لدى المستهلكين الشباب توقعات عالية بأن مواقع الويب ستحافظ على خصوصية معلوماتهم وغالبًا ما يشعرون براحة أكثر في مشاركة البيانات باستخدام مواقع تواصل اجتماعي أو منتديات كبيرة نظرًا لغطاء عدم معرفة الهوية الذي يوفره الحشد. يقول ستة وأربعون في المائة بأنهم يتوقعون حفاظ مواقع ويب معينة على أمان معلوماتهم بينما يقول 17 في المائة بأنهم يثقون في محافظة معظم مواقع الويب على خصوصية معلوماتهم. ومع ذلك، يقول 29 في المائة بأن الأمر لا يقتصر على عدم ثقتهم في محافظة مواقع الويب على خصوصية معلوماتهم فقط ولكن يشمل أيضًا قلقهم للغاية أيضًا حيال الأمان وسرقة الهوية. ويجب مقارنة هذا الأمر بفكرة مشاركة البيانات مع صاحب عمل لديه سياق حول ماهيتهم وما يفعلونه.

”يدخل جيل الألفية مكان العمل الآن ويجلبون معهم ممارسات عمل جديدة وسلوكيات جديدة للتعامل مع المعلومات والأمان المرتبط بها. حيث يريدون زوال الخصوصية ـ وهو ببساطة أمر غير مفعل بشكل عملي غير أنه ما يجب أن تفعله المؤسسات في هذا النموذج ـ وهو مفهوم سيكون مزعجًا للجيل الأكبر في مكان العمل.“ نقلاً عن آدم فيلوبوت مدير مبيعات الأمان في أوروبا والشرق الأوسط وأفريقيا وروسيا في Cisco. ”ومع ذلك، بإمكان المؤسسات السعي لتوفير تعليم أمان المعلومات لموظفيها لتنبيههم حيال المخاطر وتوفير الإرشادات عن كيفية مشاركة المعلومات على أفضل وجه والارتقاء بالأدوات الإلكترونية ضمن مجالات أمان البيانات“.

"يدخل جيل الألفية مكان العمل الآن ويجلبون معهم ممارسات عمل جديدة وسلوكيات جديدة للتعامل مع المعلومات والأمان المرتبط بها. حيث يعتقدون بزوال الخصوصية ـ وهو ببساطة أمر غير مفعل بشكل عملي غير أنه ما يجب أن تفعله المؤسسات في هذا النموذج ـ وهو مفهوم سيكون مزعجًا للجيل الأكبر في مكان العمل." نقلاً عن آدم فيلوبوت مدير مبيعات الأمان في أوروبا والشرق الأوسط وأفريقيا وروسيا في Cisco.

آدم فيلوبوت، مدير مبيعات الأمان في أوروبا والشرق الأوسط وأفريقيا وروسيا في Cisco

لماذا تحتاج المؤسسات إلى زيادة الوعي بتضليل الوسائط الاجتماعية

كتبه جوردن كوسيندا
محلل التهديدات العالمية في Cisco

أصبحت الوسائط الاجتماعية أساسًا جوهريًا في العديد من المؤسسات، حيث ساعدت القدرة على التواصل المباشر مع العملاء وغيرهم من الجمهور عبر Twitter وFacebook العديد من المؤسسات في بناء الوعي بالعلامة التجارية عبر التواصل الاجتماعي الإلكتروني.

ويتمثل الجانب السلبي لهذا التواصل المباشر فائق السرعة في أن الوسائط الاجتماعية بإمكانها السماح بمعلومات غير دقيقة أو مضللة بالانتشار كالنار في الهشيم. وليس من الصعب تخيل سيناريو يقوم فيه أحد الإرهابيين بتنسيق هجمات في الوقت الفعلي باستخدام تغريدات مضللة بنية إغلاق الطرق أو خطوط الهاتف أو إرسال الناس إلى طريق خطر. ومن بين الأمثلة: أغلقت حكومة الهند مئات من مواقع الويب وقيدت الرسائل النصية[13] هذا الصيف محاولةً لاستعادة الهدوء في الجزء الشمالي الشرقي من البلاد بعد نشر صور ورسائل نصية. حيث تسببت الشائعات في جعل آلاف من العمال المهاجرين يتدافعون ذعرًا إلى محطات القطارات والحافلات.

أثرت حملات الوسائط الاجتماعية المضللة في أسعار السوق أيضًا. وأفاد موجز أخبار تم اختراقه لرويترز على Twitter بأن الجيش السوري الحر قد انهار في حلب. وبعد عدة أيام، تم اختراق موجز أخبار على Twitter وغرد دبلوماسي روسي رفيع مزعوم بأن الرئيس السوري بشار الأسد قد مات. وقبل فقدان هذه الحسابات لمصداقيتها، قفزت أسعار الوقود في الأسواق العالمية.[14]

يجب أن ينتبه متخصصو الإنترنت لهذه المشاركات سريعة التنقل محتملة الضرر على الوسائط الاجتماعية، وخصوصًا إذا كانت موجهة إلى الشركة نفسها ويجب اتخاذ إجراء سريع للدفاع عن الشبكات من البرامج الضارة وتنبيه الموظفين بخصوص محاولة تصيد احتيالي مزيفة أو إعادة توجيه شحنة أو تقديم النصح للموظفين بخصوص الأمان. حيث إن تنبيه المديرين بخبر عاجل يتضح زيفه فيما بعد هو آخر شيء يريد مديرو الأمان التنفيذيين فعله.

يتمثل الضمان الأول لمواجهة السقوط في شرك الأخبار المزيفة في التأكد من الخبر من عدة مصادر. فيما مضى، قام الصحفيون بهذه المهمة من أجلنا بحيث تكون الأخبار قد تم التحقق من صحتها قبل قراءتنا لها أو سماعنا لها. وحاليًا، يحصل العديد من الصحفيين على أخبارهم من صفحات Twitter نفسها التي نحصل منها على الأخبار، وإذا أعجب العديد منا بالخبر نفسه، فسوف يسهل علينا الخطأ بإعادة التغريد للتأكد من الخبر.

بالنسبة للأخبار السريعة العاجلة التي تتطلب إجراءً سريعًا، قد يكون رهانك الأمثل هو استخدام الطريقة الحذرة القديمة. إذا بدا الخبر مبالغًا فيه، فكر مرتين قبل إعادة نشره أو الاقتباس منه.15

بالنسبة للأخبار السريعة العاجلة التي تتطلب إجراءً سريعًا، قد يكون رهانك الأمثل هو استخدام الطريقة الحذرة القديمة. إذا بدا الخبر مبالغًا فيه، فكر مرتين قبل إعادة نشره أو الاقتباس منه.

البيانات الكبيرة

صفقة كبيرة لمؤسسات اليوم

يضج عالم الأعمال بالاهتمام "بالبيانات الكبيرة" وباحتمالية القيمة الهائلة لدى المحللين والتي يمكن الحصول عليها من الأحجام الضخمة من المعلومات التي تصدرها المؤسسات وتجمعها وتخزنها.

درس تقرير التقنية العالمية المتصلة لعام *2012* من *Cisco* تأثير اتجاه البيانات الكبيرة على المؤسسات وعلى فرق تقنية المعلومات لديها بشكل أكثر تحديدًا. وفقًا لنتائج الدراسة، يقوم حوالي ثلاثة أرباع المؤسسات حول العالم (74 في المائة) بجمع البيانات وتخزينها، وتستخدم الإدارة تحليل البيانات الكبيرة لاتخاذ قرارات العمل. وبالإضافة إلى ذلك، قال سبعة من بين كل 10 مستجيبين في مجال تقنية المعلومات أن البيانات الكبيرة ستكون أولوية إستراتيجية لشركتهم ولفريق تقنية المعلومات في العام القادم.

بينما تتطور أو تظهر اتجاهات التنقل والسحابة والظاهرية وتزايد نقطة النهاية وغيرها من اتجاهات الشبكات، ستمهد الطريق لمزيد من فرص البيانات الكبيرة والتحليلات للأنشطة التجارية. ولكن هناك نقاط للقلق حيال الأمان بخصوص البيانات الكبيرة. توضح نتائج دراسة العالم المتصل لعام 2012 أن ثلث المستجيبين (أي 32 في المائة) يرون أن البيانات الكبيرة تزيد من تعقد متطلبات الأمان وحماية البيانات والشبكات بسبب وجود الكثير من البيانات وطرق عديدة للغاية للدخول إليها. وباختصار، تزيد البيانات الكبيرة من المتجهات والزوايا التي يجب أن تغطيها فرق الأمان وحلول الأمان في الشركة.

تشتمل كل من كوريا (45 في المائة) وألمانيا (42 في المائة) والولايات المتحدة (40 في المائة) والمكسيك (40 في المائة) على أعلى النسب المئوية من مستجيبي تقنية المعلومات الذين يرون أن البيانات الكبيرة تزيد من تعقيد الأمان. وللمساعدة في التأكيد على الأمان، ترى أغلبية المستجيبين في مجال تقنية المعلومات ـ أكثر من الثلثين (68 في المائة) ـ أن فريق تقنية

حيث يقوم حوالي 74% من المؤسسات حول العالم بجمع وتخزين البيانات وتستخدم الإدارة تحليل البيانات الكبيرة لاتخاذ قرارات العمل.

تشتمل كوريا وألمانيا والولايات المتحدة والمكسيك على أعلى نسبة مئوية من مستجيبي تقنية المعلومات الذين يرون أن البيانات الكبيرة تزيد من تعقيد الأمان.

المعلومات بأكمله يجب أن يشارك في وضع إستراتيجية جهود البيانات الكبيرة وقيادتها داخل شركته. يقول جافين ريد، مدير أبحاث التهديدات في عمليات استخبارات الأمان في Cisco أن: "البيانات الكبيرة لا تزيد من تعقيد الأمان ولكنها تجعل ذلك ممكنًا. في Cisco، نجمع 2.6 تريليون سجلاً ونخزنها يوميًا وهذا يشكل النظام الأساسي الذي يمكننا منه بدء اكتشاف الحوادث منه والتحكم فيها".

بالنسبة إلى الحلول المصممة لمساعدة المؤسسات في كل من الإدارة الأفضل والحصول على قيمة بياناتها الكبيرة، نجد عوائق تعيق تبنيها. يشير المستجيبون إلى نقص الميزانية ونقص الوقت لدراسة البيانات الكبيرة ونقص الحلول المناسبة وأيضًا نقص موظفي تقنية المعلومات ونقص خبرة تقنية المعلومات. تشير حقيقة أن واحد بالكاد من بين كل أربعة مستجيبين حول العالم (23 في المائة) قد قال بأن نقص الخبرة والموظفين كان عائقًا أمام قدرة شركته على استخدام البيانات الكبيرة بفاعلية، إلى الحاجة لدخول المزيد من المتخصصين في سوق العمل ليتم تدريبهم في هذه المنطقة.

السحابة أيضًا عامل في نجاح البيانات الكبيرة؛ وذلك وفقًا لـ 50 في المائة من مستجيبي تقنية المعلومات في دراسة العالم المتصل لعام 2012. حيث يرون أن مؤسساتهم بحاجة إلى العمل من خلال خطط السحابة وعمليات نشره لجعل البيانات الكبيرة مشروعًا جديرًا بالاهتمام. وكان هذا الشعور جليًا في الصين (78 في المائة) والهند (76 في المائة) حيث رأى أكثر من ثلاثة مستجيبين من بين كل أربعة وجوب الاعتماد على السحابة لكي تتمكن البيانات الكبيرة من الانطلاق بشكل كبير. ونتيجة لذلك، توضح الدراسة في بعض الحالات أن تبني السحابة سيؤثر على معدل تطبيق ومكاسب جهود البيانات الكبيرة.

أكد أكثر من نصف إجمالي المستجيبين في مجال تقنية المعلومات أيضًا على أن مناقشات البيانات الكبيرة داخل شركاتهم غير مجدية حتى الآن. وليس هذا مفاجئًا عند الأخذ في الاعتبار أن السوق يحاول الآن فهم كيفية تحسين بياناتهم الكبيرة وتحليلها واستخدامها استراتيجيًا. ومع ذلك، تثمر نقاشات البيانات الكبيرة ـ في بعض البلاد ـ بقرارات ذات جدوى فيما يتعلق بالإستراتيجية والاتجاه والحلول. وتأتي الصين (82 في المائة) والمكسيك (67 في المائة) والهند (63 في المائة) والأرجنتين (57 في المائة) في الصدارة مع كون أكثر من نصف

بالنسبة للحلول المصممة لمساعدة المؤسسات في كل من الإدارة الأفضل والحصول على قيمة بياناتها الكبيرة، نجد عوائق تعيق تبنيها. ويشير المستجيبون إلى نقص الميزانية ونقص الوقت لدراسة البيانات الكبيرة ونقص الحلول المناسبة وأيضًا نقص موظفي تقنية المعلومات ونقص خبرة تقنية المعلومات.

المستجيبين من هذه الدول يرون أن نقاشات البيانات الكبيرة في مؤسساتهم لا تزال قيد التطور إلى حد كبير وتؤدي إلى إجراءات ونتائج ثابتة.

يرى ثلاثة من بين كل خمسة من مستجيبي تقنية المعلومات على تقرير العالم المتصل لعام *2012* أن البيانات الكبيرة بإمكانها مساعدة الدول واقتصادها في أن تصبح أكثر تنافسية في السوق العالمية.

ومع ذلك، ففي بعض الدول، تنتج نقاشات البيانات الكبيرة قرارات ذات جدوى فيما يتعلق بالإستراتيجية والاتجاه والحلول. تأتي الصين والمكسيك والهند والأرجنتين في صدارة هذا الأمر مع كون أكثر من نصف المستجيبين من هذه الدول يرون أن نقاشات البيانات الكبيرة في مؤسساتهم لا تزال قيد التطور وأنها تؤدي إلى إجراءات ونتائج ثابتة.

حالة الاستغلال

الخطر يكمن في الأماكن المباغتة

يؤمن العديد من متخصصي الأمان ـ وعدد كبير بالتأكيد من مستخدمي الإنترنت ـ بأفكار مسبقة فيما يتعلق بالأماكن التي من المحتمل مصادفة الأشخاص لبرامج ويب ضارة وخطرة عليها.

ويتمثل الاعتقاد العام في أن المواقع التي تروج للنشاط الإجرامي ـ مثل المواقع التي تبيع مستحضرات طبية غير قانونية أو سلع فاخرة مقلدة ـ هي التي تزيد احتمالية استضافتها لبرامج ضارة. وتكشف بياناتنا حقيقة هذا المفهوم القديم، حيث إن مواجهات برامج الويب الضارة عادةً لا تكون المنتج الفرعي للمواقع "السيئة" في بيئة التهديدات اليوم.

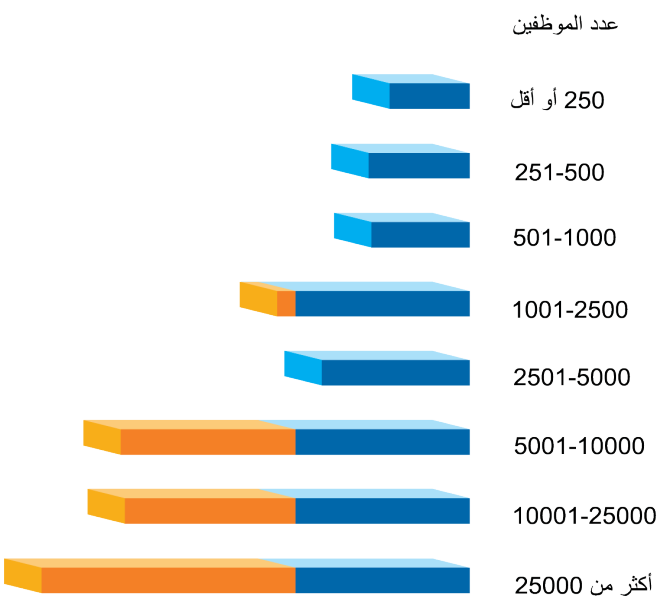
"تحدث مواجهات برامج الويب الضارة في كل مكان يزور فيه الأشخاص الإنترنت حتى لأغراض العمل؛ بما في ذلك معظم مواقع الويب القانونية التي يزورونها بشكل متكرر." نقلاً عن ماري لاندسمان، كبير باحثي الأمان مع Cisco. "وبالفعل، تعد مواقع العمل والصناعة إحدى أهم الفئات الثلاث التي تتم زيارتها عند حدوث مواجهة برنامج ضار. وبالطبع، ليس هذا نتيجة لمواقع العمل التي صممت لتكون ضارة". ومع ذلك، غالبًا ما تختفي المخاطر في إعلانات إلكترونية محملة للاستغلال وسهلة الاكتشاف والتي يتم توزيعها على مواقع الويب القانونية أو المتسللون الذين يستهدفون مجتمع المستخدمين على المواقع الشائعة التي يستخدمونها أكثر من غيرها.

