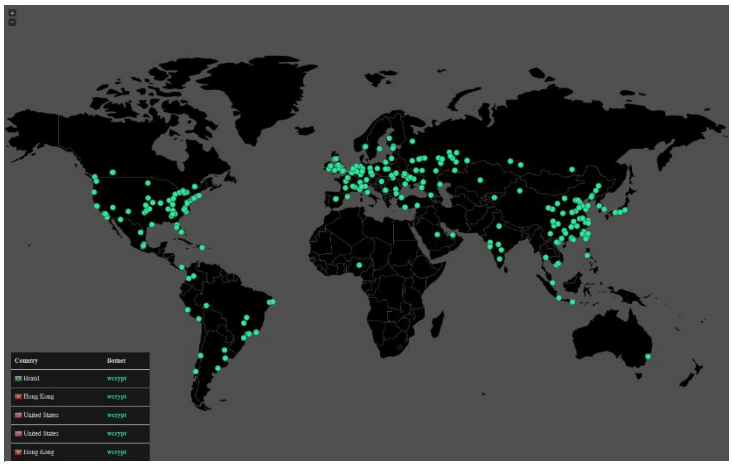
"Ooops, your important files are encrypted. If you see this text, but don't see the "Wanna Decryptor" window, then your antivirus removed the decrypt software, or you deleted it from your computer."
(Zitat der Ransomware „ WannaCrypt0r": !WannaCryptor!.bmp)

mVISE schaut hin: WannaCrypt0r

Im Rahmen der Fokussierung von mVISE auf Security-Themen haben sich unsere Security Experten die Windows Malware „WannaCrypt0r" im Detail angesehen. Wir konnten neben den aus der Presse bekannten Informationen weitere interessante Details herausfinden und aufzeigen, dass die mVISE Lösungen anbietet, die ein Unternehmen immunisieren kann.

Worum geht es?

Mitte April veröffentlichte das Hackerkollektiv „Shadows Brokers" eine umfangreiche Sammlung an Tools für den Angriff auf, unter anderem, Windows Systeme. Diese Tools stammen aus den geheimen Laboren der NSA und wurden wahrscheinlich genutzt, um ihren Spionageaufgaben nachzukommen. Viele der ausgenutzten Sicherheitslücken waren bereits oder wurden umgehend von den diversen Herstellern geschlossen. Somit konnte davon ausgegangen werden, dass keine akute Bedrohung aus dem Leak hervorgehen würde.



Ausbreitung von WannaCry, interaktiv dargestellt durch malwaretech.com

Genau so war es bei der veröffentlichten Sicherheitslücke, die für diesen Angriff verwendet wurde: EternalBlue (CVE-2017-0146 & CVE-2017-0147). Diese Lücke ermöglicht einen Angriff über das Netzwerk auf alle gängigen Windowssysteme.

Rund einen Monat vor der Veröffentlichung der Sicherheitslücke veröffentlichte Microsoft für alle unterstützten Systeme ein entsprechendes Update, was unter anderem genau diese Lücke absicherte.

Seit Freitag, den 12.05.2017, kursiert eine Ransomware mit dem Namen „WannaCry" bzw. „WannaCrypt0r" durch das Internet und infiziert diverse Windows Systeme rund um den Globus. Prominent äußerte sich dies auf den Zuginformationssystemen der Deutschen Bahn. Aber nicht nur diese waren betroffen, sondern auch Krankenhäuser des National Health Service Englands, das russischen Innenministerium, die Infrastruktur der spanischen Telefonica, sowie diverse regionale Versorger und Stadtwerke.

Was macht „WannaCrypt0r" im Detail?

Die Ransomware mit dem Namen „WannaCrypt0r" nutzt den sogenannten „EternalBlue" Exploit. Dabei wurden präparierte Emails für eine erste Infektion versendet. Diese ermöglicht daraufhin den Zugriff auf ein Windowssystem, indem ein Fehler im Server Message Block (SMB) Protokoll ausgenutzt wird.

Findet die Ransomeware ein verwundbares System, so wird in einem ersten Schritt versucht, die aktuellen Rechte auszuweiten. Dies geschieht mit dem Befehl:

```
icacls . /grant Everyone:F /T /C /
```

Sind die Rechte ausgeweitet, so wird ein Set von Dateien im aktuellen und im Temp-Ordner hinterlegt.

Wenn die infizierten Dateien im System abgelegt sind, werden mehrere Einträge in der Registry geändert. Dies hat zur Folge, dass ein automatischer Task angelegt wird, welcher die Ransomware aufruft. Gleichzeitig wird das Desktophintergrundbild geändert, um den Benutzer zu verunsichern und auf den erfolgreichen Angriff aufmerksam zu machen.

Genau 176 Datei Typen werden verschlüsselt.

Nicht nur übliche Office Dokumente werden verschlüsselt, auch lokale Datenbanken, Outlook Dateien und Archive. Auch werden vor Multimedia Dateien nicht haltgemacht. Verschlüsselte Dateien sind nicht wiederherstellbar.

UNSER TIP: Betroffene Systeme aus einem sauberen Backup wiederherstellen.

