

RSA®Conference2018

San Francisco | April 16 – 20 | Moscone Center

SESSION ID: SEM-M03

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

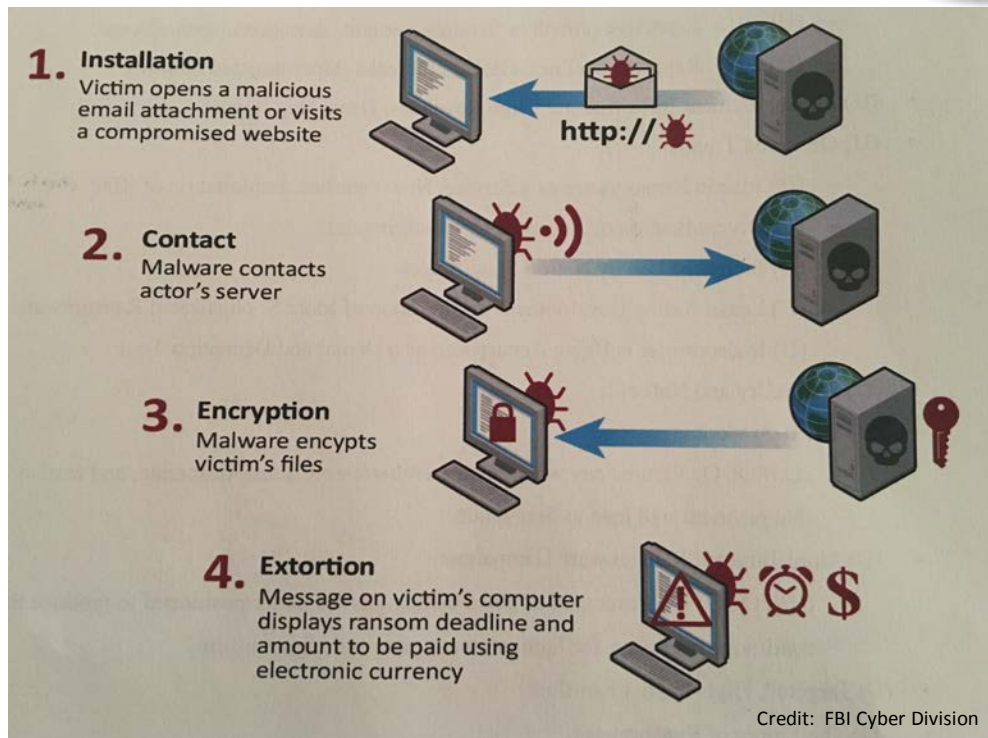
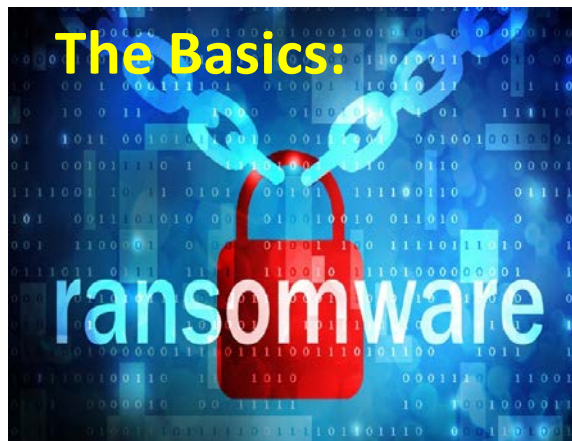
Sujit Raman

