UNLV | Howard R. Hughes College of Engineering

USSS Electronic Crimes Task Force Quarterly Meeting

March 3, 2017

Ransomware Risks and Mitigation

Yoohwan Kim, Ph.D., CISSP, CISA, CEH, CPT
Associate Professor
Computer Science Department
University of Nevada Las Vegas

Yoohwan.Kim@unlv.edu
702-895-5348
http://www.egr.unlv.edu/~yoohwan

UNLV University of Nevada Las Vegas

1. Ransomware Landscape

Ransomware

- A type of malware that prevents users from accessing their system, A form of malware that targets your critical data and systems for the purpose of extortion.
  - Either by locking the system's screen or by locking the users' files unless a ransom is paid
  - Crypto-ransomware
- The biggest cybersecurity threat

Who gets hit by ransomware?

- Hospitals
  - Hollywood Presbyterian Medical Center, whose network effectively ground to a halt after hackers breached the system. After relying on pen and paper records briefly, Hollywood Presbyterian paid the **40 bitcoin ($17,000)** ransom to regain control of its network.

http://www.pcmag.com/article2/0,2817,2499469,00.asp

Who gets hit by ransomware?

- Police
  - A police department in Tewksbury, Massachusetts, made a $500 payment after enlisting the help of the FBI.
  - A police computer in Swansea, Massachusetts. The police department decided to pay the ransom of 2 Bitcoins (about $750) rather than try to figure out how to break the lock.

http://www.pcmag.com/article2/0,2817,2499469,00.asp

UNLV
UNIVERSITY OF NEVADA LAS VEGAS

San Francisco Transport system

- Nov 28, 2016
  - By a variant of HDDCryptor to encrypt hard drives and network-shared files, and overwrite the master boot record (MBR)
  - Free rides for all as **100 bitcoin ($73,000)** demanded

Welcome to Las Vegas!

- "Las Vegas, Rust Belt, Hit Hardest By Ransomware"
  - Dark Reading, 12/8/2016
  - Study of 400,000 ransomware by malwarebytes
- Top 10 US Cities for Ransomware Detections
  1. **Las Vegas/Henderson, Nev.**
  2. Memphis, Tenn.
  3. Stockton, Calif.
  4. Detroit, Mich.
  5. Toledo, Ohio
  6. Cleveland, Ohio
  7. Columbus, Ohio
  8. Buffalo, N.Y.
  9. San Antonio, Texas
  10. Fort Wayne, Ind.

http://www.darkreading.com/endpoint/las-vegas-rust-belt-hit-hardest-by-ransomware----------/d/d-id/1327664

UNLV
UNIVERSITY OF NEVADA LAS VEGAS

Ransomware attack growing rapidly

- Check Point's ThreatCloud World Cyber Threat Map
  - 250 million addresses, 11 million malware signatures
  - Ransomware ratio grows
    - **July, 2016: 5.5%** → **Dec 2016: 10.5%**
- Kaspersky Study
  - 1Q, 2016, **2,900** → 3Q 2016, **32,000**
- Ransomware spikes 6,000% in 2016 (IBM security)
- More than 4000 attacks per day in 2016
  - Up from 1000 attacks per day in 2015
- Over 2000 new ransomware every month

http://www.sci-tech-today.com/news/Ransomware-Attacks-Growing-Rapidly/story.xhtml?story_id=12000DEGKW00
http://www.cnbc.com/2016/12/13/ransomware-spiked-6000-in-2016-and-most-victims-paid-the-hackers-ibm-finds.html

Ransom Business is Booming!

- Revenue
  - Cryptowall 3.0 alone: $325 million (according to Cyber Threat Alliance), up to Oct 2015
- FBI: **$209M** in 1Q, 2016
  - Was **$24M** in whole 2015
  - Projected to have surpassed **$1B/year**
- It is becoming more like a genuine business
  - Live customer support
  - Negotiate the fees and deadlines

Why such a boom in ransomware?

1. Money!
   - Virus, worms were for fun
   - Ransomware is purely for money

2. Ransomware as a service
   - Separation of production and distribution
   - Getting easier!

3. Hard to catch the criminal
   - Previous digital crimes (e.g., farming, Zeus) were easier to catch (stealing bank account number, mule, ATM/Camera)
   - Bitcoin is virtual!

Interests within Law Enforcement

- USSS
  - United States Secret Service & Homeland Security Investigations, 10 May 2016 - Ransomware
    - https://www.secretservice.gov/forms/Cybersecurity_Joint_USSS_ECTF_HSI_Ransomware_Advisory.pdf
    - "Unfortunately, we are currently not aware of any particular means to recover the data encrypted"
  - Cyber Hygiene & Cyber Security Recommendations, 10/5/16
    - https://www.secretservice.gov/forms/Cyber-Hygiene.pdf
- FBI
  - Warnings on Ransomware
  - https://www.fbi.gov/investigate/cyber
- Justice
  - How to protect your networks from ransomware
  - https://www.justice.gov/criminal-ccips/file/872771/download

Reporting ransomware incidents

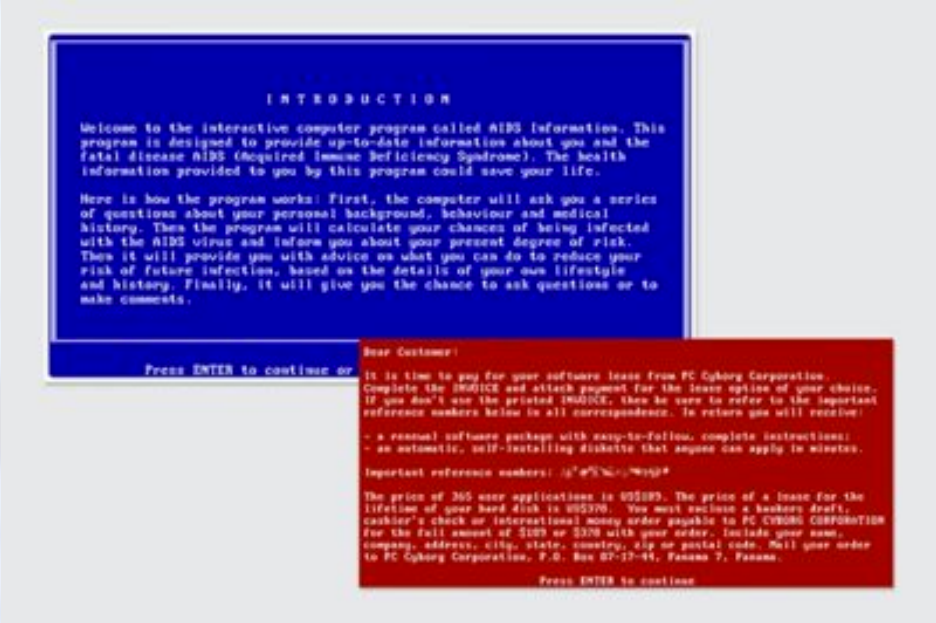
- https://www.ic3.gov/media/2016/160915.aspx
- https://www.ic3.gov/default.aspx

UNLV
UNIVERSITY OF NEVADA LAS VEGAS

2. Ransomware History and Types

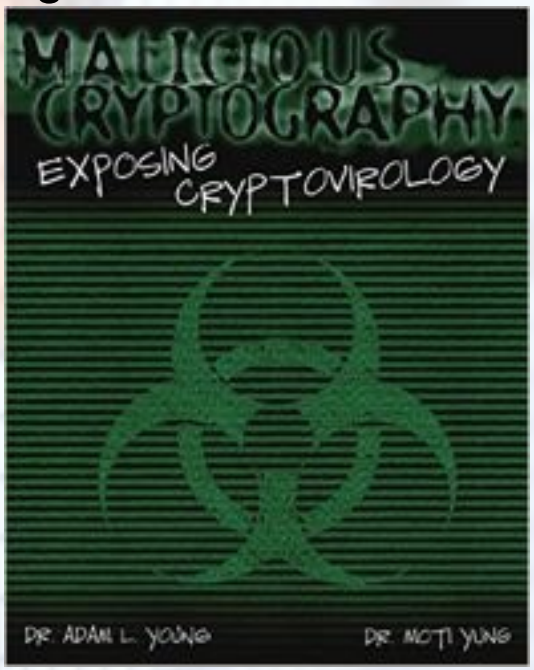
In the ancient times ….

- 1989, AIDS Info Disk Trojan
  - Floppy Disk handed out to 20,000 at WHO conference
  - Demanding $189 to a PO Box in Panama
  - Creator (Dr. Joseph Popp) got arrested
  - Only used symmetric key cryptography



