PETYA OR NOT PETYA? IT ALL JUST MAKES YOU WANNACRY!

Sujit Raman
Associate Deputy Attorney General
U.S. Department of Justice
The Changing Ransomware Landscape

1. **Installation**
   Victim opens a malicious email attachment or visits a compromised website

2. **Contact**
   Malware contacts actor’s server

3. **Encryption**
   Malware encrypts victim’s files

4. **Extortion**
   Message on victim’s computer displays ransom deadline and amount to be paid using electronic currency

Credit: FBI Cyber Division
The Changing Ransomware Landscape

**2016:** Explosive growth in families, variants, detections, demands.

**2017:** Reported declines in large-scale campaigns; two unprecedented global outbreaks; emergence of more targeted families.
The Changing Ransomware Landscape

2017: Why the decline in detections?

- Virtual disappearance of exploit kits
- Declining efficacy of malspam campaigns
- Move to cryptocurrency miners and other forms of malware
- But: according to Trend Micro, total new ransomware families continued to rise

Credit: FBI Internet Crime Complaint Center (IC3)
# The Changing Ransomware Landscape

It’s another quarter of diminishing returns for ransomware authors. They still have some interesting tricks and tactics being deployed to part potential victims with their files.

Credit: Malwarebytes Labs (Q1 2018 Report)
The Changing Ransomware Landscape

2017: Observed Trends

- Increased use by nation-state actors
- Continued rise in new families
- Rise in ransomware as a service
- Increased exploitation of RDP vulnerabilities
- Diversification of accepted cryptocurrencies
- Increased sophistication
- Ransomware can be repurposed (e.g., as a denial & deception tool)
WannaCry

200,000+ Systems Affected by WannaCry Ransom Attack

The WannaCry ransomware attack in numbers

- Affected systems: >220,000
- Affected countries: 150
- Ransom per system: $300

Average ransom in past ransomware attacks

| Year | Ransom
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>2014</td>
<td>$373</td>
</tr>
<tr>
<td>2015</td>
<td>$294</td>
</tr>
<tr>
<td>2016</td>
<td>$1,007</td>
</tr>
</tbody>
</table>

Approx. ransom in major ransomware threats

- Feb ‘16 Locky: $965
- Mar ‘16 Cerber: $1,200
- Apr ‘16 CryptXXX: $500

Sources: Media reports, Symantec

- May 2017
- Attack ebbed when kill switch discovered.
- # of US victims relatively low.
NotPetya

- June 2017
- Destructive malware disguised as ransomware
- Multinational victims; millions of $ in losses

Credit: www.bankinfosecurity.com
The Changing Ransomware Landscape

WannaCry & NotPetya: **Notable characteristics**

- Required minimal human interaction to infect other computers, execute, or encrypt data for ransom
- Very high profile; exposed as unreliable quite early
- Neither was well-executed or well-targeted
- More likely the exception rather than the rule
- Contrast to malware campaigns that are better positioned to produce the conditions necessary for (1) high payment rates and (2) high ransoms
## Top Designated FBI Ransomware Families

<table>
<thead>
<tr>
<th>Family</th>
<th>Version</th>
<th>Payment Method</th>
<th>Additional Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSIL/Samas.A (Samsam)</td>
<td>1</td>
<td>Bitcoin</td>
<td>Exploits vulnerabilities in JBOSS (a server platform that hosts Java apps and services)</td>
</tr>
<tr>
<td>Locky</td>
<td>1</td>
<td>Bitcoin</td>
<td>Uses Necurs botnet for distribution and has multiple extensions: .osiris, .zepto, .zzzzz</td>
</tr>
<tr>
<td>DMA Locker</td>
<td>4</td>
<td>Bitcoin</td>
<td>Current version is 3.0 but the actors have already developed 4.0.</td>
</tr>
<tr>
<td>Cerber</td>
<td>5</td>
<td>Bitcoin</td>
<td>Encrypts with a random 4 letter extension and maintains a distributor portal</td>
</tr>
<tr>
<td>CrySiS</td>
<td>4</td>
<td>Bitcoin</td>
<td>Uses brute force RDP and newest version uses extension .wallet</td>
</tr>
</tbody>
</table>

Credit: FBI Cyber Division
Samsam, unlike more conventional ransomware, is not delivered through drive-by-downloads or emails. Instead, the attackers behind Samsam use tools such as Jboss to identify unpatched servers running Red Hat’s JBoss enterprise products. Once the attackers have successfully gained entry into one of these servers by exploiting vulnerabilities in JBoss, they use other freely available tools and scripts to collect credentials and gather information on networked computers. Then they deploy their ransomware to encrypt files on these systems before demanding a ransom. The Samsam ransomware also differs from other ransomware due to the fact that the attackers generate the RSA key pair themselves. Most crypto-ransomware will contact a command and control server, which will generate an RSA key pair and send the public key back in order to encrypt files on the infected computers. With Samsam, the attackers generate the key pair and upload the public key along with the ransomware to the targeted computers.