Associate Deputy Attorney General
U.S. Department of Justice

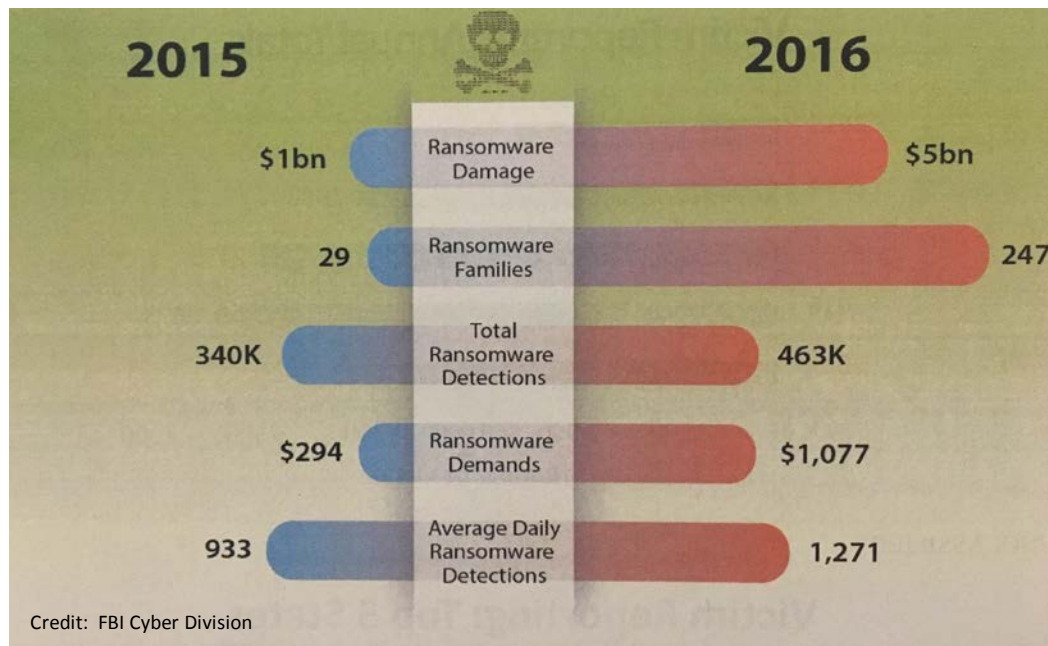


#RSAC

The Changing Ransomware Landscape



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



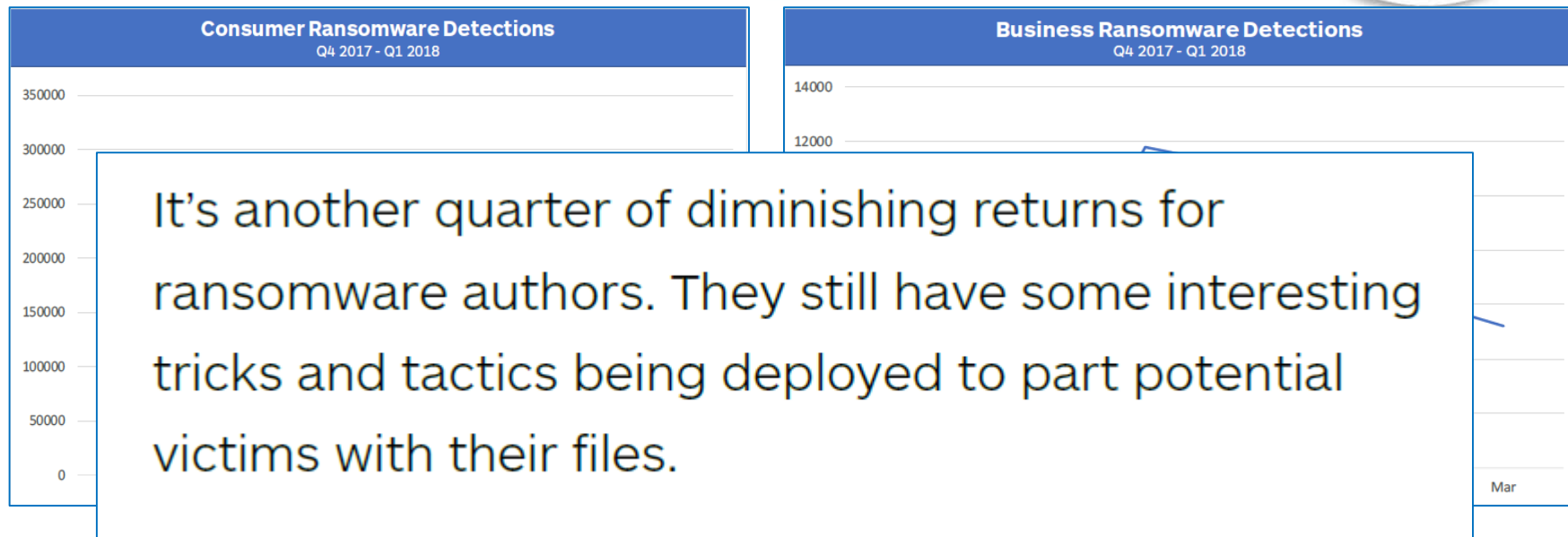
Credit: FBI Internet Crime Complaint Center (IC3)

