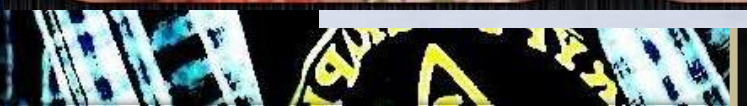
RANSOMWARE

History, Analysis and Mitigation

@R41nM4kr www.MeteorMusic.com



Agenda

- Overview
- In the News
- Timeline
- Technical Analysis
  - Analysis of Client Infection
  - Command & Control (C2) Architecture Setup/Design
- Evolved Ransomware
- Mitigation techniques

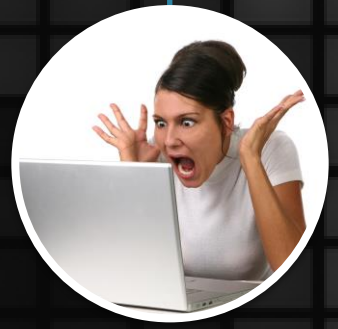
Cyber Extortion Defined

- Cyber extortion is an online crime involving an attack or threat of attack against a person or enterprise, coupled with a demand to stop the attack.
- Cyber extortions have taken on multiple forms:
  - Encrypting Data and holding it hostage
  - Threatening exposure
  - Denying access to data or services

Cyber Extortion

Cyber Extortion

DDoS



Sextortion

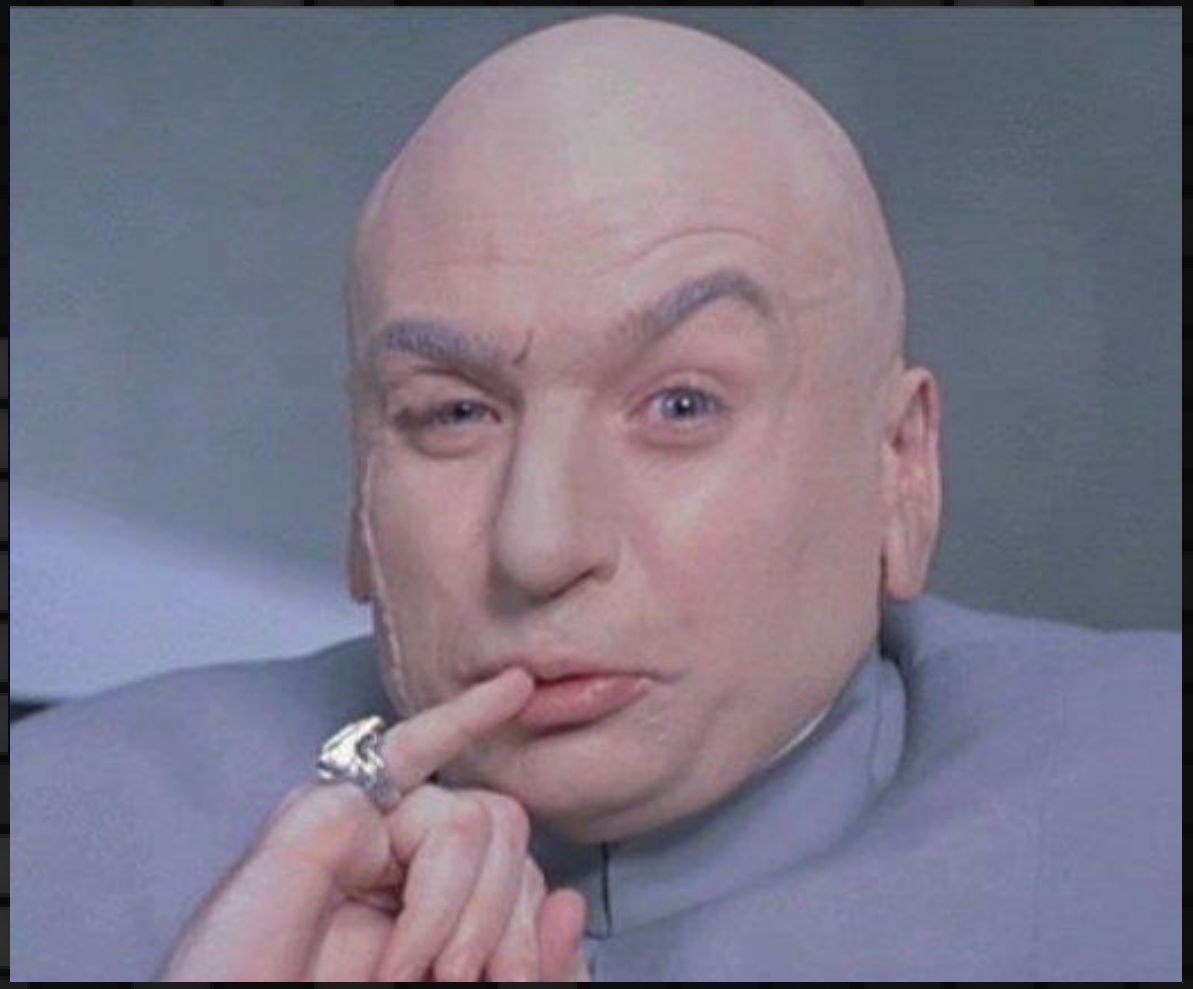
Ransomware

Ransomware Defined…

- Leveraging technical controls to inhibit use of data.
- Operates under the assumption that the data is important enough that users are willing to pay for recovery.
- There is no guarantee of actual recovery, even after payment is made.

Ransomware: A lucrative criminal industry

- Harjavec Group states $216 million in just Q1 of 2016.
- Total ransoms paid in 2016 amount to over…
  - ONE BILLION DOLLARS.



Some Scary Stats…

Much larger ransoms have been demanded into the millions. Some organizations refuse to pay and suffer the consequences. Others do not disclose they have actually paid the ransom.

- HIPPAA now considers ransomware a breach as the organization lost control of its data.
- Only a quarter of American homes back up their data on a regular basis.
- Over the past 12 months almost half of all US companies have been affected by ransomware.

