
المانيا اول من طوّرت
الهجمات على شبكة تور

!!

يمثل إخفاء الهويه على الإنترنت مشكلة خطيرة بالنسبة للحكومة ووكالات الأمن والإستخبارات ؛ فقد أجريت نقاشات طويلة حول صعوبات التحقيق عندما يستخدم المشتبه فيهم شبكات إخفاء الهوية ومنصات الاتصال التي تستخدم التشفير من طرف إلى الاخر .

كشفت وثيقة سرية حديثة أن وكالة التجسس الألمانية BND قد وضعت نظاما لمراقبة شبكة تور وكشف هوية مستخدمي تور. ووفقا للتقرير، حذرت وكالة التجسس الألمانية الوكالات الفيدرالية من إمكانية تتبع المستخدمين حتى عند إخفاء هوياتهم خلف شبكات إخفاء الهوية الشائعة .

وفقا للوثائق، سلمت الوكالة الألمانية نموذجا أوليا من هذه التكنولوجيا لوكالة الأمن القومي الأمريكى في إطار تعاونهم على المدى الطويل . شهد هارالد فيشنر، رئيس المخابرات BND حتى تقاعده في يونيه 2009 , التحقيق في فضيحة تجسس وكالة الأمن القومي قبل عامين فى اللجنة البرلمانية الألمانية . كان فيشنر رئيس جيش الكتروني يتألف من ألف جاسوس شاركوا في عملية المراقبة. كان الجواسيس يعترضون خطوط الاتصالات عبر موجات الراديو وكابلات الهاتف وكابلات الألياف الضوئية.

تحت إدارة سيجينت، هناك وحدة قرصنة سرية تركز على «الهجمات الالكترونية على أنظمة تكنولوجيا المعلومات» في جميع أنحاء العالم ، كانت المجموعة تسمى الوحدة 26E (الدعم التشغيلي وتكنولوجيا التصنت)، ثم تم تغيير اسمها أولا في «مجموعة العمل TX» (عمليات تكنولوجيا المعلومات) وأخيرا «المديرية الفرعية T4» (الاستخبارات الافتراضية).

تم الكشف عن وجود الوحدة في عام 2008 عندما تم إختراق شبكة الكمبيوتر الخاصة بوزارة التجارة الأفغانية والوصول إلى رسائل البريد الإلكتروني الخاصة بالوزير (الذي يعتبر حليف) ورسائل البريد الإلكتروني الخاصة بالصحفية الألمانية سوزان كولبل. وخلال زيارة إلى الولايات المتحدة في عهد الرئيس الأمريكى جورج بوش ، كان أحد عملاء جهاز «BND» يعرف بالأحرف الأولى «H.F.» ضيف وكالة الأمن القومي في مقر فورت ميد، وحضر مؤتمر التنمية السنوي الخاص بسيجينت . كان H.F.

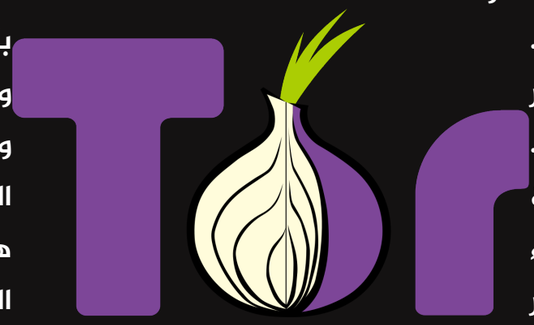
هناك لتقديم الهجوم على شبكة تور برعاية قراصنة BND لكشف هوية مستخدمين تور. وقد استخدمت شبكة تور على نطاق واسع للتحايل على الرقابة والمراقبة. لسوء الحظ، فقد اسئ استخدامها أيضا من قبل مجرمي الإنترنت و» الإرهابيين» والوكالات الحكومية . في ذلك الوقت، كان كشف هوية مستخدمي تور هدفا مشتركا لوكالات الاستخبارات في البلدان الغربية. وقد استلهم قراصنة BND من الوحدة 26E من شرح شبكة تور الذى قدمه رئيس مشروع تور روجر دينجلدين في مؤتمر CCC في مركز شرطة شتوتغارت.

