PRESSEMITTEILUNG

FAQs zum Thema Cryptolocker:

Cryptolocker kann jeden treffen

- Was Sie über diese Malware wissen sollten
- Wie Unternehmen sich schützen können

Duisburg, den 22. März 2016 – Der Trojaner ‚Cryptolocker' ist die IT-Bedrohung, über die momentan jeder spricht. Sie betrifft sowohl Privatanwender als auch Unternehmen. Firmen sind ihr aufgrund der großen Menge an vertraulichen Informationen, die sie verarbeiten, jedoch stärker ausgesetzt. Panda Security erklärt, was Cryptolocker ist, wie die Malware funktioniert und wie Unternehmen sich davor schützen können.

Was ist Cryptolocker?

Als Cryptolocker bezeichnet man eine neue Familie von Ransomware, deren Konzept darauf basiert, Geld von IT-Nutzern zu erpressen. So wird der Trend fortgeführt, der von einer anderen berühmt-berüchtigten Malware begonnen wurde – dem sogenannten „Polizei-Virus". Diese Schadsoftware forderte die PC-Nutzer auf, eine Strafe zu zahlen, um ihre Computer zu entsperren. Im Gegensatz zum Polizei-Virus „kidnappt" CryptoLocker die Dokumente von Usern und verlangt von diesen eine Lösegeldzahlung innerhalb einer bestimmten Frist, wenn sie ihre Dokumente zurückerhalten wollen.

Was unterscheidet Cryptolocker von anderen digitalen Bedrohungen, mit denen Unternehmen konfrontiert sind?

Cryptolocker ist eine bestimmte Form des sogenannten gezielten Angriffs. Wie alle gezielten Angriffen erfordert diese Schadsoftware hohen technischen Aufwand und folglich große Investitionen von den Cyberkriminellen, die diese Malware-Art nutzen.

Der große Unterschied zu anderen Hackerattacken besteht darin, dass sich in diesem Fall das Zielunternehmen des Angriffs bewusst ist, weil die Malware den infizierten Nutzer benachrichtigt.

Wie kommt die Malware auf die betroffenen Computer?

Für die Verbreitung der Cryptolocker-Malware nutzen die Hacker meist gängige Social-Engineering-Techniken. So erhält das Opfer zum Beispiel eine E-Mail mit einer als ZIP-Datei verpackten „Rechnung", die angeblich nicht bezahlt wurde. Doch auch Besuche auf infizierten Webseiten oder das Anklicken von mit Cryptolocker verseuchten Social-Media-Beiträgen können eine Infektion mit der Schadsoftware nach sich ziehen.

Der Trojaner startet, wenn der User die angehängte ZIP-Datei entpackt und versucht, das PDF zu öffnen. Dabei nutzt Cryptolocker das Windows-Standardverhalten aus, die Endungen von Dateinamen zu verstecken, und tarnt so die wahre .EXE-Endung der schädlichen Datei.

Sobald das Opfer die Datei ausführt, wird der Trojaner auf dem Computer speicherresistent und führt die folgenden Aktionen aus:

- Er speichert sich selbst in einen Ordner des Nutzerprofils (AppData, LocalAppData).
- Er fügt der Registry einen Schlüssel hinzu, um sicherzustellen, dass er jedes Mal ausgeführt wird, wenn der betroffene Computer hochfährt.

Wie funktioniert Cryptolocker genau?

Cryptolocker erzeugt einen zufälligen symmetrischen Schlüssel für jede Datei, die er verschlüsselt, und kryptografiert den Inhalt der Datei mit dem AES-Algorithmus unter Benutzung dieses Schlüssels. Dann codiert er den zufälligen Schlüssel, wofür er einen asymmetrischen öffentlich-privaten Key-Verschlüsselungsalgorithmus (RSA) benutzt sowie Schlüssel mit mehr als 1024 Bits und fügt ihn der verschlüsselten Datei hinzu. Auf diese Weise stellt der Trojaner sicher, dass nur der Inhaber des privaten RSA-Keys den zufälligen Schlüssel erhalten kann, der für die Verschlüsselung der Datei genutzt wurde. Da die Computerdateien außerdem überschrieben werden, ist es unmöglich, sie mit Hilfe von forensischen Methoden wiederherzustellen.

