سان خوان - كيف يعمل ذلك: فهم إساءة استخدام نظام DNS
الاثنين، الموافق 12 مارس 2018 – من الساعة 01:30 م إلى الساعة 03:00 م بتوقيت المحيط الأطلنطي
اجتماع ICANN61 | سان خوان، بورتوريكو

شخص غير محدد: طاب مساؤكم. اجتماع ICANN61. 12 مارس. كيف يعمل ذلك: فهم إساءة استخدام نظام DNS.

كاثي بيترسين: طاب مساؤكم جميعا. سنبدأ بعد قليل جلسة كيف يعمل ذلك: فهم إساءة استخدام نظام DNS في غضون دقيقتين. شكرا لكم.

طاب مساؤكم جميعا مرة أخرى. مرحبا بكم في جلسة كيف يعمل ذلك حول فهم إساءة استخدام نظام DNS. ومعنا كارلوس ألفاريز من مكتب CTO الذي يقدم هذه الجلسة. كارلوس؟

كارلوس ألفاريز: شكرا جزيلا لك، كاثي. وشكرا لجميع الموجودين هنا في القاعة. ولدي أيضا عدد لا بأس به من المشاركين عبر الإنترنت. وأدرك أن العدد يبلغ 23 شخص، وربما سيزيد العدد أثناء مضينا قدما خلال الجلسة.

سنتحدث عن موضوع مهم جدا. وهو وثيق الصلة للغاية. كما أنه مثير للجدل أيضا في بعض النواحي وهو موضوع يتطلب إيلاء الأشخاص اهتمام له. فإننا سنتحدث عن إساءة استخدام نظام DNS.

في البداية، سنضع بعض جوانب للمناقشة. وهناك جوانب مختلفة. حيث يدرك الأشخاص إساءة استخدام نظام DNS من زوايا مختلفة. وسنضع بعضا من هذه الزوايا هنا، ثم سنتناول بعض الأمثلة على إساءة استخدام نظام DNA أو سوء الاستخدام. وسنتحدث

قليلا عن مشهد الإنترنت المتطور فيما يتعلق بنظام DNS. وبعد ذلك، سننتهي بالحديث قليلا عن إساءة استخدام نظام DNS داخل إطار ICANN.

إن أول ما يستحق الإشارة إليه هو أنه لا يوجد تعريف موحد ومقبول عالميا لما تعنيه إساءة استخدام نظام DNS. حيث تذكر الشريحة التي تظهر أمامكم أن هناك تعريفات [متنوعة] تتضمن موضوعات مؤيدة مثل الجرائم الإلكترونية والاختراق والسلوك الضار.

يمكنكم النظر إلى إساءة استخدام نظام DNS على أنها تنقسم إلى ثلاث فئات. ويمكن أن تكون هذه الفئات تلف البيانات أو حجب الخدمات أو الخصوصية. وهناك بالطبع اختلاف بين سوء استخدام نظام DNS مقابل إساءة استخدام نظام DNS. وسأقرأ عليكم بعضا مما تذكره هذه الشريحة. يشير سوء الاستخدام إلى الأنشطة المخادعة أو التآمرية أو غير اللازمة المتعمدة والتي تستغل نظام DNS بنشاط أو الإجراءات المستخدمة لمسح أسماء النطاقات أو حلها. وسنرى ما المقصود من ذلك. وسنرى ذلك لاحقا.

ما الذي ذكرته اللجنة الاستشارية الحكومية في سعيها للوصول إلى تعريف أو تقديم العناصر لإدراك المقصود من إساءة استخدام نظام DNS؟ ما الذي ذكرته اللجنة الاستشارية الحكومية بخصوص هذا الجانب الفضفاض؟ قدمت اللجنة الاستشارية الحكومية في بيانها الضمانات التي نطبقها على جميع برامج gTLD الجديدة في مقتطفات من المستند الذي يتعلق بالتخفيف من الأنشطة المسيئة. وأشارت إلى بعض الأنشطة المسيئة مثل نشر البرمجيات الضارة أو تشغيل شبكات البوتنت أو التصيد أو القرصنة أو انتهاك العلامات التجارية وحقوق الطبع والنشر أو الممارسات الاحتيالية أو الخادعة أو التزييف والأنواع الأخرى من الأنشطة التي قد تخالف القانون المعمول به.

يبدو ذلك فضفاضا، ويرى البعض أنه توجد بعض الموضوعات المدرجة والتي قد لا تكون بالضرورة إساءة استخدام فنية لنظام DNS بوصفه نظاما فنيا. ولكن كما قلت، فإننا نقدم حاليا بعض تلك الآراء الموجودة في المجتمع. وهذه هي إحدى الآراء. وهناك جانب آخر لا ينظر إلى انتهاك العلامات التجارية وحقوق الطبع والنشر، وفي بعض

الحالات، الممارسات الاحتيالية أو الخادعة على أنها من المسائل الفنية المتعلقة بنظام DNS على هذا النحو لأسباب عديدة.

هناك سؤال مهم - سأتركه كسؤال مفتوح أثناء هذه الجلسة - بخصوص ما إذا كانت الرسائل غير المرغوب فيها تعد إساءة لاستخدام نظام DNS أو ينبغي النظر إليها على أنها كذلك.

بالنسبة لجانب المجتمع التشغيلي والأمني وإنفاذ القانون، ينظر إلى الرسائل غير المرغوب فيها على أنها مؤشر وأحد الأنواع السابقة الأخرى من الأنشطة الضارة. في حد ذاته، وحتى يومنا هذا على الأقل، لم ينظر إليها على أنها إساءة استخدام فنية، على هذا النحو، بالنسبة لنظام اسم النطاق العالمي.

عند قيامك بإجراء البحث عن تهديد وتحليل البيانات وترى إطلاق حملة للرسائل غير المرغوب فيها للتو، فإنك تحدد البنية الأساسية الجنائية التي يستغلها العناصر السيئة لهذه الحملة. وإذا لم تكف عن متابعة نشاطهم، فإنك عاجلا أو آجلا - في الغالب عاجلا وليس آجلا - سترى نشاط المتابعة الذي تتابعه بالضبط بعد إرسال الرسائل غير المرغوب فيها. ويمكن أن يكون ذلك نشرا للبرمجيات الضارة. أو يكون نشرا لمواد مسيئة للأطفال. أو يكون تصيدا - أو أنواعا أخرى من هذا القبيل. وبعبارات أبسط، تشير إساءة استخدام نظام DNS إلى أي شيء يهاجم أو يسيء استخدام البنية الأساسية لنظام DNS. وسنرى ذلك في بعض الشرائح الموجودة معي.

توجد العديد من الطرق لمعرفة إساءة استخدام نظام DNS. وسنتحدث عن طريقتين، لذلك ضع هذا الموضوع في الشريحة. أحدهما هو منظور إساءة استخدام حل أسماء النطاقات، وهو الجزء الفني لكيفية ترجمة أسماء النطاقات إلى عناوين IP. والمنظور الآخر الذي سنتحدث عنه سيكون تسجيل أسماء النطاقات، وهو فحص خدمات التسجيل.

يتم إساءة استخدام تلك الخدمات التي تقدمها السجلات وأمناء السجلات من قبل المجرمين بطرق مختلفة. وسنتحدث عن ذلك أيضا.

يشير سوء استخدام نظام DNS إلى استغلال بروتوكول DNS على مستوى فني أكثر أو عمليات تسجيل لأغراض ضارة. وسنقدم أمثلة لكل ذلك بمزيد من التفصيل ما دامت هذه تعمل. [التي أشير إليها] - نعم. هناك.

عذرا. لستم بحاجة إلى قراءة كل تلك الشرائح. فهذا ليس الهدف. والهدف من ذلك يكمن في عرض العناصر التشغيلية لنظام DNS على نطاق مبسط.

أمامكم، في الجزء العلوي كلمة مكتوبة بالخط الأزرق، خوادم الأسماء الرسمية التي تستضيف البيانات الرسمية لكل اسم نطاق أو لكل نطاق مستوى أعلى، لهذه المسألة. وفي الأسفل، أمامكم محللو الاسم المتكرر، والذي يمكنكم رؤيتهم كخوادم نظام DNS التي يسمح لك مزود خدمة الإنترنت - الشركة التي توفر لك الوصول إلى الإنترنت - باستخدامها. فهي توفر لك خدمة حل نظام DNS.

ثم لدينا العميل أو محللو التعليمات البرمجية. وما المقصود من محلل التعليمات البرمجية؟ إنها هنا. إنها وظيفة داخل مستعرض الويب، على سبيل المثال، تبحث عن المعلومات التي تحتاجها لتكون قادرة على استخدام الموارد التي أرغب في استخدامها.

على سبيل المثال، إذا ذهبت إلى مستعرض الويب وكتبت www.ICANN.org، ستظهر وظيفة محلل التعليمات البرمجية وستحل اسم النطاق في عنوان IP، حيث سيتم استضافة محتوى www.ICANN.org. وستقوم بتنزيله على جهازي وسوف أتمكن من رؤيتها والتفاعل معها، وما إلى ذلك.

تعد هذه العناصر التشغيلية الثلاثة لنظام DNS أهدافا للهجمات. وفي الأساس، سنرى أن كل ما هو متصل بالإنترنت يمثل هدفا لهجوم ما.

أمثلة: من هنا يصبح الأمر مثيرا للاهتمام. ودعونا نركز على الانعكاس/التضخيم، والذي يكون في صميم هجمات التعطيل المنتشر للخدمة (حجب الخدمات الموزع).

ما المقصود من الانعكاس؟ يقصد من الانعكاس أنه يمكنك إرسال حزمة وتقوم بتزييف المعلومات حول عنوان IP المصدر حتى يعتقد الخادم أنه قد تم إرساله من قبل شخص

آخر، مما سيجعل هذا الخادم يقوم بإرسال الرد إلى عنوان IP الآخر. ولذا، إذا كان هدفي هو مهاجمة كاثي، سأرسل الحزمة إلى خادم نظام DNS، وسيقول عنوان IP الذي سأوجهه إلى الحزمة إن الحزمة نفسها قادمة من كاثي، وليس مني.

إذا قمت بذلك باستخدام ما يسمى محللو الفتح، وهي خوادم نظام DNS موجودة - يوجد الآلاف منها - لا تقوم باستخراج عناوين IP التي تأتي منها الاستفسارات والرد على الاستفسارات من أي مستخدم من أي منطقة في العالم، سينهمر كل ذلك على كاثي لأنني سأرسل استفسارات نظام DNS إلى الآلاف من محللي الفتح الموجودون في العالم. وجميعهم سيعتقدون أن كاثي أرسلت كل هذه الاستفسارات، ولذلك فإنهم سيردون عليها. وهذا هو المقصود من الانعكاس.

