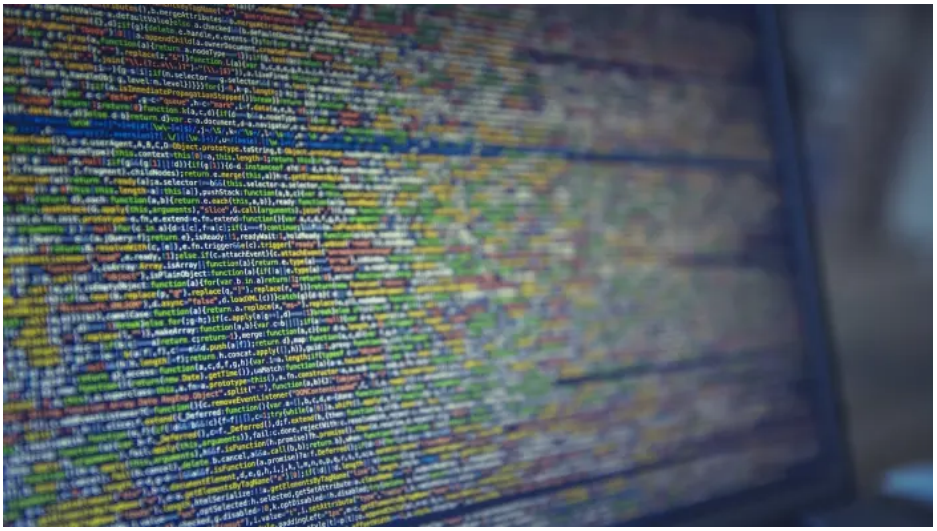
EternalBlue: Hunderttausende Rechner über alte NSA-Schwachstelle infizierbar

19.09.2018 12:48 Uhr – Fabian A. Scherschel



(Bild: Pixabay)

Viele Windows-Rechner kranken auch über ein Jahr nach dem WannaCry-Ausbruch immer noch an der ursprünglichen Schwachstelle – Schuld haben die Raubkopierer.

Altlasten des US-Geheimdienstes NSA bedrohen nach wie vor hunderttausende ungepatchte Windows-Computer. Wie mehrere Sicherheitsforscher und Anti-Viren-Hersteller berichten, gibt es immer noch haufenweise Malware, die es auf die mit dem Codenamen EternalBlue bezeichnete Schwachstelle abgesehen hat. Das Risiko trifft vor allem Rechner, auf denen raubkopierte Windows-Versionen im Einsatz sind. Für vernünftig gepflegte Systeme sollte EternalBlue schon lange keine Gefahr mehr darstellen, immerhin hatte Microsoft die zugrundeliegende Sicherheitslücke selbst in Windows-Versionen gestopft, die eigentlich schon lange keinen Support mehr bekommen.

Ewiger Infektionskreislauf

Wie der AV-Hersteller Avira berichtet, finden sich allerdings nach wie vor mehr als 300.000 Rechner, die über ungepatchte Varianten der SMB1-Schnittstelle angreifbar sind. Die Dunkelziffer ist wahrscheinlich viel höher. Die verwundbaren Rechner werden immer wieder neu über die Lücke infiziert, obwohl Anti-Viren-Programme und auch die Trojaner gegenseitig immer wieder Schadcode entfernen. Da die zugrundeliegende Lücke allerdings ohne ein entsprechendes Windows-Update weiter klafft, stecken diese Geräte in einem nicht enden wollenden Infektionskreislauf fest. Ein Aspekt dabei ist auch, dass die verschiedenen Schadprogramme dabei immer wieder die umliegenden Netze auf der Suche nach neuen Opfern mit Traffic zumüllen.

Da es unrealistisch scheint, dass Nutzer von Windows-Raubkopien Systemupdates erhalten oder gar erhalten wollen, empfiehlt Avira den Betroffenen, das SMB1-Protokoll kurzerhand abzustellen. Hinweise dazu, wie das im Detail umzusetzen ist, finden sich auch bei Microsoft. Auf Systemen, auf denen Anti-Viren-Programme von Avira laufen und die entsprechende Sicherheitsupdates nicht installiert haben, führt Avira diesen Schritt für die Nutzer automatisch aus.

