Thema Ransomware

Studiengang Digitale Forensik
Ausarbeitung im Rahmen des Modul 106

Markus Stoll

Datum 20.03.2017

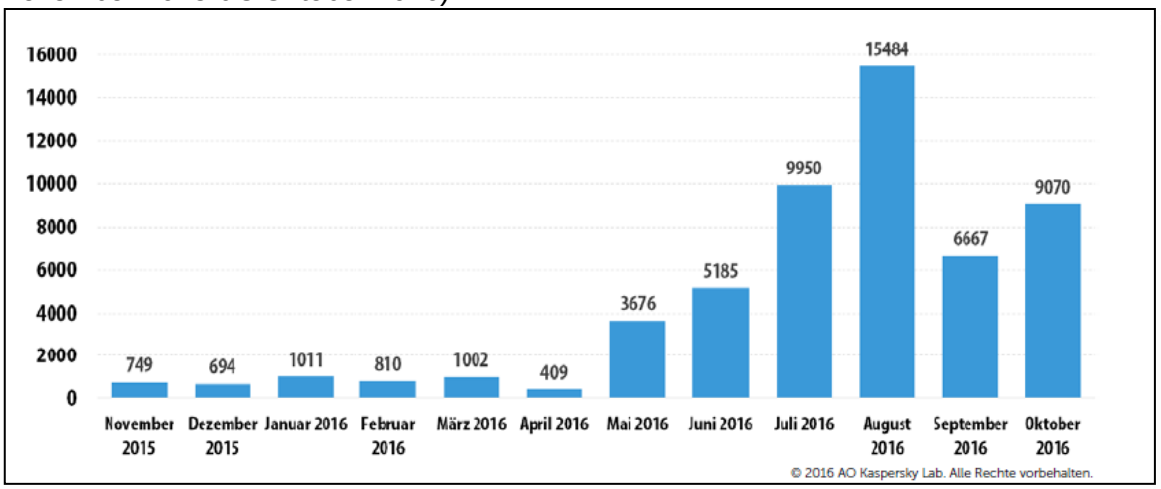
Inhaltsverzeichnis

1 T7: Ransomware

1.1 Ransomware-Angriff mit aktuellen Statistiken

1.1.1 Zahl der neuen Modifikationen von Verschlüsselungsprogrammen der Klasse Trojan-Ransom

(November 2015 bis Oktober 2016)



Im Laufe des Jahres detektierte Kaspersky Lab über 54.000 Modifikationen von Verschlüsselungs-Ransomware und entdeckte 62 neue Familien.

1.1.2 Häufigkeit der Angriffe

Alle 40 Sekunden wird ein Unternehmen von Ransomware angegriffen. Gemäß den Studien von Kaspersky Lab wurde im Jahr 2016 eines von fünf Unternehmen weltweit Opfer eines IT-Sicherheitsvorfalls infolge einer Ransomware-Attacke.

- 42 Prozent aller kleinen und mittleren Unternehmen wurden in den letzten zwölf Monaten von Ransomware angegriffen.
- 32 Prozent dieser Unternehmen zahlten Lösegeld.
- Eines von fünf dieser Unternehmen erhielt seine Dateien nicht zurück, auch nicht nach der Zahlung des Lösegeldes.
- 67 Prozent der von Ransomware angegriffenen Unternehmen verloren ihre gesamten oder einen Teil ihrer Geschäftsdaten, und eines von vier versuchte wochenlang, den Zugriff auf die Daten wiederherzustellen.

Quelle: KASPERSKY SECURITY BULLETIN 2016/2017
http://newsroom.kaspersky.eu/fileadmin/user_upload/de/Downloads/PDFs/Kaspersky_Security_Bulletin_2016_2017.pdf

1.1.3 Meist verwendete Exploits

Wie bereits im Vorjahr erfreuten sich auch im Laufe des Jahres 2016 Exploits für den Adobe Flash Player einer großen Nachfrage. Vier der entsprechenden Sicherheitslücken schafften es in die Liste der am häufigsten von Cyberkriminellen ausgenutzten Sicherheitslücken:

- **CVE-2015-8651 (Adobe Flash)**
- **CVE-2016-1001 (Adobe Flash)**
- **CVE-2016-0034 (Microsoft Silverlight)**
- **CVE-2015-2419 (Internet Explorer)**
- **CVE-2016-4117 (Adobe Flash)**
- **CVE-2016-4171 (Adobe Flash)**

Quelle: KASPERSKY SECURITY BULLETIN 2016/2017
http://newsroom.kaspersky.eu/fileadmin/user_upload/de/Downloads/PDFs/Kaspersky_Security_Bulletin_2016_2017.pdf

1.1.4 Ransomware Angriff „Locky“

1.1.4.1 Infizierte Rechner

Stand: 19.02.2016

Infizierte Rechner weltweit 400000
Infizierte Rechner innerhalb 24 Stunden:

- **Deutschland 17000**
- **USA 11000**
- **Niederlande 5000**
- **Italien 5000**
- **…**
- **…**

1.1.4.2 Betroffene Unternehmen

Betroffene Unternehmen u.a.:

- **Fraunhofer-Institut in Bayreuth**

- **Presbyterian Medical Center Philadelphia**
  Im Februar 2016 fiel das Computernetzwerk im Hollywood Presbyterian Medical Center (HPMC) in Südkalifornien mehr als eine Woche lang aus, weil das Krankenhaus mit den Folgen eines Ransomware-Angriffs zu kämpfen hatte. Die Krankenhausverwalter riefen den internen Notstand aus, da die Mitarbeiter Schwierigkeiten hatten, auf Krankenakten und Computersysteme zuzugreifen, die für die Patientenversorgung unerlässlich waren. Einige Patienten mussten in andere Krankenhäuser verlegt werden, um ihre kontinuierliche Versorgung zu gewährleisten.

Quelle: Spiegel
http://www.spiegel.de/netzwelt/gadgets/locky-17000-windows-rechner-in-deutschland-taeglich-infiziert-a-1078318.html
Quelle: LogRhythm
https://files.vogel.de/vogelonline/vogelonline/companyfiles/10993.pdf

1.1.4.3 Höhe der Lösegeldforderung

Detection name: Trojan.Cryptolocker.AF
Ransom amount: 0.5 to 1 bitcoin ($200 to $400 on February 2016 rates)
Discovery: February 2016
Known infection vectors: Spam campaigns, Neutrino exploit kit, Nuclear exploit kit

Quelle: Symantec Special Report: Ransomware and Business 2016
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ISTR2016_Ransomware_and_Businesses.pdf

1.1.4.4 Incident Taxonomy

Attacker	Tool	Vulnerability	Action	Target	Result	Objective
Erpresser	SOE	Mensch	Verschlüsselung	Dateien	Geldeinnahme	Finanzieller Vorteil

1.1.5 Was erwartet uns im Jahr 2017?

Ransomware wird leider ein Thema bleiben. Geldautomaten rücken zunehmend ins Visier Cyberkrimineller. Und im Vorfeld der Bundestagswahl im September kann es zu einem Informationskrieg im Internet kommen. Die Hintermänner der Cyberangriffe bleiben im Dunkeln und finden immer neue Wege, sich zu tarnen.

Quelle: KASPERSKY SECURITY BULLETIN 2016/2017
http://newsroom.kaspersky.eu/fileadmin/user_upload/de/Downloads/PDFs/Kaspersky_Security_Bulletin_2016_2017.pdf

1.2 Wie funktioniert Ransomware

1.2.1 Varianten

1.2.1.1 Locker-Ransomware

Die Malware sperrt den Zugang zum Betriebssystem.

1.2.1.2 Crypto-Ransomware

Diese Malware verschlüsselt Daten über kryptographische Verfahren, so dass die Daten diese nicht mehr verwertet werden können.

Für beide Varianten gilt.

Zur Entsperrung wird das Opfer zur Zahlung eines Lösegeldes aufgefordert.

Nach Erkenntnissen des BSI wurden im Februar 2016 in Deutschland am häufigsten die Ransomware-Familien TeslaCrypt, Locky sowie CryptoWall detektiert. Die Detektionszahlen zeigen auch, dass es sich bei 95 % der Angriffe um Ransomware mit Verschlüsselungsfunktion (Crypto-Ransomware) handelt.