Largest Ransoms Paid

- Los Angeles Valley College
  $30,000
- University of Calgary
  $20,000
- Presbyterian Medial Center
  $17,000

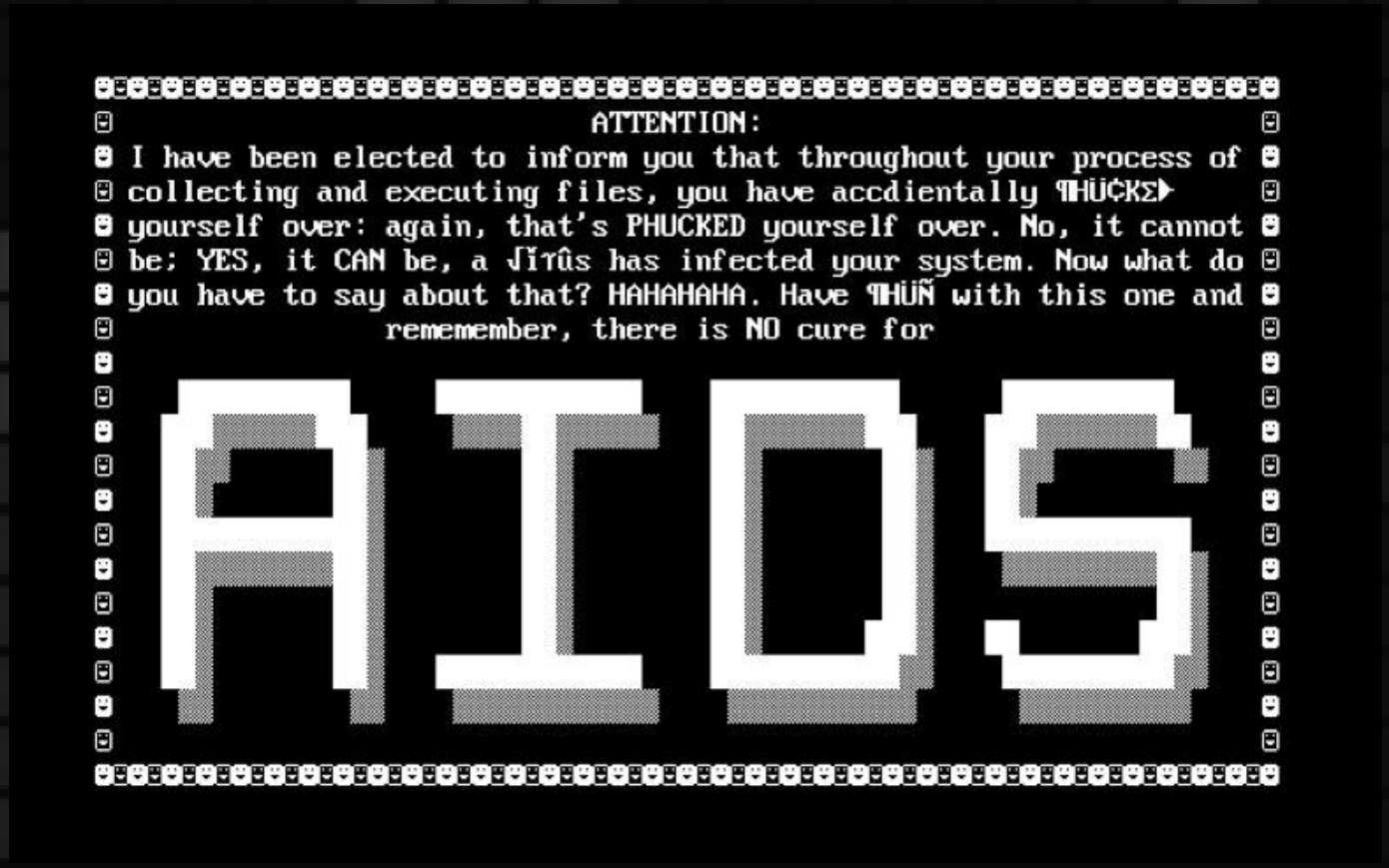
Malvertising

- Malicious Banner ads using Exploit Kits
  - Angler, Neutrino, RiG, Nuclear, ZaiXin, Magnitude
- Victim Sites include:
  - NYTimes, BBC, MSN AOL
  - InfoLinks, Realtor.com, Xfinity
  - Answers.com, Spotify, Ebay
  - DrudgeReport and many many many others.

A Brief History of Ransomware

The First Ransomware: The AIDS Virus

- Discovered in 1989
- Replaced Autoexec.bat
  - After 90 days, Encrypted file names on c:/
- Asked to ‘renew the license’
  - $189 to a PO box in Panama
- Dr. Joseph Popp was arrested by Scotland Yard later that year and charged with blackmail



Reveton

Internet Era Ransomware: FBI Lockscreen

- Circa 2011
- Reveton Trojan Family
  - Impersonates national law enforcement
  - Locks out of PC
- Easily removed
  - Boot to safemode
  - Remove registry key

Crypto-Currency

- Bitcoin
  - Anonymous
  - Secure
  - Instant
  - Not regulated
  - Perfect for EXTORTION!

