IT-Sicherheit:

Webseite des US-Finanzministeriums gehackt

Presseinformation
Duisburg, 04.05.2010

Onlinekriminellen ist es gelungen, in die Webseite des US-Finanzministeriums einen iFrame einzubetten. Er dient dazu, im Verborgenen eine der wesentlichen URLs des Eleonore Exploit Kit zu laden. Das Kit fasst verschiedenen Exploits für unterschiedliche Browser oder andere populäre Anwendungen zusammen und liefert die beste Methode, die Sicherheitslücke des jeweilig benutzen Browsers in Kürze auszuspionieren. Luis Corrons, der Direktor der PandaLabs hat das Angriffsszenario detailliert auf seinem Blog zusammengefasst.

Bilder und mehr im Online-Pressoffice:
http://panda.talkabout.de

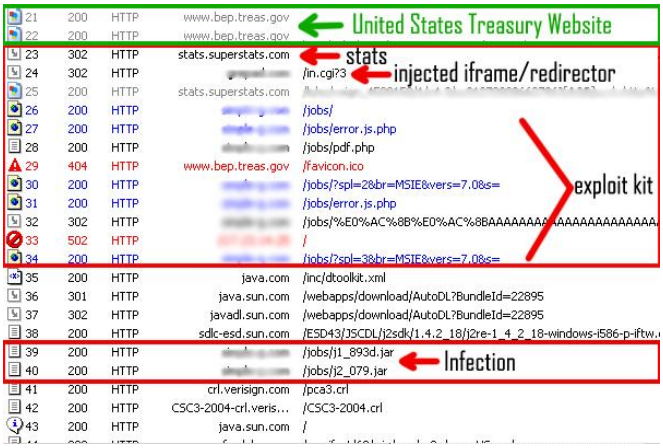
Panda Security im Netz:

http://pandanews.de/
http://twitter.com/pandanewsde
flickr.com/photos/panda_security
youtube.com/user/PandaTV
bit.ly/Panda-Security

Der iFrame leitet Besucher der gehackten Webseite (treas.gov, bep.gov oder moneyfactory.gov) unbemerkt durch statistische Server und Exploit Packs. Bei Luis Corrons fand das Exploit Kit eine Sicherheitslücke in Java, über die das System in seinem Fall am einfachsten infiziert werden konnte.

Es ist bislang unklar, welche Schwachstelle der US Treasury Webseite das Eindringen zuließ. Sicher ist jedoch, dass diese Angriffe für gewöhn-

lich immer Lücken durch veraltete Server Software, Web-Applikationen oder Sicherheitslücken in Web-Appliaktionen wie zum Beispiel SQL-Injections ausnutzen. Nach erfolgreicher Infektion wird der Browser des befallenen PCs sein Opfer zu anderen Anwendungen, im Beispiel von Corrons, zu Rogueware, also falscher Antiviren-Software umleiten.



Für sicheres Web-Browsen erinnert Corrons daran, für alle Web-Applikationen und die gesamte Server-Software jedes neue Update ohne Zeitverzug zu installieren.

Der gesamte Blogeintrag steht auf dem Blog der PandaLabs in englischer Sprache zur Verfügung: http://pandalabs.pandasecurity.com/usa-treasury-website-hacked-using-exploit-kit/

Weitere Informationen

Bilder und mehr im Pressoffice:
http://panda.talkabout.de

talkabout communications gmbh
Frank Brodmerkel
Balanstraße 73 / Gb. 10
81541 München
Tel.: +49 89 459954-18
Fax.: +49 89 459954-44
fbrodmerkel@talkabout.de
Web: http://www.talkabout.de

Panda Security
PAV Germany GmbH
Danica Dorawa
Presse & PR
Dr.-Alfred-Herrhausen-Allee 26
47228 Duisburg
Tel.: +49 2065 / 961-325
Fax: +49 2065 / 961-195
danica.dorawa@de.pandasecurity.com
Web: www.pandasecurity.com/germany

Über Panda Security

1990 in Bilbao, Spanien, gegründet, hat sich Panda Security zum Ziel gesetzt, seinen Kunden intelligenten Schutz gegen Malware bei geringstmöglicher Systembelastung zu bieten. Als erster Anbieter überhaupt hat Panda dazu eine Scan-Technik vorgestellt, die die Vorteile des Cloud-Computing mit der Schwarmintelligenz aller Panda-Nutzer kombiniert. Wird irgendwo auf der Welt ein neues Schadprogramm entdeckt, kann Panda alle seine Nutzer durch diesen „Collective Intelligence"-Ansatz aktuell in der Regel schon nach sechs Minuten schützen. Panda Security entwickelt und vertreibt leistungsfähige Consumer- wie auch Corporate-Lösungen.

In Deutschland und Österreich leitet die PAV Germany GmbH das Panda-Geschäft und bietet Unternehmenskunden kostenfreien 24/7/365-Support auf Deutsch durch die eigenen Techniker. Den Vertrieb organisiert die PAV durch Channel-Partner. Mit mehr als 56 Niederlassungen weltweit und einem Kundenstamm aus fast 200 Ländern hat sich Panda Security eine globale Präsenz geschaffen. Zahlreiche internationale Unternehmen vertrauen den Sicherheitslösungen von Panda, darunter u. a. DHL, VW, Opel, Telefonica, Hertz oder Pirelli.