في مارس 2008، كشفت وكالة BND لشركائها من الولايات المتحدة الأمريكية والمملكة المتحدة النقاب عن المشروع. «عندما زار وفد أجنبي ميونيخ، قدمت وحدة سيجينت» شبكة عدم الكشف عن الهوية تور وإمكانية الغاء ميزة عدم الكشف عن هوية المستخدمين «، وكتبت BND في تقريرها الداخلي. من أجل تنفيذ الخطة، تأمل الحكومة في «التعاون الدولي مع العديد من وكالات الاستخبارات الأجنبية». وقدمت كل من وكالات الاستخبارات الوطنية GCHQ الدعم للمشروع؛ في هذه الأثناء خططت BND لإنشاء خادم تور خاص بها لغرض الاختبار. وفي نيسان / أبريل، قدم العميل H.F. تقنية القرصنة التي وضعتها وحدته إلى أقرانه في تحالف مكافحة الإرهاب في نادي وكالة التجسس الأوروبي سيجينت. وبعد ذلك، دعت وكالة الأمن القومي إلى مؤتمر SIGDEV في مقرها. وقد صدم العرض الوكالات الأخرى، وكان نجاحا كبيرا، وبدأ خبراء آخرون في مراجعة الهجوم الذي قدمه الباحث. وبعد ذلك بأسبوع، دعت وكالة الأمن القومي H.F. مرة أخرى، وشارك مع زميله M.S. في اجتماع عقد في محطة باد ايبلنغ في بافاريا، حيث وحدة الاتصال سوسلاغ التي لديها مبنى لنشاطها في جيرمان. M.S ،H.F. وأقران من وكالة الأمن القومي عقدوا مؤتمر بالفيديو لتبادل المزيد من التفاصيل حول المشروع. وأبلغ خبراء «BND» نظرائهم من وكالة الأمن القومي عن إمكانية «اختراق شبكة تور»، مما يشير على الأرجح إلى إمكانية استغلال خيار التصميم الذي حدده تور بشكل عام.

كان المتسللون يفكرون في التسلل إلى شبكة تور مع بنية تحتية «عالمية وغير مباشرة» تتألف من العقد الخاصة بهم. وتحذر إحدى الوثائق السرية من:

«إذا كان المهاجم يمكنه مشاهدة حركة المرور الخارجة من جهاز الكمبيوتر الخاص بك، وكذلك حركة مرور حزم البيانات التي تصل إلى الوجهة التي اخترتها، فإنه يستطيع استخدام التحليل الإحصائي لاكتشاف أنها جزء من نفس الدائرة » . وقد اقترح مجتمع البحث نهجا مختلف للتحليل الإحصائي لهجمات مرور حزم البيانات ؛ لذلك قامت وكالات الاستخبارات بتصميمها لاستغلال قدرة التحليل الاحصائي على

رصد حركة مرور البيانات الشاملة على نطاق عالمي. وقد قرر قراصنة BND تنفيذ تقنية القرصنة التي اقترحتها مجموعة من الباحثين في جامعة أمريكية، لذلك خططوا لإنشاء شبكة تور خاصة بهم في مختبر لاستكشاف جدوى هذه التقنية. من جهة أخرى، وافقت وكالة الأمن القومي على الاتصال بالباحثين في الجامعة الأمريكية لاختبار تقنيتهم. وقد أنشأ BND شبكة اختبار ووضع «دليلا على المفهوم» للهجوم، وكان الهدف السماح لرئيس سيجينت هارالد فيشنر تقديم هذه التقنية في أكتوبر خلال اجتماع مع مدير وكالة الأمن القومي كيث ألكسندر. ولسوء الحظ، فإن إعادة التنظيم الداخلي لوحدة القراصنة الألمانية خصصت الخبراء الذين عملوا في المشروع في مجالين مختلفين. بعد أشهر، انتخب الرئيس الأمريكي الجديد باراك أوباما وتم تأجيل بدء المشروع مرة أخرى من جانب الرئيس والمخابرات الأمريكية. واصلت BND عملها بهدف تقديم النظام إلى وكالة الأمن القومي والحصول في المقابل علي تكنولوجيا من «مجال تحليل الشفرة» الذي يسمح لعملاءها بفك تشفير الاتصالات المشفرة.



