ICANN72 | أسبوع الإعداد - تقديم مجموعة عمل الدراسة الفنية لتيسير أمن نظام DNS (DSFI-TSG)
الخميس، 14 أكتوبر, 2021 – من الساعة 01:00 م إلى الساعة 02:00 م بالتوقيت الصيفي للباسيفيكي

ويندي بروفيت: ...إلى الجلسة التي تقدم مجموعة عمل الدراسة الفنية لمبادرة تيسير أمن نظام .DNS أسمي ويندي بروفيت وأنا مدير المشاركة عن بُعد لهذه الجلسة.

يُرجى العلم بأن هذه الجلسة يجري تسجيلها وتتبع معايير السلوك المتوقعة في ICANN. أثناء هذه الجلسة، ستتم قراءة الأسئلة أو التعليقات بصوت عال فقط إذا قُدمت في مربع الأسئلة والأجوبة. وسنقرأها عليكم بصوتٍ عالٍ في الوقت الذي يحدده رئيس هذه الجلسة أو مديرها.

ستتضمن الترجمة الفورية للجلسة خمس لغات. اضغطوا فوق رمز الترجمة الفورية في برنامج زووم Zoom وحددوا اللغة التي ستستمعون إليها أثناء هذه الجلسة.

إذا رغبتم في التحدث يرجى رفع يدكم في غرفة زووم. هذا لأعضاء اللجنة وسيقوم ميسر الجلسة بالمناداة على اسمك. وقبل التحدث، تأكدوا أنكم حددتم اللغة التي ستتحدثون بها من قائمة الترجمة الفورية، إذا كنتم ستتحدثون أي لغة أخرى غير الإنجليزية. وأيضًا، يرجى التعريف بأنفسكم من أجل التسجيل وتحديد اللغة التي ستتحدثون بها. وعند التحدث يتعين التأكد من كتم صوت جميع الأجهزة والإشعارات الأخرى. ويُرجى التحدث بوضوح وبسرعة معقولة للسماح بالترجمة الدقيقة.

يرجى استخدام القائمة المنسدلة في مربع الدردشة إذا كنتم ترغبون في التواصل من خلال الدردشة، والتأكد من تحديد "Respond to All Panelists and Attendees" (الرد على جميع أعضاء اللجنة والحضور). فسيتيح ذلك للجميع الاطلاع على تعليقك. ويُرجى ملاحظة أن الدردشة الخاصة ممكنة فقط بين أعضاء اللجنة بتنسيق ندوات Zoom عبر الويب. أي رسائل يرسلها أي عضو في اللجنة أو مشارك عادي إلى مشارك عادي آخر سيراها أيضًا مضيفو الجلسة والمضيفون المشاركون وأعضاء اللجنة الآخرون.

لعرض النسخ في الوقت الحقيقي، انقر فوق زر التسمية التوضيحية المغلقة في شريط أدوات برنامج زووم Zoom. وبهذا أترك الكلمة لجون كرين.

ملاحظة: مايلي هو ما تم الحصول عليه من تدوين ماورد في الملف الصوتي وتحويله الى ملف كتابي نصّي. ورغم أن تدوين النصوص يتمتع بدقة عالية، إلا إنه في بعض الحالات قد تكون غير مكتملة أو غير دقيقة بسبب المقاطع غير المسموعة والتصحيحات النحوية. تنشر هذه الملفات لتكون بمثابة مصادر مساعدة للملفات الصوتية الأصلية، ولكن لاينبغي أن تُعامل كما لو كانت سجلات رسمية.

جون كرين: شكرًا جزيلاً لك، ويندي. مساء الخير، وصباح الخير وطاب مساؤكم، جميعًا. أولاً، أود أن أنقل اعتذاري من غوران ماربي الذي كان يأمل أن يتمكن من التحدث في هذا الأمر ولكنه كان مشغولًا للأسف بأشياء أخرى، وطلب مني أن أقول بضع كلمات نيابة عنه. معكم جون كرين. أنا رئيس الأمن والاستقرار والمرونة في ICANN وأيضًا كبير مسؤولي التكنولوجيا المؤقت وقد شاركت بشكل كبير في هذه المبادرة. كما يعلم الكثير منكم، فإن أمان واستقرار ومرونة أنظمة المعرفات هي جوهر مهمة ICANN، حيث توجد في المقدمة والوسط في لوائحنا الداخلية وفي كل ما نقوم به.

اتصل بي غوران أثناء عملي منذ حوالي عامين والآن بعد سلسلة من الهجمات سألني كيف يمكننا كمؤسسة ICANN تسهيل الأمن بشكل أفضل في أنظمة المعرفات. كانت العملية التي توصلنا إليها هي تشكيل مجموعة دراسة فنية مع خبراء من داخل مجتمع ICANN وخارجه في مجال الأمن. تلقى غوران تقريرًا من مجموعة الدراسة الفنية في وقت سابق من هذا الأسبوع، ونعتزم نشر هذا التقرير على موقع الويب الخاص بـ ICANN في وقت مبكر من الأسبوع المقبل، جنبًا إلى جنب مع مدونة قصيرة المدى من غوران. أود أن أشكر المجموعة نيابة عن غوران على هذا العمل الشاق. يعمل المتطوعون على هذه السلسلة من التوصيات منذ أكثر من عام حتى الآن. لقد شاركت شخصيًا لذا شاهدت مدى صعوبة عمل هؤلاء المتطوعين ولا يمكننا شكرهم بما فيه الكفاية.

سوف نأخذ هذه المدخلات كمنظمة، والحافز للمدير التنفيذي، وسوف ندرسها بعناية. وسنعود بسلسلة من الأفكار حول كيفية استخدام هذه المعلومات لتسهيل أمان DNS بشكل أفضل. بهذا، أود أن أسلم الكلمة إلى ميريك كاو الذي عرض بلطف تنسيق هذه الجهود، وهو ما كان قبل عام ونصف تقريبًا. ميريك، إليك الكلمة تفضل.

ميريك كاو: أجل. شكرًا جزيلًا لك، جون. لذا فإن جلسة اليوم - هذا هو جدول أعمال الدورة - سأقدم بإيجاز شديد إجمالي العمل الذي قمنا به خلال العام ونصف العام الماضيين. وبعد ذلك سنستمر في جوهر العمل الذي سيناقش ناقلات الهجوم في نظام DNS البيئي، والتخفيف، وأخيرًا، التوصيات، ثم نترك بعض الوقت للأسئلة. سيكون لكل قسم من هذه الأقسام عضو مختلف من TSG ليتحدث. الشريحة التالية، من فضلك. الشريحة التالية.