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



The Changing Ransomware Landscape



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

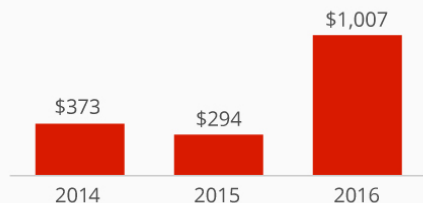


200,000+ Systems Affected by WannaCry Ransom Attack

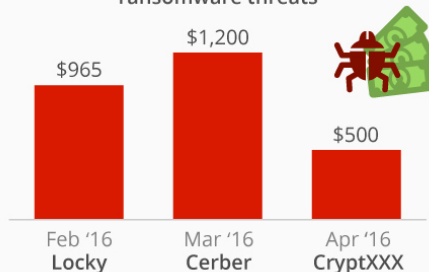
The WannaCry ransomware attack in numbers



Average ransom in past ransomware attacks



Approx. ransom in major ransomware threats



@StatistaCharts Sources: Media reports, Symantec

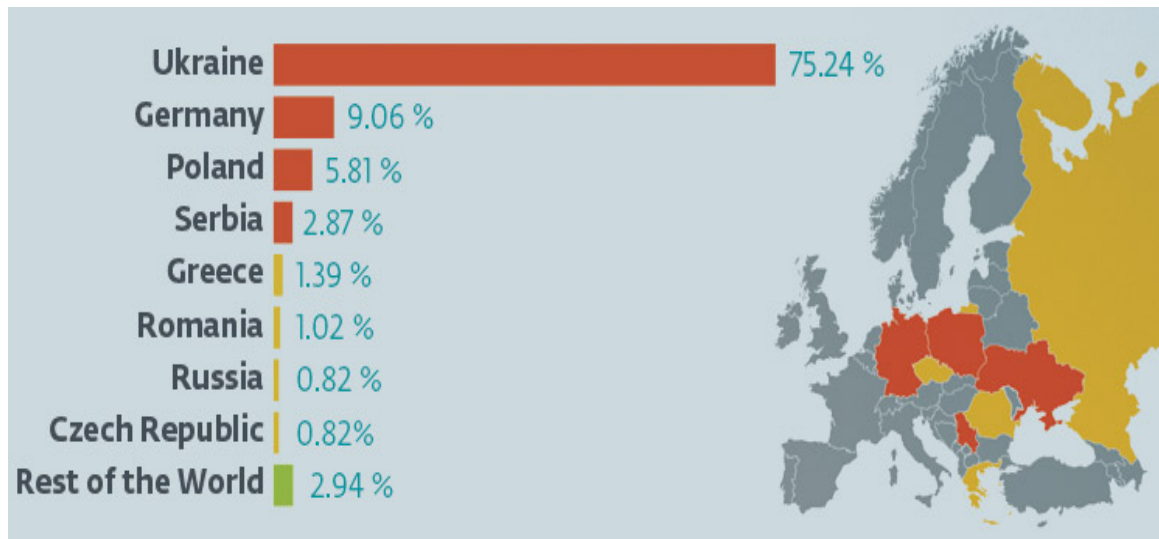
statista



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



NotPetya



Credit: www.bankinfosecurity.com



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



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



MSIL/Samas.A (Samsam)

Version 1
Payment Method
Bitcoin



Exploits vulnerabilities in
JBoss
(a server platform that
hosts Java apps and
services)

Locky

Version 1
Payment Method
Bitcoin



Uses Necurs botnet
for distribution and
has multiple
extensions: .osiris,
.zepto, .zzzzz

DMA Locker

Version 4
Payment Method
Bitcoin



Current version is 3.0 but
the actors have already
developed 4.0.

