# Neue Ransomware Petya breitet sich rasant aus

# Ransomware Petya befällt erneut viele Computer – Emsisoft Antivirus-Programm bietet Schutz

Weitere Ransomware rasant in Europa und anderen Kontinenten aus. Bei dem Schädling handelt es sich um eine neue Version der Petya-Ransomware-Familie, die in IT-Fachkreisen auch als Petna bekannt ist.

## Was ist Petya-Ransomware

Die aktuelle Petya-Version scheint eng mit der bisherigen Petya-Ransomware-Familie verwandt zu sein. Sie trieb erstmals Ende März 2016 ihr Unwesen. Das Einzigartige an Petya ist, dass ein eigenes Betriebssystem integriert ist, das installiert und anstelle von Windows ausgeführt wird. Auf diese Weise kann der Schädling beim nächsten Hochfahren auch verschiedene wichtige Dateien auf dem Startdatenträger verschlüsseln. Die neue Version hat diese Methode kopiert, wobei der Code des Petya-Betriebssystems nahezu identisch mit dem Vorgänger ist. Nur für die Verbreitung, den Systembefall und die Verschlüsselung der Dateien wird ein anderes Vorgehen eingesetzt.

Nach der erfolgreichen Infektion eines Systems wird von Petya eine Lösegeldforderung angezeigt (auf Englisch), die eine Bitcoin-Zahlung in Höhe von 300 US-Dollar auf ein über eine posteo.net-Adresse laufendes Konto verlangt:

Zum Zeitpunkt, an dem die englische Version dieses Artikels verfasst wurde, sind bereits 3,1 Bitcoin in 28 Zahlungen eingegangen – für den Ransomware-Entwickler ein Verdienst in Höhe von 7300 USD. Das klingt nach einem vergleichsweise kleinen Betrag. Angesichts des frühen Zeitpunkts und der schnellen Verbreitung werden jedoch sicher noch mehr Opfer zur Rettung ihrer

Dateien zahlen.

## Wie kommt es zu einer Infektion mit Petya?

Die erste Infektionswelle mit Petya kann bis zurück auf den Hack von MeDoc verfolgt werden, einer in der Ukraine weit verbreiteten Buchhaltungssoftware. Unbekannte Angreifer hatten sich Zugriff auf die Update-Server der Software verschafft und den Kunden der Firma die Petya-Ransomware als Software-Update „bereitgestellt". Bereits in der Vergangenheit sind andere Ransomware-Familien wie XData ähnlich vorgegangen, um ihren Angriff zu starten.

Nachdem dort einige Systeme infiziert worden waren, konnte sich Petya schnell über denselben von Shadow Brokers veröffentlichten NSA-Exploit ausbreiten, der auch schon von WannaCry genutzt worden war. Der als EternalBlue bekannte Exploit nutzt eine Schwachstelle im Microsoft SMBv1-Protokoll aus, über die ein Angreifer Kontrolle über ein System erlagen kann, wenn:

- das SMBv1-Protokoll aktiviert ist,
- es über das Internet zugänglich ist und
- es nicht mit dem im März 2017 veröffentlichten Patch MS17-010 aktualisiert wurde.

Sollte der EternalBlue-Exploit erfolgreich sein, wird auf dem System eine Hintertür mit dem Codenamen DoublePulsar eingerichtet. Die Malware nutzt diese Hintertür, um sich auf das infizierte System zu übertragen und dort auszuführen.

Petya verwendet zudem verschiedene Administrationsfunktionen von Windows, um sich im befallenen Netzwerk auszubreiten. Ein einzelner nicht aktualisierter Rechner reicht also schon aus, um ein gesamtes Netzwerk zu infizieren – selbst, wenn die anderen Computer auf dem neuesten Stand sind. Für die laterale Verbreitung der Ransomware im lokalen Netzwerk nutzt Petya die Windows-Verwaltungsinstrumentation (WMI) und das beliebte PsExec-Tool in Kombination mit Netzwerkfreigaben.