كما ذكر جون، بدأ هذا العمل في مايو من العام الماضي وكان مبادرة قادها وأنشأها الرئيس التنفيذي لـ ICANN. كانت لتنفيذ التزامه بالعمل مع المجتمع لتعزيز التعاون والتواصل بشأن قضايا الأمن والاستقرار. في المقام الأول، كان العمل يهدف إلى تقديم بعض التوصيات حول ما يمكن وما ينبغي أن تقوم به ICANN لتحسين ملف أمان DNS. وأيضًا، هل هناك أي شيء لا ينبغي أن تقوم به ICANN على وجه التحديد؟ الشريحة التالية، من فضلك.

لذلك كما ذكر جون، كان جزء من هذه المبادرة أو معظمها يرجع حقًا إلى بعض الهجمات المعقدة للغاية التي كانت تحدث قبل بضع سنوات. وأدركنا أو أدركت ICANN أن الاستجابة لبعض هذه الهجمات المعقدة كانت مخصصة. ويجب أن تكون هناك طريقة لإنشاء مزيد من البنية حول كيفية الرد على هذه الهجمات عبر نظام الإنترنت البيئي والنظر في المكان الذي يجب أن يكون فيه مستوى جديد من التعاون والفهم ضروريًا. الشريحة التالية، من فضلك.

إذن، تُظهر هذه الشريحة الجدول الزمني العام لـ TSG. بدأ العمل في مايو وقمنا بصياغة عضوية TSG. عقد الاجتماع الأول في 16 يونيو من العام الماضي. كان معظم العمل في الصيف هو تحديد النطاق وبعض الأسئلة الأساسية التي أردنا معالجتها. ثم بدأ الجزء الأكبر من العمل في أوائل الخريف واستمر حتى مايو من هذا العام، حيث استند الجزء الأول من المناقشات حول الأسباب الجذرية ونواقل الهجوم. ثم أنشأنا قائمة أولويات حول نواقل الهجوم الخاصة هذه لمعرفة أي منها كان أكثر جدية ويحتاج حقًا إلى الاهتمام لمعالجته. نظرنا إلى عوامل التخفيف التي كانت موجودة أو التي كانت موجودة ولكن لم يتم تفعيلها وأيضًا عمليات التخفيف التي قد تكون مفقودة. ثم أنشأنا مسودة الوثيقة. بمجرد الانتهاء من ذلك وكان لدينا بعض مسودات التوصيات، أجرينا مشاورات فنية مع بعض خبراء الصناعة، ثم أنتجنا التقرير النهائي وأرسلناه إلى غوران في وقت سابق من هذا الأسبوع. الشريحة التالية، من فضلك.

إذن هذه هي عضوية TSG. هناك تسع عناصر. وكما سترون، فهي مجموعة متعددة الوظائف من الخبراء الذين لديهم خبرة عميقة وخبرة في تشغيل البنى التحتية لنظام أسماء النطاقات DNS في الاستجابة لحوادث الأمان، والمعرفة الأمنية العامة، وعمليات التسجيل / المسجل، وعمليات تسجيل رمز الدولة، وأيضًا تجربة CDN و ISP. وأيضًا الخبرة الفنية المتعمقة في DNS. لذلك كانت الخبرة الوظيفية المتقاطعة واسعة وعميقة إلى حد ما. الشريحة التالية، من فضلك.

كما ذكرت، أجرينا أيضًا مراجعة استشارية فنية لمسودة الوثيقة، وهؤلاء هم الأفراد الذين قدموا تعليقات مستفيضة للغاية. إن TSG ممتن للغاية للمراجعة المتعمقة التي تم تقديمها لأنها أسفرت عن تقرير نهائي وتوصيات أكثر ثراءً. الشريحة التالية، من فضلك.

كان هناك أيضًا دعم من ICANN على مستويات متعددة. كانت هناك لجنة توجيهية في DSFI TSG تتألف من أربعة أعضاء مجلس إدارة واثنين من المديرين التنفيذيين. لقد حصلنا على دعم مكثف للغاية للعمل من ICANN لإدارة البرنامج والاتصالات وأيضًا الخبرة الفنية في الموضوع. وبعد ذلك، كان لدينا كاتبة فنية ممتازة، والتي، بمهاراتها، حولت موضوعًا معقدًا للغاية إلى تقرير ستجده عند الوصول إليه، إنه سهل القراءة للغاية. الشريحة التالية، من فضلك.

تعرض هذه الشريحة اتساع وعمق نظام DNS البيئي الشامل. كان من المتوقع أن يستغرق العمل سنة، فاستغرق سنة ونصف في الواقع. لقد تم إنجازه بشكل افتراضي بنسبة 100%، مما خلق تحدياته الخاصة. وأريد شخصيًا أن أشكر كل عضو في TSG وموظفي دعم ICANN لأن لدينا اجتماعات عديدة، وكذلك ورش عمل استمرت لمدة ساعتين أو ثلاث ساعات كل أسبوعين للوصول إلى النتيجة النهائية حقًا. إنه موضوع مثير للغاية. لكن مرة أخرى، أنا فخور جدًا بالعمل النهائي الذي توصلنا إليه بالفعل. لذلك دون مزيد من اللغط، فلنبدأ في مناقشة أهم ما في الأمر وسنبدأ بالهجوم. الشريحة التالية، من فضلك. جافين، خذ الكلمة.

جافين براون: بالتأكيد أجل، نعم. شكرًا يا ميريك. لذلك سيتحدث هذا القسم من العرض التقديمي عن بعض نواقل الهجوم التي بحثنا فيها، وننظر أيضًا في المنهجية التي استخدمناها عند النظر في تحليلها. إذن هلا انتقلنا إلى الشريحة التالية رجاء.

تهدف هذه الشريحة إلى توضيح - بمعنى مشابه للشريحة التي أظهرها ميريك للتو - عمق واتساع أو نطاق الأنظمة التي كنا ننظر إليها من حيث التهديدات ونواقل الهجوم ضدها. لذلك نحن نغطي - سترى كلا من جانب نظام أسماء النطاقات وجانب التزويد أيضًا. لذلك يوضح هذا الرسم التخطيطي العناصر الموجودة في مسار تحليل DNS من وحدات حل المشكلات إلى الخوادم الاستنادية ولكن أيضًا في جانب التوريد أيضًا. وهذا يشمل المستخدمين النهائيين

كمسجلين، والأنظمة التي يتفاعلون معها لتوفير أسماء النطاقات، والبروتوكولات بين السجلات والمسجلين وكذلك الوسطاء مثل الموزعين. لذا كان القصد من ذلك تغطية كل هذه الأنظمة المختلفة وإلقاء نظرة على جميع ناقلات الهجوم المختلفة التي يمكن أن تهدد تلك الأنظمة. الشريحة التالية، من فضلك.