بالإضافة إلى ذلك، تنتشر مواقع الويب المصابة بالبرامج الضارة في العديد من الدول والمناطق ـ وليس في دولة أو اثنتين فقط ـ مما يبدد مفهوم زيادة احتمالية استضافة مواقع الويب في بعض الدول لمحتوى ضار أكثر من غيرها. "الويب هي آلية توصيل البرامج الضارة الأكثر انتشارًا حتى الآن وتفوق أعلى الفيروسات أو الفيروسات المتنقلة إنتاجية في قدرتها على الوصول إلى جمهور كبير وإصابته في صمت وبفاعلية" نقلاً عن لاندسمان. "تحتاج المؤسسات إلى الحماية حتى إذا كانت تحجب المواقع (السيئة) الشائعة مع تفاصيل إضافية في الفحص والتحليل".

عادةً ما تكون المخاطر مخبأة في إعلانات إلكترونية محملة للاستغلال سهلة الاكتشاف.

الشكل 3: الخطر حسب حجم الشركة

حتى مرتين ونصف من المخاطر المتزايدة من مواجهة البرامج الضارة على الويب بالنسبة للمؤسسات الكبيرة.



وتواجه جميع الشركات ـ بغض النظر عن حجمها ـ مخاطر كبيرة من مواجهات برامج الويب الضارة. ويجب أن تركز كل مؤسسة على أساسيات تأمين شبكتها وملكيتها الفكرية.

مواجهات البرامج الضارة حسب حجم الشركة

تواجه المؤسسات الكبرى (المشتملة على أكثر من 25000 موظفًا) مخاطر مواجهة برامج الويب الضارة بمعدل ضعفين ونصف أكثر من الشركات الصغيرة. ويحتمل أن تكون هذه المخاطر الزائدة انعكاسًا لامتلاك المؤسسات الكبرى لملكية فكرية أعلى قيمة ومن ثم يتم استهدافها بشكل أكثر تكرارًا.

بينما تشتمل الشركات الصغرى على مواجهات أقل لبرامج الويب الضارة لكل مستخدم، فإنه من المهم ملاحظة أن جميع الشركات ـ بغض النظر عن الحجم ـ تواجه مخاطر كبيرة من مواجهات برامج الويب الضارة. ويجب أن تركز كل مؤسسة على أساسيات تأمين شبكتها وملكيتها الفكرية.

مواجهات البرامج الضارة حسب الدولة

يوضح بحث Cisco تغييرًا كبيرًا في المشهد العالمي لمواجهات برامج الويب الضارة حسب الدولة عام 2012. حيث هبطت الصين، والتي كانت تحتل المركز الثاني في قائمة عام 2011 لمواجهات برامج الويب الضارة، إلى المركز السادس عام 2012. بينما تحتل الدنمارك والسويد الآن المركز الثالث والرابع على التوالي. وتحتفظ الولايات المتحدة الأمريكية بالمركز الأعلى عام 2012 مثلما كانت عليه عام 2011، وذلك مع حدوث 33 في المائة من جميع مواجهات برامج الويب الضارة من خلال مواقع الويب المستضافة في الولايات المتحدة.

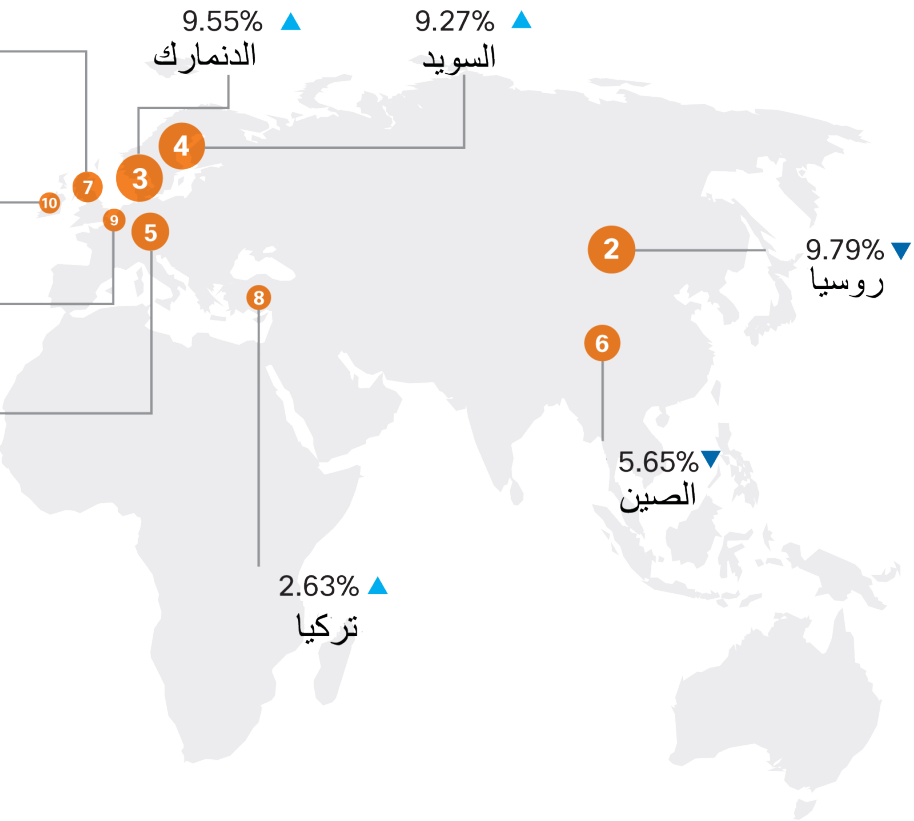
ومن المرجح أن تنعكس التغييرات في الموقع الجغرافي بين عامي 2011 و2012 على كل من تغييرات الاكتشاف وعادات المستخدم. على سبيل المثال، لعبت "الإعلانات الضارة" أو البرامج الضارة التي يتم توصيلها عبر الإعلانات الإلكترونية ـ دورًا عام 2012 أكبر من عام 2011 في مواجهات برامج الويب الضارة. ومن المهم التذكير بأن مواجهات برامج الويب الضارة تحدث بشكل أكثر تكرارًا من خلال الاستعراض العادي لمواقع ويب قانونية قد يكون تم اختراقها أو تقديمها لإعلانات ضارة دون قصد. وبإمكان الإعلانات الضارة التأثير على أي موقع إلكتروني ببساطة بغض النظر عن أصل الموقع.

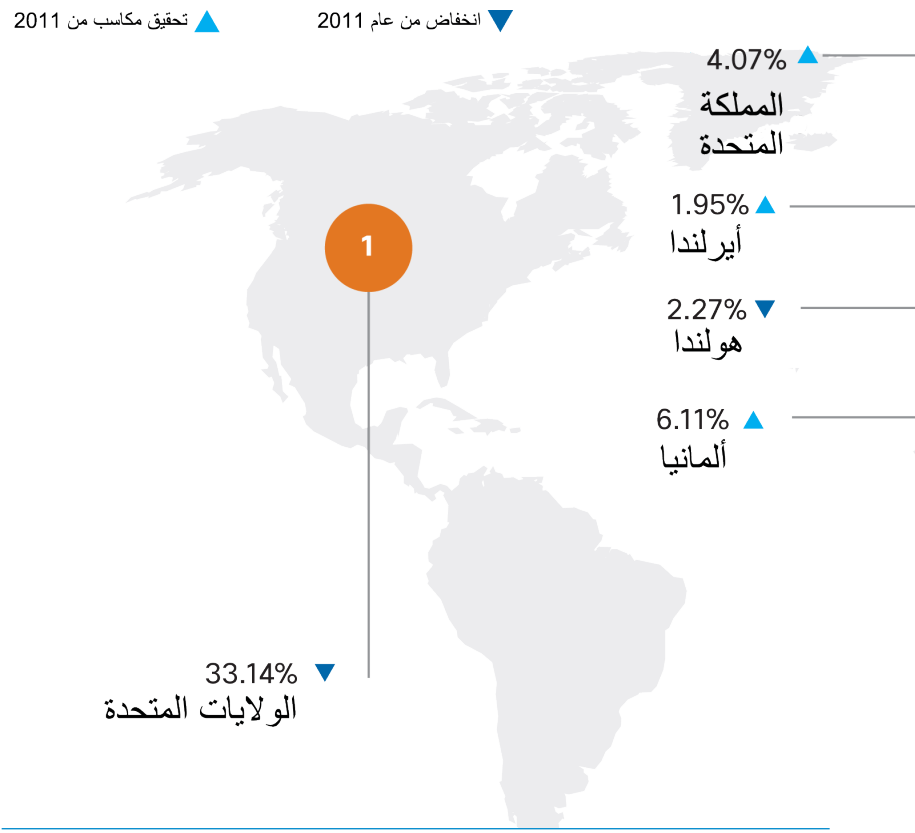
بشكل عام، توضح البيانات الجغرافية لعام 2012 أن الويب تمثل متسبب إصابة متكافئ الفرص؛ وذلك على النقيض من المفاهيم القائلة بأن دولة واحدة أو اثنتين مسؤولتان عن استضافة برامج الويب الضارة أو أن دولة معينة أكثر أمانًا من غيرها. ومثلما يتيح توصيل المحتوى التفاعلي لـ Web 2.0 تحقيق الدخل من مواقع الويب حول العالم، فيمكنه أيضًا تسهيل التوصيل العالمي لبرامج الويب الضارة.

وبالطبع، هناك فرق واضح بين مكان حدوث مواجهة برامج الويب الضارة وبين المكان الحقيقي لاستضافة البرامج الضارة. في الإعلانات الضارة على سبيل المثال، عادةً ما تحدث المواجهة عند الانتقال إلى موقع إلكتروني شهير وقانوني يحتمل اشتماله على إعلانات من جهة خارجية. ومع ذلك، تتم استضافة البرنامج الضار الفعلي المقصود توصيله على نطاق مختلف تمامًا. وبما أن بيانات Cisco قائمة على مكان حدوث المواجهة، فليس لها تأثير على أصل البرنامج الضار الفعلي. على

الشكل 4: مواجهات البرامج الضارة على الويب حسب الدولة

ثلث مواجهات البرامج الضارة المنتشرة على شبكة الإنترنت ناتجة عن النطاقات التي تستضيفها الولايات المتحدة.

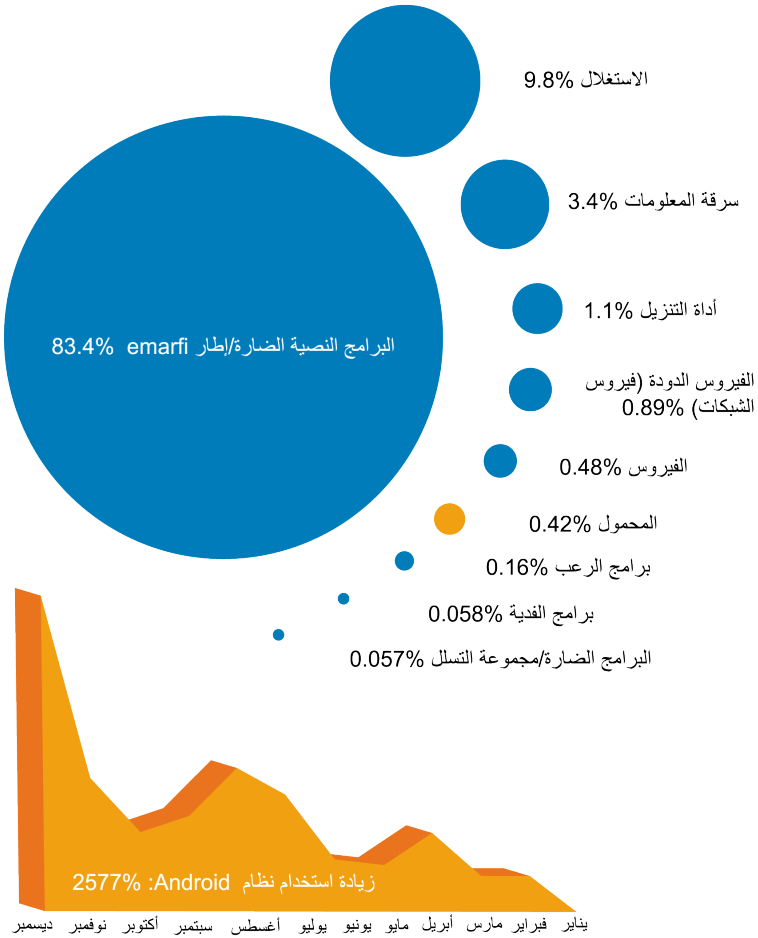




بشكل عام، توضح البيانات الجغرافية لعام 2012 أن الويب تمثل متسبب إصابة متكافئ الفرص؛ وذلك على النقيض من المفاهيم القائلة بأن دولة واحدة أو اثنتين مسؤولتان عن استضافة برامج الويب الضارة أو أن دولة معينة أكثر أمانًا من غيرها.

الشكل 5: أكثر أنواع البرامج الضارة انتشارًا على الإنترنت

نمت المواجهات الضارة لـ Android بنسبة 2577 بالمائة على مدار عام 2012، على الرغم من أن البرامج الضارة التي تغزو الهواتف المحمولة لا تشكل سوى نسبة صغيرة من إجمالي عدد مواجهات البرامج الضارة على شبكة الإنترنت.



سبيل المثال، تعد الشهرة المتزايدة لمواقع الوسائط الاجتماعية والترفيه في الدنمارك والسويد ـ والمقترنة بمخاطر الإعلانات الضارة ـ هي المسؤولة بشكل كبير عن تزايد المواجهات من المواقع المستضافة في هذه المناطق ولكنها ليست مؤشرًا على أصل البرامج الضارة الفعلي.

أشهر أنواع برامج الويب الضارة عام 2012

نمت برامج Android الضارة بسرعة هائلة أسرع من أي نوع من البرامج الضارة الموصلة عبر الويب؛ وهو اتجاه مهم مع الأخذ في الاعتبار أن التقارير تشير إلى احتفاظ Android بأغلبية حصة سوق الهواتف الجوالة على مستوى العالم. ومن المهم ملاحظة أن مواجهات البرامج الجوالة الضارة تشكل 0.5 في المائة فقط من جميع مواجهات برامج الويب الضارة عام 2012 مع تسجيل Android لحوالي 95 في المائة من جميع مواجهات الويب الضارة هذه. وبالإضافة إلى ذلك، شهد عام 2012 بزوغ أول شبكة روبوت (botnet) لنظام Android في العالم مما يشير إلى أن عمليات تطور برامج المحمول الضارة عام 2013 تستحق الدراسة.

بينما يدعي بعض الخبراء أن نظام Android هو "التهديد الأكبر" أو يجب أن يكون تركيزًا أساسيًا لفرق أمان المؤسسات عام 2013، فإن البيانات الفعلية تظهر عكس ذلك. وكما تم التوضيح أعلاه، تشكل برامج المحمول الضارة بشكل عام أقل من 1 في المائة من إجمالي المواجهات؛ وهذا بعيد عن سيناريو "الهلاك" الذي يتم سرد تفاصيله بواسطة الكثير. هذا ولا يمكن المبالغة في تأثير جلب الأجهزة الخاصة وتزايد الأجهزة ولكن على المؤسسات أن تكون أكثر اهتمامًا بتهديدات مثل خسارة البيانات بشكل عرضي مع التأكيد على أن الموظفين لا "يثبتون" أو "يهربون" أجهزتهم ولا يثبتون التطبيقات إلا من القنوات الرسمية والموثوق بها. وإذا اختار المستخدمون الخروج خارج متاجر تطبيقات المحمول الرسمية، فعليهم التأكد ـ قبل تنزيل أي تطبيق ـ من أنهم يعرفون كاتب التطبيق ويثقون به ويمكنهم التحقق من أن الكود لم يتم التلاعب به.