Credit: FBI Cyber Division
Samsam – victims by industry sector

- Trade, Transportation, and Utilities: 24%
- Education: 19%
- Manufacturing: 14%
- Professional and Business Services: 10%
- Health Services: 14%
- Construction: 9%
- Information: 5%
- Government: 5%
- Education: 19%
- Trade, Transportation, and Utilities: 24%
Locky is one of the current volume leaders in the ransomware market. Using a Ransomware as a Service model, they build the malware and the payment infrastructure, which is hosted on TOR. Affiliates buy the service, and are responsible for distribution, which is why Locky has been distributed via Malicious documents, Flash exploits, zips containing exploits, and exploit kits, and has leveraged at least Dridex and Necurs for distribution.
Locky – victims by industry sector

- Trade, Transportation, and Utilities: 14%
- Manufacturing: 10%
- Financial Activities: 9%
- Professional and Business Services: 24%
- Government: 17%
- Health Services: 11%
- Manufacturing: 10%
- Financial Activities: 9%
- Professional and Business Services: 24%
- Government: 17%
- Health Services: 11%

- Trade, Transportation, and Utilities: 14%
- Manufacturing: 10%
- Financial Activities: 9%
- Professional and Business Services: 24%
- Government: 17%
- Health Services: 11%
- Manufacturing: 10%
- Financial Activities: 9%
- Professional and Business Services: 24%
- Government: 17%
- Health Services: 11%

- Trade, Transportation, and Utilities: 14%
- Manufacturing: 10%
- Financial Activities: 9%
- Professional and Business Services: 24%
- Government: 17%
- Health Services: 11%
- Manufacturing: 10%
- Financial Activities: 9%
- Professional and Business Services: 24%
- Government: 17%
- Health Services: 11%
DMA Locker

All your personal files are LOCKED!

WHAT'S HAPPENED?
- All your important files (including hard disks, network disks, flash, USB) are encrypted.
- All files are locked with asymmetric algorithm using AES-256 and then RSA-2048 cipher.
- You are not possible to unlock your files because all your backups are removed.
- Only way to unlock your files is to pay at 7600 GBP in Bitcoin currency (10 BTC).
- After payment we will send you decryption key automatically, which allows you to unlock files.

HOW TO PAY US AND UNLOCK YOUR FILES?
1. If you want a proof that after payment your files will be unlocked, you can send us your 2 small files with size < 1 MB via e-mail and we will encrypt it and send you back FOR FREE.
2. To pay us, you have to use Bitcoin currency. You can easily buy bitcoins at following sites:
   - https://www.coinfloor.co.uk/
   - https://local-bitcoin.com/
   - https://www.coinbase.com/
3. If you already have bitcoins, pay us 10 BTC (7600 GBP) on following Bitcoin address:
4. After payment, securely contact us to get your decryption key:
   - week4064@gmail.com
   - In mail title write your unique ID.

OMALOCK:
5. We will automatically send you decryption key file after bitcoins transfer.
   - When you receive your decryption key file, press "OPEN" button and choose your received decryption key file.
   - Then, press the "UNLOCK FILES" button and it will start unlocking all your files.

DECRYPTION KEY FILE:

KEY STATUS:

UNLOCK FILES
DMA Locker – victims by industry sector

- Construction: 31
- Education...: 31
- Financial Activities: 30
- Government: 51
- Health Services: 95
- Professional and Business Services: 147
- Trade, Transportation, and Utilities: 74
- Other: 25
- Natural Resources and Mining: 4
- Manufacturing: 43
- Leisure and Hospitality: 22
- Information: 13
- Individual: 60
Cerber, which is best known for its high-creep factor in using text-to-speech to "speak" its ransom note to victims, was first spotted in the wild in February. Its typical distribution method was via exploit kits, with Magnitude and Nuclear Pack exploiting a zero day in Adobe Flash Player (CVE-2016-1019). But as recently as May 4, FireEye reports, Cerber is now part of a spam campaign linked to Dridex botnets.
Cerber – victims by industry sector (and country)

