WINTERSEMESTER 2017/2018

SEMINAR IT-SICHERHEIT

Ransomware

Eingereicht von:
Sebastian Krumm
Student Wirtschaftsinformatik
E-Mail: winf100037@fh-wedel.de

Betreuer:
Prof. Dr. Gerd Beuster

Datum: 31.03.2018

INHALTSVERZEICHNIS

Einleitung

Diese Arbeit behandelt das Thema „Ransomware“. Zunächst gehe ich allgemein auf das Thema ein und stelle eine Übersicht über die Entwicklung von und die aktuelle Bedrohungslage durch Ransomware dar. Ergänzend soll auf einige Gründe für die Infizierung von Computersystemen durch diese Form von Schadsoftware aufmerksam gemacht werden. Anschließend werden empfohlene Schutz- und Detektionsmaßnahmen aufgezeigt. Im späteren Abschnitt dieser Arbeit wird, bezogen auf Ransomware, speziell das Internet der Dinge in den Fokus rücken. Hier möchte ich das aktuelle und für die nächsten Jahre mögliche Potential für Angriffe durch Ransomware untersuchen und den Leser im Hinblick auf diese Bedrohung sensibilisieren.

Motivation

Ransomware ist für an Computersystemen und an der IT Interessierte oder in dieser Branche Beschäftigte schon lange kein Neuland mehr. Doch die rasante Entwicklung in diesem Bereich führte dazu, dass dieses Thema in der Vergangenheit immer populärer wurde, wodurch inzwischen auch allen fachfremden Personen dies zumindest ein Begriff ist. Leider ist bei dieser Bedrohung kein Ende in Sicht. Die Realität zeigt, dass Ransomware aktuell und in nächster Zeit ein für Privatperson und Unternehmen gleichermaßen ernstzunehmendes Thema ist und bleibt. Daneben ist das Internet der Dinge mit all seinen Möglichkeiten, verschiedene Geräte miteinander zu vernetzen und untereinander kommunizieren zu lassen, ein sehr populäres Thema und gewinnt in unserem Alltag immer mehr an Bedeutung. Es sollte uns bewusst sein, dass diese Plattform auch für Entwickler und Anbieter von Ransomware sehr interessant ist und bedeutsamer werden kann.

Ransomware

Ransomware ist eine Form von Malware, also Schadprogrammen, die dazu benutzt wird, fremde Systeme zu infizieren, um Leidensdruck auf dessen Besitzer auszuüben und Lösegeld zu erpressen. Ransomware lässt sich hinsichtlich der Funktionsweise im Infektionsfall in verschiedene Typen unterteilen.

Ransomware-Typen

In *Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks* [1], werden im Wesentlichen drei Typen von Ransomware unterschieden: Jene, die Dateien verschlüsseln, jene, die Dateien löschen und jene, die den Zugang zu Dateien oder dem System sperren.

Sperren

In diesem Fall erstellen die Angreifer typischerweise einen Login-Bildschirm, der dem Benutzer nach dem Starten des Systems angezeigt wird. Dieses Login-Fenster ist so aufgemacht, als stamme es von einer staatlichen Behörde, beispielsweise der Polizei oder dem FBI. Man wird gewarnt, dass man urheberrechtlich geschützte Dateien oder anderes, strafbares Material auf dem System gespeichert hat. Der Zugang zum System oder den gefragten Dateien wird blockiert, ehe man nicht eine Zahlung tätigt. Die dafür nötigen Zahlungsinformationen sind, wie auch bei den Meldungen und Warnungen der anderen Ransomware-Typen, meist direkt in das Fenster eingebettet oder über einen darin angezeigten Link zu erreichen. Dieser Typ ist zu heutigem Stand aber der aus Sicht des Opfers ungefährlichste und aus Sicht des Angreifers der am wenigsten Vielversprechendste. Eine simple Neuinstallation des Systems verschafft Abhilfe und ermöglicht wieder den Zugriff auf das System und die Dateien. Ein bekanntes Beispiel für eine Ransomware dieses Typs ist der im Jahr 2010 entdeckte und seither sogenannte „Polizei-Virus“ *Reveton.*[2] Diese Schadsoftware zeigte eine Meldung einer angeblichen Polizeibehörde, mit der Anschuldigung, eine Straftat begangen zu haben, an und forderte die Zahlung eines Bußgelds zur Wiederherstellung des Zugangs. In diesem Fall war sogar nicht einmal eine Neuinstallation des Systems notwendig, denn durch das Starten im abgesicherten Modus und das Entfernen des verursachenden Schlüssels in der Windows-Registrierungsdatei konnte das Problem ohne Zahlung eines Lösegeldes behoben werden.

LÖSCHEN

Bei dieser Variante drohen die Ersteller damit, dass Dateien gelöscht würden, sofern nicht bis zu einer angezeigten Deadline die Zahlung eines Lösegeldes erfolgt ist. Zudem wird häufig auch darauf hingewiesen, dass bereits eigenmächtige Entschlüsselungsversuche zum unwiderruflichen Löschen der Daten führt. Als bekannte Beispiele hierfür sind *GPcode(2006)* [3] und *FileCoder(2014) [4]* zu nennen. Während man anfangs befürchten musste, dass die Dateien, im Falle einer Nichtzahlung, wirklich gelöscht sind, fand man heraus, dass die Entwickler bei der Erstellung der meisten Abkömmlinge dieser Ransomware-Variante, den einfacheren Weg gewählt haben. Statt die Dateien tatsächlich von der Festplatte zu löschen, wurden diese nur aus der NTFS Master-Datei-Tabelle gelöscht. Diese Datei entspricht sinngemäß einem Inhaltsverzeichnis des Datenträgers und enthält unter anderem Informationen über den Ablageort auf dem Datenträger. Tatsächlich waren die Dateien noch auf dem Datenträger vorhanden und eine Wiederherstellung war somit möglich. Für den Fall von *GPcode* hat damals auch Kaspersky ein Tool namens StopGPcode [3] veröffentlicht, um die Betroffenen bei der Wiederherstellung der Daten zu unterstützen. Für *FileCoder* sei an dieser Stelle noch erwähnt, dass dies die erste entdeckte Ransomware für MacOS X ist, wenngleich sie zum Zeitpunkt der Entdeckung unvollständig war. [4]