وعند النظر إلى المشهد الأوسع لبرامج الويب الضارة، نجد أنه ليس من المفاجئ أن البرامج النصية الضارة والأطر المضمنة (iFrames) تشكل 83% من المواجهات عام 2012. وبينما يعد هذا متسقًا بشكل نسبي مع السنوات السابقة، إلا أنها نتيجة تستحق الدراسة. غالبًا ما تمثل هذه الأنواع من الهجمات كودًا ضارًا على صفحات ويب "موثوق بها" قد ينتقل إليها المستخدمون يوميًا؛ مما يعني أن المهاجم بإمكانه اختراق المستخدمين حتى دون إثارة الشكوك.

تأتي عمليات الاستغلال في المرتبة الثانية بمقدار 10 في المائة من إجمالي عدد مواجهات برامج الويب الضارة في العام الماضي. ومع ذلك، تعد هذه الأرقام نتيجة بدرجة كبيرة لمكان حدوث الكتلة في مقابل التركيز الفعلي على عمليات الاستغلال على الويب. على سبيل المثال، تعد نسبة الـ 83 في المائة من البرامج النصية وiFrames المخفية كتلاً تحدث في مرحلة مبكرة قبل أي تقديم للاستغلال ومن ثم قد يقل ـ بشكل زائف ـ عدد عمليات الاستغلال التي تتم ملاحظتها.

تظل عمليات الاستغلال سببًا رئيسيًا في الإصابة عبر الويب ويؤكد وجودها المستمر على حاجة البائعين إلى تبني أفضل ممارسات الأمان في دورات حياة منتجاتهم. ويجب أن تركز المؤسسات على الأمان كجزء من تصميم المنتج وعملية التطوير مع كشف الثغرات الأمنية في الوقت المناسب ودورات التصحيح الفورية/المنتظمة. لذا يتعين جعل المؤسسات والمستخدمين أيضًا على دراية بمخاطر

الأمان المقترنة باستخدام المنتجات التي لم تعد مدعومة بواسطة البائعين. ومن المهم أيضًا أن تحتفظ المؤسسات بعملية إدارة أساسية للثغرات الأمنية وأن يقوم المستخدمون بتحديث أجهزتهم وبرامجهم.

عند تقريب أعلى خمسة، سنجد أنهم سارقو المعلومات، مع نسبة 3.5 في المائة من إجمالي مواجهات برامج الويب الضارة في عام 2012 وأدوات التنزيل (1.1 في المائة) والفيروسات المتنقلة (0.8 في المائة). ومرة أخرى، تعد هذه الأرقام انعكاسًا لمكان حدوث الكمية الكبيرة، وهي بشكل عام في النقطة التي تمت عندها مواجهة البرنامج النصي أو iFrame الضار لأول مرة. ونتيجة لذلك، لا تعد هذه الأرقام انعكاسًا للعدد الحقيقي لسارقي المعلومات أو أدوات التنزيل أو الفيروسات المتنقلة التي يجري نشرها من خلال الويب.

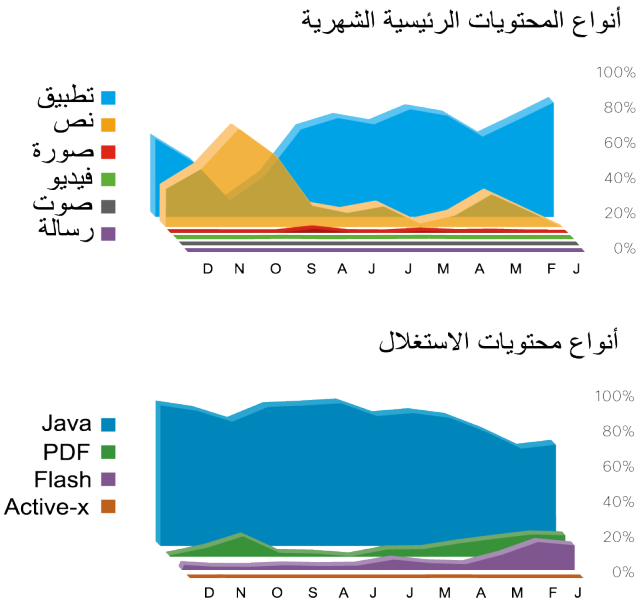
أشهر أنواع المحتوى الضار

يسعى منشئو البرامج الضارة إلى مضاعفة عائد الاستثمار الخاص بهم باستمرار من خلال التعرف على طرق للوصول إلى العدد الأكبر من الضحايا المحتملين بأقل مجهود وغالبًا ما يستغلون تقنيات الأنظمة الأساسية المتقاطعة عندما يتيسر ذلك. ولتحقيق هذه الأهداف، عادةً ما تقوم أدوات الاستغلال بتوصيل عمليات الاستغلال بترتيب معين، ولا تتم محاولة عمليات استغلال أخرى بمجرد توصيل عملية استغلال ناجحة. يوضح المستوى العالي من التركيز على عمليات استغلال Java ـ 87 في المائة من إجمالي عمليات الاستغلال على الويب ـ أنه تتم محاولة استخدام الثغرات الأمنية هذه قبل أنواع أخرى من عمليات الاستغلال وتوضح أيضًا أن المهاجمين ينجحون في استغلال Java. وبالإضافة إلى ذلك، ومع تشغيل أكثر من 3 مليارات جهاز لـ Java،[16] تمثل التقنية طريقة واضحة للمتسللين لتسلل هجماتهم عبر الأنظمة الأساسية المتقاطعة.

تحتل تقنيتان أخريان من الأنظمة الأساسية المتقاطعة ـ وهما PDF وFlash ـ المركز الثاني والثالث في تحليل Cisco لأعلى أنواع المحتوى نشرًا للبرامج الضارة. وعلى الرغم من أن Active X لا يزال يتم استغلاله، فإن باحثي Cisco وجدوا استخدامًا منخفضًا بشكل متسق لهذه التقنية كوسيلة للبرامج الضارة. ومع ذلك، وكما تم توضيحه سابقًا بخصوص Java، تعد الأعداد القليلة من أنواع معينة من عمليات الاستغلال انعكاسًا للترتيب التي تتم به محاولة عمليات الاستغلال بشكل كبير.

وعند فحص محتوى الوسائط، تكشف بيانات Cisco أن البرامج الضارة المستندة إلى الصور تبلغ حوالي ضعف الفيديو الذي لا يستند إلى Flash. ومع ذلك، يرجع هذا بشكل جزئي إلى الطريقة التي تتعامل بها المستعرضات مع أنواع المحتوى المعلنة وجهود المهاجمين لخداع عناصر التحكم هذه من خلال إعلان أنواع محتوى غير صحيحة. وبالإضافة إلى ذلك، فغالبًا ما تقوم أنظمة البرامج الضارة التي تعمل بطريقة الأمر والتحكم بنشر معلومات ملقم من خلال التعليقات المخفية في ملفات الصور العادية.

الشكل 6: أكثر أنواع البرامج الضارة انتشارًا على الإنترنت لعام 2012
شكلت عمليات استغلال Java 87% من إجمالي عمليات استغلال على الويب.

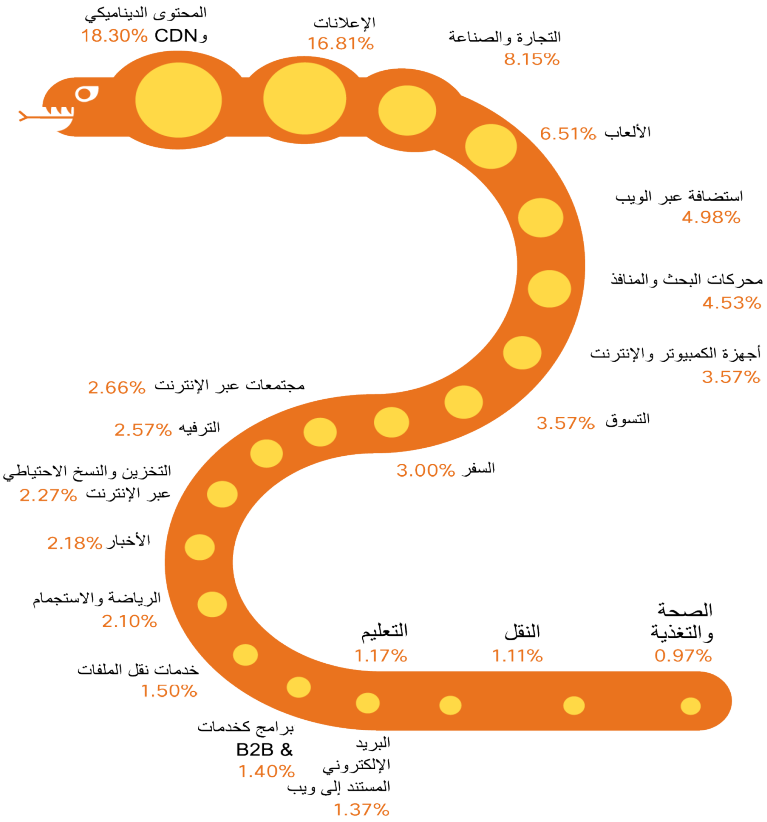


يوضح المستوى العالي من التركيز على عمليات استغلال Java أنه تتم محاولة الثغرات الأمنية هذه قبل أنواع أخرى من الاستغلال وتوضح أيضًا أن المهاجمين ينجحون في استغلال Java.

الشكل 7: أعلى فئات المواقع

مواقع التسوق عبر الإنترنت هي العرضة للإصابة بالمحتويات الضارة بمقدار 21 مرة أكثر من مواقع البرامج المزيفة.

ملاحظة: تأتي فئة "المحتوى الديناميكي" على رأس قائمة Cisco لأعلى المواقع احتمالاً للإصابة بالمحتويات الضارة. وتتضمن هذه الفئة أنظمة توفير المحتويات مثل إحصائيات الويب، وتحليلات المواقع، ومحتوى الأطراف الخارجية الأخرى التي ليس لها صلة بالإعلانات.



فئة أشهر المواقع

كما توضح بيانات Cisco، يعد المفهوم القائل بأن إصابات البرامج الضارة تنشأ في الأغلب عن مواقع "خطرة" - مثل البرامج المزيفة - مفهومًا خاطئًا. يوضح تحليل Cisco أن الأغلبية العظمى من مواجهات برامج الويب الضارة تحدث بالفعل من خلال الاستعراض القانوني للمواقع الإلكترونية الأساسية. بمعنى آخر، تحدث أغلبية المواجهات في الأماكن التي يزورها المستخدمون عبر الإنترنت أكثر من غيرها ويظنون أنها آمنة.

وتأتي الإعلانات الإلكترونية في المركز الثاني في القائمة حيث تشكل 16 في المائة من إجمالي مواجهات برامج الويب الضارة. الإعلانات المجمعة هي وسيلة شائعة لتحقيق الدخل من المواقع الويب ولذا قد يكون لإعلان ضار واحد تم نشره بهذه الطريقة تأثيرًا ضارًا هائلاً.

وعند النظر إلى المراكز الأدنى في قائمة فئات المواقع التي تحدث بها مواجهات البرامج الضارة، تأتي مواقع الأنشطة التجارية والصناعة في المركز الثالث؛ وهي المواقع المشتملة على كل شيء بدءًا من مواقع الشركات إلى الموارد البشرية وخدمات الشحن. وتأتي الألعاب عبر الإنترنت في المركز الرابع متبوعة بمواقع الاستضافة على الويب ومحركات البحث في المركز الخامس والسادس على التوالي. وتخلو أول 20 فئة للمواقع الإلكترونية من المواقع التي يعتقد عادةً أنها ضارة. وهناك مزيج سليم من أنواع المواقع الشائعة والقانونية مثل التسوق الإلكتروني في المركز الثامن والأخبار في المركز الثالث عشر وتطبيقات البرامج كخدمات/العمل للعمل في المركز السادس عشر.

اهتم مجرمو الإنترنت اهتمامًا كبيرًا بعادات الاستعراض الحديثة لتعريض أكبر عدد ممكن من الناس للبرامج الضارة عبر الويب. فأينما تواجد المستخدمون عبر الإنترنت، سيتبعهم منشئو البرامج الضارة مستفيدين من ميزة مواقع الويب الموثوق بها من خلال الاختراق المباشر أو شبكات التوزيع الخاصة بجهة خارجية.

التطبيقات الشائعة بحسب مرات الوصول إليها

تؤدي تغيرات كيفية قضاء الناس أوقاتهم على الإنترنت إلى توسيع المجال للمجرمين الإلكترونيين لإطلاق عملياتهم الاستغلالية. وتتبنى المؤسسات بجميع أحجامها الوسائط الاجتماعية ومقاطع الفيديو على الإنترنت؛ حيث تتواجد معظم العلامات التجارية الشهيرة على Facebook وTwitter ويقوم العديد بدمج الوسائط الاجتماعية في منتجاتهم الفعلية. وبينما تجتذب وجهات الويب هذه أعدادًا هائلة من الجمهور ويتم قبولها في إعدادات الشركة، يتم إنشاء المزيد من فرص توصيل البرامج الضارة أيضًا.

تحدث الأغلبية العظمى من مواجهات برامج الويب الضارة بالفعل من خلال الاستعراض القانوني للمواقع الإلكترونية الأساسية. بمعنى آخر، تحدث أغلبية المواجهات في الأماكن التي يزورها المستخدمون عبر الإنترنت أكثر من غيرها ويظنون أنها آمنة.

اهتم مجرمو الإنترنت اهتمامًا كبيرًا بعادات الاستعراض الحديثة لتعريض أكبر عدد ممكن من الناس للبرامج الضارة عبر الويب.

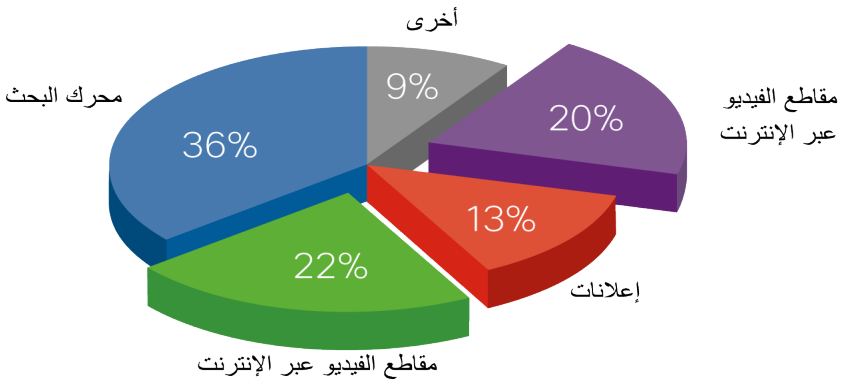
وفقًا لبيانات رؤية وتحكم التطبيقات من Cisco (AVC)، انقسمت الأغلبية العظمى (91 في المائة) من طلبات الويب بين محركات البحث (36 في المائة) ومواقع الفيديو على الإنترنت (22 في المائة) والشبكات الإعلانية (13 في المائة) والشبكات الاجتماعية (20 في المائة).

وإذا كانت البيانات في أشهر مواقع الويب التي تتم زيارتها على الإنترنت مرتبطة بأكثر فئات مواقع الويب خطورة، فإن الأماكن نفسها التي يواجه فيها المستخدمون عبر الإنترنت أعلى تعرض للبرامج الضارة، مثل محركات البحث، ستكون من بين أشهر الأماكن التي تجتذب مواجهات برامج الويب الضارة. وتظهر هذه العلاقات مرة أخرى أن منشئي البرامج الضارة يركزون على مضاعفة عوائد الاستثمار لديهم ولذا سيركزون جهودهم في الأماكن التي تكون فيها أعداد المستخدمين وسهولة التعرض عند أعلى المستويات.

وتتبنى المؤسسات بجميع أحجامها الوسائط الاجتماعية ومقاطع الفيديو على الإنترنت؛ حيث تتواجد معظم العلامات التجارية الشهيرة على Facebook وTwitter ويقوم العديد بدمج الوسائط الاجتماعية في منتجاتهم الفعلية.

الشكل 8: التطبيقات الشائعة حسب عدد الزيارات

تغير الوسائط الاجتماعية ومقاطع الفيديو على شبكة الإنترنت من طريقة قضاء الموظفين لأوقاتهم في العمل – وتعرضهم لثغرات أمنية جديدة.