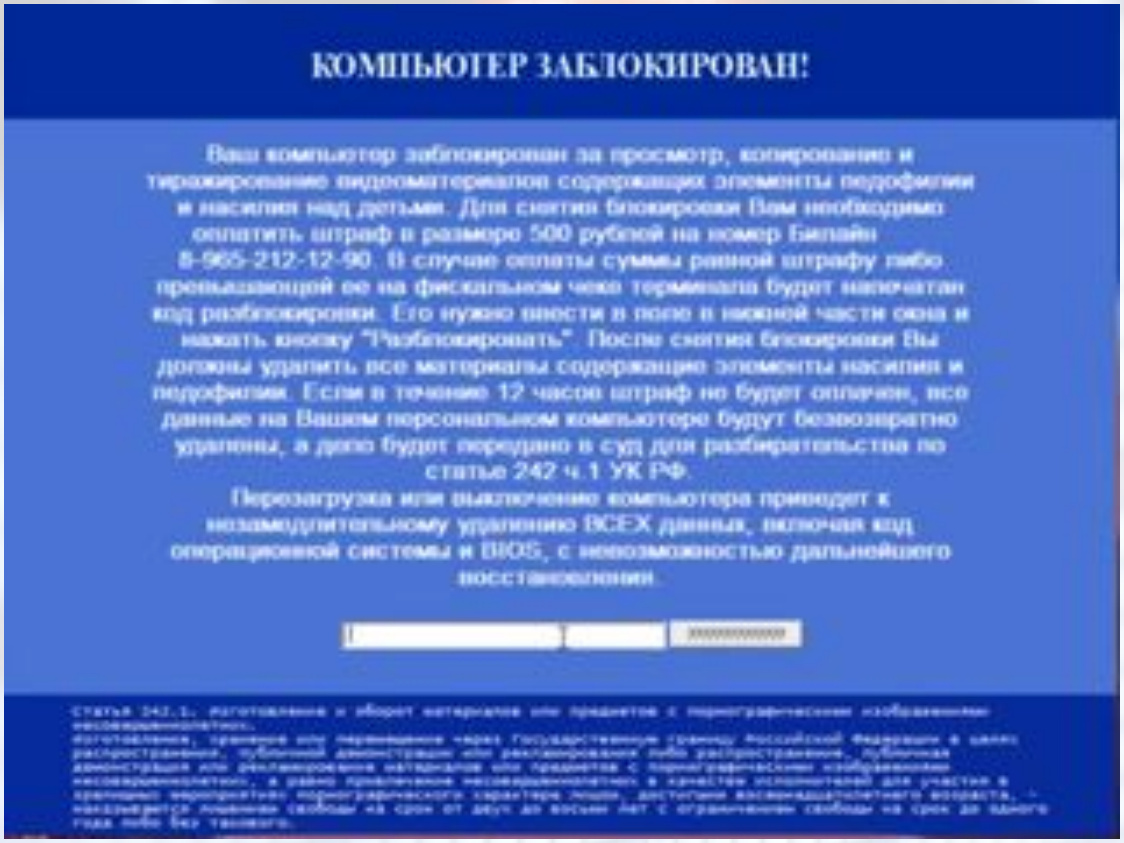
7 years later ….

- In 1996, two researchers Adam Young (Columbia University) and Moti Yung (IBM) published a paper "Cryptovirology: Extortion-Based Security Threats and Countermeasures"
  - Proposed public-key cryptography, making reverse engineering impossible
  - Used the term, "Crypto-viral extortion" and "Cryptovirology"



10 years later ….

- Created by Russian organized criminals in 2005 ~ 2006
- Demanded $300 transfer to E-Gold



UNLV
UNIVERSITY OF NEVADA LAS VEGAS

Finally the word “Ransomware”!

- Network World, Sep 26, 2005
  - “Files for ransom”, Susan Schaibly
- 2005 - 2006
  - Several Ransomware Trojans : Gpcode, TROJ.RANSOM.A, Archiveus, Krotten, Cryzip, MayArchive
  - Gpcode.AG was encrypted with a 660-bit RSA public key.
  - June 2008, Gpcode.AK was encrypted with 1024-bit RSA key
- The payment methods
  - Gpcoder (2005): Demanded a ransom of $100~200 to an **e-gold or Liberty Reserve account.**
    - E-gold: digital gold currency (Banned in 2009)
    - Liberty Reserve: Costa Rica-based digital currency

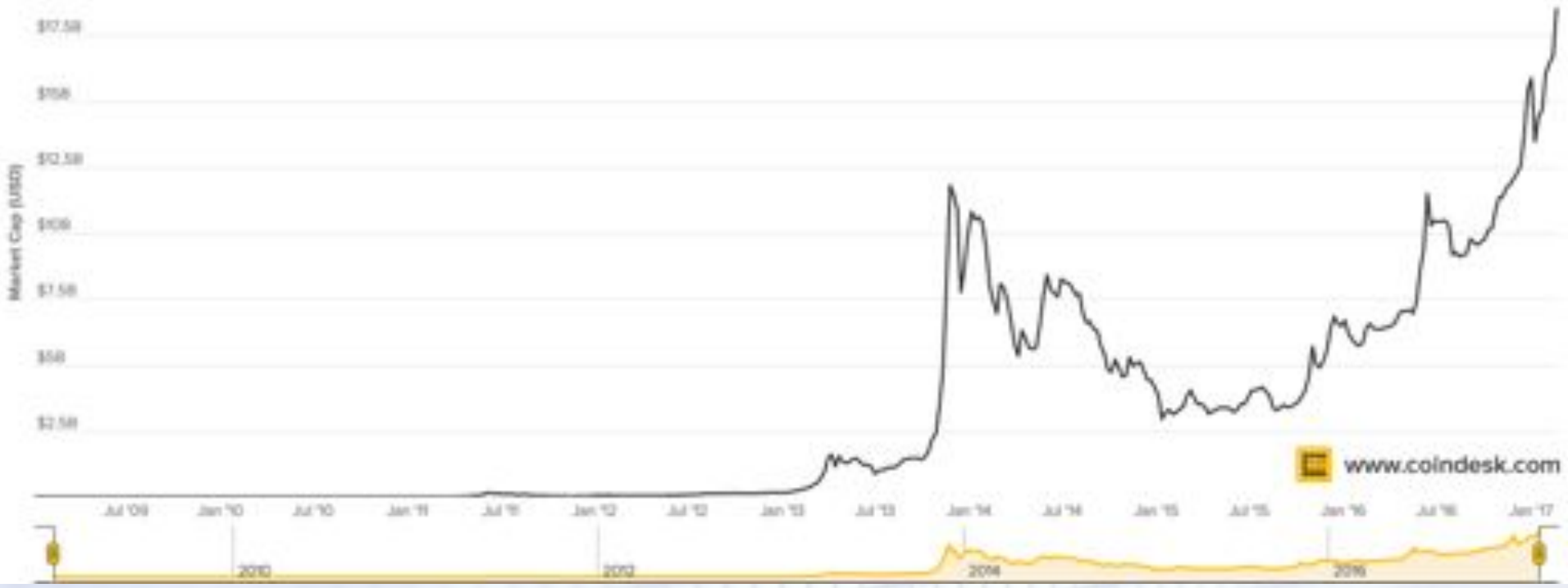
Police Ransomware / FBI Ransomware

- Reveton (2012) is a ransomware that impersonates law enforcement agencies. (not crypto-ransomware)
  - Show a notification from law enforcement, informing them that they were caught doing an illegal activity online (child porn, etc). Threatened to arrest. Locked screen.
  - Contact at fines@fbi.gov
  - Demand payments through **Ukash, PaySafeCard, MoneyPak**

UNLV UNIVERSITY OF NEVADA LAS VEGAS

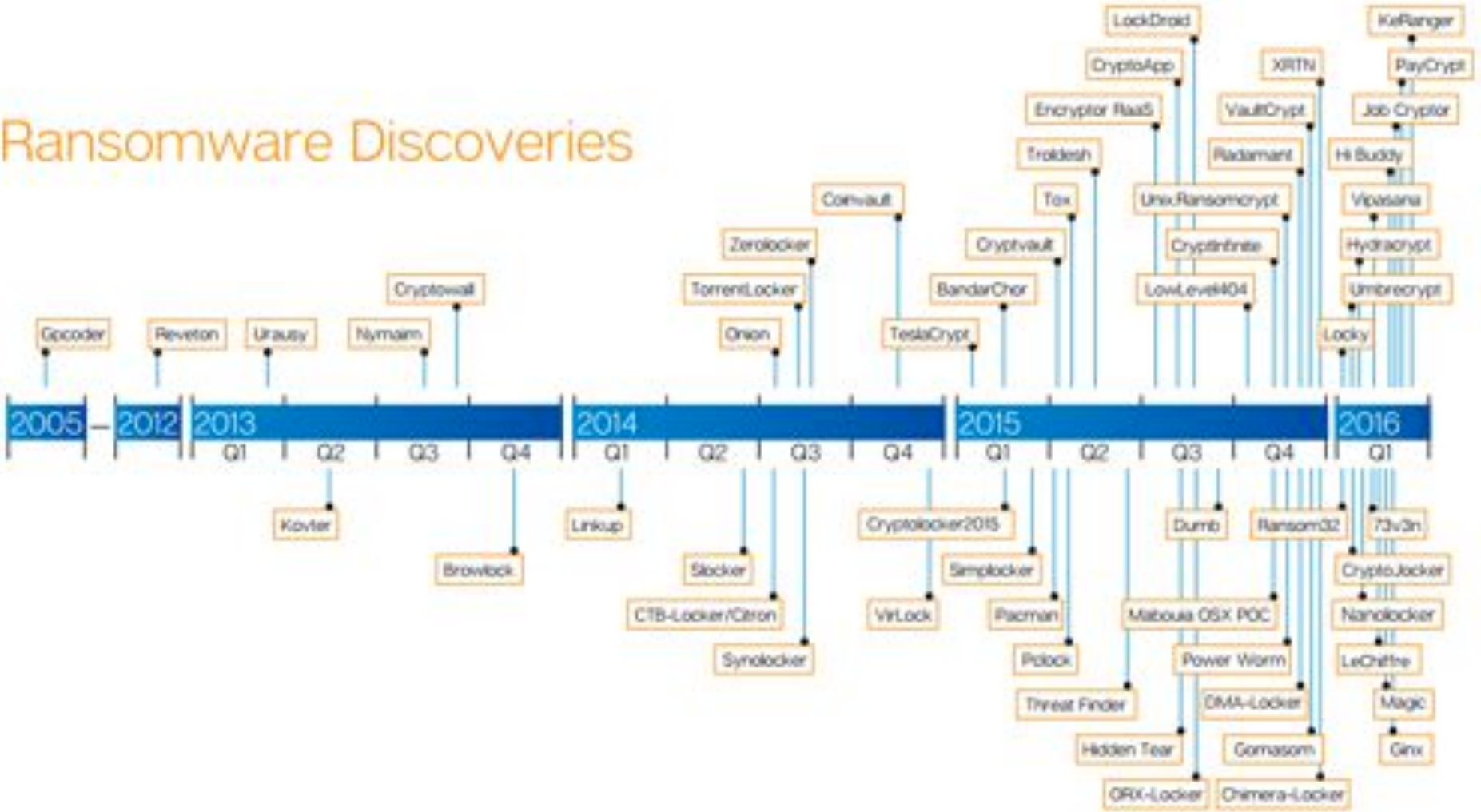
The Big Bang – Birth of Bitcoin

- Introduced on Oct 31, 2008
- Release as open source software in January 3, 2009



UNLV
UNIVERSITY OF NEVADA LAS VEGAS

Thanks to Bitcoin…



https://heimdalsecurity.com/blog/wp-content/uploads/ransomware-discoveries-CERT-RO-2.png

The First Major Ransomware

- 2013, Cryptolocker
  - Crypto-ransomware
  - Spread via an email purporting to
  - Demanded $400 in bitcoin in 72 hours
  - Infected half million, 1.3% paid
  - Estimated payment of $27M

- Operation Tovar
  - International collaboration to crack down Gameover Zeus botnet and Cryptolocker
  - Russian hacker got charged
  - The captured information allowed 500,000 victims to find the key without paying ransom

Copycats

- CryptoDefense
  - After 4 days the ransom doubled
  - Poorly implemented - Left decryption key!

