Vom aggressiven Infekt zum fragwürdigen Impfstoff: WannaCry bildet immer neue Varianten aus. Mit überraschendem Immunisierungseffekt.

Sophos-Report zu WannaCry Ransomware:
Tausende Mutationen, zahlreiche ungepatchte Computer, zufälliger Impf-Effekt.
USA absolute Hochburg.

Die Beute bleibt die gleiche. Aber das Jagdverhalten ändert sich. Der neueste Report von Sophos „WannaCry Aftershock“ gibt einen Überblick über die WannaCry Schadsoftware, die es mit einer weltweiten Angriffswelle am 12. Mai 2017 zu einiger Bekanntheit geschafft hat. Die Analysen der Sophos-Forscher zeigen, dass WannaCry weiterhin aktiv ist, mit Millionen versuchten Neuinfizierungen jeden Monat.

Die mit sehr großem Abstand meisten Infektionen (22 Prozent weltweit) konnten die Sophos-Experten dabei in den USA nachweisen, gefolgt von Indien und Pakistan mit jeweils rund 8 Prozent. Deutschland rangiert mit nur 0,5 Prozent relativ weit hinten in der Rangliste, noch weniger betroffen sind in Europa Großbritannien und die Niederlande. Deren Nachbar, Belgien, ist mit 2,1 Prozent europaweit am zweitstärksten betroffen, Spitzenreiter bei den Infektionen in Europa ist Italien mit knapp 6 Prozent.

Clever, aber nicht smart: Mutationen umgehen „Kill Switch“ sind aber wirkungslos
Während der Originalstamm der Schadware bis heute unverändert geblieben ist, fanden sich zuletzt zahlreiche kurzlebige Mutationen. Die ursprüngliche WannaCry-Malware wurde nur 40 Mal erkannt. Bis Ende 2018 haben die SophosLabs-Forscher 12.480 Varianten des ursprünglichen Codes identifiziert. Allein im August 2019 betrug die Anzahl der beobachteten verschiedenen Varianten 6.963, davon waren 5.555 oder 80 Prozent neue Dateien.

Das Fortbestehen der WannaCry-Bedrohung ist im Wesentlichen auf die Fähigkeit der neuen Varianten zurückzuführen, den "Kill Switch" zu umgehen – hierbei handelt es sich um eine spezifische URL, die, wenn die Malware eine Verbindung herstellt, den Infektionsprozess automatisch beendet. Bei tieferer Betrachtung von mehr als 2.700 Proben stellte sich jedoch gleichzeitig heraus, dass alle Proben zwar den "Kill Switch" umgangen, alle nun aber auch eine beschädigte Ransomware-Komponente hatten und keine Daten verschlüsseln konnten.

WannaCry-Mutationen immunisieren anfällige Computer
Die Art und Weise, wie WannaCry seine Opfer infiziert – kurzer Check, ob der Computer bereits befallen ist und wenn ja, den nächsten PC testen – führt zu einer Art Schutzimpfung: die schon bestehende Infektion durch eine inaktive Version der Schadsoftware schützt vor der Neu-Infektion mit einem aktiven Stamm. Neue Varianten der Malware wirken auf diese Weise also wie ein versehentlicher Impfstoff und bieten nach wie vor ungepatchten und anfälligen Computern eine Art Immunität gegen spätere Angriffe derselben Malware.

Die Tatsache aber, dass diese PCs überhaupt infiziert werden konnten, lässt den Rückschluss zu, dass der Patch für den Exploit (durch den WannaCry ins System gelangt) noch nicht installiert wurde. Ein Patch, der vor mehr als zwei Jahren herausgegeben wurde.

Hohe Infektionsquote zeigt sorglosen Sicherheitsumgang

Michael Veit, Security Experte bei Sophos, ordnet die Ergebnisse des aktuellen WannaCry Reports so ein: „Der WannaCry-Ausbruch 2017 veränderte die Bedrohungslandschaft weltweit. Der Report zeigt auf, wie viele ungepatchte Computer es noch immer gibt. Und wenn bereits das Sicherheitsupdate, das vor mehr als zwei Jahren schon notwendig war, noch nicht umgesetzt ist, ist anzunehmen, das nachfolgende Patches auch nicht installiert wurden. Auch wenn die Varianten von WannaCry eine Art Immunisierung mitliefern, sollte sich niemand auf diesen zufälligen Schutz verlassen. Das Installieren von Sicherheitspatches sollte Standard-Praxis werden, in Kombination mit einer konsistenten Sicherheitsstrategie, die Endpoint, Netzwerk und Systeme abdeckt."

Sicherheitstipps zum Schutz vor Wannacry und Ransomware-Angriffen im Überblick:

- Komplette Inventur aller Geräte, die mit dem eigenen Netzwerk verbunden sind. Sie sollte alle über die neueste Sicherheitssoftware verfügen.
- Die aktuellsten Patches sollten so schnell wie möglich ans Gerät.
- Das Patch gegen das EternalBlue Exploit, das WannaCry nutzt, ist eingespielt? Bei Unsicherheit, dieser Anleitung folgen: How to Verify if a Machine is Vulnerable to EternalBlue - MS17-010
- Reguläre Back-ups machen und offline lagern. Sehr hilfreich bei einer Ransomware-Attacke.
- Am besten auf das bewährte, mehrschichtige Security-Modell setzen. Sophos Intercept X, zum Beispiel, arbeitet mit einem übergreifenden Defense-in-Depth-Ansatz für den Endpoint-Schutz, der Kombination mehrerer führender Next-gen-Technologien zum Aufspüren von Schadsoftware und EDR (Endpoint Detection and Response).

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 +49-172-4536839
sophos@tc-communications.de