Cryptolocker

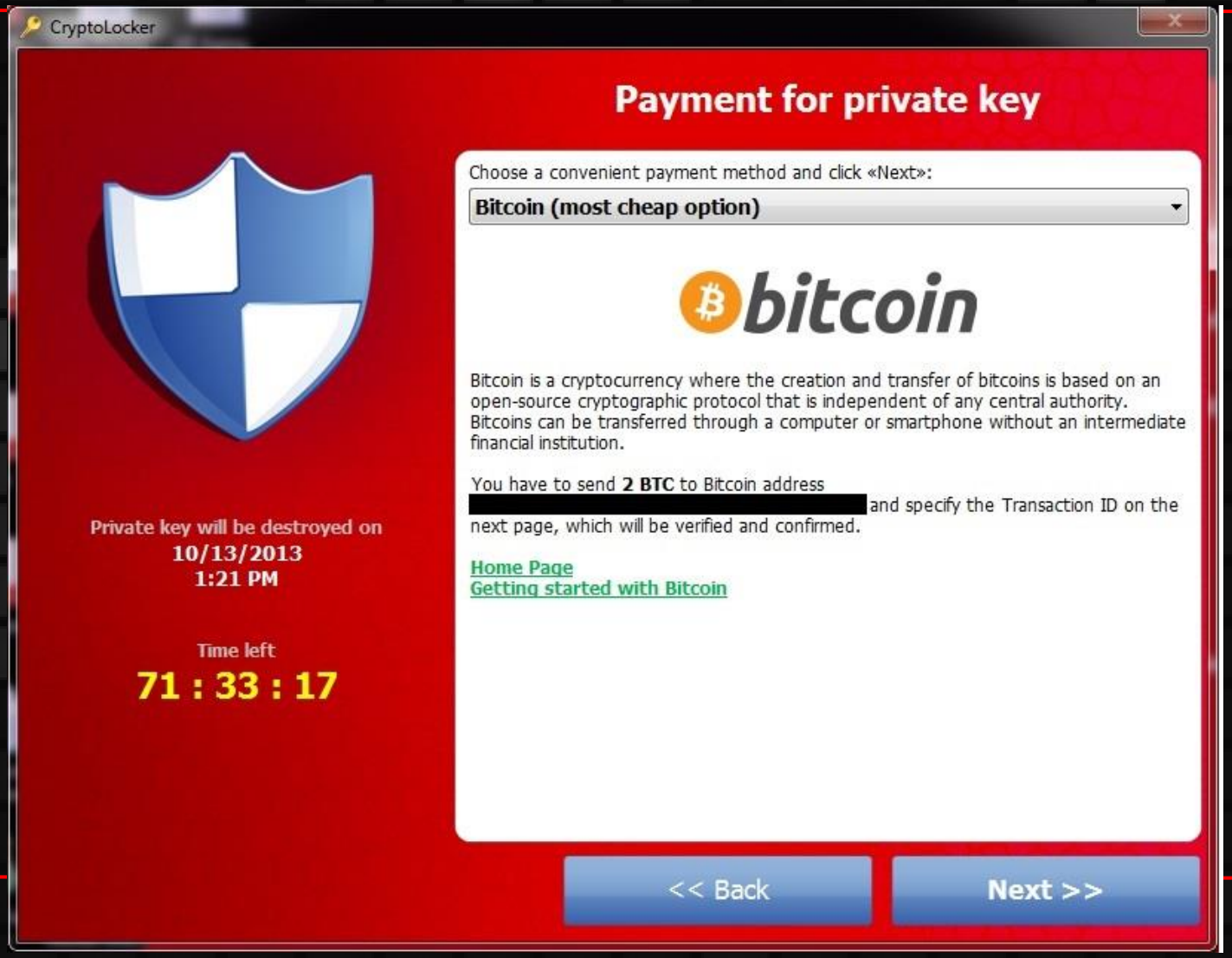
CryptoLocker

- Started to appear around September 2013
  - Delivered mainly though the GamoverZeus (GoZ) P2P Botnet
  - Used Domain Generated Algorythms (DGA)
    - Produce thousands of domains
    - Only 1 or 2 were real

Example: Faoefijawjfaslekf9ejaklja[.]ru

CryptoLocker…a deeper look.

- Infected local drives AND network storage
- AES-2048 Asymmetrical Encryption
- De-facto name for every ‘crypto’ infection today



CryptoLocker continued…

- Mid 2014 GoZ is shut down.
  - Down goes CryptoLocker
  - Keys recovered from c2c allow for decryption.
- New variants emerge shortly thereafter

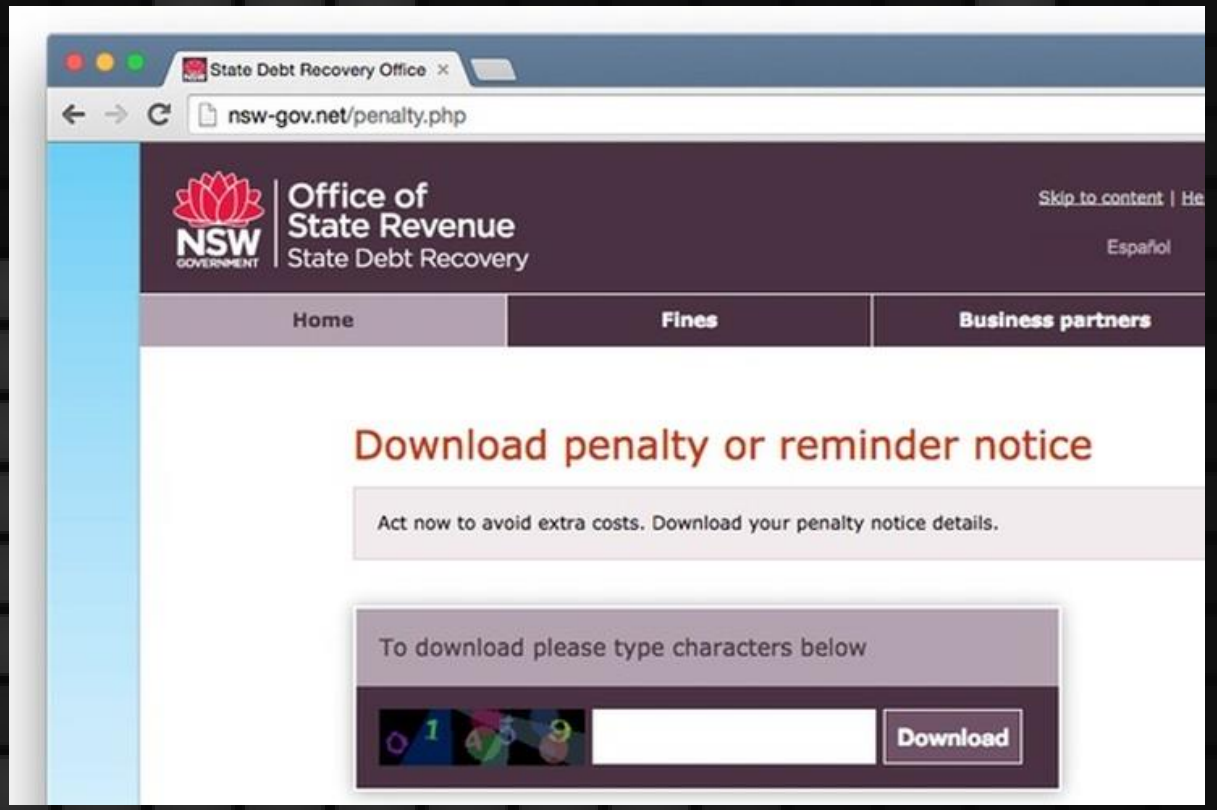
TorrentLocker

Torrentlocker

- Mainly seen in Australia & New Zealand.
- Phishing disguised as red-light tickets and Tax notices.