Cerber

Version 5
Payment Method
Bitcoin



Encrypts with a
random 4 letter
extension and
maintains a distributor
portal

CrySiS

Version 4
Payment Method
Bitcoin



Uses brute force RDP
and newest version
uses extension .wallet

Credit: FBI Cyber Division



MAR 2016

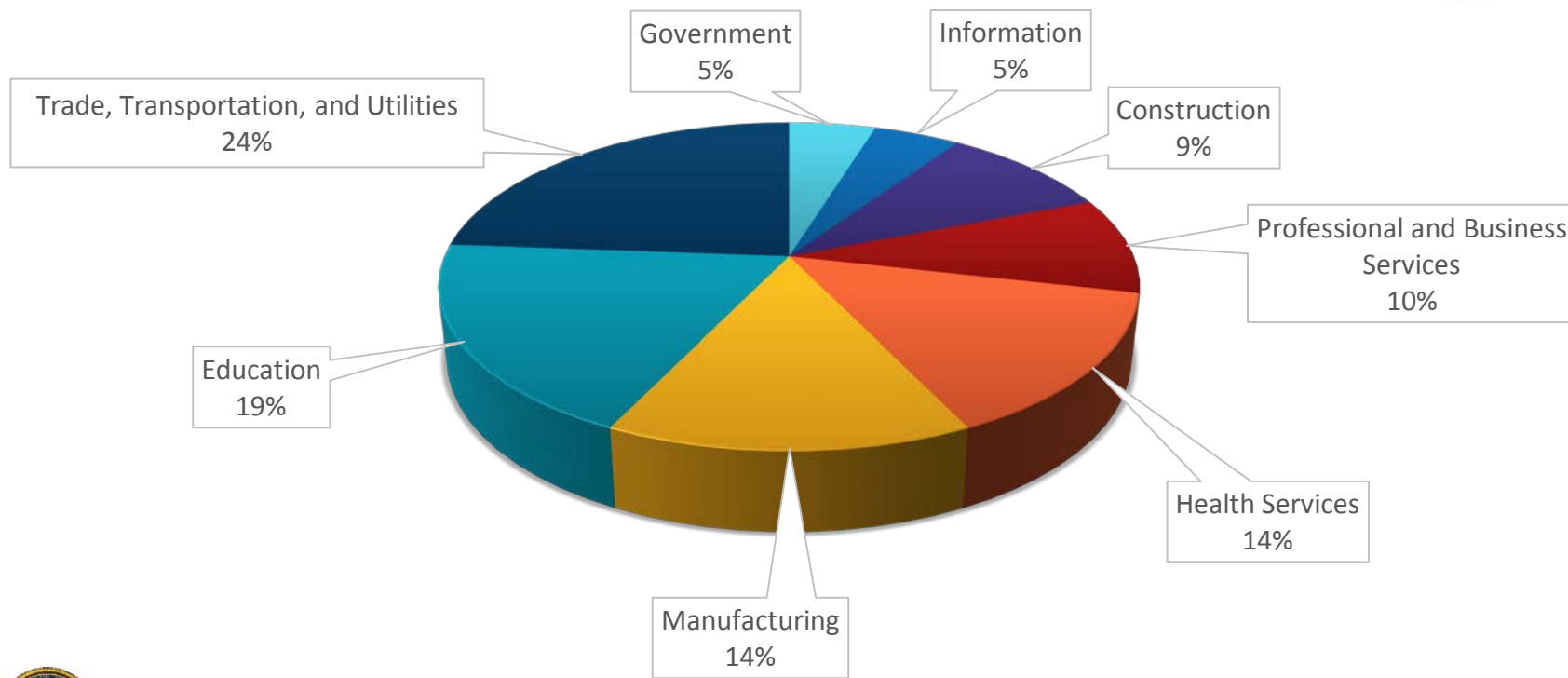
SAMSAM (SAMAS)

Samsam, unlike more conventional ransomware, is not delivered through drive-by-downloads or emails. Instead, the attackers behind Samsam use tools such as Jexboss 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