أمرت BND العميل M.S. بكتابة تقرير توضيحي تم إنجازه في شهر واحد فقط في 20 شباط / فبراير 2009. وثيقة من 16 صفحة «مفهوم لتتبع حركة المرور على الإنترنت، والتي تم اخفاء هويتها عن طريق نظام تور». «لتبرير الهجوم على تور، نقل M.S. عن مؤتمر فرض القانون في برلين من هذا العام الذي أقيم تحت شعار «WWW - مسرح الجريمة الافتراضي». فصل حول «كيف تعمل شبكة تور»، كتبه المؤلف بطريقة مبسطة، ونسخ النص من ويكيبيديا و أخذت صور من موقع تور. «كما ذكرت نيتزبوليتيك. «على وجه التحديد كيف تخطط BND إلى» اختراق «تور للأسف محذوف من الوثيقة التي حصلنا عليها. ولكن كما علمنا من قبل، تشير وكالة التجسس إلى البحث العام لتنفيذ الهجوم، فمن المرجح أن الجواسيس لديهم خوادم خاصة بهم داخل شبكة تور. اشار العميل M.S. إلى خوادم التطفل الغير مباشرة، والتي يفترض أن تشغلها وكالة الأمن القومي، ويؤكد على عدم الكشف عن هوية وكالات التجسس. وكان التقرير ناجحا، وقام فريق من جواسيس GCHQ بزيارة مقر BND في 11 مارس 2009 حيث عقدوا اجتماعا لمناقشة تطوير التعاون مع سيجينت، مع التركيز بشكل خاص على خدمات عدم الكشف عن الهويه. وقد ترأس الاجتماع رئيس فريق سيغينت هارالد فيشنر؛ وكان الخبراء البريطانيون مهتمين جدا

بالمساهمة في المشروع.

بعد بضعة أيام من الاجتماع التقى فيشنر مع وكالة الأمن القومي و GCHQ في الولايات المتحدة، وقدم لهم نتائج تحليلهم وبدوره حصل علي التكنولوجيا التي طلبها. في هذه المرحلة، تعاون علماء NSA و GCHQ لوضع طريقة لمراقبة المستخدمين على شبكة تور. وبعد مرور عام ونصف العام، حذر BND الوكالات الاتحادية الألمانية من استخدام تور؛ ونشرت وحدة «عمليات تكنولوجيا المعلومات» تقريرا بعنوان بليغ «خدمة تور لا تضمن إخفاء الهوية على الإنترنت». وتم إرسال تقرير من ست صفحات إلى المستشارية والوزارات والخدمات السرية والهيئات العسكرية والشرطة في 2 سبتمبر 2010.

ووفقا للموجز التنفيذي للتقرير، فإن تور «غير مناسب» للأنشطة التالية:

- الأنشطة العبثية على شبكة الإنترنت.
- التحايل على تدابير الرقابة.
- عمليات شبكات الكمبيوتر لأجهزة الاستخبارات.

ويفترض «مستوى عال جدا من المراقبة داخل الشبكة»، بما في ذلك احتمال أن المهاجم المثابر يمكنه «إنشاء ما يسمى عقدة الخروج لمراقبة حزم البيانات» . ووفقا لـ BND ، ليس سوى جزء صغير من مستخدمين تور مثيرين للاهتمام في طريقة الحفاظ على إخفاء هويتهم، في معظم الحالات يتم إساءة استخدام شبكة إخفاء الهوية لإخفاء بعض الأنشطة.

