PRIVATRECHNER mit Totalausfall

Nutzlose Neustarts, übler Grund: Versteckte Malware hat das Gerät zugemüllt. Für einfache Laien wäre jetzt Schluss – PC-Exitus

Die Sache beginnt als kleiner Freundschaftsdienst eines Kaspersky-Virenjägers, der nach einem PC-Problem schauen soll. Der Besitzer ist sich sicher: Es handelt sich um einen Hardware-Fehler, denn der Rechner zeigt typische Symptome: Schon während des Bootens erscheint ein Bluescreen, bis zum Betriebssystem – Windows 7 – fährt der Computer gar nicht mehr hoch. Zahllose Neustarts ändern daran nichts. Ein defektes Motherboard? Mit Malware rechnet erst niemand, denn schließlich wollen Virenentwickler für gewöhnlich keine Hardware-Schäden anrichten – das würde ihnen keinen Profit bringen. Gauner verdienen nur Geld, wenn der Schädling unerkannt bleibt und im Hintergrund Banking- und Kreditkartendaten abgreift oder Spam verschickt. Daher nehmen sich Cyberkriminelle viel Zeit dafür, dass ihre Schadsoftware keine offensichtlichen Schäden am Rechner verursacht. Dennoch stutzt der Sicherheitsexperte.

Er versucht, auf den Rechner zuzugreifen, um ein Backup der Festplatte anzufertigen. Dazu stöpselt er einen USB-Stick an, über den er ein Linux Live-System starten will. Doch der USB-Anschluss scheint defekt zu sein. Ein Test des DVD-Laufwerks zeigt: Auch hier geht nichts mehr. Für Laien wäre jetzt Schluss, doch der Fachmann weiß sich trotzdem zu helfen: Er greift per Netzwerkboot über einen PXE-Server auf den Rechner zu und zieht sich ein Image. Dieses mountet er auf seinem eigenen Notebook mit Ubuntu und checkt es mit einem aktuellen Virenscanner – mit fast schon schockierendem Ergebnis. Hier hat sich ein richtig fieser Genosse breitgemacht, ein Schädling mit TDL-2-Rootkit-Technologie, welcher die Bootsektoren befällt und dadurch direkt beim Rechnerstart aktiviert wird. Doch das ist noch nicht alles: Über einen Command-&-Controll-Server gelangen unzählige weitere Schädlinge auf den PC, das meiste davon erweist sich aber glücklicherweise als relativ harmlose Scareware.

Infektion Hinter dem Zumüllen steckt gewöhnlich ein Pay-per-Install-Modell (PPI). Das heißt: Installiert ein Cracker auf einem Rechner eine Malware, erhält er vom jeweiligen Virenprogrammierer ein Entgelt – eine lohnenswerte Einnahmequelle für die Gauner. Es ist eine Art Affiliate-Programm, das ursprünglich aus der Werbebranche kommt. Ein legales Beispiel ist die Yahoo-Toolbar, über die viele Anbieter von kostenlosen Programmen Geld verdienen. Doch mittlerweile ist das Modell auch im Untergrund angekommen. Virenentwickler und andere Cyberkriminelle arbeiten Hand in Hand und treffen sich in Foren, um Geschäfte zu machen.

Will ein Krimineller ein Botnetz aufbauen, meldet er sich bei einer PPI-Plattform an. Dort kann er sich in Foren von erfahrenen und abgebrühten Gaunern Tipps holen, auf welche Art er am schnellsten Geld verdient – was meist über den üblichen Weg funktioniert: Er bestellt bei den PPI-Betreibern eine Malware, die er verbreiten muss. Damit ahnungslose Opfer sie installieren, muss er sie mit einer normalen Software bündeln. Bevorzugt verseuchen Gangster Key-Generatoren, sodass die Opfer den Schädling freiwillig installieren. Über P2P-Netzwerke oder Hostingwebseiten gelangt die Malware auf den Rechner. Das Verteilen ist gar nicht einfach, da die Tauschbörsen verseuchte Dateien sofort löschen. Doch PPI-Seiten bieten sogenannte Crypter an, die das schädliche Bundle so verschlüsseln, dass ein Antivirenprogramm es nicht entdeckt. Diese Crypter sind beliebt und teuer: Entwickler erhalten etwa 100 Dollar für eine Lizenz.

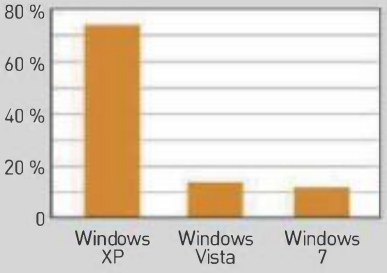
Schafft es ein Gangster beispielsweise, 1.000 US-Rechner mit einem Bot-Client zu infizieren, zahlt die PPI-Plattform dafür 180 Dollar, asiatische Rechner sind weniger lukrative Opfer, sie bringen nur sechs Dollar. Ein Detail weist darauf hin, wo die meisten Drahtzieher dieses Bezahlmodells sitzen könnten: Viele PPI-Handelsplätze zahlen kein Geld für befallene Rechner in Russland. Damit sich der Aufwand lohnt, müssen die Gangster die Malware weit verbreiten und installieren möglichst viel davon auf einem PC.

Desinfektion In unserem Fall ist der Angreifer über das Ziel hinausgeschossen: Die Vielzahl der installierten Schädlinge hat dazu geführt, dass der PC in die Knie ging und gar nicht mehr funktionierte. Dem Experten bleibt nur eine Neuinstallation, die er ebenfalls über das Netzwerk mit dem PXE-Server erledigt. →

GEFÄHRLICHES ROOTKIT

Auf dem PC im obigen Fall ist ein Schädling mit TDL-2-Rootkit-Technologie am Werk, der die Bootsektoren befällt und dadurch direkt beim Rechnerstart aktiviert wird. Der Rootkit-Bausatz TDL ist sehr aktiv und hat weltweit über 4,5 Millionen PCs befallen, etwa 135.000 davon stehen in Deutschland. Es ist eines der ersten Rootkits, das sogar 64-Bit-Systeme in großem Stil infizieren konnte, die meisten betroffenen Rechner laufen allerdings mit XP.

BETROFFENE SYSTEME



VERBREITUNG DES SCHÄDLINGS