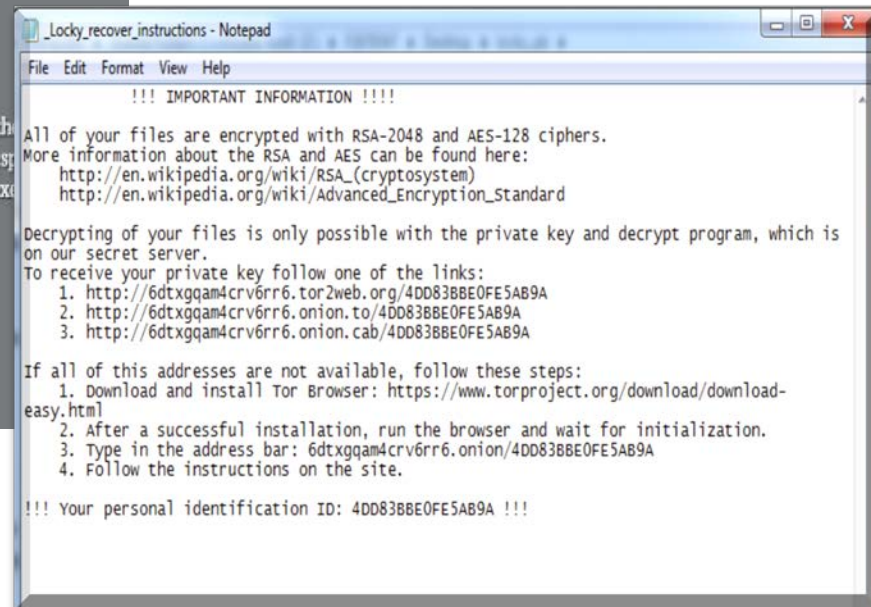
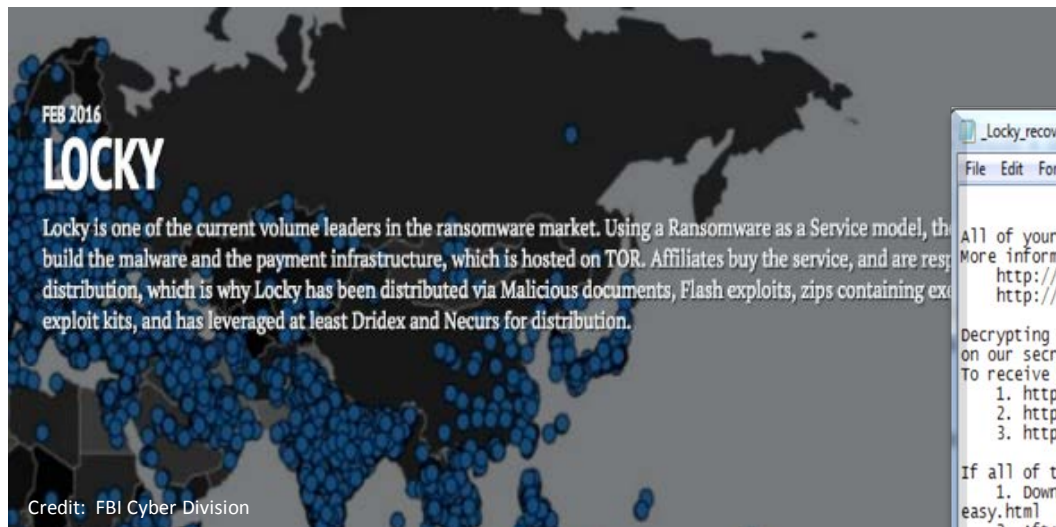
Samsam – victims by industry sector