المتجه الآخر هو التضخيم. ما المقصود من التضخيم؟ يقصد منه حصولك على تلك الاستفسارات التي أرسلها - فهي صغيرة للغاية. وعادة ما تكون فقط سطر الأوامر. ويمكن أن يكون هذا السطر بسيطا مثل البحث عن اسم نطاق خادم الأسماء بأداة البحث dig. وتكون المفاجأة. يكون الأمر قد انتهى. فحجمه سبعة بايت، ربما. وهو صغير حقا. فهو مجرد سطر نصي، في حين سيكون ردهم ضخما. حيث يمكن أن يكون 2.3 أو 2.5 أو 2.7 ميغابايت. واضرب ذلك بآلاف الاستفسارات التي أجعل شبكات البوتنت تقوم بإرسالها. وهل تتذكرون شبكات البوتنت، تلك الشبكات الضخمة من الأجهزة المخترقة التي يشغلها المجرمون؟ يمكن أن يكون لديهم مئات الآلاف من الأجهزة المخترقة. ويمكن للمجرم الذي يستخدم شبكة البوتنت أن يجعل كل هذه الأجهزة المخترقة تقوم بإرسال استفسارات إلى جميع محللي الفتح الموجودون، وإرسال تلك الردود لكاثي.

إنه تأثير مضاعف بسبب عدد الأجهزة المخترقة التي قمت بتوظيفها والتي تعد جزءا من شبكة البوتنت الخاصة بي ومن ثم هناك الآلاف من محللي الفتح الذين أقوم بتفعيلهم وطريقة إرسال أمر - استفسار بأداة البحث dig. وأداة البحث Dig عبارة عن أمر يسمح لك بالحصول على معلومات من نظام DNS. فهو يطلق ردا. والطريقة التي يصيغون بها ذلك الأمر هي أن ردها يكون ضخما، كما ذكرت للتو.

لذا، فإنه من المرجح جدا اختراق كاثي وهي في وضع عدم الاتصال بالإنترنت إذا لم تكن على نوع من خدمات الحماية من التعطيل المنتشر للخدمة أو what-have-you. وإذا لم تستطع تحمل كثرة المرور الذي سيأتي إليها، فإنها ستتحول إلى وضع عدم الاتصال بالإنترنت. ولا توجد وسيلة لمنع ذلك.

كان أول هجوم كبير للتعطيل المنتشر للخدمة [غير مسموع] الذي تمت مشاهدته باستخدام نظام DNS كمتجه للهجوم في عام 2003 ضد Spamhaus. وSpamhaus هي مؤسسة لا تركز على الرسائل غير المرغوب فيها فحسب، بل وعلى البرمجيات الضارة، وما إلى ذلك، وتجري التحقيقات. فهي توفر تاريخا مثيرا للاهتمام للتخفيف والحماية من التهديدات وما إلى ذلك.

وبالطبع، تستمر الهجمات في المشاركة. والآن، بالطبع، لا يعد نظام DNS متجه الهجوم الوحيد على أي حال. فهو أحدهم، ولكن كبروتوكول، يتم استغلاله في كثير من الأحيان.

سنتناول أيضا هجمات إفساد الذاكرة المؤقتة أو الاستنفاد. وذلك وارد في الشريحة الثانية إلى الأخيرة. وسنتحدث أيضا عن آخر هجوم تصنت لنظام DNS بعد عدة شرائح.

هذا بالأساس ما قمت بوصفه للتو. فهذا هجوم كبير للتعطيل المنتشر للخدمة يستخدم أسلوب الانعكاس، حيث يقوم بإرسال الحزم التي تقوم بتزييف عنوان IP الخاص بالمصدر، مما يجعل جميع محللو الفتح يعتقدون أن جهاز كاثي هو الذي يرسل الاستفسارات. ومن ثم يجعلهم الاستفسار الذي استلموه يرد ردا ضخما. وهذا هو متجه التضخيم. وينهمر كل ذلك على كاثي. وهذا بالضبط ما قمت بوصفه للتو.

لم أقصد نفسي. عند حديثي عن التغلب على نفسي. فلقد احتسيت الكثير من القهوة. أين وصلنا؟

هنا. ويوجد طريقة أخرى يمكنك من خلالها مهاجمة نظام DNS عن طريق الذهاب إلى خوادم أسماء شخص ما. ويعد خادم الأسماء جزءا من البنية الأساسية المستخدمة لتوفير الحل لاسم النطاق. ولذا إذا قمت بمحو carlos.whatever، سأضطر إلى تعيين

خادمين على الأقل لأن نظام DNS هو نظام عالمي يحصل على معلومات حول الموارد التي قمت بربطها بهذا الاسم. وبعبارة أخرى، سأقوم بتحديد وإتاحة تلك المعلومات لخوادم الأسماء - عناوين IP؛ ويمكننا القول ببساطة شديدة، في مكان خادم البريد ومكان خادم الويب ومكان خادم بروتوكول نقل الملفات، وما إلى ذلك.

لذلك، إذا قام أي شخص باختراق خوادم الأسماء الخاصة بي في وضع عدم الاتصال بالإنترنت، لن يتمكن أحد من الوصول إلى تلك المعلومات، وهو ما يعني بأنني لن أقوم بإستلام أي بريد إلكتروني أو أرسله. ولن يتمكن الأشخاص من الوصول إلى موقع الويب الخاص بي، وما إلى ذلك، وقد يكون لذلك عواقب إذا كان اسم نطاق عالي القيمة. ولا يعني ذلك أن carlos.whatever هدف ذات قيمة عالية. ومن المحتمل عدم وجوده، لكنه قد يكون موجود.

الطريقة التي يعمل بها - هذا النوع من الهجوم - هي أن المجرمين يسيئون استخدام بروتوكول التحكم في نقل البيانات (TCP). فعند إرسال حزمة TCP إلى خادم، يقوم الخادم بالرد. وأطرح ذلك مرة أخرى ببساطة شديدة. فعندما يرد الخادم على اتصال TCP، ينشئ كل من الجهاز الذي بدأ الاتصال والخادم الذي رد على الاتصال مصافحة، مما يؤدي إلى إنشاء قناة اتصال يحتفظ بها كليهما. ويعني ذلك أنه يتعين على كل منهما تخصيص موارد معينة للحفاظ على قناة الاتصال تلك.

لذا، إذا كان لديك الكثير من الأجهزة المخترقة في شبكة بوتنت وجعلتهم يرسلون ردود/استفسارات إلى خادم أسماء بطريقة ستجبر ذلك الخادم على إنشاء عدد كبير جدا من مصافحات TCP بحيث يتعين عليه تخصيص موارد للحفاظ على تلك القنوات القائمة للاتصالات عبر TCP، فإنك ستصل قريبا إلى مرحلة لن يتوفر فيها أي موارد لهذا الخادم بعد الآن لتخصيص أي اتصالات TCP أخرى، مما يعني أنه لن يتمكن أي شخص آخر من الطلب من ذلك الخادم الحصول على معلومات نظام DNS. وسيظل متاحا عبر الإنترنت، ولكنه لن يتمكن من الرد على أي استفسار. وكما تذكر الشريحة، فإن حل الاسم يكون متدهور أو متقطع.

إذا كنت محظوظا، ستتمكن من الحصول على رد بعد بضع دقائق. واضرب ذلك بآلاف المرات إذا كان اسم نطاق عالي المرور أو قد تفقد الحل. وهذا هو السيناريو الأسوأ الذي يريد الجميع تجنبه.

إفساد الذاكرة المؤقتة. إن ذلك أمر مخادع. ويعني ذلك وجود أشرار مبدعين، كما هم دائما - حسنا، في بعض الأحيان. وأحيانا يتم ذلك حقا. وهل تذكرون أننا أشرنا في شريحة سابقة موجودة في الأعلى أنه كان لدينا خوادم أسماء رسمية - مثل ما إذا كنت قد أنشأت carlos.whatever، وربطتهم بـ ns1.carlos.whatever وسجلت ns2.carlos.whatever لتوفير المعلومات المتعلقة بخادم البريد وخادم الويب، وما إلى ذلك إلى نظام DNS؟ فتلك هي خوادم الأسماء الرسمية.

يكون كل مزود خدمة إنترنت - وهم متواجدون بكثرة؛ 9.9.9.9 أو 8.8.8.8 أو OpenDNS أو UltraDNS؛ هناك العديد من مزودي نظام DNS - متكررون، مما يعني أنهم يطرحون الأسئلة نيابة عن شخص آخر. ولا يتمتع بعض هؤلاء المحللون المتكررون، كما يشار إليهم، بحماية جيدة. فهم ضعفاء. وإذا كنتم تتخيلون جميع الآلاف من مزودي خدمات الإنترنت الموجودين في جميع المناطق، ستجدون أن بعضها يتم تشغيله من قبل شركات صغيرة ليس لديها الكثير من الموارد. ولذلك لديهم البنية الأساسية للتشغيل، لكن قد لا تتوفر لديهم الموارد اللازمة لحمايتها.

عندما لا تتوفر الحماية الكافية لهذه الخوادم، قد يخترقها المجرمون بطرق مختلفة، وأحد تلك الطرق يمكن أن يعني أنه إذا كنت مستخدما لمزود خدمة إنترنت لديه محلل متكرر مخترق وأرسلت استفسارا يبحث عن البيانات المرتبطة بـ what-have-you – PayPal.com – قد أحصل على الرد الصحيح، ولكن لأن الخادم لا يزال مخترقا، سيضيف المجرمون بعض المعلومات الإضافية هناك. وسيكون هذا الجزء البسيط من المعلومات مثل القول، "أوه، بالمناسبة، إن عنوان IP الخاص بـ BankOfAmerica.com هو ذلك."

وستقوم تلقائيا بتحديث ذاكرة جهازي المؤقتة. وفي رأيي، سيكون ذلك ملف المضيف. وعندما يحدث ذلك، خمن إلى أين سيأخذني جهازي في المرة القادمة التي أرغب فيها في زيارة موقع BankOfAmerica.com؟ وإذا حدث ذلك خلال فترة زمنية محددة، سيأخذني إلى عنوان IP الذي يريدني المجرمون زيارته. وهذا هو السيناريو السيئ. وهذا ليس رائعا.

ما الذي سيحدث حينها؟ سأزور خادم المجرم المشغل. وسأرى المحتوى الذي يريدون مني أن أراه، والذي سيكون في هذه الحالة موقعا للتصيد يحاكي بنك أوف أمريكا. ثم سأقدم لهم بكل سرور اسم المستخدم وكلمة المرور الخاصة بي، وهو أمر ليس جيدا لأموري المالية الشخصية، بالطبع.

