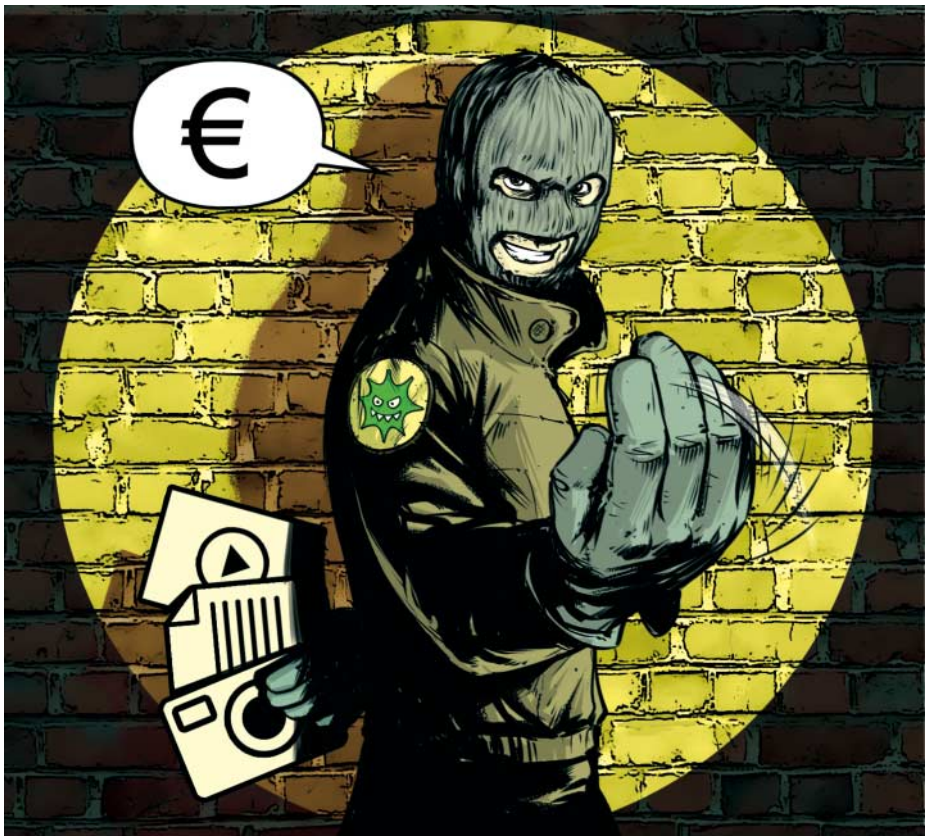

Bild: Albert Hulm

Erpressung macht sich breit

Ransomware mit neuen Tricks und Techniken

Das Jahr 2017 brachte einige entscheidende Neuerungen bei Erpressungstrojanern. WannaCry, Petya/NotPetya & Co. setzten beispielsweise auf neue Verbreitungswege und hatten zum Teil weitere Schädlinge im Gepäck. Insbesondere Firmen und Behörden stehen stärker im Fokus der Kriminellen als je zuvor.

Von Jürgen Schmidt

Die Erpressung mit verschlüsselten Daten hat sich seit 2016 als einer der profitabelsten Geschäftsbereiche der Malware-Szene etabliert. Kein Wunder: Anders als etwa beim Online-Banking-Betrug sind sowohl die technischen als auch die organisatorischen Anforderungen so niedrig, dass auch minderbegabte Kleinkriminelle auf den Zug aufspringen können: Software, die Dateien verschlüsselt, und ein Bitcoin-Konto sind kein Hexenwerk – und außerdem im Rahmen von Angeboten zu „Ransomware as a Service“ bereits im Paket mit dabei.

Doch 2017 hat sich einiges getan. Die wohl größte Neuerung ist die Form der Verbreitung: Klassiker wie Locky & Co. landen primär über E-Mails bei den potenziellen Opfern; sogenannte Drive-by-Infektionen durch Webseiten mit Schadcode sind der zweite wichtige Weg, auf dem Ransomware Systeme der Opfer infiziert. WannaCry jedoch nutzte im Mai erstmals eine Windows-Lücke aus dem NSA-Arsenal (EternalBlue), um sich wie ein Wurm selbsttätig im Netz weiter zu verbreiten. Die Infektion erfolgte völlig ohne Zutun der Anwender. Noch hinterhältiger war NotPetya, der heimlich über den Update-Mechanismus einer legitimen Software auf das System kam. Von dort aus verbreitete er sich ebenfalls über die EternalBlue-Lücke im Windows SMB-Stack weiter. Doch diese beiden Formen der Verbreitung werden wohl die Ausnahme bleiben. Wurm-taugliche Sicherheitslücken in PCs sind sehr selten und Malware über reguläre Updates einzuschleusen lässt sich ebenfalls nicht beliebig wiederholen.