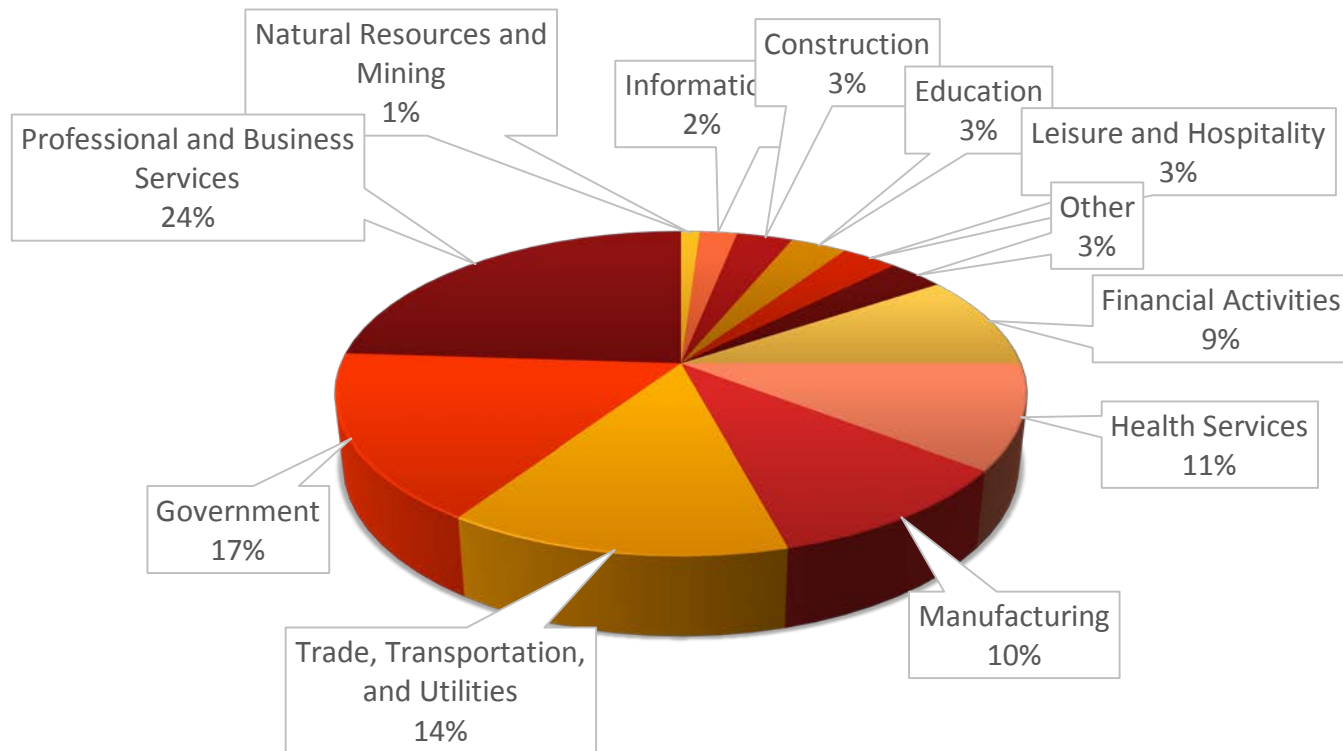
Locky



#RSAC



Locky – victims by industry sector




DMA Locker



#RSAC

DMA Locker 3.0

All your personal files are LOCKED!



WHAT'S HAPPENED?

- * All your important files(including hard disks, network disks, flash, USB) are encrypted.
- * All of 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 us 7000 GBP in Bitcoin currency (10 BTC). After payment we will send you decryption key automatically, which allow you to unlock files .

HOW TO PAY US AND UNLOCK YOUR FILES?

1. If you want a proof that after payment your files will get unlocked, you can send us your 2 small files with size < 1 MB via e-mail and we will decrypt 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://localbitcoins.com/>
 - * <https://www.coinbase.com/>
3. If you already have Bitcoins, pay us 10 BTC (7000 GBP) on following Bitcoin address:
4. After payment, necessarily contact with us to get your decryption key:
week4004@fastmail.com . In mail title write your unique ID:
5. We will automatically send you decryption key file after bitcoin 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:

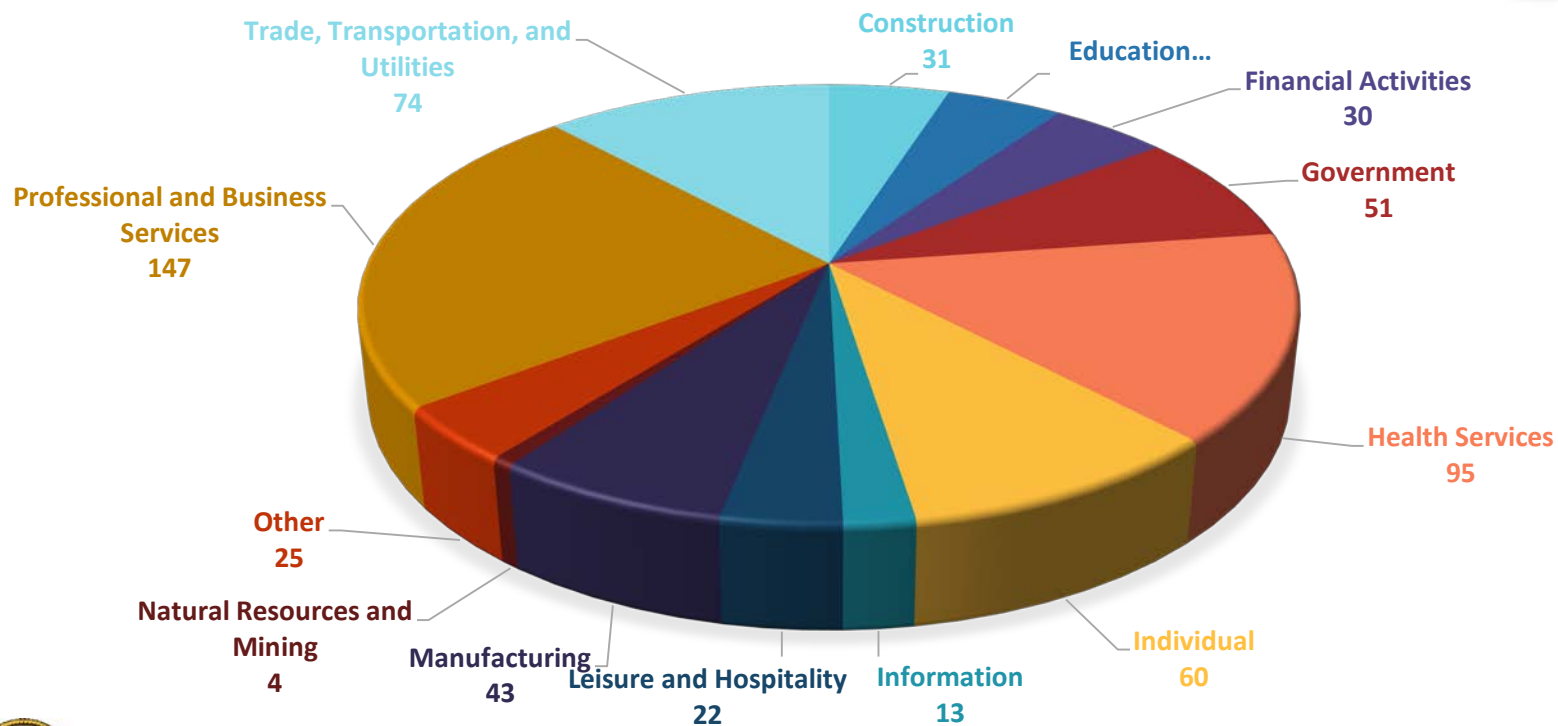
* You have 96 hours to pay us!

