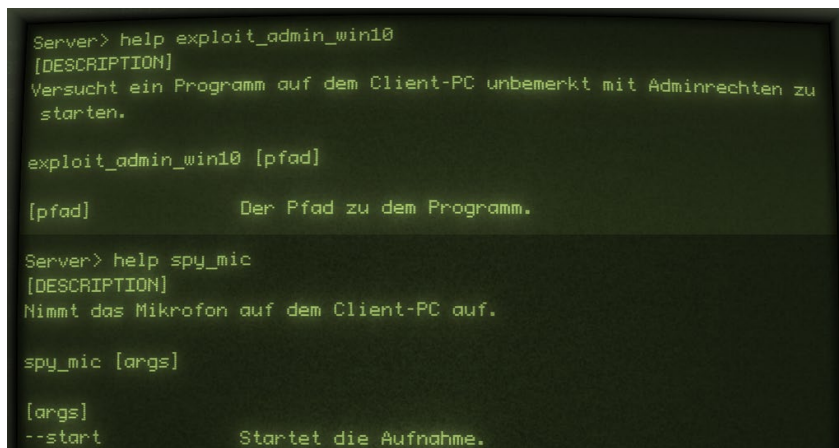


Persönliche Daten in Gefahr: Deutsche Schadsoftware Pekraut ermöglicht die Fernsteuerung von Windows-Rechnern

G DATA Virus-Analysten entdecken Schadprogramm „Made in Germany“

Bochum (Deutschland), 02. April 2020

Die Security-Experten von G DATA CyberDefense haben einen sogenannten Remote Access Trojaner (RAT) entdeckt, der die unbemerkte Fernsteuerung und administrative Kontrolle eines Computers ermöglicht. Das neue Schadprogramm verfügt über viele Funktionen. Die Angreifer können so beispielsweise ohne die Kenntnis des Nutzers dessen persönliche Daten oder Passwörter ausspionieren. G DATA Kunden sind vor Pekraut geschützt.



```
Server> help exploit_admin_win10
[DESCRIPTION]
Versucht ein Programm auf dem Client-PC unbemerkt mit Adminrechten zu
starten.

exploit_admin_win10 [pfad]

[pfad]                Der Pfad zu dem Programm.

Server> help spy_mic
[DESCRIPTION]
Nimmt das Mikrofon auf dem Client-PC auf.

spy_mic [args]

[args]
--start                Startet die Aufnahme.
```

"Pekraut ist für einen neuen RAT schon recht weit ausgebaut und kann wegen des vermuteten Malware-as-a-Service Charakters über alle üblichen Verbreitungswege auf Rechner gelangen. Zum Beispiel via E-Mail-Spam und Software-downloads. Angreifer können die Malware mit 27 verschiedenen Befehlen steuern. Sie sind in der Lage den infizierten Rechner auszuspähen, ohne dass der Nutzer es bemerkt. Die von uns untersuchte Pekraut-Variante nistet sich als Fake-Updater für Internet Explorer ein. Antiviren-Programme schützen davor, sofern die Virensignaturen aktuell sind. Dies stellen automatische Updates sicher", sagt Karsten Hahn, Virus Analyst bei G DATA CyberDefense.

Als Remote Access Trojaner (RAT) ermöglicht Pekraut die vollständige administrative Übernahme und Steuerung des infizierten Windows-Computers. Nutzer bemerken nichts davon, so dass das Schadprogramm unbemerkt seine schädlichen Funktionen ausführen kann. Pekraut kann mit Hilfe von 27 Befehlen gesteuert werden. Je nach Zielsetzung der Attacke spähen die Angreifer beispielsweise persönliche Informationen oder Passwörter zu Benutzerkonten aus oder löschen Dateien. Die so erbeuteten Informationen, zum Beispiel Zugänge zu Onlinebankkonten oder Shops, lassen sich gewinnbringend in speziellen Untergrundmärkten verkaufen.

Schadcode „Made in Germany“

Pekraut enthält einen Hilfetext in deutscher Sprache, dieser enthält Informationen über die 27 Kommandos, die die Angreifer ausführen können. Daher vermuten die G DATA Security-Experten, dass das Schadprogramm deutschen Ursprungs ist.

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

Remote Access Trojaner gehören nach Einschätzung von G DATA CyberDefense zu den aktuell aktivsten Schädlingstypen. [2019 waren bereits fünf der zehn häufigsten Malwarefamilien RATs](#), dazu gehörten zum Beispiel njRAT oder BlackShades.

Weitere Informationen zu Pekraut sind im [G DATA Blog](#) zu finden.

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