Game Over für ZeuS ? aber das war erst der Anfang

"Game Over für ZeuS - aber das war erst der Anfang"

Kommentar zum aufgedeckten Hackerring "GameOver ZeuS" von Lucas Zaichkowsky, Enterprise Defence Architect bei AccessData
Gerade erst gab das U.S. Department of Justice (DOJ) bekannt, dass es das gefährliche Betrugs-Botnet GameOver ZeuS zerschlagen habe. Mittels bösartiger Software hatte der sich dahinter verbergende Hackerring unzählige Finanz- und Privatdaten von Internetnutzern gestohlen. Weltweit seien zwischen 500.000 und einer Million Computer mit der Schadsoftware GameOver ZeuS infiziert gewesen. Die Cyberkriminellen konnten dadurch mehr als 100 Millionen US-Dollar erbeuten. Von den Attacken waren viele Organisationen aus dem Finanzsektor betroffen.
Das Auflösen dieses Hackerrings wird kurzfristig einen signifikanten Rückgang von ZeuS-Malware-Infektionen zur Folge haben. Zudem konnte das DOJ auch die gefährliche Ramsomware CryptoLocker auslöschen. Diese Malware verschlüsselt Dokumente in infizierten Systemen und macht sie dadurch unlesbar. Die Opfer konnten ihre verlorenen Daten bei den Urhebern von CryptoLocker zurückkaufen. Das DOJ deckte 234.000 solcher Vorfälle auf. In den ersten zwei Monaten des CryptoLocker-Projekts flossen insgesamt 27 Millionen Dollar an Zahlungen.
Eines muss uns aber bewusst sein: Vielleicht ist bei ZeuS nun sozusagen Game Over, und das Zerschlagen des Netzwerks ist ein Teilerfolg. Aber das Ende war das noch nicht. Allein die Nachfrage nach Ersatz für ZeuS auf dem Schwarzmarkt wird stark steigen. Die nicht festgenommenen Mitglieder der Cybergang lassen sich zudem nicht davon abbringen, andere große Botnets zu gründen, unabhängig davon, ob ihr Anführer in Haft ist. Viele der Cyberkriminellen kommen übrigens aus Osteuropa. Insbesondere hier lassen sich Millionen mit Malware verdienen.
Als Schutz vor Malware wird stets eine Antivirus-Software empfohlen. Doch die ist längst nicht immer der Weisheit letzter Schluss. Die Schwierigkeit beim Entwirren der GameOver ZeuS-Botnet-Infrastruktur ist, dieses Netzwerk verständlich und übersichtlich abzubilden. Eine strukturierte Peer-to-Peer-Architektur erlaubt es Angreifern, ihre Botnet-Armee beim Zugriff auf jedes infizierte System zu kontrollieren. Doch die ZeuS-Betreiber machten es schwierig, die infizierten Systeme überhaupt mit Antivirus- oder Antimalware-Lösungen aufzuspüren.
Die Cyberkriminellen verteilten generische Dropper via E-Mail, indem sie eine ZIP-Datei anfügten. Dieser Anhang enthält eine ausführbare Datei, getarnt als unauffälliges Dokument, oder Links zu Webseiten, die populäre Exploit-Kits wie z.B. Blackhole hosten. Diese Exploit-Kits identifizieren ungepatchte Software jedes Webseiten-Besuchers und nutzen die entsprechenden Schwachstellen aus. Wird der angesprochene Dropper nicht von Schutzlösungen als ZeuS klassifiziert, löst sich durch eine Liste verschlüsselter Adressen automatisch ein ZeuS-Download aus. Die Download-exe von ZeuS wird danach sofort gelöscht und kann im System nicht mehr aufgespürt werden. Ich habe selbst Tests durchgeführt, um zu prüfen, wie schwer es Antivirus-Lösungen fällt, ZeuS oder Cryptolocker aufzuspüren. Das Ergebnis: Nur sechs von 52 Lösungen haben die Malware überhaupt entdeckt.
Organisationen und Nutzer, die besorgt über die Bedrohungen sind, können das Risiko für ihre IT-Umgebung mit ein paar Vorsichtsmaßnahmen reduzieren; zum Beispiel, indem sie Mail-Anhänge mit ausführbaren Dateien oder ZIPs wie exe und scr generell blocken. Zudem sollte man eine Software zum Aufspüren von Schwachstellen einsetzen, unter anderem um Exploit Kits zu identifizieren. Obwohl Antivirus-Software bekanntlich Schwächen offenbart, sollte trotzdem eine solche Lösung eingesetzt werden, denn diese fängt nichtsdestotrotz große Mengen an Malware ab. Organisationen mit IT-Sicherheitspersonal empfehle ich den Erwerb konsolidierter Plattformen wie ResolutionOne von AccessData. Diese Plattformen helfen dem Personal dabei, Security-Vorfälle zu analysieren, nachzuvollziehen und den Urheber der Malware zu identifizieren. Die Lösung besteht aus einem Sammelsurium an Tools, die aus vielen manuellen Schritten ein großes und verständliches Gesamtbild der Bedrohung zusammenfügen.
Über AccessData:
Die AccessData Group ist seit 25 Jahren Wegbereiter für Entwicklungen im Bereich der digitalen Ermittlungen und entsprechender Unterstützung in Rechtsstreitigkeiten. Die Produktfamilie besteht aus Stand-Alone- und Enterprise-Class-Lösungen mit dem Fokus auf Digital Forensik, E-Discovery und Cyber Security. Hierzu gehören unter anderem die Produkte FTK, SilentRunner, Summation und das CIRT Security Framework. Sie ermöglichen digitale Untersuchungen jeder Art, wie z.B. Computerforensik, Vorfallsanalyse, Hosted Review Services, rechtliche Nachprüfungen und Compliance-Audits. Mehr als 100.000 User, die weltweit im Gesetzesvollzug, in Regierungsbehörden, Unternehmen und Rechtanwaltskanzleien etc. tätig sind, vertrauen bereits auf die AccessData Software-Lösungen. AccessData ist zudem Anbieter für Trainings und Zertifizierungen in den Bereichen digitale Forensik und Rechtsstreitigkeiten. Weitere Informationen unter www. accessdata.com .

AccessData Group
Nicole Reid
International Marketing Manager
1 Bedford Street
3rd Floor
London
E-Mail: nreid@accessdata.com
Internet: www.accessdata.com
Ansprechpartner (in Deutschland):
Abdeslam Afras
Director, EMEA
 India
E-Mail: aafras@accessdata.com
PR-Agentur:
Sprengel
 Partner GmbH
Nisterstraße 3
D-56472 Nisterau
 www.sprengel-pr.com
Ansprechpartner:
Olaf Heckmann
Marius Schenkelberg
Tel.: +49 (0)26 61-91 26 0-0
Fax: +49 (0)26 61-91 26 0-29
E-Mail: ms@sprengel-pr.com
<img src="http://www.pressrelations.de/new/pmcounter.cfm?n_pinr_=566725" width="1" height="1">

Pressekontakt

AccessData Group

84042 Lindon, UT

nreid@accessdata.com

Firmenkontakt

AccessData Group

84042 Lindon, UT

nreid@accessdata.com

Weitere Informationen finden sich auf unserer Homepage