توجد طرق أخرى يستطيع من خلالها المجرمون القيام بأمور مثل هذه. حيث يمكنهم اختراق جهازك بشكل مباشر وتغيير/تعديل تكوين نظام DNS الخاص بك. وسنرى مثالا لاحقا على شبكة بوتنت سيئة تم إزالتها قبل أربع سنوات، على ما أعتقد. وإذا تم تكوين جهازي لإرسال استفسارات نظام DNS، على سبيل المثال 1.1.1.1، فإنهم يغيرون عنوان IP الموجود هنا أو على الكمبيوتر المحمول، وبدلا من عنوان IP المخصص للمستخدم، فإنهم يضعون عناوينهم الخاصة. فهم يضعون عنوان IP لخادم نظام DNS الذي يشغلونه وتمت تهيئته لتوفير عناوين IP للبنية الأساسية الخاصة بهم. وبعبارة أخرى، سيجعلون جميع المستخدمين الذين تم اختراق أجهزتهم زيارة مواقع الويب الخاصة بهم، وهو مجددا أمر ليس رائعا. وسنتحدث عن هذا بعد قليل.

في حالة كهذه، عند التحدث تحديدا عن إفساد الذاكرة المؤقتة بالطريقة التي يتبعونها، فإنهم يجعلون جهاز المستخدم المخترق يقوم بإرسال الاستفسارات إلى خادم نظام DNS الخاص بهم. ولنفترض أنني أطلب موقع غير ذي صلة بالمجرمين - موقع جديد (على الرغم من أن أي شيء يمكن أن يكون ذا صلة بهم). ولنفترض أن news.whatever ليس موقع ذا صلة بالمجرمين. ومثلما هو الحال مع المثال السابق الذي قدمته، فإنهم يضيفون جزءا بسيطا من المعلومات إلى ذلك الرد الذي يرسله خادمهم إلى جهازي. ويمكن أن يكون هذا الجزء البسيط من المعلومات مماثلا لعنوان IP - أوه، بالمناسبة، إن

عنوان IP الخاص بموقع البنك الذي تتعامل معه هو ذلك. ولذلك، مرة أخرى، وخلال فترة زمنية محددة، أستفسر عن اسم نطاق البنك الذي أتعامل معه لأنني أريد الدخول إلى بعض الخدمات البنكية المتاحة عبر الإنترنت، و-فجأة! - ينتهي بي الحال في موقع المجرم. ومرة أخرى، فهذا أمر سيئ لأموري المالية الشخصية.

إن DNSChanger هو بالضبط نوع البرمجيات الضارة التي كنت أشير إليها. وهذا بالضبط ما قام به. لقد غير تكوين نظام DNS المخصص للمستخدم. وهو منتشر للغاية. وكان المجرمون الذين قاموا بتوجيه شبكة البوتنت هذه - العقل المدبر وراء هذه العملية - قادرين على كسب الكثير من المال. وفي الوقت الذي تمت فيه عملية إنفاذ القانون، تمكنت جهات إنفاذ القانون من الإثبات بأدلة دامغة على أنهم حصلوا بصورة غير قانونية على مبلغ 25 مليون يورو. وهذا لا يعني أنهم لم يحققوا أكثر من ذلك. بل يعني أن ذلك فقط هو ما تمكنت جهات إنفاذ القانون إثباته بأدلة فعلية.

باستخدام DNSChanger، يقوم المجرمون بتغيير تكوين نظام DNS على أجهزة المستخدمين. ولقد فعلوا شيئا يبدو غير ضار جدا حيث أنهم كانوا يستبدلون الإعلانات التي قد يشاهدها المستخدمون عندما ينتقلون إلى مواقع الويب. فإذا دخلت إلى الموقع الإخباري المفضل في الصباح وأنا أحتسي كوب القهوة في مكتبي، فبدلا من مشاهدة الإعلانات المشروعة، أشاهد إعلاناتهم التي استبدلونها. وقد ولدت دخلا لهم على أساس مستمر. وحدث ذلك لوقت طويل جدا. فهذه آلة نقود.

إن ذلك غير ضار، أو هكذا يبدو. حيث لم يشاهد المستخدمون أي سلوكيات غريبة في أجهزتهم. وكانوا لا يزالون قادرين على الوصول إلى المحتوى الذي يريدون الوصول إليه. وكانوا لا يزالون قادرين على التفاعل مع الإنترنت والموارد التي يريدونها. ولذلك، لم يكن هناك شيء غريب يحدث على ما يبدو.

حسنا، كان هناك شيء غريب. لذلك تم اتخاذ الإجراء، وكان هناك قلق لأن هناك الكثير من الأجهزة المصابة. ولا أتذكر الحجم الدقيق للأجهزة، ولكن كان هناك مئات الآلاف من الأجهزة التي تم اختراقها ضمن شبكة البوتنت هذه بهذا النوع من البرمجيات الضارة

في عدد من البلدان. ولا أريد الكذب - ربما كان ذلك في حوالي 20 بلدا. ولكنني لست متأكدا.

لذا، جاء السؤال عندما كانوا - أقصد "بكانوا" - جهات إنفاذ القانون - على وشك القيام بشيء ما مع خوادم نظام DNS التي يشغلها المجرمون. فإما أن يتمكنوا من إيقاف تشغيلها، وفي هذه الحالة - ما الذي تعتقدون أنه قد يحدث لو أنهم قاموا بإيقاف تشغيل خوادم نظام DNS؟ إذا كانت جميع أجهزة المستخدم ترسل استفسارات نظام DNS إلى تلك الخوادم، ماذا كان سيحدث؟

كان المستخدمون سيعتقدون أنهم فقدوا الاتصال بالإنترنت. وسيزالون مرتبطين بالإنترنت، ولكن لن تعمل أجهزتهم على حل أي اسم لأن خوادم نظام DNS كانت متوقفة. ولا يمكنهم مجرد إيقاف تشغيلها.

يمكننا القول إنهم تمكنوا من استبدال تلك الخوادم باستخدام الهندسة. وعينت المحكمة مسؤولا لهذه الخوادم خلال فترة من الزمن من خلال الشهادات [الوطنية] والتقنيات المختلفة. ونفذت حملات التوعية في جميع الولايات القضائية بحيث أدرك المستخدمون ضرورة تنظيف أجهزتهم.

بالطبع، منذ ذلك الحين، المجرمون هم المجرمون. فقد وجدوا العديد من الطرق المختلفة لإساءة استخدام بروتوكول نظام DNS والعناصر التشغيلية المختلفة لنظام DNS، وبعضها مثير للاهتمام، على الأقل من منظور أكاديمي، لأنها تظهر إبداعا - للأغراض السيئة ولكنها إبداعية، مثل قناة استخراج سرية. وأعتقد أن ذلك في الشريحة التالية - لا. دعونا نتحدث عن ذلك.

بالطبع، عندما تكون قادرا على إرسال البيانات من شبكة مخترقة دون أن يدرك مسؤول الشبكة تعرض بياناتهم للسرقة، فهذا هو الجزء السري. ويعتبر نظام DNS قناة استخراج سرية مثيرة للاهتمام لأن المنفذ الصغير المستخدم في اتصالات نظام DNS عادة ما يكون غير محظور. ولا يمكن حظره.

ينتقل المرور الموجود في الشبكة عبر منافذ، من منفذ إلى آخر. والمنفذ الذي يستخدمه بروتوكول نظام DNS هو المنفذ رقم 53. وفي حين توجد طرق يمكن للمهندسين إعادة تعيين ذلك المنفذ داخليا داخل شبكتهم، إلا أنه قد توجد بعض التعقيدات. ولذلك لا يتم إعادة تعيينها أو نقلها إلى منفذ آخر. وهذا يعني أنه لا يمكن حظر المرور عبر المنفذ رقم 53. ومن الصعب جدا إعادة تعيينها، لذا لا يمكن حظرها ببساطة. وإذا تم حظرها، لن يحصل الأشخاص على حل نظام DNS، مما يعني أنهم يعتقدون أنهم بخير.

كيف تسير الأمور عندما يكون لديكم قناة استخراج سرية؟ هناك طرق مختلفة - وأفكر في طريقتين على الأقل الآن. وبإحدى هذه الطرق، يمكنك اختراق الجهاز وجعل هذا الجهاز يبدأ في إرسال استفسارات نظام DNS ببطء إلى خادم أسماء المجرم. والمسألة هي أنه، ضمن كل استفسار من استفسارات نظام DNS، قام المجرمون باستبدال البتات الأقل صلة بالبتات التي تتوافق مع البيانات التي يقومون باستخراجها. وإذا نظر الفريق الهندسي أو مسؤول الشبكة إلى تلك الاستفسارات وإلى المرور، سيظل يقول فقط إنها استفسارات نظام DNS. وسيكون عليهم جمع كل استفسارات نظام DNS التي يتم استخدامها لاستخراج جزء محدد من البيانات. ويحتاج ذلك إلى إجراء تحليل، في الأساس. ولتدرك أن البتات الأقل صلة قد تم تعديلها، وقم بتجميع تلك البتات الأقل صلة سويا، وحاول أن تستفيد منها، ثم أدرك ما كان يتم استخراجه. وتلك إحدى الطرق.

هناك طريقة أخرى يستخدم فيها المجرمون نظام DNS لاستخراج المعلومات، وهي أسهل قليلا، من خلال سجلات TXT. وعند إنشاء اسم نطاق، ستقوم بشكل افتراضي بتنظيم وإدارة ما يسمى بملف المنطقة.

في ملف المنطقة لاسم نطاقك، يمكنك تحديد الموارد المرتبطة به. وهذا هو المكان الذي تقوم فيه بإدراج المعلومات الخاصة بموقع الويب وخادم البريد وخادم FTP. إذا كان النطاق موقعا بالامتدادات الأمنية لنظام اسم النطاق، فإن هذه المعلومات ستمر إلى هناك. وإذا كان لديك جميع التقنيات لحماية عملائك أو عامة الناس - لا أعرف، ربما سمع بعضكم عن ذلك. ويمكننا القول ببساطة إنها مجرد مزيد من الاختصارات، للأسف - SPF وDKIM وDMARC - والتي تحمي المستخدمين ببساطة.

تمر كل هذه الأنواع من المعلومات إلى ما يعرف باسم سجلات TXT. ويمكنكم بالفعل وضع أي شيء في سجل TXT. ولا توجد قيود على نوع النص الذي يمكن أن ينتقل إلى سجل TXT. فهو مجرد نص. ويستخدم المجرمون سجلات TXT هذه لاستخراج معلومات مفيدة أيضا. ويمكنهم إرسال استفسارات بأداة البحث dig مع معلومات تتعلق بسجلات TXT لخادم الأسماء الذي يقوم بعد ذلك بجمع المعلومات وتجميعها وإعادة إنشاء البيانات التي تم استخراجها وما إلى ذلك.

التدفق السريع. أعتقد أنه تم الإشارة إلى ذلك من قبل. وإذا لم يكن الأمر كذلك، سنعود إليه، لكنني أعتقد أنه تم الإشارة إليه.