Die einfachen Sperrbildschirme im Desktop-Bereich aus den vergangenen Jahren haben heute keine Relevanz mehr.

Quelle: BSI Ransomware Bedrohungslage, Prävention & Reaktion
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware.pdf?__blob=publicationFile&v=2

1.2.2 Angriffsvektoren

1.2.2.1 Spam

Bei Angriffen mittels Spam wird versucht den Benutzer zum Öffnen von E-Mail-Anhängen zu bewegen. So werden angebliche Rechnungen, Bestellbestätigungen, Paketempfangsbestätigungen, eingescannte Dokumente, empfangene Faxe, teilweise unter Verwendung von echten Firmennamen und -adressen und zum Teil in perfekter Nachahmung tatsächlicher Firmen-E-Mails, versendet.

Im Anhang befindet sich meist ein Downloader, der die eigentliche Schadsoftware nachlädt. So bleibt das Verteilungsnetz flexibel, da die Angreifer die zum Download bereit gestellte Schadsoftware auf aktuellem Stand (d. h. schlechte AV-Erkennung) halten können. Der Download findet meist von kompromittierten Webservern vor allem kleiner Webpräsenzen statt. Es wird vermutet, dass die Angreifer diese Webpräsenzen über Schwachstellen in nicht aktuell gehaltener Serversoftware und über Trojaner abgegriffene Zugangsdaten die Webserver kompromittieren konnten.

In der Vergangenheit wurden auch Kampagnen gesichtet, in denen die Schadsoftware direkt verteilt wurde, z. B. als (meist gezippte) EXE-Datei oder eingebettet / kodiert in einem Microsoft-Office-Dokument. Das Entpacken und Starten musste dann vom Benutzer manuell durchgeführt werden oder wurde von Makros erledigt.

In den bisher am weitesten verbreiteten Kampagnen wurden Microsoft Office Dokumente mit stark verschleierten Makros und JavaScript- sowie VirtualBasicScript-Dateien versendet. Oft wurden die Dateien in einem Archiv (meist ZIP) ausgeliefert.

Unter anderem wurde das auf die Verteilung des Banking-Trojaners DRIDEX spezialisierte Spamnetzwerk, die seit Monaten größte Schadsoftware-Spam-Quelle, Mitte Februar auf Verteilung der Ransomware LOCKY umgestellt. Als Größenordnung kann man Erfahrungen aus dem DRIDEX-Vorläufer GEODO extrapolieren, bei dem auf einem von vielen Kommando-Servern (C&C) binnen eines Monats etwa 60.000 deutsche Betroffene verwaltet wurden.

Quelle: BSI Ransomware Bedrohungslage, Prävention & Reaktion
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware.pdf?__blob=publicationFile&v=2

1.2.2.2 Drive-By Infektionen mittels Exploit-Kits

Exploit-Kits gehören seit mehreren Jahren ebenfalls zu den Infektionsvektoren für Ransomware. Zero-Day-Exploits oder Exploits für neue Schwachstellen in weit verbreiteten Programmen werden binnen kürzester Zeit in Exploit-Kits integriert und auch zur Verteilung von Ransomware oder anderen Schadprogramm-Typen verwendet. In den vergangenen Monaten ging von den Exploit-Kits die meiste Aktivität aus. Alle der genannten Exploit-Kits wurden in der Vergangenheit auch zur Installation von Ransomware verwendet.

In vielen Fällen werden die Exploit-Kits über Drive-By-Infektionen auf kompromittierten Webseiten oder Werbebannern verbreitet. Danach wird die jeweilige Schadsoftware, z. B. Ransomware, nachgeladen.

1.2.2.3 Schwachstellen in Servern

Die Ransomware ***CTB-Locker*** nutzt Schwachstellen in Webservern zur Infektion aus und verschlüsselt dann die Inhalte des Web-Auftritts.

