Schlag gegen Botnetz-Infrastruktur

Mit vereinten Kräften ist es Ermittlern aus etlichen Ländern gelungen, gegen ein Schwergewicht der Botnetz-Szene vorzugehen, das im großen Stil für Online-Banking-Betrug, Erpressung und Spam-Versand genutzt wurde. Es geht um die Botnetz-Infrastruktur Avalanche, die mindestens seit 2009 dafür sorgt, dass rund zwanzig Botnetze weitgehend unbehelligt große Mengen von Rechnern und auch Smartphones missbrauchen. Dabei geht es stets ums Geld: Von Avalanche betroffene Online-Banking-Nutzer sollen im Durchschnitt um 5000 Euro erleichtert worden sein.

An den Ermittlungen waren unter anderem die Zentralinspektion Lüneburg, die Staatsanwaltschaft Verden und US-Behörden wie das FBI beteiligt. Es gelang ihnen, 16 Avalanche-Betreiber aus zehn Ländern zu identifizieren; gegen sieben Tatverdächtige hat die Staatsanwaltschaft Haftbefehl wegen verschiedener Tatbestände wie der Bildung einer kriminellen Vereinigung erlassen. Die Ermittlungen haben über vier Jahre angedauert. Auslöser waren die ersten Wellen von BKA-Trojanern, die Rechner ihrer Opfer vorgeblich im Namen des BKA oder BSI gesperrt und anschließend ein Lösegeld gefordert hatten. Zum Zeitpunkt des Zugriffs sollen allein in Deutschland über 50.000 Rechner unter der Kontrolle der Gang gestanden haben.

Bedeutend ist dieser Ermittlungserfolg vor allem deshalb, weil es nicht um ein einzelnes Botnetz geht, sondern um einen Dienstleister der Crimeware-Szene, der den Betreibern von rund 20 Botnetzen das Leben leicht gemacht hat: Avalanche ist darauf spezialisiert, die sichere Kommunikation zwischen Bot und Steuer-Rechnern (Command-and-Control-Servern, C&C) mit einer speziellen Verschleierungstaktik zu gewährleisten. Dabei kommuniziert der Bot niemals direkt mit dem C&C, um dessen Identität zu schützen. Stattdessen läuft die Verbindung über Proxy-Systeme wie infizierte Webserver oder andere Bots, die sehr schnell wechseln (Fast Flux). Die Bots nutzen einen zeitabhängigen Algorithmus, um die aktuelle Domain des C&C-Servers zu ermitteln. Diese Domains müssen die Avalanche-Betreiber zeitnah registrieren.

Dabei sind enorm viele Domains im Spiel – daher war es für die beteiligten Ermittler auch eine Mammutaktion, alle bisher genutzten und die anhand der Algorithmen für den zukünftigen Einsatz geplanten Domains zu sperren. Insgesamt geht es um hunderttausende Domains bei allen erdenklichen Registraren. Des Weiteren wurden beteiligte Server beschlagnahmt und auf sogenannte Sinkholes umgeleitet. Dabei handelt es sich um harmlose Systeme unter Kontrolle der Ermittler, die keine Befehle absetzen, sondern lediglich die eingehenden Verbindungen infizierter Systeme registrieren.

Diese Informationen hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) an die betroffenen Provider ausgehändigt, die daraufhin ihre Kunden warnen konnten. Seit 2014 sollen so über 4,5 Millionen Warnmeldungen verschickt worden sein. Wer den Verdacht hegt, dass sein System betroffen ist, sollte es einem Virencheck mit einem Live-System wie Desinfec't unterziehen. Erhärtet sich der Verdacht, sollte man den Schädling entfernen und alle Passwörter ändern, die der Trojaner auf dem kompromittierten System potenziell abgreifen konnte. *(rei@ct.de)*

Auch Avira schießt sich auf Ransomware ein

Bild: Avira

Die neue Internet Security Suite enthält ein Management-Programm für die Windows-Firewall und einen Virenscanner, der darauf spezialisiert ist, Erpressungstrojaner abzuwehren.

Der deutsche Hersteller Avira hat neue Versionen seiner Schutzsoftware herausgegeben. Die Internet Security Suite, die Total Security Suite und die Avira Optimization Suite gibt es jetzt als Ausgabe für 2017. Die Firma vom Bodensee hebt dabei, wie andere AV-Hersteller auch, vor allem den Schutz vor Erpressungs-Trojanern hervor. Man habe beobachtet, dass sich Angriffe mit Ransomware in deutschsprachigen Ländern von Mai bis Oktober verneunfacht hätten. Die neue Ausgabe des Avira-Scanners Antivirus Pro bedient sich außer herkömmlicher Signaturen auch künstlicher Intelligenz und einer Analyseinfrastruktur in der Cloud, um verdächtige Aktivitäten in Echtzeit zu entdecken.

Die Internet Security Suite 2017 enthält einen neuen Firewall-Manager, der ein Frontend zur Windows-eigenen Firewall darstellt. Er soll es Anwendern erlauben, ihr System auf optimalen Schutz hin zu konfigurieren. In der Total Security Suite kombiniert der Hersteller seinen Virenscanner mit dem neuen Firewall Manager, einem Werkzeug zum Entschlacken nicht mehr benötigter Dateien und Software (System Speedup), und dem hauseigenen Phantom VPN.

Aviras Internet Security Suite und die Optimization Suite kosten jeweils 45 Euro. Benutzen kann man die Software auf drei Geräten ein Jahr lang. Die kombinierte Total Security Suite kostet 85 Euro. Außerdem bietet Avira eine kostenlose Free Security Suite an, bei der der enthaltene Virenscanner Einschränkungen in seinen Zusatzfunktionen aufweist, aber den Basisschutz weiter gewährleistet. Auch wird dem Nutzer bei der Benutzung Werbung angezeigt. *(fab@ct.de*

Sicherheits-Notizen

Die Mozilla-Entwickler haben eine kritische Sicherheitslücke in **Firefox** und dem **Tor-Browser** geschlossen. Die entsprechenden Updates wurden bereits verteilt.

Durch Unachtsamkeit der Betreiber von **Mitfahrgelegenheit.de und Mitfahrzentrale.de** wurden Mail-Adressen, Mobilfunknummern und Kontodaten von hunderttausenden Nutzern der Seite im Internet verteilt.