- 2014, Cryptowall
  - Improved version
  - Contains junk code and anti-emulation features (anti-AV)
  - Demanded $500 in Bitcoin
  - Provided decryption of one file for verification via a TOR
  - Variants: Cryptorbit, CryptoDefense, Cryptowall 2.0, Cryptowall 3.0 (uses I2P network proxies)

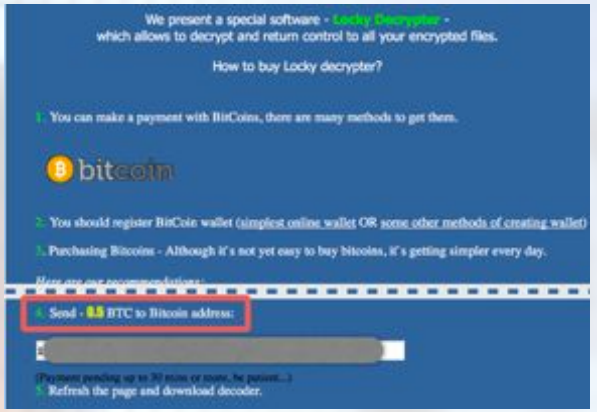
More crypto-ransomware

- TorrentLocker, 2015
  - Harvests victims' email addresses to spam other victims
- CTB-Locker, 2015
  - Curve-TOR-Bitcoin (CBT)
  - Uses Elliptic curve crypto
  - TOR component is embedded
  - Facebook/Chrome suspension warning
- TeslaCrypt, Feb 2015
  - Targeted video game community
  - Deleted shadow volume copies

https://www.wired.com/2015/09/hacker-lexicon-guide-ransomware-scary-hack-thats-rise/

More crypto-ransomware

- Locky, Feb 2016
  - Distributed as a Word macro attachment
  - Deletes shadow copies
  - Used in healthcare facilities
  - Changes file extension to .locky



- Petya, Mar 2016
  - Overwrites master boot record (MBR) → **disables booting**
  - Delivered through legitimate cloud such as Dropbox
  - Decrypted thanks to sloppy implementation

- Cerber, Mar, 2016
  - Voice feature

https://www.wired.com/2015/09/hacker-lexicon-guide-ransomware-scary-hack-thats-rise/
http://thehackernews.com/2016/04/ransomware-decrypt-tool.html

More crypto-ransomware

- 7ev3n
  - Demands random demand of **13 bitcoins**
- SlientShade
  - Demand low ransom: **$30**
- CryptXXX
  - Distributed via Angler Exploit Kit
  - Decrypted thanks to sloppy implementation

https://blog.kaspersky.com/cryptxxx-ransomware/11939/

Free decryption, if you infect two!

- Popcorn Time
  - Dec 8, 2016

Restoring your files - The fast and easy way

To get your files fast, please transfer **1.0 Bitcoin** to our wallet address **1LEiPgvh6S9VEXWV2dZTytSRd7e9B1bWt3**. When we will get the money, we will immediately give you your private decryption key. Payment should be confirmed in about 2 hours after payment made.

Restoring your files - The nasty way

Send the link below to other people, if two or more people will install this file and pay, we will decrypt your files for free.

https://3hnuhydu4pd247qb.onion.to/r/0e72bfe849c71dec4a867fe60c78ffa5

https://www.bleepingcomputer.com/news/security/new-scheme-spread-popcorn-time-ransomware-get-chance-of-free-decryption-key/

Ransomware for Mac

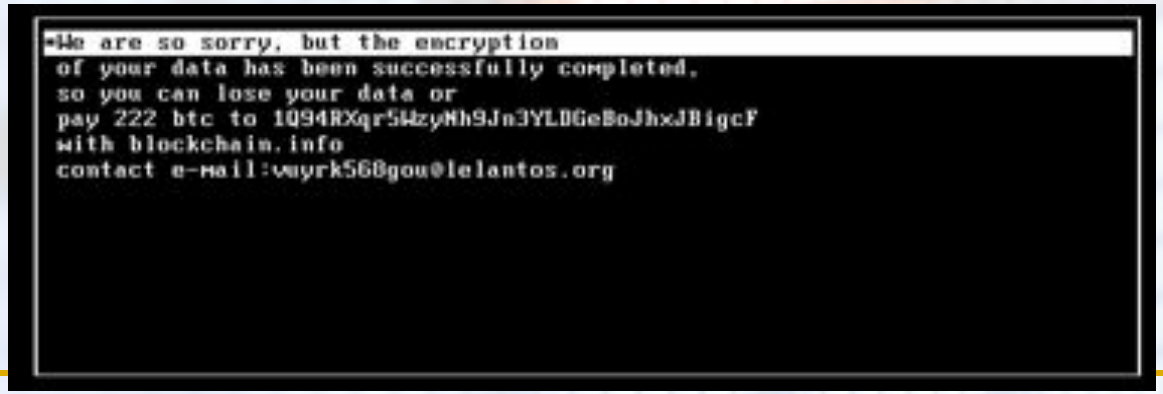
- Mac: only 7.4% of global market share of PC

- March, 2016
  - First live Ransomware for Mac found: **KeRanger**
  - Compromised Transmission, a popular BitTorrent client
  - Sleeps 3 days before activation
  - Demand 1 bitcoin (~$400)

Ransomware for Linux

- November, 2015
  - Linux.Encoder.1 ransomware
  - Infects Magento

- January, 2017
  - KillDisk Ransomware targets Linux
  - Wipes disk
  - Demand 222 Bitcoins (~$218,000) !
  - Researchers found a way to recover the key

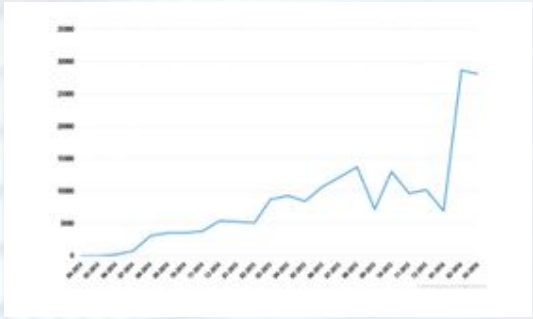


UNLV
UNIVERSITY OF NEVADA LAS VEGAS

Mobile Ransomware

- **50% increase** in one year (Feb 2017), ZDnet
- Android
  - Porn Droid app locks the phone and change its PIN number while demanding a $500 ransom from victims.

Porn Droid Android ransomware



https://www.wired.com/2015/09/hacker-lexicon-guide-ransomware-scary-hack-thats-rise/
http://www.zdnet.com/article/android-ransomware-attacks-have-grown-by-50-percent-in-a-year/

Ransomware for Cloud

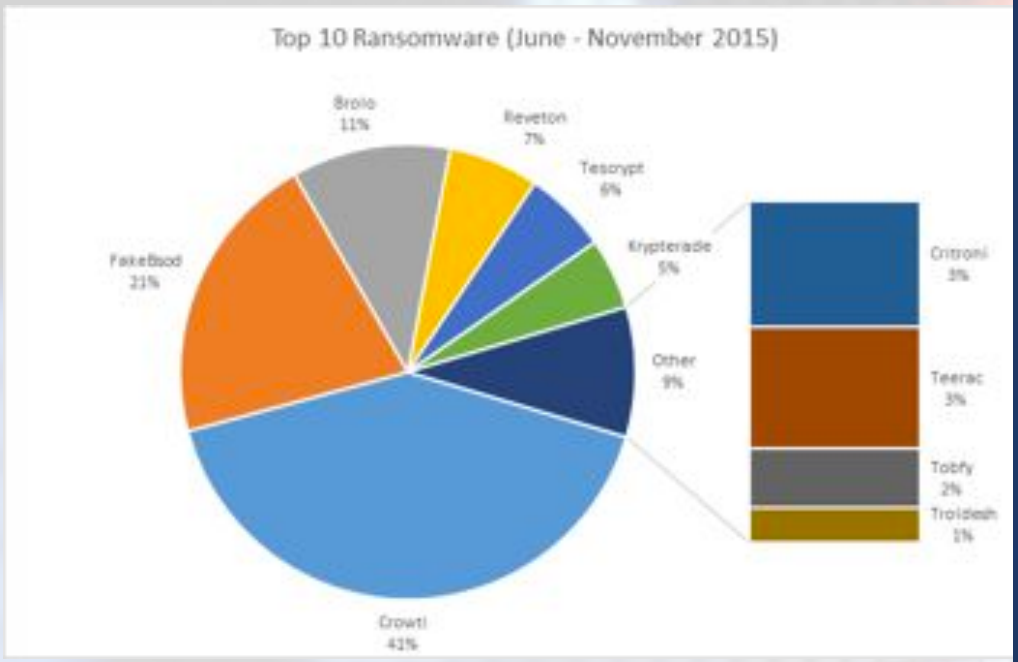
- Cloud storage ransomware usually self-propagates after being installed on cloud servers
  - With Cloud synch, cloud collaboration
  - E.g., Virlock (2014) (2016cloud version)
    - It impersonates FBI authorities and requests victims to pay the fine of $250 due to alleged misconduct.