1.2.2.4 Fernwartungszugänge

Bei Vorfällen mit der Ransomware ***GPCode*** wurde in einigen Fällen ein zusätzlicher Modus Operandi der Täter festgestellt. Diese scannen das Internet aktiv nach solchen Systemen, die Fernwartungszugänge ins Internet anbieten, wie zum Beispiel Microsoft Remote-Desktop. Dort führen Sie Brute-Force Angriffe auf das Passwort durch. Bei einem erfolgreichen Login installieren sie eine Ransomware-Malware. Aufgrund der geringen Verbreitung von GPCode wird dieser Infektionsvektor durch Ransomware aber nur selten ausgenutzt.

Quelle: BSI Ransomware Bedrohungslage, Prävention & Reaktion
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware.pdf?__blob=publicationFile&v=2

1.2.3 Ablauf eines Angriffs

Opfer

Benutzer PC

C&C - Server & Datenbank

Benutzer PC wird mit Schadsoftware infiziert.

Schadsoftware enthält feste C&C Serveradressen oder generiert diese dynamisch (Domain generation alogrithm).

C&C Server wird kontaktiert, der schadhafte Programmcode wird nachgeladen und installiert.

Individuelle ID (Client ID) wird dem Server übermittelt.

Individuelle ID (Client ID) wird gespeichert.

Kryptografisches Schlüsselpaar wird generiert. Öffentlicher Schlüssel (nur zur Verschlüsselung) wird übermittelt.

Daten werden verschlüsselt (mit öffentlichen Schlüssel) und C&C-Server bei Erfolg benachrichtigt.

Bitcoin-Zahlungsadresse wird generiert und an den Benutzer-PC übermittelt

Warnmeldung mit Opfer-PC übermittelt Hinweisen zur Zahlung wird angezeigt.

Das Opfer führt die Zahlung aus.

C&C Server prüft, ob Zahlung eingegangen ist und übermittelt im Erfolgsfall den Schlüssel zur privaten ID.
Das Zahlungssystem Bitcoin besteht aus einer Datenbank, der Blockchain, in der alle Transaktionen verzeichnet sind.

Daten können entschlüsselt werden.

1.3 Entschlüsselung von Dateien

1.3.1 Vorgehensweise

Fast alle Anitvirenhersteller wie z.B. Trend Micro, Bitdefender, Kaspersky Lab stellen Hilfsprogramme zur Entschlüsselung von durch Ransomware verschlüsselten Dateien bereit.

Die Vorgehensweise ist dabei wie folgt:
Quelle: Kaspersky Lab

- Zuerst muss ermittelt werden von welcher Ransomware die Dateien verschlüsselt wurden. Im einfachen Fall kann dies über den Benutzerdialog der Schadsoftware ermittelt werden. Ansonsten müssen die Inhalte der verschlüsselten Dateien oder deren Dateiname / Dateiendung untersucht werden.

- Danach kann zur Entschlüsselung das entsprechende Hilfsprogramm vom Antiviren Hersteller heruntergeladen werden.

- Nach Anleitung können dann die Dateien mit dem Hilfsprogramm entschlüsselt werden.

1.3.2 Beispiele

1.3.2.1 Trojan-Ransom.Win32.Scatter oder Trojan-Ransom.BAT.Scatter

- **Entschlüsselung**
  Durch das Hilfsprogramm ScatterDecryptor.

- **Infektionszeichen**
  Die Trojaner Trojan-Ransom.Win32.Scatter oder Trojan-Ransom.BAT. Scatter verschlüsseln Dateien ändern ihre Erweiterung wie folgt.

