Weltweiter Spam sinkt um mehr als die Hälfte – was kommt jetzt?

Die Menge an weltweit verschicktem Spam ist seit Dezember dramatisch gesunken. Das an sich ist nichts Neues – aber die Dauer verblüfft. Wurde das bekannte Botnet Necurs in einen Schlafmodus versetzt? Wird es wieder aktiv? Es bleibt spannend. Und: Die Gefahren durch Mal- und Ransomware bestehen derweil weiter. Drei Empfehlungen von Sophos, wie wir uns weiterhin schützen können.

Von Michael Veit, Security Experte bei Sophos

Wiesbaden, 7. März 2017. Die Menge an weltweit verschicktem Spam ist dramatisch gesunken. Wir reden hier nicht über Phishing Mails, billige Viagra-Pillen oder endlose Umfragen, bei denen man ein iPhone gewinnen kann – dieser Spam müllt nach wie vor unser Postfach voll. Nein, wir reden über eine andere Sorte von heimtückischen Emails: Versandinformationen über angebliche Paketlieferungen, falsche Lebensläufe in Bewerbungsunterlagen sowie Rechnungen und Mahnungen nicht gekaufter Waren. Das Ziel: der Adressat soll den Anhang öffnen und sich damit Ransomware wie Locky oder Banking-Trojaner wie Dridex auf den PC laden.

Hübsch verpackt, aber mit tückischen Makros, als Microsoft Word und Excel oder wie kürzlich als JavaScript und Windows Script Files, folgen die Anhänge einem einfachen Regelwerk: wenn man sie startet, sprechen sie umgehend ihren Home Server an, der von den Betrügern gesteuert wird. Dann wird ein Malware Sample heruntergeladen, um den PC zu infizieren. Oder – wie zur Zeit gängig – gleich mehrere verschiedene Schädlinge.

Rückgänge gibt es immer wieder, neu ist aber die Dauer

Soweit das bekannte Spam-Prinzip. Seit kurz vor Weihnachten 2016 aber hat sich das Spam-Niveau um mehr als die Hälfte verringert. Solche Unterbrechungen sind nicht gänzlich neu, wohl aber, dass sie seit über zwei Monaten bestehen – ohne nennenswerte Anzeichen für ein erneutes Anwachsen des Spam-Levels.

Das Sophos Spamtrap Network zeichnet täglich das weltweite Spamvolumen auf. Grafisch dargestellt wird der Einbruch besonders sichtbar: Kurz vor Weihnachten 2016 endet das hohe Level abrupt. Statt spitzer Ausschläge, ein basso continuo auf deutlich gesenktem Niveau. Ähnliche Ergebnisse zeigen auch die öffentlich zugänglichen Daten von CBL (Composite Blocking List), auf die sich auch Spamhaus stützt.

Eine nachgewiesene Erklärung gibt es nicht, wohl aber Hinweise darauf, dass das bekannte Botnet Necurs stillgelegt ist. Necurs wird nachgesagt, als eines der größten Botnetze mehr als 6 Millionen Computer infiziert zu haben. Die Mehrheit davon scheint in Indien zu stehen. Aber fast jedes Land der Welt ist von dieser Schadsoftware betroffen – mit Ausnahme von Russland: die Necurs Malware verschont gezielt Computer mit russischer Tastatur.

Was passiert, wenn Necurs wieder „aufwacht“?
Interessanterweise gab es schon einmal einen starken Rückgang des Spamlevels im Juni 2016. Nach weniger als einem Monat hatte Necurs wieder seine volle Schlagkraft entwickelt, mit einer neuen Version von Locky. Warum das Botnet dieses Mal stillgelegt ist, wie lange die Unterbrechung dauert und ob es danach zu seinem vorherigen Umfang zurückkehrt? Keiner weiß es. Was wir aber wissen: dieser Zustand hat nicht dazu geführt, dass User nicht mehr von Locky & Co. attackiert werden– trotz des dramatischen Spam-Rückgangs. Wir wissen auch, dass Necurs nicht komplett abgeschaltet ist, nur sehr viel ruhiger ist als vorher. Mit anderen Worten: wenn Ihr Computer Teil dieses Botnets ist, ist er immer noch infiziert und wartet auf weitere Anweisungen. Und wenn irgendwann der Weckbefehl kommt, geht der Spamversand weiter.

Das empfehlen die Sophos-Sicherheitsexperten, damit Ihr Computer die Kriminellen nicht unterstützt:

1. **Halten Sie Ihre Anti-Virus-Software aktuell**
   Spielen Sie regelmäßig die neuesten Sicherheits-Patches ein, um optimal geschützt zu sein.

2. **Seien Sie vorsichtig beim Öffnen von Anhängen und Programmen**
   Wenn Sie den Absender nicht kennen oder sich unsicher sind, schauen Sie sich die Versandadresse an oder machen Sie einen Mouseover über den anzuklickenden Link. Häufig geben kryptische Zeichen bereits einen Hinweis darauf, dass es sich um Spam handelt.

3. **Als Sys-Admin: Spam Filter für rausgehende Mails setzen**
   Lassen Sie ausgehende Mails ebenfalls über einen Spam-Filter laufen und vermeiden Sie so, dass aus Ihrem Unternehmen selbst Spam versendet wird. Diese Vorgehensweise erleichtert auch das Auffinden eines Zombie-Computers in Ihrem Netzwerk. Darüber hinaus hilft es, den Teufelskreis von Neu-Infektionen zu stoppen.

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