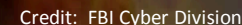
* After this time ransom will grow to 200 percent

* Ransom grow time:
17/2/2017 1:27

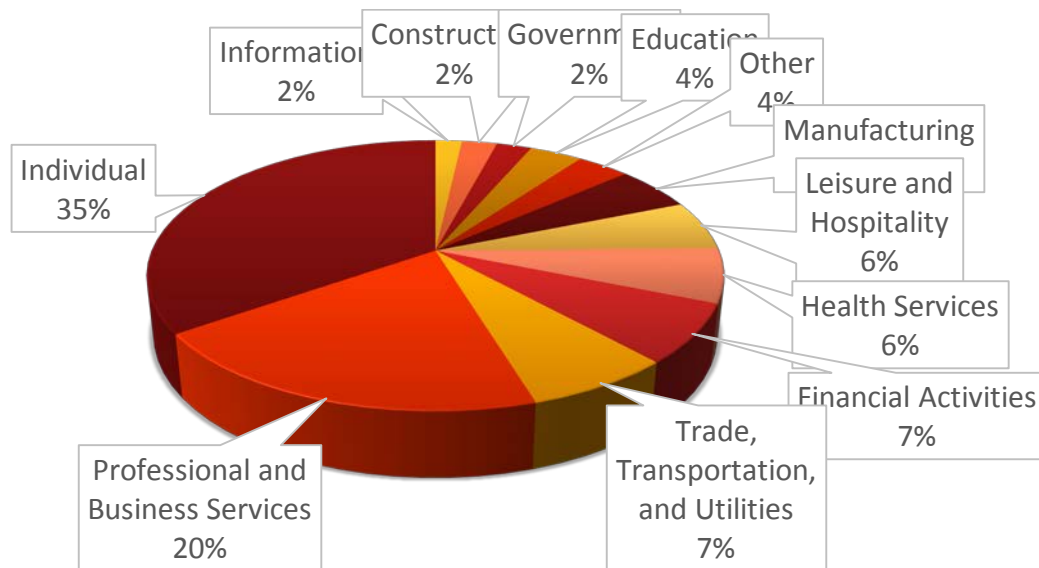
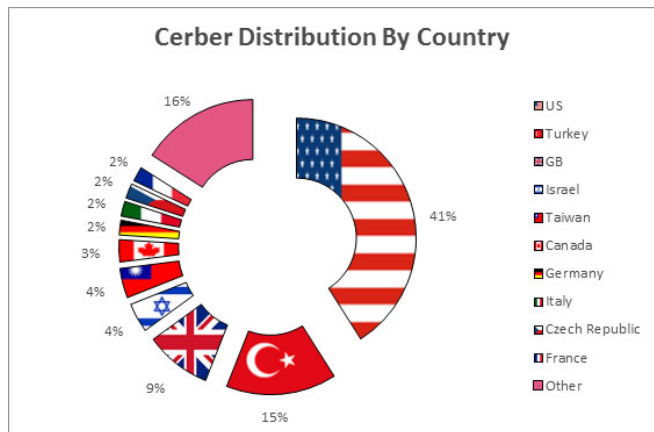


DMA Locker – victims by industry sector





Cerber – victims by industry sector (and country)





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 crypted file, also attach to email 3 crypted 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.