لذا فإن العملية التي مررنا بها، تشبه إلى حد كبير في تجربتي تحليل المخاطر حيث نظرنا إلى مختلف ناقلات الهجوم المحتملة وحاولنا تصنيفها والتوصل إلى قواسم مشتركة بينها. لذلك تحدثنا عن كل من ناقلات الهجوم المحددة واستخرجناها من الحوادث التي شهدنا تجربة العالم الحقيقي منها. وبعد ذلك عندما نظرنا إلى كل ناقل هجوم، نظرنا في عدد من الأسئلة المختلفة حول وسائل التخفيف التي قد تكون متاحة - سنتحدث عن عمليات التخفيف لاحقًا - أين قد تكون الفجوات، وما إذا كانت المشكلات متعلقة بالفهم غير الكامل للمخاطر، وما إذا كانت البنية التحتية لنظام أسماء النطاقات، ونظام DNS نفسه معرضًا بشكل فريد لأنواع معينة من المشكلات التي لم تكن تعاني منها أجزاء أخرى من النظام البيئي للإنترنت. الشريحة التالية.

لذا على مستوى عالٍ، توصلنا إلى عدد كبير نسبيًا من ناقلات الهجوم التي قمنا بتكثيفها في تلك التي سترونها هنا. إنها واسعة جدًا وستلاحظون أن بعضها عام نوعًا ما لأن المشاركين في نظام DNS البيئي، وهم مؤسسات، وشركات مثل أي شركة أخرى، ولديهم نفس تحديات الأمان مثل كل شركة أخرى، سواء كنت بنكًا أو مغسلة سيارات أو مشغل gTLD. بعضها فريد بالنسبة إلى DNS وأيضًا فريد بالنسبة للبروتوكولات والأنظمة التي يستخدمها المشاركون في النظام. لذلك سترى أننا نغطي أشياء مثل اختيار TTL في السجلات، ولكن أيضًا الأشياء الأساسية فقط مثل مدى جودة سياسات كلمة المرور وما إلى ذلك. ثم تم تكثيفها بشكل أكبر في الناقلات الموضحة في الشريحة التالية. يمكننا المضي قدما من فضلك.

لذلك تم تكثيفها في هذه الفئات من ناقلات الهجوم. مرة أخرى، سنتحدث عن بعض هذه الأشياء بمزيد من التفصيل، بدءًا من تلك التي تعتبر عامة تمامًا بشكل عام. لذا، تعد إدارة الهوية والوصول تحديًا أمنيًا ليس فريدًا في عالمنا. يجب على كل شركة لديها جهاز كمبيوتر في مكان ما أن تفكر في هذا الأمر. نفس الشيء مع التحكم في الوصول والترخيص. هناك بعض المجالات التي تكون خاصة بنظام DNS. ومع ذلك، هناك أشياء مثل انتحال هوية الموارد، والمشكلات المتعلقة برفض الخدمة وأيضًا المشكلات المتعلقة بالثغرات الأمنية، سواء

في التنفيذ في التعليمات البرمجية ولكن أيضًا في البروتوكولات نفسها. والاختيارات التي اتخذناها عندما نبني البنية التحتية التي تجعل الأنظمة عرضة للاختراق والتي قد لا تتوقع المضي قدمًا فيها. هل يمكننا الانتقال إلى الشريحة التالية، رجاءً؟

بدءًا من الأول، إدارة الهوية والوصول، توجد بيانات الاعتماد في كل مكان في البنية التحتية ونظام التزويد، وكذلك في النظام الرسمي أيضًا. يتم استخدامها لمصادقة التفاعلات بين المشاركين. لذلك إذا كنت موظفًا في السجل، فستستخدم اسم المستخدم أو كلمة المرور لتسجيل الدخول إلى نظام الإدارة الخاص بالسجل. إذا كنت مسجلاً، فستستخدم اسم مستخدم وكلمة مرور للوصول إلى نظام EPP الخاص بالسجل. إذا كنت موظفًا في السجل، فأنت تدخل إلى أنظمته باستخدام اسم المستخدم وكلمة المرور الخاصين بك وما إلى ذلك وهكذا، وصولاً إلى المستخدم النهائي. أي نقطة في هذا النظام، بيانات الاعتماد هذه عرضة للتسوية. ويتعين على المنظمات المشاركة في إدارة بيانات الاعتماد هذه اتخاذ قرارات بشأن تنفيذ السياسات لحمايتها من أنواع الهجمات التي تتوقع رؤيتها - إظهار كلمات المرور، وإعادة استخدام كلمات المرور، والتصيد الاحتيالي، وما إلى ذلك. لذلك كان هذا هو محور عملنا في هذا المجال، مع التركيز بشكل خاص على بيانات اعتماد المسجلين، والمصادقة بين السجلات والمسجلين والبائعين، والتهديد باستخدام بيانات الاعتماد المخترقة لبدء المعاملات مع السجل عن طريق انتحال شخصية أحد الكيانات في السلسلة بين المسجل والسجل. الشريحة التالية، من فضلك.

إذن هنا مثال على عدم كفاية مسألة إذن التحكم في الوصول. هذا يتعلق حقًا بالاستيلاء على النطاق الفرعي. هذا هو السيناريو حيث يوجد سجل داخل اسم النطاق الذي يحتوي على اسم مستعار أو سجل CNAME الذي يشير إلى بعض الموارد الأخرى. يسمح هذا بموقف يمكن فيه للمهاجم بشكل أساسي التحكم في اسم النطاق هذا دون الكثير من التحقق من أنه في الحقيقة الشخص الذي يمتلك النطاق. الشريحة التالية، من فضلك.