وإذا كانت البيانات في أشهر مواقع الويب التي تتم زيارتها على الإنترنت مرتبطة بأكثر فئات مواقع الويب خطورة، فإن الأماكن نفسها التي يواجه فيها المستخدمون عبر الإنترنت أعلى تعرض للبرامج الضارة، مثل محركات البحث، ستكون من بين أشهر الأماكن التي تجتذب مواجهات برامج الويب الضارة.

عندما يولد الرعب القوطي البرامج الضارة

بواسطة كيفين و. هاملين
، أستاذ مشارك، قسم علوم الحاسبات، جامعة تكساس بدالاس

خداع البرامج الضارة هو تهديد مستجد يواجهه متخصصو الأمان بشكل متزايد. بينما تستخدم معظم البرامج الضارة تبديلاً أو تشويشًا بسيطا للتنويع وجعل هندستها عكسيًا أكثر صعوبة، تعد البرامج الضارة ذاتية الخداع أكثر تخفيًا حيث تندمج مع البرامج المحددة الموجودة بالفعل على كل نظام تصيبه. ويمكن لهذا أن يضلل أدوات الدفاع التي تبحث عن انحراف البرامج مثل فك حزمة وقت التشغيل أو الكود المشفر والتي غالبًا ما تكتشف برامج ضارة أكثر تقليدية.

أحدث تقنية برنامج ضار ذاتي الخداع ـ والذي أطلق عليه اسم فرانكينشتين (Frankenstein)[17] ـ هو ناتج أبحاثنا هذا العام عن مركز أبحاث وتعليم أمان الإنترنت بجامعة تكساس بدالاس. مثل العالم المجنون الخيالي في رواية الرعب لماري شيلي عام 1818، ينشئ "البرنامج الضار فرانكينشتين" طفرات من خلال سرقة أجزاء من الجسم (أي الكود) من برامج أخرى يواجهها ويجمع الكود معًا لإنشاء أشكال متنوعة من نفسه. ولذا تتكون كل طفرة من فرانكينشتين من برامج غير ضارة في مظهرها وغير غريبة ولا تقوم بفك حزمة وقت التشغيل أو التشفير المثير للشك؛ وتدخل إلى مجمع دائم التوسع من تحويلات الكود الذي تعلمته من العديد من البرامج التي تواجهها.

وبشكل متخف، يقوم فرانكينشتين بتشغيل ما أنشأه باستخدام مجموعة من الأساليب التي تم اجتذابها من نظرية المحول البرمجي وتحليل البرامج. ويتم فحص ثنائيات الضحايا أولاً للتحقق من وجود تسلسل بايت قصير يفك التشفير إلى سلاسل الإرشادات المحتمل أن تكون مفيدة والمسماة **بالأدوات**. ثم يستنتج المترجم المجرد التأثيرات الدلالية المحتملة لكل أداة تم اكتشافها. ثم يتم تطبيق بحث التتبع الخلفي لاكتشاف سلاسل الأداة التي تشتمل ـ عند التنفيذ بالترتيب ـ على تأثير تطبيق السلوك الضار لحمولة البرنامج الضار.

وأخيرًا، يتم تجميع كل سلسلة شبيهة مكتشفة لتكوين طفرة جديدة. وبشكل عملي، يكتشف فرانكينشتين ما يزيد عن 2000 أداة في الثانية ويجمع ما يزيد عن 100000 من اثنين أو ثلاثة فقط من ثنائيات من الضحايا خلال أقل من خمس ثوان. وباستخدام مثل هذا المجمع الكبير للأدوات تحت تصرفها، نادرًا ما تشترك الطفرات الناتجة في أية سلاسل إرشادات مشتركة؛ ولذا تبدو كل طفرة مميزة.

مثل العالم المجنون الخيالي في رواية الرعب لماري شيلي عام 1818، ينشئ "البرنامج الضار فرانكينشتين" طفرات من خلال سرقة أجزاء من الجسم (أي الكود) من برامج أخرى يواجهها ويجمع الكود معًا لإنشاء أشكال متنوعة من نفسه.

بشكل عام، ترجح أبحاثنا أن الجيل القادم من البرامج الضارة قد يتحاشى بشكل متزايد عمليات التحول البسيطة القائمة على التشفير والتعبئة في صالح عمليات التشويش الثنائية المتحولة المتقدمة مثل تلك المستخدمة بواسطة فرانكينشتين.

بشكل عام، ترجح أبحاثنا أن الجيل القادم من البرامج الضارة قد يتحاشى بشكل متزايد عمليات التحول البسيطة القائمة على التشفير والتعبئة في صالح عمليات التشويش الثنائية المتحولة المتقدمة مثل تلك المستخدمة بواسطة فرانكينشتين. حيث تعد عمليات التشويش هذه ممكنة التطبيق وتدعم الانتشار السريع كما أنها فعالة في إخفاء البرامج الضارة من مراحل التحليل الثابتة لمعظم محركات اكتشاف البرامج الضارة. ولمواجهة هذا الاتجاه، ستكون أدوات الدفاع بحاجة إلى نشر بعض التقنيات الشبيهة المستخدمة في تطوير فرانكينشتين، بما في ذلك التحليلات الثابتة القائمة على استخراج الميزات الدلالية بدلاً من البنائية والتوقيعات الدلالية المستخلصة من التعلم الآلي[18] بدلاً من التحليل اليدوي البحت.

تم دعم بحث تقارير هذه المقالة بشكل جزئي بواسطة جائزة المؤسسة الوطنية للعلوم *(NSF)* رقم *1054629* وجائزة مكتب سلاح الطيران الأمريكي للأبحاث العلمية *(AFOSR) FA9550-10-1-0088*. أية آراء أو نتائج أو استنتاجات أو توصيات تم التعبير عنها تخص المؤلف ولا تعبر بالضرورة عن آراء المؤسسة الوطنية للعلوم أو مكتب سلاح الطيران الأمريكي للأبحاث العلمية.

[17] فيشواث موهان وكيفين و. هاملين. "فرانكنيشتين: تلفيق البرامج الضارة من الثنائيات غير الضارة." في وقائع ورشة عمل USENIX حول التقنيات الهجومية (WOOT)، الصفحات 84-77، أغسطس 2012.

[18] محمد م. مسعود وتحسين م. الخطيب وكيفين و. هاملين وجينج جاو ولاتيفور خان وجياوي هان وبهافاني ثورايسيجام. اكتشاف البرامج الضارة "المستندة إلى السحابة" لإطلاق تدفقات البيانات. معاملات ACM حول أنظمة معلومات الإدارة 2(3)، (TMIS) أكتوبر 2011.

تحليل الثغرات الأمنية والتهديدات لعام 2012

يوضح جدول فئات الثغرات الأمنية والتهديدات زيادة كبيرة في إجمالي التهديدات؛ حيث زادت التهديدات عام 2012 بنسبة 19.8 في المائة خلال 2011. تشكل هذه الزيادة الحادة في التهديدات ضغطًا كبيرًا على قدرة المؤسسات على استمرار تحديث أنظمة إدارة الثغرات الأمنية وتصحيحها؛ وخصوصًا مع أخذ تغير البيئات الافتراضية في الاعتبار.

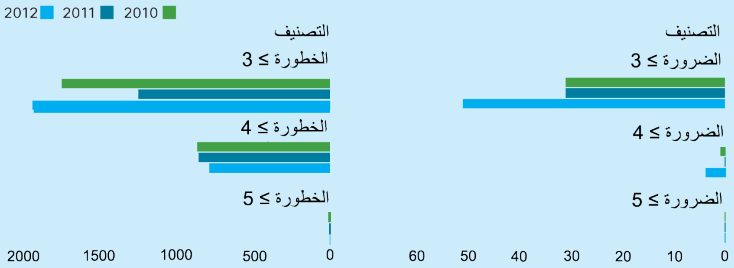
تحاول المؤسسات أيضًا أن تتعامل مع الاستخدام المتزايد لبرامج الجهات الخارجية ومفتوحة المصدر المضمنة في منتجاتها وفي بيئاتها. يقول جيف شيبلي، مدير أبحاث وعمليات الأمان في Cisco: "بإمكان ثغرة أمنية واحدة فقط في حلول جهة خارجية أو مفتوحة المصدر التأثير على مجموعة كبيرة من الأنظمة في البيئة بأكملها، مما يجعل تحديد جميع هذه الأنظمة وتصحيحها أو تحديثها صعبًا للغاية".

بالنسبة إلى أنواع التهديدات، تتمثل المجموعة الأكبر في تهديدات إدارة الموارد والتي تشتمل بشكل عام على رفض ثغرات رفض الخدمة وتهديدات التحقق من صحة الإدخال مثل حقنة SQL وأخطاء البرامج النصية للمواقع المشتركة وتجاوزات الاحتياطي التي تؤدي إلى رفض الخدمة. يشير توفر التهديدات المشابهة من السنوات السابقة بالإضافة إلى الزيادة الحادة في التهديدات إلى أن مجال الأمان بحاجة إلى الاستعداد بشكل أفضل لاكتشاف الثغرات الأمنية هذه والتعامل معها.

تعكس تصنيفات ضرورة تنبيه Cisco IntelliShield مستوى نشاط التهديد المتعلق بثغرة أمنية معينة. وتشير الزيادة الهائلة في تصنيفات ضرورة المستوى 3 أن المزيد من الثغرات الأمنية يتم استغلالها بالفعل. ويرجح أن يكون هذا بسبب الزيادة في عمليات الاستغلال المطروحة بشكل عام إما بواسطة الباحثين أو أدوات الاختبار ودمج عمليات الاستغلال هذه في مجموعات أدوات الهجوم. ويسمح هذا العاملان بتوفر المزيد من عمليات الاستغلال واستخدامها بشكل واسع بواسطة المتسللين والمجموعات الإجرامية.

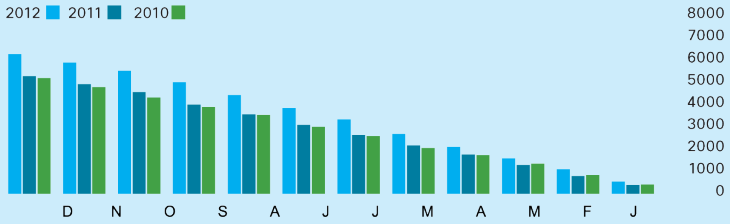
تعكس تصنيفات خطورة تنبيه Cisco IntelliShield مستوى تأثير عمليات الاستغلال الناجحة للثغرات الأمنية. كما توضح تصنيفات الخطورة زيادة ملحوظة في تهديدات المستوى 3؛ وذلك للأسباب نفسها الموضحة أعلاه فيما يتعلق بالتوفر الجاهز لأدوات الاستغلال.

الشكل 9: معدلات الخطورة والضرورة



الشكل 10: فئات الثغرات الأمنية والتهديدات

	أرقام التنبيه الشهري لعام 2010				أرقام التنبيه الشهري لعام 2010				أرقام التنبيه الشهري لعام 2010			
	الإجمالي	إعادة التوجيه	جديد		الإجمالي	إعادة التوجيه	جديد		الإجمالي	إعادة التوجيه	جديد	
يناير	417	158	259	417	403	166	237	403	552	208	344	552
فبراير	430	177	253	847	400	224	176	803	551	234	317	1103
مارس	518	194	324	1364	501	225	276	1304	487	249	238	1590
أبريل	375	208	167	1740	475	246	229	1779	524	218	306	2114
مايو	322	148	174	2062	404	219	185	2183	586	243	343	2700
يونيو	534	240	294	2596	472	251	221	2655	647	258	389	3347
يوليو	422	212	210	3018	453	240	213	3108	514	237	277	3861
أغسطس	541	255	286	3559	474	248	226	3582	591	285	306	4452
سبتمبر	357	190	167	3916	441	207	234	4023	572	242	330	5024
أكتوبر	418	227	191	4334	558	244	314	4581	517	237	280	5541
نوفمبر	476	224	252	4810	357	162	195	4938	375	200	175	5916
ديسمبر	400	197	203	5210	363	185	178	5301	376	193	183	6292
	5210	2430	2780		5301	2617	2684		6292	2804	3488	



"بإمكان ثغرة أمنية واحدة فقط في حلول جهة خارجية أو مفتوحة المصدر التأثير على مجموعة كبيرة من الأنظمة في البيئة بأكملها، مما يجعل تحديد جميع هذه الأنظمة وتصحيحها أو تحديثها صعبًا للغاية".

جيف شيبلي، مدير أبحاث وعمليات الأمان في Cisco

التهديدات المتطورة

طرق جديدة، عمليات الاستغلال نفسها

كل شيء مباح عندما يتعلق الأمر بعمليات الاستغلال على الإنترنت اليوم؛ طالما ستقوم الطريقة المختارة بإنجاز المهمة.

وهذا لا يعني أن اللاعبين في اقتصاد الظل لا يظلون ملتزمين بإنشاء أدوات وأساليب أكثر تعقيدًا لاختراق المستخدمين وإصابة الشبكات وسرقة بيانات مهمة؛ من بين العديد من الأهداف الأخرى. ومع ذلك، كان هناك اتجاه عام 2012 للرجوع مرة أخرى إلى "الأساليب القديمة الجيدة" للعثور على طرق جديدة للتسبب في إزعاج أدوات حماية الأمان بالمؤسسات أو التهرب منها.

تعد هجمات رفض الخدمة الموزع مثالاً أساسيًا وكانت عدة مؤسسات مالية أمريكية هامة هي الأهداف رفيعة المستوى لاثنتين من الحملات الرئيسية ذات الصلة والتي تم إطلاقهما بواسطة المجموعات الأجنبية للنضال عبر الاختراق البرمجي في الستة أشهر الأخيرة من عام 2012 (للحصول على تحليل مفصل، اطلع على قسم اتجاهات رفض الخدمة الموزع لعام 2012). هذا ويحذر بعض خبراء الأمان من أن هذه الأحداث ما هي إلا بداية وأن "المناضلين عبر الاختراق البرمجي وحلقات الجريمة المنظمة وحتى الدول سيكونون الجناة"[19] في الهجمات المستقبلية التي تعمل بشكل تعاوني وبشكل مستقل.

"نرى اتجاهًا لرفض الخدمة الموزع؛ وهذا من خلال إضافة المهاجمين لسياق إضافي عن موقعهم المستهدف لجعل الانقطاع أكثر ضخامة". نقلاً عن جافين ريد، مدير أبحاث التهديدات في عمليات استخبارات الأمان بـ Cisco . "وبدلاً من إجراء انتشار SYN، يحاول رفض الخدمة الموزع الآن التلاعب بتطبيق معين في المؤسسة؛ مما قد يتسبب في حدوث مجموعة متتالية من الأضرار في حالة الفشل".

بينما قد ترى المؤسسات أنها محمية بما فيه الكفاية ضد تهديدات رفض الخدمة الموزع، فإنه من المرجح ألا تتمكن شبكتهم من الدفاع في مواجهة النوع ذي الحجم الكبير وهجمات رفض الخدمة الموزع القاسية التي شهدها عام 2012. يقول جريجوري نيل أكيرس، نائب رئيس مجموعة مبادرات الأمان المتقدمة في Cisco قائلاً "حتى في مواجهة خصم متطور، ولكنه متوسط المستوى، غالبًا ما يتم التغلب بشكل كبير على أمان الشبكة الحالي والمتطور".

كان هناك اتجاه عام 2012 للرجوع مرة أخرى إلى "الأساليب القديمة الجيدة" للعثور على طرق جديدة للتسبب في إزعاج أدوات حماية الأمان بالمؤسسات أو التهرب منها.

"حتى في مواجهة خصم متطور، ولكنه متوسط المستوى، غالبًا ما يتم التغلب بشكل كبير على أمان الشبكة الحالي والمتطور".

جريجوري ديل أكيرس، نائب الرئيس لمجموعة مبادرات الأمان المتقدمة في Cisco

وهناك اتجاه آخر في مجتمع جرائم الإنترنت يدور حول "ديمقراطية" التهديدات. فنحن نشهد بشكل متزايد "مشاركة واسعة النطاق" الأدوات والتقنيات- والمعلومات حول كيفية استغلال الثغرات- في اقتصاد الظل في الوقت الحاضر. ويضيف أكيرس "لقد تطورت إمكانيات الأساليب المستخدمة في العمليات السرية بشكل كبير". "فنحن نشاهد الآن المزيد من التخصص والمزيد من التعاون بين منتجي البرامج الضارة. إنها أحد خطوط تجميع التهديد: فهناك من يقوم بتطوير الأخطاء، وشخص آخر يكتب برنامجًا ضارًا، وشخص آخر يصمم مكونات الهندسة الاجتماعية وما إلى ذلك ".

