Ransomware bleibt ein Problem – nicht nur für Windows

SophosLabs analysiert in einem Whitepaper die diesjährige Schadsoftware und beschreibt die voraussichtlichen Gefahren für 2018. Ransomware ist gefährlicher denn je und hat zunehmend Linux, Mac und Android-Systeme im Blick.

Wiesbaden, 16. November 2017 – Ransomware hat Unternehmen und Privatanwender in diesem Jahr auffällig zugesetzt. SophosLabs kommt nach seiner Analyse von Daten aus April bis Oktober 2017 zur Prognose, dass auch das nächste Jahr von Ransomware und RaaS (mit DIY-Bausätzen) geprägt sein wird. Neben Windows müssen sich zukünftig auch Linux, Mac und Android User wappnen.

RaaS (Ransomware as a Service) sind ein ernstzunehmendes und wachsendes Problem: die DIY-Kits sind für jedermann im Dark Web erhältlich, unabhängig von IT-Know-how. Beispiele: Cerber Satan, Philadelphia (das sich sogar ein YouTube-Werbevideo im offenen Web verpasste). Und: setzten die Entwickler als Währung bislang auf Bitcoin, weiteten sie die Zahlungsmodalitäten in 2017 auch auf Crypto-Währungen wie Monero aus.

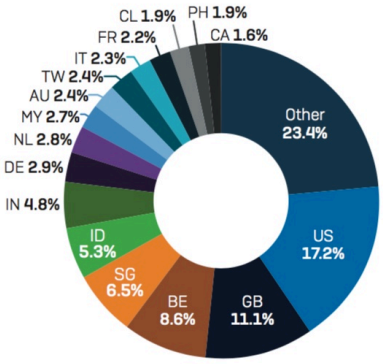
WannaCry und Cerber dominieren die Ransomware-Landschaft
Während Cerber lange Zeit als produktivste Ransomware-Familie galt, wurde seine Schlagkraft für ein paar Monate überschattet. Denn Mitte Mai stürmte WannaCry die Bühne, auf dem Rücken eines Wurms, der eine alte Windows Schwachstelle nutzte. WannaCry lassen sich mehr als 45,3 Prozent aller Ransomware zwischen April und Oktober 2017 zuschreiben.

WannaCry war eine Überraschung mit Retrocharme: es war nicht die typische Ransomware, die sich via Link oder Anhang in Emails verbreitet. Sie kaperte hunderttausende Computer weltweit mit Hilfe eines Wurms – und erinnerte damit an die frühen 2000er. Auch wenn WannaCry den Rest des Jahres aktiv war, lässt sich bereits ein Rückgang erkennen. Leider muss für 2018 mit steigenden Angriffen gerechnet werden angesichts von WikiLeaks und Shadow Brokers, die Maßnahmen der Regierungen gegen weitere Angriffe veröffentlichen.

Cerber mit 44,2 Prozent aller Ransomware-Angriffe nur minimal hinter WannaCry bleibt gefährlich. Besonders seine mutierende Fähigkeit, Sandboxes und Antiviren-Schutz zu umgehen. Die Entwickler der Schadsoftware kümmern sich liebevoll um ihren Schützling, mit konsequenten Updates und Verbesserungen. Das macht Cerber so produktiv wie gefährlich.

Kaum ins Gewicht für Ransomware (3,9 Prozent Anteil) fällt die dritte Erpresser-Familie Locky. Im Sommer aber zeigte sie Tendenzen zur Wiederauferstehung, mit vier neuen Variationen (.diablo6, .lukitus, .ykcol, .asasin).

Die meisten Ransomware-Angriffe in USA und Großbritannien, Deutschland 7.
Zwischen 1. April und 3. Oktober zirkulierte mit 17,2 Prozent die meiste Ransomware in den USA. Vize-Ransomware-Meister ist Großbritannien mit 11,1 Prozent, Belgien belegt den dritten Platz. Deutschland schafft es unter die Top Ten an 7. Stelle (2,9 Prozent).



Ransomware-Angriffe nach Ländern

Die Analyse der Attacken gibt neben dem Verbreitungsort aber noch etwas anderes preis: die stärksten Aktivitäten waren Mitte Mai und Ende Juni, zuzuschreiben WannaCry und NotPetya. Ein weiterer Peak Mitte/Ende August lässt sich auf die Wiederauferstehung von Locky zurückführen. WannaCry und Cerber blieben währen der gesamten Beobachtungsperiode präsent. Während NotPetya den größten Peak verantwortete, passierte danach kaum noch etwas: die Opfer konnten ihren Erpresser zur Lösegeldzahlung gar nicht mehr erreichen. SophosLabs geht nach seiner Untersuchung davon aus, dass NotPetya eher ein Experiment war. Oder: das Ziel der Software war, nicht Ransomware sondern etwas weitaus Zerstörerisches zu entwickeln, wie einen Data Wiper (Dateien-Löscher).

Aussichten für 2018 und Tipps
Die Mehrheit der Ransomware-Angriffe betraf 2017 Windows-Nutzer. Doch die Analyse zeigt auch eine wachsende Anzahl an Attacken auf Android, Mac, und Linux Systeme. Und: RaaS-Bausätze müssen als ernstzunehmende Gefahrenquelle eingeordnet werden.

Neben den gängigen und bewährten Empfehlungen für jeden User, sich vor Ransomware zu schützen, wie regelmäßige Back-ups auf anderen Geräten, Explorer-Einstellungen zu Dateiendungen und Java-Script Anhängen, aktuellem Anti-Ransomware-Schutz (wie Intercept X), gilt besonders:

Unternehmen sollten ihre Mitarbeiter konsequent zum Thema Schadsoftware und Social Engineering schulen. Und auch die eigenen Systeme regelmäßig updaten und auf Schwachstellen überprüfen.

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