يتعلق ناقل الهجوم التالي بانتحال صفة المورد. هذه طريقة يمكن للمهاجم من خلالها إعادة توجيه استعلامات DNS إلى طرف ثالث. يمكن أن يكون لهذا الاتجاه عدد من الآثار المختلفة اعتمادًا على مكان حدوثه في النظام. لذلك يمكن القيام بذلك في بعض الأحيان كجزء من الاستخدام المشروع. لذا فإن البوابات المقيدة - مكان شائع تمامًا حيث يتم اعتراض حركة مرور DNS التي تهدف إلى الخروج من الشبكة من خلال تلك الشبكة من أجل تقديم نموذج

تسجيل دخول للمستخدم للبوابة المقيدة. لكن يمكن أن يكون أيضًا نتيجة نشاط ضار، على سبيل المثال، عن طريق تثبيت برامج ضارة على الكمبيوتر أو جهاز المستخدم النهائي عن طريق اعتراض نشط على الشبكة. لذا فإن بعض الطرق التي يمكن بها تنفيذ ذلك من خلال تمثيل وحدة الحل التكراري، عن طريق تمثيل الخادم الرسمي الذي هو خوادم متكررة تقع بين المستخدم النهائي ومصدر بيانات المنطقة الرسمية.

النطاقات المشابهة أو نطاقات الفاكس. قد يختلف هذا إلى حد ما عما قد تقوله - هذا ليس مجرد تصيد احتيالي ولكنه يختلف إلى حد ما من حيث أن الهدف في هذه الحالة هم مستخدمي البنية التحتية وليس المستخدمين النهائيين لخدمات المستهلك. كما تم اعتبار الشهادات الصادرة الاحتيالية والتلاعب بالجذر جزءًا من ناقل الهجوم هذا. فلننتقل إلى الشريحة التالية.

هذا مثال على ما نتحدث عنه مع نطاق الفاكس. الهجمات المتجانسة هي أوضح مثال على هذا الشكل من ناقلات الهجوم.

كان ناقل الهجوم التالي الذي تحدثنا عنه هو الثغرات الأمنية في التعليمات البرمجية والبروتوكول. هناك مشكلات وتحديات مختلفة نتعامل معها مع هذين النوعين المختلفين من نقاط الضعف عندما تكون هناك مشكلة في برنامج DNS. هذه هي الطريقة التي يتم بها التخفيف بشكل واضح مختلف تمامًا عن الطريقة التي يتم بها تخفيف ثغرة البروتوكول. لأنه عندما تكون هناك مشكلة في بروتوكول DNS، كما رأينا، ليس مؤخرًا، ولكن مع عدد من الثغرات الأمنية حول أشياء مثل SADDNS، وبالطبع، أشهر هجوم كامينسكي. تغيير البروتوكول الخاص بك له آثار التشغيل البيني. إذا قمت بتغيير البروتوكول الخاص بك دون تنسيق دقيق مع جميع المشغلين والمنفذين المختلفين، فأنت معرض لخطر زعزعة استقرار النظام. لكنها تحتاج إلى المعالجة ويمكن أن يكون لها تأثير سلبي على الأنظمة المعرضة للخطر. وكما ترون، فإن أشياء مثل تسمم ذاكرة التخزين المؤقت ذات صلة خاصة في حالة ثغرات البروتوكول. الشريحة التالية.

هذا مثال على كيفية عمل تسمم ذاكرة التخزين المؤقت. كما سترون - أعتقد أننا فقدنا الأسهم. هل ترونهم؟ ها هم. لذا فهي مرئية في الشريحة التالية.

لذلك عندما يتلقى الخادم التكراري استعلامًا من مستخدم نهائي، لذلك يبحثون عن icann.org ويكون المهاجم النشط قادرًا على اعتراض هذا الاستعلام أو إرسال استجابة احتيالية مخادعة مرة أخرى إلى الخادم التكراري قبل الإجابة من الخادم الموثوق يمكن أن يستقبلها الخادم التكراري الذي ينتهي بإرسال الإجابة المخادعة إلى المستخدم النهائي قبل تلقي الاستجابة القانونية من قبل الخادم التكراري من الخادم الموثوق الصحيح. فلننتقل إلى الشريحة التالية.

اختيارات البنية التحتية. هذه قرارات يتخذها مشغل نظام DNS أو خدمة DNS والتي يمكن أن يكون لها عواقب غير مقصودة فيما يتعلق بأمن هذا النظام وتوافره. TTL هي مثال جيد على ذلك. ومن الواضح أننا قمنا بإدراج كل من TTL الطويلة وTTL القصيرة كمشكلات هنا. لذا فالأمر يتعلق حقًا بـ Goldilocks TTL بأنه ليس قصيرًا جدًا، وليس طويلًا جدًا، ولكن في المنتصف تمامًا. هناك سيناريوهات يكون فيها TTL القصير مفيدًا ومناسبًا. وهناك سيناريوهات يكون فيها TTL الطويل مفيدًا ومناسبًا. لكن العواقب غير المقصودة تعني أنك بحاجة إلى إجراء تقييم دقيق للمخاطر للتأكد من أن عواقب تلك القرارات لن تعود وتؤثر عليك. لذا إذا كان بإمكاننا الانتقال إلى الشريحة التالية لتوضيح ذلك فقط.

إذن هذا هو السيناريو الذي تم فيه تنفيذ TTL على سجل على خادم رسمي. يضمن TTL أن المستخدمين النهائيين سيستمرون في تلقي الاستعلامات أو الإجابات على الاستعلامات داخل مساحة TTL حيث سيتم توفير السجل المخزن مؤقتًا بواسطة المحلل. ولكن إذا كان المهاجم قادرًا على اعتراض الاستعلام إما عن طريق اختطاف اسم النطاق أو عن طريق أحد الناقلات الأخرى التي تحدثنا عنها في هذا القسم، فسيتم تخزين الإجابة الخبيثة مؤقتًا لتلك الفترة وسيظل المستخدمون عرضة للخطر ليتم استغلالها من خلال TTL تلك حتى انتهاء صلاحية السجل ويمكن استرداد الإجابة الصحيحة من الخادم الموثوق. الشريحة التالية.

لذلك تحدثنا عن DNS باعتباره ناقل هجوم بحد ذاته. لا يتعلق هذا في المقام الأول بأشياء مثل استخراج البيانات واستخدام DNS كقناة سرية. غالبًا ما يُسمح لـ DNS بالعبور والخروج من الشبكة دون أن يتم تصفيته أو حظره، ويتم استغلال ذلك بعدة طرق مختلفة للسماح للمهاجمين إما بالتسلل إلى نظام أو سرقة البيانات من ذلك النظام إلى الخارج. الشريحة التالية، من فضلك.

