« Vorige | Nächste »

WannaCry: Gewaltiger Schaden, geringer Erlös

14.05.2017 17:46 Uhr – Christof Windeck vorlesen

Erpressungs-Trojaner WannaCry (WanaDecrypt0r 2.0) (Bild: Securelist)

Der Erpressungstrojaner WannaCry schadet hunderttausenden Windows-Rechnern, brachte seinen Autoren bislang aber wohl kaum mehr als 30.000 Euro Lösegeld ein.

Der erst am Freitag aufgetauchte Erpressungstrojaner WannaCry soll innerhalb von drei Tagen schon mehr als 220.000 Computer in 150 Ländern befallen haben und richtet enorme Schäden an. In krassem Missverhältnis dazu steht das Lösegeld von schätzungsweise wenig mehr als 30.000 Euro, das die Autoren der gefährlichen Schadsoftware bisher erpressen konnten. Damit verschärft sich die Bedrohung durch Computerkriminalität abermals: Die Erpresser handeln anscheinend völlig skrupellos. Gleichzeitig sind ihre Motive schwer zu durchschauen: Um möglichst viel Lösegeld zu kassieren, wären wohl andere Strategien vielversprechender.

Riesenwelle

Die Ransomware WannaCry (WanaDecrypt0r 2.0) verbreitet sich als Wurm von befallenen Systemen aus weiter. Auch wenn Sicherheitsexperten bereits eine Art "Notabschaltung" aktivieren konnten, welche die Ausbreitungsgeschwindigkeit drosselt, befürchten andere, dass die Verbreitungswelle zum Wochenstart wieder anschwillt: Am Wochenende laufen viele der potenziell anfälligen Windows-Systeme nicht.

Außerdem könnten die Malware-Autoren leicht eine verbesserte Version der Software in Umlauf bringen. Der "Erfolg" ihrer Schadsoftware zeigt, dass nach wie vor sehr viele Computer unzureichend gewartet werden. Im Interview mit dem britischen Sender ITV erklärte Europol-Chef Rob Wainwright, dass nur wenige Banken von WannaCry befallen seien: Sie hätten in der Vergangenheit schmerzhaft aus ihren Erfahrungen gelernt. Diese Lektion stünde anderen noch bevor. Mittlerweile seien Rechner in 150 Ländern betroffen.

Auch das BKA ermittelt, das BSI fordert zur Meldung von Infektionen auf. Die Firma AV-

Angriff mit Krypto-Trojaner WannaCry

Es begann am Abend des 12. Mai 2017 mit Schreckensmeldungen aus Großbritannien: Computer des nationalen Gesundheitssystem waren von einer Ransomware infiziert. Danach verbreitete sich der Krypto-Trojaner WannaCry weltweit, legte hunderttausende nicht gepatchter oder veralteter Rechner lahm und richtete immensen Schaden an.

WannaCry: Angriff mit Ransomware legt weltweit Zehntausende Rechner lahm

WannaCry: Was wir über die Ransomware-Attacke wissen

Microsoft: Angriff durch Krypto-Trojaner WannaCry sollte Weckruf für Regierungen sein

Kommentar: Staatliche Dienste müssen Erkenntnisse teilen

WannaCry: Gewaltiger Schaden, geringer Erlös

Dienste

Security Consulter Emailcheck
Netzwerkcheck Browsercheck
Anti-Virus Krypto-Kampagne

Artikel

Forensik-Tools patzen bei neuer Windows-Kompression

Mit Hilfe einer noch weitgehend unbekannten Dateikompression namens "Compact OS" könnten sich Schad-Programme und andere Beweismittel einer forensischen Untersuchung eines PCs entziehen. Wir haben sechs Standard-Forensik-Tools getestet.

Vom Leben und Sterben der 0days

Viele diskutieren über Zero-Day-Exploits, doch die wenigsten haben je ein lebendiges Exemplar gesehen. Zwei interessante Studien bringen überraschende Erkenntnisse zur Lebenserwartung dieser gefährlichen Spezies.

Warum SHAttered wichtig ist

Die SHAttered benannten Kollisionen zum SHA-1-Verfahren sind ein wichtiger Meilenstein. Sie zeigen klar und deutlich, dass SHA-1 für den Einsatz als kryptographische Hash-Funktion nicht mehr geeignet ist.