Torrentlocker: A common naming convention

- "(AUS|NSW)"-"(POST|GOV)"."(com|org|net|etc)
  - Example: enforcement-aus-gov.org
  - Example: nsw-post.com
- Easy to block Top Level Domain (TLD)



AlphaTeslaCrypt

Alpha/TeslaCrypt

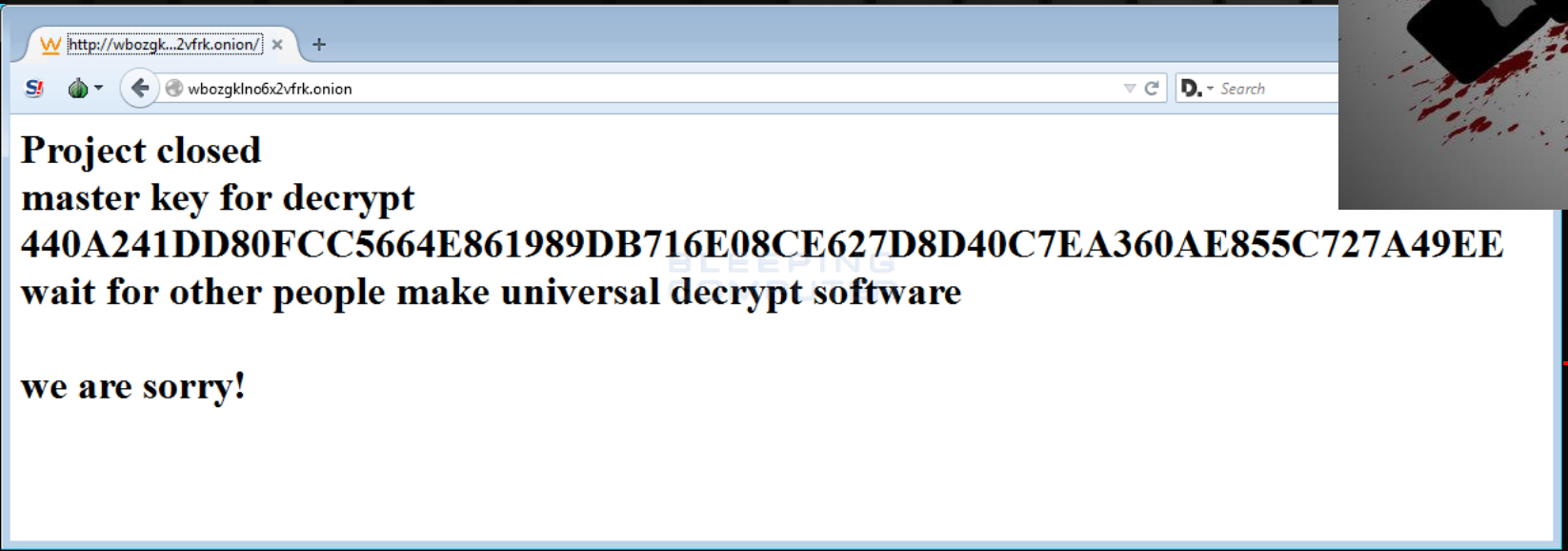
- Initially
  - attacked gamers (game related file extensions)
  - DGA based domains for C2
    - Example: asdfwef23sdf.com
- Evolved
  - Expanded file extensions
  - Compromised domains for c2
  - Exploit kits and now Spam

Alpha/TeslaCrypt

- V1.0 used symmetric AES Keys
  - TALOS group released TeslaDecrypt
- V2.0+ used Asymmetric Keys
- Still in the wild
  - V4.1 discovered April 22, 2016

Smell ya Later TeslaCrypt!