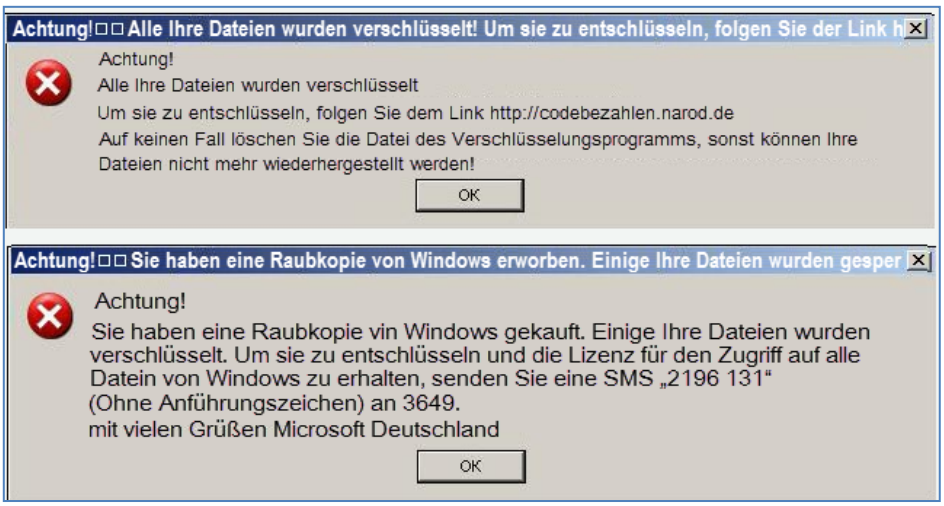
  - **.pzdc**
  - **.crypt**
  - **.good**

Quelle: Kaspersky Lab.
http://support.kaspersky.com/de/viruses/disinfection/11333

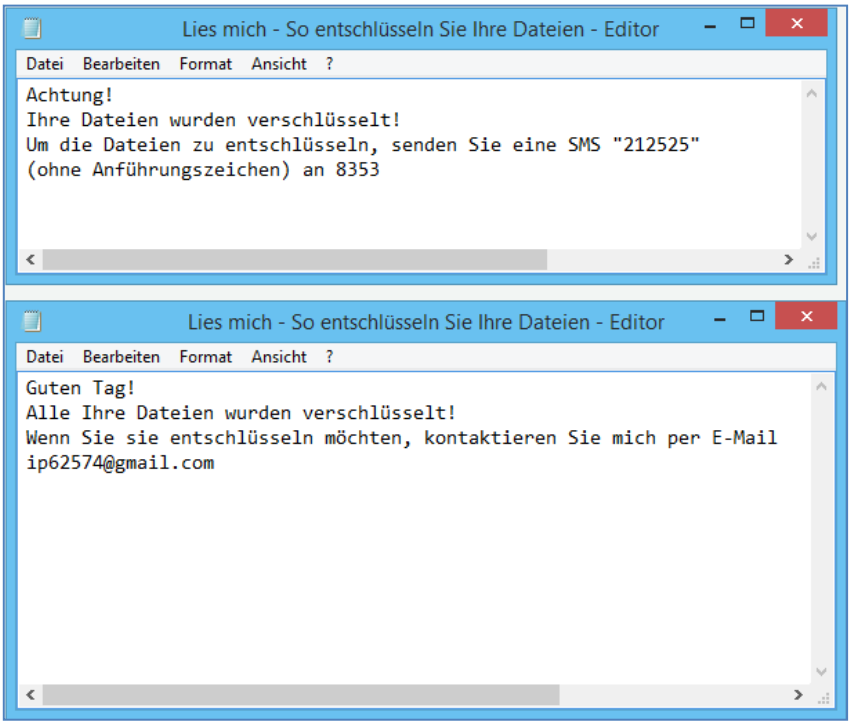
1.3.2.2 Trojan-Ransom.Win32.Xorist oder Trojan-Ransom.MSIL.Vandev

- **Entschlüsselung**
  Durch das Hilfsprogramm XoristDecryptor.

- **Infektionszeichen**
  Auf dem Bildschirm kann eine Meldung mit der Forderung nach Sendung einer SMS zur Entschlüsselung von Daten angezeigt werden.



Anstatt der Meldung kann eine Textdatei „Lies mich – So entschlüsseln Sie Ihre Daten“ im Stammordner des Datenträgers C erstellt werden.



Quelle: Kaspersky Lab.
http://support.kaspersky.com/de/viruses/disinfection/2911?omreferrer=http%3a%2f%2fsupport.kaspersky.com%2fde%2fsearch%3fomreferrer%3dhttp%3a%2f%2fsupport.kaspersky.com%2fviruses%2fdisinfection%2f3043%26query%3dXoristDecryptor%26sec%3dSupportViruses#block2

1.3.2.4 Trojan-Ransom.Win32.Rannoh

- **Entschlüsselung**
  Durch das Hilfsprogramm RannohDecryptor.