تعد تسجيلات أسماء النطاقات أهدافا رائعة للمهاجمين. وهذا واضح جدا. وللأسف، يعمد المجرمون والعناصر الضارة إلى إساءة استخدام مزودي خدمات تسجيل النطاق في مساحات برنامج gTLD ونطاق المستوى الأعلى لرمز البلد. فهم يحبون إساءة استخدام أمناء السجلات والموزعين. كما أنهم يحبون الحصول على كميات كبيرة من أسماء النطاقات. وهي مشكلة معقدة للغاية يجب معالجتها. وأعتقد أن انخفاض أسعار أسماء النطاقات يغري العناصر السيئة، وهذه هي الطبيعة البشرية. فالسعر الأقل يكون الأفضل، لذلك فهم يتقدمون ويسجلون المزيد من أسماء النطاقات، مثلما يتم إغراء المشتركين والمستخدمين الشرعيين في تسجيل الأسماء عندما يكون سعرها أقل. ومرة أخرى، كما سبق لي القول، فهذه هي الطبيعة البشرية. ولا يوجد شيء خاطئ في ذلك. فهذه هي الطريقة التي تسير بها الأمور.

ينشأ التسجيل الآلي لأسماء النطاقات - وهو ليس أمرا جيدا ولا سيئا مرة أخرى. فهذه هي طريقة اشتراك المجال. فهو بالطبع يسمح بتشغيل المحافظ الكبيرة من أسماء النطاقات الشرعية.

لكن بعد ذلك، كان المجرمون يتواجدون هناك ويسيئون استخدامها، للأسف. وعندما أذكر ذلك، فإنني أفكر في نطاقات DGA، التي تعد في الأساس الأتمتة الموجودة لدى المجرمين لتساعدهم في إنشاء كميات كبيرة من أسماء النطاقات أو التسجيل فيها.

ما المقصود من DGA؟ يقصد منها خوارزمية إنشاء النطاق. وتخيلوا معي شبكة البوتنت. فيجب أن يكون لكل شبكة بوتنت بنية أساسية للقيادة والتحكم يستخدمها المجرمون لكي يتمكنوا من قيادة بنيتهم الأساسية الضارة والتحكم فيها بدقة.

لكن ماذا يحدث إذا تم إزالة هذه البنية الأساسية؟ حسنا، سيكون هناك الخطة ب، ج، د، هـ، و، ز، وهكذا. وهذا هو غرض وجود نطاقات DGA. فعندما تدرك شبكة البوتنت تعطل أحد هذه الخوادم المرتبطة بالقيادة والتحكم أو تم تعليقه أو لم يتم تعريفه أو مهما كان، حسنا - تكون المفاجأة! - يقوم بالتسجيل. وهذا مجرد مثال. حيث توجد جميع الألوان والنكهات والاختلافات في سلوك DGA. وهذا مجرد تفسير مبسط. تكون المفاجأة! يقوم [بتسجيل] أي سلسلة تحت أي نطاق مستوى أعلى، ويتم إيقاف تشغيله.

في حال تدهورت قدرات قيادة وتحكم شبكة البوتنت بسبب إجراء التخفيف من التهديد، هل من الممكن تسجيل سلسلة DGA الجديدة هذه؟ تكون المفاجأة! يحدث الأمر مجددا. لقد فقدوا القدرة على القيادة والتحكم واستمروا في عملهم.

سنذكر حالة مثيرة جدا للاهتمام. وأرجو أن نكون بالقرب من هذه الشريحة. لماذا يقوم المهاجمون والمجرمون بتسجيل أسماء نطاقات لكل شيء؟ أي شيء يمكنكم التفكير فيه - فهم يقومون بالتسجيل للتصيد وبرمجيات الدفع القسري للفدية ونشر البرمجيات الضارة والحيل والبضائع المزيفة والمنتجات الصيدلانية غير القانونية - وغير ذلك الكثير.

السطر الأخير - لا أعرف سبب ظهوره على هذا النحو - هو القيادة والتحكم، وهو ما يتعلق بالاستقرار والمرونة. وهذا هو مصدر القلق الأكبر بسبب حجم الهجمات.

تثار الأسئلة أحيانا عن المنتجات الصيدلانية غير القانونية - سواء ينبغي اعتبار ذلك إساءة استخدام نظام DNS أم لا، عندما يكون من الواضح أنه ليس مرتبطا بإساءة استخدام نظام DNS - من الناحية الفنية، على الأقل. فالأمر مماثل أكثر للتزوير - بيع مواقع الويب، وما إلى ذلك. وهذا صحيح، ولكن هناك أحيانا أشياء مستترة وراء ما هو ظاهر على السطح. ولا يمكنني الخوض في التفاصيل، ولكن ضعوا في اعتباركم أن هناك أشياء مستترة وراء ما تشاهدونه بأعينكم على السطح. فقد ترون أنها مجرد مجموعة

من مواقع الويب التي يتم استخدامها لإرسال الأدوية غير القانونية في بعض الولايات القضائية. ولكن ما يوجد وراء ذلك أشياء تؤذي الكثير من الناس.

هل لديك أي سؤال؟ من فضلك تقدم نحو الميكروفون؟

كاثي بيترسين: لا تترددوا رجاء في استخدام أي ميكروفون على الطاولات. والرجاء التفضل بذكر الاسم والجهة التي تتبعونها إن وجدت. شكرا لكم.

فرزانه بديع: اسمي فرزانه بديع. وأنا رئيسة مجموعة أصحاب المصلحة غير التجارية. وأطرح سؤالي بصفتي الشخصية. عندما ذكرت أن اسم النطاق، الذي تباع فيه العقاقير غير المشروعة، قد ينطوي على بعض الأمور السيئة الأخرى، هل تقصد أنه قد تكون هناك إساءة استخدام فنية؟ أم أننا نتحدث عن محتوى الموقع ذاته؟

كارلوس ألفاريز: أنا أتحدث عن العمليات الإجرامية التي تستغل أسماء النطاقات. فاستخدامها لأسماء النطاقات يتعلق بمحتوى مواقع الويب والمزيد من الأنشطة الإجرامية التي تلي ذلك.

فرزانه بديع: أرغب في المتابعة. هل لا توجد علاقة لهذا بنظام DNS وتشغيله على المستوى الفني؟

كارلوس ألفاريز: هي تستخدم اسم النطاق لذلك الغرض.

فرزانه بديع: شكرا لكم.

كارلوس ألفاريز: بالطبع.

إذن، لماذا تدفع إن كان يمكنك التسلل وكسر الحماية؟ لماذا قد يلجأ المجرمون إلى الدفع مقابل أسماء النطاقات أو لماذا قد يختار بعضهم أن يدفع للحصول على أسماء النطاقات إن كان يمكنهم التسلل إليها والتحكم فيها؟

توجد حالات مختلفة يفضل فيها المجرمون اللجوء إلى إيقاف أسماء النطاقات وسرقتها بدلا من تسجيلها. كيف يقومون بذلك؟ يمكنهم اختراق بيانات اعتماد المستخدم. ويمكنهم اختراق بيانات دخول المسجلين إلى لوحة التحكم. وكما تعلمون، فإن لوحة التحكم هي واجهة الويب التي تسمح للمسجلين بإدارة اسم نطاقهم.

تخيلوا معي أن مؤسسة إجرامية تريد الاستيلاء على اسم نطاق معين عالي القيمة أو تريد الإضرار بعملاء بنك معين. فليس عليهم سوى إرسال حملة تصيد بحتة، وهي حملة تصيد استهدافية تكون موجهة إلى موظفي ذلك البنك، وبعد القيام ببعض أعمال الهندسة الاجتماعية، كالمعتاد، يتم إغراء عمال ذلك البنك بالنقر فوق رابط معين ما كان ينبغي لهم النقر فوقه، وبذلك تتم سرقة بيانات اعتماد الدخول.

وأيا كان الذي سيحدث بعد ذلك يمكن أن يمتد كما يشاء المجرم. ويمكنهم ببساطة إنشاء نطاق من المستوى الثالث تحت نطاق المستوى الثاني الذي ترونه. فإذا كان البنك الخاص بي يعاني من حالة كهذه، دعنا نقول إن نطاق بنكي هو carlosbank.whatever – بإمكان المجرم أن ينشئ نطاقا تحت مسمى "I'llphishyou.carlosbank.whatever" ثم يبدأ بإرسال رسائل البريد الإلكتروني كجزء من حملة التصيد والاحتيال، فينجح في إغراء المزيد من الضحايا لأنهم يرون أن نطاق المستوى الثاني هو فعلا اسم النطاق الحقيقي لبنكهم الخاص.

أو يمكنهم تغيير خوادم الأسماء تماما. فيمكنهم تغيير أي معلومات تتصل باسم النطاق. ويمكنهم تغيير أي سجل. كما يمكنهم الاستيلاء على كافة المعلومات الموجودة ضمن ملف المنطقة لهذا الاسم.

ثم بعد ذلك، هناك حالات أخرى حيث يغفل أمناء السجل -للأسف- عن تأمين بنيتهم الأساسية كما يجب ومن ثم تتعرض للاختراق. أعلم أن هذا لا يحدث كثيرا، وهو أمر جيد، ولكنه حدث بالفعل. وعندما يحدث ذلك، لا يكون الوضع جيدا على الإطلاق. ولكن لحسن الحظ، في هذه الحالات القليلة جدا التي شهدناها، سعى المجرمون وراء أهداف معينة عالية القيمة، ولكن سرعان ما كان يرد أمناء السجلات. وفي الحقيقة، كان هذا منذ مدة. وقد تم التعامل معه بطريقة مناسبة جدا. ويسعى المجرمون وراء أهداف هم يعلمون سلفا أنه سيكون بمقدورهم الحصول عليها لو استولوا على هذه الخوادم.

وهكذا كما ترون، تنجح حالة تصيد عادية من جانب المستخدم، إذا تم إغراء أمناء السجلات بالنقر فوق رابط معين. أو بالهجوم على البنية الأساسية للتسجيل، لو نجح التصيد.

حسنا، هذا جانب آخر من التصيد. كم عدد أمناء السجلات الذين يكون لديهم بيانات اعتماد الدخول نفسها إلى لوحة التحكم والذي يمكنهم من خلالها إدارة أسماء النطاق الخاصة بهم؟ كم عدد أمناء السجلات الذين يكون لديهم بيانات اعتماد الدخول نفسها في لوحة التحكم هذه كما كان الحال في الحساب الذي تم اختراقه من قبل؟ وفي أي حالة من عشرات الاختراقات والانتهاكات الكبيرة التي نشهدها كل أسبوع، بصورة أساسية، أو كل شهر، يكون ذلك العدد غير معروف.

يعد حشو بيانات الاعتماد من الطرق التي يلجأ إليها المجرمون في محاولة تسجيل الدخول في أكثر عدد ممكن من الخدمات، ويمكنهم القيام بذلك من خلال استخدام أسماء المستخدمين وكلمات المرور التي تم سرقتها في حالات اختراق البيانات السابقة. وعندما يحصلون عليها، يدخلون هم وينتهي أمرك أنت. وهذا أمر خطير لا نعلمه. فيجب ألا نجرب ذلك. فهذا أمر خطير لا علم لنا به، كم عدد أمناء السجلات الذين يعيدون استخدام

كلمات المرور الخاصة بهم لإدارة تسجيلات نطاقهم؟ فعليكم بالتوعية، فالتوعية هي الحل كالعادة.