VERSCHLÜSSELN

Dies ist ohne Zweifel der wichtigste Ransomware-Typ. Für die Betroffenen am schwierigsten zu beseitigen und daher für den Angreifer sicherlich den größten Erfolg versprechend. Demzufolge kann man sich leicht vorstellen, dass sich dieser Typ durchgesetzt hat und am häufigsten zur Anwendung kommt. Bei dieser Form von Ransomware werden Dateien oder ganze Ordner verschlüsselt. Auch hier erhält man erst durch die Zahlung eines ausgewiesenen Betrags wieder Zugriff auf seine Daten. In diesem Fall erhält man nach Zahlungstätigung den Schlüssel zum Entschlüsseln der Dateien. Bezüglich dieser Ransomware-Variante ist *CryptoLocker* [5] als populäres Beispiel zu nennen. Diese im Jahr 2013 entdeckte und nicht zuletzt durch viele Medienberichte bekannt gewordene Ransomware vereint sowohl die asymmetrische als auch symmetrische Verschlüsselungsart und ist somit sehr schwer eigenständig, ohne Zahlung des Lösegeldes, zu beseitigen.

Allen Ransomware-Typen gemeinsam ist häufig die Zahlungsaufforderung an ein Bitcoin-Konto, also an einen pseudynomen Zahlungsempfänger. Außerdem sei an dieser Stelle noch erwähnt, dass die bis heute existenten, verschiedenen Ransomwares in sehr eindeutiger Mehrheit auf PC- und Computersysteme ausgerichtet sind. Also auf Systeme und Geräte, deren primärer Einsatzzweck auch die Verarbeitung von Dateien an einem Bildschirm ist. Im Unterschied dazu wird im späteren Teil dieser Arbeit auf IoT-Geräte eingegangen, deren primärer Einsatzzweck eben nicht das Verarbeiten von Dateien, sondern beispielsweise das

Öffnen eine Tür oder die Steuerung der Heizung ist. Außerdem zielt bisherige Erpressungssoftware zum erheblichen Großteil auf Systeme mit Windows als installiertem Betriebssystem ab.

ENTWICKLUNG

In diesem Abschnitt wird ein Blick auf die Historie von Ransomware geworfen. Eine umfassende, vollständige Auflistung aller bekannten Ransomwares würde den Rahmen dieser Arbeit bei weitem sprengen, allerdings sollen bestimmte Meilensteine auch hier nicht fehlen und zusammen mit einigen prägnanten Zahlen soll die Bedeutung und Aktualität dieser Bedrohung noch einmal betont werden.

Als erstes dokumentiertes Beispiel für eine Ransomware gilt der PC Cyborg, auch AIDS-Trojaner genannt, aus dem Jahr 1989. Der Evolutionsbiologe Joseph L. Popp schickte damals 20.000 infizierte Disketten mit der Beschriftung „AIDS Information – Introductory Diskettes“ an Teilnehmer der Welt-AIDS-Konferenz der Weltgesundheitsorganisation. [6] Diese Ransomware meldete dem Anwender, dass eine Lizenz abgelaufen sei und ein neuer Lizenzschlüssel erworben werden müsse. Die Zahlung des Betrags ging dann an die Firma PC Cyborg Corp. mit einem Postfach in Panama.

Als weitere bekannte Ransomwares seien aufgelistet:

- Archiveus (2006)
- GPcode (2006)
- CryptoLocker, CryptoLocker2.0 (2013)
- Locker (2013)
- Cryptorbit (2013)
- CTB-Locker (2014)
- Cryptowall (2014)
- TeslaCrypt (2015)
- Locky (2016)
- KeRanger (2016) - OS X
- Petya (2016)
- WannaCry (2017)
- Bad Rabbit (2017)

Die Jahre 2011/2012 gelten als Startschuss für den Boom von Ransomware. Seitdem, gepaart mit dem grundsätzlichen Aufschwung des Internets, kam Ransomware sehr in Mode. Diese Schadprogramme sind für die Ersteller so ein lukratives Geschäft, dass es daraus u.a. ein Dienstleistungsangebot geworden ist, welches auch als Ransomware-as-a-Service(RaaS) [7]

bekannt ist. Auch sogenannte Crimekits, mit denen im Baukastenprinzip Ransomware konstruiert werden kann, sind über Darknet-Plattformen zugänglich.

Wie eingangs in dieser Arbeit erwähnt, ist diese Entwicklung keinesfalls rückläufig, sondern eher im Gegenteil. Es ist nicht abzusehen, dass sich die Lage in den nächsten Jahren spürbar bessert. Dies zeigen auch Zahlen über die jüngste Entwicklung.

In seinem Whitepaper *„ISTR Special Report: Ransomware and Business 2016“* schreibt das Unternehmen Symantec, dass die Zahl der Infizierungen mit Ransomware im März 2016 mit ca. 120.000 ungefähr um das Doppelte der Anzahl aus dem März 2015 gestiegen ist. Dabei seien 43 Prozent der Opfer Privatanwender. Dieser Anstieg im März 2016 steht insbesondere mit dem Bekanntwerden und der Verbreitung der Locky-Ransomware im Zusammenhang. [8]

In seiner Veröffentlichung *„Ransomware – Bedrohungslage, Prävention & Reaktion“* schreibt das BSI zur aktuellen Bedrohungslage, dass, gegenüber Oktober 2015, im Februar 2016 mehr als zehn Mal so häufig Ransomware durch Virenschutzprogramme in Deutschland detektiert wurde. Auch weltweit sei die Anzahl um den Faktor 6 angestiegen. [9] Insbesondere das Jahr 2016 gilt dabei als das Jahr der Ransomware. Kaspersky Lab veröffentlichte im Juni 2016 einen Bericht zu diesem Thema, wonach die Anzahl der betroffenen Nutzer im März 2016 bei 2.315.931 lag und im Vergleich zum Vorjahr um 17,7% gestiegen ist. [10]

ANGRIFFSVEKTOREN

In den vergangenen Abschnitten wurde deutlich, wie aktuell Ransomware und deren Verbreitung ist. Der folgende Abschnitt dient dem Verständnis für und dem Bewusstsein über die Gründe der vielen und stetig wachsenden Infizierungen. Dafür soll ein Blick auf die Mittel und Wege geworfen werden, die allgemein für die Infizierung mit Schadprogrammen genutzt werden. Diese werden dann später noch einmal aufgegriffen und ergänzt, wenn es um Ransomware für das Internet der Dinge geht.