Erpressung und Spionage

Allerdings sehen Malware-Analysten mittlerweile vermehrt Angriffe auf Firmen, die primär das Ziel haben, dort Erpressungstrojaner zu platzieren. Das sind dann beispielsweise angebliche Bewerbungen, die sich auf tatsächliche Stellenanzeigen der Firma beziehen und an die Personalabteilung adressiert sind. Nachdem der Rechner des Personalers infiziert wurde, breiten sich die Angreifer von dort aus weiter im Netz aus, suchen und übernehmen Systeme mit wichtigen Daten und verschlüsseln Dateien dann sehr koordiniert überall gleichzeitig. Ein weiteres, aktiv genutztes Einfallstor sind Remote-Desktop-Dienste (RDP). Die Crysis-Gang sucht in großem Stil erreichbare RDP-Ports und versucht deren Zugangsschutz mit einfachen Passwörtern auszuhebeln. Haben sie damit Erfolg, laden sie die Crysis-Ransomware herunter und infizieren das System.

Ransomware-Angriffe auf Firmen ähneln in der Vorgehensweise und den eingesetzten Tools immer häufiger professionellen Spionage-Angriffen. In manchen Fällen sind sich die Forensiker, die die Vorfälle untersucht haben, sogar recht sicher, dass es den Angreifern eigentlich um Spionage ging. Die vorgefundene Ransomware war nur ein kleines „Abschiedsgeschenk“, das zwei Fliegen mit einer Klappe schlagen sollte: Zum einen vernichtet man damit Spuren und zum anderen ergibt sich ja vielleicht auch noch eine nette Nebeneinkunft.

Pay per Install

Außerdem bandeln die Ransomware-Autoren offensichtlich mit der etablierten Crimeware-Szene an. So erklärte uns Holger Unterbrink von Ciscos Threat-Research-Abteilung Talos, dass er bereits mehrfach Fälle gesehen habe, in denen

die Opfer nach einer Bezahlung zwar den Schlüssel für den Zugang zu ihren Daten erhielten und ihre Daten auch zurück bekamen – sich aber weitere Schadsoftware auf dem System befand. Da hatte dann etwa ein Exploit Kit auf einer Website im Kombi-Pack mit dem Erpressungstrojaner einen Bitcoin-Miner geliefert, der dann natürlich nach der Datenwiederherstellung munter weiter schürfte.

Es ist durchaus üblich, dass Malware auf Befehl ihres Herrn und Meisters auch nachträglich noch andere Schadprogramme installiert. Da lädt dann etwa der Online-Banking-Trojaner nach getaner Arbeit noch Locky oder eine andere Erpressungssoftware nach. „Pay per Install“ nennt sich dieses ursprünglich aus der Freeware-Szene stammende Geschäftsmodell, das sich auch in der Malware-Community durchgesetzt hat. Wer eine große Zahl an Installationen vorweisen kann – also entweder beliebte Freeware vertreibt oder große Bot-Netze administriert –, hilft dabei Dritten gegen kleine Provision bei der Verbreitung ihrer Software.

Bröckelndes Image

Insgesamt hat die Ransomware-Szene sehr bewusst an dem Ruf gearbeitet, dass man nach dem Bezahlen des Lösegelds auch eine realistische Chance hat, wieder an seine Daten zu kommen. Die Jigsaw-Gang bot bei Problemen sogar einen Chat als Hotline-Service an. Das zahlt sich aus.

Auch wenn etwa das BSI nicht müde wird, vor den Risiken zu warnen, ringen sich vor allem Firmen und auch Behörden mittlerweile regelmäßig dazu durch, der Erpressung nachzugeben und die geforderte Summe zu entrichten. Symantec ermittelte, dass in den USA rund 64 Prozent der Betroffenen das Lösegeld entrichten; für Deutschland konnten wir keine konkreten Zahlen finden, aber Insider schätzen, dass auch hier über die Hälfte der Firmen bezahlt.

Diese Zahlungsbereitschaft steht und fällt mit der Zuversicht, dass man eine reelle Chance hat, seine Daten zurückzubekommen. Und wenn man ehrlich ist, stimmt das in den meisten Fällen auch. Allerdings zeigt dieses Bild erste Risse. So gibt es immer mehr Erpresser, deren Software die technischen Voraussetzungen für eine Wiederherstellung gar nicht an Bord hat. Malware-Experten sprechen dann von Wipern, weil die Schadsoftware die Daten praktisch löscht. Der bislang prominenteste Wiper war NotPetya/Petya/Netya – je nach Namensgeber. Der überschrieb Daten des Boot-Sektors unwiederbringlich und machte sich nicht einmal die Mühe, eindeutige IDs für seine Opfer zu erstellen. Selbst wenn sie es wollten, könnten die Kriminellen einem Opfer keinen Schlüssel zu dessen Daten liefern. Nach aktuellem Kenntnisstand hat auch wirklich kein einziges NotPetya-Opfer seine Daten zurückbekommen. Bei NotPetya handelte es sich vermutlich um eine politisch motivierte Kampagne, bei der Erpressung nur als Kulisse diente. Doch dessen Vorgehen ahmen immer mehr Gauner nach, denen es vor allem um die schnelle Bitcoin geht, erklärt Unterbrink gegenüber c’t. Sie sparen sich den ganzen Aufwand mit den Schlüsseln, kassieren ab und tauchen dann wieder unter. Dass sie damit das Image der Branche ruinieren und irgendwann darunter die Zahlungsmoral leiden wird, ist ihnen dabei egal.