Nach dem Start besorgt sich der Trojaner als erstes den öffentlichen Schlüssel (PK) von seinem Command-and-Control (C&C)-Server. Damit er einen aktiven C&C-Server finden kann, enthält der Trojaner einen Domain-Generation-Algorithmus

(DGA), auch als ‚Mersenne-Twister' bekannt, um zufällige Domain-Namen zu generieren. Dieser Algorithmus nutzt das aktuelle Datum als ‚Keimzelle' und kann jeden Tag bis zu 1.000 verschiedene Domains mit fester Größe erzeugen.

Nachdem der Trojaner den PK heruntergeladen hat, speichert er ihn innerhalb des folgenden Windows Registry-Keys:

HKCUSoftwareCryptoLockerPublicKey.

Dann beginnt er mit der Verschlüsselung der Dateien auf der Computerfestplatte und jedem Netzlaufwerk, auf das der infizierte User zugreifen kann.

Cryptolocker verschlüsselt nicht jede Datei, die er findet, sondern nur die nicht ausführbaren Dateien mit den Endungen, die im Code der Malware enthalten sind:

*.odt	*.ods	*.odp	*.odm	*.odc	*.odb
*.wps	*.xls	*.xlsx	*.xlsm	*.xlsb	*.xlk
*.ppt	*.pptx	*.pptm	*.mdb	*.accdb	*.pst
*.dwg	*.dxf	*.dxg	*.wpd	*.rtf	*.wb2
*.mdf	*.dbf	*.psd	*.pdd	*.eps	*.ai
*.indd	*.cdr	????????.jpg	*.doc	????????.jpe	*.jpg
*.dng	*.3fr	*.arw	*.srf	*.sr2	*.bay
*.crw	*.cr2	*.dcr	*.kdc	*.erf	*.mef
*.mrw	*.nef	*.nrw	*.orf	*.raf	*.raw
*.rwl	*.rw2	*.r3d	*.ptx	*.pef	*.srw
*.x3f	*.der	*.cer	*.crt	*.pem	*.pfx
*.p12	*.p7b	*.p7c	*.docx	*.docm	

Außerdem protokolliert Cryptolocker jede verschlüsselte Datei im folgenden Registry-Key:

HKEY_CURRENT_USERSoftwareCryptoLockerFiles

Wenn der Trojaner mit der Verschlüsselung aller Dateien, welche die zuvor genannten Bedingungen erfüllen, fertig ist, zeigt er eine Nachricht an, die den Nutzer auffordert, ein Lösegeld für die gekidnappten Daten zu zahlen. Zudem bekommt das Opfer ein bestimmtes Zeitlimit für die Zahlung, bevor der private Schlüssel, der im Besitz des Malware-Entwicklers ist, zerstört wird.

Wie können sich Unternehmen vor dieser Art von Bedrohung schützen?

Im Allgemeinen sind Unternehmen kaum gegen diese Angriffsart geschützt, daher kommen auch die hohen Infektionsraten und das Echo in den Medien. Diese Schwachstelle ergibt sich aus der Tatsache, dass die herkömmlichen Erkennungsmechanismen, wie zum Beispiel E-Mail- oder Webfiltersysteme und Antivirenlösungen, einfach nicht effizient genug sind.