- Unaufmerksames, blindes Akzeptieren
    - Als Benutzer bekommt man im Internet häufig Einblendungen und/oder Eingabeaufforderung. Durch unaufmerksame Klicks, bspw. durch das Zustimmen einer dubiosen Virenüberprüfung, kann schnell eine Datei auf den Computer geladen werden, die genau das Gegenteil bewirkt und man hat sein System infiziert.
    - Gleiches Szenario gilt auch für in Installationsroutinen anderer Programme enthaltene Software, welche sich durch das Setzen eines Hakens im entsprechenden Kontrollkästchen de-/aktivieren lässt.
- Herunterladen infizierter Software
    - Ein gutes Beispiel hierfür ist *KeRanger.* Während die Mehrzahl an Ransomware auf Windows ausgerichtet ist, ist KeRanger eine für MacOS entwickelte Erpressersoftware. MacOS Benutzer, die die Version 2.90 des BitTorrent Clients *Transmission* installierten, erhielten drei Tage später eine Zahlungsaufforderung um ihre verschlüsselten Dateien wieder entschlüsseln zu können. [11]
- Öffnen von E-Mail Anhang
    - Dies ist ein sehr häufig angewandtes Mittel, um Ransomware auf Systeme zu laden. Häufig machen die E-Mails bzw. die Anhänge der E-Mails den Anschein, als handle es sich um eine Rechnung, eine Bewerbung oder Ähnliches. In Wahrheit verbirgt sich dahinter eine .exe oder .js Datei, die dann die Ransomware ausführt.
    - Nutzer dieses Angriffsvektors ist zum Beispiel die Cerber Ransomware. [12]
- Einlegen oder Einbinden infizierter CDs oder USB-Sticks
    - 2010 verteilte auserechnet IBM auf der AusCERT Konferenz in Sidney mit Malware infizierte USB-Sticks. Auch wenn es damals keine Malware war, ist dies sicherlich ein für Ransomware ebenso denkbares Szenario. [13]

- Anklicken unbekannter Links
    - Als Beispiel dient hier Ransomware, die sich über Twitch verbreiten kann. Twitch ist eine Plattform für Livestreaming mit enthaltener Chatfunktion, die insbesondere von Videospielern gern genutzt wird. In diesen Chats werden häufig sehr fragwürdige Links zu Seiten oder Dateien gepostet, deren Dateiendungen beispielweise .scr lauten. Aufgrund der Dateiendung könnte man annehmen, dass es sich um Screenshots handelt. In Wahrheit sind dies allerdings script-Dateien, die nach dem Download zur Ausführung kommen.
- Veraltete Software- und Systemversionen
    - Sehr eindrucksvoll wurde dies durch die WannaCry-Ransomware bewiesen. WannaCry und vor allem dessen rasante Verbreitung hätte nahezu komplett verhindert werden können, wenn jeder sein System aktuell gehalten hätte. Diese Ransomware nutzte eine zu dem Zeitpunkt bekannte Sicherheitslücke im SMB-Protokoll, die von Microsoft im März 2017 durch Sicherheits-Updates geschlossen wurde. [14] Dennoch kam es danach zu einer großen Anzahl an Infizierungen mit dieser Version von Erpressersoftware, weil viele Benutzer ihr System und ihre Software nicht aktuell halten und wie in diesem Fall, verfügbare Patches nicht installieren.
- Software-, Musik- und Videopiraterie
    - Dies ist ein sehr gebräuchlicher Weg, den Vertreiber jeglicher Art von Malware nutzen, um mit ihren Schadprogrammen eine große Reichweite zu erzielen. Während man an legalen und offiziellen Stellen davon ausgehen kann, dass die kostenpflichtigen Produkte frei von Schadcode sind, unterliegen die Inhalte, die auf solchen Portalen verfügbar sind oder die zum Herunterladen dieser Inhalte benutzten Torrent Programme, meist keinerlei Kontrollen und können somit leicht manipuliert sein. [15]
- Kein installiertes oder nicht aktuelles Antivirenprogramm
    - Nahezu identisch mit dem Punkt „Veraltete Software- und Systemversionen“
- Standardpasswörter von Administratoraccounts/-konten
    - Computer, Systeme und Geräte werden in der Regel bei Auslieferung mit einem Standardpasswort für den Administrator (Root) ausgeliefert. Der erste Schritt eines Besitzers sollte sein, dieses in ein eigenes, sicheres Passwort zu ändern. *Mirai* ist beispielweise eine Malware, die das Internet nach Geräten durchsucht, dessen Werkseinstellungen und insbesondere deren Standardbenutzer und Passwörter nicht verändert wurden. Mithilfe des Zugriffs auf viele solcher Geräte und Systeme wurde dann ein Botnetz erstellt, aus dem diverse DDoS Angriffe gestartet wurden. [16]

SCHUTZMAßNAHMEN

Aus den nun bekannten Angriffsvektoren ergeben sich automatisch geeignete Maßnahmen und Verhaltensempfehlungen, um sich möglichst gut und vor allem vorbeugend gegen Ransomware zu schützen. Diesbezüglich veröffentlichte *Sophos* in einem Whitepaper neun Empfehlungen, die man befolgen soll, um das eigene Verhalten gegen Ransomware sicherer zu gestalten. [17]

- Updates sollten früh und oft installiert werden
- Regelmäßige Erstellung von Backups
- Die Anzeige von Dateiendungen aktivieren
- JavaScript (.js) Dateien in einem Texteditor öffnen
- Deaktivierung von Makros in E-Mail-Dateianhängen
- Generell vorsichtiger Umgang mit Anhängen
- Rootuser bzw. Administratoraccounts nur verwenden, wenn es nötig ist
- Informieren über neue Sicherheitsfunktionen in den verwendeten Programmen

Um die Dringlichkeit und Wichtigkeit zu unterstreichen, wird der erste Punkt ein zweites Mal zum Schluss aufgeführt.

