Neues Computer-Botnet missbraucht Regierungs-Server

Win32/Georbot treibt in Georgien ein perfides Spiel

(ddp direct) Die Schadsoftware Win32/Georbot erregte bei den ESET-Virenspezialisten bereits Anfang dieses Jahres enorme Aufmerksamkeit. Dieser virtuelle Agent aus Trojaner und Bot stiehlt in meisterhafter James Bond-Manier wertvolle Daten und Informationen auf infizierten Systemen. Dabei nutzt er auf illegale Weise Webseiten und Server der georgischen Regierung. Eine umfangreiche Analyse des Botnets befindet sich unter www.eset.de oder unter http://www.themenportal.de/dokumente/analyse-von-win32-georbot

Die Entdeckung eines Botnets ist inzwischen nichts Ungewöhnliches mehr. Den meisten Funden können Technikfreaks und Virenexperten nur noch ein müdes Lächeln abringen. Doch Win32/Georbot sorgte im ESET-Virenlabor bereits zum zweiten Mal in diesem Jahr für Aufsehen.

Nach ersten Forschungen konnten ESET-Experten auf das Kontrollzentrum der Schadsoftware zugreifen. Im Gegensatz zu den kürzlich entdeckten Schadprogrammen Win32/Stuxnet und Win32/Duqu, die ein Beispiel gut organisierter und professioneller Cyberkriminellen sind, verfügt Win32/Georbot über eine einzigartige Technologie und noch ausgefeiltere Funktionen, um an Informationen zu gelangen. Das Bemerkenswerte und Interessante an Win32/Georbot ist, dass die Schadsoftware Dokumente und Zertifikate stiehlt. Zudem ist sie in der Lage, neben dem üblichen Bespitzelungsdienst Audio-, Videoaufnahmen und Screenshots zu erstellen, lokale Netzwerke nach Informationen zu durchsuchen, das System auf Remote Desktop Konfigurationsdateien zu überprüfen und DDoS Attacken durchzuführen. Hacker können diese Dateien auf andere Rechner laden und sich Zugriffsrechte verschaffen, ohne dass der Nutzer es bemerkt. Hinzu kommt, dass Win32/Georbot einen Update-Mechanismus beinhaltet, der immer wieder neue Versionen des Bots herunterlädt und auf diese Weise den Viren-Scannern verborgen bleiben kann.

Dabei nutzt Win32/Georbot illegal Webseiten der georgischen Regierung, um seine Command-and-Control-Informationen (C&C) herunterzuladen. Sobald die Schadsoftware den C&C-Server nicht erreichen kann, greift ein integrierter Fall-Back-Mechanismus. Sodann verbindet sich das Programm zu einer bestimmten Webseite, das von der georgischen Regierung gehostet wird. Dies aber heißt nicht, dass diese in die Vorfälle verwickelt ist. Oft wissen viele nicht einmal, dass Ihre Systeme gefährdet sind, sagt Marc-Pierre Bureau, Sicherheitsexperte bei ESET. Allerdings nahmen die Agentur für Datenaustausch des Georgischen Justizministeriums und das georgische CERT bereits letztes Jahr dieses Problem wahr und kooperieren seitdem mit ESET. In Georgien sind 70% der Rechner infiziert, gefolgt von den USA (5.07%), Deutschland (3.88%) und Russland (3.58%). Die Tatsache, dass Win32/Georbot eine georgische Webseite nutze, um seine C&C-Informationen zu aktualisieren und die Schadsoftware zu verbreiten, spreche für einen gezielten Angriff auf die georgische Bevölkerung, so Bureau weiter.

Die ESET-Experten entdeckten im Kontrollzentrum des Bots nicht nur Details über die Anzahl und Orte der gefährdeten Systeme, sondern auch eine Liste mit Stichwörtern, anhand derer Dokumente und Dateien durchsucht wurden. Darunter befinden sich viele englischsprachige Suchbegriffe wie agent, army, secret, weapon, phone, number und Abkürzungen wie FBI, CIA, KGB und FSB.

Auch wenn die Intention der Hacker eindeutig scheint, bleibt offen, wohin diese Daten letztendlich fließen.

Weitere Informationen erhalten Sie unter www.eset.de.

Shortlink zu dieser Pressemitteilung:
http://shortpr.com/vm7w9y

Permanentlink zu dieser Pressemitteilung:
http://www.themenportal.de/digital-world/neues-computer-botnet-missbraucht-regierungs-server-88295

Pressekontakt

DATSEC Datsec Security

Herr Michael Klatte
Talstraße 84
07743 Jena

michael.klatte@eset.de

Firmenkontakt

DATSEC Datsec Security

Herr Michael Klatte
Talstraße 84
07743 Jena

eset.de
michael.klatte@eset.de

Der slowakische Antivirenhersteller ESET schützt seit 1992 mit modernsten Antivirenlösungen Unternehmen und Privatanwender vor Malware aller Art. Das Unternehmen gilt - dank der vielfach ausgezeichneten ThreatSense-Engine - als Vorreiter bei der proaktiven Bekämpfung selbst unbekannter Viren, Trojaner und anderer Bedrohungen.

Die hohe Malwareerkennung und Geschwindigkeit sowie eine minimale Systembelastung zeichnen die Top-Produkte ESET NOD32 Antivirus und ESET Smart Security aus. Inzwischen vertrauen mehr als 100 Millionen PC-Anwender weltweit den ESET-Lösungen.

Für Firmenkunden bietet ESET umfassenden MalwareâÂ?Â?Schutz an, der auch Lösungen für Mailserver, Netzwerk-Gateways und Fileserver

unterschiedlicher Serverbetriebssysteme und EâÂ?Â?MailâÂ?Â?Serverplattformen umfasst. Sie gewährleisten proaktiven und präzisen Antivirenschutz für HighâÂ?Â?TrafficâÂ?Â?Server und umfangreiche Dateisysteme.

ESET beschäftigt in seiner Unternehmenszentrale in Bratislava (Slowakei) und in der Niederlassung in San Diego (USA) mehr als 500 Mitarbeiter. ESET betreibt zudem eigene Büros in Prag (Tschechische Republik), Bristol (UK) und Buenos Aires (Argentinien). ESET-Lösungen sind über ein weltweites Partnernetzwerk in mehr als 180 Ländern vertreten. Exklusiver Distributor in Deutschland ist DATSEC Data Security e.K. aus Jena.