«يستخدم تور في الغالب لإخفاء الأنشطة، حيث المستخدمين غير مقتنعين بمشروعية أفعالهم. عدد مستخدمي تور الذين يهدفون إلى الحفاظ على عدم الكشف عن هويتهم لمجرد اعتبارات الخصوصية صغير نسبيا» ووفقا للوكالة، فإن وكالات التجسس ووكالات الأمن والإستخبارات في جميع أنحاء العالم «لديها طرق لمواجهة إخفاء الهويه. احد هذه الطرق إنشاء عقد تور خاصة ورصد تلك الانشطة بشكل مكثف لجمع المعلومات الاستخبارية والأدلة .

حذرت المخابرات الألمانية وكالاتها من وجود العقد الخارقة لتور المثبتة من قبل وكالات أخرى لأغراض المراقبة. «وقد ذكرت بعض الوكالات بالفعل عن تثبيت عقد تور خاصة بهم واستخدام البيانات المسجلة لمشاريع مختلفة وتحقيقات جنائية». ويعتقد BND أن المخابرات الأمريكية تدير العديد من العقد الخارقة لتور، وكثير منها تقع «بالقرب من واشنطن العاصمة».

«إن مستخدمي برامج عدم الكشف عن هويتهم يتوقعون مستوى من التنكر، وهو ما لا يوفره الكثير من خدمات إخفاء الهوية المنتشرة على نطاق واسع» وكان

قلق BND مبرر ، فقد تم توثيق جهود الفريق البريطاني في GCHQ's internal wiki التي نشرت من قبل مجلة دير شبيغل الألمانية من تسريبات سنودن. الهدف الاستخباراتي البريطاني هو كشف هوية مستخدمي تور إذا تم توفير جزء من حركة المرور من عقدة خروج تور ثم العثور على عنوان الـIP للمستخدم المرتبط بتلك الحركة» .

بدأت المخابرات البريطانية العمل على المشروع في ديسمبر 2010؛ وتركزت الجهود على «هجوم ارتباط عقد الدخول والخروج». عمل خبراء GCHQ على تحليل حركة المرور التي تدخل شبكة تور والتي تخرج منها عن طريق استخدام خوادم تور خاصة بهم.

«في وقت مبكر من يونيه 2011، تم الانتهاء من دراسة 18 صفحة وشفرة المصدر في لغة البرمجة الإحصائية R، مقدمة في عرض بالشرائح المرئية.» لم تستهدف وكالات الاستخبارات سوى البنية الأساسية تور، على الأقل منذ عام 2013 كانت وكالة الأمن القومي و GCHQ قادرة على إختراق متصفح تور المبني علي فايرفوكس لتسوية نظام المستخدمين تحت مشروع باسم Egotistical Giraffe .

وواصل قراصنة BND أبحاثهم حول كيفية إختراق شبكات تور، ولكن وفقا للوثائق التي حصلت عليها وسائل الإعلام الألمانية في يونيه 2012 فإنه لا تزال هناك مشاكل لكشف هوية المستخدمين على شبكة إخفاء الهوية.

«أثناء زيارته واشنطن في يونيه 2012، طلب وفد من وكالة الأمن القومي إذا كان يمكن»تحديد» أو»فك تشفير» تور. لكن الجواب الأمريكي لم يرضيهم. وفي تقييم الزيارة، كتب الألمان أن الزيارة كانت «مهمة من الناحية الاستراتيجية»، ولكن «كانت أكثر اهمية حول إدارة العلاقات».

في أكتوبر 2013، أصدر الخبير إدوارد سنودن وثيقة سرية من وكالة الأمن القومي بعنوان «تور ستينكس» اعترفت فيها وكالة الاستخبارات بأنها قادرة على كشف هوية جزء صغير فقط من مستخدمي تور يدويا.

«لن نكون قادرين كشف هوية جميع مستخدمي تور في كل وقت» ولكن «مع التحليل اليدوي، يمكننا كشف هوية جزء صغير جدا من مستخدمي تور»

وكشفت الوثيقة أيضا أن NSA كانت تعمل على افشال تجربة المستخدمين لثني الناس عن استخدام متصفح تور.

تعتمد استراتيجية الأمن القومي على المبادئ التالية لإخفاء هوية تور.