- **Infektionszeichen**
  Wenn das System mit einem schädlichen Programm der Gattung Trojan-Ransom.Win32.Rannoh, Trojan-Ransom.Win32.AutoIt, Trojan-Ransom.Win32.Fury, Trojan-Ransom.Win32.Crybola, Trojan-Ransom.Win32.Cryakl oder Trojan-Ransom.Win32.CryptXXX infiziert ist, dann werden alle Dateien auf dem Computer auf folgende Weise verschlüsselt:

  Bei der Infektion mit Trojan-Ransom.Win32.Rannoh werden Namen und Erweiterungen wie folgt geändert: locked-<ursprünglicher_Name>.<4 zufällige Buchstabe>.

  Bei der Infektion mit Trojan-Ransom.Win32.Cryakl wird das Tag {CRYPTENDBLACKDC} am Ende des Inhalts der Dateien stehen.

  Bei der Infektion mit Trojan-Ransom.Win32.AutoIt wird die Erweiterung nach der folgenden Vorlage geändert: <ursprünglicher_Name>@<Mail-Domäne>_.<zufälllige_Zeichen>.
  z. B. ioblomov@india.com_.RZWDTDIC.

  Bei der Infektion mit Trojan-Ransom.Win32.CryptXXX wird die Erweiterung auf folgende Weise geändert:
  <ursprünglicher_Name>.crypt
  <ursprünglicher_Name>.crypz
  <ursprünglicher_Name>.cryp1

Quelle: Kaspersky Lab.
http://support.kaspersky.com/de/viruses/disinfection/8547

1.4 Technisches Know-how zum Erstellen einer Ransomware

1.4.1 Ohne Crimeware-Kits

Hier benötigt der Angreifer technische Details in:

Softwareentwicklung	um Software zu erstellen
Kryptographie	um Dateien zu verschlüsseln/entschlüsseln
Exploits z.B. in Betriebssystemen, Flash, Java oder Silverlight	um die Schadsoftware zu verteilen
Social Engineering z.B. Erstellen von SPAM Nachrichten	um die Schadsoftware zu verteilen
Zahlungssystem Bitcoin	Um Zahlungen der Opfer zu erhalten und kontrollieren.

1.4.2 Mit Crimeware-Kits, Ransomware-as-a-Service

Hier benötigt der Angreifer keine speziellen Kenntnisse.

Crimeware Kits verfügen in der Regel über eine grafische Benutzeroberfläche, mit der auch nicht-technische Benutzer anspruchsvolle Angriffe verwalten können. Die Kits werden von professionellen Entwicklern erstellt, diese nutzen zumeist bereits öffentlich bekannte Schwachstellen in Browsern und auf Clients aus.

Über ein Web-Frontend kann sich der Nutzer einloggen. Die grafische Oberfläche stellt Werkzeuge bereit, die das effektive automatisierte Verteilen der durch den Nutzer definierten Schadfunktion ermöglichen. Zu diesen Werkzeugen gehören neben den Exploits selbst unter anderem technischer Support, regelmäßige Updates und detaillierte Statistiken zu den gestarteten Malware-Kampagnen.

Kommerziell erhältlich sind die Kits unter anderem in Untergrundforen, die Preise variieren häufig zwischen drei- und fünfstelligen US-Dollar-Beträgen. Auch Provisionsmodelle sind gängig.

Exploit Kits bringen in aller Regel die üblichen folgenden Merkmale mit:

- Eine einfache Klick-Umgebung zum Erstellen der Malware.
- Die Möglichkeit den Angriff in unterschiedlichen Sprachen zu gestalten.
- Ein webbasiertes Dashboard zum Verwalten der durch die infizierten Systeme anfallenden Daten.
- Eine Schnittstelle, mit deren Hilfe sich die Verbreitung der Malware über E-Mail, Online-Werbung oder soziale Netzwerke vereinfachen lässt.

Bekannte Crimeware Kits sind unter anderem Angler, Nuclear, RIG, Sweet Orange, Zeus, MPack, Neosploit, BlackHole, Nukesploit P4ck und Phoenix.