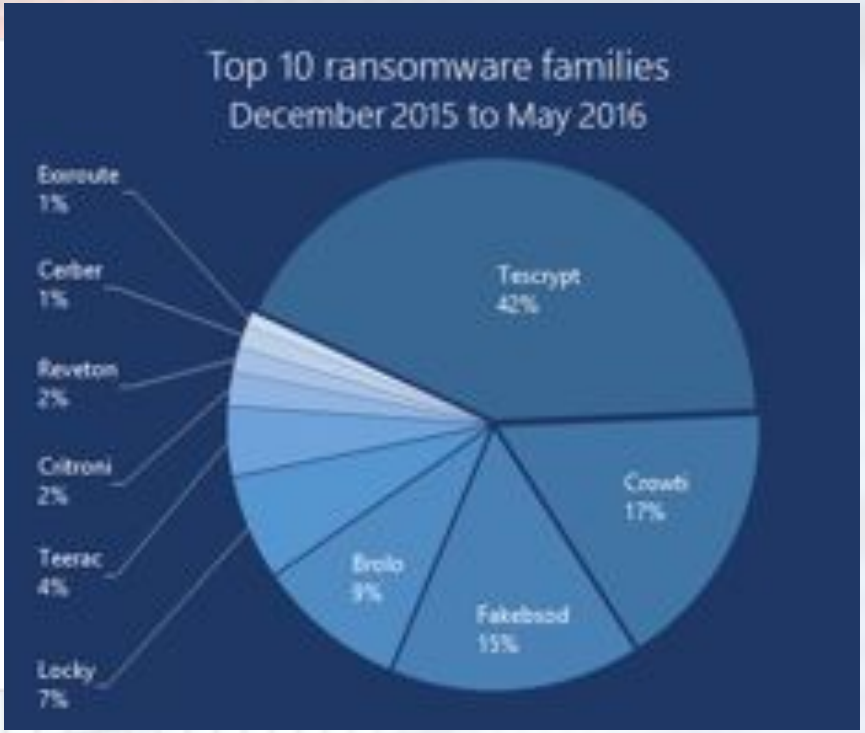
Ransomware + IoT = Jackware?

- Manufacturing plants, SCADA, process control
  - Proof of concept, RSA Conference, 2017
- Huge potentials
  - Connected cars (Jeep Grand Cherokee)
  - Home IoT devices
  - Wearable (FitBit)

https://www.scmagazine.com/ransomware-of-things-researchers-predict-future-of-ransomware-attacks/article/633842/
http://www.welivesecurity.com/2016/07/20/jackware-connected-cars-meet-ransomware/

Landscape changing rapidly





https://www.microsoft.com/en-us/security/portal/mmpc/shared/ransomware.aspx

UNLV UNIVERSITY OF NEVADA LAS VEGAS

Your Own Custom Ransomware

- No computer programming skills?
  - No problem. Purchase your own ransomware
  - Cryptolocker, Cerber, Locky and Stampado

1. Outsourcing development: Specify the requirements
   - Distribution method (web vuln, email, etc)
   - Type of file (.doc, .jpg, etc)
   - Bitcoin address, keys

2. DIY kit
   - Cheaper
   - $39 - $3000, or free,

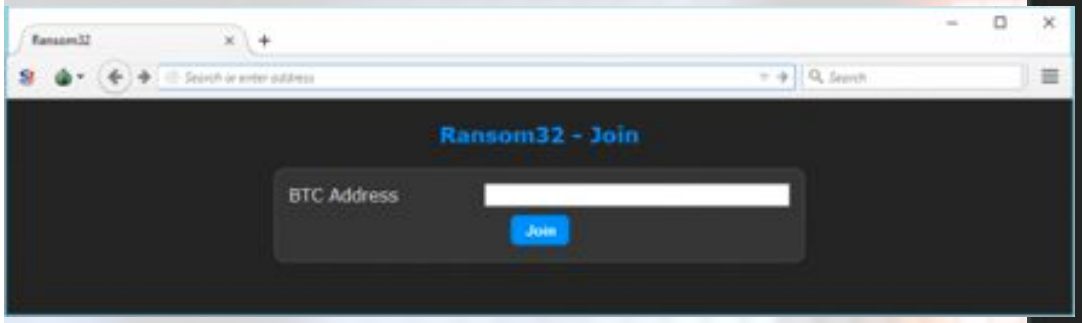
Ransomware-as-a-Service (RaaS)

- **Outsourcing the distribution** element of the ransomware while still collecting the ransom.
  - Such systems offer distributors a percentage of the ransoms received.
    - Petya, Mischa, Tox, Ransom32 and Cryptolocker Service follow this model
  - All future extortionists need is a bitcoin account to sign up and they can download the ransomware for distribution

https://fightransomware.com/ransomware-articles/cybercriminals-turn-diy-kits-ransomware-service-raas/

Ransomware-as-a-service

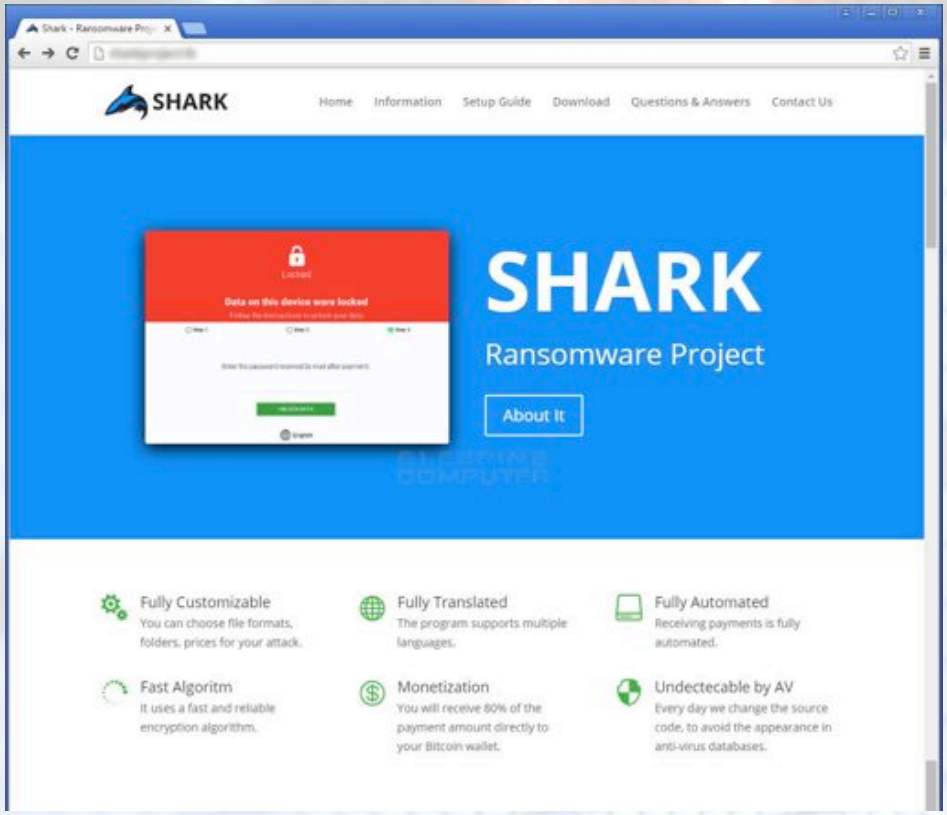
- Ramsom32



http://blog.emsisoft.com/2016/01/01/meet-ransom32-the-first-javascript-ransomware/?ref=ticker160111&utm_source=newsletter&utm_medium=newsletter&utm_content=mainnews&utm_campaign=ticker160111

Shark Ransomware Project

- Went live in July 2016, discovered in August 2016
  - Shark RaaS developer keeps **20% of the ransom** payments and give the rest to distributor/affiliate



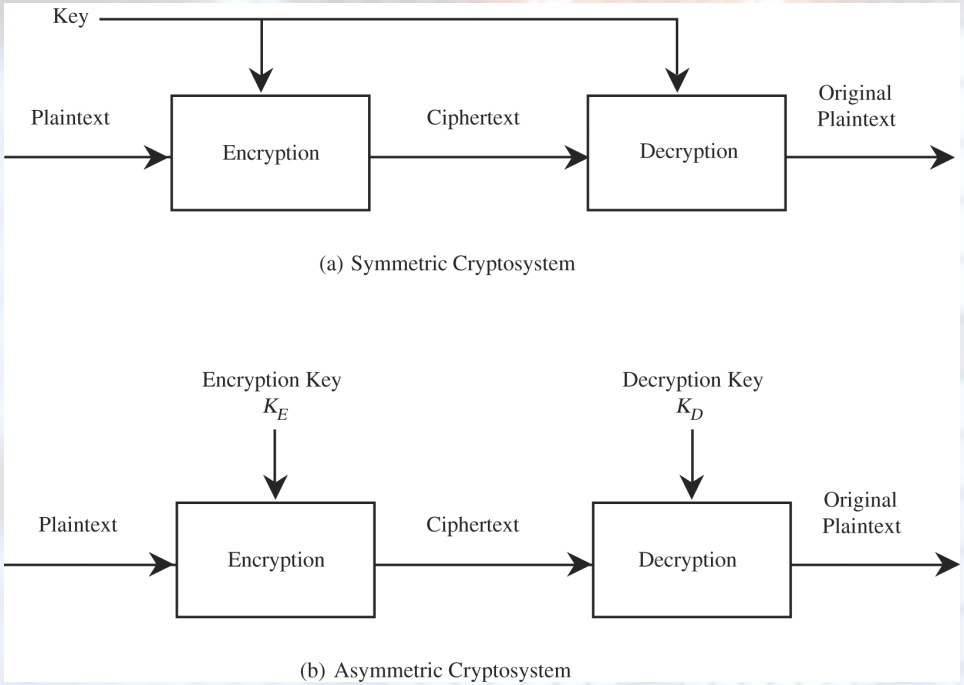
https://www.bleepingcomputer.com/news/security/the-shark-ransomware-project-allows-to-create-your-own-customized-ransomware/

