PRESSEMITTEILUNG

Panda Security entdeckt neuen Trojaner RDPPatcher

Malware-Analyse der PandaLabs zeigt: Cyberkriminelle weiten ihre Geschäftsfelder zunehmend aus

***Duisburg, den 22. Februar 2017* - Panda Security, einer der weltweit führenden Hersteller für IT-Sicherheitssoftware, hat einen neuen Trojaner namens RDPPatcher entdeckt. Das Ungewöhnliche an dieser Ransomware ist, dass sie nicht dazu genutzt wird, Anmeldedaten zu stehlen. Stattdessen sammelt sie so viele Daten wie möglich. Der Trojaner wurde offenbar speziell dafür entwickelt, die infizierten Systeme zu inventarisieren und insbesondere nach POS-, ATM- und Online-Glücksspielsoftware zu suchen. Ziel dieser Hacker-Methode ist es, den Zugriff auf die Geräte an spezialisierte Gruppen von Cyberkriminellen zu verkaufen.**

In jüngster Zeit verzeichnen die PandaLabs, Panda Securitys Anti-Malware-Labor, einen starken Aufwärtstrend bei Malware, die mithilfe eines Remote Desktop Protokolls (RDP) installiert wird. Jeden Tag registrieren die PandaLabs-Experten inzwischen Tausende von Infektionsversuchen, die eine Sache gemeinsam haben: Den Zugriff auf infizierte Systeme über RDP, nachdem man mittels Brute-Force-Methode in den Besitz der Anmeldedaten gelangt ist.

Es gibt viele nützliche Verwendungsmöglichkeiten für RDP, doch in den falschen Händen kann es zu einer Waffe für Cyberkriminelle werden. Die Tatsache, dass Hacker RDP nutzen, um Ransomware zu verbreiten, ist nicht neu. Besonders Firmenumgebungen waren und sind davon seit längerem betroffen. Der Trojaner RDPPatcher, der jetzt entdeckt wurde, nutzt dieselbe Zugangstechnik, doch sein Ziel ist ein völlig anderes als das der bis dato analysierten Angriffe. Diesmal konzentriert sich die Malware darauf, POS-Terminals und Geldautomaten zu finden, nachdem sie das System infiltriert hat. Die Motivation dahinter ist, dass dies Terminals sind, die man leicht anonym aus dem Internet angreifen kann. Zudem ist der wirtschaftliche Gewinn beim Verkauf von gestohlenen Daten hoch.

Das Motiv hinter RDPPatcher: Verkauf von Systemzugriffsdaten

Im aktuellen Fall dauerte die Brute-Force-Attacke etwas über zwei Monate, bis die Angreifer im Januar 2017 auf die richtigen Anmeldedaten stießen und Zugang zum System erhielten. Nachdem das System kompromittiert war, versuchten die Cyberkriminellen, es mit Malware zu infizieren. Ihre Versuche wurden von Adaptive Defense 360, Pandas moderner Cyberabwehrtechnologie, blockiert.

Daraufhin modifizierten die Angreifer die Malware und starteten einen neuen Versuch. Wiederum ohne Erfolg. Da Pandas fortschrittliche Cybersicherheitslösung nicht auf Signaturen basiert und sich nicht auf bisheriges Wissen über Malware verlässt, um diese zu blockieren, änderte die Modifizierung das Ergebnis nicht.

Die Vorgehensweise von RDPPatcher im Detail:

Die Malware-Analyse der PandaLabs-Experten zeigt, was der Zweck der Attacke ist. Die Hashwerte der beiden Dateien lauten wie folgt:

MD5 d78be752e991ccbec16f11e4fc6b2115

SHA1 4cc9d2c98f22aefab50ee217c1a0d872e93ce541

MD5 950e8614db5c567f66d0900ad09e45ac

SHA1 9355a60dd51cfd02a921444e92e012e25d0a6be

Beide wurden mit Delphi programmiert und mit Aspack gepackt. Nachdem die PandaLabs-Experten sie entpackt hatten, stellten sie fest, dass diese einander sehr ähnlich waren. Die Experten haben die Neueste analysiert:

(950e8614db5c567f66d0900ad09e45ac).

