



c't - Magazin für Computertechnik, 07/2016, S. 86

Trojaner auf Raubzug

Verschlüsselungs-Malware analysiert

Bei Verschlüsselungs-Trojanern handelt es sich in aller Regel um recht einfach gestricktes Teufelszeug. Wir haben uns TeslaCrypt, den Trun-Trojaner und Locky etwas genauer angesehen.

Das Herzstück der Erpressungs-Trojaner ist die Verschlüsselung. Viele behaupten, die Daten mit RSA mit mindestens 2048 oder 4096 Bit zu verschlüsseln. Das soll wohl die Opfer beeindrucken, ist aber Blödsinn. RSA wird eigentlich nie für das Verschlüsseln nennenswerter Datenmengen verwendet - das Verfahren arbeitet dafür viel zu langsam.

Manche Ransomware benutzt zwar RSA. Sie verschlüsselt aber damit lediglich die nur wenige Byte langen Schlüssel - reguläre Verschlüsselungsprogramme machen das übrigens auch so. Die Verschlüsselung der eigentlichen Daten erfolgt immer mit einem schnellen, symmetrischen Verfahren wie AES. Das ist schon mit 128 Bit nicht zu knacken; bei den oft eingesetzten 256-Bit-Schlüsseln ist ein solcher Versuch völlig aussichtslos. Das bedeutet konkret: Ohne den AES-Schlüssel gibt es keinen Zugang zu den Daten.

Dieser AES-Schlüssel steht typischerweise im Kopf der verschlüsselten Dateien - ist dort aber seinerseits durch Verschlüsselung vor dem Zugriff gesichert. An diesem Punkt haben die Entwickler von TeslaCrypt geschlampt. Statt auf bewährte Verfahren wie RSA zu setzen, haben sie etwas Eigenes zusammengepfuscht. Das führt dazu, dass im Kopf einer TeslaCrypt2-typischen .vvv-Datei das Produkt zweier Schlüssel steht - von denen einer der benötigte AES-Schlüssel ist. Da es sich bei beiden Schlüsseln um 256-Bit-Zahlen handelt, muss man lediglich eine 512-Bit-Zahl faktorisieren und die Faktoren danach wieder richtig zusammensetzen, um den benötigten AES-Schlüssel zu errechnen.

Das kann im Extremfall einige Tage dauern, oft aber auch nur wenige Minuten, weil es viele kleine Prim-Faktoren gibt, die schnell gefunden werden. Allerdings zöge sich der Vorgang trotzdem unangenehm in die Länge, wenn man ein paar tausend Dateien entschlüsseln muss. Da kommt den Opfern ein zweiter Bock zugute, den die TeslaCrypt-Entwickler geschossen haben: Der Trojaner würfelt beim Start zwar einen zufälligen AES-Schlüssel aus, verwendet diesen aber für alle Dateien. Nur wenn der Trojaner etwa durch einen Neustart unterbrochen wird, kommt ein neuer Schlüssel zum Einsatz. Im Normalfall kann man also alle Dateien mit dem einmal errechneten AES-Schlüssel dekodieren; ansonsten ist noch eine zweite Faktorisierung nötig.

Mit GPG verschlüsselt

Der weniger bekannte Trun-Trojaner arbeitet sorgfältiger und setzt das Open-Source-Tool GnuPG ein, um Dateien zu verschlüsseln. Dazu holt er sich von einem Server das Original-Programm gpg.exe und erzeugt damit im Batch-Modus auf dem infizierten Rechner ein neues PGP-Schlüsselpaar für einen Benutzer namens "Cellar". Dessen geheimen Schlüssel exportiert er aus dem GPG-Schlüsselbund und verschlüsselt ihn dann.

```
echo Key-Type: RSA > vrbom6q1.jt0bpfga echo Key-Length: 1024 >> vrbom6q1.jt0bpfga echo Name-Real: Cellar >>
vrbom6q1.jt0bpfga gpg.exe --batch --gen-key vrbom6q1.jt0bpfga gpg.exe -r Cellar --export-secret-keys ... gpg.exe -r kkkkk ...
-o trun.KEY
```

Die Verschlüsselung richtet sich an einen Benutzer mit den Pseudonym "kkkkk", dessen öffentlichen PGP-Schlüssel der Trun-Trojaner bereits mitbringt. Anschließend löscht der Trojaner den geheimen Cellar-Schlüssel und macht sich ans Werk: Er verschlüsselt alle möglichen Dateien mit dem öffentlichen Cellar-Key.