يعد إنشاء تهديدات قوية من شأنها أن تساعدهم على الوصول إلى كميات كبيرة من الأصول ذات القيمة المرتفعة التي يجدونها مصادفةً عبر الشبكة هو أحد الأسباب التي تجعل مجرمي الإنترنت يوحدون خبرتهم في أكثر الأحيان. ولكن مثل أي منظمة في العالم الحقيقي حيث تعد مهام الاستعانة بالجهات الخارجية والكفاءة وتوفير التكاليف من بين المحركات الرئيسية لنهج "إنشاء تهديد" في مجتمع جرائم الإنترنت. وتعمل "المواهب المستقلة" المعينة لهذه المهام على الإعلان عن مهاراتهم ودفع نسب لمجتمع جرائم الإنترنت الأوسع انتشارًا بشكل نموذجي من خلال الأسواق السرية عبر الإنترنت.

هجمات التضخيم والانعكاس

تستخدم هجمات تضخيم وانعكاس DNS[20] نظام أسماء النطاقات (DNS) لفتح محللات متداخلة أو ملقمات مخولة لزيادة حجم حركة الهجوم المرسل إلى ضحية ما. من خلال رسائل طلب DNS المخادعة[21]، تخفي هذه الهجمات المصدر الحقيقي للهجوم وترسل استعلامات DNS تعرض رسائل استجابة DNS بنسبة من 1000 إلى 10000 في المائة أكبر من رسالة طلب DNS. وتتم ملاحظة هذه الأنواع من ملفات تعريف الهجوم بشكل عام أثناء هجمات رفض الخدمة الموزع (DDoS)[22].

تشارك المؤسسات في هذه الهجمات دون قصد من خلال ترك محللات متداخلة مفتوحة على الإنترنت. ويمكنها اكتشاف الهجمات باستخدام أدوات[23] وتقنيات بيانات تتبع الاستخدام[24] ويمكنها المساعدة في منعها بواسطة تأمين[25] ملقم DNS التابع لها أو تقييد معدل[26] رسائل استجابة DNS.

اتجاهات رفض الخدمة الموزع لعام 2012

تم استخلاص التحليل التالي من مستودع Arbor Networks ATLAS، والذي يتكون من بيانات عمومية من عدد من المصادر؛ وذلك من 240 من موفري خدمات الإنترنت الذين يراقبون ذروة نسبة استخدام الشبكة التي تبلغ 37.8 تيرابت/الثانية.[27]

تستمر أحجام الهجوم في الاتجاه لأعلى

بشكل عام، كانت هناك زيادة في متوسط حجم الهجمات على مدار العام الماضي. كانت هناك زيادة 27 في المائة في إنتاجية الهجمات (من 1.23 جيجابت/ثانية عام 2011 إلى 1.57 جيجابت/ثانية عام 2012) وزيادة 15 في المائة في الحزم لكل ثانية مستخدمة في الهجمات (من 1.33 ميجابت/الثانية عام 2011 إلى 1.54 ميجابت/ثانية عام 2012).

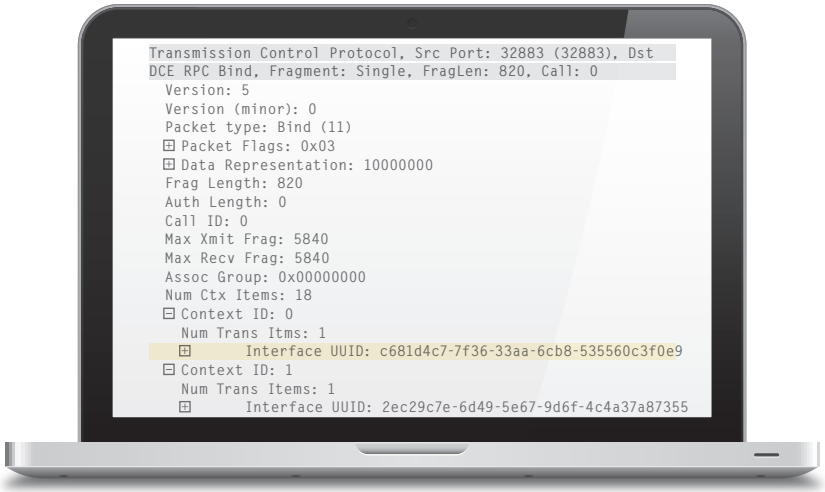
التركيبة الإحصائية للهجمات

أعلى مصادر الهجمات التي تمت مراقبتها ـ وذلك بعد إزالة 41 في المائة من المصادر الخالية من السمات بسبب تجهيل البيانات ـ هي الصين (17.8 في المائة) وكوريا الجنوبية (12.7 في المائة) والولايات المتحدة (8.0 في المائة).

الهجمات الكبرى

تم قياس أكبر الهجمات التي تمت مراقبتها عند 100.84 جيجابت/ثانية واستمرت لمدة 20 دقيقة تقريبًا (مصدر الهجمات غير معروف بسبب إخفاء هوية البيانات). تم قياس أكبر الهجمات التي تمت مراقبتها عند 82.36 ميجابت/ثانية واستمرت لمدة 24 دقيقة تقريبًا (مصدر الهجمات غير معروف بسبب إخفاء هوية البيانات).

الشكل 11: عمليات التهرب من نظام الوقاية من الاقتحام المباشر (IPS)



يدير قسم الأبحاث وعمليات الأمان في Cisco مختبرات البرامج الضارة العديدة لمراقبة حركة المرور الضارة في البيئة الطبيعية. حيث يتم إصدار البرامج الضارة عمدًا في المختبر للتأكد من أن الأجهزة الأمنية فعالة، ويتم ترك أجهزة الكمبيوتر أيضًا عرضة للهجوم والتعرض للإنترنت عن قصد.

أسلحة تقنيات التهرب الحديثة

يطور مجرمو الإنترنت باستمرار تقنيات جديدة لتجاوز الأجهزة الأمنية. ويراقب الباحثون في Cisco بيقظة التقنيات الجديدة و"أسلحة" التقنيات المعروفة.

يدير قسم الأبحاث وعمليات الأمان في Cisco مختبرات البرامج الضارة العديدة لمراقبة حركة المرور الضارة في البيئة الطبيعية. حيث يتم إصدار البرامج الضارة عمدًا في المختبر للتأكد من أن الأجهزة الأمنية فعالة، ويتم ترك أجهزة الكمبيوتر أيضًا عرضة للهجوم والتعرض للإنترنت عن قصد.

خلال اختبار واحد من هذا القبيل، اكتشفت تقنية نظام الحماية من التطفل (IPS) من Cisco إحدى الهجمات المعروفة لاستدعاء الإجراء البعيد (MSRPC) من .Microsoft وأفاد تحليل دقيق أن الهجوم كان يستخدم تكتيك تهرب البرامج الضارة غير المرئية في السابق في محاولة لتجاوز الأجهزة الأمنية.[28] حيث أرسل برنامج التهرب معرفات سياق ارتباطية عديدة ضمن طلب الارتباط الأولي. ويمكن لهذا النوع من الهجوم أن يتهرب من عمليات الحماية ما لم يراقب نظام الحماية من برامج التطفل ويحدد أيًا من المعرفات كانت ناجحة.

يطور مجرمو الإنترنت باستمرار تقنيات جديدة لتجاوز الأجهزة الأمنية. ويراقب الباحثون في Cisco بيقظة التقنيات الجديدة و"أسلحة" التقنيات المعروفة.

دراسة حالة

عملية أبابيل

خلال شهري سبتمبر وأكتوبر 2012، رصدت شبكات Cisco وArbor حملة هجوم خطيرة جدًا لهجوم رفض الخدمة الموزع (DDoS) المعروفة بعملية Ababil (أبابيل) والتي كانت تستهدف المؤسسات المالية الموجودة بالولايات المتحدة. "لقد تمت هجمات رفض الخدمة الموزع (DDoS) مع سبق الإصرار والترصد وبتركيز وبشكل معلن عنه قبل الواقعة وتم تنفيذها حرفيًا . تمكن المهاجمون من اختراق العديد من المواقع المالية الرئيسية غير المتاحة للعملاء الشرعيين في دقائق -وفي الحالات الأكثر خطورة في ساعات. على مدار الأحداث، ادعت عدة مجموعات مسؤوليتها عن الهجمات؛ وادعت مجموعة واحدة على الأقل أنها تحتج على حقوق الطبع والنشر والملكية الفكرية في الولايات المتحدة. وآخرون قاموا بنشر مشاركتهم كرد على الفيديو المسيء لبعض المسلمين على موقع YouTube.

من وجهة نظر الأمن المعلوماتي على الإنترنت، فإن عملية أبابيل جديرة بالذكر لأنها استغلت تطبيقات الويب المشتركة واستضافة الخوادم التي تحظى بشعبية لأنها عرضة للهجوم. كان العامل الآخر الواضح والغير مألوف والمستخدم في هذه السلسلة من الهجمات أنه تم إطلاق الهجمات المتزامنة، في مستوى نطاق ترددي عريض، ضد شركات متعددة في نفس المجال (المجال المالي).

كما يُشاهد في مجال الأمان في كثير من الأحيان، أن ما هو قديم قد يكون جديدًا مرة أخرى.

في 18 سبتمبر، 2012، "نشرت كتائب عز الدين القسام الإلكترونية على موقع Pastebin[29] يلتمسون من المسلمين استهداف المؤسسات المالية والأنظمة الأساسية لتداول السلع الرئيسية. وقد تم تدبير التهديدات والأهداف المحددة ليراها العالم واستمرت لمدة أربعة أسابيع متتالية. كل أسبوع، تحدث تهديدات جديدة مع أهداف جديدة تعقبها أعمال في أوقات وتواريخ معينة. بحلول الأسبوع الخامس، توقفت الجماعة عن تحديد الأهداف إلا أنه من الواضح أن الحملات ستستمر. وكما وعدت، فقد تجددت الحملات بشكل جدي في ديسمبر 2012، مرة أخرى باستهداف المنظمات المالية الكبيرة والعديدة في الولايات المتحدة.

تم الإعلان أيضًا عن المرحلة الثانية لعملية أبابيل على موقع Pastebin.[30] فيدلاً من الأجهزة المصابة، استُخدمت مجموعة متنوعة من تطبيقات الويب PHP،بما في ذلك نظام إدارة المحتوى لبرنامج Joomla كبرامج تحكم سرية رئيسية في الحملة. بالإضافة إلى ذلك، تتعرض العديد من مواقع WordPress، والتي تستخدم غالبًا الوظيفة الإضافية TimThumb للخطر في نفس الوقت تقريبًا. لاحق المهاجمون في كثير من الأحيان الخوادم التي لا تتم صيانتها التي تستضيف تلك التطبيقات وحملوا برامج webshell التي تعمل وفق لغة PHP لنشر المزيد من أدوات الهجوم. ولم يتم تطبيق مفهوم "الأمر والتحكم" بالطريقة المعتادة، ومع ذلك، اتصل المهاجمون بالأدوات مباشرةً أو عن طريق خوادم وسيطة وبرامج نصية ووكلاء. خلال أحداث جرائم الإنترنت في سبتمبر وأكتوبر 2012، تم استخدام مجموعة كبيرة من الملفات والأدوات التي تستند إلى لغة PHP وليس مجرد الأدوات التي تم الإبلاغ عنها على نطاق واسع مثل "tsoknoproblembro" والمعروفة أيضًا باسم (aka "Brobot"). وفي الجولة الثانية من النشاط استخدمت أيضًا أدوات هجوم محدثة مثل Brobot V2.

نشرت عملية أبابيل مجموعة من الأدوات مع متجهات تتقاطع مع هجمات طبقة التطبيق على HTTP وHTTPS وDNS مع تنفيذ حركة مرور هجوم كبيرة على مجموعة متنوعة من البروتوكولات مثل TCP وUDP وICM وغيرها من بروتوكولات IP. وأظهر تحليل Cisco أن أغلب الحزم تم إرسالها إلى TCP/UDP منفذ 53 (DNS) أو 80 (HTTP). بينما تمثل حركة المرور على منفذ UDP رقم 53 ومنفذ TCP رقم 53 و80 حركة مرور صالحة عادةً، تمثل الحزم الموجهة إلى منفذ UDP 80 حالة شاذة لا يتم استخدامها عمومًا من خلال التطبيقات.

ويمكن الاطلاع على تقرير مفصل عن أنماط وحمولات حملة عملية أبابيل في استجابة Cisco للحدث: هجمات رفض الخدمة الموزع على المؤسسات المالية.[31]

الدروس المستفادة

بينما تعتمد الأجهزة الخاصة بأنظمة الحماية من التطفل وجدار الحماية على اختبار حالة الزيارة، فهي تعد جزءًا هامًا لأي مجموعة أمان خاصة بالشبكة. تقوم التقنيات على مستوى التطبيق المستخدمة في حملة عملية أبابيل بارباك جداول الحالات تلك وفي حالات عديدة تؤدي إلى إخفاقها كانت تقنية تخفيف رفض الخدمة الموزع (DDoS) الذكية هي الإجراء المضاد الفعال.

لدى خدمات الأمن المدارة وموفري خدمة الإنترنت الحدود الخاصة بهم. في إحدى هجمات رفض الخدمة الموزع (DDoS) الفعلية، توصي الحكمة السائدة بالتعامل مع الهجمات الكبيرة داخل الشبكة. بالنسبة للحملات على مستوى التطبيق التي يتم نشرها بالقرب من الضحية، فينبغي أن تعالج مثل تلك الحملات في مركز البيانات أو على "جهاز التوجيه الخاص بالعميل." لأن هناك منظمات متعددة تم استهدافها في وقت واحد، كما تم إجهاد مراكز أجهزة الشبكة.

فمن الأهمية الحفاظ على الأجهزة والبرامج محدثة على أجهزة تخفيف رفض الخدمة الموزع (DDoS). لا تتمكن عمليات النشر القديمة دومًا من التعامل مع التهديدات الحديثة. لذا من المهم أيضًا أن يكون لديك السعة المناسبة في الأماكن الصحيحة. أن تكون قادرًا على الحد من هجمة كبيرة أمر لا طائل منه إذا كان لا يمكن توجيه حركة المرور إلى موقع يتم من خلاله نشر التقنية.

في حين أن تقنية التخفيف باستخدام السحابة أو رفض الخدمة الموزع (DDoS) الشبكية لديها فعليًا سعة عرض نطاق ترددي كبير للغاية، وتوفر الحلول في مقر المؤسسة تفاعلاً ضد الهجمات وتحكمًا فيها ومراقبتها على نحو أفضل. ويؤدي دمج التقنيتين إلى توفر حل أكثر اكتمالاً.

بالإضافة إلى استخدام تقنيات السحابة و تنفيذ رفض الخدمة الموزع (DDoS) عن طريق الشبكة، وكجزء من الضمانات المقدمة لأحداث عملية أبابيل، حددت Cisco أساليب الاستشعار والتخفيف في تحديد هجمات رفض الخدمة الموزع (DDoS) التي تستهدف المؤسسات المالية والحد منها والتي طبقت نشرة التخفيف من الهجمات.[32] هذه التقنيات تشمل استخدام تصفية قائمة التحكم بالوصول إلى نقطة الانتقال (tACL) و تحليل بيانات NetFlow، وإعادة التوجيه العكسي للمسار ذي البث الأحادي (uRPF). وبالإضافة إلى ذلك، هناك عدد من أفضل الممارسات التي ينبغي مراجعتها بانتظام واختبارها، وتنفيذها والتي من شأنها أن تساعد إلى حد كبير المؤسسات للتحضير لأحداث الشبكة والتعامل معها. يمكن العثور على مكتبة تضم أفضل الممارسات من خلال الرجوع إلى المصادر التكتيكية الخاصة بـ Cisco SIO[33] وأفضل الممارسات الأمنية لمزود الخدمة.[34]

الرسائل غير المرغوب فيها الموجودة دومًا

تستمر كميات الرسائل غير المرغوبٍ فيها في الانخفاض في جميع أنحاء العالم، وفقا لبحث Cisco، ولكن تظل الرسائل غير المرغوب فيها أداة الوصول للعديد من مجرمي الإنترنت، الذين ينظرون إليها على أنها وسيلة فعالة وسريعة لتعريض المستخدمين للبرامج الضارة وتسهيل إجراء مجموعة واسعة من الحيل.

