Smart Install macht tausende Cisco-Switches angreifbar

Kriminelle Hacker haben Ciscos Plug&Play-Dienst Smart Install, der eigentlich der Fernkonfiguration dient, für Remote-Angriffe auf schätzungsweise 200.000 Netzwerk-Switches missbraucht. Davon stehen rund 6400 in Deutschland, einige bei Betreibern kritischer Infrastrukturen, die mittlerweile informiert sind.

Anfällig sind prinzipiell alle Geräte, die Smart Install unterstützen – vor allem Cisco-Switches der Catalyst-Serie, aber auch einige Integrated Service Router. Der Dienst, über den sich die aktuelle Konfiguration auslesen und ändern sowie die Firmware aktualisieren lässt, erfordert keinerlei Authentifizierung. Sofern er direkt über das Internet erreichbar ist, können Angreifer ganz einfach darauf zugreifen.

Cisco sieht den Fehler bei den Admins: Wer Smart Install aus dem Internet erreichbar mache, handle grob fahrlässig. Dementsprechend gibt es vom Hersteller keinen Patch – immerhin aber einen Scanner namens smi_check für die Suche nach anfälligen Geräten. Alternativ schafft ein schneller Scan auf TCP-Port 4786 Klarheit. Wer fündig wird, sollte Smart Install entweder abschalten oder den Zugriff nur über ein separates Admin-Netz ermöglichen. *(ovw@ct.de)*

#AVGater: Angriff aus der Viren-Quarantäne

Bei einer ausgefallenen Angriffstechnik namens #AVGater missbraucht ein Angreifer den Quarantäne-Ordner von Anti-Viren-Programmen für die Systemübernahme. Dazu benötigt er allerdings physischen oder Remote-Zugriff mit einem Standard-Benutzerkonto auf den jeweiligen Rechner.

Zunächst legt der Angreifer eine mit Schadcode präparierte Programmbibliothek (DLL) in die Viren-Quarantäne und tarnt sie durch passende Namensgebung als oft genutzte Windows-Library. Dann präpariert er das System mit Verknüpfungen (NTFS junction points) auf das Verzeichnis eines Windows-Dienstes mit Systemrechten.

Betätigt der Angreifer nun die Wiederherstellungsfunktion, verschiebt die mit den benötigten Privilegien ausgestattete AV-Anwendung die DLL dorthin. Sofern der Angriff gelingt, lädt der Windows-Dienst die DLL beim nächsten Reboot. Sie läuft dann mit Systemrechten und ist vom Angreifer fernsteuerbar.

Emsisoft, Ikarus, Kaspersky, Malwarebytes, Trend Micro und ZoneAlarm haben ihre AV-Produkte mit Patches gegen #AVGater abgesichert und verteilen diese über den normalen Update-Prozess. Weitere Hersteller arbeiten noch an der Behebung der Schwachstelle; AV-Nutzer sollten deshalb verstärkt auf die Aktualität ihrer Software achten. Laut Microsoft ist der Windows Defender nicht betroffen. *(ovw@ct.de)*

Der rätselhafte Fall „Ordinypt“

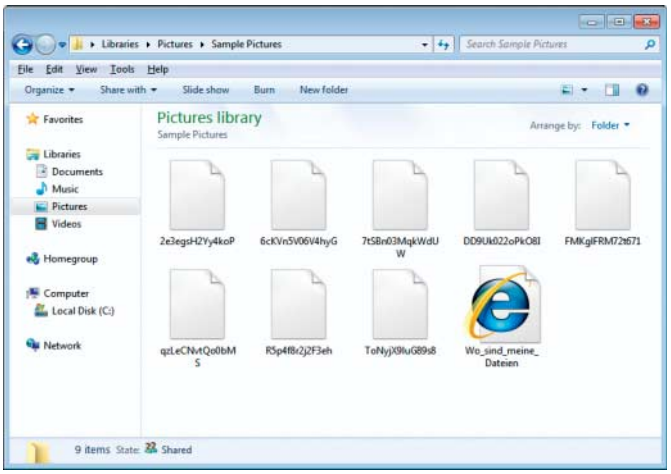

Bild: GData

Ordinypt: umbenannte Dateien samt Erpresser-Botschaft

Mitte November entdeckten Sicherheitsforscher des Antiviren-Herstellers GData einen neuen Erpressungstrojaner, den sie auf den Namen „Ordinypt“ tauften. Schnell stellte sich heraus, dass der Schädling nur vorgab, die Dateien auf den befallenen Systemen zu verschlüsseln – in Wirklichkeit benannte er die Dateien lediglich um und löschte deren Inhalt. Ein Bezahlen des geforderten Lösegeldes ist also zwecklos.

Rätsel gibt die Verbreitung des Schädlings auf. Ähnlich wie beim Massenausbruch des Trojaners Goldeneye im Dezember 2016 wurden raffiniert gemachte Phishing-Mails direkt an Personalabteilungen deutscher Firmen geschickt. Die als Bewerbungs-PDFs getarnten EXE-Dateien waren in Wirklichkeit der in Delphi geschriebene Schadcode des Trojaners. Allerdings scheinen die aktuellen Mails, anders als bei Goldeneye, nur an sehr wenige Empfänger versandt worden zu sein; insgesamt sind c’t nur ein paar Dutzend Opfer bekannt.

Eine große Infektionswelle blieb aus. Dementsprechend konnten die Angreifer auch nur wenig Geld verdienen und richteten geringen Schaden an. Ob dahinter Absicht steckt oder ob bei der Verteilung der Mails etwas schiefgelaufen ist, ist nach wie vor unklar. *(fab@ct.de)*

Sicherheits-Notizen

VMware hat zum Teil kritische Sicherheitslücken in **AirWatch Launcher, AirWatch Console for Android, Fusion, Horizon View Client** und **Workstation** geschlossen.

Nutzer der Sicherheitslösung **Symantec Endpoint Protection (SEP)** sollten zügig auf die Versionen 12.1 RU6 MP9 oder 14 RU1 updaten. Alle Vorgänger-Versionen enthalten drei Schwachstellen, die unter anderem das Umgehen von Sicherheitsmechanismen erlauben.