أصبحت تقنية التدفق السريع متاحة الآن. تقنية التدفق السريع هي تقنية يستخدمها المجرمون لتتيح لهم القفز من عنوان IP إلى عنوان IP آخر بسرعة للغاية، وذلك بغرض تعقيد الأمر أكثر وأكثر على موظفي إنفاذ القانون وتخفيف المخاطر.

يقومون بذلك عن طريق تعيين قيم TTL لفترات قصيرة في ملفات المنطقة الخاصة بهم. وترمز كلمة TTL إلى مصطلح Time to Live (فترة بقاء البيانات فعالة). وهذا هو الوقت الذي قد يكون فيه عنوان IP المرتبط - مثلا - بموقع الويب صالحا. وبعد ذلك، سيعرف المحللون المتكررون أن عليهم الاستفسار مرة أخرى للحصول على تلك المعلومات مجددا. وعندما يفعلون ذلك، سيتلقون عنوان IP مختلف. لذا، عندما ترون فترات بقاء قصيرة ((TTL، مثل 120 ثانية أو 180 ثانية أو دقيقتين أو 3 دقائق أو حتى 4 دقائق، فهذا شيء ينظر إليه الباحثون وهم يفكرون بشأنه.

يكمن الخطر هنا في أن تشغيل شبكات توريد المحتوى الكبيرة (CDN) يستلزم أيضا استخدام فترات بقاء قصيرة (TTL) لتوفير الاستقرار وضمان توازن الحمل ولأغراض فنية أخرى. ولكن هذا مختلف. لذا، إذا كنت باحثا في مجال التهديدات، فأنت على علم بالشبكات الكبيرة التي تستخدم فترات البقاء القصيرة، وهذا أمر جيد. ولكن إذا صادفت نطاقا جديدا يحتوي على فترة بقاء قصيرة مرتبطة ببنية أساسية [حديثة] نوعا ما وربما كانت مرتبطة بالرسائل غير المرغوب فيها أو شيء من هذا القبيل، لا بد أن يثير ذلك بعض الشكوك في الحال. هذا عندما يتم إغراء باحثي التهديدات بحظر مرور البيانات المرتبطة بهذه البينة الأساسية لغرض الحماية.

ما يحدث إذا كنت موظفا في جهات إنفاذ القانون وتحقق في بنية أساسية/عملية إجرامية حيث تستخدم العناصر السيئة تقنية التدفق السريع، إذ ترى أن المحتوى موجود في هذا الخادم الكائن في هذا البلد، وبعدها بدقيقتين، لم يعد المحتوى ذاته موجودا، ويصبح موجودا في خادم آخر في بلد آخر، وبعد ذلك بدقيقتين، يقفز المحتوى إلى خادم آخر في

بلد آخر، وبعدها بدقيقتين أخريين، يقفز المحتوى إلى الخادم التالي في بلد رابع أو خامس وهكذا. فكيف تتعامل جهات إنفاذ القانون مع هذا الأمر؟

هذا صعب. صعب للغاية. الآن نواجه تقنية التدفق السريع المزدوج. وهي تقنية رأيناها في خدمة – كيف أصيغها؟ – خدمة سحابية إجرامية ضخمة. وتسمى "أفالانش". في شبكة "أفالانش"، كانت العناصر السيئة تستخدم تقنية التدفق السريع المزدوج. وما كان يعنيه ذلك هو أن تغيير خوادم الأسماء كان يحدث دائما مرارا وتكرارا.

فلو أردت الاستفسار عن نطاق carlos.whatever الآن، لاستفسرت عن ns1.carlos.whatever. ولو أردت الاستفسار في خلال دقيقتين، لاستفسرت عن ns1.cathy.next. وفي خلال الدقيقتين التاليتين، كنت لأستفسر عن ns3.cameron.yoohoo. وكل دقيقتين أو ثلاثة، ستتغير خوادم الأسماء. وكانت خوادم الأسماء على رأس ذلك، إذ يتم تغيير عناوين IP كل دقيقتين أو ثلاث دقائق أو كل فترة بقاء قصيرة يعينها المجرمون. فكان ذلك أكثر سوءا وأكثر إزعاجا وتعقيدا، ولكن استطاع المحققون الأكفاء كشف ذلك الأمر والتعامل معه. والآن هؤلاء المجرمون موجودون خلف القضبان. كما أن زعيمهم موجود أيضا خلف القضبان.

لقد ذكرت من قبل أن نظام DNS عبارة عن قناة استخراج سرية وأن أنواع البرمجيات الضارة في الحقيقة، ليست لاستخراج البيانات فحسب، ولكنها أيضا للتحكم الفعلي في البرمجيات الضارة التي أصابت أو اخترقت الأجهزة. ومن خلال نظام DNS، يستطيع المجرمون تقديم تعليمات إلى الأجهزة. ويقوم المجرمون بتعديل البرمجيات الضارة التي اخترقت الأجهزة بالفعل. ويمكن للمجرمين إقحام المزيد من البرمجيات الضارة خلال نظام DNS.

إنه أمر مزعج - كما قلت - بسبب المنفذ رقم 53، الذي يجري استخدامه لاتصالات DNS ولا يمكن حظره. لذلك يحق لمدير الشبكة أن يطالب بتوفير تقنيات جيدة حتى يكون قادرا على كشف هذه الأشياء.

وهناك بعض التقنيات التي لا يمكنني أن أشير إليها الآن لأن ذلك سيتطلب ثلاث ساعات أخرى. الأمر عائد إليهم. من حق كل مدير شبكة أن يطبق هذه التقنيات.

لقد عرفنا ذلك للتو. ويفعل ذلك نموذجان فقط من بين أنواع البرمجيات الضارة، الكثيرة جدا والتي تفعل ذلك وأكثر، ويطلق عليهما Feederbot وMorto. هل تلاحظون هنا أن خوادم القيادة والتحكم في شبكة البوتنت تقوم بتشفير التعليمات في ردود TXT الخاصة بنظام DNS. لذا، يقوم الجهاز المخترق بإرسال استفسار إلى خادم الاسم ثم يقوم المجرم بتكوين خادم نظام DNS بحيث يقدم ردا بنفس الصيغة التي كان الاستفسار عليها لتسجيل TXT، ويقدم التسجيل النصي هذا تعليمات إلى الجهاز المخترق، هذا بشكل أساسي. ويمكن أن تكون هذه التعليمات عبارة عن أي شيء. فيمكن أن تكون عبارة رسالة نصها "نفذ هجوما على هذه الأهداف ومرور البيانات بهذه الطريقة". لذا، يمكن أن تكون أي شيء.

كمشهد نظام DNS المتطور. أو الحرمان المنتشر للخدمة كخدمة. أو الحديث عن ميراي. هل يتذكر أحدكم ميراي؟ أجل. إنه موقف سيء.

ميراي كانت - كيف يمكننا طرح هذا الأمر مرة أخرى؟ كان هناك ارتباط بين مزودي ما يعرف باسم خدمات البوتر أو خدمات اختبارات الضغط مع هذا الهجوم على بشكة البوتنت.

إذا، ما المقصود من خدمة البوتر أو خدمة اختبارات الضغط؟ إنها عبارة عن موقع ويب ينشئه أحد الأطفال في مكان ما، حيث يزعمون أنهم يبيعون القدرة على اختبار مدى مرونة واستقرار الخوادم الخاصة بك. وتدفع مبلغا معينا من المال ويقولون لك حسب ما يدعون "سنرسل هذا الكم من المرور خلال هذه الفترة الزمنية حتى تتمكن من اختبار البنية الأساسية لمعرفة مدى مرونها وما إذا كانت ستتحمل هجوما أم لا."

يكمن الأمر في أن خدمات البوتر أو خدمات اختبارات الضغط هذه تبيع هذه الخدمة إلى أي شخص، سواء أكان يعمل على البنية الأساسية التي يتم اختبارها أم لا. بعبارة أخرى، إنهم يقومون بتشغيل خدمات الحرمان المنتشر للخدمة للتوظيف. وليس من الصعب

العثور عليهم. حيث يمكنهم الاتصال بالإنترنت وإجراء بحث في غاية السهولة باستخدام محرك البحث المفضل لديك، ويمكنك العثور عليهم بسهولة. وهناك بعض الأغبياء الذين يقبلون مدفوعات بطاقات الائتمان، مما يجعل الأمر أسهل للجانب المشرق من القوة. وكل ما عليك فعله هو الدفع ثم تقديم المعلومات والهدف الذي تود اختباره، لأنك بالطبع، ترغب في التأكد من أنها شبكة مرنة. [غير مسموع] حسنا. هذا ليس رائعا.

إنهم يفعلون ذلك بوسائل مختلفة، وإحدى تلك الوسائل هو تشغيل شبكات البوتنت، بالطبع. ولقد تحدثنا بالفعل عن التدفق السريع والتدفق السريع المزدوج. وأشرت إلى عملية أفالانش. وسوف نتحدث عن هذا الموضوع بعد عدة شرائح. وتعد أفالانش حالة رائعة جدا، وسوف ترون السبب.

إنترنت الأشياء. لم أكن أرغب في الإشارة إلى الكلمة الخفية بين "إنترنت" و"الأشياء"، إلا أنها حقيقية للأسف. وجميعنا يعرف أن هذا شيء ليس جديدا.

هناك مثال جيد لمعرفة كيف يمكن أن تسوء الأمور: فكر في الهجوم - أعتقد أنه كان ضد بريان كريبس - في أكتوبر 2016، ربما؟ أو سبتمبر؟ وضد شركة أو في إتش، التي تعد أحد أمناء السجلات المعتمدين لدى ICANN. كما أنها تعتبر مزود كبير لخدمات الاستضافة في فرنسا. وكانت قادرة على اكتشاف أن الهجوم كان قادما من حوالي 146,000 كاميرا فيديو رقمية.

استطاعت شبكة البوتنت إرسال 1.5 تيرابايت من البيانات. وفي ذلك الوقت، كان ذلك بمنأى عن البصر. هذا جنون. أنا لا استطيع تخيل هذا الكم من البيانات. ثم استطاعت قياس 1.1 تيرابايت في حركة المرور الفعلية الموجهة ضدهم. وكانت عبارة عن كاميرات فيديو. مرة أخرى، هذا ليس شيئا جديدا، لكنه أمر يستحق الإشارة إليه، على ما أعتقد. كان نظام DNS أحد المتجهات المستخدمة في هذا الهجوم - ليس المتجه الوحيد، لكنه أحد المتجهات الذي تم استخدامه بالتأكيد.

