Exhibit 31

CYPHORT™

WHITE PAPER

Ransomware Tactics & Detection Techniques

Contents

Ransomware Evolution

Ransomware is one of the most pervasive and destructive threats that organizations and individuals face today. It is malware that takes your computer or its data hostage and demands the payment of a ransom to return control of the computer or restore the data.

Over the years, ransomware evolved to take many forms, the goal being the same: extort a ransom from the victims.

- **Application-level Lockers:** Some ransomware prevents victims from using their computer. Reveton, for instance, prevents users from logging in and displays a note purporting to be from a law enforcement agency and demands payment of a "fine" to unlock the computer. Others, such as the Manifesto or Ransom Locker, display a ransom note and prevent the user from doing anything else on their computer. Other ransomware can hijack the browser and make it look like you cannot browse to any other site until the ransom is paid.
- **System-level lockers:** Some ransomware like Petya or PetrWrap will overwrite the Master Boot Record with its own mini kernel and render the computer useless except for dealing with the ransom. Other ransomware in this category include HDDCryptor, GoldenEye and Satana.
- **File encryptors:** This category has become the most widespread of all ransomware and is today the method of choice for cyber criminals. It consists of encrypting user files and demanding a ransom for the encryption key. There are many notable examples in this category, like Cryptowall, TeslaCrypt, Cerber, TeslaCrypt, Radamant, KeRanger and WannaCrypt0r.
- **Fake ransomware:** This type doesn't actually encrypt data or hold any resource captive while asking for a ransom. Instead, it rides on the popularity of other ransomware and uses scare tactics to trick its victims into paying.

Although ransomware is not new, it has grown exponentially in the past few years given the success some of the campaigns have enjoyed. The table below shows that we have gone from almost nothing in 2012 to a plethora of ransomware in 2017.

Although ransomware is not new, it has grown exponentially in the past few years given the success some of the campaigns have enjoyed. The table below shows that we have gone from almost nothing in 2012 to a plethora of ransomware in 2017.

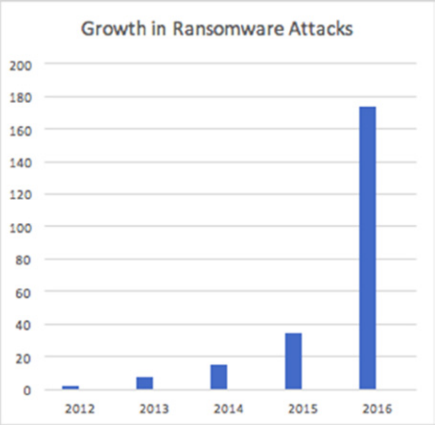
Year	2012	2013	2014	2015	2016
Count of ransomware families	2	8	15	35	174
Most prominent ransomware	Rannoh, Reveton	CryptoLocker, Kovter, Urausy	CryptoWall, CryptoLocker, CBT-Locker	TeslaCrypt, DMA-Locker, Cryptonite	Cerber, Locky, CryptXXX

The continued growth of ransomware is driven by several key factors:

- **Efficacy of the threat.** Many victims depend on the data that's taken hostage to run the day to day operations of their business. If the victim has no backup, their only remedy is to pay the ransom and hope they can recover the data.
- **Time pressure.** In most cases, time is on the side of the attacker. A hospital or airline, for example, may not be able to sustain a non-functional IT infrastructure for too long. To make matters worse, many ransomware attacks rely on clever tactics to push victims to pay quickly: ransom amounts may double after some time, files may start getting deleted every hour, all files deleted after a certain deadline.

- **Success rate of previous campaigns.** According to many sources, the ransomware economy has reached $1B in 2016. CryptoLocker alone has raked more than $390M in 2016 by infecting an average of 90,000 victims a day.

- **Availability of CryptoCurrency.** It is important for cyber criminals to launder their proceeds from the ransoms and crypto currency makes it somewhat easier. Bitcoin is the currency of choice and even though transactions on Bitcoin wallets are public, it's almost impossible to track the parties to a transaction.



- **Exploit Kits.** The availability of very successful exploit kits, mainly Angler, Nuclear, Neutrino and RIG made it relatively painless for ransomware actors to deliver their payloads over proven infection methods.

Infection Vectors

Email

Email remains the number 1 method of delivery of ransomware. Using a very convincing message, cyber criminals may get a victim to open an email attachment or click on a link that ultimately leads to the infection.

Email Attachment

Usually these attachments take the form of a Word document purporting to be a shipment notification, which in fact contains malicious obfuscated Visual Basic script. The VB script will either embed the ransomware binary in its own data and proceed to decrypt it and write it to disk then launch it, or it will reach out to a web site to download the ransomware binary then execute it.

The Locky campaign was particularly successful at attaching a malicious JavaScript code inside a zip file to emails. The script files will have file extensions that seem to be documents to entice the victim to open them. The script would then download the ransomware from the internet and launch it.

Sometimes, the attachments will attempt to take advantage of a vulnerability in the handler application. For example, a malicious PDF could attempt to exploit an unpatched or zero-day vulnerability in Adobe Acrobat Reader, drop the ransomware binary, then execute it. The same goes for Microsoft Office documents. This approach has nonetheless diminished lately due to the low number of known vulnerabilities that are unpatched.

Sometimes the Office or PDF attachments contain nothing but links to a website which hosts the ransomware. This method is rarely used because it requires the user to interact with the downloaded file and agree to execute it, which raises suspicion of the victim.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

WHAT WILL YOU BUILD? | sales@docketalarm.com | 1-866-77-FASTCASE

fastcase®
Smarter legal research.