- Updates sollten früh und oft installiert werden

ABWEHRSYSTEME

Privatanwender erreichen für den eigenen Schutz schon sehr viel, wenn sichergestellt ist, dass neueste Updates installiert werden und aktuelle Software verwendet wird. Durch regelmäßige Backups und die Aufbewahrung dieser an separaten Orten ohne Internet- oder Netzwerkanbindung, ist man auch im unglücklichen Fall einer Infizierung abgesichert und muss keine Zahlung tätigen, um wieder Zugriff auf die eigenen Daten zu erhalten.

Da für Unternehmen die Erstellung von Backups eine in der Regel zeit- und kostenaufwendige Prozedur ist und es im Ernstfall nicht nur um den Lösegeldbetrag, sondern vorrangig um den durch Ausfallzeiten des Systems verursachten und daraus resultierenden Schaden geht, existieren auch Programme und Systeme, die zur Abwehr von Ransomware im laufenden Betrieb zum Einsatz kommen. Diese können grob in drei Gruppen eingeteilt werden. [18]

Behavioral analysis:

Systeme, die dieser Gruppe zugehörig sind, zeichnen sich dadurch aus, dass sie das Verhalten von Programmen und deren Interaktionen mit der Umgebung überwachen. Nachfolgend drei Beispielsysteme, die zwar grundsätzliche zur selben Gruppe von Abwehrsystemen gehören, sich aber in ihrer Funktionsweise und ihrem Ansatz zum Teil stark unterscheiden.

- *UNVEIL*
  - Generiert eine künstliche Benutzerumgebung und überwacht Bildschirmsperrungen, Zugriffsmuster von Dateien und die Dateistruktur von Ein- und Ausgaben. [19]
- *CRYPTOPDROP*
  - Überwacht Dateitypänderungen und misst und beurteilt Dateiänderungen, um Ransomware zu erkennen. [20]
- *SHIELDFS*
  - Kontrolliert Aktivitäten von Programmen tief im Dateisystem und sammelt Eigenschaften von Dateien und Ordnern, wie zum Beispiel die Ordnerstruktur, die Lese- und Schreibbefehle, Dateiumbenennungen, Dateitypen und die Struktur von Schreibbefehlen. Eine Ransomware ist erkannt, wenn diese Eigenschaften von denen gutartiger Programme abweichen.
  - Die Besonderheit von SHIELDFS ist, dass es, im Gegensatz zu den anderen beiden genannten Systemen, bereits verschlüsselte Dateien wiederherstellen kann. [21]

Detection of cryptographic primitives:

Bei diesem Ansatz werden Programme, genauer gesagt deren Binärcode, analysiert, um mögliche kryptografische Operationen im ausführbaren Code zu identifizieren.

In [22] wird ein Verfahren vorgestellt, bei dem die Ausführung von Programmen verfolgt wird und die Beziehungen von Ein- und Ausgaben im Programmablauf überwacht werden. Zusammen mit dem Vorhandensein von bitweisen arithmetischen Operationen werden Heuristiken angewandt, um kryptografische Algorithmen aufzuspüren.

Key escrow strategies:

Systeme dieser Kategorie zielen darauf ab, das kryptografische Material einer Ransomware zu beziehen und dieses zu nutzen, um die Effekte bei einer Infizierung mit dieser Ransomware aufheben zu können. In der Literatur als vermeintlich bekanntester Vertreter dieser Gruppe gilt Paybreak.

- *PAYBREAK*
  - Die Funktionsweise dieses Systems nutzt die Tatsache, dass die sichere Dateiverschlüsselung, die von Ransomwares auf infizierten Computern durchgeführt wird, auf hybrider Verschlüsselung basiert. Dabei werden symmetrische Sitzungsschlüssel generiert und benutzt. Paybreak überwacht die Nutzung solcher Sitzungsschlüssel, speichert sie und kann sie dann selbst nutzen, um die Dateien ohne Bezahlung des Lösegelds wieder zu entschlüsseln. [23]
  - Logischerweise kann Paybreak nur erfolgreich sein, wenn die Schlüssel der Ransomware richtig erkannt wurden. Nutzt eine Ransomware die kryptografischen Funktionen des infizierten Host-Systems, ist die Chance auf eine erfolgreiche Entschlüsselung durch Paybreak groß. Leider kann dies von Seiten der Ransomware-Entwickler durch die Nutzung kryptografischer Funktionen von Drittanbietern und Code-Obfuscation umgangen werden.

Neben technischen Lösungen wird auch in [18] noch einmal ausdrücklich darauf hingewiesen, dass das Bewusstsein und Verhalten der Benutzer einen ganz entscheiden Anteil am Erfolg oder Misserfolg von Ransomware hat. Es werden Sicherheitsschulungen für Endanwender empfohlen und als effektive Maßname zur Vermeidung von Ransomware angesehen.

Wie bei allen bisherigen Formen von Malware, bei denen es auf der einen Seite die Angreifer und auf der anderen Seite die Verteidiger gibt, ist auch beim Thema Ransomware schnell ein Wettkampf entstanden. Leider schlafen auch hier die Angreifer nicht und nutzen Verfahren, um die Verteidigungssysteme zu überlisten. Genc, Lenzini und Ryan nennen diesbezüglich Rootkitbasierende Ransomware, Obfuscation und White-Box Cryptography. [18]
Rootkitbasierende Ransomware ist in der Lage, ihre Aktivitäten auf einem Computer zu verbergen, wodurch diese nicht, oder nur deutlich schwieriger, von auf behavioral analysis basierenden Verteidungssystemen erkannt werden.
Wie bereits erwähnt, wird Obfuscation genutzt, um Systeme wie Paybreak, die der „key escrow Gruppe“ angehören, zu überlisten. Durch Obfuscation wird der Programmcode von Applikationen durch eine Reihe von Transformationen unverständlich bzw. sehr viel schwieriger zu Lesen, während die Semantik beibehalten wird.

White-Box Cryptography ist ein Konzept, um im Softwarecode enthaltene kryptografische Operationen oder Informationen, wie zum Beispiel den verwendeten Schlüssel, zu schützen. Dabei liegt der Fokus darauf, kryptografische Algorithmen zu implementieren, sodass es sehr schwer wird, die sensiblen Informationen aus dem kompilierten Binärcode auszulesen.