ومع ذلك، على الرغم من إدراك أنه يتم نشر البرامج الضارة عادةً من خلال مرفقات البريد الإلكتروني غير المرغوب فيها، يبين بحث Cisco أنه يعتمد عدد قليل جدًا من مرسلي رسائل غير المرغوب فيها اليوم على هذه الطريقة، بدلاً من ذلك، فإنهم يلجأون إلى الارتباطات الضارة داخل البريد الإلكتروني كآلية توزيع أكثر كفاءة.

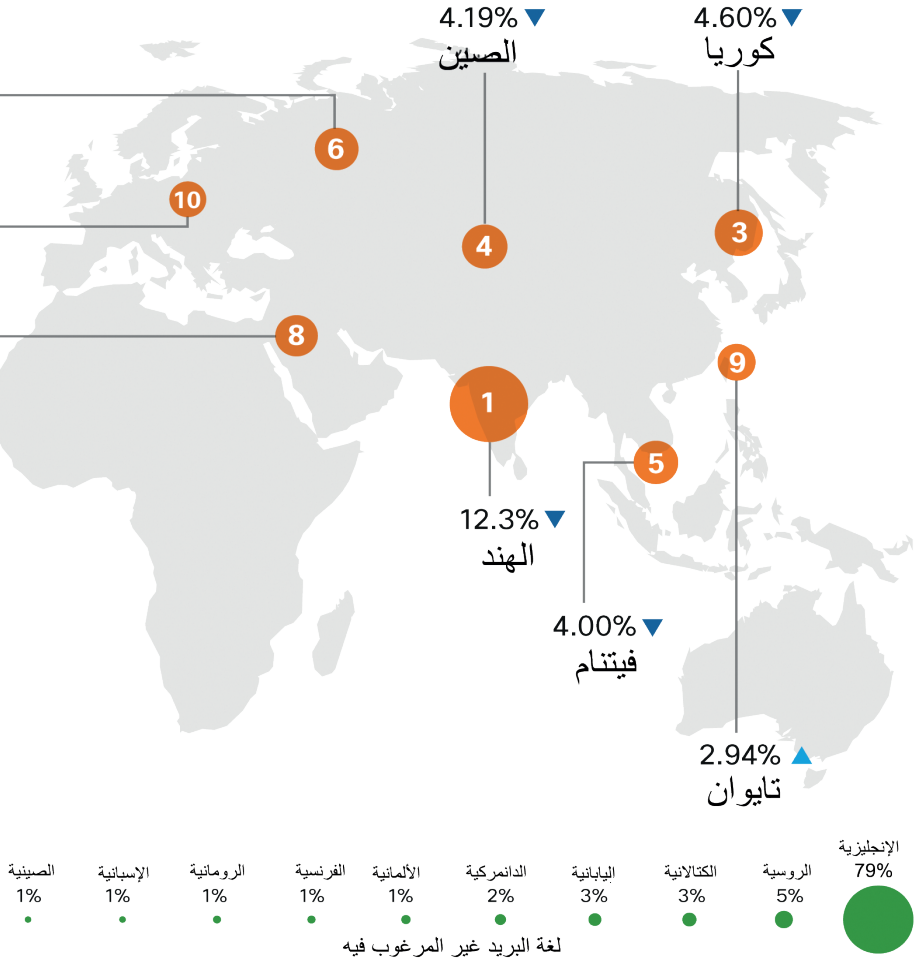
الرسائل غير المرغوب فيها هي أيضًا أقل "تبعثرًا" مما كانت عليه في الماضي، مع تفضيل العديد من مرسلي رسائل البريد غير المرغوب فيها لاستهداف مجموعات محددة من المستخدمين على أمل تحقيق أرباح مرتفعة. تعتلي الأدوية ذات الأسماء التجارية المعروفة و الماركات الفاخرة من الساعات والأحذاث مثل موسم الضرائب قائمة أكثر الأشياء التي يروج لها مرسلو البريد غير المرغوب فيه في حملاتهم. مع مرور الوقت، تعلم مرسلو البريد غير المرغوب فيه أن أسرع طريقة لجذب المزيد من النقرات وإجراء عمليات الشراء- ولتحقيق الربح- هو رفع العلامات التجارية الانتحالية والاستفادة من الأحداث الجارية التي تحظى باهتمام مجموعات كبيرة من المستخدمين.

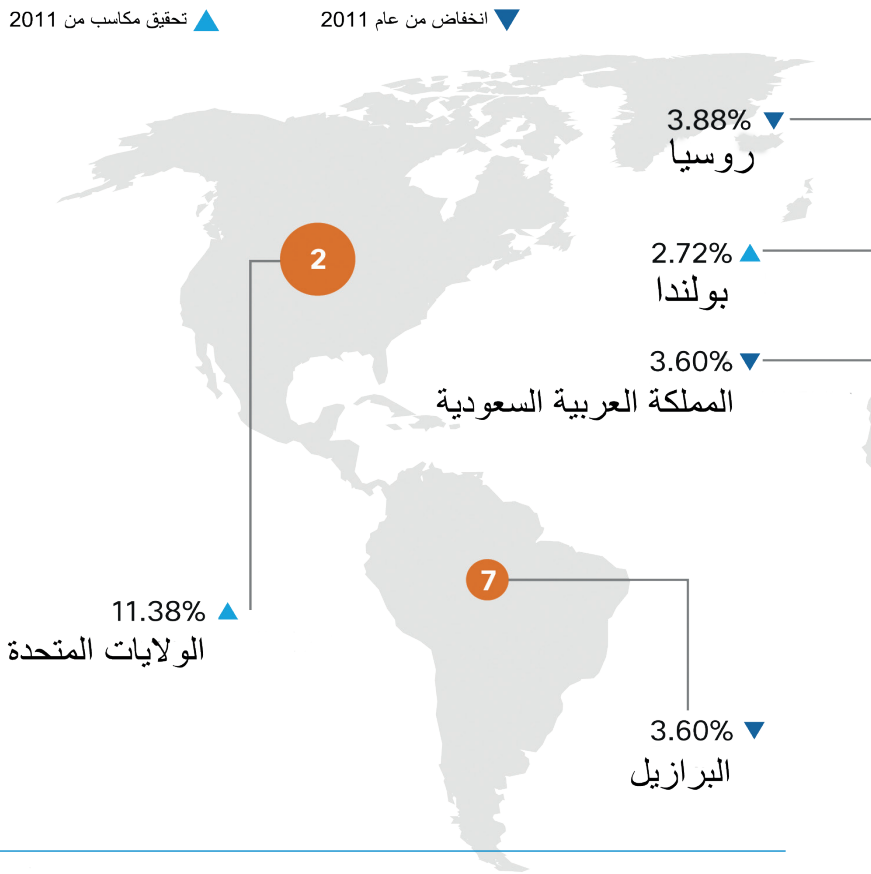
الاتجاهات العالمية لرسائل البريد غير المرغوب فيها

منذ الاختراقات واسعة النطاق التي قامت بها أجهزة الروبوت عام 2010، لم تعد رسائل البريد غير المرغوب فيها فعالة كما كانت عليه سابقًا، وقد تعلم مرسلو الرسائل غير المرغوب فيها وقاموا بتغيير أساليبهم التكتيكية. هناك تطور واضح تجاه الحملات الأصغر حجمًا والأكثر استهدافًا والتي تستند إلى الأحداث العالمية ومجموعات فرعية معينة من المستخدمين. يمكن ملاحظة الرسائل غير المرغوب فيها ذات الحجم الكبير بشكل محتمل من قبل مزودي خدمات البريد وإغلاقها قبل أن يتحقق الغرض منها.

الشكل 12: اتجاهات البريد العالمي غير المرغوب فيه

انخفض حجم البريد العالمي غير المرغوب فيه بنسبة 18%، مع حفاظ معظم مرسلي البريد العشوائي على ساعات المصرفيين في عطلات نهاية الأسبوع.





يمكن ملاحظة الرسائل غير المرغوب فيها ذات الحجم الكبير بشكل محتمل من قبل مزودي خدمات البريد وإغلاقها قبل أن يتحقق الغرض منها.

في عام 2012، كان هناك عدة أمثلة لمرسلي رسائل البريد غير المرغوب فيها باستخدام أخبار عن أحداث العالم -وحتى عن المآسي التي يمر بها الأشخاص- لاستغلال المستخدمين.

في عام 2011، كان إجمالي أحجام رسائل البريد العالمية غير المرغوب فيها أقل من 18 في المائة. هذا أبعد ما يكون عن نسبة الانخفاض الكبيرة في الحجم التي تم رصدها في عام 2010 في أعقاب الاختراقات التي أحدثتها أجهزة الروبوت، ولكن استمرار اتجاه الهبوط هو تطور إيجابي مع ذلك.

واصل مرسلو رسائل البريد غير المرغوب فيها تركيزهم على الحد من المجهود مع زيادة التأثير. وفقًا لبحث Cisco، تنخفض أحجام رسائل البريد غير المرغوب فيها من 25 بالمائة في عطلات نهاية الأسبوع، عندما يكون المستخدمون بعيدين عن بريدهم الإلكتروني في كثير من الأحيان. يرتفع حجم رسائل البريد غير المرغوب فيها إلى أعلى مستويات يومي الثلاثاء والأربعاء- في المتوسط 10 بالمائة أعلى من غيرها في أيام الأسبوع. يتيح هذا النشاط المتزايد في منتصف الأسبوع وانخفاض الكميات في عطلة نهاية الأسبوع لمرسلي رسائل البريد غير المرغوب فيها عيش "حياة طبيعية."

كما أنه يتيح لهم الوقت لإجراء حملات خادعة مخصصة تستند إلى أحداث العالم في وقت مبكر من الأسبوع من شأنها أن تساعدهم على إنشاء معدل استجابة أعلى لحملاتهم.

في عام 2012، كان هناك عدة أمثلة لمرسلي رسائل البريد غير المرغوب فيها باستخدام أخبار عن أحداث العالم -وحتى عن المآسي التي يمر بها الأشخاص- لاستغلال المستخدمين. خلال إعصار ساندي الهائل، على سبيل المثال، حدد الباحثون في Cisco وجود عمليات احتيال ضخمة تعرف بـ "الضخ والإغراق" للأسهم استنادًا إلى حملة الرسائل غير المرغوب فيها. باستخدام رسالة بريد إلكتروني موجودة من قبل والتي طالبت الأشخاص بالاستثمار في الأسهم الرخيصة التي ركزت على استكشاف الموارد الطبيعية، بدأ مرسلو رسائل البريد غير المرغوب فيها بإرفاق العناوين المثيرة عن إعصار ساندي. أحد الجوانب غير العادية من هذه الحملة هو أن مرسلي رسائل غير المرغوب فيها استخدموا عناوين IP فريدة لإرسال مجموعة من الرسائل غير المرغوب فيها والتي لم تنشط هذه العناوين منذ ذلك الحين.

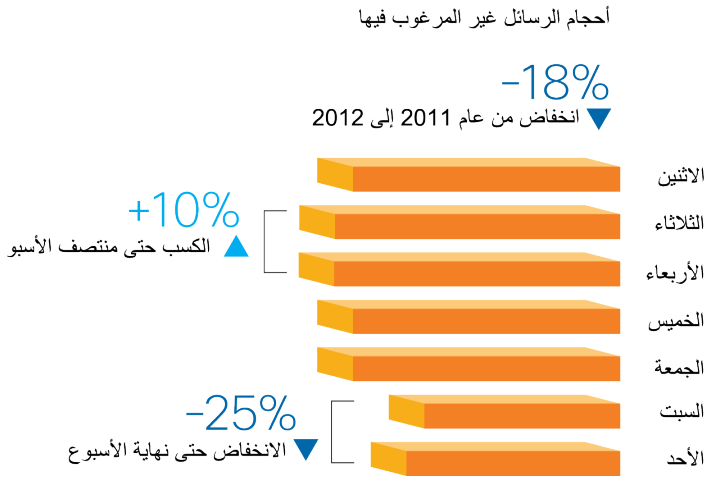
إنشاء رسائل بريد غير مرغوب فيها

في عالم رسائل البريد غير المرغوب فيها، بعض البلدان لا تزال كما هي بينما يقوم الآخرين بتغيير ترتيبهم بشكل كبير. في عام 2012، احتفظت الهند بأعلى مركز كأحد مصادر الرسائل غير المرغوب فيها، وانتقلت الولايات المتحدة صعودًا من المركز السادس في عام 2011 إلى المركز الثاني في عام 2012. وبتقريب أعلى خمس دول متصدرة في إرسال الرسائل غير المرغوب فيها نجد كوريا تحتل المركز الثالث، والصين في المركز الرابع وفيتنام في المركز الخامس.

وعمومًا، يركز غالبية مرسلي الرسائل غير المرغوب فيها جهودهم على إنشاء رسائل غير مرغوب فيها تشتمل على لغات يتحدث بها أكبر عدد من الجماهير التي تستخدم البريد الإلكتروني بشكل منتظم. وفقًا لبحث Cisco، فإن اللغة الأولى للرسائل غير المرغوب فيها في عام 2012 هي اللغة الإنجليزية، تليها الروسية، الكتالانية، واليابانية، والدنماركية. معلومة هامة، هناك فجوات بين

الشكل 13: منشأ البريد غير المرغوب فيه

تحتل الهند قمة الدول التي بها بريد غير مرغوب فيه، بينما يسطع نجم الولايات المتحدة لتأتي في المركز الثاني.



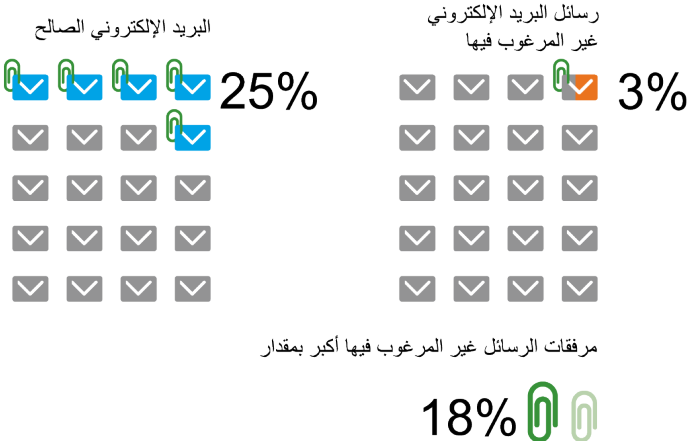
المكان الذي يتم من خلاله إرسال الرسائل غير المرغوب فيها واللغات التي يتم استخدامها في الرسالة غير المرغوب فيها: على سبيل المثال، بينما كانت الهند هي الدولة الأولى في إرسال الرسائل غير المرغوب فيها في عام 2012، لم تتخطَ اللهجات المحلية أعلى 10 دول من حيث اللغات المستخدمة في الرسائل غير المرغوب فيها التي تم إرسالها من الهند. وينطبق نفس الشيء على كوريا وفيتنام والصين

مرفقات رسائل البريد الإلكتروني

كان يعتقد منذ فترة طويلة أن الرسائل غير المرغوب فيها تعمل كآلية تسليم للبرامج الضارة، وخصوصًا عندما يتم تضمين أحد المرفقات. لكن يبين أحدث أبحاث Cisco بشأن استخدام مرفقات البريد الإلكتروني في حملات الرسائل غير المرغوب فيها أن هذا التصور قد يكون من الأوهام.

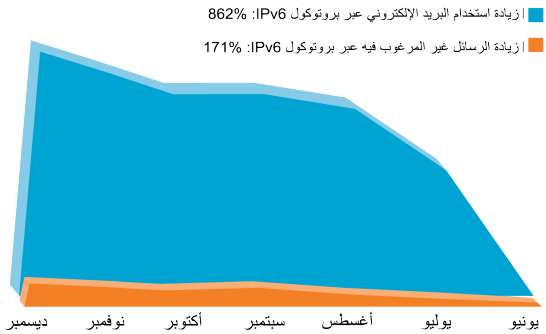
الشكل 14: مرفقات البريد الإلكتروني

هناك فقط نسبة 3 بالمائة من البريد غير المرغوب فيه بها مرفقات مقابل 25 بالمائة من البريد الإلكتروني الصحيح، ولكن مرفقات البريد غير المرغوب فيه تزيد بنسبة 18 بالمائة.