Traditionelle Erkennungsmechanismen basieren mehr oder weniger darauf, Software, URLs oder E-Mail-Signaturen mit bekannten Mustern von bereits entdeckten und klassifizierten Bedrohungen zu vergleichen. Doch bei durchschnittlich 230.000 neuen Malware-Exemplaren pro Tag ist diese Strategie hinfällig geworden. Selbst wenn IT-Security-Unternehmen viel investieren, um die Effizienz ihrer althergebrachten Schutzmechanismen zu verbessern und die Reaktionszeiten zu verkürzen, bleiben diese weiterhin nur reaktive Mechanismen. Diese Strategie läuft letztlich auf ein Wettrennen zwischen den Kriminellen und den Sicherheitsanbietern hinaus, welches letztere nicht immer gewinnen können.

Deshalb benötigen wir für die Erkennung von Cryptolockern – aber auch ganz allgemein für den Schutz vor anderen fortschrittlichen Hackerangriffen – eine völlig neue Herangehensweise an das Thema IT-Security. Panda hat das bereits vor sieben Jahren erkannt, was zur Entwicklung von Panda Adaptive Defense führte – einem ganz neuen, einzigartigen Schutzsystem. Dieses ist tatsächlich in der Lage, Cryptolocker zu stoppen, und – was noch wichtiger ist – all seine Varianten.

Was unterscheidet Adaptive Defense von anderen Lösungen?

Zunächst einmal ist Adaptive Defense eher ein Service als eine Lösung. Adaptive Defense evaluiert und klassifiziert alle Anwendungen, die auf den Endpoints der Kunden laufen, basierend auf der Analyse von mehr als 2.000 Aktionen, die jede Anwendung ausführen kann. Dieser Prozess findet in unserer weitestgehend automatisierten Big-Data-Umgebung statt. Ergänzt wird er durch die manuellen Analysen unserer Sicherheitsexperten in den PandaLabs.

Die ständige Klassifizierung und Überwachung aller Anwendungen ermöglicht es nicht nur, Malware zu identifizieren und zu kategorisieren, sondern auch Goodware und ihre Schwachstellen. Pandas Datenbank enthält mehr als 1,2 Milliarden Goodware-Anwendungen. Während eine traditionelle Antivirenlösung bekannte Malware blockiert und davon ausgeht, dass jede andere Anwendung harmlos ist,

erlaubt Adaptive Defense nur die Ausführung von Anwendungen, die bereits als Goodware klassifiziert wurden.

Ist diese Vorgehensweise nicht mit dem klassischen Whitelisting identisch?

Man könnte argumentieren, dass es bereits Whitelisting-Tools mit einer ähnlichen Herangehensweise gibt. Adaptive Defense geht jedoch über das traditionelle Whitelisting hinaus, indem es die gesamten Klassifizierungsarbeiten automatisch und transparent für den Systemadministrator des Unternehmens ausführt. Zudem handelt es sich bei Adaptive Defense um einen sogenannten ‚Managed Service'. Das bedeutet, dass der Systemadministrator keine Arbeitszeit in das Whitelisting investieren muss, da dieses komplett von Pandas ‚Collective Intelligence' sowie von unseren Experten in den PandaLabs übernommen wird.

Trotzdem bietet Adaptive Defense, nachdem es auf dem Endpoint installiert worden ist, vollen Einblick in alle auf dem Gerät installierten Anwendungen. Die IT-Administratoren werden über jede entdeckte Bedrohung informiert, sodass sie entsprechende Gegenmaßnahmen ergreifen können.

Gezielte Angriffe, APTs, Cryptolocker… Werden Firmen auch in Zukunft dermaßen im Fadenkreuz von Cyberkriminellen stehen?

Cyberkriminalität ist für Hacker zu einem sehr profitablen Geschäft geworden. Die Ressourcen und Tools, die den Cyberkriminellen heutzutage zur Verfügung stehen, sind beträchtlich. Ohne entsprechende Schutzmaßnahme ist deswegen definitiv kein Unternehmen – egal wie groß oder klein es ist – vor Cryptolocker und ähnlichen Angriffen sicher.

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/