Neben der Nutzung von Verfahren zur Überwindung der Verteidigungssysteme werden die Verteidiger noch mit einer weiteren Problematik konfrontiert. Während anfänglich fast ausschließlich Computer und Computersysteme Ziel von Ransomware waren, dauerte es nicht sehr lang, bis Smartphones und Tablets mehr in den Fokus rückten. Noch recht jung, aber von Forschern bereits als das für die nächste Generation von Ransomware große Ziel auserkoren, ist das Internet der Dinge. [24] In diesem Gebiet steckt für die Entwicklung und den Vertrieb von Ransomware ein sehr großes Potential. Im weiteren Verlauf dieser Arbeit sollen daher die bisherigen Erkenntnisse einmal auf das Internet der Dinge übertragen und ein Augenmerk auf die mögliche Bedrohungslage gelegt werden.

RANSOMWARE OF THINGS

Das Internet der Dinge (im Folgenden mit „IoT“ für „Internet of Things“ abgekürzt) bezeichnet die Vernetzung von physischen Geräten, die über das Internet miteinander kommunizieren können. Neben Geräten wie Fernsehern, Smartphones, Tablets und Überwachungssystemen, sind inzwischen immer mehr, unter anderem auch kleinere, Geräte und Systeme mit dem Internet verbunden. Dazu zählen beispielsweise Autos, Smartwatches, Küchengeräte, Lampen, Alarmsysteme, Türverriegelungen, Heizungssteuerungen und viele weitere Gadgets, die uns durch Automatisierung und Fernzugriffsmöglichkeiten den Alltag erleichtern sollen. Damit steht für Ransomware ein Gebiet bereit, dass mit seinen vielen miteinander vernetzten Geräten ein breites Spektrum für potentielle Angriffsmöglichkeiten bietet. [25] Diese Geräte unterscheiden sich wegen ihres primären Einsatzzwecks insbesondere in ihrer Hardwarezusammensetzung von traditionellen Computern und sind meist sehr limitiert in puncto verfügbarer Ressourcen.
Daher sind hier zum einen nicht dieselben kryptografischen Möglichkeiten verfügbar, zum anderen sind aber auch die Angriffsvektoren und Ziele der Ransomware-Entwickler anders gewichtet beziehungsweise nicht dieselben.
Während der primäre Zweck von Computern die Datenspeicherung und -verarbeitung ist und der Großteil der Ransomware hier darauf abzielt, genau diese Daten zu verschlüsseln, um Lösegeld zu erpressen, sieht es bei den meisten IoT-Geräten anders aus. Hier ist das Ziel von Ransomware, Zugriff zu den Geräten zu erlangen und diese zu sperren und nur gegen Lösegeld wieder freizugeben.
Aus diesem Grund sollen nun die zuvor herausgestellten Angriffsvektoren noch einmal herangezogen werden und für die Geräte des IoT überprüft werden. Am Ende sollen sich jene Angriffsvektoren herauskristallisieren, die für diese Geräte vermeintlich am entscheidendsten sind.
Wie bereits erwähnt, zeichnet sich das IoT vor allem durch die Vernetzung vieler, unterschiedlicher Geräte aus. Deswegen soll bei der nachfolgenden Beurteilung ein besonderes Augenmerk auf das Potential gelegt werden, dass sich Ransomware automatisch, ohne Wissen und Interaktion des Benutzers, verbreitet.

ANGRIFFSVEKTOREN

- Unaufmerksames, blindes Akzeptieren
    - Kommt nur für Geräte in Frage, die eine Benutzeroberfläche beinhalten. Denkbar wären gefälschte Sicherheits- oder Firmwareupdates
    - Wegen der nötigen Interaktion des Benutzers aber für automatische und unbewusste Verbreitung der Ransomware von geringerer Bedeutung
- Herunterladen infizierter Software
    - Hier gilt prinzipiell selbiges. Auch hier ist eine Interaktion des Benutzers nötig und eine Benutzeroberfläche muss vorhanden sein. Zudem muss es sich bei der infizierten Software um eine bekannte und auf vielen Geräten verfügbare Software handeln, damit diese auf möglichst viele Geräte streuen kann.
- Öffnen von E-Mail Anhang
    - Spielt für, abgesehen von Smartphones, Tablets und Smartwatches eine untergeordnete Rolle, da man mit den meisten Geräten keinen Zugriff auf die eigenen E-Mails hat.
- Einlegen oder Einbinden infizierter CDs oder USB-Sticks
    - Auch dies ist eher unwahrscheinlich, da es voraussetzen würde, dass die IoT-Geräte entsprechende Laufwerke bzw. Ports besitzen.
- Anklicken unbekannter Links
    - Analog zum Herunterladen infizierter Software
- Veraltete Software- und Systemversionen
    - Dies ist ein weitaus wahrscheinlicherer Angriffsvektor. Ein Gerätehersteller schließt eine bekannte Sicherheitslücke, bietet die nötigen Updates an, doch viele Benutzer installieren diese Updates erst einige Zeit nach der Veröffentlichung. Für Ransomware genug Zeit, die Sicherheitslücke auszunutzen. Stellt man sich nun vor, dass viele Geräte vom gleichen Hersteller sind oder auf demselben System basieren, ist auch das Potential zur eigenständigen Verbreitung der Ransomware gegeben.
- Software-, Musik- und Videopiraterie
    - Analog zum Herunterladen infizierter Software
- Kein installiertes oder nicht aktualisiertes Antivirenprogramm
    - Dies ist ein interessanter Punkt, denn aufgrund der Tatsache, dass die meisten IoT-Geräte nur sehr begrenzte Hardwareressourcen zur Verfügung haben, wird häufig auf explizite Sicherheitstools verzichtet. Auf der anderen Seite stellt sich dann die Frage, ob ein so in der verfügbaren Hardware limitiertes Gerät überhaupt in der Lage ist, Viren auszuführen.

