PRESSEMITTEILUNG

Sticky-Keys-Attacke: Wenn sich das Betriebssystem gegen Sie richtet

Panda Security entdeckt neuen Typ von gezielten Cyberangriffen

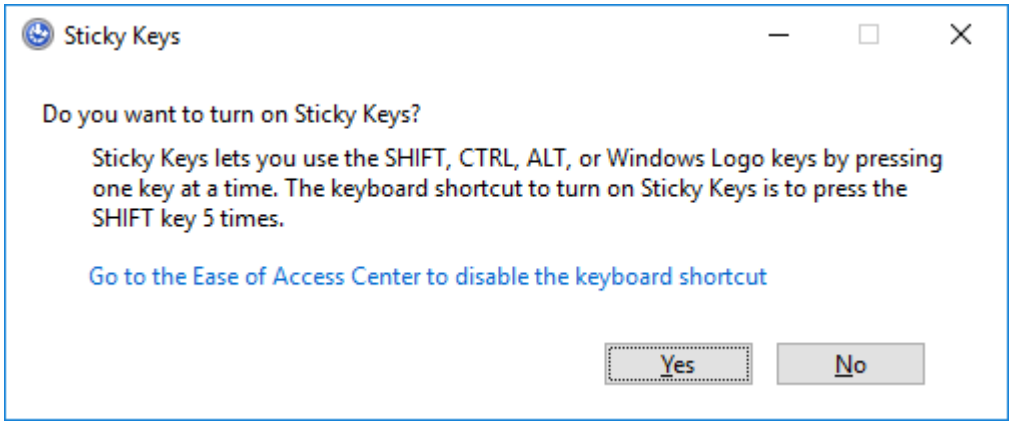
***Duisburg, den 10. März 2017* – PandaLabs, Panda Securitys Anti-Malware-Labor, hat einen neuen Typ von gezielten Angriffen gegen Unternehmen entdeckt. Dabei nutzen die Hacker keinerlei Malware, um Daten von Unternehmensnetzwerken zu stehlen. Alles, was der Angreifer tun muss, ist, fünf Mal die Shift-Taste eines Computers zu drücken, um das Sticky-Keys-Feature zu aktivieren und das betroffene System zu kompromittieren. Denn diese Keys ermöglichen es den Cyberkriminellen, eine Back Door auf dem attackierten Computer zu öffnen – normalerweise ein Server, der zuvor mithilfe einer Brute-Force-Attacke gegen das Remote Desktop Protokoll (RDP) gehackt wurde. Selbst wenn der Angriff bemerkt und die Zugangsdaten zum RDP geändert werden, können die Cyberkriminellen so weiterhin Sticky Keys aktivieren und sozusagen ‚durch die Hintertür' auf das System zugreifen, ohne die (neuen) Zugangsdaten zu kennen.**

Entdeckt wurde diese clevere Masche erst kürzlich von den PandaLabs, als deren IT-Experten eine Attacke gegen ein ungarisches Unternehmen analysierten. Das Besondere daran: Der Angriff nutzte nicht irgendwelche Malware als solche (Phishing, Würmer oder die gefürchteten Verschlüsselungstrojaner) sondern Skripts und andere zum Betriebssystem gehörige Tools, um die Malware-Scanner zu umgehen. Dies ist nur ein weiteres Beispiel für die zunehmende Selbstsicherheit und Professionalität, die IT-Security- bei Cyberkriminellen in den letzten Monaten beobachtet haben.