أخيرًا، تحدثنا عن رفض الخدمة. هذا بالنسبة لأي مشغل للبنية التحتية لنظام DNS يمثل تحديًا ومشكلة مستمرة وهائلة. نظرًا للطريقة التي يعمل بها بروتوكول DNS، فإن استخدام UDP يعني أن خدمات DNS معرضة لهجمات الانتحال، وهي عرضة لهجمات التضخيم والانعكاس. يمكن أن تؤدي هجمات رفض الخدمة على مزودي DNS إلى تعطيل عمل المزيد من المؤسسات بشكل كبير، ثم يكون هذا هو الحال إذا كان هذا الهدف هو المشغل لخوادم جذر التسجيل أو خدمة المسجل وليس مجرد مستخدم نهائي يتعرض لهجوم رفض الخدمة. الشريحة التالية، من فضلك.

بهذا نختتم عرضنا العام لناقلات الهجوم. سأنتقل إلى أحد زملائي للتحدث عن التخفيفات. دووين؟

دووين ويسلز: مرحبًا بالجميع. أنا دووين ويسلز وسأنتقل إلى قسم التخفيف في هذا العرض التقديمي وتقريرنا. الشريحة التالية، من فضلك.

كما تحدث جافين عن بعض الهجمات بالفعل، نقضي أيضًا وقتًا في المجموعة نتحدث عن طرق يمكن من خلالها تخفيف هذه الهجمات، وتوصلنا إلى الكثير من الأشياء المختلفة. بعضهم لم يدخل في الواقع في التقرير النهائي ولكني هنا للحديث عن تلك التي وصلت إلى التقرير. الشريحة التالية.

لقد أمضينا الكثير من الوقت في المجموعة نتحدث عن المصادقة والكثير من التوصيات وعمليات التخفيف التي ستراها تتعلق بضوابط الوصول والمصادقة. لذا فإن أحد أفضل الأشياء التي يمكن للأشخاص القيام بها للحفاظ على أمان موارد DNS هو استخدام كلمات مرور معقدة. هناك عدد من الحالات التي أدت فيها كلمات المرور البسيطة للغاية إلى التعرض للخطر. على غرار كلمات المرور المعقدة، يمكن للأشخاص استخدام بيانات اعتماد الاستخدام لمرة واحدة أو المصادقة متعددة العوامل. وبالطبع، نظرًا لأن بيانات الاعتماد وكلمات المرور الخاصة بنا تصبح أكثر تعقيدًا، يصبح من الضروري تقريبًا استخدام نوع من إدارة كلمات المرور حيث يكون هذا هو الشيء الذي يتذكر كلمات المرور الخاصة بك بدلاً من محاولة تذكرها بنفسك.

تحدثنا عن الوعي بالمخاطر، والذي يشير حقًا إلى إدراك الطرق المختلفة التي يمكن أن تتعرض فيها بيانات الاعتماد للخطر، على سبيل المثال، بهجمات التصيد الاحتيالي. تحدثنا عن مدى توفر واستخدام الخدمات التي يمكن أن تمنع كلمات المرور الضعيفة. لذلك، على سبيل المثال، قد يكون هناك بعض الرموز التي يمكن أن تخبرك ما إذا كانت كلمة مرور معينة قوية بما يكفي أو لها متطلبات قوة معينة أم لا. هناك أيضًا قواعد بيانات لكلمات المرور المعروفة التي تم اختراقها والتي يمكنك التحقق منها. من الجيد دائمًا افتراض أن الأشرار يمكنهم الوصول إلى قواعد البيانات هذه أيضًا. لذلك لا تريد استخدام كلمات المرور التي تم اختراقها بالفعل في مكان آخر.

تحدثنا عن بعض الحلول العلاجية التي يمكن أن تحدث في حالة وقوع هجوم. أخيرًا، تحدثنا عن الطرق التي يمكن من خلالها التحقق من المجالات والمسجلين والتحقق من صحتها للعملاء المحتملين عند تقديم طلبات الخدمة. الشريحة التالية، من فضلك.

التخفيفات من حيث التوافر والنزاهة والخصوصية. أود أن أقول إن بعضًا من هؤلاء معروفون جيدًا بالفعل. بالنسبة للتوافر، أعتقد أن الكثير من الناس يعرفون أن نقاط الفشل الفردية هي فكرة سيئة حقًا. غالبًا ما نفكر في هذا من حيث الشبكات وخدمات الشبكة. لا تضع جميع خوادم DNS الخاصة بك على نفس الشبكة أو في نفس مركز البيانات، على سبيل المثال. ولكن هناك بالطبع أنواع أخرى من نقاط الفشل الفردية التي قد تفكر فيها مثل استخدام نوع واحد فقط من البرامج أو حتى نوع واحد من الأجهزة، وما إلى ذلك. أيضًا، كما تم توضيحه للكثير من الأشخاص في هجوم Dyn المعروف جيدًا، إذا كنت تستخدم خدمات DNS ثانوية، فمن الجيد عادةً نشر ذلك بين الأنظمة الأساسية المختلفة. لأنه، مرة أخرى، إذا كان لديك نظام أساسي واحد وتعطل هذا المزود، فقد لا يحالفك الحظ.

فيما يتعلق بالنزاهة، فإن أحد أفضل وسائل التخفيف بالطبع هو DNSSEC لتوقيع المجالات وتنفيذ DNSSEC على كل من جانب النشر وعلى جانب القرار لتنفيذ التحقق من الصحة. يعد قفل السجل وبعض هذه المنتجات المماثلة أفكارًا جيدة حقًا لمنع الاستيلاء على النطاق، إذا كانت متوفرة لك. ثم تحدثنا أيضًا عن استخدام بعض البروتوكولات الأحدث مثل بروتوكولات CDS و CDNSKEY و CSYNC التي تسهل بشكل أساسي نقل مواد DNSSEC بين منطقة فرعية ومنطقة أصل.

فيما يتعلق بالخصوصية، من الواضح أنه كان هناك الكثير من العمل مؤخرًا حول استخدام نقل DNS المشفر. لقد بدأنا في رؤية المزيد والمزيد من ذلك، وهذه طريقة جيدة حقًا لتطبيق الخصوصية في نظام أسماء النطاقات. التالية رجاءً.