- Standardpasswörter von Administratoraccounts-/konten
    - Dies ist definitiv ein entscheidender Angriffsvektor für IoT-Geräte. Wie der Fall der *Mirai*-Malware auch schon gezeigt hat, ist hier enormes Potential vorhanden, um Ransomware auf möglichst viele Geräte im Internet oder Netzwerk zu verbreiten. [16]
- Malware auf tragbaren Geräten
    - Sogenannte „Wearables“ wie Smartwatches oder Fitnesstracker sind sehr beliebte Geräte. Da sie, wie es der Name verrät, meist überall getragen werden, wo sich der Besitzer aufhält, können sie mit sehr vielen anderen Geräten in Kontakt kommen und diese infizieren. [26]

Da es für Ransomware bei den IoT-Geräten primär darum geht, selbst Zugriff zu erlangen und diesen für den Besitzer zu sperren, sind vor allem zwei Angriffsvektoren interessant: „Veraltete Software- und Systemversionen“ und „Standardpasswörter von Administratoraccounts-/konten“.

Geräte und Szenarien

Nun ist zu überlegen, welche Geräte für Ransomware interessant sind und wie mögliche Szenarien aussehen. Die verschiedenen im IoT involvierten Geräte haben unterschiedliches Potential, um möglicherweise in das Visier von Ransomware zu geraten. In dieser Hinsicht wurde bereits die zur Verfügung stehende Hardware der jeweiligen Geräte angedeutet. Wie auch bei Ransomware für herkömmliche Computer stellt sich den Verantwortlichen die Frage, wie hoch das geforderte Lösegeld gesetzt wird. Logischerweise kann so eine Ransomware für die Vertreiber nur zum gewünschten Erfolg führen, wenn der Wert der Daten oder, im Fall von IoT, der Gerätewert die Lösegeldforderung übersteigt. Allein wegen dieser Tatsache kommen viele Geräte, deren Anschaffungskosten nicht hoch genug sind und bei denen die Besitzer ohne Zweifel einfach das infizierte Gerät durch ein Neues ersetzen würden, anstatt ein Lösegeld zu zahlen, nicht in Frage. Zudem machen sicherlich schon die Entwicklungskosten einer Ransomware für solche Geräte das Projekt unrentabel.
Daneben sind die entscheidenden Angriffsvektoren zu berücksichtigen. Die Geräte müssen auch so beschaffen sein, dass es überhaupt die Möglichkeit gibt, dass Software- und Systemversionen vom Besitzer nicht auf dem neuesten Stand gehalten werden oder im Auslieferungszustand eingestellte Benutzer- und Administratorkonten mit samt Passwörtern vom Besitzer nicht geändert werden.
An dieser Stelle seien einige Beispiele aus dem Smart Home Bereich erwähnt, die besonders interessant sind und bei denen zu erwarten ist, dass sie zuerst Ziel von Ransomware sein werden, sofern sie nicht ohnehin schon zum Ziel geworden sind.

- IP-Überwachungskameras
    - Diese Geräte werden meist über ein Web-Portal mit Anmeldemaske erreicht und besitzen Firmware, die aktuell gehalten werden muss.
- Software von Boardcomputern in Autos
    - Auch hier ist der Zugriff und die Bedienung über eine Software mit Anmeldeinformationen geregelt.
    - Häufig kann auch mittels einer App auf dem Smartphone auf Funktionen des Autos zugegriffen werden. Denkbar ist ein Szenario, bei dem durch Ransomware der Zugriff auf das Auto nicht mehr möglich ist, ehe man ein Lösegeld zahlt.
- Fernsteuerung von Heizung, Alarmsystemen, Haustüren, Steckdosen
    - Die Steuerung erfolgt auch hier über eine Bedienoberfläche mit Anmeldung. Was wäre, wenn eine Ransomware die Kontrolle darüber übernimmt, man die eigene Haustür nicht mehr öffnen kann oder diese geöffnet wird während man im Urlaub ist? Würde man den Urlaub abbrechen oder das geforderte Lösegeld zahlen?

In Anbetracht der Anzahl verschiedener IoT-Geräte könnte man diese Liste sicherlich endlos fortführen. Ein Gerät, oder vielmehr System, das in dieser Hinsicht als Ziel für Ransomware besonders geeignet ist und alles vereint, soll allerdings nochmal explizit genannt sein. Dieses System besitzt ein Betriebssystem, Software die aktuell gehalten werden muss, Standardbenutzer und -passwörter im Auslieferungszustand und hat besonders großes Potential, als zentraler Knoten zur Verbreitung von Ransomware auf vernetzte Geräte zu dienen. Die Rede ist von Virtuellen Assistenten aus dem Smart Home Bereich.
Virtuelle Assistenten erlauben dem Besitzer, andere vernetzte Geräte zu kontrollieren und zu bedienen. Die Bedienung erfolgt häufig per Sprachbefehlen oder auch per App. Beispiele für solche Virtuellen Assistenten sind Google Home, Amazon Echo, aber auch umfangreichere digitale Assistenten die vermehrt in Neubauten gehobener Preisklasse integriert sind und in der Lage sind, viele Gerätschaften des Haushalts zu kontrollieren. Je gebräuchlicher und bekannter ein Gerät ist, desto höher ist dann auch die Wahrscheinlichkeit, dass es in vielen Haushalten eingesetzt wird. Ist ein Betriebssystem dann auch nicht nur auf eine Art von Gerät beschränkt, sondern auf mehreren Verschiedenen installiert, könnte dieselbe Sicherheitslücke dafür sorgen, dass mehrere, unterschiedliche Geräte gleichzeitig angreifbar sind. Als Beispiel soll hier Android herhalten. [27] Dieses System ist schon lang nicht mehr nur die Basis von Smartphones, sondern auch von Tablets, Fernsehern und bspw. Smart Hubs. Geht man dann eine Ebene tiefer und schaut sich an, welche Geräte auf Linux basieren, könnte sich eine Sicherheitslücke im Linux-Kernel, je nach Art der Sicherheitslücke, auf eine enorm große Anzahl verschiedener, auf diesem System basierender, Geräte auswirken.

Dies stellt natürlich ein sehr reizvolles Ziel dar, wodurch bei den Betroffenen ein großer Leidensdruck erzeugt werden kann um Lösegeldzahlungen zu erpressen. Es ist daher durchaus zu erwarten, dass Ransomware-Entwickler große Anstrengung und Motivation in die Entwicklung von Erpressersoftware stecken, die genau auf solche Konstellationen ausgerichtet ist.