Die Schlüssel-Datei trun.KEY verbleibt zwar auf dem infizierten System; sie lässt sich aber nicht knacken. Gemäß Anleitung sendet sie ein zahlungswilliges Opfer an den Erpresser, der sie mit seinem geheimen kkkkk-Schlüssel dechiffrieren kann. Das liefert den geheimen Cellar-Schlüssel für ein Entschlüsselungs-Skript, das er nach Eingang des Lösegeldes zurückschickt.

Auch GPG arbeitet beim Verschlüsseln von Daten mit einem symmetrischen Verfahren. Standardmäßig kommt CAST5 zum Einsatz, das ebenso wenig zu knacken ist wie AES. Nur der für jeden Verschlüsselungsvorgang zufällig ausgewürfelte CAST5-Schlüssel wird mit RSA verschlüsselt.

Knacken lässt sich die Verschlüsselung des Trun-Trojaners somit nicht. Einziger Schwachpunkt ist der lokal auf dem System des Opfers erzeugte geheime Cellar-Schlüssel. Ihn löscht der Trojaner zwar, aber mit etwas Glück findet man bei einer forensischen Analyse der Festplatte noch Spuren davon.

Locky auf die Finger geschaut Wie es aussieht, wenn sich Profis der Sache annehmen, demonstriert Locky mit erschreckender Perfektion. Der Krypto-Trojaner ist derzeit einer der erfolgreichsten und gefährlichsten Vertreter seiner Gattung. Zeitweise hat er über 5000 Rechner pro Stunde verschlüsselt - allein in Deutschland. Soweit bisher bekannt, gibt sich die vermutlich von der Dridex-Gang geschriebene Ransomware keine Blöße.

Nach dem Start nimmt der Krypto-Trojaner sofort Kontakt mit einem Command-and-Control-Server (C&C) auf - natürlich verschlüsselt. Dabei übermittelt er eine 16-stellige GUID, die von der einzigartigen Volume-ID der Windows-Platte abgeleitet wird. Über diese GUID verwalten die Täter ihre Opfer. Der HTTP-Post-Request an main.php enthält unter anderem den Parameter act=getkey, über den Locky einen individuellen RSA-Schlüssel (Public Key) für die Verschlüsselung anfordert. Der für die Entschlüsselung benötigte geheime Schlüssel verbleibt auf dem C&C-Server - außer Reichweite der Opfer.

Auch Locky verschlüsselt die Dateien nicht mit dem 2048 Bit langen RSA-Schlüssel, sondern lediglich mit AES-Schlüssel. Doch anders als TeslaCrypt erzeugt Locky für jede Datei einen neuen, zufälligen AES-Schlüssel.

Dabei nimmt der Schädling alles ins Visier, was Anwendern lieb und teuer ist: Bilder, Musik, Videos, Dokumente, Datenbanken, Programm-Code - selbst Zertifikate, PGP-Schlüssel und Bitcoin-Wallets bleiben nicht verschont. Der Name der verschlüsselten Dateien beginnt mit der 16-stelligen Opfer-ID und endet auf .locky. Bislang zeichnet sich kein Weg ab, wie man diese Dateien ohne die Hilfe der Erpresser wieder dechiffrieren könnte.

Verbreitet wird Locky vor allem über Mails, denen ein Zip-Archiv anhängt. Darin befindet sich entweder ein Office-Dokument mit Makro-Code oder ein wenige KByte großes Skript (zum Beispiel mit der Endung .js), das vom Windows Script Host ausgeführt wird. Der Zweck der Anhänge ist identisch: Es handelt sich um sogenannte Dropper, die per HTTP die aktuelle Version des Krypto-Trojaners herunterladen und ausführen - meist von irgendeinem gehackten Server.

Eine von uns untersuchte Locky-Payload hieß bba3e983& eec12a4.exe und war etwa 186 KByte groß. Sie landete im Temp-Ordner von Windows; das kann sich aber ebenso wie der Verbreitungsweg bei künftigen Versionen ändern. Das Programm enthält einige fest einprogrammierte C&C-Server-Adressen.