- Information: 2%
- Construction: 2%
- Government: 2%
- Education: 4%
- Other: 4%
- Manufacturing: 5%
- Leisure and Hospitality: 6%
- Health Services: 6%
- Financial Activities: 7%
- Trade, Transportation, and Utilities: 7%
- Professional and Business Services: 20%
- Individual: 35%

Cerber Distribution By Country:

- US: 16%
- Turkey: 10%
- GB: 4%
- Israel: 2%
- Taiwan: 2%
- Canada: 2%
- Germany: 2%
- Italy: 2%
- Czech Republic: 2%
- France: 2%
- Other: 15%
CrySiS

Attention!
Your computer has been encrypted by cryptographically strong algorithm. All your files are now encrypted. You have only one way to get them back safely - using original decryption tool. Using another tools (back-ups, recovery soft and others) could corrupt your files, in case of using third party software we don't give guarantees that full recovery is possible, so use it on your own risk.

To get original decryptor contact us with email. In subject line write your ID, which you can find in name of every encrypted file, also attach to email 3 encrypted files. (files have to be less than 2 MB.)

JohnnyCryptor@hackermail.com

It is in your interest to respond as soon as possible to ensure the restoration of your files, because we won't keep your decryption keys at our servers more than one week in interest of our security.
P.S. only in case you don't receive a response from the first email address within 24 hours, please use this alternative email address.

JohnnyCryptor@india.com

Also you can contact us with questions about our old builds:
ppaycrypt
cryptopay
CrySiS – victims by industry sector

- Health Services: 27%
- Professional and Business Services: 33%
- Trade, Transportation, and Utilities: 18%
- Government: 18%
- Construction: 4%
- Other: 5%
- Manufacturing: 1%
- Leisure and Hospitality: 1%
Next Big Threat?

Crypto-Jacking:

• Secret use of your computing device to mine cryptocurrency
• Daily rise in new cryptocurrencies
• IoT devices at risk
• Websites that exploit visitors
• In December 2017, Check Point announced that crypto-miners had impacted 55% of organizations globally
What is the government doing about this?

- Targeting dark marketplaces
- Opening investigations on new families
- Leveraging resources to identify ransomware infrastructure
- Partnering with private industry to increase ransomware awareness
What can you do?

Key areas to focus on with ransomware are prevention, business continuity, and remediation. As ransomware attacks continue to evolve and become more sophisticated, even with the most robust prevention controls in place, there is no guarantee against exploitation. This makes contingency and remediation planning crucial to business recovery and continuity.

**Prevention Considerations**
- Implement an awareness and training program. Because end users are targeted, employees and individuals should be made aware of the threat of ransomware and how it is delivered.
- Patch operating systems, software, and firmware on devices, which may be made easier through a centralized patch management system.
- Ensure anti-virus and anti-malware solutions are set to automatically update and that regular scans are conducted.
- Manage the use of privileged accounts. Implement the principle of least privilege: no users should be assigned administrative access unless absolutely needed; those with a need for administrator accounts should only use them when necessary.
- Configure access controls, including file, directory, and network share permissions, with least privilege in mind. If a user only needs to read specific files, they should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via e-mail. Consider using Office Viewer software to open Microsoft Office files transmitted via e-mail instead of full Office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

**Business Continuity Considerations**
- Back up data regularly, and regularly verify the integrity of those backups.
- Secure your backups. Ensure backups are not connected to the computers and networks they are backing up. Examples might be securing backups in the cloud or physically storing offline. Some instances of ransomware have the capability to lock cloud-based backups when systems continuously back up in real time, also known as persistent synchronization. Backups are critical in ransomware if you are infected, this may be the best way to recover your critical data.

**Other Considerations**
- Implement application whitelisting only allow systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical/logical separation of networks and data for different organizational units.

**The Ransom**

The FBI does not support paying a ransom to the adversary. Paying a ransom does not guarantee that an organization will regain access to their data; in fact, some individuals or organizations were never provided with decryption keys after having paid a ransom. Paying a ransom emboldens the adversary to target other organizations for profit, and provides for a lucrative environment for other criminals to become involved. While the FBI does not support paying a ransom, there is an understanding that when businesses are faced with an inability to function, executives will evaluate all options to protect their shareholders, employees, and customers.

In all cases the FBI encourages organizations to contact a local FBI field office immediately to report a ransomware event and request assistance. Victims are also encouraged to report cyber incidents to the FBI’s Internet Crime Complaint Center (www.ic3.gov).
PETYA OR NOT PETYA? IT ALL JUST MAKES YOU WANNACRY!

Sujit Raman
Associate Deputy Attorney General
U.S. Department of Justice