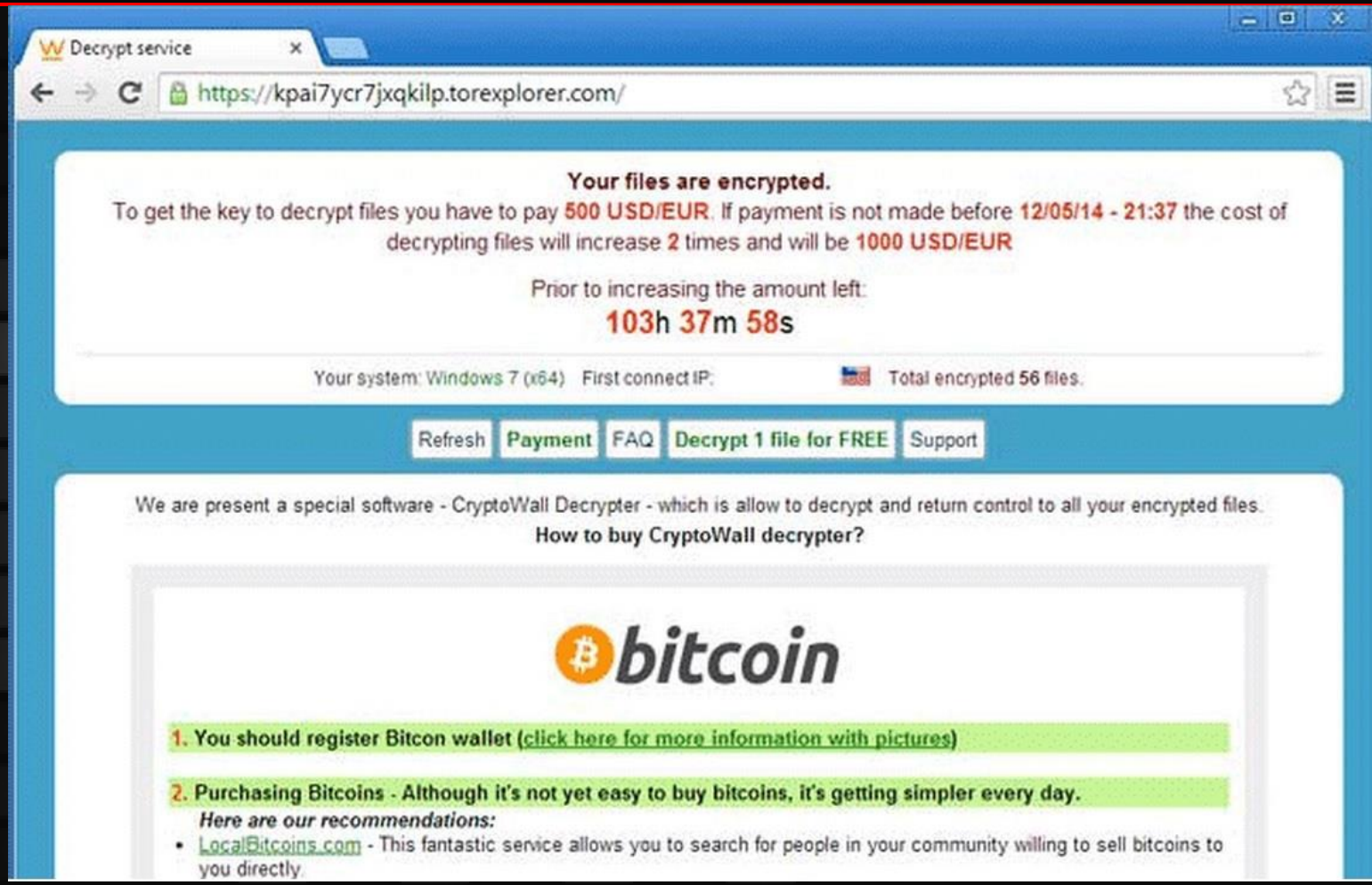
- May 18th
- Distributors Switching to CryptXXX & other variants
- Researcher asked in chat for the master decryption key.



Cryptowall

CryptoWall

- Exploded in end of 2014
  - Compromised Servers & Exploit Kits
  - Used anonymous Tor & I2P



Interesting Variants in Ransomware

Petya – The MBR Encryptor

- Rewrites systems MBR and forces BSOD.
- Fake “check disk” runs and encrypts Master File Table.
- Blocks access to entire machine, not just your files.

PowerWare – Using your own tools against you.

- Leverages MS Word and Native PowerShell.
- Does not pull down any additional binaries, and leverages PowerShell (already on the system and approved to be there) to do the dirty work.

What happened to your files?
All of your files were protected by a strong encryption with RSA-2048.
More information about the encryption keys using RSA-2048 can be found here: http://en.wikipedia.org/wiki/RSA_(cryptosystem)

What does this mean?
This means that the structure and data within your files have been irrevocably changed, you will not be able to work with them, read them or see them, it is the same thing as losing them forever, but with our help, you can restore them.

How did this happen?
Especially for you, on our server was generated the secret key pair RSA-2048 - public and private.
All your files were encrypted with the public key, which has been transferred to your computer via the Internet.
Decrypting of your files is only possible with the help of the private key and decrypt program, which is on our secret server.

What do I do?
Alas, if you do not take the necessary measures for the specified time then the conditions for obtaining the private key will be changed.
If you really value your data, then we suggest you do not waste valuable time searching for other solutions because they do not exist.

For more specific instructions, please visit this home page:

1.http://v2aahgcan6ed564p.onion.nu
Please scroll below for your #UUID

If for some reasons the address is not available, follow these steps:

1. Download and install tor-browser: http://www.torproject.org/projects/torbrowser.html.en
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: v2aahgcan6ed564p.onion
4. Follow the instructions on the site.

IMPORTANT INFORMATION:

Your Home PAGE: http://v2aahgcan6ed564p.onion.nu
Your Home PAGE(using TOR): 3afd57c4dchzp3pe.onion
Please scroll below for your #UUID

Your #UUID is MNfYUEmu30dlgv5jnIPoD9akc

The price to obtain the decrypter goes from 500 $ to 1000 $ on the day of 04/01/2016 02:37:20

Jigsaw – I want to play a game.

- Ransom payment of $150
- Serious about its threats
  - Every hour it deletes 100 files permanently.
  - Every reboot it deletes 1000 files.
- Decrypter available now.

SAMSAM/MAKTUB

مكتوب

Samas/Samsam/MSIL.B/C

- Exploits known vulnerabilities in unpatched servers.
  - Specifically JBOSS.
  - 3.2 Million Servers vulnerable.
- Once in, laterally moves to cause the most amount of destruction

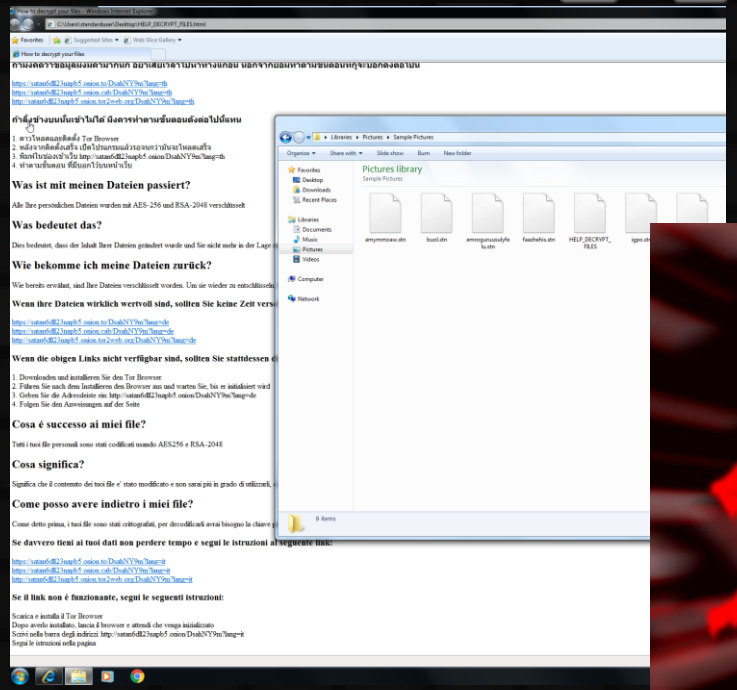
Donald Trump Ransomware

- Builds a wall around your files and,
- Makes you pay for it!

