تقرير:

برمجية طلب الفدية الخبيثة واناكراي (WannaCry)

طريقة عملها واجراءات الوقاية منها

ينتشر منذ الساعات الماضية برنامج خبيث لطلب الفدية يدعى واناكراي (WannaCry)، ويقدر أنه أصاب أكثر من 200,000 ضحية في أكثر من 150 دولة حول العالم، ويتركز معظم الأنظمة المصابة في روسيا يليها في ذلك كل من أوكرانيا والهند وتايوان ودول الاتحاد الأوروبي وامريكا الشمالية، ويعمل البرنامج الخبيث بعدد كبير من اللغات وصل حتى 28 لغة، وقد تسبب هذا البرنامج في تعطل عدد كبير من الأنظمة في عدة مؤسسات ذات الطبيعة المهمة والحساسة كالمستشفيات والمصارف وشركات الاتصالات ومحطات القطارات، إذ يقوم هذا البرنامج الخبيث بتشفير محتويات الأجهزة من ملفات ومن ثم طلب فدية مالية من الضحية مقابل الحصول على مفتاح فك التشفير.

تم اكتشاف انتشار هذه الدودة أول مرة يوم الجمعة الموافق 12 مايو2017 من قبل باحث مستقل، ومن ثم بدأت أولى التقارير تتوالى تباعاً محذرة من انتشار هذا البرنامج الخبيث خلال ساعات قليلة لعدد كبير من الأجهزة والأنظمة المختلفة بداية من الساعة 10:00 صباحاً بتوقيت طرابلس، ويشير عدد من التقارير أن الفدية التي تُطلب من الضحية تبلغ حوالي 0.1781 بِت كوين (Bitcoin) وهوما يعادل حوالي 300 دولار أمريكي، ويظهر للضحية ساعة تعداد تنازلي تهدد بتضاعف الفدية حال انتهاء المهلة.

من خلال التحاليل الأولية التي أجريت على هذا البرنامج الخبيث، يعتقد أن هذه الدودة تعتمد في انتشارها على ثغرة تدعى (EternalBlue) والتي تم الافصاح عنها في التسريبات المنشورة مؤخراً الخاصة بالكشف عن بعض الأدوات التي تم تطويرها في وكالة الأمن القومي (NSA) الامريكية والتي تستهدف قرصنة أنظمة التشغيل ويندوز والسيطرة عليها، إلا أن العدوى بهذا البرنامج الخبيث تبدأ من خلال عملية تصيد (Phishing) عبر البريد الإلكتروني أوأي وسائل تواصل أخرى، بحيث تصل رسالة مرفق بها وصلة أوملف يحتوي على البرنامج الخبيث، وعند النقر عليه يقوم بتنصيب نفسه بالجهاز ويشفر جميع محتويات الجهاز ومن ثم يستغل الثغرة المذكورة آنفاً للانتشار لكل الأجهزة الأخرى المجاورة للجهاز المصاب على الشبكة المحلية وخاصة تلك التي بينه وبينها مجلدات مشاركة (Shared Folders) والتي لم يتم سد الثغرة التي تسهل عملية تنقّل الدودة، ومرة أخرى يقوم البرنامج الخبيث بتشفير الملفات في تلك الأجهزة واستغلالها للانتشار إلى الأجهزة الأخرى وهكذا حتى يصيب جميع الأجهزة داخل نطاق المؤسسة أوالمنزل الذي يصاب أحد اجهزته.

مؤشرات التحقق من حصول العدوى

هناك عدد من مؤشرات حصول الضرر (Indicator of Compromise) والتي من أهمها:

Indicator type	Indicator
CVE	CVE-2017-0144
domain	57g7spgrzlojinas.onion
domain	76jdd2ir2embyv47.onion
domain	cwwnhwhlz52maqm7.onion
domain	gx7ekbenv2riucmf.onion
domain	sqjolphimrr7jqw6.onion
domain	xxlvbrloxvriy2c5.onion
FilePath	C:\@WanaDecryptor@.exe
FilePath	C:\111.exe
FilePath	C:\m.vbs
FilePath	C:\taskdl.exe
FilePath	C:\taskse.exe
FilePath	C:\Windows\mssecsvc.exe
FilePath	C:\WINDOWS\tasksche.exe
Hostname	www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
FileHash-MD5	007a71c83b7e5e7dee8cca4cb13e86c1
FileHash-MD5	08bab082019257268a3726ae75463f47
FileHash-MD5	1c615bf80a47848f17f935e689ae7ee2
FileHash-MD5	246c2781b88f58bc6b0da24ec71dd028
FileHash-MD5	26b205ffe4adaadbb442442cae653bdd
FileHash-MD5	29365f675b69ffa0ec17ad00649ce026
FileHash-MD5	2b4e8612d9f8cdcf520a8b2e42779ffa
FileHash-MD5	3175e4ba26e1e75e52935009a526002c

باقي المؤشرات يمكن الحصول عليها من الرابط التالي:
/https://otx.alienvault.com/pulse/5916cee44da2584776eaf2f6

الإجراءات الوقائية الواجب اتخاذها:

- قم بتطبيق تحديث شركة مايكروسوفت المقيدة كالتالي (MS17-010 SMB)، والثغرة مؤرخة في يوم 14 مايو2017 وذلك بالطريقة التالية :
- تمكين مصفيات البريد المزعج القوية لمنع وصول رسائل التصيد الالكتروني للمستخدم والقيام بمصادقة عبر تقنيات مختلفة مثل إطار سياسة المرسل Sender Policy Framework (SPF)، وDomain Messageg Authentication Reporting and Conformance (DMARC)، وDomainKeys Identified Mail (DKIM) لمنع حدوث عمليات تصيد للبريد.
- فحص كل رسائل البريد الوارد والصادر لاكتشاف تهديد ما، وتصفية الملفات التنفيذية قبل أن تصل إلى مستخدمين آخرين.
- التأكد من جاهزية الحلول المقدمة من مضادات الفيروسات والبرامج الخبيثة وقدرتها على إجراء عمليات فحص منتظمة.
- إدارة استخدام صلاحيات الحسابات وذلك بتنفيذ مبدأ أقل صلاحيات حيث لا ينبغي منح أي مستخدم إمكانية الوصول المطلق مالم تكن هناك حاجة ملحة لذلك، كذلك يجب على الأشخاص الذين يتعاملون مع حساباتهم كمشرفين استخدامها عند الضرورة فقط.
- تعديل أدوات التحكم في الوصول بما في ذلك الملف والدليل وأذونات مشاركة الشبكة إلى أقل ما يمكن من السماحية، فإذا طلب مستخدم ما إذناً بقراءة ملف ما.. فعليه ألا يحصل على إذن للكتابة في ذات الملف وكذلك الأدلة والمشاركات.
- تعطيل البرامج الماكرو (Macro Scripts) من ملفات ميكروسوفت أوفيس المرسلة عبر البريد الإلكتروني، ويمكن استخدام برنامج عارض أوفيس (Office Viewer software) لفتح الملفات بدلاً استخدام تطبيقات أوفيس.
- تطوير وتوعية وتدريب العاملين على برامج تثقيف للتعرف على عمليات الاحتيال الالكتروني والروابط الخبيثة، ومحاولات الهندسة الاجتماعية.
- عمل اختبارات اختراق منتظمة على الشبكة على الأقل مرة في السنة بشكل عملي قدر الإمكان.
- اختبار النسخ الاحتياطية للتأكد من عملها بشكل سليم عند الاستخدام.

الاحتياطات الواجب اتباعها للوقاية من برامج الفدية الخبيثة بشكل عام:

- عدم الضغط على أي وصلات أوفتح أي ملفات أوبرامج تصلك عبر أي وسيلة الكترونية من مصادر غير موثوقة أومعروفة والتدقيق في أي مرفقات تصلك ممن تعرف أوتثق بهم كالأصدقاء والزملاء.
- تحديث نظام تشغيل ويندوز بآخر التحديثات وخاصة تلك المتعلقة بالثغرة التي يستغلها هذا البرنامج الخبيث.
- تحديث مضاد الفيروسات بآخر التعريفات والمداومة على بقاءه محدثاً.
- حفظ نسخ احتياطية من البيانات المهمة وتحديثها بشكل دوري لتحوي آخر التعديلات وتخزينها في وسائط مفصولة شبكياً عن أصولها، ويتم العمل على اتباع سياسات الحفظ الاحتياطي للمؤسسة إن وجدت والعمل على وضع خطط تفصيلية بالخصوص إن لم توجد بحيث تتبع في صياغتها أفضل الممارسات المتعارف عليها دولياً في هذا المجال.
- عدم تحميل وتنصيب البرامج إلا من مصادر معروفة وموثوق بها.
- تفعيل آليات التحديث الآلي لكل البرمجيات وأنظمة التشغيل المستخدمة.

تعريفات:

ما المقصود ببرمجيات طلب الفدية الخبيثة - رانسوم وير (Ransomware)؟

هي برمجيات خبيثة تغلق الكمبيوتر أوالجهاز اللوحي أوالهاتف الذكي، أوتُشفِّر ملفاتك ثم تطلب منك فدية لإعادة فتح تلك الملفات.

هناك نوعان من البرمجيات التي تطلب الفدية:

الأول: هوالمُشفِّرات التي تشفر الملفات لتجعل فتحك لها مستعصياً؛ لأن فك شفرتها يحتم حصولك على المفتاح المستخدم في تشفيرها، والذي تُدفع الفدية في مقابله.

أما الثاني: فيُطلق عليه اسم العائق (بلوكر) لأنه ببساطة يعيق تشغيل الكمبيوتر أوأي جهاز، إلا أن العائق (بلوكر) يتميز بكونه أبسط في نص السيناريومن المشفِّرات لأن الضحية قد يكون قادراً على إعادة تشغيل الجهاز، لكنه يصعب عليه الوصول إلى ملفاته التي تم تشفيرها بسبب البرنامج الخبيث.

العملة المعماة (مشفرة) Bitcoin

هي عملة رقمية (وتسمى أيضا عملة مشفرة) لا يدعمها بنك مركزي في أي بلد أوحكومة ولا توجد هيئة تنظيمية مركزية تقف خلفها، حيث تستخدم عبر الإنترنت فقط من دون وجود فيزيائي لها. ويتم مقايضتها بسلع أوخدمات مع بائعين يقبلونها كوسيلة للدفع، اوتحويلها الى العملات التقليدية. لا تملك العملة المعماة رقماً متسلسلاً ولا أي وسيلة أخرى تتيح تتبع ما أنفق للوصول إلى البائع أوالمشتري، مما يجعل منها فكرة رائجة لدى كل من المدافعين عن الخصوصية، أوبائعي البضاعة غير المشروعة عبر الإنترنت على حد سواء.

دودة Worm

برنامج ينسخ نفسه وينتشر ذاتياً مستخدماً آليات التشبيك المختلفة مثل الشبكات المحلية والانترنت وغيرها، ولديه القدرة على التخفي من برامج الحماية.