3. Ransomware Operation

Symmetric key vs. Asymmetric key

- Secret key cryptography vs. Public key cryptography
  - Encryption key: K_E
  - Decryption key: K_D
  - $P = D(K_D, E(K_E, P))$

Key distribution problem



Fast

Easy Public Key Distribution

Slow (100x)

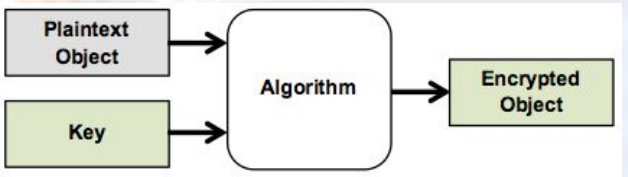
Cryptographic Process

- Symmetric Key cryptography
  - AES (128 to 256 bit key), 3DES, DES
- Asymmetric key cryptography
  - RSA, Elliptic Curve Cryptography (ECC)
- Encryption: 2 step process
  1. User file (M)→ encrypt with AES with a secret key (K)

     $C_1 = E(K, M)$

  2. K → encrypt with a public key (K_E)

     $C_2 = E(K_E, K))$



- K can be decrypted only with a private key (K_D)

  $K = E(K_D, C_2)), \quad M = E(K, C_1)$

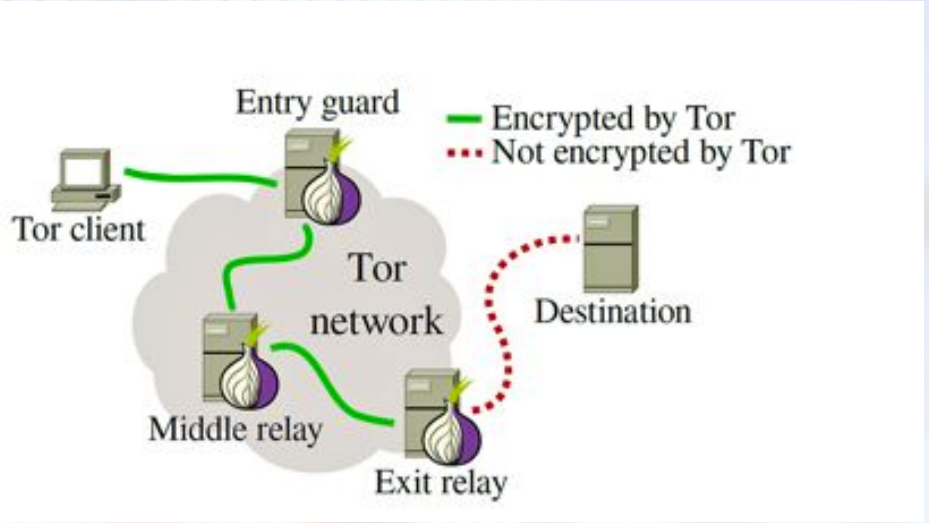
Encrypt what?

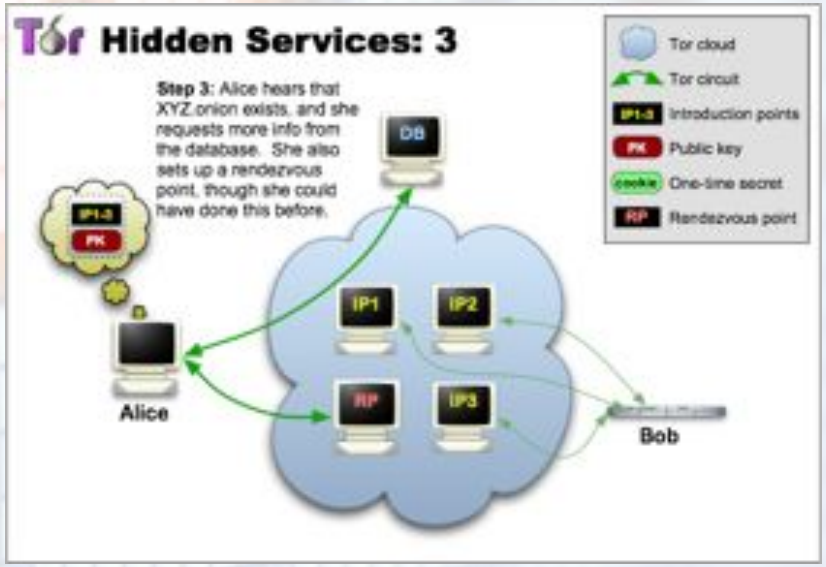
- Usually user data files
  - Allows normal system operation
    - Microsoft Office files (.doc, .docx, .xls, .xlsx, .ppt, .pptx, .rtf)
    - Open Office files (.odt, .ods, .odp)
    - Adobe PDF files
    - Popular image files (.JPG, .PNG, raw camera files, etc.)
    - Text files (.txt, .RTF, etc.)
    - Database file (.sql, .dba, .mdb, .odb,. db3, .sqlite3, etc.)
    - Compressed file (.zip, .rar, .7z, etc.)
    - Mail files (.pst)
    - Key files (.pem, .crt, etc.)
- System files or the whole disk
  - E.g. Petya: Encrypt the MBR
  - Disable booting

Command and Control server (C&C)

TOR for anonymous communication

- The Onion Router (TOR)
  - 7000 relay nodes
  - 2M users
- Tor Hidden Service
  - Running a web server anonymously
  - Uses rendezvous points
  - 60,000 ".onion" addresses
- Similar network: I2P
  - Invisible Internet Project

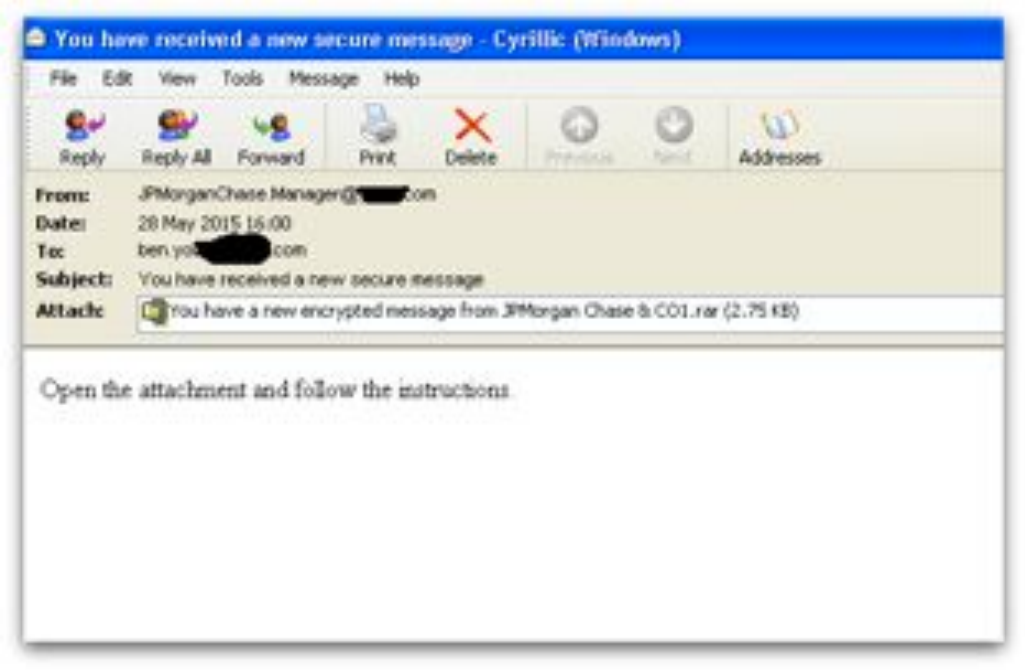




UNLV UNIVERSITY OF NEVADA LAS VEGAS

Attack Vectors

1. Email/Spam
   - Malicious attachment
   - Especially Word documents with malicious macros
   - Need human interaction
   - E.g., Cryptowall



UNLV UNIVERSITY OF NEVADA LAS VEGAS

Attack Vectors

2. Drive-by download
   - Visiting a compromised website with an old browser or software plug-in or an unpatched third party application
   - Compromised web sites runs exploit kit (E.g., Angler exploit kit)

3. Free software
   - "cracked" version of expensive software
4. Cryptoworm
   - To be seen

Sequence of Operation

1. Connect to the C&C server
2. Download the RSA public key unique to this computer
3. Search for target files
4. Generate random AES key for each file (only in RAM)
5. Encrypt files and delete the original files
6. Encrypt AES keys using RSA public key, and store them along with the encrypted file
7. (Cryptowall 4.0) Rename all infected files
   - Make the back up difficult
8. After finishing, open a ransom notice window