Dienste

Security Consulter
Emailcheck
Netzwerkcheck
Browsercheck
Anti-Virus
Krypto-Kampagne

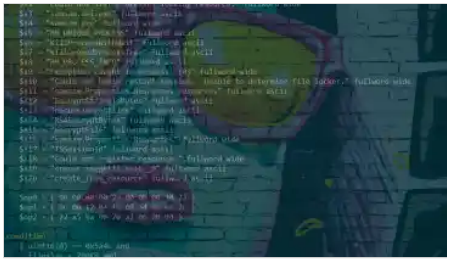
Alerts! alle Alert-Meldungen

Enigmail UPDATE

Kritisches Update: Adobe Acrobat und Reader

Verschiedene Cisco-Produkte

Artikel



YARA Rulez! Malware-Samples suchen und finden

Online-Sandbox-Services sind echte Fundgruben für Sicherheitsforscher. Hybrid Analysis erleichtert ihnen die Malware-Jagd jetzt mit YARA-Regeln.

Hintergrund

Folgen der NSA-Spionagetaktik

Die Auswirkungen der EternalBlue-Schwachstelle sind der Allgemeinheit spätestens nach den Massenausbrüchen der Trojaner WannaCry und Petya bekannt. Die Lücke stammt ursprünglich aus dem Zero-Day-Arsenal der NSA. Der US-Geheimdienst hatte sie mehr als drei Jahre lang für verdeckte Angriffe auf alle möglichen Ziele eingesetzt, bis die Agency die Lücke schließlich aus Angst vor der Hackergruppe Shadow Brokers an Microsoft meldete.

Das wiederum führte dazu, dass Microsoft zum ersten mal in seiner Firmengeschichte einen Patchday absagte, um die Schwachstelle so schnell wie möglich zu stopfen. Bei der NSA hieß es, die Ausbeute aus dieser einen Lücke sei "unglaublich" gewesen. Wie sich jetzt zeigt sind die Folgen der US-Sicherheitspolitik im Fall EternalBlue ebenfalls noch nicht ausgestanden. (fab)

Kommentare lesen (320 Beiträge)

Forum zum Thema: Desktopsicherheit

https://heise.de/-4167918 Drucken

Mehr zum Thema:

GEHEIMDIENSTE | MICROSOFT | NSA | SMB | TROJANER | WINDOWS

Googles Security-Chefin: Mehr Sicherheit durch bessere Zusammenarbeit

Parisa Tabriz steuert maßgeblich Googles Sicherheits-Aktivitäten und ist damit eine der einflussreichsten Persönlichkeiten der Security Szene. In ihrer Keynote erklärt sie, worauf es ankommt.

Lesetipp 122

Man-in-the-Middle-Angriff: Online-Zocker im Visier von Online-Kriminellen

Mit einem ungewohnt ausgefeilten Trojaner machen Online-Ganoven derzeit Jagd auf Gamer: Der Schädling installiert ein Root-Zertifikat und manipuliert damit TLS/SSL-Verbindungen. Er wird über YouTube verbreitet

Hintergrund

Neueste Forenbeiträge

Im Klartext?

Ungesalzenes MD5 wäre ja noch plausibel und traurig genug, Klartext nicht - so ein Hoster gehört vorsorglich stillgelegt.

Forum: Domainfactory-Hacker knackt Kundendate…

von RealFreeJack; vor 55 Sekunden

Re: "Kundenpasswörter im Klartext" - ernsthaft? Noch immer in 2018?

jop hab ich auch so im Kopf, dass Behörden und Geheimdienste (ich glaub sogar Ausländische) in AT nicht belangt werden können zu mindestens…

Forum: Domainfactory-Hacker knackt Kundendate…

von blablub84; vor einer Minute

Doch

semanino schrieb am 05.10.2018 13:31: Entscheident ist der Sitz der Firma, nicht die Besitzverhältnisse.

Forum: Domainfactory-Hacker knackt Kundendate…

von nibbles.bas; vor 2 Minuten

nach oben

NEWS UND ARTIKEL

News
7-Tage-News
News-Archiv
Hintergrund-Artikel
Alert-Meldungen

SERVICE

Newsletter
Tools
Foren
RSS
mobil

DIENSTE

Security Consulter
Netzwerkcheck
Anti-Virus
Emailcheck
Browsercheck
Krypto-Kampagne

Datenschutzhinweis Impressum Kontakt Mediadaten 2504068