« Vorige | Nächste »

WannaCry: Was wir bisher über die Ransomware-Attacke wissen UPDATE

13.05.2017 16:20 Uhr – Volker Briegleb vorlesen

Nicht nur die Deutsche Bahn ist von WannaCry betroffen... (Bild: Martin Wiesner)

Es begann am Freitagabend mit Schreckensmeldungen aus Großbritannien: Computer des nationalen Gesundheitssystem waren von einer Ransomware infiziert. Inzwischen hat sich WannaCry weltweit verbreitet.

Seit Freitagabend breitet sich die Ransomware WannaCry (WanaDecrypt0r 2.0) im weltweiten Internet aus. Es handelt sich um einen Kryptotrojaner, der Daten auf den betroffenen Computern verschlüsselt. Gegen die Zahlung einer bestimmten Summe in Bitcoin soll der Nutzer den Code für die Entschlüsselung erhalten. Weltweit sollen zur Stunde über 100.000 Systeme betroffen sein. Anders als Locky & Co springt der Schädling von einem infizierten Rechner auf andere, übers Netz erreichbare Windows-Systeme über. In Deutschland hat das Bundeskriminalamt BKA Ermittlungen aufgenommen.

Großbritannien schwer getroffen

Nach bisherigen Erkenntnissen hat sich der Schädling am Freitag zunächst in Russland ausgebreitet und dann schnell auch in anderen Ländern verbreitet. Es sind vor allem ältere Windows-Versionen betroffen, die nicht mehr mit Sicherheits-Updates versorgt werden. Besonders schwere Folgen hatte das in Großbritannien, wo WannaCry zahlreiche Rechner des National Health Service (NHS) befallen hat und die staatliche Gesundheitsversorgung massiv gestört ist. Autohersteller Nissan hat gegenüber britischen Medien einen Befall der Fabrik in Sunderland bestätigt. In dem Werk war die Produktion am Wochenende ohnehin unterbrochen.

Renault stoppte laut Agenturberichten den Betrieb in einigen Werken in Frankreich. Das seien "Schutzmaßnahmen, um eine Ausbreitung der Schadsoftware zu verhindern", sagte ein Firmensprecher der Nachrichtenagentur AFP. Nach Informationen aus Gewerkschaftskreisen sei das Werk in Sandouville in der Region Seine-Maritime mit rund 3400 Mitarbeitern besonders betroffen gewesen, hieß es. Allerdings sei dort am Wochenende auch nur eine eingeschränkte Produktion geplant gewesen.

Auch aus anderen Ländern werden Infektionen von wichtigen Unternehmen gemeldet, in Spanien und Portugal sind zum Beispiel die großen Netzbetreiber Telefónica und Telecom betroffen. Aus den USA meldet der Logistikriese FedEx eine Infektion. Hierzulande hat es bisher vor allem die Deutsche Bahn erwischt, deren Anzeigesystem auf vielen Bahnhöfen ausgefallen ist. Der Fahrbetrieb soll nicht gefährdet sein. Auch bei anderen Unternehmen wurden Fahrschein- und andere Automaten infiziert; ein Leser schickte ein Bild von einem betroffenen Bezahlautomaten im Parkhaus des Berliner Flughafens Tegel.

Zwei Angriffsvektoren

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.

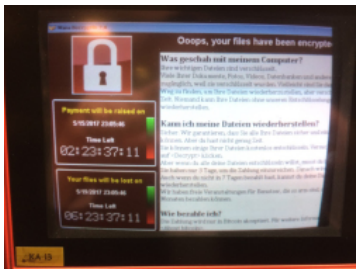
Vom Leben und Sterben der 0days

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.

Nach bisherigen Erkenntnissen nutzt WannaCry zwei Angriffsvektoren: Einmal verbreitet er sich – wie bei Kryptotrojanern üblich – per E-Mail. So sagte ein DB-Sprecher der dpa, der Angriff auf die Bahn sei durch E-Mails ausgelöst worden. Doch wenn der Schädling ein Sytem infiziert hat, versucht er auch, wie ein Wurm andere Rechner im gleichen Netz zu kompromittieren. Dafür nutzt WannaCry offenbar eine Lücke in Windows Dateifreigaben (SMB). Diese Lücke war bekannt geworden, nachdem eine Hackergruppe namens Shadow Brokers einige Exploits der NSA-nahen Equation Group veröffentlicht hatte. Der Exploit, der die von WannaCry genutzte Lücke ausnutzt, ist unter dem Namen EternalBlue bekannt.



...auch bei den Bezahlautomaten im Parkhaus des Berliner Flughafens Tegel ging nichts mehr. Die Kunden durften dann so ausfahren.