Vorfälle

Diese Arbeit soll keinesfalls den Eindruck erwecken, dass bisher, im Jahr 2017, noch keine Ransomware-Angriffe, die explizit dem Internet der Dinge gerichtet sind, vorgefallen sind und man sicher daher mit Überlegungen bezüglich der Sicherheit noch Zeit lassen kann. Um dies zu vermeiden, folgt jetzt noch eine Auswahl dokumentierter Vorfälle. [18]

- Angreifern ist es gelungen, die Kontrolle über das Ticketsystem des öffentlichen Transportnetzes von San Francisco zu übernehmen und Lösegeld zu fordern. [28]
- In einem Hotel in Österreich wurde das Verwaltungssystem infiziert. Die Türen des Hotels konnten so vom Angreifer blockiert werden und dem Hotelbetreiber war das Generieren neuer Schlüsselkarten für die Türen nicht möglich und wurde nur gegen Lösegeld wieder freigegeben. [29]
- Forschern ist es gelungen, zu demonstrieren, dass die Kontrolle über ein Auto übernommen werden und das Auto per Fernzugriff gestoppt werden kann. [30]
- Eine weitere Gruppe von Forschern konnte zeigen, dass 75% der smarten Türsysteme, die über Bluetooth gesteuert werden, drahtlos gehackt werden kann. [31]

Fazit

Ransomware ist und wird für das Internet der Dinge eine ernstzunehmende Bedrohung. Das IoT ist in Umfang und Variantenreichtum extrem schnell gewachsen und beliebt geworden. So schnell, dass nötige Sicherheitsmaßnahmen und Sicherheitsstandards nicht immer Schritt halten konnten und können. Bei all der Beliebtheit muss sichergestellt sein, dass die nötigen Sicherheitsvorkehrungen getroffen werden und sich der Sicherheitsgedanke im Bewusstsein der beteiligten Personen manifestiert. Während für Privatanweder direkte Kosten in Form des Lösegelds entstehen, stehen für Unternehmen vor allem die Schäden durch Ausfallzeiten der Systeme auf dem Spiel. Das Internet der Dinge wird als Ziel für die nächste Generation von Ransomware gesehen. Für die Hersteller von IoT-Geräten wird es eine große und wichtige Herausforderung, ihre Geräte gegen Infizierung durch Ransomware zu schützen, denn im Gegensatz zu manch anderen, bisherigen Varianten von Malware, sind Infizierungen mit Ransomware für die Betroffenen häufig direkt mit finanziellem Schaden oder Beeinträchtigung der persönlichen Sicherheit verbunden. Umso wichtiger ist, dass bereits positive Entwicklungen in diese Richtung zu verzeichnen sind, wie die Veröffentlichungen des Bundesamts für Sicherheit in der Informationstechnik [9] und die des National Institute of Standards and Technology, in der es um die Entwicklung von Sicherheitssystemen und sichere Software- und Systementwicklung geht, beweisen. [32]

LITERATURVERZEICHNIS

[1] Kharraz A., Robertson W., Balzarotti D., Bilge L., Kirda E. (2015) Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks. In: Almgren M., Gulisano V., Maggi F. (eds) Detection of Intrusions and Malware, and Vulnerability Assessment. DIMVA 2015. Lecture Notes in Computer Science, vol 9148. Springer, Cham
http://www.eurecom.fr/en/publication/4548/download/rs-publi-4548.pdf
[abgerufen am: 03.12.2017]

[2] Krebs on Security, Inside a Reveton Ransomware Operation, August 2012
http://krebsonsecurity.com/2012/08/inside-a-reveton-ransomware-operation/
[abgerufen am: 31.03.2018]

[3] David Emm (2008) Cracking the code: The history of Gpcode, Computer Fraud & Security, Volume 2008, Issue 9, September 2008, pages 15-17
http://www.sciencedirect.com/science/article/pii/S1361372308701398
[abgerufen am: 11.03.2018]

[4] Mikhail Kuzin (2014) Unfinished ransomware for MacOS X, June 2014
https://securelist.com/unfinished-ransomware-for-macos-x/66760/
[abgerufen am: 11.03.2018]

[5] Abrams, Lawrence. (2013) CryptoLocker Ransomware Information Guide and FAQ, October 2013
https://www.bleepingcomputer.com/virus-removal/cryptolocker-ransomware-information
[abgerufen am: 11.03.2018]

[6] Alina Simone (2015) The Strange History of Ransomware, March 2015
https://medium.com/un-hackable/the-bizarre-pre-internet-history-of-ransomware-bb480a652b4b
[abgerufen am: 17.03.2018]

[7] Bill Brenner (2017) 5 ransomware as a service (RaaS) kits – SophosLabs investigates, December 2017
https://nakedsecurity.sophos.com/2017/12/13/5-ransomware-as-a-service-raas-kits-sophoslabs-investigates/
[abgerufen am: 11.03.2018]

[8] Symantec Corporation World Headquarters (2016) An ISTR Special Report: Ransomware and Business 2016, August 2016
https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ISTR2016_Ransomware_and_Businesses.pdf
[abgerufen am: 03.12.2017]

[9] Bundesamt für Sicherheit in der Informationstechnik (2016) Ransomware – Bedrohungslage, Prävention & Reaktion, März 2016
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware.pdf?__blob=publicationFile&v=2
[abgerufen am: 03.12.2017]

[10] Kaspersky Lab (2016) PC-Ransomware in den Jahren 2014-2016 Entwicklung und Zukunft einer Bedrohung, Juni 2016
https://de.securelist.com/pc-ransomware-in-2014-2016/71625/
[abgerufen am: 03.12.2017]

[11] Claud Xiao and Jin Chen (2016) New OS X Ransomware KeRanger Infected Transmission BitTorrent Client Installer, Palo Alto Networks Blog, March 2016
https://researchcenter.paloaltonetworks.com/2016/03/new-os-x-ransomware-keranger-infected-transmission-bittorrent-client-installer/
[abgerufen am: 03.12.2017]