Bei dem Aufruf der automatischen Tasks wird die Ransomware aktiv. Zunächst werden diverse Programme beendet, um das System in einen stabilen Zustand zu überführen. Hierzu wird folgender Befehl verwendet:

```
taskkill /f /iml
```

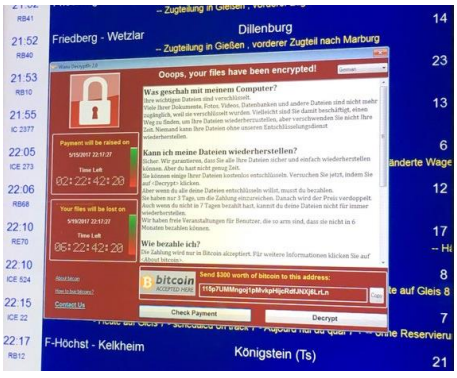
Beendet wird neben dem Microsoft SQL Server, auch der Microsoft Exchange Server. Danach wird nach 176 verschiedenen Dateiendungen gesucht und jede Datei, die eine dieser Endungen besitzt, verschlüsselt. Als Verschlüsselungsverfahren wird das als sicher angesehene AES-128 in Kombination mit RSA verwendet. Die verschlüsselten Dateien erhalten die erweiterte Endung „.wcry“ und die Originaldateien werden, wie auch die Sicherheitskopien, gelöscht.

Anschließend wird sowohl die Windows Server Backup History gelöscht, als auch das Windows Startup Recovery deaktiviert. Somit verhindert die Ransomware, dass ein befallendes System mit Bordmitteln repariert werden könnte.

Ist das System nun komplett infiziert, befindet sich in jedem Ordner der Hinweis auf die Lösegeldforderung. Der Hinweis enthält sämtliche Informationen, wie der Nutzer den Schlüssel zum Entschlüsseln seiner Daten erwerben kann. Des Weiteren wird im Hintergrund ein TOR Browser heruntergeladen, um sich damit zu Servern über das TOR Netzwerk (auch bekannt als Darknet) zu verbinden. Diese tragen die kryptischen Namen:

- 57g7spgrzlojinas.onion
- xxlvbrloxvriy2c5.onion
- 76jdd2ir2embyv47.onion
- cwwnhwhlz52maqm7.onion

Letztlich erscheint ein Fenster mit einem Countdown und der Lösegeldforderung auf rotem Hintergrund. Dies ist auch das Erscheinungsbild, was viele Reisende und Pendler auf dem Fahrplaninformationssystem der Deutschen Bahn gesehen haben:



Quelle: Zeit.de © Raphael Henkel/dpa

Warum haben Antiviren Programme und Firewalls das Problem verstärkt?

Die Aufgabe einer Antiviren Software ist der Schutz vor Viren, Ransomware und ähnlichem. Gleiches gilt für Firewalls mit sogenannte „Advanced Persistent Threat“ (APT) Funktionalität von großer, namhafter Hersteller. Da sich die klassische Signatur von Schadsoftware sehr leicht ändern lässt und somit nicht mehr erkannt wird, gehen die Hersteller dazu über, verdächtige Systeme in der Kommunikation zu blocken. Die Wirkung der Schadsoftware kann zwar nicht unterbunden werden, jedoch kann diese keine Befehle mehr von außen annehmen und wird somit für den Angreifer nutzlos.

Gleiches passierte auch mit der URL, welche die WannaCry Ransomware aufruft. So wird geprüft, ob die URLs www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com und www.ifferfsodp9ifjaposdfjhgosurijfaewrwergwea.com Inhalte zurück liefern. Diese URLs wurden von Sicherheitsforschern nachträglich reserviert und überraschenderweise so die weitere Ausbreitung gestoppt. Dies war möglich, da WannaCry nur aktiv wurde, wenn genau diese URL nicht verfügbar war – eine Art KillSwitch also. Durch das Blocken der URL durch entsprechende Antivirensoftware oder Firewalls hingegen konnte keine Antwort geliefert werden und die Malware breitet sich weiter unbehelligt aus.

Die meisten Hersteller dürften jedoch schon reagiert haben bzw. werden dies umgehend tun.

Warum waren mVISE Kunden nicht betroffen?

Die mVISE bietet ihren Kunden unter anderem einen Workshop zum Thema WSUS Patch Management. Dieser zeigt die Möglichkeit auf, auch in komplexen Umgebungen Windows Patches kontrolliert zu verteilen. So muss das einzelne System keine direkte Verbindung zum Internet haben. Mit dem Wissen aus dem Workshop, sowie der Umsetzung des Patch Management Prozesses kann sichergestellt werden, dass die Windows Systeme auf aktuellem Patch-Stand sind. Dieser stellt sicher, dass bekannte Sicherheitslücken geschlossen sind.

Das WSUS Patch Management System ist kostenlos für Kunden von Windows Server Systemen verfügbar.

Was bietet mVISE an?

Diese Art von Bedrohung beweist, wie wichtig es ist, Systeme auf dem aktuellen Stand zu halten. Unsere Experten haben ein eigenes Programm zusammengestellt, um unseren Kunden zu ermöglichen, sich mit geeigneten Maßnahmen gegen Bedrohungen dieser Art zu schützen. Dabei bieten wir Workshops zu Themen wie Patch Management, Applikationssicherheit, dynamischer und statischer Codeanalyse und Mobile Threat Protection an.

Das Sensibilisieren von Mitarbeitern ist ein erster Schritt hin zu einem sicheren Einsatz von stationären und mobilen Systemen im Unternehmen – jedoch nur der Erste von weiteren.

Bernhard Borsch
Senior Security Consultant bei der mVISE AG
Mail: bernhard.borsch@mvise.de
Mobil: +49 152 34151236

Über den Autor

Bernhard Borsch ist seit zwei Jahren als Senior Consultant im Bereich Security für die mVISE AG tätig. Zu seinen Kernkompetenzen zählen neben PKI, Kryptographie, Mobile Security auch das Themenfeld Enterprise Security.

Zurzeit unterstützt er mit seinem Team Kunden bei der Absicherung ihr Enterprise Serverlandschaft. Professionelle und fachkompetente Beratung sind sein Schlüssel zum Erfolg.