بعض وسائل التخفيف الأخرى التي يجب أن يكون الناس على دراية بها هي المراقبة. يمكنك الاشتراك في خدمات حماية العلامة التجارية. من شأن ذلك، على سبيل المثال، تنبيهك إذا كانت العلامة التجارية الخاصة بشركتك واسم النطاق مسجلين في سجل آخر أو نطاق مستوى أعلى. ربما يكون هذا شيئًا قد ترغب في معرفته. شهادة الشفافية هي مشروع يجعل طلبات شهادة SSL متاحة ليراها الناس. هناك خدمات ستنبهك إذا كانت هناك شهادة صادرة لنطاقك. وإذا لم تصدر ذلك بنفسك، فهذا شيء ربما تريد أن تعرف عنه.

هناك سجلات تفويض لهيئة إصدار الشهادات، سجل CAA الذي يمكنك وضعه في منطقتك والذي يحدد المراجع المصدقة المسموح لها بإصدار الشهادات لنطاقك. هذه فكرة جيدة للنظر في ذلك.

فيما يتعلق بتوجيه RPKI وأصل المسار، فإن إعلانات المصادقة هي شيء يمكن أن يساعد في حماية شبكاتك من الإعلانات الخاطئة. يمكنك مراقبة هؤلاء أيضًا.

بالنسبة للمؤسسات التي تحتاج إلى تنفيذ أي نوع من فحص البيانات التي تم تمريرها إلى الشبكة، فربما تحتاج إلى التفكير في أجهزة التوجيه أو المحولات التي تم تحسينها لفحص الحزم العميقة ويمكنها إلقاء نظرة خاطفة على هذه الحزم وإبلاغ الأشخاص بما يمر عبر الشبكة.

بالنسبة لمطوري البرمجيات، تحدثنا عن الحاجة إلى وجود ممارسات دورة حياة تطوير برمجيات جيدة. هذا مجرد نهج قياسي لتطوير البرامج يقدم أفضل الممارسات الحالية للحفاظ على تحديث البرامج وتصحيحها واختبارها. وبالطبع، أنا متأكد من أن الجميع يعلم أنه من المهم تصحيح البرامج بانتظام، ليس فقط من وجهة نظر المستخدم ولكن أيضًا من وجهة نظر المطورين، لتحديث التصحيحات باستمرار وإصلاح المشكلات كلما تم العثور عليها. التالية رجاءً.

تشمل عمليات التخفيف المتعلقة بالتحكم في الوصول استخدام ما نسميه ببنيات الوصول القائمة على السلوك. على سبيل المثال، انعدام الثقة هو أحد هذه البنيات. لقد حظيت بالكثير من

الاهتمام مؤخرًا. من الجيد دائمًا تقسيم الخدمات المهمة. على سبيل المثال، افصل خدمات DNS الخاصة بك عن خدمات البريد الإلكتروني الخاصة بك، عن خدمات الويب الخاصة بك إلى أنظمة مختلفة بحيث إذا تعرضت إحداها للهجوم، فلن تؤثر على الأخرى. ضع في اعتبارك بالطبع ضوابط وصول أكثر تقييدًا للحسابات التي قد تكون أكثر حساسية.

في الحالات التي تكون فيها قادرًا على تقسيم الخدمات على وجه الخصوص، من الجيد تقييد الوصول إلى خدمات البيانات على منافذ نظام أسماء النطاقات فقط. هذا هو المنفذ 53، المنفذ 853 الآن مع TLS، وربما المنفذ 443 مع DNS عبر HTTPS. وإذا كنت تقوم بتشغيل محلل DNS، فهذا ليس مصممًا حقًا للاستخدام من قبل أطراف ثالثة، فتأكد من أن لديه عناصر تحكم وصول مناسبة تقصر استخدامه على المستخدمين الذين يجب أن يستخدموه فقط. التالية رجاءً.

مؤشرات لنقطة النهاية وضوابط الشبكة. يعد برنامج مكافحة الفيروسات شيئًا موجودًا منذ فترة طويلة ولا يزال مناسبًا لكثير من المستخدمين. لم نقض الكثير من الوقت في الحديث عن برامج مكافحة الفيروسات في التقرير ولكن كان هناك ذكر موجز لها هناك. تعني السيطرة الصارمة على اختيار محلل DNS أنه في هذه الأيام تتلقى الكثير من الأجهزة من الشبكة، من خادم DHCP، على سبيل المثال، يخبرهم خادم TCP عن المحلل الذي يجب استخدامه. هذا يعمل بشكل عام ولكن هناك أيضًا طرقًا يمكن للبرامج الضارة أو غيرها من نواقل الهجوم من خلالها تغيير خادم الاسم المتكرر الذي منحه الجهاز لشيء آخر. يريد مشغلو الشبكات الانتباه إلى ذلك. إما أن تحظر محللات DNS غير المصرح بها على جدار الحماية أو تقوم بإجراء فحوصات أخرى للتأكد من أن محلل DNS الذي يستخدمه الجهاز صحيح ومناسب. بالطبع، مرة أخرى، بالنسبة للمؤسسات القادرة على حماية مستخدميها، يعد شيء مثل جدار حماية DNS فكرة جيدة للتأكد حقًا من أن هؤلاء المستخدمين سيذهبون إلى وجهات مناسبة وآمنة فقط. التالية رجاءً.

حول عوامل التخفيف التي تحدثنا عنها في التقرير، تم تقسيمها إلى هذه الفئات التي غطيتها بالفعل في الغالب. بعض هذه، مرة أخرى، تحديات بيانات الاعتماد، وضوابط الوصول لحسابات المستخدمين، وما إلى ذلك. انتحال هوية المورد هو شيء تحدث عنه جافين، بالإضافة إلى الثغرات الأمنية في التعليمات البرمجية والبروتوكول. يتحدث التقرير عن

استخدام DNS كناقل للهجوم مقابل DNS كهدف. هجمات رفض الخدمة، بالطبع، وآليات الاستجابة للحوادث. أعتقد أن هذه هي الشريحة الأخيرة لي. أعطي الكلمة إلى مارك.

مارك روجرز: مرحباً. المايكروفون الخاص بي لا يعمل. حسنًا. الشريحة التالية. سأتحدث عن التوصيات التي خرجت من المناقشات التي أجريناها في المجموعة. هناك ارتباط واضح بالرجوع إلى نواقل الهجوم التي تمت مناقشتها والتخفيف من حدتها التي تمت مناقشتها. وهي تقع على نطاق واسع في هذه المجالات الخمسة: التحسينات التشغيلية، والبحوث، والتعاقد، والتمويل، والتعليم والتوعية. الشريحة التالية.

