

Uroburos - hochkomplexe Spionagesoftware mit russischen Wurzeln

G Data entdeckt mutmaßliche Geheimdienstsoftware.

Bochum (Deutschland), 28. Februar 2014

Die Sicherheitsexperten von G Data haben eine hochentwickelte und komplexe Schadsoftware entdeckt und analysiert, deren Ziel es ist, hochsensible und geheime Informationen aus High-Potential-Netzwerken, wie staatlichen Einrichtungen, Nachrichtendiensten oder Großunternehmen zu stehlen. Das Rootkit mit dem Namen Uroburos arbeitet autonom und verbreitet sich selbstständig in den infizierten Netzwerken. Auch Rechner, die nicht direkt am Internet hängen, werden von diesem Schädling angegriffen. Eine solche Software kann nach Einschätzung von G Data nur mit hohen Investitionen in Personal und Infrastruktur realisiert werden. Das Design und der hohe Komplexitätsgrad des Schädlings lassen daher einen Geheimdienstursprung vermuten. Aufgrund technischer Details, wie Dateinamen, Verschlüsselung, Verhalten der Schadsoftware, besteht die Vermutung, dass Uroburos von derselben Quelle stammen könnte, die bereits 2008 eine Cyberattacke gegen die USA durchgeführt hat. Damals kam eine Schadsoftware namens „Agent.BTZ“ zum Einsatz. Nach Einschätzung des deutschen IT-Security Herstellers, ist das Spionageprogramm seit gut drei Jahren unentdeckt geblieben. Die Experten der G Data SecurityLabs werden noch heute im G Data Sicherheitsblog (<http://blog.gdata.de>) weitere Details und ein umfassendes Analyse-Paper veröffentlichen.

Uroburos ist ein Rootkit, das aus zwei Dateien besteht, einem Treiber sowie einem verschlüsselten virtuellen Dateisystem. Mit Hilfe dieses Schadprogramms kann der Angreifer die Kontrolle über den infizierten PC bekommen, beliebigen Programmcode auf dem Computer ausführen und dabei seine Systemaktivitäten verstecken. Uroburos ist außerdem in der Lage, Daten zu stehlen und den Netzwerkdatenverkehr mitzuschneiden. Durch den modularen Aufbau können Angreifer die Schadsoftware um weitere Funktionen erweitern. Aufgrund dieser Flexibilität und Modularität wird das Rootkit von G Data als sehr fortschrittlich und gefährlich eingestuft.



Technische Komplexität lässt Geheimdienstursprung vermuten

Die Komplexität und das Design von Uroburos zeugen von einer sehr aufwendigen und kostenintensiven Entwicklung des Schadprogramms, an der nach Einschätzung von G Data sehr gut ausgebildete Entwickler beteiligt waren. Der deutsche IT-Security-Hersteller geht daher davon aus, dass Cyberkriminelle nicht an der Entwicklung beteiligt waren und vermutet, dass ein Geheimdienst hinter Uroburos steckt. Die Experten halten es außerdem

G DATA CyberDefense AG Unternehmenskommunikation

G DATA CyberDefense AG

G DATA Campus

Königsallee 178

44799 Bochum

www.gdata.de

E-Mail: presse@gdata.de

Tel.: +49 (0) 234 9762-239

Fax: +49 (0) 234 9762-299

Uroburos ist darauf ausgelegt in großen Netzen von Firmen, Behörden, Organisationen und Forschungseinrichtungen zu agieren: Das Schadprogramm verbreitet sich selbstständig weiter und arbeitet in einem „peer-to-peer“ Modus, dabei kommunizieren die infizierten Computer in einem geschlossenen Netzwerk direkt miteinander. Die Täter brauchen dabei nur einen einzigen Rechner mit Internetzugang. Das Muster zeigt, dass die Angreifer den Umstand berücksichtigen, dass in den Netzwerken oft auch PCs eingebunden sind, die nicht ans Internet angeschlossen sind. Die infizierten Rechner spionieren Dokumente und andere Daten aus und leiten diese an den PC mit der Internetverbindung weiter, hierüber werden alle zusammengetragenen Informationen an den Angreifer übermittelt. Uroburos unterstützt dabei sowohl 32- als auch 64-Bit Microsoft Windows-Systeme.

Verbindung zu russischer Attacke gegen die USA vermutet

Aufgrund technischer Details, Dateinamen, Verschlüsselung und dem Verhalten der Schadsoftware, sehen die G Data Experten einen Zusammenhang zwischen Uroburos und einer im Jahr 2008 erfolgten Cyberattacke gegen die USA - vermutlich stecken die gleichen Drahtzieher hinter den Angriffen und dem jetzt entdecktem Rootkit. Damals kam die Schadsoftware „Agent.BTZ“ zum Einsatz. Uroburos überprüft die infizierten Systeme darauf, ob das Schadprogramm bereits installiert ist, in diesem Fall wird das Rootkit nicht aktiv. G Data fand außerdem Hinweise darauf, dass die Entwickler beider Schadprogramme Russisch sprechen.

Die Analyse zeigt, dass das Ziel der Angreifer nicht einfache Internetnutzer sind. Der betriebene Aufwand ist nur bei lohnenswerten Zielen gerechtfertigt, also Großkonzernen, staatlichen Einrichtungen, Nachrichtendiensten, Organisationen oder vergleichbaren Zielen.

Wahrscheinlich seit über drei Jahren unentdeckt

Beim Uroburos Rootkit handelt es sich um das fortschrittlichste Stück Schadsoftware, das die Security-Experten von G Data je in diesem Umfeld analysiert haben. Der älteste Treiber, welcher bei der Analyse gefunden wurde, ist 2011 kompiliert worden. Dies deutet darauf hin, dass die Kampagne seitdem unentdeckt geblieben ist.

Infektionsvektor bleibt unklar

Wie Uroburos ein High-Profile Netzwerk initial infiltriert, lässt sich nach aktuellem Stand nicht ermitteln. Die Angriffe können über vielfältige Wege geschehen, z.B. über Spear-Phishing, Drive-by-Infektionen oder Social Engineering Attacken.

Was bedeutet der Name?

Die Schadsoftware wurde von G Data entsprechend der Bezeichnung im Quellcode auf den Namen >>Uroburos<< getauft, angelehnt an ein altes griechisches Symbol einer Schlange oder eines Drachen welcher seinen eigenen Schwanz frisst.

G DATA CyberDefense AG Unternehmenskommunikation

G DATA CyberDefense AG

G DATA Campus

Königsallee 178

44799 Bochum

www.gdata.de

E-Mail: presse@gdata.de

Tel.: +49 (0) 234 9762-239

Fax: +49 (0) 234 9762-299