الشكل 15:الرسائل غير المرغوب فيها لبروتوكول IPv6

بينما يظل البريد الإلكتروني المستند إلى البروتوكول IPv6 يمثل نسبة صغيرة للغاية من نسبة استخدام الشبكة بوجه عام، فهو في ازدياد حيث ينتقل الكثيرون من مستخدمي البريد الإلكتروني إلى البنية التحتية التي يدعمها بروتوكول IPv6.



هناك 3 بالمائة فقط من إجمالي الرسائل غير المرغوب فيها بها مرفقات، مقابل 25 بالمائة من البريد الإلكتروني الصالح يكون بها مرفقات. وفي حالات نادرة عندما لا تتضمن إحدى الرسائل غير المرغوب فيها مرفقًا، يكون المتوسط البالغ 18 % أكبر من مرفق نموذجي سيتم تضمينه في بريد إلكتروني صالح. ونتيجة لذلك، تميل هذه المرفقات إلى الظهور.

في رسائل البريد الإلكتروني الحديثة، تعد الارتباطات هي أهم جزء. يصمم مرسلو رسائل البريد غير المرغوب فيها حملات لإقناع المستخدمين بزيارة مواقع ويب حيث يمكنهم شراء منتجات أو خدمات (غالبًا ما يكون مشكوك فيها). وبمجرد دخولهم، يتم تجميع المعلومات الشخصية للمستخدمين، وغالبًا دون علمهم، أو يتعرضون للخطر بطريقة أخرى.

كما يكشف تحليل "العلامات التجارية الانتحالية" الذي يظهر لاحقًا في هذا القسم، أن غالبية الرسائل غير المرغوب فيها يتم إرسالها من جماعات تسعى لبيع مجموعة محددة جدًا من سلع لها اسم تجاري - بدءًا من الساعات الفخمة إلى الأدوية التي تكون - في معظم الحالات - وهمية.

الرسائل غير المرغوب فيها لبروتوكول IPv6

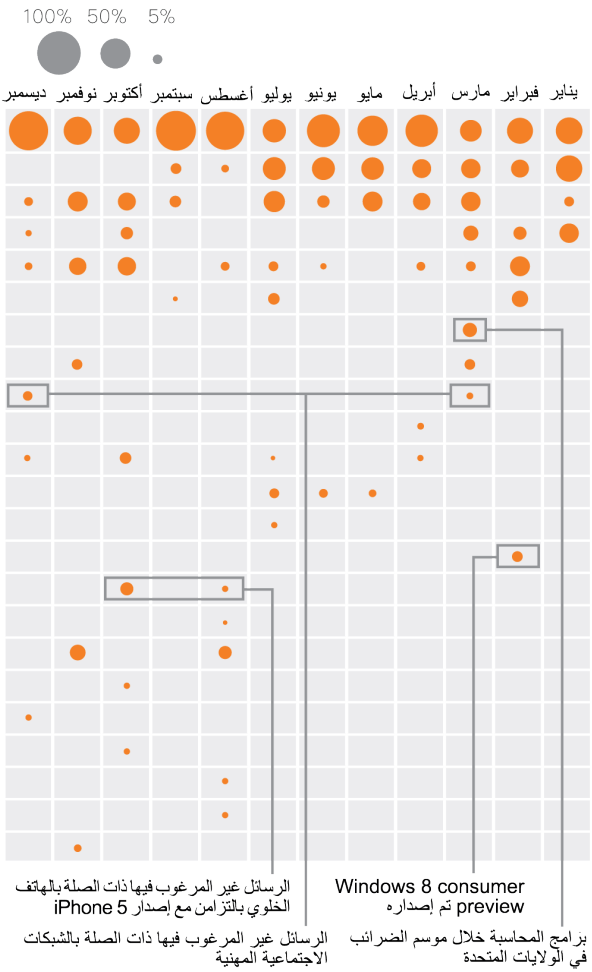
بينما يظل البريد الإلكتروني المستند إلى البروتوكول IPv6 يمثل نسبة صغيرة للغاية من نسبة استخدام الشبكة بوجه عام، فهو في ازدياد حيث ينتقل الكثيرون من مستخدمي البريد الإلكتروني إلى البنية التحتية التي يدعمها بروتوكول IPv6.

ومع ذلك، في حين أن حجم البريد الإلكتروني الإجمالي ينمو بوتيرة سريعة، فإن هذه الحالة لا تنطبق على رسائل البريد غير المرغوب فيها لبروتوكول IPv6. وهذا يشير إلى أن مرسلي الرسائل غير المرغوب فيها يتحوطون ضد الوقت والنفقات للانتقال إلى معيار جديد للإنترنت. ليست هناك حاجة محركة لمرسلي الرسائل غير المرغوب فيها - ولا تتوفر فائدة أساسية أو لا توجد- لإحداث هذا التحول في الوقت الحاضر. حيث يتم استنفاد عناوين IPv4 وتسير أجهزة الجوال ووسائل الاتصال عن طريق M2M نحو النمو السريع في بروتوكول IPv6، فيتوقع أن يقوم مرسلو الرسائل غير المرغوب فيها بتحديث البنية الأساسية وتسريع مجهوداتهم.

في رسائل البريد الإلكتروني الحديثة، تعد الارتباطات هي أهم جزء. يصمم مرسلو الرسائل غير المرغوب فيها حملات لإقناع المستخدمين بزيارة مواقع ويب حيث يمكنهم شراء منتجات أو خدمات. وبمجرد دخولهم، يتم تجميع المعلومات الشخصية للمستخدمين، وغالبًا دون علمهم، أو يتعرضون للخطر بطريقة أخرى.

الشكل 16: العلامات التجارية الانتحالية

يستهدف مرسلو البريد غير المرغوب فيه الأدوية والساعات الفاخرة وموسم الضرائب.



العلامات التجارية الانتحالية

مع الرسائل غير المرغوب فيها والخاصة بالعلامات التجارية الانتحالية، يستخدم مرسلو الرسائل غير المرغوب فيها منظمات ومنتجات لإرسال رسائلهم على أمل أن ينقر مستخدمو الإنترنت المتصلين على ارتباط أو يقوموا بإجراء عملية شراء. إن أغلب الأسماء التجارية الانتحالية تتمثل في الوصفات الطبية، مثل الأدوية المضادة للقلق والمسكنات. وبالإضافة إلى ذلك، تشكل ماركات الساعات الفاخرة طبقة ثابتة من "الجلبة" تستمر على ذلك طوال العام.

يبين تحليل Cisco أن مرسلي الرسائل غير المرغوب فيها يتمتعون أيضًا بمهارة في ربط حملاتهم بالأحداث. من يناير إلى مارس 2012، تظهر بيانات Cisco ارتفاعًا مفاجئًا في رسائل البريد غير المرغوب فيها في ما يتعلق ببرامج Window، التي تزامنت مع إصدار نظام التشغيل Windows 8. من فبراير إلى أبريل 2012 أثناء موسم الضرائب في الولايات المتحدة، يظهر التحليل زيادة شديدة في رسائل البريد غير المرغوب فيها المرتبطة ببرامج الضرائب.

من يناير إلى مارس 2012، ومرة أخرى من سبتمبر إلى ديسمبر 2012 - بداية ونهاية العام- قامت الرسائل غير المرغوب فيها المتعلقة بالشبكات المهنية باختراقات كبيرة، ربما لأن مرسلي الرسائل غير المرغوب فيها يعرفون أن الأشخاص غالبًا ما يبدؤون في إجراء عمليات البحث عن وظائف خلال هذه الأوقات من السنة.

وخلاصة القول: إن ما يقوم به مرسلو الرسائل غير المرغوب فيها هو من أجل المال، وعلى مر السنين، قد تعلموا أن أسرع طريقة لجذب النقرات وإجراء عمليات الشراء يتمثل في عرض أدوية وبضائع فاخرة ومن خلال تخصيص هجماتهم للأحداث التي تلفت انتباه الكثير في العالم.

من سبتمبر إلى نوفمبر 2012، أجرى مرسلو الرسائل غير المرغوب فيها سلسلة من الحملات متنكرين في هيئة شركات خلوية وبالتزامن مع إصدار iPhone 5.

من يناير إلى مارس 2012، ومرة أخرى من سبتمبر إلى ديسمبر 2012 - بداية ونهاية العام- قامت الرسائل غير المرغوب فيها المتعلقة بالشبكات المهنية باختراقات كبيرة، ربما لأن مرسلي الرسائل غير المرغوب فيها يعرفون أن الأشخاص غالبًا ما يبدأون في إجراء عمليات البحث عن وظائف خلال هذه الأوقات من السنة.

إدارة الثغرات: على المورد أن يقوم بأداء المزيد أكثر من سرد إيجابيات وسلبيات المنتج [35]

كيف يكشف بائع ما مشاكل الأمان المتعلقة بالمنتج هو الجانب الأكثر وضوحًا لممارسات إدارة الثغرات. في Cisco، يتم إجراء أبحاث على تقارير الأمان الإرشادية [36] ونشرها من قبل فريق الاستجابة للحوادث الأمنية الخاصة بالمنتج (PSIRT)، وهو فريق مكون من كبار الخبراء الأمنيين الذين يدركون أن حماية عملاء Cisco وحماية الشركة عملية مترابطة.

يصرح روسيل سمواك، كبير مديري البحث وعمليات الأمان في Cisco "تعلن تقارير الأمان الإرشادية عن أكثر مشاكل أمان المنتج خطورة وعادةً ما تكون أول دليل عام لوجود ثغرة أمنية في منتج Cisco "، ويضيف "على هذا النحو، من المهم جدًا أن تكون إحدى وسائل الاتصال الفعالة التي تساعد العملاء على اتخاذ قرارات واعية وإدارة المخاطر الخاصة بهم. بالإضافة إلى تقنيات التخفيف المتقدمة[37] التي نوفرها لعملائنا لدعم القدرات في أدوات Cisco الحالية، فنحن قادرون على توفير الكثير من التفاصيل للرد بسرعة وثقة."

ومع ذلك، تبدأ إدارة الثغرات، في وقت مبكر في دورة حياة الثغرة ويمكن أن تمتد إلى ما بعد الكشف الأولي. يواصل سمواك قائلاً " التحسين المستمر في ممارسات إدارة الثغرات هو أمر ضروري لمواكبة البيئة الأمنية المتغيرة نتيجة لتطور التهديدات وكذلك تطور المنتجات والتقنيات الجديدة."

وبعبارة أخرى، المورد الذي يفشل في مواكبة تقنيات التهديد - ولا يكشف عن التهديدات - فسيواجه مخاطر التأخر عن غيره. على سبيل المثال، حدث ابتكار لأدوات إدارة الثغرات الداخلية في Cisco في مجال برامج مجمعة تابعة لجهة خارجية. البرامج التابعة لجهة خارجية هي أي كود يتم إدراجه في منتج المورد الذي لم يكتبه المورد بنفسه، وهذا يشمل عادةً البرامج التجارية التابعة للجهة الخارجية أو البرامج مفتوحة المصدر.

تستفيد Cisco من الأدوات المخصصة التي تستخدم بيانات ثغرات من Cisco IntelliShield[38] لإعلام فرق تطوير المنتجات عندما قد تؤثر مسألة أمنية تنشأ في برامج الجهة الخارجية على منتج Cisco. تعمل هذه الأداة، التي تسمى إدارة التنبيه الداخلي في Cisco على زيادة القدرة إلى حد كبير على إدارة المسائل الأمنية التي تنشأ في كود غير تابع لشركة Cisco.

المورد الذي يفشل في مواكبة تقنيات التهديد - ولا يكشف عن التهديدات - سيواجه مخاطر التأخر عن غيره.

ينبغي أن تكون ممارسات الكشف الأمني مستمرة أيضًا. في أوائل عام 2013، ستبدأ Cisco باستخدام نوع مستند جديد - ملاحظات أمان Cisco - للكشف عن مشكلات أمان المنتج ذات مستوى الخطورة المنخفضة إلى المتوسطة. سيحسن مستند ملاحظة أمان Cisco فعالية الاتصال حول المشكلات الأمنية والتي لا تعتبر خطيرة بما يكفي لضمان استشارات أمان Cisco. ستتوفر هذه الوثائق للعامة وسيتم فهرستها حسب معرف الثغرة والتعرض المشترك (CVE) لتحسين قابلية الرؤية.

لتحسين كيفية تنظيم الإبلاغ المتطور عن مشكلات الأمان بشكل أكبر، بدأ الموردون (بما فيهم Cisco) في تضمين تنسيقات إطار عمل الإبلاغ عن الثغرات المشتركة (CVRF)[39] ولغة تقييم الثغرات المفتوحة (OVAL)[40] في حالات الكشف الخاصة بهم. تساعد هذه المعايير الناشئة المستخدمين لتقييم الثغرات عبر برامج أساسية وتقنيات متعددة بثقة - وهذه المعايير قادرة على التوسع نظرًا للميزات التي توفرها الأجهزة - وذلك بتنسيق سهل القراءة. يقول سمواك، "يساعد ضمان أن عملاءنا يملكون الأدوات التي يحتاجون إليها لتقييم التهديدات التي تتعرض لها شبكاتهم بشكل صحيح على تقليل المخاطر ويتيح لهم تحديد أولويات المهام اللازمة لتأمين بنياتهم الأساسية".

في العام المقبل، للحصول على التحديثات الإضافية والتحليل المفصل بشأن الاتجاهات الأمنية، وللحصول على معلومات تتعلق بأحدث المطبوعات الخاصة بأمان المؤسسة منCisco انتقل إلى موقع الويب الخاص بالتقارير الأمنية من Cisco.
http://www.cisco.com/go/securityreport

للحصول على نظرة دائمة من خبراء Cisco على مجموعة واسعة من الموضوعات الأمنية، انتقل إلى مدونة أمان Cisco.
blogs.cisco.com/security

تطلعات الأمان لعام 2013

إن مشهد التهديد اليوم ليس مشكلة يسببها المستخدمون غير المتعلمين الذين يزورون المواقع الضارة أو أنها تُحل من خلال حظر المواقع "السيئة" المعروفة على الويب.

وقد وضح هذا التقرير كيف أصبح المهاجمون متطورين على نحو متزايد، في ملاحقة المواقع والأدوات والتطبيقات التي هي أقل احتمالاً أن يشتبه بها، ويزورها المستخدمون كثيرًا. تستطيع التهديدات الحديثة إصابة الجمهور العريض بصمت وبشكل فعال، ولا تميز بحسب الصناعة أو حجم الأعمال أو البلد. يستفيد مجرمو الإنترنت من مساحة الهجوم التي تتسع دائرتها بشكل سريع في عالم اليوم الذي يحمل شعار "الاتصالات المفتوحة" حيث يستخدم الأفراد أي جهاز للوصول إلى شبكة أعمالهم.

كبنية أساسية وطنية هامة، تواصل الشركات والأسواق المالية العالمية خطاها تجاه الخدمات القائمة علي تقنية السحابة واتصال المحمول، هناك حاجة إلى نهج متكامل ومتراكب إلى توفير الأمان لحماية المعلومات المتزايدة التي يتم الحصول عليها من الإنترنت. يقول جون ستيوارت "يستغل المتسللون ومجرمو الانترنت حقيقة أن كل مؤسسات القطاع الخاص أو القطاع العام لديها برنامج أمان لتقنية المعلومات خاص بها". "نعم، نذهب إلى المؤتمرات ونبقى على اتصال مع بعضنا البعض، ولكن نحن حقًا في حاجة للانتقال من أمان تقنية المعلومات خاصة إلى نظام قائم على تبادل المعلومات في الوقت الحقيقي والرد الجماعي".

إن بناء بنية أساسية جيدة لا يعني إنشاء هيكل أكثر تعقيدًا - في الواقع، بل على العكس تمامًا. فالأمر يتعلق بإنشاء البنية الأساسية والعناصر داخلها تعمل معًا، بذكاء أكثر للكشف و الحد من التعرض للتهديدات. مع الاتجاه السريع نحو سياسة "أحضر جهازك معك" BYOD، وحقيقة الأجهزة المتعددة لكل مستخدم ونمو الخدمات القائمة علي تقنية السحابة، انتهى عهد إدارة قدرات الأمان على كل نقطة نهاية. يقول مايكل كوفينجتون، مدير منتجات في عمليات معلومات الأمان في Cisco "من الواجب علينا اتخاذ نهج شامل للأمان يضمن مراقبتنا للتهديدات عبر جميع المتجهات، بدءًا من البريد الإلكتروني إلى الويب وحتى المستخدمين أنفسهم. "تحتاج تقنية التهديد إلى تقييم أكثر من البرامج الفردية للحصول على تصور للشبكة".

