

Spionageprogramm Uroburos attackierte Belgiens Außenministerium

Erste Informationen über den Einsatz des Rootkits gegen einen EU-Staat bekannt geworden

Bochum (Deutschland), 14. Mai 2014

Das von G DATA entdeckte Spionageprogramm Uroburos konnte erstmals in einem Ministerium eines EU-Staates nachgewiesen werden. Bereits am vergangenen Wochenende wurde über die Cyber-Attacke auf das belgische Außenministerium berichtet. Die belgische Zeitung De Standaard hat aus einer geheimdienstnahen Quelle in Erfahrung bringen können, dass die Spionagesoftware Uroburos das Netzwerk der Regierungseinrichtung befallen hat. Die Sicherheitsexperten von G DATA hatten bereits im Februar 2014 vor dem hochkomplexen und fortschrittlichen Rootkit gewarnt und auf das Gefährdungspotential hingewiesen: "Uroburos ist darauf ausgelegt in großen Netzen von Firmen, Behörden, Organisationen und Forschungseinrichtungen zu agieren."



Was ist passiert?

Am Wochenende bestätigte das belgische Außenministerium eine Cyber-Attacke auf ihre Netzwerke. Dabei sollen „Informationen und Dokumente über die Ukraine-Krise“ aus den Netzwerken geschleust worden sein, so Belgiens Außenminister Didier Reynders. Der eigentliche Angriff auf die Einrichtung habe sich bereits vergangene Woche ereignet. Über die Täter ist bisher nichts bekannt, außer, dass diese Russisch sprechen sollen.

Die veröffentlichten Informationen legen den Schluss nahe, dass hier das Uroburos Rootkit zum Einsatz kam. Bereits im Februar 2014 haben die Sicherheitsexperten von G DATA die Spionagesoftware analysiert und die technische Komplexität aufgedeckt.

Hintergrundinformationen zu Uroburos

Das von G DATA entdeckte 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.

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

Pressemitteilung

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.

Die [Analyse zu Uroburos steht im G DATA Security Blog](#) zur Verfügung, ebenso wie ein [detaillierter technischer Einblick in die Funktionsweise der Malware](#).



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