Analyse der Windows Malware „WannaCrypt0r“

mVISE IT-Security-Experten nehmen die Malware *„WannaCrypt0r“* ins Visier und zeigen, welche Lösungen die mVISE anbietet, um ein Unternehmen zu imunisieren.

Zusammenfassung

Mitte April 2017 veröffentlichte das Hackerkollektiv *„Shadows Brokers“* eine umfangreiche Sammlung an Tools für den Angriff auf 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. 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 Windows-Systeme.

Rund einen Monat vor der Bekanntgabe der Sicherheitslücke, veröffentlichte Microsoft für alle unterstützten Systeme ein entsprechendes Update, welches 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 russische Innenministerium, die Infrastruktur der spanischen Telefonica, sowie diverse regionale Versorger und Stadtwerke.

Funktionsweise „WannaCrypt0r“

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 Windows-System, 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 Desktop-Hintergrundbild geändert, um den Benutzer zu verunsichern und auf den erfolgreichen Angriff aufmerksam zu machen.
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 Datei-Endungen 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 befallenes System mit Bordmitteln repariert werden könnte.
Ist das System nun vollständig 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

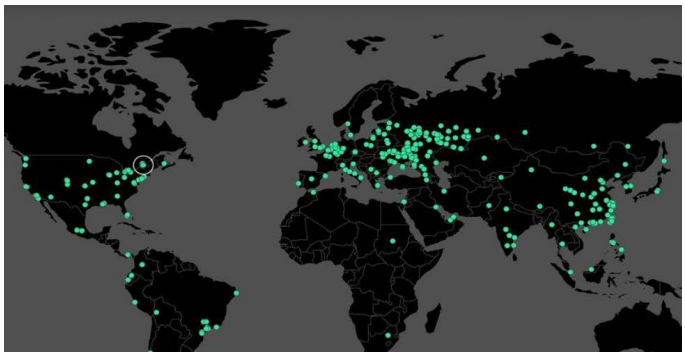
Letztlich erscheint ein Fenster mit einem Countdown und der Lösegeldforderung auf rotem Hintergrund. Dies ist auch das Erscheinungsbild, welches viele Reisende und Pendler auf dem Fahrplaninformationssystem der Deutschen Bahn gesehen haben.

176 Datei-Typen werden verschlüsselt
Nicht nur übliche Office Dokumente, auch lokale Datenbanken, Outlook-Dateien und Archive werden verschlüsselt. Auch vor Multimedia-Dateien wird nicht haltgemacht. Verschlüsselte Dateien sind **nicht** wiederherstellbar!

UNSER TIPP:
Betroffene Systeme aus einem sauberen Backup wiederherstellen.

Die Herausforderung

Die Aufgabe einer Antiviren-Software ist der Schutz vor Viren, Ransomware und Ähnlichem. Gleiches gilt für Firewalls mit sogenannter „Advanced Persistent Threat“-Funktionalität (APT) 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 Inhalte zurück liefern. Diese URLs wurden von Sicherheitsforschern nachträglich reserviert und konnten so – überraschenderweise – die weitere Ausbreitung stoppen. 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.



Ausbreitung von „WannaCry“, interaktiv dargestellt durch malware-tech.com

Profitieren Sie von qualifizierten Lösungen

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 dieses Workshops, 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.

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 mobilen Devices im Unternehmen – jedoch nur der erste von mehreren."

ÜBER DEN AUTOR

Bernhard Borsch ist seit 2014 für die mVISE AG tätig. Als Manager für das IT-Security Consulting beraten sein Team und er Kunden zum Thema IT-Security im Zuge der Herausforderungen der Digitalisierung. Zu seinen persönlichen Themenfeldern gehört neben den klassischen Themen, wie Enterprise- & Cloud-Security, PKI und Kryptographie, auch Zukunftsthemen der IT Security, wie Blockchain und Deception Technology. Professionelle und fachkompetente Beratung sind sein Schlüssel zum Erfolg.

mVISE

Wir unterstützen mittelständische und große Unternehmen aller Branchen dabei, von der digitalen Revolution zu profitieren. Die besondere Kombination aus firmeneigenen Software-Lösungen mit ausgewählten Experten-Teams in den relevanten und aktuellen IT-Themengebieten schafft nachhaltige Wettbewerbsvorteile für unsere Kunden.

Unsere Experten bestimmen, gestalten, kreieren und steuern IT-Infrastrukturen und Software-Lösungen für Datenintegrations- und Enterprise-Data-Management-Projekte, mit dem Ziel, die aktuellen Geschäftsmodelle unserer Kunden zukunftssicher zu machen und gleichzeitig neue Geschäftsmodelle zu identifizieren.

Sprechen Sie uns an – gerne stellen wir Ihnen unser Angebot
in einem persönlichen Gespräch näher vor.
service@mvise.de | www.mvise.de

mVISE AG
Wahler Straße 2
40472 Düsseldorf
Fon: +49 211 78 17 80 – 0