تستطيع التهديدات الحديثة إصابة الجمهور العريض بصمت وبشكل فعال، ولا تميز بحسب الصناعة أو حجم الأعمال أو البلد.

حيث إن التهديدات تستهدف على نحو متزايد المستخدمين والمنظمات من خلال توجيه هجمات متعددة، تحتاج الشركات لتجميع وتخزين ومعالجة كل نشاط شبكة على صلة بالأمان لاستيعاب أفضل لنطاق ومدى الهجمات. ويمكن أن يزداد هذا المستوى من التحليل باستخدام السياق الخاص بنشاط الشبكة لاتخاذ قرارات أمان دقيقة وفي الوقت المناسب. وحيث إن المهاجمين أصبحوا أكثر تطورًا، يجب على المؤسسات تصميم قدرات أمان في الشبكة من البداية، مع الحلول التي تجمع بين تقنية التهديد، وسياسة الأمان، والضوابط القابلة للتنفيذ في جميع نقاط التعامل على الشبكة.

بما أن المهاجمين أصبحوا أكثر تطورًا أيضًا، فيجب استخدام أدوات لإحباط جهودهم. مع توفير الشبكة نسيج مشترك للاتصال من خلال البرامج الأساسية، فسوف تمثل أيضًا وسيلة لحماية الأجهزة والخدمات والمستخدمين الذين يستخدمونها بشكل روتيني لتبادل المحتويات الحساسة. شبكة الغد هي إحدى الشبكات الذكية التي يجب أن توفر أمانًا على نحو أفضل من خلال إطار تعاوني بخلاف الإمكانية السابقة التي تعتمد على مجموع مكوناته الفردية.

شبكة الغد هي إحدى الشبكات الذكية التي يجب أن توفر أمانًا على نحو أفضل من خلال إطار تعاوني بخلاف الإمكانية السابقة التي تعتمد على مجموع مكوناته الفردية.

حول عمليات معلومات الأمان من Cisco

لقد أصبح هناك تحدٍ على نحو متزايد لإدارة وتأمين شبكات اليوم الموزعة والذكية.

دأب مجرمو الإنترنت على استغلال ثقة المستخدمين في تطبيقات العملاء وأجهزتهم، الأمر الذي يؤدي إلى زيادة تعرض المؤسسات والموظفين للمخاطر. ولا تكفي الخدمات الأمنية التقليدية، التي تعتمد على وضع المنتجات في طبقات واستخدام عدة عوامل تصفية، للتحصن ضد أحدث جيل من البرامج الضارة التي تتسم بسرعة الانتشار، ولها أهداف عالمية وتستخدم العديد من المتجهات للانتشار.

لذا تحرص Cisco على أن تنتهج نهجًا استباقيًا للتعرف على أحدث التهديدات باستخدام معلومات التهديدات في الوقت الفعلي من عمليات معلومات الأمان من Cisco. حيث تعد عمليات معلومات الأمان من Cisco نظام الأمان البيئي الأكبر المعتمد على تقنية السحابة، حيث يتم تحليل أكثر من 75 تيرابايت من البيانات المباشرة التي يتم الحصول عليها من البريد الإلكتروني الموزع الخاص بـ Cisco والويب وجدار الحماية وحلول أنظمة الحماية المتكاملة كل يوم.

تعمل عمليات معلومات الأمان في Cisco على تجميع البيانات من كل متجهات التهديدات وتحللها باستخدام كل من الخوارزميات الآلية والمعالجة اليدوية في إطار التوصل لفهم طريقة انتشار التهديدات. ثم تقوم عمليات معلومات الأمان بتصنيف التهديدات ووضع القواعد باستخدام أكثر من 200 معلمة. كما يقوم باحثو عمليات الأمان بتحليل المعلومات الخاصة بالأحداث الأمنية التي لها القدرة على التأثير واسع الانتشار على الشبكات والتطبيقات والأجهزة. ويتم تسليم القواعد بشكل حيوي إلى الأجهزة الأمنية المنتشرة من Cisco كل ثلاث
إلى خمس دقائق.

حيث تعد عمليات معلومات الأمان من Cisco نظام الأمان البيئي الأكبر المعتمد على تقنية السحابة، حيث يتم تحليل أكثر من 75 تيرابايت من البيانات المباشرة التي يتم الحصول عليها من البريد الإلكتروني الموزع الخاص بـ Cisco والويب وجدار الحماية وحلول أنظمة الحماية المتكاملة كل يوم.

كما يقوم فريق عمليات معلومات الأمان في Cisco بنشر التوصيات الخاصة بأفضل الممارسات الأمنية والإرشادات التكتيكية لإحباط التهديدات. وتلتزم Cisco بتقديم حلول أمنية كاملة تتميز بكونها حلولاً موحدة، ومناسبة وشاملة وفعالة - مما يمكّن من توفير الأمن الشامل للمؤسسات في جميع أنحاء العالم. مع Cisco، يمكن للمؤسسات توفير الوقت في البحث عن التهديدات والثغرات الأمنية والتركيز بشكل أكبر على اتخاذ نهج استباقي لتحقيق الأمان.

للحصول على معلومات حول التحذير المبكر، وتحليل التهديدات والثغرات الأمنية، وحلول التخفيف الموثقة من Cisco، يرجى زيارة: http://www.cisco.com/security.

المنهجية

يعتمد التحليل المقدم في هذا التقرير على البيانات التي تم تجميعها من مجموعة متنوعة من المصادر العالمية مجهولة المصدر، بما في ذلك البريد الإلكتروني والويب وجدار الحماية والحلول الأمنية لنظام الحماية من الاقتحام (IPS) من Cisco؛ تمثل هذه النظم الأساسية خطوط المواجهة المعنية بحماية شبكات العملاء من المحتويات الضارة والمتطفلين.

تقوم Cisco بتجميع البيانات من نشر أدوات استشعار في جميع أنحاء العالم، تلك الأدوات التي تقوم بوظائف مثل تطويق البريد غير المرغوب فيه والزحف على شبكة الإنترنت للسعي بنشاط للكشف عن حالات جديدة من البرامج الضارة.

بالإضافة إلى آليات حماية مقرات العملاء هذه، تقوم Cisco أيضًا بتجميع البيانات من نشر أدوات استشعار في جميع أنحاء العالم، تلك الأدوات التي تقوم بوظائف مثل تطويق البريد غير المرغوب فيه والزحف على شبكة الإنترنت للسعي بنشاط للكشف عن حالات جديدة من البرامج الضارة.

باستخدام هذه الأدوات والبيانات التي نقوم بتجميعها، تزود بصمة الشبكات الضخمة الخاصة بـ Cisco أنظمة عمليات معلومات الأمان والباحثين برؤية تجاه نموذج هائل للأنشطة المشروعة والضارة على الإنترنت على حد سواء. فلا يتوفر لدى موردي خدمات الأمان رؤية إجمالية لكل المواجهات الضارة. تمثل البيانات الواردة في هذا التقرير منظور Cisco حول الوضع الحالي للخصائص الرئيسية للتهديدات كما تمثل في الوقت ذاته أفضل محاولاتنا لتطبيع البيانات وعكس الاتجاهات والنماذج العالمية المستندة إلى البيانات المتوفرة في الوقت الحالي.

خدمة إدارة تنبيهات IntelliShield للأمان من Cisco

توفر خدمة إدارة تنبيهات IntelliShield للأمان من Cisco حلاً شاملاً واقتصاديًا من حيث التكلفة لتزويد المؤسسات التي تعتمد على معلومات الأمان ولا تدار بواسطة المورد باحتياجاتهم لتحديد الهجمات على تقنية المعلومات ومنعها وتخفيفها. تتيح هذه الخدمة القابلة للتخصيص والخاصة بالتنبيهات ضد الثغرات الأمنية والتهديدات المستندة إلى الويب لمتخصصي الأمان للوصول إلى المعلومات الدقيقة والموثقة في الوقت المناسب حول التهديدات والثغرات الأمنية التي قد تؤثر على بيئاتهم. كما تتيح خدمة إدارة تنبيهات IntelliShield الفرصة للمؤسسات لتقليل جهود البحث عن التهديدات والثغرات الأمنية، والتركيز أكثر على نهج استباقي لتحقيق الأمان.

توفر Cisco إصدارًا تجريبيًا مجانًا لمدة 90 يومًا لتجربة خدمة إدارة تنبيهات IntelliShield للأمان من Cisco. بتسجيل هذا الإصدار التجريبي، سيكون لك حق الوصول الكامل إلى الخدمة، بما في ذلك الأدوات وتنبيهات وجود تهديدات وثغرات أمنية.

للتعرف على المزيد حول خدمات Cisco Security IntelliShield Alert Manager، تفضل بزيارة:
https://intellishield.cisco.com/security/alertmanager/trialdo?dispatch=4.

للحصول على مزيد من المعلومات

عمليات معلومات الأمان من Cisco
www.cisco.com/security

مدونة أمان Cisco
blogs.cisco.com/security

خدمات الإدارة عن بُعد من Cisco
www.cisco.com/en/US/products/ps6192/serv_category_home

منتجات أمان Cisco
www.cisco.com/go/security

مؤسسة برامج أمان الشركات من Cisco
www.cisco.com/go/cspo

[1] "The Internet of Things"، بواسطة Michael Chui وMarkus Löffler وRoger Roberts، McKinsey Quarterly، مارس 2010: http://www.mckinseyquarterly.com/The_Internet_of_Things_2538.

[2] "Distributed Denial of Service Attacks on Financial Institutions"، Cisco Event Response: 1 أكتوبر 2012: http://www.cisco.com/web/about/security/intelligence/ERP-financial-DDoS.html.

[3] مجموعة حلول الأعمال عبر الإنترنت من Cisco.

[4] "The World Market for Internet Connected Devices—2012 Edition"، النشرة الإعلامية، بحث IMS، 4 أكتوبر، 2012: http://imsresearch.com/press-release/Internet_Connected_Devices_Approaching_10_Billion_to_exceed_28_Billion_by_2020&cat_id=210&type=LatestResearch.

[5] مجموعة حلول الأعمال عبر الإنترنت من Cisco.

[6] "Internet of Everything: It's the Connections That Matter"، بواسطة Dave Evans، مدونة Cisco، 29 نوفمبر 2012: http://blogs.cisco.com/news/internet-of-everything-its-the-connections-that-matter/.

[7] مجموعة حلول الأعمال عبر الإنترنت من Cisco.

[8] Cisco 2011 Annual Security Report, ديسمبر 2011: http://www.cisco.com/en/US/prod/collateral/vpndevc/security_annual_report_2011.pdf.

[9] "Remote Access and BYOD :Enterprises Working to Find Common Ground with Employees", 2011 Cisco Annual Security Report، ديسمبر 2011، الصفحة 10: http://www.cisco.com/en/US/prod/collateral/vpndevc/security_annual_report_2011.pdf.

[10] "Cisco Global Cloud Index: Forecast and Methodology، 2011–2016": http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns1175/Cloud_Index_White_Paper.html.

[11] Ibid

[12] "A Deep Dive Into Hyperjacking"، بواسطة Dimitri McKay, SecurityWeek، 3 فبراير 2011: http://www.securityweek.com/deep-dive-hyperjacking.

[13] "India Asks Pakistan to Investigate Root of Panic"، بواسطة Jim Yardley, The New York Times، 19 أغسطس 2012: http://www.nytimes.com/2012/08/20/world/asia/india-asks-pakistan-to-help-investigate-root-of-panic.html?_&r=1.

[14] "Twitter Rumor Sparked Oil-Price Spike"، بواسطة Nicole Friedman, WSJ.com، 6 أغسطس 2012: http://online.wsj.com/article/SB10000872396390444246904577573661207457898.html.

[15] ظهر هذا في الأصل على مدونة أمان Cisco: http://blogs.cisco.com/security/sniffing-out-social-media-disinformation/

[16] Java.com: http://www.java.com/en/about/.

[17] Frankenstein: Stitching Malware from Benign Binaries. Kevin W. Hamlen و Vishwath Mohan. In Proceedings of the USENIX Workshop on Offensive Technologies (WOOT)، الصفحات 84-77، أغسطس 2012.

[18] Mohammad M. Masud وTahseen M. Al-Khateeb وKevin W. Hamlen وJing Gao وLatifur Khan وJiawei Han و Bhavani Thuraisingham. Cloud-based Malware Detection for Evolving Data Streams. ACM Transactions on Management Information Systems (TMIS)، 2(3) أكتوبر 2011.

[19] "DDoS Attacks: Forecast 2013 ,Experts Say Recent Hits Only the Beginning"، بواسطة Tracy Kitten, BankInfoSecurity.com، 30 ديسمبر 2012: http://ffiec.bankinfosecurity.com/ddos-attacks-2013-forecast-a-5396.

[20] "Maliciously Abusing Implementation Flaws in DNS", DNS Best Practices, Network Protections and Attack Identification: Cisco.com, http://www.cisco.com/web/about/security/intelligence/dns-bcp.html#3.

[21] "IP Spoofing" بواسطة Farha Ali, Lander University، متوفر على Cisco.com: http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_10-4/104_ip-spoofing.html.

[22] "Distributed Denial of Service Attacks"، بواسطة Charalampos Patrikakis وMichalis Masikos وOlga Zouraraki و The Internet Protocol Journal ،National Technical University of Athens - المجلد 7، رقم 4. متوفر على: http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_7-4/dos_attacks.html.

[23] "DNS Tools", The Measurement Factory: http://dns.measurement-factory.com/tools.

[24] للحصول على مزيد من المعلومات حول أدوات DNS، يرجى مراجعة DNS-OARC (https://www.dns-oarc.net/oarc/tools) وThe Measurement Factory (http://dns.measurement-factory.com/tools/index.html).

[25] "Secure BIND Template Version 7.3 07 Aug 2012"، بواسطة TEAM CYMRU, cymru.com: http://www.cymru.com/Documents/secure-bind-template.html.

[26] "Response Rate Limiting in the Domain Name System (DNS RRL)", RedBarn.org: http://www.redbarn.org/dns/ratelimits.

[27] بيانات Arbor Networks' ATLAS مستمدة من "honey pots" الموزعة في إطار شبكات موردي الخدمات حول العالم; بحث البرامج الضارة ASERT; وتغذية على مدار الساعة بالبيانات مجهولة الهوية بناءً على العلاقة المتبادلة بين NetFlow، وBGP، وSNMP. ويتم تجميع البيانات مجهولة المصدر من قِبل عملاء Arbor Peakflow SP داخل ATLAS لتوفير رؤية تفصيلية للتهديدات وأنماط المرور على الإنترنت.

[28] "IPS Testing", Cisco.com: http://www.cisco.com/web/about/security/intelligence/cwilliams-ips.html.

[29] "Bank of America and New York Stock Exchange under attack unt [sic]"، Pastebin.com، 18 سبتمبر 2012: http://pastebin.com/mCHia4W5.

[30] "Phase 2 Operation Ababil", Pastebin.com، 18 سبتمبر 2012: http://pastebin.com/E4f7fmB5.

[31] "Distributed Denial of Service Attacks on Financial Institutions: Cisco Event Response": http://www.cisco.com/web/about/security/intelligence/ERP-financial-DDoS.html.

[32] Identifying and Mitigating the Distributed Denial of Service Attacks Targeting Financial Institutions Applied Mitigation Bulletin: http://tools.cisco.com/security/center/viewAMBAlert.x?alertId=27115.

[33] "Security Intelligence Operations Tactical Resources", Cisco.com: http://tools.cisco.com/security/center/intelliPapers.x?i=55.

[34] "Service Provider Security Best Practices", Cisco.com: http://tools.cisco.com/security/center/serviceProviders.x?i=76.

[35] Anagram courtesy of anagramgenius.com.

[36] Cisco Security Advisories: http://cisco.com/go/psirt.

[37] Cisco Applied Mitigation Bulletins, Cisco.com: http://tools.cisco.com/security/center/searchAIR.x.

[38] Cisco Intellishield Alert Manager Service: http://www.cisco.com/web/services/portfolio/product-technical-support/intellishield/index.html.

[39] CVRF, ICASI.com: http://www.icasi.org/cvrf.

[40] OVAL, Oval International: http://oval.mitre.org/.