ثم لدينا هجوم واناكراي الإلكتروني، الذي أشرت إليه أيضا، ولذلك، سأتخطى الحديث عنه الآن.

كانت عملية أفالانش إحدى الخدمات السحابية الإجرامية. تخيل أنك دخلت موقع ويب وأنشأت حسابا وقمت بتسجيل الدخول، وكان بإمكانك اختيار نوع البرمجيات الضارة ونوع الحملة التي تود تشغيلها. ما فعله هؤلاء الأشخاص هو تشغيل كل شيء من أجلك. وكل ما عليك فعله هو أن تدفع لهم المال ثم يمكنهم تشغيل كل شيء من أجلك. سيوفرون لك البرمجيات الضارة لإصابة عملائك. ويمكنهم إصابتهم بالفعل من أجلك. فهم يستطيعوا استخدام [غير مسموع] اسم النطاق للقيادة والتحكم نيابة عنك. كما أنهم يستطيعوا استخدام [غير مسموع] أسماء النطاق هذه من أجلك.

سيوفرون الاستضافة لمواقع نشر البرمجيات الضارة. بالطبع، يمكنهم تشغيل كل ذلك من أجلك. إذا، كان هذا هو المستوى التالي في التطور بخصوص [اختبار] الخدمات الإجرامية.

لقد كان لعملية أفالانش أثرا كبيرا في تسجيل DGA في النطاقات التي تم إنشاؤها تلقائيا باستخدام خوارزمية. عندما تم تطبيق إجراءات إنفاذ القانون، تم اتباع عملية داخل مؤسسة ICANN، تسمى بعملية طلب أمان السجل السريع. ومن خلال هذه العملية، تم استعادة 832,000 اسم نطاق من أيدي المجرمين.

لذا، من حالة إلى أخرى، وبفضل تعاون جميع شركاء إنفاذ القانون وبعض الأفراد في القطاع الخاص، فقد المجرمون السيطرة تماما على بنيتهم الأساسية. وتلاشت هذا البنية تماما. وأعني، أنها لا تزال موجودة، لكنهم لا يستطيعون استخدامها. فلا يمكنهم التحكم في أي شيء بعد الآن. إنه شعور رائع عند حدوث ذلك.

هذه هي بعض السلاسل التي كان من المقرر إنشاؤها بواسطة عملية أفالانش، عن طريق شبكة البوتنت، لأغراض القيادة والتحكم. وكان من المقرر إنشاء جميع أسماء النطاقات هذه البالغ عددها 830,000 اسم تحت مجموعة من نطاقات المستوى الأعلى لتشمل كلا من نطاقات المستوى الأعلى لرمز البلد وبرامج gTLD. وكما قلت، فإن المجرمين سيسيئون لكل من يستطيعوا توجيه الإساءة إليه. وبالطبع، فإنهم لا يهتمون بشيء مطلقا.

حسنا، هناك شيء واحد. حيث أن بعض المجرمون في مناطق معينة من العالم سيصممون برمجياتهم الضارة بطريقة لا تهاجم عنوان IP ضمن نطاق ولايتهم القضائية لأنهم لا يريدون أن تلاحقهم جهات إنفاذ القانون داخل بلادهم لأن الأمر قد يصبح سيئا لهم. لذا، فهم يتخطون مساحة عنوان IP الخاصة ببلدهم تماما.

الشيء المثير، هو أنهم لا يستطيعون مغادرة بلدهم، وهذا في الحقيقة ليس أمرا سيئا. فهم يجعلون أنفسهم سجناء داخل حدود بلدهم. من الجيد وجودهم هناك، إلا أن هذا الأمر يعد سيئا لأنهم يؤذون الكثير.

تلك هي نتيجة إزالة عملية أفالانش. وبفضل المحتوى الذي قدمته وكالة يوروبول ومكتب التحقيقات الفيدرالي، فإن العرض التقديمي بالكامل مخصص للحديث عن هذه الحالة فقط. هذه مجرد نتيجة لا أكثر. وتم تسجيل خمس حالات اعتقال في أربعة بلدان و37 عملية بحث في سبعة بلدان وضبط 39 خادما في 13 بلد والاستحواذ على 221 خادما في وضع عدم الاتصال بالإنترنت و64 نطاقا من نطاقات المستوى الأعلى/832,000 نطاقا في 26 بلد إلى جانب الكثير من عمليات تعويض الضحايا ورفع الوعي والتدابير الوقائية. إذا، هذه عملية واسعة النطاق. وهذا أمر جيد. إنها بمثابة ضربة كبيرة جدا.

كان هجوم واناكراي الإلكتروني شيء غريب إذا نظرت إليه من منظور نظام DNS. وكان المثير للاهتمام في هذا الأمر، على عكس ما كان يحدث عادة في أنواع البرمجيات الضارة الأخرى التي تستخدم عادة أسماء النطاقات بهدف القيادة والتحكم ضمن أي نطاق من نطاقات المستوى الأعلى العادية - برامج gTLD أو نطاقات المستوى الأعلى لرمز البلد، وكانت أغلب عمليات القيادة والتحكم من هجوم واناكراي عن طريق سبعة نطاقات onion. على ما أعتقد. وإذا كنتم تتذكرون نطاق .onion الذي عرفه فريق عمل هندسة الإنترنت على أنه نطاق المستوى الأعلى المستخدم بشكل خاص، مما يعني أنه لن يتواجد في الجذر مطلقا، وهو ما يعني أن مؤسسة ICANN لن يكون أمامها أي شيء لتقوم به حيال هذا النطاق. لذلك لم تكن هناك طريقة لإزالة البنية الأساسية للقيادة والتحكم المرتبطة بهجوم واناكراي الإلكتروني.

ومع ذلك، كان الباحث البريطاني الشاب ماركوس هاتشينز يحلل الكود. وتمكن من الحصول على عينة من هجوم واناكراي. وكان يحللها وصادف سلسلة كانت ضمن الكود على ما أعتقد. بالطبع كان كودا مشفرا بطريقة صعبة في البرمجيات الضارة. وقد تحقق من ذلك. ولم تكن هذه السلسلة مسجلة. ثم قام بتسجيلها وأوقف انتشار البرمجيات الضارة. وكان ذلك بمحض الصدفة. فلم يكن لديه أي فكرة عما كان سيحدث. لكنه نجح في ذلك الأمر فقط لمجرد تسجيل اسم النطاق هذا، وتمكن من إيقاف انتشار البرمجيات الضارة.

فالمنطق هو أساس ما يحدث هنا. فإذا كانت برمجيات الدفع القسري للفدية ترتبط بالقيادة والتحكم، إذا فالعملية المناسبة هي تفادي التحليل. ولحسن الحظ، كان هذا موجودا. ومن ثم نجح في إيقاف هجوم واناكراي الإلكتروني.

ثم حاول المجرمون الذين يقفون وراء هجوم واناكراي الإلكتروني تسجيل سلسلة ثانية، إلا أنه تم تسجيلها بسرعة كبيرة أيضا. وفي النهاية، توقف انتشار الهجوم بشكل كامل. ولم يكن أمامهم سوى الانتقال إلى مكان آخر.

يعد موضوع إساءة استخدام نظام DNS مثيرا للجدل داخل مؤسسة ICANN. وتوجد وجهات نظر مختلفة حيال هذا الأمر. حيث أن البعض، ممن يركزون على الناحية الأمنية، من جانب إنفاذ القانون، لديهم مخاوف تتعلق بدقة نظام WHOIS، وكذلك التأثير الذي سينتج عن القواعد العامة لحماية البيانات على العمليات وكيفية عناية نظام WHOIS بعد 25 مايو، عندما يتم تطبيق القواعد العامة لحماية البيانات.

هناك مخاوف تتعلق ببعض الأمور مثل وقت الرد ووقت التفاعل، كلما تم تقديم منفذا لإساءة الاستخدام. وهناك أنواع مختلفة من المخاوف في هذا الشأن.

على الجانب الآخر، وهو جانب يجب أن نستمع إليه أيضا بصفتنا مؤسسة، وهو القلق حيال عدم خروج مؤسسة ICANN من اختصاصها أو من نطاقها بمعنى أنه إذا كان هناك محتوى، فيجب ألا يكون أمام مؤسسة ICANN أي شيء لتقوم به. وهذا يعني أن عقود مؤسسة ICANN لا تتضمن أحكاما تسمح بإزالة محتوى مقرصن على سبيل

المثال. وسوف يجري المجتمع هذه المناقشة، وليس المؤسسة. لذا، عليكم أنتم أيها الرفاق إجراء هذه المناقشات. ويمكننا تيسير هذه المناقشات، لكن لا يمكننا المشاركة فيها.

الأهم من ذلك، هو أن مجموعة عمل الأمن العام هي جهة إنفاذ القانون، سواء القانون المدني أو الجنائي، داخل هيكل مؤسسة ICANN والمجموعات الأكبر من لجان مؤسسة ICANN، وما إلى ذلك. وقبل مجموعة عمل الأمن العام، كما تعرفون، لم يجد مجتمع إنفاذ القانون موطنه، وأعتقد أنه بكين، عندما سألت لورين كابين من لجنة التجارة الفيدرالية الأمريكية فادي شحاده، الرئيس التنفيذي السابق، عما إذا كان يرغب في التفكير بأنه ينبغي أن يكون لمجتمع إنفاذ القانون مقرا رسميا ضمن هيكل مؤسسة ICANN. إلا أنه ترك الأمر لمجتمع إنفاذ القانون: "وقال أحضروا لي مقترحا." ولذلك، أحضروا هذا المقترح. وهذا المقترح هو ما نعرفه اليوم باسم مجموعة عمل الأمن العام، وهي عبارة عن مجموعة عمل أو مجموعة فرعية ضمن اللجنة الاستشارية الحكومية الأكبر. وهذا هو مقر تواجدهم.

يتمثل الغرض من إنشاء مجموعة عمل الأمن العام في تقديم المشورة للجنة الاستشارية الحكومية ومجتمع ICANN الأكبر. وهناك بعض الموضوعات التي يركزون عليها وهي إساءة استخدام نظام DNS، وأيضا، الطرق التي يتم بها استخدام أسماء النطاقات لأغراض ضارة ولإلحاق الضرر بالمستخدمين، وسيكون للقواعد العامة لحماية البيانات، تأثيرا على معلومات نظام WHOIS المتاحة لأبحاث التهديد وعمليات التحقيق، وتحويل فئة الناقل الشبكي (CGN NAT). باختصار، هذه تقنية يستخدمها بعض مزودي خدمات الإنترنت. هذه التقنيات والتقنيات الشبيهة يستخدمها بعض مزودي خدمات الإنترنت عندما يفضلون عدم الانتقال إلى بروتوكول الإنترنت- الإصدار السادس (IPv6).