Ransomware for Skiddies…

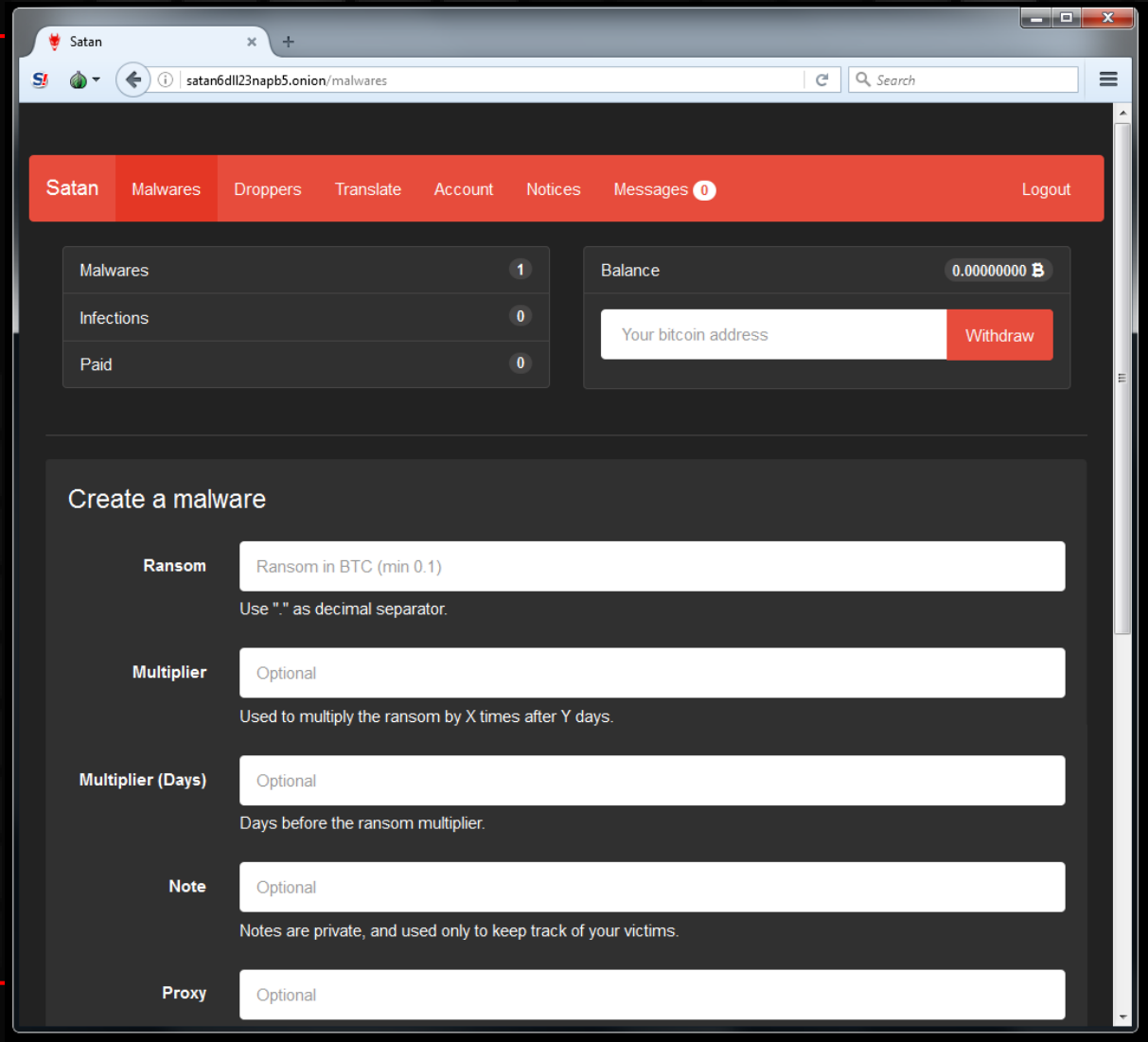
- OpenSource
  - Hidden Tear
  - Ransom
- RaaS
  - Shark/Atom
  - And…

FLAVOR OF THE MONTH



SATAN - Continued.

- Customize your ransomware:
  - Pick your ransom amount.
  - Add your own BTC address.
  - Choose the multiplier.
- Authors keep 30%