التوصية الأولى التي نتجت هي أن ICANN يجب أن تعمل مع منظمات أخرى مثل SSAC و GNSO و ccNSO و TLD Ops لإعداد برنامج للتمارين المنضدية. من خلال هذا البرنامج يجب أن يتم العمل على خلق فرص لممارسة الوظائف التشغيلية خلال المواقف الشبيهة بالحادث لتحديد الفجوات التشغيلية التي قد تظهر. من خلال القيام بذلك باستمرار، يمكن تحديد هذه الفجوات التشغيلية وتسجيلها وتتبعها بواسطة ICANN والهيئات الأخرى بحيث يمكن العمل عليها بعد ذلك والإبلاغ عنها في التوصيات المستقبلية. الشريحة التالية.

خرجت العديد من التوصيات البحثية بهذا. الأول حول إساءة استخدام DNS. مشهد التهديد ليس ثابتًا أبدًا. إنه يتطور باستمرار وكذلك إساءة استخدام نظام أسماء النطاقات. تقنيات الإساءة بالأمس تتطور وتصبح تقنيات جديدة غدًا. كما يتم فتح طرق جديدة مع نشر تقنيات مختلفة أو عند نشر بنيات DNS مختلفة. لذلك كانت توصيتنا هي أنه يجب علينا مواصلة البحث في إساءة استخدام نظام أسماء النطاقات للتأكد من أننا نتفهم دائمًا الشكل الحالي لإساءة الاستخدام وأين تتجه إساءة الاستخدام حتى نتمكن من المضي قدمًا في ذلك.

التوصية التالية هي أنه يجب علينا التحقيق في التوصية التي تقضي بضرورة التحقيق في تحسينات أمان DNS. وبالمثل، لأن مشهد التهديدات يتغير باستمرار، وكذلك تحسينات أمان DNS. مرة أخرى، نعتقد أنه يجب أن يكون هناك برنامج تم تطويره يبحث في حدود ومخاطر وفوائد تحسينات أمان DNS المختلفة. تم سرد عدد من هذه التحسينات أدناه في التقرير. لكن التفكير العام يشبه إساءة الاستخدام، فنحن بحاجة إلى مواكبة ذلك، نحتاج إلى الاستمرار في

مراقبته، ونحتاج إلى إنشاء دورة ملاحظات حيث يتم تحديد الثغرات، وتحديد التحسينات، وإعادتها باستمرار.

من خلال ربط المحادثات حول المصادقة في الأقسام السابقة، نعتقد أنه يجب أن يكون هناك تحقيق في أفضل الممارسات المناسبة للمصادقة. أعتقد أنه ينبغي على ICANN، جنبًا إلى جنب مع مجتمعات المنظمات الأخرى ذات الصلة، إجراء دراسة وتقديم تقرير حول ما يجب اعتباره أفضل ممارسة للمصادقة عند النظر في مقابل الأدوار والمخاطر المختلفة التي تواجه DNS. الشريحة التالية.

في العقود والتمويل، كانت توصية العقد تقضي بأن تعمل ICANN على تمكين الأطراف المتعاقدة على اعتماد تحسينات أمنية لأنظمة تسجيل النطاق وخدمات الأسماء الرسمية باعتبارها عملية. نعتقد أنه من خلال القيام بذلك، يمكننا ضمان وتمكين المنظمات لتنفيذ أمان DNS أقوى بكثير.

يركز البرنامج التالي على برامج مكافأة الإبلاغ عن الأخطاء. كان هذا موضوعًا حيويًا للمجموعة نظرًا لوجود الكثير من وجهات النظر حول المكان المناسب لمكافآت الإبلاغ عن الأخطاء ومدى فعاليتها وكيفية تبنيها. ما اتفقنا عليه جميعًا، على الرغم من ذلك، هو أن ICANN يجب أن تقود العمل في جدوى القيام ببرامج مكافأة الإبلاغ عن الأخطاء لـ DNS. نظرًا لوجود عدد من المجالات حيث، على سبيل المثال، البنية التحتية لنظام أسماء النطاقات غير مملوكة لمنظمة معينة أو لم تعد تتم صيانة البنية التحتية لنظام أسماء النطاقات، حيث سيكون من المفيد أن يكون لديك برنامج مكافأة الإبلاغ عن الأخطاء مُدار للتركيز على تلك المناطق والتركيز على تلك الأجزاء من البرامج لتحديد الثغرات الأمنية. الآن، نظرًا لأن هذا الموضوع يمثل تحديًا كبيرًا، نعتقد أن أفضل نهج هو إجراء دراسة جدوى حول هذا الموضوع للنظر في أفضل نهج، وإلقاء نظرة على النهج الأكثر فعالية من حيث التكلفة، والنظر في الكيفية التي يمكن بها تحويل الثغرات الأمنية إلى الكيانات الصحيحة للتأكد من معالجتها بالفعل. الشريحة التالية.

نعتقد أن هناك حاجة ماسة جدًا للتعليم والوعي. نعتقد أنه يجب على ICANN العمل على بناء وإيصال البرامج التعليمية التي تشجع أصحاب المصلحة في DNS على إنشاء آليات مصادقة قائمة على المعايير المناسبة لجميع التفاعلات التي يجب أن تتم المصادقة عليها. بالإضافة إلى

إبلاغ أصحاب المصلحة هؤلاء بالمخاطر المرتبطة بأنظمة المصادقة الضعيفة، وأن هناك الكثير من المصادقات القديمة التي يتم الاستفادة منها بسبب الجهل البسيط. ونعتقد أن هناك فرصة قوية من خلال التعليم والوعي للتحرك نحو أنظمة مصادقة أقوى بكثير.

قفل السجل. يجب أن تبذل ICANN جهودًا لتحسين التوثيق وفهم ميزات قفل السجل وتعزيز استخداماته عندما يكون ذلك مناسبًا، وكذلك لتحسين الفهم فيما يتعلق بالاختلافات بين السجل وقفل المسجل. يجب أن يكون المسجلين قادرين على إيجاد تعريفات واضحة لما توفره هذه الميزات، وما لا توفره هذه الميزات، وما هي الاختلافات بينها. يجب أن تنظر ICANN أيضًا في تسهيل توحيد الحد الأدنى من المتطلبات لخدمات قفل السجل والمسجل. الشريحة التالية.