لذا، بدلا من الاضطرار إلى الترقية إلى IPv6، يقومون بإنشاء شبكات محلية ضخمة وتعيين عناوين IP داخلية لعملائهم. وهناك عناوين IP مصممة فقط لتكون في الإنترنت العام والتي كنا سنراها علنا لو كنا نحلل حركة مرور البيانات، كما أن عناوين IP الخاصة بهم والمصممة لتكون موجودة في الشبكات الخاصة فقط، ينبغي ألا تكون ظاهرة

للجمهور في الإنترنت العام. فهذا هو الحال، على سبيل المثال، في شركتك وفي منزلك. فالأجهزة الخاصة بك يكون معين لها عناوين IP الخاصة هذه.

ما يفعله مزودو خدمات الإنترنت هو أنهم يقومون بتعيين عناوين IP الخاصة هذه لعملائهم، حتى لو كانوا 500 أو 1,000 أو 10,000، وينشئون شبكات خاصة على مستوى الأحياء، أي شبكات محلية، بعنوان IP عام واحد. وهذا يسبب المزيد من التعقيد لجهات إنفاذ القانون لأنه عندما يأتي موظف إنفاذ القانون ويطرق الباب لتسليم أوراق قانونية - مثلا - أو عندما يرسلون أمر مثول أمام المحكمة إلى مزود خدمة الإنترنت ويطلبون معلومات بخصوص المستخدم الذي أرسل هذا المرور من عنوان IP هذا في ذلك اليوم وفي هذه الساعة، سيكون رد مزود خدمة الإنترنت:" حسنا، لا أدري. فيوجد خلف عنوان IP العام هذا نحو 10,000 مستخدم."

في العديد من البلدان، لا توجد التزامات، أو قد توجد الالتزامات ولكنها ليست سارية فيما يتعلق بالتقيد بهذه الالتزامات وصونها وحفظ سجلات المرور وتسجيلات الدخول والخروج. لذلك في أماكن عديدة، تسجل الدخول ثم تسجل الخروج وإذ فجأة! تختفي البيانات. ولا أحد يعلم أنك كنت هناك. ولا حتى مزود خدمة الإنترنت يعلم أنك كنت هناك. لذا، فإن الأمر معقد. وهذا أحد الأمور التي ناقشتها مجموعة عمل الأمن العام في السابق. وكما نعلم، تقنية التدفق السريع هي تقنية يستخدمها المجرمون.

هذان مجرد مثالان فقط. وهذا لا علاقة له [بالضرائب] أو الأمور التقييدية بأي حال من الأحوال، بل إن الفحوصات التعاقدية داخل ICANN، شبكة التعاقدات الأكبر هي التي تكون على علاقة بإساءة الاستخدام. هناك العديد. يمكننا إجراء محادثة تستمر لساعات للحديث فقط عن مكافحة إساءة الاستخدام من منظور تعاقدي داخل ICANN.

أذكر أن السجلات تلتزم بالفعل بمراقبة منطقتها لرصد التهديدات الأمنية. ويعني ذلك أن عليها التزام بالنظر في النطاقات الموجودة بداخلها.

فلو كانت مسؤولا عن نطاق المستوى الأعلى .carlos، لنظرت في كافة أسماء نطاق .carlos ثم قمت بتحديد أيها يقوم بالتصيد وأيها رسائل غير مرغوب فيها وأيها

برمجيات ضارة وأيها قيادة وتحكم، وبعد ذلك كنت لأبلغ هذه الإحصاءات والمؤشرات إلى ICANN. هذا هو الالتزام الذي يقع على جانب السجلات.

وأعتقد كذلك، لو لم أكن مخطئا، أن السجلات ملزمة أيضا بتوفير معلوماتهم عن نقاط الاتصال المتعلقة بإساءة الاستخدام. ولكنني أظن أن هذا أقصى ما يمكن تحقيقه، لا سيما فيما يتعلق بمكافحة إساءة الاستخدام للسجلات.

ومع ذلك يكون الأمر أكثر تحديدا من جهة أمناء السجلات. حيث توجد هذه الأحكام الأكثر تحديدا في تلك الاتفاقية. وهذه الاتفاقية تسمى اتفاقية اعتماد أمين السجل، أو RAA، مثلما نطلق عليها بشكل غير رسمي.

صدرت هذه الأحكام الأكثر تحديدا نتيجة لاثنى عشر توصية من توصيات إنفاذ القانون والتي تم تقديمها من خلال ما يعرف الآن بمجموعة عمل الأمن العام - وكانت في ذلك الوقت مجرد مجتمعا لإنفاذ القانون - وكان ذلك من خلال اللجنة الاستشارية الحكومية في اجتماع كوستاريكا عام 2012. وأعتقد أن ذلك هو وقت تقديمهم للاثنى عشر توصية.

أدى ذلك بدوره إلى حث مجلس الإدارة على توجيه الموظفين لبدء المفاوضات مع مجموعة أصحاب المصلحة من أمناء السجلات. وقد استمرت تلك المفاوضات طوال بضعة أشهر، وتم التوصل من خلالها إلى أن تشتمل اتفاقية اعتماد أمين السجل لعام 2013 على أحكام أكثر تحديدا بشأن مكافحة إساءة الاستخدام.

إذ لا يزال يرغب بعض العاملين في مجتمع أمن العمليات في رؤية أحكام أكثر وضوحا وصرامة، ولكن عند هذه المرحلة، كان إنفاذ القانون عملا لا بأس به مع النص المتفق عليه من قبل كل من مجموعة أصحاب المصلحة من أمناء السجلات ومؤسسة ICANN.

كما تشمل بعض هذه الالتزامات، على سبيل المثال أن يقوم أمناء السجلات باتخاذ إجراء معقول عند تلقيهم تقارير تتعلق بإساءة الاستخدام وذلك عند ذكر نبذة سريعة عنها. وبالطبع، إذا توجهت بالسؤال عن معنى كلمة "معقول" إلى 10 محامين، ستحصل على

20 إجابة مختلفة وهو ما يساهم في تعقيد الأمر. ولكن هذا هو ما يوجد في اتفاقية اعتماد أمين السجل.

كما أنه لديهم التزام آخر يتمثل في ضرورة تقديمهم نقاط الاتصال المتعلقة بإساءة الاستخدام. وحسب اعتقادي، يجب نشر هذه المعلومات على موقع الويب و/أو بيانات نظام WHOIS. وأعتقد أيضا أنها توجد عادة في بيانات نظام WHOIS. وعليهم أيضا نشرها على مواقع الويب الخاصة بهم. أنا غير متأكد، كما ترون. أعتقد ضرورة وجودها هناك، لكنني لست متأكدا من ذلك.

فهناك حكم مثير للاهتمام خاص بإنفاذ القانون. وعندما ترسل وكالة إنفاذ القانون من جهة الاختصاص التابعة لأمين السجل ذاته تقريرا عن إساءة الاستخدام إلى ذلك الأمين - تذكر أنه يجب أن يكون له نفس الاختصاص - ويجب على أمين السجل تقديم رد بشري خلال 24 ساعة. وكما ذكرت يجب أن يكون هذا الرد بشريا وليس آليا. ولا يجب أن يكون الرد متمثلا في عبارة "لقد علقنا النطاق." ويمكن أن يكون الرد ببساطة "نحن نقر بالاستلام." وهذا رد مناسب.

يجب أن يتمتع الشخص الذي يقدم هذا الرد، وفقا لنص الاتفاقية، بإمكانية تحديد ما سيحدث نتيجة تقرير إساءة الاستخدام من حيث ما إذا كان يجب تعليق النطاق أم لا.

يساعد هذا الحكم بدرجة كبيرة في بعض الولايات القضائية، حيث يوجد العديد من أمناء السجلات العاملين فيها، ولكن هناك بعض الولايات القضائية التي يوجد فيها عدد قليل جدا منهم أو قد لا يوجد أي منهم على الإطلاق. لذلك، تختلف بالطبع فعالية هذا الحكم أو نتائجه باختلاف الولاية القضائية.

يتمثل مزودو الخصوصية والوكلاء؛ إذا كنت تذكر، في تلك الخدمات التي يستخدمها أمناء السجلات للحصول على معلومات شخص آخر عن نتائج نظام WHOIS لأسماء نطاقاتهم بدلا من الأسماء الخاصة بهم. إذا كان لدي موقع ويب ولا أريد أن يكون اسمي أو عنواني أو عنوان بريدي الإلكتروني موجودين، يتعين على مزودي الخصوصية

والوكلاء الذين يتحكم فيهم أمناء السجلات توفير معلوماتهم الخاصة بنقاط الاتصال المتعلقة بإساءة الاستخدام.

أعتقد أن هذا كل ما لدي. وتلك هي الموضوعات التي أردنا أن نغطيها. وهي موضوعات كثيرة. كما قلت، بخصوص إساءة استخدام نظام DNS، بينما يبدو الأمر مباشرا، عندما ترى اسم نطاق يستخدم في قيادة شبكات البوتنت والتحكم فيها، حينئذ يكون من الواضح أن هذا هو الحال. وعندما ترى ذلك، يمكنك إجراء جميع التحليلات الفنية ولا توجد طريقة لنفي صحة ما يظهره الدليل العلمي والفني الفعلي لأنه هو الموجود. ولكن هناك حالات يكون فيها الأمر أكثر تعقيدا بعض الشيء.

هذا الموضوع مطروح للمناقشة المستمرة. فالأمر يرجع إلى المجتمع لمتابعة تطوير هذه الموضوعات والتوسع فيها.

مهمتنا - لقد أخفقت في قول ذلك عند البداية. أنا مدير إدارة الأمن والاستقرار والمرونة ومشترك مع فريق عمل الأمن والاستقرار والمرونة. نحن نتبع مكتب CTO. حيث نشارك بقوة مع المجتمع التشغيلي والأمني وإنفاذ القانون.

إننا نهدف إلى تحقيق أشياء كثيرة. فنحن نحاول تقريبهم من عالم ICANN وتعريفهم به. كما أننا مهتمون بشدة في إدراكهم لجميع المناقشات التي تجري لدينا هنا. قبل بضعة أسابيع، حضر ممثل عن مجال اسم النطاق مؤتمرا أمنيا بناء على دعوتنا. وهذه هي مجموعة العمل المختصة بمكافحة الرسائل والبرمجيات الضارة وسوء استخدام الهواتف النقالة. وكان ذلك جوناثان فراكس والمدير التنفيذي لرابطة اسم النطاق. وكان لديه تفاعلات إيجابية.

يعد ذلك من بين المهام التي نقوم ونشترك فيها. إذ أننا نسعى إلى استقطاب أشخاصا ربما كان قد سبق لهم رؤية بعضهم بعضا بشكل تقليدي كما هو الحال في [المقاعد] المتقابلة. فنحن نحاول تقريب وجهات نظر هؤلاء الأشخاص إلى الآخرين. فإذا تمكنوا من فهم مصدر وجهة نظر كل واحد منهم، فيمكن بناء شيء ما على هذا الفهم.

