Und täglich grüßt das Würmertier – oder warum wir von Ransomware nicht wirklich überrascht sein sollten

Ein Kommentar zur aktuellen Ransomware-Welle von Michael Veit, Security-Experte bei Sophos

Wiesbaden, 17. Mai 2017 – „Es ist ziemlich aggressiv und vermehrt sich sehr schnell" – das könnte die Aussagen eines gestressten System-Administrators sein, der vergangene Woche von der WannaCry (Wanna Decryptor) Ransomware betroffen war. Tatsächlich ist dies aber ein Statement, das ein Security-Experte vor 13 Jahren zu einer neuen Variante des Sasser-Wurms gab. WannaCry zielt auf nicht gepatchte Windwows SMB-Fehler. Genauso wie seinerzeit 2004 Sasser auf nicht gepatchte Windows Exploits in lokalen Security Authority Subsystem Services (LSASS – daher „Sasser") aus war, die ironischerweise ein Teil des Betriebssystems sind, das Security-Einstellungen verwaltet.

Zwar denkt man, dass die Zahl der Opfer von WannaCry imposant ist, doch von Sasser waren so bekannte Unternehmen wie die Deutsche Post, die EU-Kommission und Delta Airlines – um nur ein Auswahl zu nennen – betroffen. Kurioserweise wurde Sasser eher als harmlos denn als existenzbedrohend eingestuft, da es nach einer Reihe an Mega-Würmern wie ILOVEYOU, Nimda, Welchia, Nesky, SoBig, Blaseroder oder SQL Slammer erschien. Viele dieser Schadprogramme nutzten Microsoft-Schwachstellen aus und sorgten für so viel Ärger, dass man sich schwor: „Nie wieder!"

Doch 2008 erschien mit Conficker der nächste große Wurm auf der weltweiten Bühne, der auch drei Jahre danach noch 1,7 Millionen Systeme pro Jahr infizierte. Was war das für eine Welt, in der der Sasser-Wurm hunderttausende Netzwerke infizierte und lediglich als bloßes Ärgernis angesehen wurde? Anscheinend ein Welt, in der Würmer üblich waren und deren Ära wir als „Goldenes Malware-Zeitalter" bezeichnen könnten. Experten wissen, warum Würmer zu Beginn der 2000er so erfolgreich waren: Das Internet ermöglichte die rapide Infektion und Patching steckte noch in den Kinderschuhen. Wenn etwas möglich wird, wird es irgendwann jemand versuchen. Nicht lange danach wird jemand es kopieren und so geht der Zyklus weiter.

Würmer sind in den letzten Jahren selten geworden. Vielleicht deshalb, weil Cyberkriminelle Stealth-Attacken mittlerweile als die bessere Angriffstaktik sehen. Und doch bleibt die Verteidigung gegen Würmer schwierig. Admins können Dienste oder Ports auf Firewall-Ebene blockieren, aber oft nicht unbegrenzt. Das Aufhalten und Checken von E-Mails ist eine weitere Taktik, die aber oft nur solange funktioniert, bis sich alle beklagen.

Der WannaCry-Wurm erinnert die Menschen daran, dass sie schnell vergessen. Der Mensch hat sich zur Gewohnheit gemacht, von neuer Malware, die thematisch alt ist, überrascht zu werden. Und beim nächsten Mal kann es aber noch schlimmer werden, wie ein Blick in die jüngere Vergangenheit zeigt. 2012 wurde zum Beispiel die Saudi Aramco Oil Company von einer Malware namens Shamoon angegriffen, die sehr schnell die Master Boot Record (MBR) von 35.000 PC-Festplatten enterte. Und auch danach gab es immer wieder derartige Attacken, die sehr zeitraubend und teuer für die betroffenen Unternehmen sind.

Eine Malware, die die Zerstörung von Festplatten mit einem Wurm kombiniert, kann nicht nur Tage sondern Wochen der Unterbrechung verursachen, und es kostet viel Geld, die

Schäden zu beheben – vom Vertrauensverlust noch gar nicht gesprochen. Wir alle sollten aus der Historie lernen und die entsprechenden Konsequenzen ziehen. Wirklich jetzt!

Über Sophos
Sophos ist führender Anbieter von Endpoint- und Network-Security-Lösungen der nächsten Generation. Als Pionier der Synchronized Security entwickelt Sophos sein innovatives Portfolio an Endpoint-, Netzwerk-, Verschlüsselungs-, Web-, E-Mail- und mobilen Security-Lösungen, die miteinander kommunizieren. Mehr als 100 Millionen Anwender in 150 Ländern verlassen sich auf Lösungen von Sophos mit hervorragendem Schutz vor anspruchsvollen Bedrohungen und Datenverlust. Sophos Produkte sind exklusiv über den weltweiten Channel mit mehr als 26.000 registrierten Partnern erhältlich. Sophos hat seinen Hauptsitz in Oxford, Großbritannien, und wird an der Londoner Börse unter dem Symbol "SOPH" öffentlich gehandelt. Weitere Informationen unter www.sophos.de

Pressekontakt:

Sophos
Jörg Schindler, PR Manager CEEMEA
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +172 4536839
sophos@tc-communications.de