نعتقد أن هناك حاجة لزيادة الوعي بأفضل الممارسات فيما يتعلق بأمن البنية التحتية. تحتاج ICANN إلى العمل مع مبادرات مثل الأسلوب واللطف لقياس وتقديم التقارير عن اعتمادها واستخدامها للتقارير لاستهداف المواد التعليمية التي من شأنها تحسين الوعي حول أمن البنية التحتية. يجب أن تتخذ ICANN أفضل الممارسات المنبثقة عن تلك المبادرات والتأكد من أن الأطراف المتعاقدة ومجتمع ICANN على دراية بها. في حالة عدم وجود أفضل الممارسات، يجب أن تعمل ICANN لتشجيع تطوير ونشر هذه الممارسات وتعزيز اعتماد ميزات إعلان أمان DNS عبر نظام DNS البيئي. على سبيل المثال، TLSA، SPF، DMARC، DANE، DNSSEC، إلخ.

بعد ذلك، توصيات حول حظر وتصفية DNS. يجب على ICANN إنشاء مواد إعلامية وتعليمية لمساعدة مجتمع ICANN والأطراف المتعاقدة والأطراف المهتمة الأخرى على فهم مخاطر وفوائد حظر وتصفية DNS لأسباب تتعلق بالأمان والاستقرار في جميع أنحاء مجتمع DNS العالمي. الشريحة التالية.

فيما يتعلق بالاستجابة للحوادث، يجب على ICANN، جنبًا إلى جنب مع جميع الأطراف ذات الصلة، تشجيع تطوير ونشر عملية استجابة رسمية للحوادث عبر صناعة DNS التي تسمح بالتفاعل مع الآخرين في النظام البيئي. ومن شأن هذا الجهد أن يشمل التعامل مع الاستجابة للحوادث فضلاً عن المشاركة المحمية في معلومات التهديد والحوادث. وهذا مرة أخرى يمكن أن يرتبط بالتمرين المنضدي لضمان أنه يمكن تحديد أي خطط للاستجابة للحوادث والتي يمكن تفعيلها في أي ثغرات في الوظائف التشغيلية للقيام بذلك.

التوصية E6، كانت عبارة عن الوعي بالقناة السرية. يجب أن تنشر ICANN المواد التعليمية حول استخدام القنوات السرية كناقل للهجوم، والتي قد يُنظر إليها على أنها إساءة استخدام لـ DNS نفسه، وبالتالي يتطلب التعامل مع مشكلات إساءة استخدام DNS الأخرى. الشريحة التالية.

فيما يتعلق بالأولويتين الرئيسيتين اللتين يمكن أن نختارهما من التوصيات المقدمة، نشعر أنه أولاً، التوصية R3، تحقق من أفضل الممارسات المناسبة للمصادقة. والثانية هي التوصية E5، الاستجابة للحوادث. الشريحة التالية.

حسنًا. إليك الكلمة ميريك.

ميريك كاو: رائع. شكرًا جزيلاً. بالنسبة لأي شخص يرغب في الحصول على مزيد من المعلومات حول مجموعة الدراسة الفنية ووجهة النظر حول ماهية الميثاق ووثيقة النطاق والجداول الزمنية لخطة العمل وجداول أعمال الاجتماع والملاحظات والموارد الأخرى، يرجى الانتقال إلى الموقع. وكما ذكر جون، سيتم نشر التقرير للعامة في وقت ما من الأسبوع المقبل مع مدونة. سأحذركم في وقت مبكر، فهو يحتوي على الكثير من المحتوى بتفاصيل أكثر مما كنا قادرين على تقديمه هنا في هذا الوقت القصير. لكنه يحتوي على الكثير من المحتوى الجيد حقًا وأعتقد أنكم ستجدوه ذا قيمة كبيرة. آمل بالتأكيد أن يجد الرئيس التنفيذي لـ ICANN هذا تقريرًا قيمًا ويتحرك بناء عليه. في هذا الوقت، أود أن أفتح المجال لأية أسئلة لا تزال قائمة. لا أرى أي أسئلة في اللوحة في هذا الوقت.

ويندي بروفيت: أعتقد أنه تمت الإجابة على جميع الأسئلة الموجودة في اللوحة كتابةً.

ميريك كاو: نعم، تم ذلك. أتساءل عما إذا كانت هناك أي أسئلة جديدة، يرجى كتابتها في لوحة الأسئلة والأجوبة، وسنكون سعداء للإجابة عليها. حسنًا. هناك سؤال مرة أخرى، "أين يمكنني الحصول على التقرير النهائي؟" سيتم إتاحة التقرير النهائي الأسبوع المقبل مع المدونة. أعتقد أن المؤشر

سيكون أيضًا في موقع wiki الذي أشرت إليه للتو. كان السؤال، "هل هذه الأسئلة والأجوبة متوفرة مع التسجيل؟" سأترك ذلك للفريق. هل سيكون هناك نسخة مع التسجيل؟

ويندي بروفيت: اسمحوا لي أن أتحقق من ذلك مع فريق MTS.

ميريك كاو: حسنًا. شكرًا جزيلاً. شكرًا على هذا السؤال، دونا. كما يمكن القول، أعني، كان هناك الكثير من الوقت في الأشهر الثمانية عشر الماضية في هذا العمل والخبرة الوظيفية المتقاطعة بلا استثناء بالفعل. كان هذا رائع. وأود توجيه الشكر إلى كل عضو ساهم في هذا التقرير.

وعند هذه النقطة، لا أرى أن هناك أي أسئلة أخرى. وإذا كان ذلك هو الحال، أود أن أشكر كل من شارك في هذه الجلسة التحضيرية. مرة أخرى، يرجى قراءة التقرير عندما يكون متاحًا الأسبوع المقبل ونتطلع إلى معرفة ما سيحدث معه.

ويندي بروفيت: لدينا سؤال آخر في اللوحة بينما ننتظر الإجابة الأخرى، وهو، "ما هي الدوافع الرئيسية للمهاجمين؟ وأين هي دول المنشأ؟"

ميريك كاو: سأتولى ذلك. لكن أي شخص آخر من TSG يمكنه المساهمة أيضًا. الدوافع متنوعة فقط. يمكن أن يكون الأمر مجرد أفراد، وهناك أيضًا جريمة منظمة، ويمكن أن تأتي حقًا من أي دولة قومية. هذه هي طبيعة العالم الافتراضي الذي نعيش فيه اليوم. حسنًا، بهذا، سأختتم هذه الجلسة. وشكرًا جزيلاً لكم جميعًا على الحضور.

[إنتهاء التدوين]