إننا نعمل على تدريب جهات إنفاذ القانون. يتمثل أحد مهام ICANN، كما تذكر، في المساعدة في الحفاظ على أمان نظام اسم النطاق واستقراره ومرونته. ويعني ذلك أنه على جهات إنفاذ القانون أن تدرك حقيقة الأمر عند النظر في تحقيق شبكة البوتنت أو عند النظر في تحقيق ما يتعلق بنشر البرمجيات الضارة. فعليهم أن يفهموا الطريقة التي تسير بها عمليات نظام DNS. ونحن نساعدهم على فهم ذلك من هذا المنظور بحيث يمكنهم المساعدة في الحفاظ على أمن النظام واستقراره ومرونته مثلما نسميه في شكل اختصار آخر.

أعتقد أن هذا كل ما لدي. وإذا كان لدى أي شخص آخر أي أسئلة، فرجاء التفضل.

كاثي بيترسين: للتذكير، يرجى تقديم اسمك وجهة انتمائك إن وجدت.

[مارسي سورمو]: مرحبا. معكم [مارسي سورمو] من الهند. [غير مسموع] سؤال أيضا: سواء أعدت ICANN بعض المعايير الأمنية الأساسية لعمليات نظام DNS أو طرق تنفيذه. هل يمكن الاحتفاظ بها؟ يمكنه أن يكون جهازا تشغيليا فقط ولا يوجد أمان. وسوف تحدث كل أنواع الانتهاكات. ثم سيكون هناك تحليلات لاحقة فقط. إذا، هل يمكن وضع بعض الحدود الدنيا للمعايير الأمنية الأساسية قبل إعداد أي نظام DNS تشغيلي؟

كارلوس ألفاريز: أود أن أقترح عليك البحث عن الوثائق التي نشرها مركز عمليات وتحليلات وأبحاث نظام اسم النطاق، والذي يمثل مجتمع مشغلي نظام DNS. بالطبع، لا داعي للقول أن هناك معايير IETF التي قد تحتوي على بعض المكونات الأمنية فيما يتعلق بنظام DNS. ثم تحقق من مجموعة العمل المختصة بمكافحة الرسائل والبرمجيات الضارة وسوء استخدام الهواتف النقالة. منذ حوالي عام ونصف، قاموا بتحديث ما يعرف باسم ... لقد نسيت الاسم. وإذا بحثت عن تهديدات نظام DNS لمجموعة العمل المختصة

بمكافحة الرسائل والبرمجيات الضارة وسوء استخدام الهواتف النقالة، ستجدها معرضة لذلك. أنا متأكد. كما يوفر أيضا بعض المعلومات الجيدة.

إذا، هذه هي المجتمعات أو المجموعات التي أعتقد أنها عملت وقدمت وثائق أو معايير كما سبق وذكرت.

[مارسي سورمو]: إن ذلك مجرد توجيه. هل يمكننا فقط [غير مسموع] قبل وصول [غير مسموع] إلى هذه الأجهزة، وتنفيذ الحد الأدنى من معايير الأمن هذه؟

كارلوس ألفاريز: لا يمكن إنفاذه. يمكن لأي شخص إعداد خادم نظام DNS وتشغيله. أي شخص في العالم. وليس هناك ثمة طريقة لإنفاذه. فهو أمر مستحيل منعه من الناحية الفنية. ليس هناك قاعدة لذلك. وليس هناك التزام. يمكن لأي شخص القيام بذلك مهما كان. الأمر تطوعي، مما يجعله غير محدد.

الآن، فيما يتعلق بما كنت تقوله عند التحدث عن المكون التطوعي الخاص به، توجد معايير ووسائل للقيام بالأمور التي حددها المجتمع الفني لسنوات؛ منذ عام 1997، على سبيل المثال، تصفية عناوين IP [الأربعة]. أما إذا بحثت عن BCP 38 أو BCP 84، ستجد أن أفضل الممارسات الحالية تذكر 20 سنة أو أكثر. ومع ذلك، وبسبب كونها تطوعية، لم يتم تطبيقها على نطاق واسع أو نطاق واسع بالمعنى الذي كنت تتوقعه. هذا أمر تطوعي.

هل توجد أي أسئلة أخرى؟

نعم سيدي؟

[هارو الحسن]: حقا -

كارلوس ألفاريز: يرجى ذكر اسمك وجهة انتمائك.

[هارو الحسن]: معكم [هارو الحسن] من نيجيريا. تتمثل التحديات التي تواجهنا في البلدان النامية في: كيف نقوم بتدريب وكالات إنفاذ القانون لدينا للتصدي لهجمات المجرمين؟ نظرا لأنك أظهرت الكثير من الطرق التي يمكن من خلالها إفساد نظام DNS، عندما يمكن مهاجمتها، كيف يمكننا تدريب جهات إنفاذ القانون لدينا للتصدي لهجمات المجرمين؟

كارلوس ألفاريز: أعتقد أن المسار السليم قد يكون هو التواصل مع موظفي ICANN العاملين في أفريقيا. أعتقد أنه بيير. أنا لا أعرف ما إذا كنتم قد قابلتموه بالفعل. اعرض مخاوفك عليه.

ما سيحدث بعد ذلك هو أن بيير، مع فريق الأمن والاستقرار والمرونة لدينا، سيقوم بالتنسيق والمشاركة مع وكالات إنفاذ القانون في التدريب على إساءة استخدام نظام DNS. لذا، فإن اقتراحي هو التواصل مع بيير لأن ذلك الأمر مهم جدا.

نعم سيدي؟

برنت كاري: برنت كاري من نطاق .nz. إنني أتساءل عما إذا كنت قد حصلت على أي روابط خاصة بالإنترنت والولاية القضائية. في الأسبوع الماضي جئت من أوتاوا وكان هناك سلالة لاسم النطاق. من الواضح، أنه يتم دمج كل ما يتعلق بسوء استخدام البنية الأساسية والتسجيل والمحتوى معا. كنت أتمنى فقط أن يكون لديك بعض الروابط هناك أيضا.

كارلوس ألفاريز: ليس لدي أي منهم. استنتج أنت. لكن نعم، أعلم أنه سبق لنا محاولة تنظيم هذا المنتدى في أوتاوا. وبعض زملائي في ICANN كانوا حاضرين هناك.

برنت كاري: يرجع ذلك لأنه كان هناك غياب ملحوظ بشدة لمنطقة إنفاذ القانون.

كارلوس ألفاريز: حسنا. لم أكن أدري. ربما تكون تلك محادثة خاصة بمجموعة عمل الأمن العام. شكرا لكم.

برنت كاري: شكرا لكم.

كارلوس ألفاريز: حسنا. انتظر، هناك شخص آخر.

شخص غير محدد: بجوارها مباشرة] لن أذكر أننا لا نملك آلية قوية [غير مسموع] للقواعد العامة لحماية البيانات هذه لنظام WHOIS. بطريقة أخرى، لا نملك السيطرة على هذه القضايا الأمنية. سيكون الأمر صعبا ولكن يبدو أنه مألوف [مستمرا].

كارلوس ألفاريز: ما الذي سيكون صعبا؟

شخص غير محدد: ليس لدينا نظام WHOIS حقيقي وذلك من أحد الجوانب. فربما لن نكون قادرين على رؤية من القادم إلينا وإلى أين نحن متجهون من خلال القواعد العامة لحماية البيانات هذه.

كارلوس ألفاريز: هذا صحيح.

شخص غير محدد: ثانيا، ليس لدينا أمن يتعلق بنظام DNS. ونحن لا نسيطر على ذلك. لذلك، لا يوجد سيطرة أو حقيقة للشخص الذي سنتجه إليه.

كارلوس ألفاريز: لننتظر. اقتراحي لك هو المشاركة في هذه المناقشات وتقديم التعليقات من خلال مكالمات من مؤسسة ICANN. وعادة ما يكون المدير التنفيذي هو من يدعو الأفراد لتقديم تعليقات مؤخرا. لذلك عليك المشاركة، لأن هذه هي الطريقة التي يمكن من خلالها سماع صوتك. وهذا أمر معروف بالفعل. فهو لا يمثل تعبير بلاغي. إنه أمر معروف. لذا، تخلص من مخاوفك هناك. وهذا هو المكان المناسب.

هذه هي بعض الجلسات. وعلى كل حال، هذه هي الجلسة الوحيدة التي تتعلق بإساءة استخدام نظام DNS. يجب أن تضع ذلك في الاعتبار. إذا استطعت العودة في الوقت المناسب، ستتمكن من الانتقال إلى الأمس الساعة 11:30 للحصول على تحديث مجموعة عمل الأمن العام. أما اجتماع اللجنة الاستشارية الحكومية لمجموعة عمل الأمن العام فسيحين غدا الساعة 8:30 صباحا. أود أن أوصيك بحضور هذين الاجتماعين في الصباح.

نعم، لدي تفضيل طفيف للقواعد العامة لحماية البيانات، وذلك لأننا عند هذه المرحلة المهمة من الأمور. ولكن كلا الاجتماعين سيكونان مثيرين للاهتمام.

بعد ذلك، سيكون من المثير للاهتمام معرفة الدور الذي يقوم به مجال اسم النطاق في مبادرة النطاقات السليمة. ومن الجيد أن ترى ما يفعلونه لأنهم يضطلعون بتنفيذ أمور مثيرة للاهتمام أيضا.

تعد DAAR إحدى الأدوات التي طورها فريقي. فهي توفر معلومات حول التسجيلات السيئة وكيفية تجميعها بشكل أكبر في جزء واحد بدلا من أجزاء متعددة. ولذلك، سيكون هذا الأمر مثير للاهتمام أيضا. لن أقول الكثير عن ذلك لأنني أود منكم حضور هذه الجلسة بأنفسكم. لذا من فضلكم اذهبوا. واذهبوا إلى هناك واستمتعوا بالأمر.

حسنا. حسنا، شكرا جزيلا على الحضور هنا.

كاثي بيترسين: مجرد تذكير: تعد شرائح العرض التقديمي في هذه الجلسة موجودة بالفعل في الجدول العام. وسنقوم بإضافة النصوص علاوة على تسجيل هذه الجلسة أيضا في الجدول العام خلال الأيام القليلة المقبلة. لذلك، يمكنك العودة مرة أخرى ورؤية كل شيء مرة ثانية.

شكرا جزيلا. سننظم جلسة "كيف يعمل ذلك" التالية على شبكة الإنترنت في الساعة 3:30. ليس 3:15، ولكن 3:30 تماما. ونعتذر، لأننا سنكون متأخرين قليلا عن موعد جلسة "كيف يعمل ذلك" التالية. ستدور الجلسة على شبكة الإنترنت عن الكثير من الحديث عن بروتوكولات IPv4 وIPv6.

أرجو أن تتمكنوا من التجول واحتساء بعض القهوة ثم العودة. شكرا لكم.

[نهاية النص المدون]