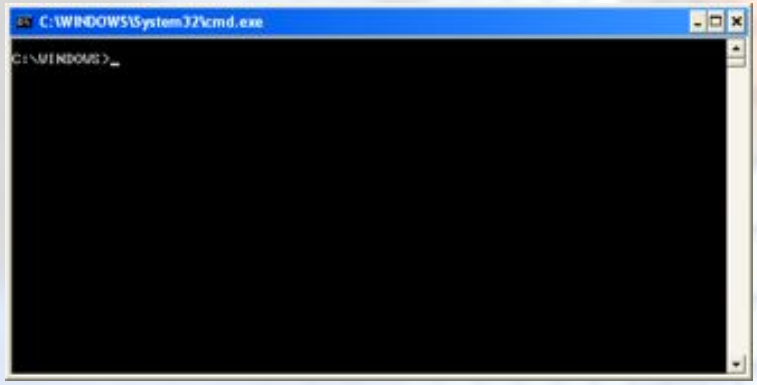
- **Takes 5 minutes to 1 hours**

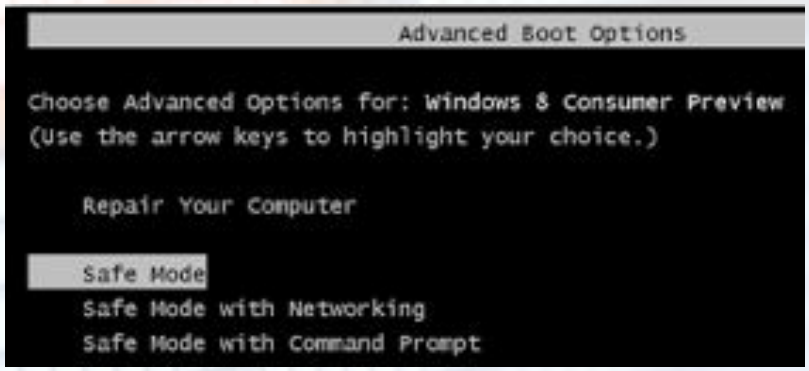
During Encryption

- CPU and memory overloaded
  - Loud fan noise
- The extension of the files are getting changed
  - .crypt, .vvv. zepto, .fun…
- Users cannot open encrypted files
  - If a user is working on unencrypted file, the file gets encrypted as soon as saved.
- Forcefully disconnects external hard drive or USB drive
  - External drive can be infected with the Ransomware, or physically damaged during repeated forceful eject
- The threatening letter appears with a timer
  - Not always

Aftermath

- Antivirus may be stopped or deleted
- Cannot open some system programs
  - cmd, some control panel, regedit, msconfig, crtl-alt-del,
- Cannot boot from safe mode
- OS updates may be blocked
- Removes Windows rollback points





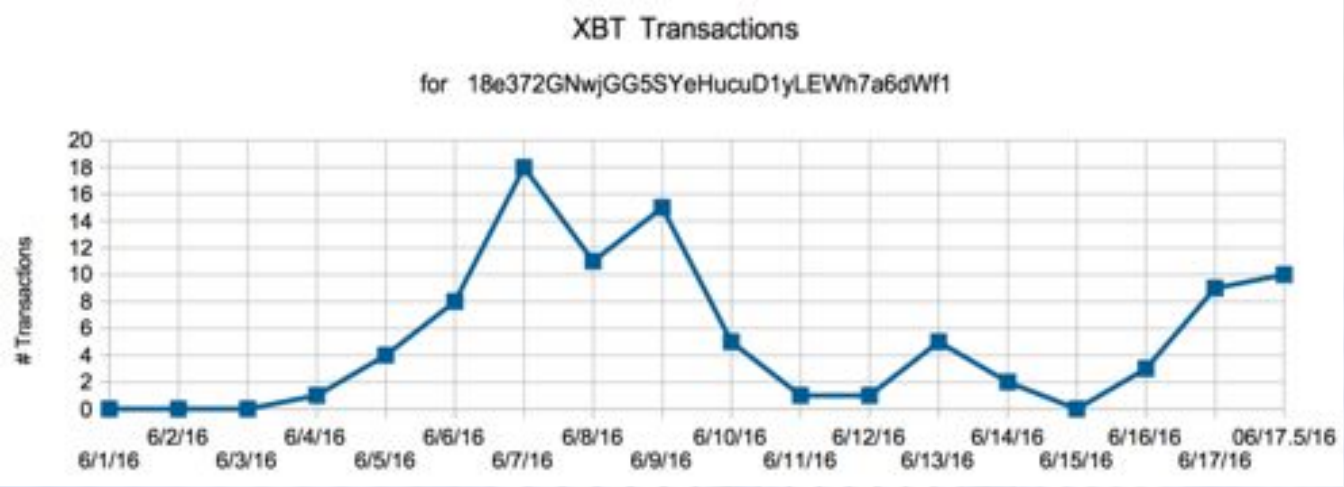
Payment process

- Bitcoin!
  - Other cryptocurrency (Ethereum, litecoin,…) not used
  - E.g., TorrentLocker displays the price based on the location (local currency), payable in bitcoin
    - Shows the exchange rate too

- Sometimes Amazon gift cache, apple iTunes gift cards
- SMS/Call to a premium mobile number

Bitcoin Tracking

- Can we track the payments?
  - By Chainalysis or Bitcluster
- CryptXXX
  - https://sentinelone.com/blogs/new-cryptxxx-variant-discovered/, June 27, 2016
  - Between 6/4 ~ 6/21, 2016, 70+ bitcoins received, $49,700 ($710/BTC)



UNLV UNIVERSITY OF NEVADA LAS VEGAS

4. Ransomware Incident handling

Infected! What now?

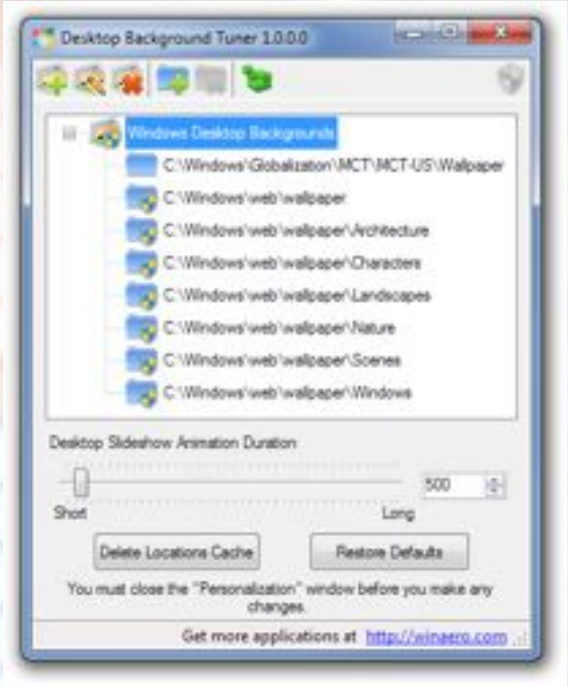
1. Can you stop it now? → Do something!!!
2. Got backup? → Restore files
3. Recovery tools exist? → Recover files
4. Ummm, no…
   - → Pay ransom
   - → Lose the files

1. Do Something!!

- By the time the ransom notice pops up, it is too late
- Kill the suspicious programs
  - E.g., ransom.exe
- Change file extensions to uninteresting extensions (e.g., .pdf → myp) to hide them from ransomware
  - It can be done in advance as a preparation
  - You can write a emergency script in advance
- But can you stay calm enough?
  - Besides, cmd, ctrl-alt-del, Process Explorer may not work

Delay Tactic

- Ransomware scans file from C:\ drive, and encrypt files in alphanumeric order
  - Keep many large junk files in C:\ directory
- Helps detection
  - Store desktop background files in C:\
  - Reload them frequently (slideshow)
  - Image is gone after encryption



Emergency measure

- **Unplug** power or remove notebook battery

- If safe mode booting is possible, boot into safe mode
  - Remove the ransomware using AV
- If not, mount the hard drive on another OS, and copy the files to a backup drive, and reinstall Windows
  - If keys and tools available, use the tools to decrypt the files

- Hard drive MBR encryption ransomware won't allow any kind of booting including safe mode
  - e.g., Petya, Mischa, Goldeneye, Santana
  - Need to recover MBR using Windows CD

Keeping the encryption key

- The AES key is kept in the memory, which will be removed after encryption
  - Freezing the memory will preserve the AES keys, but shutting down will destroy DRAM content

- Solutions
  - After emergency shutdown, freeze the memory with hair spray, and thaw later for analysis (lasts a few days easily)
  - No hair spray? Hard reset, boot into Linux, and memory dump (dd)

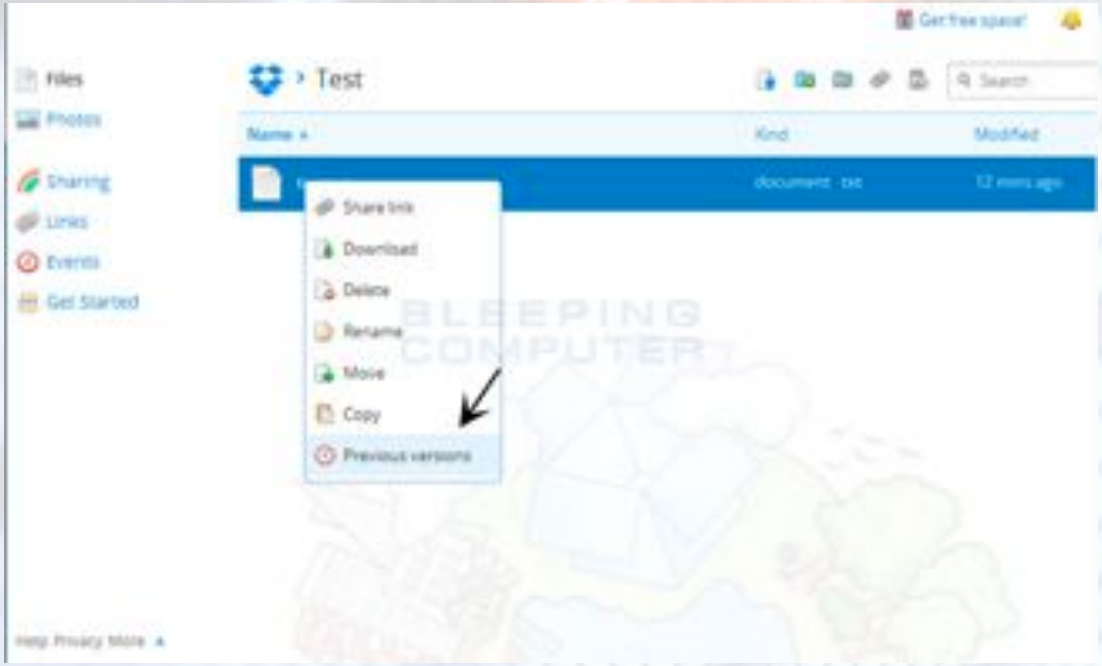
2. Backup, yes, BACKUP!

