Studie von Sophos Labs

Man spricht (auch) deutsch: Korrekte Sprache, perfektes Logo – maßgeschneiderte Malware auf dem Vormarsch

Schadsoftware Versionen werden gezielt auf lokale Begebenheiten zugeschnitten

Wiesbaden, 9. Mai 2016 – In einer aktuellen Studie von Sophos zeigt sich der wachsende Trend in der Cyberkriminalität, Schadsoftware zu lokalisieren und Cyber-Attacken gezielt auf bestimmte Länder zuzuschneiden. Für die Studie wurden zwischen dem 1. Januar und dem 8. April 2016 Informationen von Millionen von Endpoints weltweit gesammelt und von den internationalen Security-Experten der Sophos Labs rund um die Uhr analysiert.

Auch Cyberkriminelle stehen innerhalb ihrer Branche unter dem Druck, sich immer weiter professionalisieren zu müssen, um im hart umkämpften Markt zu bestehen. Ein Ergebnis dessen ist eine vermehrt zu beobachtende, lokal designte Maßschneider-Malware: Cyberkriminelle bedienen sich zunehmend korrekter Sprachen und lokaler Zahlungsmethoden sowie landestypischer Marken, um ihre Opfer in den unterschiedlichen Ländern zu ködern.

Fehlerfrei und mit lokaler Dienstleistung
Für den Einsatz einer regional zugeschnittenen Malware checken die Cybergauner zunächst, aus welchem Land die IP-Adresse der Ziel-Computer stammt und in welcher Sprache die Windows Einstellungen vorgenommen wurden.

Um dann die Glaubwürdigkeit beispielsweise von betrügerischen E-Mails zu steigern, wird auf geschickte Weise Ransomware in authentisch aussehenden E-Mail-Benachrichtigungen mit täuschend echt gefälschten Logos bekannter lokaler Marken versteckt. So imitieren die Betrüger etwa äußerst professionell die digitalen Benachrichtigungen lokaler Postgesellschaften, Steuer- und Strafverfolgungsbehörden oder Versorgungsunternehmen. Es werden gefälschte Lieferscheine, Rückerstattungen, Strafzettel oder Stromrechnungen versendet. Auch der Versand von Ransomware in professionell und seriös anmutenden Bewerbungsschreiben nimmt zu. Die bekannten hanebüchenen Schreib-, Interpunktions- und Grammatikfehler, bisher untrügliches Indiz für gefälschte E-Mails, fanden die SophosLabs-Experten im Analysezeitraum dagegen immer seltener. „In zunehmendem Maße nehmen Cyberkriminelle sogar die Dienste professioneller Übersetzer in der Zielregion in Anspruch, um ihre E-Mail-Fallen so echt wie möglich aussehen zu lassen“, weiß Chester Wisniewski, leitender Sicherheitsberater bei Sophos. „Außerdem wissen wir, dass gerade Kriminelle, die Banking Trojaner einsetzen wollen, sich der regionalen Varianten bedienen. Schadware, die die größten regionalen Geldinstitute zum Ziel hat ist also ebenso lohnenswert wie wahrscheinlich.“

Immer häufiger infizieren die Angreifer ihre Ziele darüber hinaus nicht selbst, sondern greifen auf die Dienstleistungen anderer Cyberkrimineller zurück, die bereits Tausende von Computern unbemerkt infiziert haben und den Zugriff darauf nun meistbietend verkaufen. Auch der Einsatz so genannter „Money Mules“, (Geld-Maultiere) kommt vermehrt vor. Ein Beispiel: Ein Cyberkrimineller von irgendwo auf der Welt hat Banking Malware auf Computern in Deutschland installiert. Um an das Geld der ahnungslosen Opfer zu kommen,

nutzt er nun vor Ort seine Money Mules, also Leute, die er angeheuert hat, um an deutschen Geldautomaten mit gefälschten Karten Geld abzuheben. Gefälschte Karten wohlgemerkt, die mithilfe von Kartendaten und PIN-Nummern produziert wurden, die zuvor durch die Schadsoftware gestohlen wurden.

Maßschneider-Malware entsteht aus alten Bekannten, Trustezeb spricht deutsch
Die Schadsoftware-Stämme, die von den Cyberkriminellen für ihre lokalen Angriffe genutzt werden sind indes allesamt keine Unbekannten: Interessante Ergebnisse konnten die Sophos-Forscher aus der Analyse verschiedener Ransomware-Stämme ziehen, die jeweils lokalisiert Ziele in unterschiedlichen Ländern attackieren. So zielen lokalisierte Versionen von Cryptowall beispielsweise überwiegend auf Opfer in den USA, Großbritannien, Kanada, Australien, Deutschland und Frankreich. TorrentLocker-Variationen bedrohen in erster Linie Großbritannien, Italien, Australien und Spanien und TeslaCrypt attackiert maßgeschneidert vor allem Großbritannien, die USA, Kanada, Singapur und Thailand.

Weiterhin wird durch die Analyse der Sophos Forscher erstmals deutlich, welche regional zugeschnittenen Trojaner verwendet werden, um Banken und Finanzinstitute in verschiedenen Ländern zu infiltrieren. Für die deutschsprachigen Regionen sind dies maßgeblich drei: Trustezeb spricht ausdrücklich Deutsch, durch diese Schadware wird vor allem die DACH-Region attackiert. Dridex ist vorherrschend in Deutschland und in den USA und Zbot ist zwar weltweit verbreitet, wird aber vor allem in Deutschland, den USA, Großbritannien, Kanada, Australien, Italien, Spanien und Japan genutzt.

Neue Wege auch beim kriminellen Abkassieren
Mit Schadware-Varianten ist es nicht getan, wie die Studie außerdem zeigt. "Sogar Geldwäsche scheint lokalisiert lukrativer zu sein“, sagt Chester Wisniewski. „Die Nutzung von Kreditkarten ist für Kriminelle naturgemäß riskant – also haben sie sich darauf verlegt, die erpressten Zahlungen von Ransomware-Opfern über anonyme Internet-Zahlungsmethoden abzuwickeln.“ Vor allem in den USA und im Vereinigten Königreich konnten die Sophos-Forscher dieses Vorgehen nachverfolgen. Es ist nur eine Frage der Zeit, bis sich dieser Trend auch hierzulande deutlich zeigt.

Über Sophos
Mehr als 100 Millionen Anwender in 150 Ländern verlassen sich auf Sophos‘ Complete-Security-Lösungen als den besten Schutz vor komplexen IT-Bedrohungen und Datenverlust. Sophos bietet dafür preisgekrönte Verschlüsselungs-, Endpoint-Security-, Web-, Email-, Mobile- und Network Security-Lösungen an, die einfach zu verwalten, zu installieren und einzusetzen sind. Das Angebot wird von einem weltweiten Netzwerk eigener Analysezentren, den SophosLabs, unterstützt.
Sophos hat seinen Hauptsitz in Boston, USA, und Oxford, Großbritannien. In Deutschland hat das Unternehmen seinen Hauptsitz in Wiesbaden und ist in Österreich und der Schweiz je an einem Standort vertreten. 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
Christiane Capps, +49-174-3335550
Ulrike Masztalerz, +49-30-55248198
sophos@tc-communications.de