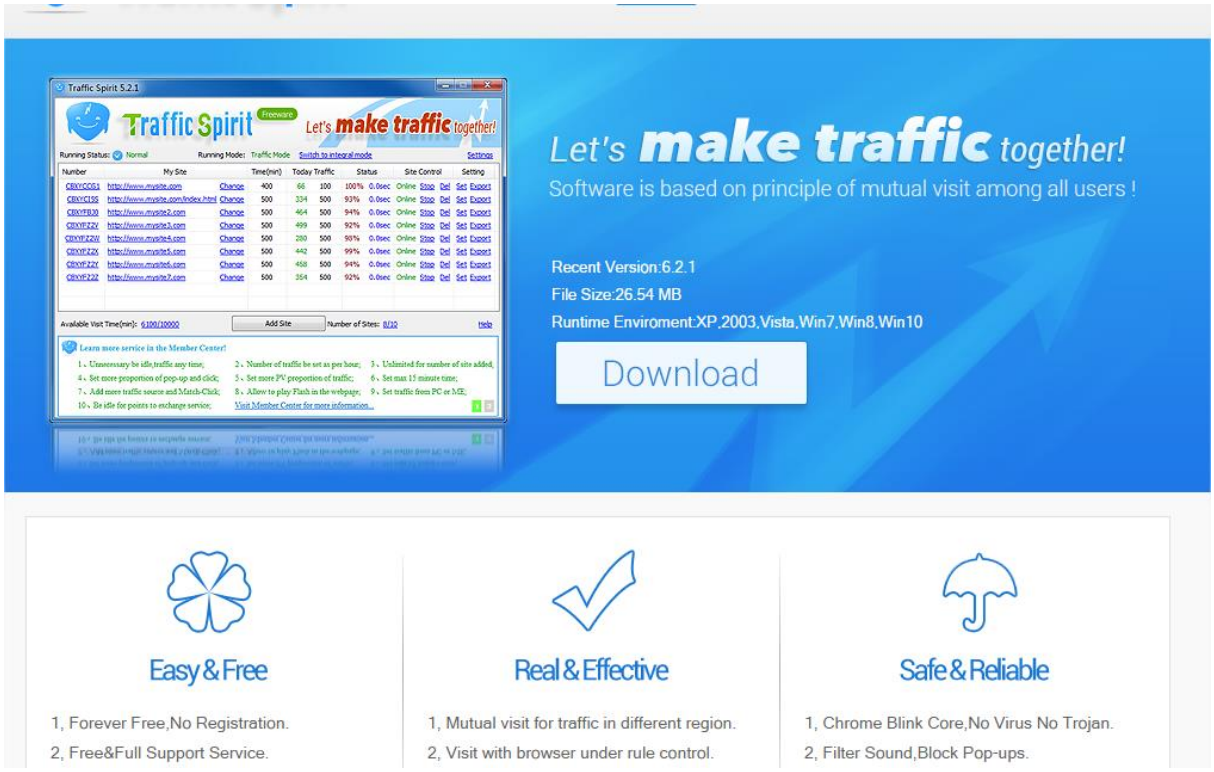
Analyse einer Attacke ohne Malware-Verwendung

Zunächst starten die Hacker ihren Angriff, indem sie mithilfe des Remote Desktop Protokolls (RDP) eine Brute-Force-Attacke gegen einen Server einleiten. Sobald sie die Login-Daten des Computers bekommen haben, haben sie kompletten Zugriff auf diesen.

Das Nächste, was die Hacker tun, ist, dass sie die sethc.exe-Datei mit dem Parameter 211 vom Command Prompt Window (CMD) des Computers starten. Dies aktiviert das ‚Sticky Keys'-Feature des Systems. Sicherlich haben Sie diese Nachricht schon mal gesehen:



Dann wird ein Programm namens ‚Traffic Spirit' heruntergeladen und gestartet. ‚Traffic Spirit' ist eine Anwendung zur Traffic-Generierung, die in diesem Fall dazu genutzt wird, um Geld mit den kompromittierten Computern zu machen.



Anschließend wird eine selbst-extrahierende Datei gestartet, die die folgenden Dateien in den %Windows%\cmdacoBin-Ordner dekomprimiert:

- registery.reg
- SCracker.bat

- sys.bat

Die Angreifer fahren dann mit dem Start des Windows Registry Editors (Regedit.exe) fort und fügen den folgenden in der registery.reg-Datei enthaltenen Key hinzu:

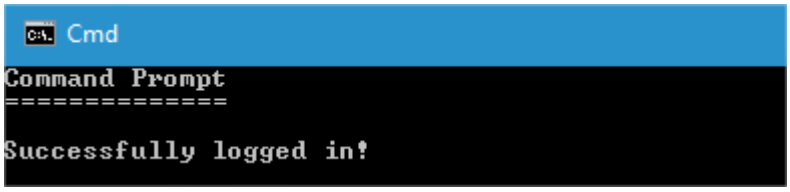
```
ion 5.00

\Microsoft\Windows NT\CurrentVersion\Image File Executi
acoBin\\SCracker.bat"
```

Der Key hat folgendes Ziel: Jedes Mal, wenn das Sticky-Keys-Feature genutzt wird (sethc.exe), startet eine Datei namens SCracker.bat. Dies ist eine Batch-Datei, die ein sehr einfaches Authentifizierungssystem implementiert. Beim Start der Datei wird folgendes Fenster angezeigt:

Der Benutzername und das Passwort werden aus zwei in der Datei sys.bat enthaltenen Variablen abgerufen:

```
1  set realusername=sys
2  set password=hudd.123
```

Auf diese Weise installiert der Angreifer eine Back Door auf dem betroffenen System. Mit dieser ‚Hintertür' ist der Angreifer in der Lage, sich mit dem Zielcomputer zu verbinden, ohne die Anmeldeinformationen eingeben zu müssen. Er aktiviert die Sticky-Keys-Funktion (z. B. durch fünfmaliges Drücken der SHIFT-Taste) und gibt den entsprechenden Benutzernamen und das Passwort in die Command Shell ein:



Die Command Shell Shortcuts erlauben dem Angreifer, auf bestimmte Verzeichnisse zuzugreifen, die Konsolenfarbe zu ändern und andere typische Befehlszeilenbefehle zu verwenden.

```
:cmd
echo Directory: %CD%
set /P CMD=Command:
if "%CMD%" == "cls" goto cls
if "%CMD%" == "home" goto home2
if "%CMD%" == "win" goto win
if "%CMD%" == "desktop" goto desktop
if "%CMD%" == "red" goto red
if "%CMD%" == "green" goto green
if "%CMD%" == "normal" goto normal
```

Der Angriff hört hier aber nicht auf. In ihrem Versuch, so viel Gewinn wie möglich von mit der angegriffenen Firma zu machen, installiert der Angreifer einen Bitcoin-Miner, um mit jedem kompromittierten Computer weiteres Geld zu erhalten. Bitcoin-Mining-Software zielt darauf ab, die Computerressourcen der Opfer zu nutzen, um die virtuelle Währung zu erzeugen, ohne dass sie es bemerken. Eine billige und sehr effektive Möglichkeit, Computerinfektionen zu monetarisieren.

Wie hilft die Sticky-Keys-Funktion den Cyberkriminellen?

Wofür benötigen Angreifer eine Back Door wenn sie über eine RDP-Verbindung gezielt auf einen Computer zugreifen können? Die Antwort auf diese Frage ist einfach: Die Installation einer Hintertür auf dem betroffenen System ermöglicht es dem Angreifer, durch Aktivierung der Sticky-Keys-Funktion jederzeit wieder auf das System zugreifen zu können, selbst wenn das Opfer den Angriff bemerkt und seine Login-Daten ändert.

Adaptive Defense 360, die fortschrittliche Cyber-Security-Lösung von Panda Security, konnte diesen **gezielten Angriff durch die kontinuierliche Überwachung des IT-Netzwerks des betroffenen ungarischen Unternehmens bereits in den Anfängen stoppen**. Die Firma wurde somit vor ernsthaften finanziellen Einbußen und Reputationsschäden bewahrt.

Über Panda Security

Seit seiner Gründung 1990 in Bilbao kämpft Panda Security gegen jedwede Bedrohung der IT-Infrastrukturen von Unternehmen bis zu Heimanwendern. Als Pionier der IT-Security-Branche gelang es dem Entwicklerteam immer wieder, mithilfe bedeutender technologischer Meilensteine den Sicherheitslevel seiner Kunden entscheidend zu erhöhen. So gilt Panda heute als ‚Entwickler des Cloud-Prinzips bei der Malware-Bekämpfung'.(Quelle: Magic Quadrant for Endpoint Protection Platforms, Gartner, 2012)
Basierend auf seinen Entwicklungen stellt das Unternehmen heute eine einzigartige Plattform zur Verfügung, die unter der Bezeichnung Adaptive Defense verschiedenste Technologien wie EDR (Endpoint Detection and Response), EPP (Endpoint Protection Platform), SIEM (Security Information and Event Management) und DLP (Data Loss Prevention) verbindet. Dadurch wird ein zuverlässiger Schutz wie zum Beispiel vor Ransomware (Cryptolocker) auf den Endpoints realisiert.
Das Unternehmen Panda Security mit Hauptsitz in Spanien ist aktuell in 60 Ländern präsent, schützt weltweit mehr als 25 Millionen Anwender und stellt seine Lösungen in 23 Sprachen zur Verfügung.

Pressekontakt

Kristin Petersen
Presse & PR
PAV Germany GmbH
Dr.-Alfred-Herrhausen-Allee 26
47228 Duisburg

Tel: +49 2065 961 352
Fax: +49 2065 961 195
Kristin.Petersen@de.pandasecurity.com
www.pandanews.de
www.pandasecurity.com/germany