Für Backup sorgt ein sogenannter Domain Generation Algorithmus, der abhängig vom aktuellen Datum die Domain eines C&C-Servers errechnet. Die Locky-Hintermänner registrieren diese Domains zeitnah, um die Informationen der infizierten Rechner einzusammeln und Schlüssel auszuliefern. Ist keiner der Server erreichbar, schlägt Locky mangels Krypto-Schlüssel auch nicht zu und löscht sich klammheimlich. Solche DGAs für C&C-Server kommen übrigens bei Bot-Netzen schon länger zum Einsatz.

Im Rahmen der Kommunikation mit dem C&C informiert Locky seinen Herrn und Meister über die installierte Windows-Version, ob es sich um ein 64-Bit-System handelt und welche Systemsprache eingestellt ist. Über die Action "gettext" fragt der Schädling die aktuelle Erpresser-Botschaft in der passenden Sprache ab, über die Action "stats" übermittelt er zudem Informationen über die verschlüsselten Dateien.

Der Erpressungs-Trojaner hinterlässt in der Registry unter HKEY_CURRENT_USER\SOFTWARE\Locky die Opfer-ID ("id"), die Erpresser-Botschaft ("paytext"), den eingesetzten RSA-Key ("pubkey") und die Informationen, ob die Verschlüsselung erfolgreich vollzogen wurde ("completed").

Locky verschlüsselt nicht nur Dateien auf Platten, USB-Speicher, RAM-Disks und eingebundenen Netzwerk-Laufwerken. Er macht sich auch im Netz auf die Suche nach erreichbaren Netzwerk-Freigaben. Wird er dabei fündig, bindet er das Laufwerk ein, um dort mit seinem zerstörerischen Tun fortzufahren. Wenn ein Netz-Admin also allzu freizügig Freigaben eingerichtet hat und für den einfachen Datenaustausch kurzerhand auf allen Systemen komplette Laufwerke exportiert, rächt sich das bei einer Locky-Infektion bitter.

Doppelt und dreifach Eine Locky-Infektion kann man kaum übersehen. Nicht nur legt der Schädling in jedem Ordner eine Datei namens _Locky_recover_instructions.txt ab, die in der Systemsprache informiert, wie das Opfer den zur Entschlüsselung der .locky-Dateien nötigen Decryptor kaufen kann. Um sicherzustellen, dass das Opfer diese Kaufempfehlung auch nicht übersieht, speichert Locky die Textdatei auch auf dem Desktop und öffnet sie mit dem Editor.

Damit nicht genug, generiert der Trojaner aus dem abgerufenen Erpressertext dynamisch noch eine Bitmap namens _Locky_recover_instructions.bmp, die ebenfalls geöffnet und sogar als Desktop-Hintergrund gesetzt wird. Nach getaner Arbeit löscht sich Locky dann selbstständig.

Der Decryptor kostet in der Regel ein halbes Bitcoin, was umgerechnet rund 190 Euro entspricht. Das Opfer muss ihn bei einem Hidden Service im Tor-Netz erwerben, dessen Adresse die Erpresser-Botschaft nennt. Das dient nicht etwa der Sicherheit des Opfers, sondern der Erpresser: Durch das zwischengeschaltete Anonymisierungs-Netz lassen sich deren Systeme nicht lokalisieren.


Der mit etwas Glück zurückgelieferte Decryptor bringt den geheimen RSA-Schlüssel mit, der zu dem von Locky abgerufenen Public Key passt. Das Tool funktioniert somit nur auf dem Rechner des Opfers, das bezahlt hat. Es handelt sich um ein unspektakuläres Kommandozeilen-Tool, das sich - wie zuvor Locky - durch Datenträger und Freigaben frisst, um die Verschlüsselung wieder umzukehren. (ju@ct.de)

Ronald Eikenberg, Jürgen Schmidt

Quelle:	c't - Magazin für Computertechnik, 07/2016, S. 86
ISSN:	0724-8679
Dokumentnummer:	20160319160319103

Dauerhafte Adresse des Dokuments: https://www.wiso-net.de/document/PMGC__20160319160319103

Alle Rechte vorbehalten: (c) Heise Zeitschriften Verlag GmbH & Co KG

 © GBI-Genios Deutsche Wirtschaftsdatenbank GmbH