إيقاف انتشار فيروس wannacry بأقل من 11 دولاراً



تمكن باحث بريطاني مختص بالهجمات الالكترونية، يبلغ من العمر 22 عاماً، من إيقاف الانتشار العالمي لفيروس وناكراي wannacry.

اكتشف الباحث المختص بالهجمات الالكترونية "مفتاح الإغلاق **Kill switch**" الذي منع انتشار فيروس الفدية **wannacry**، في الوقت الراهن. وذلك بعد أن شنّ قراصنة الانترنت هجوماً الكترونياً على عدد كبير من المؤسسات والشركات الرئيسية في مختلف دول العالم باستخدام فيروس فدية **ransomware** أطلق عليه اسم وناكراي **WannaCry**، مما تسبب في تشفير بياناتها مع المطالبة بدفع مبلغ مالي لقاء إعادتها. ونُفذ الهجوم في منتصف ليل الثالث عشر من أيار/مايو.

وقال الباحث صاحب الحساب على تويتر **MalwareTechBlog**: "لقد اعتمد القراصنة في هجومهم بشكل أساسي على نطاق غير مسجل، ومن خلال تسجيله استطعنا ايقاف الهجوم".

ووفقاً لمدونة الباحث فقد حصل على عينة من البرمجية الخبيثة بمساعدة صديق له. وعند تشغيل العينة في بيئة تحليل، لاحظ على الفور استعلامها عن نطاق غير مسجل (وهو عبارة عن موقع غير مفعل على الإنترنت يقوم الفايرس بالإتصال به آلاف المرات كل ثانية)، فقام سريعاً بتسجيله وشرائه بمبلغ 10.69 دولار.

وباستخدام مظلة سيسكو **Cisco Umbrella**، يمكننا أن نرى فعلاً حجم الاستعلام إلى النطاق قبل تسجيله والذي يدل على بدء الهجوم.

DNS queries: استعلامات نظام أسماء النطاقات DNS DNS queries/hour: استعلامات نظام أسماء النطاقات/ساعة

وبينما كان النطاق ينتشر، قام الباحث بتشغيل العينة مرة أخرى في بيئة افتراضية ليشاهد صفحة الفدية من **WannaCry**، ولكن ما أثار دهشته أنه بعد تشفير الملفات الوهمية وتركها كاختبار، بدأ الفيروس بالاتصال بعناوين **IP** عشوائية على المنفذ 445 (منفذ يستخدم من قبل البروتوكول **SMB** الخاص بمشاركة الملفات في ويندوز).

مما ولّد عند الباحث الشك بأن هذه الهجمات ذات صلة بتسريبات الأمن القومي الأمريكي **NSA** التي قام بها مجموعة أطلقوا على أنفسهم **ShadowBroker**، حيث نفذوا هجومهم مستغلين ثغرات على بروتوكول **SMB**. إلا أن الباحث لم يتيقن من ذلك، وهذه هي النتائج التي حصل عليها:

435435.exe ...	WIN-NV80LHBLSR...	50518	157.218.242.157	445	TCP	SYN sent	mssecsvc2.0
435435.exe ...	WIN-NV80LHBLSR...	50519	148.139.43.66	445	TCP	SYN sent	mssecsvc2.0
435435.exe ...	WIN-NV80LHBLSR...	50520	17.228.203.222	445	TCP	SYN sent	mssecsvc2.0
435435.exe ...	WIN-NV80LHBLSR...	50521	41.46.48.170	445	TCP	SYN sent	mssecsvc2.0
435435.exe ...	WIN-NV80LHBLSR...	50522	137.67.186.53	445	TCP	SYN sent	mssecsvc2.0
435435.exe ...	WIN-NV80LHBLSR...	50523	18.64.83.93	445	TCP	SYN sent	mssecsvc2.0
435435.exe ...	WIN-NV80LHBLSR...	50524	105.147.164.200	445	TCP	SYN sent	mssecsvc2.0
435435.exe ...	WIN-NV80LHBLSR...	50525	211.227.52.180	445	TCP	SYN sent	mssecsvc2.0
435435.exe ...	WIN-NV80LHBLSR...	50526	56.197.45.53	445	TCP	SYN sent	mssecsvc2.0
435435.exe ...	WIN-NV80LHBLSR...	50527	106.34.250.175	445	TCP	SYN sent	mssecsvc2.0
435435.exe ...	WIN-NV80LHBLSR...	50529	12.177.12.162	445	TCP	SYN sent	mssecsvc2.0
435435.exe ...	WIN-NV80LHBLSR...	50530	11.62.1.98	445	TCP	SYN sent	mssecsvc2.0
435435.exe ...	WIN-NV80LHBLSR...	50531	141.148.252.178	445	TCP	SYN sent	mssecsvc2.0
435435.exe ...	WIN-NV80LHBLSR...	50532	98.127.183.59	445	TCP	SYN sent	mssecsvc2.0
435435.exe ...	WIN-NV80LHBLSR...	50533	141.146.18.59	445	TCP	SYN sent	mssecsvc2.0
435435.exe ...	WIN-NV80LHBLSR...	50534	200.188.113.253	445	TCP	SYN sent	mssecsvc2.0
435435.exe ...	WIN-NV80LHBLSR...	50535	2.176.145.178	445	TCP	SYN sent	mssecsvc2.0
435435.exe ...	WIN-NV80LHBLSR...	50536	46.191.249.228	445	TCP	SYN sent	mssecsvc2.0
435435.exe ...	WIN-NV80LHBLSR...	50537	182.25.59.180	445	TCP	SYN sent	mssecsvc2.0
435435.exe ...	WIN-NV80LHBLSR...	50538	200.134.101.224	445	TCP	SYN sent	mssecsvc2.0
435435.exe ...	WIN-NV80LHBLSR...	50539	205.88.12.239	445	TCP	SYN sent	mssecsvc2.0
435435.exe ...	WIN-NV80LHBLSR...	50540	50.21.130.41	445	TCP	SYN sent	mssecsvc2.0
435435.exe ...	WIN-NV80LHBLSR...	50541	173.36.198.1	445	TCP	SYN sent	mssecsvc2.0
435435.exe ...	WIN-NV80LHBLSR...	50542	193.237.150.202	445	TCP	SYN sent	mssecsvc2.0
435435.exe ...	WIN-NV80LHBLSR...	50543	181.62.191.92	445	TCP	SYN sent	mssecsvc2.0
435435.exe ...	WIN-NV80LHBLSR...	50544	181.52.67.187	445	TCP	SYN sent	mssecsvc2.0
435435.exe ...	WIN-NV80LHBLSR...	50545	14.147.181.30	445	TCP	SYN sent	mssecsvc2.0
435435.exe ...	WIN-NV80LHBLSR...	50546	166.0.177.184	445	TCP	SYN sent	mssecsvc2.0
435435.exe ...	WIN-NV80LHBLSR...	50548	125.34.248.162	445	TCP	SYN sent	mssecsvc2.0
435435.exe ...	WIN-NV80LHBLSR...	50549	91.59.250.112	445	TCP	SYN sent	mssecsvc2.0
435435.exe ...	WIN-NV80LHBLSR...	50552	82.55.103.152	445	TCP	SYN sent	mssecsvc2.0
435435.exe ...	WIN-NV80LHBLSR...	50553	198.29.125.7	445	TCP	SYN sent	mssecsvc2.0

عينة من الهجمات على IP عشوائية على المنفذ 445

ومما يجدر ذكره أن التسجيل الفعلي للنطاق لم يكن عن غير دراية كما قيل. فمهمة الباحثين هي البحث عن طرق لتتبع وإيقاف برمجيات البوت **botnets** المحتملة (والأنواع الأخرى من البرمجيات الضارة)، لذا فهم دائمو البحث عن نطاقات خادم التحكم للبرمجيات الخبيثة **malware control server (C2) domains** غير المسجلة.

ويتابع الباحث في تدوينته أنه قام بربط النطاق بخادم يطلق عليه **sinkhole**، وتأكد من حصوله على البيانات المتوقعة من النطاق الذي سجله، ووجد أن هناك الآلاف من محاولات الاتصال بالخادم كادت أن تستهلك كامل قدرته. وسرعان ما كان قادراً على إعداد خريطة تتبع للفايروس ونشرها عبر تويتر.

لكن، هذا لا يعني أننا أصبحنا في أمان. فكما صرح الباحث، يمكن لصاحب الهجوم أن يطلق نسخة أخرى باسم نطاق آخر مجهول، أو حتى بهجوم يتطلب طريقة إيقاف مختلفة تماماً.

- التاريخ: 2017-05-14
- التصنيف: تكنولوجيا

#الانترنت #فيروسات الكمبيوتر #فيروس فدية #الهجمات الالكترونية #قراصنة الانترنت

المصادر

- malwaretech
- ناسا بالعربي
- الصورة

المساهمون

- إعداد
  - دانا أسعد
- مُراجعة
  - علي مرعي
- تحرير

- مريانا حيدر
- تصميم
  - أنس محادين
- نشر
  - مي الشاهد