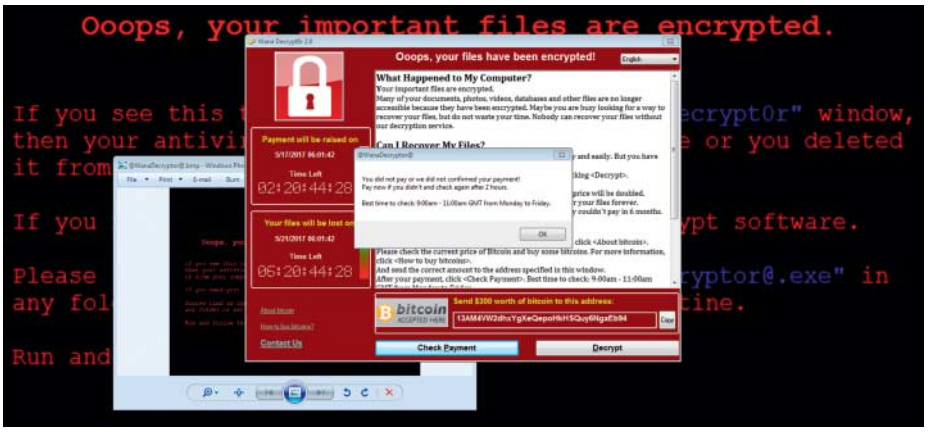

Bild: Checkpoint

WannaCry war der erste Erpressungstrojaner, der sich in Netzwerken wurmartig weiter verbreitete.

Es ist schwer, die Schäden durch Ransomware zu beziffern. Klar ist, dass es sich für die Cyber-Kriminellen um ein äußerst lukratives Millionengeschäft handelt. Für die Opfer liegt der Schaden durch die von der Ransomware verursachten Verluste noch um ein vielfaches höher. Der deutsche Konzern Beiersdorf schätzt die eigenen NotPetya-Verluste durch Verzögerungen bei Versand und Produktion auf etwa 35 Millionen Euro; andere Firmen meldeten ähnliche Zahlen. Allein WannaCry und NotPetya verursachten somit Schäden im Milliardenbereich.

Zusammenfassend kann man feststellen, dass Ransomware zur beliebtesten Schädlingsgattung der Cyber-Kriminellen avanciert ist. Der Fokus der Angriffe hat sich ein wenig auf den Firmenbereich verschoben, weil dort angesichts des drohenden materiellen Schadens die Zahlungsbereitschaft größer ist als bei Privatpersonen. Außerdem kann man bei Firmen mit höheren Lösegeldforderungen weit über 1000 Euro operieren. Für Firmen ist Ransomware somit die derzeit größte Bedrohung für ihre Daten. Doch auch für Endanwender gibt es keineswegs Entwarnung: Die Macher von Locky, Cerber & Co. werden auch 2018 wieder auf Sie losgehen.

Was tun?

Wenn es Sie erwischt hat, sollten Sie keinesfalls einfach zahlen. Erstatten Sie Anzeige und versuchen Sie auf jeden Fall zunächst, mehr über die Malware herauszufinden. Dienste wie ID Ransomware (siehe ct.de/yzh4) helfen dabei, den Typ des Erpressungstrojaners zu identifizieren. Trauen Sie sich das nicht selbst zu, ziehen Sie Spezialisten zu Rate.

Bei einem bekannten Wiper ist der Fall hoffnungslos – das Geld wäre verschwendet. Auch nach einer Bezahlung bekommen Sie Ihre Daten nicht zurück. Bei manchen Erpressungstrojanern wurde die Verschlüsselung geknackt, sodass sich die Daten auch ohne Bezahlung wiederherstellen lassen. Die Macher von Crysis haben auch bereits mehrfach Master-Keys für ihre Software veröffentlicht. Warum, ist nach wie vor unklar. Vielleicht ging es einfach nur darum, den Kunden ein kostenpflichtiges Update der Mietsoftware aufzuzwingen. Jedenfalls kann man mit dem Master-Key ebenfalls ohne Lösegeld an die Daten kommen. Erst als allerletzte Option sollten Sie eine Bezahlung ins Auge fassen. *(des@ct.de)* c't

Ransomware identifizieren: ct.de/yzh4