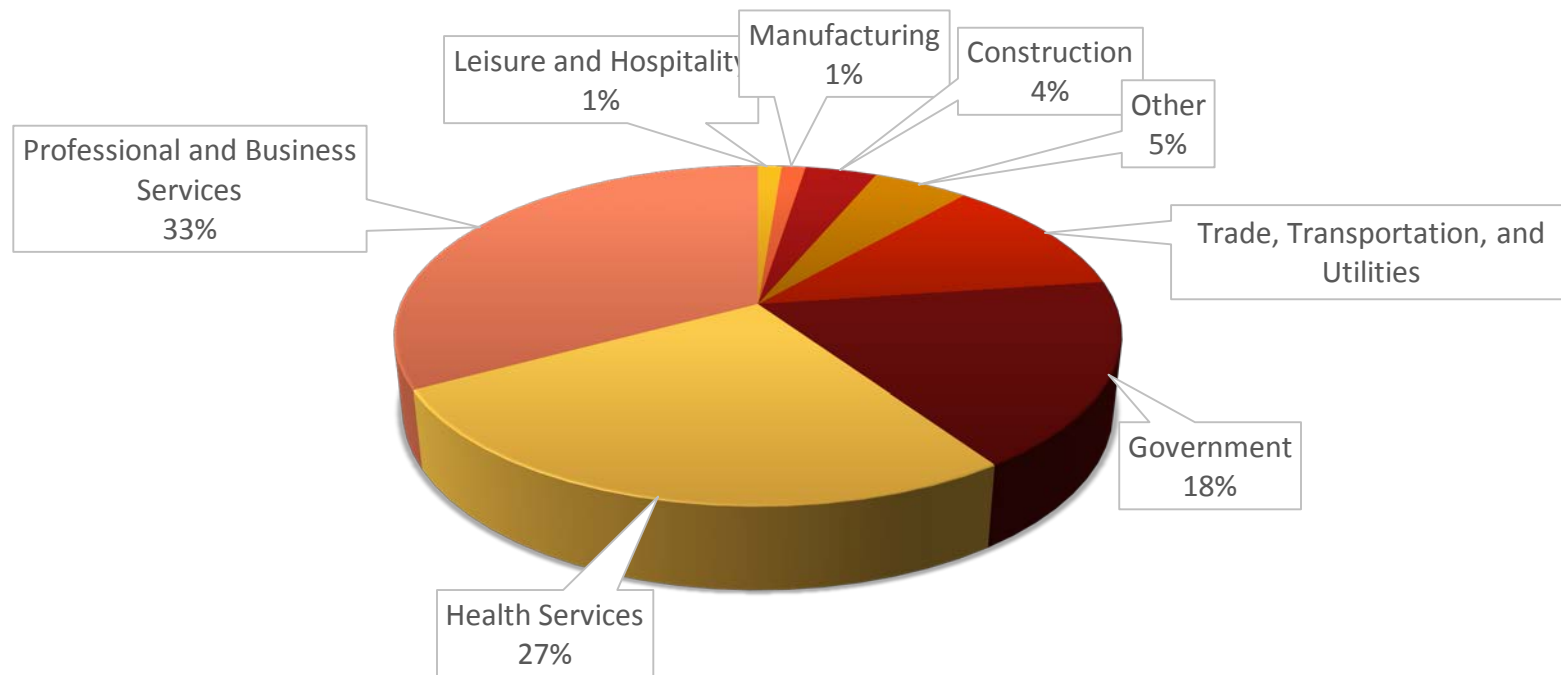
P.S. only in case you don't receive a response from the first email address within 24 hours, please use this alternative email address.

JohnnyCryptor@india.com

Also you can contact us with questions about our old builds:
paycrypt
cryptopay



CrySiS – victims by industry sector



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

JUSTICE NEWS

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE

Thursday, July 20, 2017

AlphaBay, the Largest Online 'Dark Market,' Shut Down

'Dark Net' Site Was Major Source of Fentanyl and Heroin, Linked to Overdose Deaths, and Used By Hundreds of Thousands of People to Buy and Sell Illegal Goods and Services Anonymously over the Internet

The Justice Department today announced the seizure of AlphaBay, a major online dark market that operated for over two years on the dark web and was a source of fentanyl, heroin, counterfeit goods, and other illegal items throughout the world. The international operation involved cooperation and efforts by law enforcement agencies in the United States, United Kingdom, and France, as well as the European



What can you do?



CyberDIVISION FEDERAL BUREAU OF INVESTIGATION

Key areas to focus on with ransomware are prevention, business continuity, and remediation. As ransomware techniques 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 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).



RSA®Conference2018

San Francisco | April 16 – 20 | Moscone Center

SESSION ID: SEM-M03

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

Sujit Raman

Associate Deputy Attorney General
U.S. Department of Justice



#RSAC