Dieser Trojaner, der als Trj/RDPPatcher.A entdeckt wurde, modifiziert die Windows-Datensätze, um die Art der RDP-Validierung zu ändern. Dies sind die Einträge, die das System modifiziert:

HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp /v UserAuthentication /t REG_DWORD /d 1

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" /v UserAuthentication /t REG_DWORD /d 1

Zudem löscht die Malware die folgenden Einträge, wenn diese im System sind:

"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" /v legalnoticecaption /f

"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" /v legalnoticetext /f

Anschließend hinterlässt sie eine andere Datei

(MD5: 78D4E9BA8F641970162260273722C887)

im %TEMP% Verzeichnis. Diese Datei ist eine Version der Anwendung rdpwrap und wird über den Befehl runas ausgeführt mit den Parametern „-i –s", um simultane Sessions auf dem System zu aktivieren.

Dann fährt RDPPatcher fort, den Rechner zu inventarisieren und folgende Informationen zu sammeln:

- Benutzername
- Gerätename
- Zeit, in der das Gerät eingeschaltet gewesen ist
- Version des Betriebssystems
- Sprache
- Virtuelle Maschinen
- Speicher
- Prozessorname
- Anzahl der Prozessorkerne
- Prozessorgeschwindigkeit
- Antivirus

Danach verbindet der Trojaner sich mit dem Control Server (C&C-Server), um auf eine Liste der Services zuzugreifen, die die Geschwindigkeit der Internetverbindung messen. Später speichert er die Daten in Bezug auf die Upload- und Download-Geschwindigkeit. Als Nächstes überprüft er, welcher Antivirus auf dem Computer installiert ist. Im Gegensatz zu dem, was wir von den meisten Malware-Angriffen gewohnt sind, geht es jedoch nicht darum, den installierten Antivirus zu entfernen oder sein Verhalten zu ändern. Der Trojaner sammelt einfach Daten.

Die PandaLabs-Experten haben eine Liste aus den ausführbaren Programmen extrahiert, mit den Prozessen, die er durchsucht:

Siehe RDPPatcher_Tabelle1_antivirus

Im Anschluss beginnt RDPPatcher mit der Suche nach verschiedenen Softwaretypen, um den Computer weiter zu inventarisieren. Er sucht hauptsächlich nach POS-, ATM- und Online-Glücksspielsoftware. Die PandaLabs-Experten haben einen Auszug erstellt von der Liste von Software, nach der er sucht (insgesamt gibt es mehrere Hundert):

Siehe RDPPatcher_Tabelle2_software

Der Trojaner durchforstet auch die Browser-Chronik und erstellt dabei eine weitere Liste, kategorisiert nach Interessensgebieten:

Siehe RDPPatcher_Tabelle3_browser-history

Nach diesen Strings wird in der Browser-Chronik von der Malware selbst gesucht. Sie werden genutzt, um den Computer zu „kennzeichnen“, basierend auf der genutzten Software und den besuchten Webseiten.

Wenn sie mit dem Sammeln der Daten vom System fertig ist, stellt die Malware eine Web-Anfrage an den C&C-Server. Um das Senden der Informationen via Web-Traffic vor den Erkennungssystemen zu verbergen, verschlüsselt sie diese zuerst mit AES128 mithilfe des Passwortes “8c@mj}| |v*{hGqvYUG”, das in das analysierte Sample eingebettet ist. Dann kodiert es dieses auf Basis von Base64.

Beispiel einer verschlüsselten Anfrage

Der C&C-Server, der für dieses Malware-Sample genutzt wurde, befindet sich in Gibraltar.

Cyberkriminelle erschließen mit RDPPatcher neue Geschäftsfelder

Wie die Malware-Analyse zeigt, bemüht sich der Angreifer zuerst darum, den Computer zu inventarisieren, indem er alle möglichen Informationen sammelt (Hardware, Software, besuchte Webseiten, Geschwindigkeit der Internetverbindung), und eine Anwendung installiert, die mehrere RDP-Sessions gleichzeitig ermöglicht. Zu keinem Zeitpunkt findet ein Diebstahl von Anmeldedaten oder anderen Informationen statt.

Die Motivation, die hinter RDPPatcher steckt, scheint folgende zu sein: Die Cyberkriminellen verkaufen den Zugang zu den kompromittierten Computern gegen ein (verhältnismäßig) geringes Entgelt. Die Tatsache, dass die Angreifer im Besitz so vieler Informationen auf diversen Systemen sind, ermöglicht ihnen, die Zugriffsdaten an diverse Gruppen von Cyberkriminellen zu verkaufen, die sich auf unterschiedliche Bereiche spezialisiert haben. Die Arbeitsweise von RDPPatcher bestätigt einmal mehr, dass Cyberkriminalität zu einem profitablen Geschäft geworden ist, das zunehmend neue, unterschiedliche Tätigkeitsfelder für Hacker erschließt.

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