Dennis Schirrmacher

Erpressungs-Trojaner

Geschäftsmodell: Ihre Daten als Geisel

Verschlüsselungs-Trojaner sind in der Malware-Szene der letzte Schrei: Das legen die in den letzten Monaten rasant angestiegenen Infektionsraten nahe. Offensichtlich geht das Konzept der Erpresser auf: Viele Opfer zahlen die geforderten Beträge, um ihre Dateien zurückzubekommen. Online-Schwarzmärkte bieten Bausätze für technisch unbedarfte Kriminelle an, mit denen sie direkt zum Angriff übergehen können.

Erpressungs-Trojaner

Geschäftsmodell Erpressung	Seite 76
Schützen und vorbeugen	Seite 78
Erste Hilfe	Seite 82
Hinter den Kulissen	Seite 86

© Copyright by Heise Medien
Persönliches PDF für alle Leser der c't aus 30625 Hannover

Der erste dokumentierte Verschlüsselungs-Trojaner namens AIDS tauchte im Jahr 1989 auf und infizierte Computer über eine präparierte Diskette. Der Schädling verschlüsselte nach dem neunzigsten Bootvorgang alle Daten auf der Systemfestplatte und machte den Computer damit unbenutzbar. Opfer wurden aufgefordert, rund 170 Euro an ein Postschließfach in Panama zu schicken. An diesem Konzept haben sich seitdem nur Kleinigkeiten geändert: Aus dem Postfach sind Bitcoins geworden und durch stetige Weiterentwicklung wird jede Malware-Generation heimtückischer als ihre Vorgängerin.

Ransomware-Gauner haben es in erster Linie auf Windows-Nutzer abgesehen. Mit KeRanger ist vor kurzem aber auch der erste Erpressungs-Trojaner für Apples Betriebssystem OS X aufgetaucht. Im Vergleich zu den Millionen Opfern im Windows-Bereich sind die 6500 KeRanger-Infektionen jedoch bestenfalls ein Versuchsballon.

Das Jahr der Krypto-Trojaner

2015 waren laut einer Studie von iSense Solutions 13,1 Millionen US-Amerikaner und 3,1 Millionen Deutsche von Krypto-Trojanern betroffen. Das war noch vor der Locky-Welle. Eset zufolge lässt sich für 2016 bereits abschätzen, dass es im Februar einen Peak in der Verbreitung von Ransomware gab. Dieser Anstieg übertrifft alle Spitzen in 2015 deutlich. Auch Avira bestätigt das. Kaspersky berichtet, dass die Angriffsversuche in Deutschland im Vergleich zu 2015 um den Faktor 2,6 gestiegen sind; global liegt die Erhöhung bei Faktor 1,5. Diese Einschätzungen stützt auch Google Trends: Gibt man dort die Suchbegriffe Cryptowall, Locky und TeslaCrypt ein, sieht man seit Ende 2015 einen deutlichen Anstieg. Anfang Februar explodierten die Zahlen insbesondere durch Locky. Seit diesem Zeitpunkt treten auch vermehrt betroffene Leser mit c't in Kontakt.

Krypto-Trojaner agieren äußerst heimtückisch: TeslaCrypt & Co. verschlüsseln neben Foto- und Musiksammlungen auch Word- und PDF-Dokumente. CryptoLocker nimmt rund 70 verschiedene Dateitypen zur Geisel. Verschlüsselte Dateien sind anschließend mit einer weiteren Endung versehen, etwa „Urlaub2016.jpg.vvv“, und lassen sich nicht mehr öffnen. Den Schlüssel zum Dechiffrieren der Daten rücken die Erpresser nur gegen Lösegeld raus. Damit die Opfer auch glauben, dass es einen Weg zurück gibt, bieten Kriminelle häufig eine Test-Entschlüsselung ausgewählter Dateien an.

Wenn die Gauner keine Fehler bei der Verschlüsselung gemacht haben, würde sich selbst ein Super-Computer der NSA die Zähne an der Chiffrierung ausbeißen: Die persönlichen Daten sind vorerst verloren.

Neben Privatpersonen geraten auch Firmen und öffentliche Einrichtungen in das Fadenkreuz von Ransomware-Banden. In Deutschland waren Anfang dieses Jahres mehrere Krankenhäuser betroffen, deren Betrieb durch digitale Infektionen eingeschränkt wurde. Die Höhe der geforderten Beträge variiert, von Privatpersonen wird meist ein Bitcoin (rund 350 Euro) eingefordert. Ein Krankenhaus in Los Angeles sah sich gezwungen, 40 Bitcoins (rund 15 000 Euro) Lösegeld zu zahlen. Eine Zahlung garantiert aber nicht, dass die Gauner auch tatsächlich die Schlüssel rausrücken. Im Fall des Krankenhauses in Los Angeles waren die Daten nach der Zahlung aber wieder lesbar, teilte der Klinik-Chef mit.

Millionen-Geschäft

Selbst das FBI empfiehlt Opfern zu zahlen. Der Ermittlungsbehörde zufolge waren Bemühungen, die Verschlüsselung aufzubrechen, nicht von Erfolg gekrönt. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) rät Opfern hingegen ab, sich auf die Forderungen einzulassen: In vielen Fällen bekämen Betroffene trotz Zahlung des Lösegelds keinen Zugriff mehr auf ihre Daten. Geschädigte sollen Infektionen zur Anzeige bringen, empfiehlt das BSI.