[12] Catalin Cimpanu (2016) Cerber Ransomware Spreads via Fake Credit Card Email Reports, December 2016
https://www.bleepingcomputer.com/news/security/cerber-ransomware-spreads-via-fake-credit-card-email-reports/
[abgerufen am: 17.03.2018]

[13] Sophos Ltd. (2010) IBM distributes USB malware cocktail at AusCERT security conference May 2010
https://nakedsecurity.sophos.com/2010/05/21/ibm-distributes-usb-malware-cocktail-auscert-security-conference/
[abgerufen am: 03.12.2017]

[14] Lawrence Abrams (2017) WannaCry / Wana Decryptor / WanaCryptor Info & Technical Nose Dive, May 2017
https://www.bleepingcomputer.com/news/security/wannacry-wana-decryptor-wanacrypt0r-info-and-technical-nose-dive/
[abgerufen am: 03.12.2017]

[15] Andrew D. Berns and Eunjin Jung. (2008) Searching for malware in BitTorrent. University of Iowa, Tech. Rep. UICS-08-05, April 2008
http://www.cs.uni.edu/~adberns/papers/UICS-08-05.pdf
[abgerufen am: 17.03.2018]

[16] Zeifman, Igal; Bekerman, Dima; Herzberg, Ben (2016). Breaking Down Mirai: An IoT DDoS Botnet Analysis, October 2016
https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html
[abgerufen am: 09.12.2017]

[17] Sophos Ltd. (2017) How To Stay Protected Against Ransomware
https://www.sophos.com/en-us/medialibrary/Gated%20Assets/white%20papers/sophosransomwareprotectionwpna.pdf?la=en
[abgerufen am: 09.12.2017]

[18] Z.A. Genç, G. Lenzini, and P.Y.A. Ryan (2017) The Cipher, the Random and the Ransom: A Survey on Current and Future Ransomware, CECC 2017 Ljubljana, Slovenia, November 2017
http://hdl.handle.net/10993/32574
[abgerufen am: 10.12.2017]

[19] Amin Kharaz, Sajjad Arshad, Collin Mulliner, William Robertson and Engin Kirda. (2016) UNVEIL: A Large-Scale, Automated Approach to Detecting Ransomware 25th USENIX Security Symposium, August 2016
https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/kharaz
[abgerufen am: 31.03.2018]

[20] N. Scaife, H. Carter, P. Traynor and K. R. B. Butler (2016) CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data, IEEE 36th International Conference on Distributed Computing Systems (ICDCS), Nara, 2016, pp. 303-312.
http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7536529&isnumber=7536347
[abgerufen am: 31.03.2018]

[21] Continella, Andrea, Alessandro Guagnelli, Giovanni Zingaro, Giulio De Pasquale, Alessandro Barenghi, Stefano Zanero and Federico Maggi. (2016) ShieldFS: a self-healing, ransomware-aware filesystem. ACSAC, Proceedings of the 32nd Annual Conference on Computer Security Applications, December 2016, pp. 336-347.
http://shieldfs.necst.it/continella-shieldfs-2016.pdf
[abgerufen am: 31.03.2018]

[22] Gröbert F., Willems C., Holz T. (2011) Automated Identification of Cryptographic Primitives in Binary Programs. In: Sommer R., Balzarotti D., Maier G. (eds) Recent Advances in Intrusion Detection. RAID 2011. Lecture Notes in Computer Science, vol 6961. Springer, Berlin, Heidelberg
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.653.7728&rep=rep1&type=pdf
[abgerufen am: 10.12.2017]

[23] Eugene Kolodenker, William Koch, Gianluca Stringhini, Manuel Egele (2017) PayBreak: Defense Against Cryptographic Ransomware, ASIA CCS '17, Abu Dhabi, United Arab Emirates, April 2017
https://megele.io/paybreak.pdf
[abgerufen am: 10.12.2017]

[24] Stephen Cobb (2017) RoT: Ransomware of Things, March 2017
https://cdn1-prodint.esetstatic.com/ESET/US/Newsroom/2017/03/ESET_Trends-and-Prediction_2017_Ransomware.pdf
[abgerufen am: 31.03.2018]

[25] Fu K., Kohno T., Lopresti D., Mynatt E., Nahrstedt K., Patel S., Richardson D., & Zorn B., (2017) Safety, Security, and Privacy Threats Posed by Accelerating Trends in the Internet of Things, March 2017
https://pdfs.semanticscholar.org/4955/2619facd570a34becd8e3fa41d5f99da10e2.pdf
[abgerufen am: 31.03.2018]

[26] Liquid Web Inc. (2017) Carrie Wheeler: Three New Attack Vectors That Will BeBorn Out Of IoT, April 2017
https://www.liquidweb.com/blog/three-new-attack-vectors-will-born-iot/
[abgerufen am: 10.12.2017]

[27] F. Mercaldo, V. Nardone and A. Santone (2016) Ransomware Inside Out, 11th International Conference on Availability, Reliability and Security (ARES), 2016, pp. 628-637
http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7784627&isnumber=7784494
[abgerufen am: 31.03.2018]

[28] Elizabeth Weise. (2016) Ransomware attack hit San Francisco train system, November 2016
https://www.usatoday.com/story/tech/news/2016/11/28/sanfrancisco-metro-hack-meant-free-rides-saturday/94545998/
[abgerufen am: 16.12.2017]

[29] Dan Bilefsky. (2017) Hackers Use New Tactic at Austrian Hotel Locking the Doors, January 2017
https://www.nytimes.com/2017/01/30/world/europe/hotel-austria-bitcoin-ransom.html
[abgerufen am: 16.12.2017]

[30] Andy Greenberg. (2015) Hackers Remotely Kill a Jeep on the Highway—With Me in It, July 2017
https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/
[abgerufen am: 16.12.2017]

[31] Paul Wagenseil. (2016) 75 Percent of Bluetooth Smart LocksCan Be Hacked, August 2016
http://www.tomsguide.com/us/bluetooth-lock-hacks-defcon2016,news-23129.html
[abgerufen am: 16.12.2017]

[32] Ron Ross, Michael McEvilley, Janet Carrier Oren (2016) Systems Security Engineering, National Institute of Standards and Technology Special Publication 800-160, November 2016
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160.pdf
[abgerufen am: 16.12.2017]