Technical Analysis

Attack Anatomy

Installation

Phone Home

Key Exchange

Encrypt

Extortion

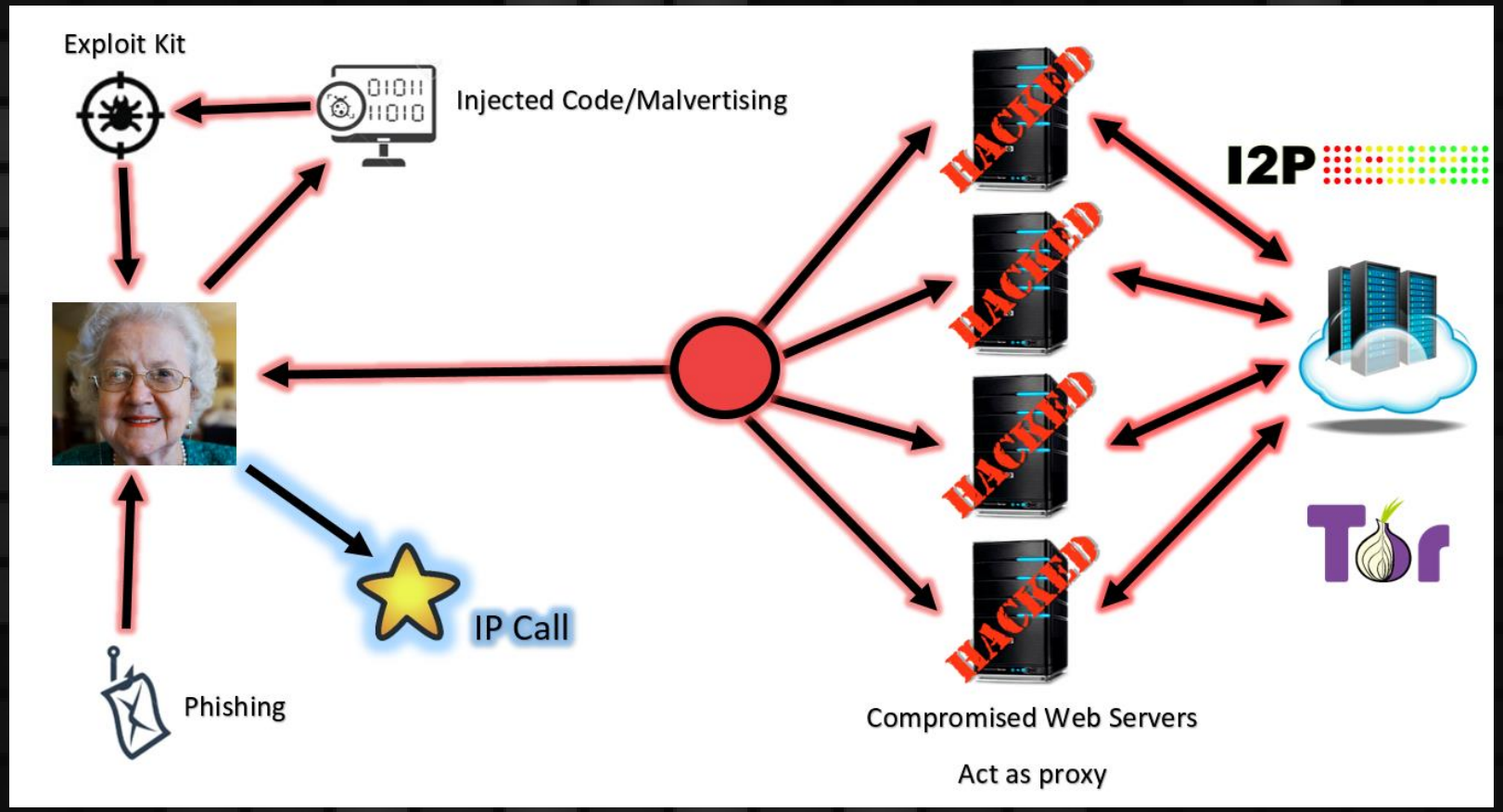
Typical Ransomware Request

- Exploit kit fires starting Process
- Geolocation call
- C2 Exchange

18:24:25	wefasdif.facetrap.io
18:24:26	m.wordpress.com
18:24:38	ip-addr.es
18:24:45	travelsecretstoday.com
18:24:45	banzaiitreesofdallas.net
18:24:45	mrchinscyberfriends.org
18:27:04	api.uark.edu

