Uroburos - hochkomplexe Spionagesoftware mit russischen Wurzeln

(Mynewsdesk) 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 Hersteller, ist das Spionageprogramm seit gut drei Jahren unentdeckt geblieben. Die Experten der G Data SecurityLabs haben im G Data Sicherheitsblog (http://blog.gdata.de) weitere Details und ein umfassendes Analyse-Paper veröffentlicht.Was ist Uroburos?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 vermutenDie 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 für wahrscheinlich, dass die Programmierer ein noch fortschrittlicheres Rootkit entwickelt haben, das bisher noch nicht entdeckt worden ist.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 Internetzugriff. Das Muster zeigt, dass die Angreifer den Umstand berücksichtigen, dass in den Netzwerke 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 vermutetAufgrund 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 unentdecktBeim 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 unklarWie 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-Infektione 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.

Shortlink zu dieser Pressemitteilung:
http://shortpr.com/k1288f

Permanentlink zu dieser Pressemitteilung:
http://www.themenportal.de/it-hightech/uroburos-hochkomplexe-spionagesoftware-mit-russischen-wurzeln-23921

Pressekontakt

-

Kathrin Beckert
Königsallee b 178
44799 Bochum

kathrin.beckert@gdata.de

Firmenkontakt

-

Kathrin Beckert
Königsallee b 178
44799 Bochum

shortpr.com/k1288f
kathrin.beckert@gdata.de

IT Security wurde in Deutschland erfunden: Die G Data Software AG gilt als Erfinder des AntiVirus. Das 1985 in Bochum gegründete Unternehmen hat vor mehr als 25 Jahren das erste Programm gegen Computerviren entwickelt. Heute gehört G Data zu den weltweit führenden Anbietern von IT-Security-Lösungen.

Testergebnisse beweisen: IT-Security Made in Germany schützt Internetnutzer am besten. Seit 2005 testet die Stiftung Warentest InternetSecurity Produkte. In allen sechs Tests, die von 2005 bis 2013 durchgeführt wurden, erreichte G Data die beste Virenerkennung. In Vergleichstests von AV-TEST demonstriert G Data regelmäßig beste Ergebnisse bei der Erkennung von Computerschädlingen. Auch international wurde G Data InternetSecurity von unabhängigen Verbrauchermagazinen als bestes Internetsicherheitspaket ausgezeichnet u.a. in Australien, Belgien, Frankreich, Italien, den Niederlanden, Österreich, Spanien und den USA.

Das Produktportfolio umfasst Sicherheitslösungen für Endkunden, den Mittelstand und für Großunternehmen. G Data Security-Lösungen sind weltweit in mehr als 90 Ländern erhältlich.Â

Weitere Informationen zum Unternehmen und zu G Data Security-Lösungen finden Sie unter http://www.gdata.de