Der Fall PowerLocker – Analyse einer Ransomware

13.03.2014, 18:08 | IT, New Media & Software

Pressemitteilung von: *Panda Security PAV Germany GmbH*

PowerLocker, auch PrisonLocker genannt, ist eine neue Familie von Ransomware, die Dateien auf dem Computer des Opfers verschlüsselt (wie bei anderer solcher Malware) und außerdem damit droht, die Computer von Anwendern zu blockie-ren, bis sie ein Lösegeld zahlen (wie beim „Police Virus“).
Obwohl die Idee, diese beiden Techniken zu kombinieren, mehr als ein paar schlaflose Nächte gekostet haben mag, ist die Malware in diesem Fall nur ein Prototyp. In der Entwicklungsphase hat der Malware-Autor in Blogs und Foren gepostet und seine Fortschritte beschrieben sowie die verschiedenen Techniken erklärt, die in den Code integriert sind.
Nachricht des Malware-Autors in Pastebin:
In diesem Post beschreibt der Autor beispielsweise, dass PowerLocker eine in c/c++ geschriebene Ransomware ist, die Dateien auf infizierten Computern ver-schlüsselt, den Bildschirm sperrt und Lösegeld fordert.
Die Ransomware verschlüsselt die Dateien, was typisch für diese Art von Malware ist. Dazu benutzt sie Blowfish als Verschlüsselungsalgorithmus mit einem einzig-artigen Schlüssel für jede verschlüsselte Datei. Sie speichert jeden Schlüssel, der mit einem öffentlichen/privaten RSA-2048 Schlüsselalgorithmus erzeugt wurde, sodass nur der Inhaber des privaten Schlüssels alle Dateien entschlüsseln kann.
Außerdem benutzt PowerLocker laut Aussage seines Autors sowohl anti-debugging, anti-sandbox und anti-VM Features als auch Tools, die beispielsweise den Task Manager, den Registry-Editor oder das Befehlszeilenfenster ausschal-ten.
Jedoch hat all die Publicity für PowerLocker, die der Autor in Foren und Blogs vor dem Erscheinen dieser Ransomware erzeugt hat, dazu geführt, dass er in Florida, USA, verhaftet wurde. Infolgedessen gibt es heute keine endgültige Version die-ser Malware und es gibt keine Beweise dafür, dass sie In-the-wild (in freier Wild-bahn) existiert.
Nichtsdestotrotz sind wir der Meinung, dass es sich lohnt, die aktuelle Version von PowerLocker zu analysieren, da noch jemand anders im Besitz des Quellco-des oder sogar einer neueren Version sein könnte.
Analyse von PowerLocker
PowerLocker überprüft zuerst, ob bereits zwei Dateien mit RSA-Schlüsseln er-stellt worden sind. Wenn das nicht der Fall ist, generiert er den öffentlichen und privaten Schlüssel in zwei Dateien auf der Festplatte (pubkey.bin und priv-key.bin).
Im Gegensatz zu anderen Ransomware-Exemplaren, welche den Windows Cryto-API-Service nutzen, benutzt PowerLocker die openssl-Programmbibliothek, um die Schlüssel zu erzeugen und die Dateien zu verschlüsseln.
Wenn er die Schlüssel hat, startet PowerLocker ein rekursives Durchsuchen der Verzeichnisse, um Dateien zum Verschlüsseln zu finden. Dabei schließt er – nicht sehr effektiv – Dateien aus, die einen der Dateinamen haben, die von der Malwa-re genutzt werden: privkey.bin, pubkey.bin, countdwon.txt, cryptedcount.txt. Er meidet auch $recycle.bin, .rans, .exe, .dll, .ini, .vxd oder .drv Dateien, um zu verhindern, dass dem Computer ein irreparabler Schaden zugefügt wird. Der Au-tor hat jedoch vergessen, bestimmte Erweiterungen auszuschließen, die Dateien entsprechen, welche empfindlich genug sind, um die Funktionalität des Systems zu beeinträchtigen, wie z. B. .sys Dateien. Das bedeutet, dass jeder mit Power-Locker infizierte Computer nicht mehr in der Lage wäre, einen Neustart auszu-führen.
Darüber hinaus ist es in dieser Version möglich, einen Parameter zu nutzen, um zu kontrollieren, ob die Ransomware mithilfe der anfangs erzeugten pubkey.bin und pivkey.bin Schlüssel Dateien verschlüsselt oder entschlüsselt.
Diese Version enthält nicht das vom Autor beschriebene Feature zum Sperren des Bildschirms, obwohl sie eine Konsole mit Debug-Nachrichten, Namen von zu verschlüsselnden/entschlüsselnden Dateien, etc. anzeigt und den Anwender auf-fordert, vor jeder Verschlüsselung oder Entschlüsselung eine Taste zu drücken.
Schlussfolgerungen
Gegenwärtig gibt es nur eine halbfertige Version von PowerLocker, die praktisch als harmlos bezeichnet werden kann und der viele der wichtigsten Features feh-len, die der Autor in Foren und Blogs beschrieben hat, wie z. B. Anti-Debugging, Bildschirmsperre, etc.
Obwohl die Ransomware noch nicht voll funktionsfähig ist, empfehlen wir ein System zum Sichern wichtiger Dateien, nicht nur um Sicherheit im Falle von Hardwareproblemen zu bieten, sondern auch um den Schaden solcher Arten von Malwareinfektionen zu minimieren.
Außerdem sollten User nicht vergessen, dass wenn sie kein Backup-System ha-ben und Ihr System infiziert wird, wir

dringend davon abraten, das Lösegeld zu zahlen.

Portrait

1990 in Bilbao, Spanien, gegründet, hat sich Panda Security zum Ziel gesetzt, seinen Kunden intelligenten Schutz gegen Malware bei geringstmöglicher Systembelastung zu bieten. Als erster Anbieter überhaupt hat Panda dazu im Jahr 2006 eine Scan-Technik vorgestellt, die die Vorteile des Cloud-Computing mit dem Wissen aller Panda-Nutzer kombiniert. Wird irgendwo auf der Welt ein neues Schadprogramm entdeckt, kann Panda alle seine Nutzer durch diesen „Collective Intelligence“-Ansatz in kürzester Zeit schützen. Panda Security entwickelt und vertreibt leistungsfähige Consumer- wie auch Enterprise-Lösungen. In Deutschland und Österreich leitet die PAV Germany GmbH das Panda-Geschäft und bietet Unternehmenskunden kostenfreien 24/7/365-Support auf Deutsch durch die eigenen Techniker. Den Vertrieb organisiert Panda Security durch Channel-Partner. Mit 61 Niederlassungen weltweit und einem Kundenstamm aus fast 200 Ländern hat sich Panda Security eine globale Präsenz geschaffen.

News-ID: 783162 • Views: 120 (Stand: 25.07.2026)

Link zur Pressemitteilung:

https://www.openpr.de/news/783162/Der-Fall-PowerLocker-Analyse-einer-Ransomware.html