# Wie verschlüsselt Petya Ihre Dateien?

Petya besteht aus zwei verschiedenen Ransomware-Modulen. Das erste ähnelt stark typischen Ransomware-Familien und verschlüsselt den Anfang (bis zu 1 MB) von Dateien mit folgenden Erweiterungen:

> *.3ds, .7z, .accdb, .ai, .asp, .aspx, .avhd, .back, .bak, .c, .cfg, .conf, .cpp, .cs, .ctl, .dbf, .disk, .djvu, .doc, .docx, .dwg, .eml, .fdb, .gz, .h, .hdd, .kdbx, .mail, .mdb, .msg, .nrg, .ora, .ost, .ova, .ovf, .pdf, .php, .pmf, .ppt, .pptx, .pst, .pvi, .py, .pyc, .rar, .rtf, .sln, .sql, .tar, .vbox, .vbs, .vcb, .vdi, .vfd, .vmc, .vmdk, .vmsd, .vmx, .vsdx, .vsv, .work, .xls, .xlsx, .xvd, .zip*

Zum Verschlüsseln wird der AES-Algorithmus mit einem 128-Bit-Schlüssel verwendet. Dieser wird dann mit einem öffentlichen RSA-Schlüssel verschlüsselt, der in der ausführbaren Datei der Ransomware integriert ist. Weitere Informationen darüber, wie Ransomware mithilfe von RSA und AES Dateien sicher verschlüsselt, können Sie in dem Artikel zu Verschlüsselung unserer „Ransomware im Fokus“-Reihe nachlesen.

Das zweite Modul wurde direkt aus der Petya-Familie kopiert. Es handelt sich um ein kleines selbst erstelltes Betriebssystem, das in den MBR (Master Boot Record) des Systems installiert wird – sofern das System über MBR hochfahren kann und die Ransomware die dazu erforderlichen Rechte erlangen konnte. Wenn das Petya-Betriebssystem startet, wird die Masterdateitabelle (MFT) des Startlaufwerks mit einer Salsa20-Stromchiffre verschlüsselt.

Die Masterdateitabelle ist die interne Datenstruktur des Windows-Dateisystems NTFS. Hier wird letztendlich für jede Datei verzeichnet, wo sich welche Daten auf der Festplatte befinden. Darüber hinaus verschlüsselt das Petya-Betriebssystem die ersten Sektoren jeder Datei, damit auch keine Wiederherstellungstools mehr funktionieren. Ohne die Masterdateitabelle kann Windows nichts mehr mit den Daten auf der Festplatte anfangen, was schließlich dazu führt, dass der Benutzer nicht mehr auf sein System zugreifen kann.

# Wie können Sie sich vor Petya schützen?

Unsere für den WannaCry-Angriff gegebenen Ratschläge gelten auch für Petya. Stellen Sie also am besten sofort sicher, dass Sie die neuesten Sicherheitsupdates auf Ihren Windows-Computern und -Servern installiert haben. Nach dem letzten Angriff hatte Microsoft ausnahmsweise Sicherheitspatches für „nicht mehr unterstützte Systeme", wie Windows XP und Windows Server 2003 bereitgestellt, damit selbst bei diesen die Sicherheitslücke behoben werden kann.

Wie bereits in unserem Artikel zu Ransomware erläutert, ist der beste Schutz eine gut organisierte Sicherungsstrategie. Das gilt umso mehr, da die Verschlüsselung von Petya sehr sicher ist und die Daten nur über den Ransomware-Entwickler oder Sicherungen wiederhergestellt werden können. Ein weiterer wichtiger Punkt beim Schutz Ihres Systems ist die Installation wichtiger Windows-Updates, da ein wesentlicher Infektionsweg von Petya bis dato der EternalBlue-SMBv1-Exploit ist, für den es bereits seit einigen Monaten einen Patch gibt.

Sie werden sich freuen zu erfahren, dass sich das von Emsisoft Anti-Malware und Emsisoft Internet Security in seiner Verhaltensanalyse eingesetzte Anti-Ransomware-Modul als eine wirkungsvolle Verteidigung erwiesen hat. Der Ransomware-Angriff über die DoublePulsar-Hintertür wird erkannt, bevor die Datei ausgeführt werden kann. Damit sind alle unsere Benutzer vor dieser und Hunderten anderen Arten von Ransomware geschützt – unabhängig von Signaturen.

Schützen Sie sich sofort mit der aktuellen Version von Emsisoft Antivirus-Software!

Schauen Sie hier nach unserem Angebot.

Text mit freundlicher Genehmigung von Emsisoft