- The most important methods!!!
  - Back up multiple versions over time to recover the pre-encryption files

- Types
  1. External hard drive: Not very useful
     - Vulnerable to Ransomware attack
     - Must have been disconnected while attack occurred
  2. DVD-ROM
  3. NAS
     - Ransomware won't start within NAS due to different OS, and lack of access rights
     - Make the SMB read only, upload files using sftp
  4. Cloud service

Cloud Services

- Google drive, Dropbox, Amazon, Backblaze, Crashplan, etc.
- File history is usually available
  - Exception: MS OneDrive does not have history



3. Recover files

- Windows Shadow Volume Copies
  - Windows creates shadow copy snapshots that contain copies of the files when the system restore snapshot was created.
  - These snapshots may allow us to restore a previous version of our files from before they had been encrypted.

- Ransomware will attempt to delete all VSS, but it may fail

Forensic techniques

- Recover deleted files
  - If the ransomware did not overwrite them (not Cryptowall 2.0 or later), it may be possible to recover. (works on TeslaCrypt)
  - Even if it did, it may not actually overwrite the same sector due to wear-leveling algorithm in case of SSD
  - DIY: Use R-studio, or Photorec
  - Call the forensic experts
    - But may be more expensive than ransom and take longer time
- Recover windows temporary files
  - Deleted upon finishing editing, but not the file content
- Caution:
  - **Do not continue to use the machine**. It makes the forensic file recovery more difficult

Recover Files Using Free Tools

- Kaspersky
  - Free ransomware decryptors
  - https://noransom.kaspersky.com/

- Trend Micro
  - Ransomware File Decryptor
  - https://success.trendmicro.com/solution/1114221-downloading-and-using-the-trend-micro-ransomware-file-decryptor

No More Ransom

- Industry consortium
  - https://www.nomoreransom.org/

Commercial services

- http://www.rm-ransomwarerecovery.com/

Data Encrypted by Ransomware?

We can help you get it back TODAY, quickly and easily.

The following are some of the more common variants of computer ransomware:

LOCKY Ransomware	CERBER Ransomware	DMA LOCKER Ransomware	MALWARE Data Recovery	VIRUS Encryption
Zepto (.zepto)	Cerber 1	DMA Locker 1	CryptoLocker	CrySiS
ZZZZZ (.zzzzz)	Cerber 2	DMA Locker 2	CryptOL0cker	Crypto Virus
Thor (.thor)	Cerber 3	DMA Locker 3	CryptoWall 3	Tesla Crypt
Odin (.odin)	Cerber 4	DMA Locker 4	CryptoWall 4	Globe
Osiris (.osiris)	Cerber 5	DMA Locker 5	CryptXXX	Troldesh
Aesir (.aesir)			Dharma	XTBL

- Las Vegas
  - Axiom cyber solutions
    - https://www.axiomcyber.com/
  - Secured IT Solutions
    - http://www.secureditsolutions.com

5. To Pay or Not To Pay?

To Pay or Not to Pay

- Chance of getting the key
  - Was high previously. Attackers needed to build trust to encourage ransom payment. Had a good customer service.
  - Now getting lower due to more irresponsible nomadic attackers

- Out of 5 who paid, 1 didn't get the key
  - Getting lower because customer service (trouble shooting capability) is getting worse as more criminals don't have the programming skills

Dilemma

- Doctor ($5,000) or Antidote ($500)?
- Cybersecurity ($5,000) or Ransom ($500)?
  - E.g., 2 experts working for 25 hours at $100/hour = $5,000 (and not guaranteed)
- Quickest, cheapest, and cleanest way
  - Ransom!
  - Much safer

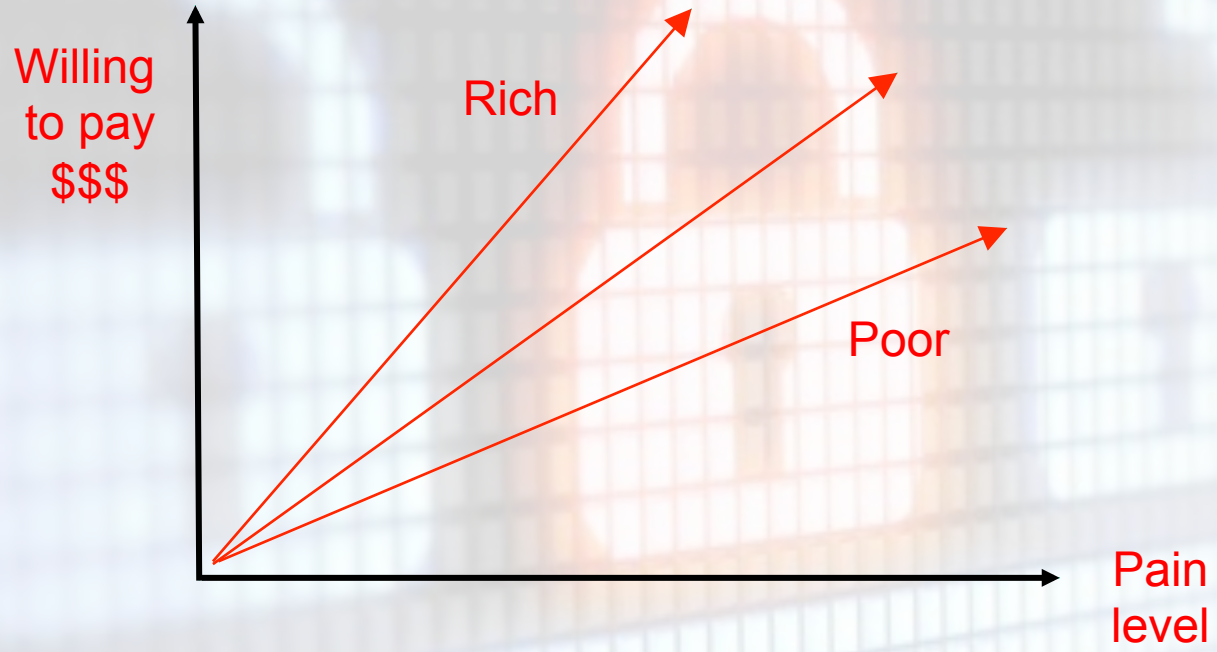
Real Loss: Productivity hit

- "How Ransomware Became a Billion-Dollar Nightmare for Businesses", Sep 3, 2016
  - Extortive attacks now cost companies at least **$75 billion** in expenses and lost productivity each year.
  - Less than 1 in 4 attacks are reported
  - Banks are stocking bitcoins in preparation

https://www.theatlantic.com/business/archive/2016/09/ransomware-us/498602/

How much?

- Pain level vs. amount willing to pay



- Study by SkyHight security
  - A quarter of companies **(24.6%)** would pay a ransom, even if such amount **exceeds USD 1 million** (14% respondents).

Who pays?