Analysten von Cisco gehen davon aus, dass die Gauner hinter dem Angler-Exploit-Kit jährlich einen hohen zweistelligen Millionenbetrag erwirtschaften – es ist eines der Mittel, Erpressungs-Trojaner auszuliefern. Das FBI gibt an, dass die Bande um den Erpressungs-Trojaner Cryptowall und seine Varianten 2015 allein in den USA rund 318 Millionen Euro erpresst habe. Die USA sind das Hauptziel der Ransomware-Banden, wie Statistiken von verschiedenen Anbietern von Antiviren-Anwendungen nahelegen.

Im Zuge der iSense-Studie vom November 2015 wurden weltweit 3009 Internetnutzer befragt. Davon haben 50 Prozent der mit Ransomware infizierten US-Amerikaner schon Lösegeld bezahlt; 40 Prozent würden bezahlen, wenn sie betroffen sind. In Deutschland haben 33 Prozent gezahlt; 36 Prozent wären dazu bereit. In den USA sind Betroffene im Mittel gewillt, maximal rund 320 Euro zu zahlen; hierzulande liegt die Schmerzgrenze bei knapp über 200 Euro. Symantec berichtet, dass Deutschland 2015 unter den Ransomware-Zahlen hinter den USA den zweiten Platz belegt.

Das lohnende Geschäft bewegt auch einige weltweit im großen Stil operierende Kriminelle umzuschwenken. So steckt laut BSI hinter Locky die bisher auf Banking-Trojaner spezialisierte Dridex-Bande. Offensichtlich wirft Ransomware mit weniger Aufwand mehr Gewinn ab.

Entwickler von Verschlüsselungs-Trojanern bieten ihre Schädlinge auch als Dienstleistung an: Auf im Tor-Netz versteckten Malware-Marktplätzen kann jeder halbwegs kompetente Kriminelle einen maßgeschneiderten Verschlüsselungs-Trojaner kaufen und nach wenigen Klicks loslegen. Neben dem Schädling kann man die komplette Infrastruktur buchen, um eine Ransomware-Kampagne zu starten. Die Nutzung der Command-and-Control-Server (C&C) zum Steuern der Erpresser-Kampagne gehört mit zum Service.

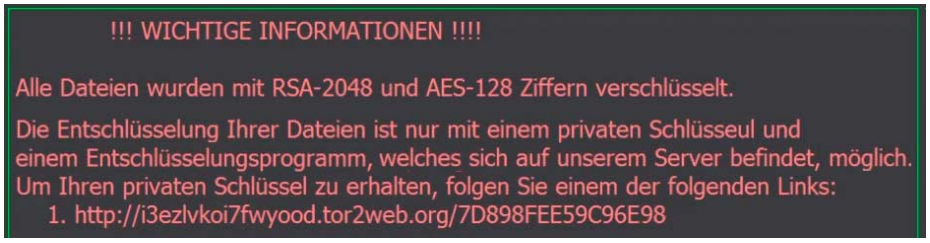
Das All-in-one-Paket GinX ist umgerechnet für 450 Euro zu haben. Die Gewinnbeteiligung für Anbieter und Käufer beträgt dabei 50/50. Möchte man mehr Geld einstreichen, fallen bei einem Verhältnis von 30/70 einmalig 1360 Euro an. GinX soll nach dem Kauf „out of the box“ funktionieren und selbst für Computer-Laien einfach nutzbar sein, versichert der Anbieter.

Verbreitung inklusive

Einige Verkäufer gehen noch weiter und bieten unterschiedliche Verbreitungswege mit an. So können Kriminelle etwa Spam-Mails oder Exploit-Kits dazuzukaufen, die den Krypto-Trojaner an die Opfer ausliefern.

Auch der berüchtigte Erpressungs-Trojaner CryptoLocker ist im Online-Schwarzmarkt erhältlich. Der Schädling kostet rund 180 Euro. Der vergleichsweise günstige Preis rührt daher, dass der Verkäufer nur die Ransomware und ein PHP-Skript anbietet, das die Schlüssel an einen Webserver sendet: Die Infrastruktur müssen Käufer also selbst stellen. Auf Anfrage verspricht der Anbieter sogar Zugriff auf den Source Code seines Trojaners. Bitdefender zufolge kostet CryptoLocker inklusive Quelltext rund 2700 Euro.

Alle Zeichen stehen also auf Sturm: Bis auf Weiteres haben sich Verschlüsselungs-Trojaner fest im Computer-Alltag eingenistet. Die Welt geht davon aber nicht unter. Wenige Schritte reichen, um seinen PC effektiv zu schützen. Wen es doch erwischt, der muss sich von seinen Daten nicht endgültig verabschieden. Es gibt Situationen, in denen man ohne Lösegeld zu zahlen wieder Zugriff auf seine Fotos und Dokumente erhält. Den effektiven Schutz- und Vorbeugungsmaßnahmen und der ersten Hilfe für Betroffene haben wir jeweils einzelne Artikel gewidmet. Den Abschluss macht ein Blick hinter die Kulissen mehrerer Verschlüsselungs-Trojaners und wie diese ticken. (des@ct.de) c't



Die Locky-Botschaft ist eindeutig: Die Daten sind unter Verschluss.

© Copyright by Heise Medien
Persönliches PDF für alle Leser der c't aus 30625 Hannover