HINTERGRUNDINFORMATION

2015 war das Jahr der Cryptolocker

Duisburg, den 04. Februar 2016 - Ende 2013 wurden in den PandaLabs, dem Anti-Malware-Labor des spanischen IT-Sicherheitsspezialisten Panda Security, erste Anzeichen für das entdeckt, was in 2015 schließlich zur lukrativsten Angriffsart für Cyberkriminelle geworden ist: Cryptolocker. Jedoch handelt es sich bei Cryptolocker nicht, wie der Name vielleicht suggerieren könnte, um eine einzige Malware. Sondern die Bezeichnung Cryptolocker steht für diverse Varianten einer bestimmten Ransomware, deren Geschäftsmodell auf Erpressung basiert.

Die Schadsoftware arbeitet dabei immer nach demselben einfachen Prinzip: Sie verschlüsselt Dokumente und verlangt ein Lösegeld für die Entschlüsselung. Die Cyberkriminellen geolokalisieren die IP-Adresse des Opfers, um die Nachricht anzuzeigen, die die Anweisungen für die Zahlung des Lösegeldes enthält. Die Nachricht ist immer in der jeweiligen Landessprache verfasst. Die Zahlungen müssen in Bitcoins erfolgen. Der Kontakt mit den Kriminellen erfolgt via „Tor", einem Netzwerk zur Anonymisierung von Verbindungsdaten, das es den Kriminellen ermöglicht, anonym mit ihren Opfern in Verbindung zu treten und so von den Strafverfolgungsbehörden nicht entdeckt zu werden.

Im Laufe des Jahres 2014 wurden die Cyptolocker-Angriffe immer beliebter. Die Cyberkriminellen begannen mit gelegentlichen Attacken auf Einzelpersonen, bevor sie sich auf Unternehmen konzentrierten. Das stellte sich bald als weitaus lohnender heraus: Die gestohlenen Informationen hatten einen höheren Wert und das (verhältnismäßig geringe) geforderte Lösegeld von ca. 300 bis 500 € war für die Mehrheit der Unternehmen nicht der Rede Wert und wurde meist ohne groß zu zögern gezahlt.

2015 haben die Experten der PandaLabs die Entwicklung der Cryptolocker-Familien weiter beobachtet und dabei festgestellt, dass die Cyberkriminellen ihre Angriffe immer stärker perfektioniert und angepasst haben, um alle Verteidigungs-maßnahmen zu umgehen, die ihre ‚Geschäfte' vereiteln sollten:

- Die Verschlüsselung der Dateien ist professioneller geworden. Kleine Fehler beim Verschlüsseln ermöglichten es Sicherheitsunternehmen zuvor, Tools zu entwickeln, um die betroffenen Daten und Dokumente wiederherzustellen, ohne auf die Lösegeldforderung eingehen zu müssen.

- Neue Cryptolocker-Familien sind erschienen. Dies ist ein Zeichen dafür, dass immer mehr cyberkriminelle Gruppen Gebrauch von der beliebten Ransomware machen.
- Als Zahlungsmittel werden ausschließlich Bitcoins genutzt, eine sogenannte ‚Kryptowährung', die die Anonymität der Empfänger garantiert.
- Die Cyberkriminellen haben sich auf zwei Verbreitungswege der Cryptolocker konzentriert:
    - über Exploit Kits
    - per E-Mail mit komprimierten Anhängen
- Es wurden neue Angriffsformen entwickelt. In jüngster Zeit haben die Hacker begonnen, für die Einschleusung von Cryptolockern PowerShell Skripte zu nutzen, da diese standardmäßig in Windows 10 enthalten sind.

Wie man sich vor Cryptolockern schützen kann

Wenn es darum geht, uns selbst zu schützen, müssen wir daran denken, dass Cryptolocker - im Vergleich zu traditioneller Malware - andere Ziele verfolgen. Zum Beispiel sind sie nicht beständig, da sie nach dem Verschlüsseln der Dokumente nicht im System bleiben müssen; und es gibt tatsächlich Varianten, die sich selbst löschen. Zudem macht es Cryptolockern nichts aus, wenn sie von einem Antivirus entdeckt werden. Es kommt nur darauf an, dass sie ihren Angriff starten können, bevor sie entdeckt werden. Was danach passiert, spielt für sie keine Rolle.

Traditionelle Antivirenlösungen sind im Fall von Cryptolocker meist nutzlos, da die Ransomware vor dem Angriff überprüft, ob diese Technologien das Sample entdecken können. Wenn dies der Fall ist, verändert sie sich, um die Sicherheitsmaßnahmen zu umgehen. Auch eine Verhaltensanalyse kann in den meisten Fällen nicht erkennen, was die Ransomware tut, da diese sich gewöhnlich selbst in den Verarbeitungssystemen installiert und die Dateien von dort aus verschlüsselt. Dadurch sieht es wie ein ganz normaler Prozess aus.

Tatsächlich kann nur ein System, das alle auf einem Computer laufenden Anwendungen überwacht (wie zum Beispiel Panda Adaptive Defense 360), eine effektive Methode sein, um derartige Cryptolocker-Angriffe rechtzeitig zu stoppen und unsere Dokumente zu schützen.

In der Regel verbreitet sich CryptoLocker allerdings noch immer durch Besuche auf infizierten Social Media- oder anderen Webseiten oder via Phishing-Mails. Dabei werden Social-Engineering-Techniken benutzt, die die Opfer dazu verleiten, auf

bestimmte Dateien oder Links zu klicken. Daher empfehlen die IT-Experten von Panda Security folgende Vorsichtsmaßnahmen:

- Nehmen Sie sich vor E-Mails von unbekannten Absendern in Acht und klicken Sie keinesfalls auf mitgesandte Anhänge.
- Deaktivieren Sie das Ausblenden von bekannten Dateiendungen in Windows, damit Sie verdächtige Dateien besser erkennen können.
- Denken Sie daran, dass Sie unbedingt ein Backupsystem für Ihre wichtigen Dateien haben sollten. Damit können Sie nicht nur den durch Malwareinfektionen verursachten Schaden minimieren, sondern auch Datenverluste durch Hardwareprobleme und andere Störfälle.
- Sollte Ihr PC trotzdem mit Cryptolocker infiziert sein und Sie haben keine Sicherungskopie von Ihren Dateien, empfehlen wir Ihnen trotzdem, das Lösegeld nicht zu zahlen. Das ist niemals eine gute Lösung, da es die Malware in ein äußerst profitables Geschäftsmodell verwandelt und zum Erfolg dieser Angriffsart beiträgt.

Über PandaLabs

PandaLabs ist das Anti-Malware-Labor des weltweit agierenden IT-Spezialisten Panda Security und fungiert als dessen zentrale Stelle für Malware-Treatment. PandaLabs entwickelt kontinuierlich und in Echtzeit die notwendigen Gegenmaßnahmen, um Panda-Security-Kunden vor allen Arten von schädlicher Software auf globalem Level zu schützen. PandaLabs ist somit verantwortlich für die Durchführung detaillierter Scans aller Malware-Arten. Ziel ist es, sowohl den Schutz für die Panda Security Kunden zu verbessern, als auch die Öffentlichkeit aktuell und zeitnah zu informieren.

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/