Bild: Hagen Meischner

Microsoft hatte die verantwortliche Sicherheitslücke bereits im März durch Sicherheits-Updates geschlossen. Diese Patches liefert der Hersteller jedoch nur für die aktiv unterstützten Windows-Versionen. Ältere Windows-Versionen blieben also weiter ungeschützt – dazu gehören insbesondere Windows XP und Windows Server 2003. Updates für diese hat das Unternehmen am Samstag kurz nach Ausbruch der WannaCry-Epidemie nachgereicht. Manche Anwender schalten allerdings die automatische Installation von Sicherheits-Updates ab, was dazu führt, dass derartige Lücken offen bleiben.

Unbedingt Patchen!

Nutzer sollten Windows-Sicherheitspatches grundsätzlich immer installieren. Wer Microsofts Sicherheitsupdate MS17-010 noch nicht eingespielt hat, muss das jetzt nachholen. Das gilt auch für Besitzer älterer, nicht mehr offiziell supporteter Windows-Versionen wie XP. Wer so einen Rechner am Netz betreibt, setzt sich einem erhöhten Risiko aus und sollte ernsthaft darüber nachdenken, ein aktuelles Betriebssystem zu nutzen. Windows-10-Installationen sind bisher nicht von WannaCry betroffen.

Insbesondere Unternehmen sind aufgerufen, sich um ihre Sicherheit zu kümmern. Der aktuelle Angriff sei "ein erneuter Weckruf für Unternehmen, IT-Sicherheit endlich ernst zu nehmen und nachhaltige Schutzmaßnahmen zu ergreifen", sagte Arne Schönbohm, Präsident des Bundesamts für Sicherheit in der Informationstechnik (BSI). Das BSI ruft zudem betroffene Institutionen auf, Vorfälle zu melden, "um einen möglichst vollständigen Überblick über die Lage zu bekommen".

Inzwischen scheint die Verbreitung des Schädlings zumindest verlangsamt. Sicherheitsforscher haben durch Zufall einen Mechanismus entdeckt, der die Verbreitung von WannaCry stoppt. Im Code des Schädlings fanden sie den Hinweis auf eine seltsame URL, zu der noch keine passende Domain registriert war. Einer der Forscher registrierte die Adresse, weil er sich davon weitere Erkenntnisse über den Kryptotrojaner versprach. Auf einem unter dieser Adresse betriebenen Server verzeichnete er sofort tausende Verbindungsversuche.

Verbreitung verlangsamt?

Damit haben die Forscher offenbar zufällig eine Art Sicherheitsmechanismus ausgelöst. Bisherigen Erkenntnissen zufolge beendet der Trojaner seine Weiterverbreitung, sobald er auf Anfragen an die kryptische Domain eine Antwort bekommt. Seit der Server der Sicherheitsforscher antwortet, verbreiten sich die mit einer Antwort ruhig gestellten Instanzen des Schädlings nicht weiter. Das ist aber keine Entwarnung – zumal einmal infizierte Rechner verschlüsselt bleiben. Es ist auch damit zu rechnen, dass sehr bald neue Schädlinge erscheinen, die den Notaus-Server ignorieren.

Unbestätigten Berichten zufolge blockieren auch einige Antivirus-Programme den Zugriff auf die betreffende Domain, weil sie den Traffic für verdächtig halten. Das ist immens kontraproduktiv: Wenn der Wurm keine Antwort bekommt, verbreitet er sich munter weiter.

Update 17:32 Uhr: *Angaben zu Renault in Frankreich im dritten Absatz ergänzt.* (vbr)

Kommentare lesen (417 Beiträge) « Vorige | Nächste »

Forum bei heise online: **Sicherheit**

Unternehmensdaten in der Cloud – ein Risik o?

Neueste Forenbeiträge

Neuer Treiber seit dem 11.05.2017

HP hat auf seinen Software- und Treibersupport-Seiten für die betroffenen Geräte einen Conexant HD Audiotreiber zur Verfügung gestellt. Er trägt…

Forum: HP-Notebooks: Audio-Treiber belauscht T..

von lliberty123de; 14.05.2017 03:12

Re: Könnten Sie Bitte einen Perma-Link anbringen ,mit lauffähigem Desinfect?

Es wird immer Probleme mit spezieller HW geben. Bei mir kann ich das Wifi nicht aktivieren. Aber die ct hat ja auch einen Artikel wie man…

Forum: Desinfect

von chilango; 13.05.2017 23:56

Re: Liebe HP, das ist kein "Fehler", das ist mehr

salametti schrieb am 13.05.2017 22:12: Wie willst du das denn beweisen? [/quote] HP will sich doch entlasten, IMHO müßten sie den Beweis…

Forum: Keylogger auf HP-Notebooks: Hersteller g..

von amnesie; 13.05.2017 23:01

Der Kommentar

1 2 3 4 5

Warum wir Forward Secrecy brauchen

Der SSL-GAU zeigt nachdrücklich, dass Forward Secrecy kein exotisches Feature für Paranoiker ist. Es ist vielmehr das einzige, was uns noch vor einer vollständigen Komplettüberwachung aller Kommunikation durch die Geheimdienste schützt.