Test hat 147 Varianten des Schädlings gefunden.

Schwacher Ertrag

Das geforderte Lösegeld von 300 bis 600 Euro muss in Form von Bitcoins gezahlt werden; bisher sind fünf Bitcoin-Adressen der Erpresser bekannt geworden. Auf diese "Konten" sind bisher wohl nicht mehr als 130 Zahlungen eingegangen, daraus schließt man auf Erlöse von maximal rund 30.000 Euro. Allerdings ist der Verschlüsselungstrojaner auch erst seit Freitag aktiv und die Beschaffung von Bitcoins für das Lösegeld kann etwas dauern.

WannaCry: Microsoft liefert Sicherheits-Patches für veraltete Windows-Versionen

Ransomware WannaCry befällt Rechner der Deutschen Bahn

Ransomware WannaCry: Sicherheitsexperte findet "Kill-Switch" – durch Zufall

Wegducken sinnlos

Doch gerade mit seiner geringen Effizienz belegt WannaCry, wie wichtig konsequenter Schutz vor Schadsoftware ist. Offensichtlich attackieren Computerkriminelle nicht mehr nur Systeme, bei denen sie besonders hohe Erträge vermuten, sondern wahllos alle erreichbaren Rechner. Somit steigt die Wahrscheinlichkeit, dass aggressive Schädlinge auch auf "unscheinbare" oder selten genutzte Computer gelangen.

Möglicherweise verändern sich auch die Angreifer: Frühere Attacken mit Krypto-Trojanern wie Locky schienen auf maximalen Ertrag ausgelegt zu sein. Im Fall von WannaCry scheinen die Autoren die Vorarbeit anderer genutzt zu haben, beispielsweise den EternalBlue-Exploit aus dem Umfeld der NSA.

Mysteriöse Abschalt-URL(s)

Weshalb die WannaCry-Programmierer allerdings einen "Notschalter" eingebaut haben, ist bisher unerklärlich. Der hilft indes bereits Betroffenen nichts und kann wohl auch nicht wirken, wenn ein potenziell verletzbarer Rechner die blockierende URL über seinen Internet-Proxy nicht erreicht.

Laut Twitter-Posts sind mittlerweile WannaCry-Varianten ohne diesen "Kill Switch" und mit anderen Abschalt-Adressen aufgetaucht.

- Kommentar zu WannaCry: Staatliche Dienste müssen Erkenntnisse teilen

(ciw)

Kommentare lesen (485 Beiträge) « Vorige | Nächste »

https://heise.de/-3713689 Drucken

Mehr zum Thema **WannaCry** **Ransomware** **Virenscanner** **Malware**

Neueste Forenbeiträge

Re: ich brauche eine VERSTÄNDLICHE Backupsoftware!!!!!! NICHT Paragon!!!!!!!

Forenpilz schrieb am 15.05.2017 21:21: Zitiert aus einem Rundmail aus den 90ern?

Forum: WannaCry & Co.: So schützen Sie sich

von Clö; 15.05.2017 22:04

Was ist der Unterschied zwischen Zeugen Jehovas und Linuxern?

1) Zeugen Jehovas sind von ihrem Produkt nicht so überzeugt wie Linuxer 2) Bei Zeugen Jehovas ist der Missionierungsdrang nicht so hoch 3)…

Forum: WannaCry & Co.: So schützen Sie sich

von ginfizz53; 15.05.2017 22:04

Re: Backups alternativlos ?

Das kommt auf da Backup an..... Ein Backup auf eine USB Platte die immer am PC steckt = kein Backup Ein Backup auf eine USB Platte die nicht…

Forum: WannaCry & Co.: So schützen Sie sich

von Alias77; 15.05.2017 22:01

Der Kommentar

1 2 3 4 5

Truecrypt ist unsicher - und jetzt?

Sollten wir jetzt wirklich alle auf Bitlocker umsteigen, wie es die Truecrypt-Entwickler vorschlagen? Einen echten Nachfolger wird es jedenfalls so bald nicht geben - und daran sind nicht zu letzt auch die Truecrypt-Entwickler schuld.