التسلل الى شبكة تور باستخدام العقد. كل من NSA و GCHQ تستخدم عقد تور لتتبع حركة المرور إلى مستخدم معين، ويستند الأسلوب على إعادة إعمار دائرة

معرفة العقد «تتابع الدخول والخروج» بين المستخدم والموقع المستهدف.

استغلال ثغرات «Zero-Day» من متصفح فايرفوكس المبني مع تور، مع هذه التقنية كانت NSA قادرة على الحصول على عنوان IP للمستخدم. وبهذه الطريقة، اعتقل مكتب التحقيقات الفدرالي صاحب خدمة استضافة الحرية المتهم بالمساعدة والتحريض على استغلال الأطفال في المواد الإباحية.

تستخدم NSA أيضا ملفات الإنترنت لتتبع مستخدم تور تقنية فعالة أيضا لمتصفح تور. ملفات تعريف تجربة المستخدم و كا لة تملك أو سلسلة على ا لتي ملفات تعريف في الماضي الجهاز الضحية. تقوم الوكالة بجمع ذلك عنوان IP. وبطبيعة الخبراء تجنب هذا النوع بطرق متصفح مخصص لاستخدام شبكة تور ، وذلك باستخدام حزمة تور تم تكوينها مسبقا أو إدارة ملفات تعريف الارتباط المخزنة على الجهاز بشكل صحيح. هناك وثائق سربها إدوارد سنودن تبين أن وكالة الأمن القومي تستخدم الإعلانات عبر الإنترنت ، أي إعلانات جوجل لجعل عمليات التتبع منتشرة على شبكة الانترنت . لحسن الحظ، يواصل مجتمع تور أيضا المساهمة في تحسين المشروع، وفقا لمدير المشروع روجر دينجلدين فإن وكالات التجسس لا تزال غير قادرة على كشف مستخدمي تور.

تعريف الارتباط على شبكة على نطاق واسع.

و تستخد م الارتباط لتحليل على الإنترنت، ا لمخا بر ا ت تسيطر على من المواقع شبكة الانترنت يمكنها قراءة الارتباط المخزنة من المتصفح على باستخدام هذه التقنية، بيانات المستخدم بما في الحال، يمكن للمستخدمين عديدة، على سبيل المثال باستخدام

تعليق :

المقال السابق يوضح إستهداف شبكة تور من قبل أجهزة الإستخبارات وأجهزة الأمن على مستوى العالم حيث تمثل شبكة تور « صداع مزمن » لأجهزة الإستخبارات وعلى الرغم من القدرات الهائلة التى تمتلكها تلك الأجهزة إلا أنه لا يمكن الجزم بشكل مطلق أن أجهزة الإستخبارات تستطيع كشف هوية جميع مستخدمى شبكة تور لكن يجب أخذ الحيطة والحذر لذلك إحرص على :

1- تجنب تصفح المواقع الإلكترونية التى تستخدم بروتوكول HTTP من خلال شبكة تور لأن مدير عقدة الخروج يمكنه الإطلاع على البيانات الغير مشفرة لذلك إحرص دائماً على إستخدام بروتوكول HTTPS .

2- تحقق من تحديث متصفح تور لأحدث نسخة و تجنب تفعيل JavaScript قدر الإمكان بمتصفح تور كما يمكنك رفع مؤشر الحماية بمتصفح تور للمستوى الأمنى المناسب لك

3- تجنب ممارسة جميع أنشطتك من خلال متصفح تور فلا تستخدم متصفح تور فى تسجيل الدخول الى فيسبوك و النشر و تصفح مواقع شبكة الإنترنت الأخرى الخاصة باهتماماتك بجلسة واحدة .

4 - إستخدم خدمة VPN آمنة تحافظ على خصوصيتك ومن ثم إستخدم متصفح تور فذلك سيمنع مزود الخدمة المحلى من معرفة أنك تستخدم شبكة تور .

مؤسسة آفاق الإلكترونية

تهتم بنشر الوعي الامني والتقني بين المسلمين

@TECH_SUPPORT SR444TAW Horizons@chatwith.xyz

تم ترجمة هذا المقال من قبل موقع InfoSec Institute