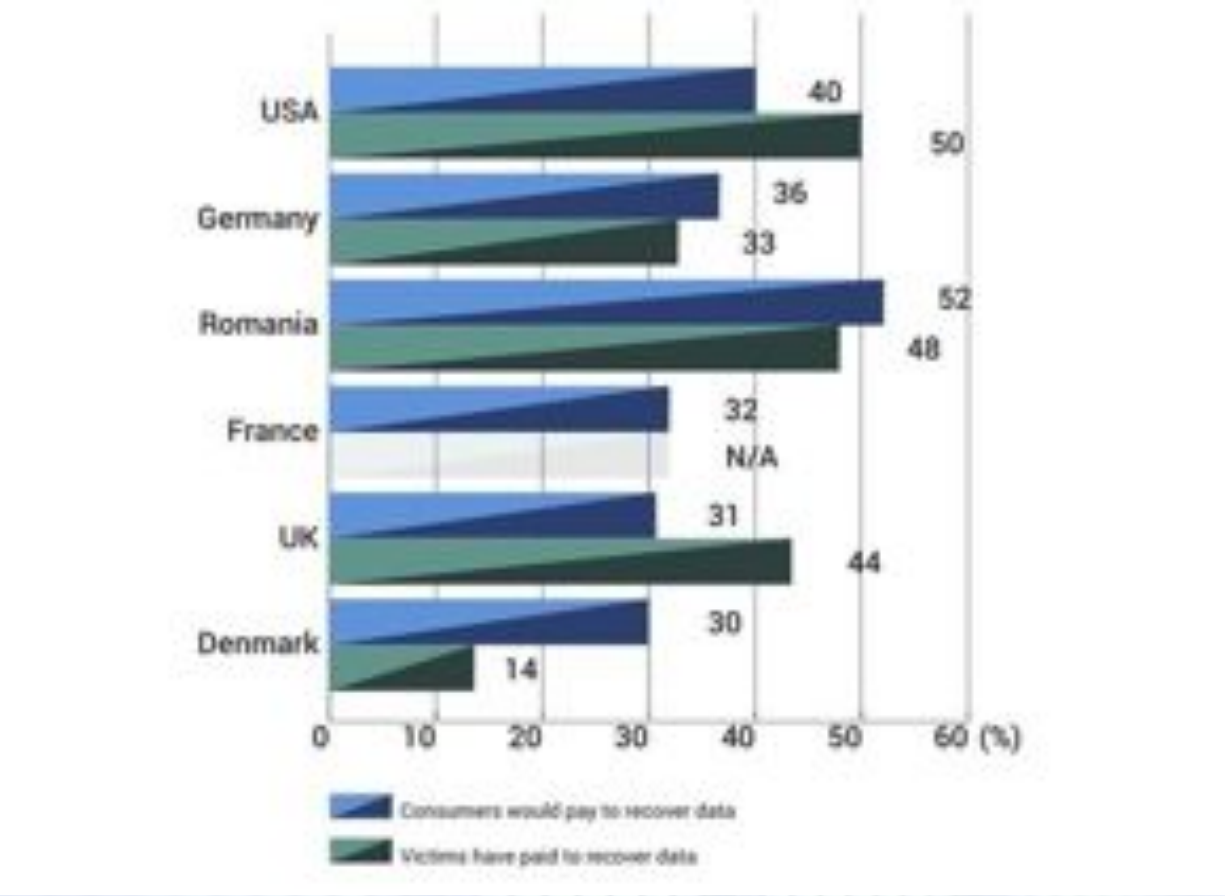
- Ransom payment rate by Osterman research
  - Nearly 60 percent demanded over $1,000.
  - Over **20 %** asked for more than **$10,000**, 1 % even asked for over $150,000.
  - Globally, more **than 40 % of victims paid** the ransom.
  - Healthcare and financial services were the leading industries
    - penetration rate of 39 %
  - Potential loss of life: **3.5 %**even said lives were at stake

- IBM security
  - 70% of business victims paid
  - Of those, 50% paid more than **$10,000**, 20% more than **$40,000**

https://press.malwarebytes.com/2016/08/03/international-study-finds-nearly-40-percent-of-enterprises-hit-by-ransomware-in-the-last-year/

BitDefender Poll

- June, 2016



http://www.pcworld.com/article/3083772/security/how-greed-could-destroy-the-ransomware-racket.html

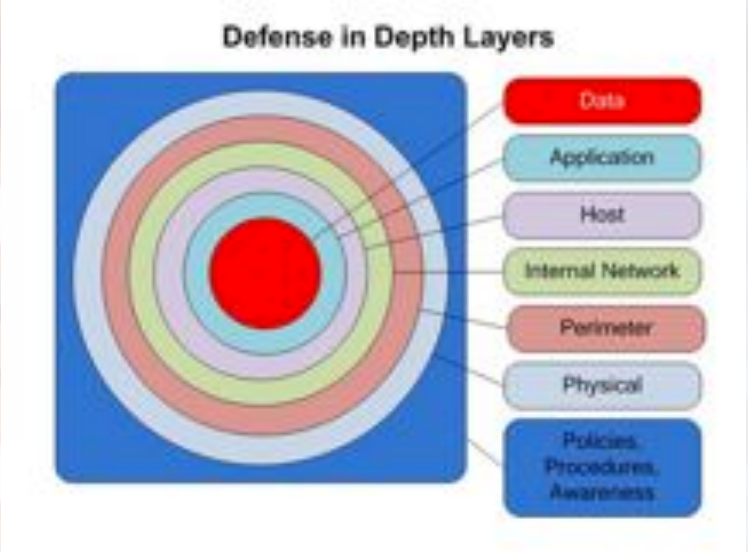
FBI Policy Swings?

- 2/18/2016
  - FBI's general advice to ransomware victims is to pay the ransom. Joseph Bonavolonta, assistant special agent at FBI's CYBER and counterintelligence program explained:
  - "The ransomware is that good. To be honest, we often advise people just to pay the ransom."
    - https://www.cryptocoinsnews.com/ransomware-extortionists-land-17000-in-bitcoin/
- 8/9/2016
  - supervisory special agent for the FBI's Cyber Division, Will Bales, said that businesses or individuals targeted by ransomware should refuse to pay the ransom,
    - https://www.cryptocoinsnews.com/fbi-now-says-dont-pay-bitcoin-ransomware-extortionists/

6. Preparation

Defense In Depth

1. Browser level
2. Email attachments
3. AV, anti-ransomware tools
4. OS level
   - Least privilege
5. Hardware level
   - Physical and logical separation
6. Network Level
   - Mapping drive
   - SIEM
7. Awareness training and drill



1. Browser

- Avoid drive-by-download
  - Update Patch
- Many Ransomware utilizes IE, Adobe Flash, Java
  - Do not use IE, but use Edge, **Chrome** or Firefox
  - Remove Adobe Flash. (Some vuln exists with Acrobat reader, Silverlight, Java). Disable ActiveX. Use HTML 5
  - **Few Ransomware uses Chrome vulnerability**
- If you must use IE, set the security level to high
  - Most ransomware can work only at lower security level
  - IE 10/11: activate sandbox option
- Ransomware propagates through advertisement
  - Block the ads using ad blockers, NoScript browser add-ons

2. Email handling

- Be cautious about unsolicited attachments
  - Avoid clicking untrusted email links or opening attachments
- Don’t enable Macro
- Install MS Office viewer
  - Preview the mail attachments
  - It doesn’t support macros at all
- Use spam mail detection tools
  - AV/ IDS/IPS/UTM/SIEM
  - Anti-phishing software

3. Anti-Virus

- Keep updated

- AV is not perfect!!
  - AV can detected Angler exploit kit only 5 to 6 %
  - Use Specialized tools

4. OS

- Keep updating OS, especially security patches
- Enable multiboot just in case, and install Linux
- Use least privilege
  - Activate UAC (windows 7 or above)
  - Do not stay logged in as an Admin for long
  - Don’t do web surfing, email, document editing in admin account
  - Configure access controls—including file, directory, and network share permissions— with least privilege in mind
    - Limit write access to network mapped shares

4. OS

- Implement Software Restriction Policies (SRP) to block binaries running from
  - %AppData", "%TEMP%", %LocalAppData%, %ProgramData%
  - Use Windows Group or Local policy editor

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

5. Hardware

- Air gap
  - Separate critical computers from the Internet
- Use separate computers for risky activities
  - E.g., web surfing, email, bittorrent
  - Implement roll back whenever reboot
  - Much cheaper than ransom!
- External hard drive
  - Connect only during backup
  - Once backed up, set it to “Read Only”. (diskpart command)
- Virtual machine (VMware, Virtual PC…)
  - Do not share the host folders

6. Network – Enterprise level

- Install Firewall/SIEM
  - block proxy services (TOR, I2P)
  - block access to known malicious IP addresses

- Patch operating systems, software, and firmware on devices.
  - Consider using a centralized patch management system.

6. Network – Enterprise level

- Email security
  - Email web gateway
  - Cloud-based email security
  - Consider using encrypted email / sender verification
    - PGP, GPG
  - Enable strong spam filters using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and Domain Keys Identified Mail (DKIM).
  - Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.

7. Training

- Employee education on
  - Spam email, Phishing
  - Drive-by download
- Periodically remind them
- Simulated attacks
  - Boost user awareness occasionally

Cyber Insurance

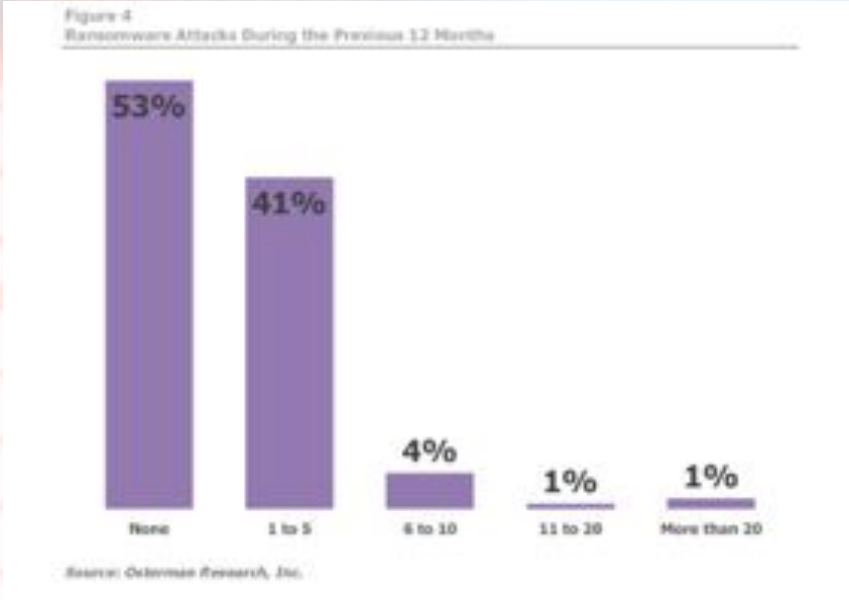
- Cyber insurance allows the insured persons to mitigate the financial losses caused by cyber-attacks. It may cover the ransoms which organizations need to pay to criminals.

- Ransomware insurance. Beware,
  - Time limit
  - Deductibles
  - Fees to paid to cybersec experts

http://resources.infosecinstitute.com/insurance-ransomware-threats/

Confident with backup?

- Ransomware statistics in 2016
- 50% of organizations have been hit
- 100% companies did some backup
  - **But only 41% recovered data from backup**
  - Failed backup, newest data lost, backup infected



https://blog.barkly.com/ransomware-statistics-2016

UNLV UNIVERSITY OF NEVADA LAS VEGAS

Thank You!

Questions?