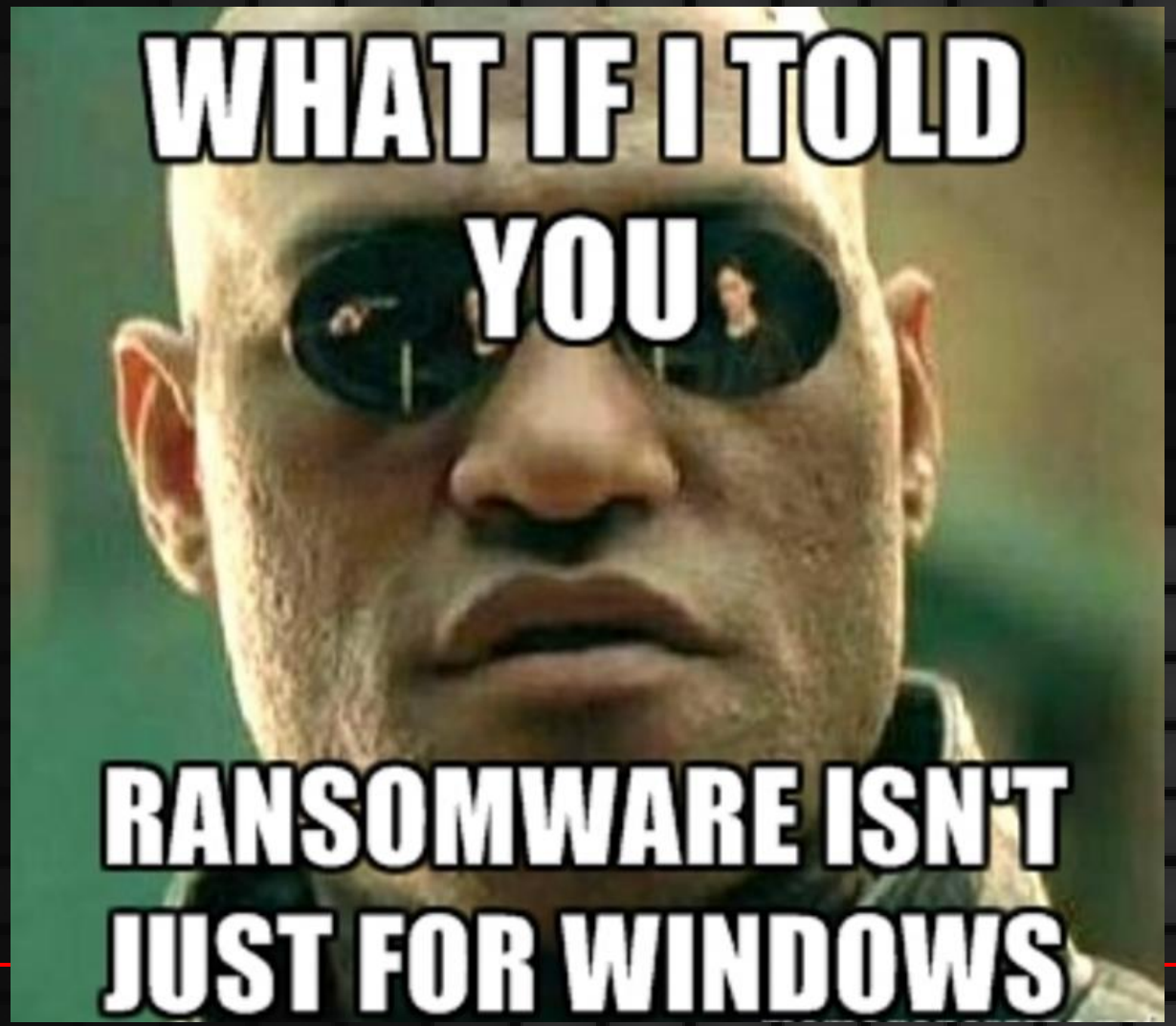
Chain of Events - a.k.a Path of Pain

- Any Attack Vectors initiates chain
  - Phishing
  - Compromised Server
  - Malvertising



The RAW IP Address

- Used for Geolocation
  - Exclude code execution or perform different operation based on global position
  - Attempt to display message in native language
- Unique Identifier
  - Added hash with other system info.
  - Can restrict one infection per IP address
  - Identify possible analysis attempts



iOS

Ransomware Evolved

Linux.Encoder Ransomware

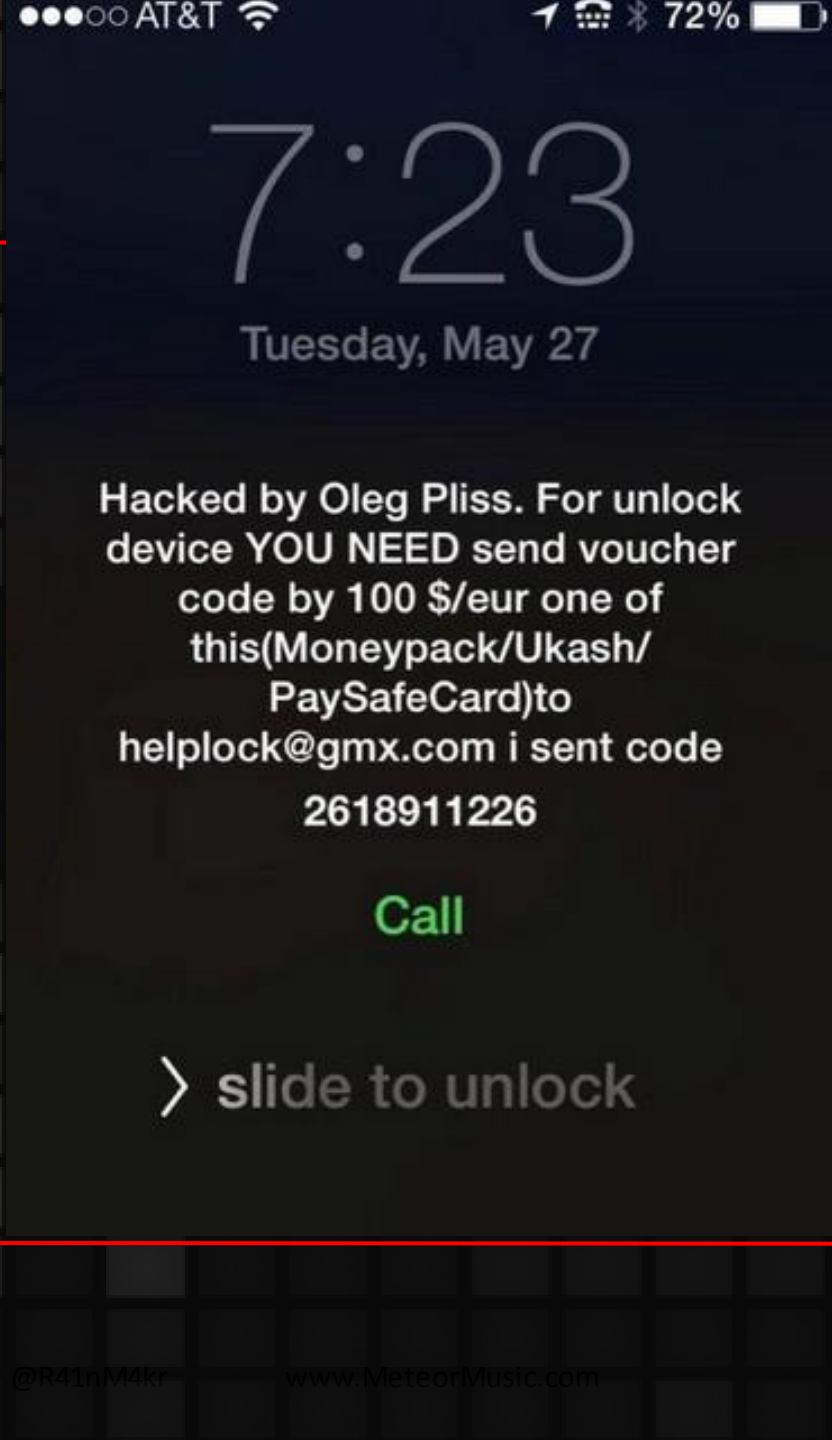
- Targets Linux powered web servers by encrypting MySQL, Apache, and home/root folders associated with the target
- Asks for 1 bitcoin to decrypt crucial files.
- 3 versions currently. All have been already decrypted
- Written by this guy.

OSX KeRanger

- Discovered March 4, 2016
- Downloaded 6000 times before it was shut down.
- Variant of Linux.encoder & “Educational” Hidden Tear Ransomware
- Recompiled into the Open Source Bit torrent client Transmission.
  - Published on their site with updated MD5 Hash.
- Turkish Developer Key was used to bypass Apple’s Gatekeeper Security Feature

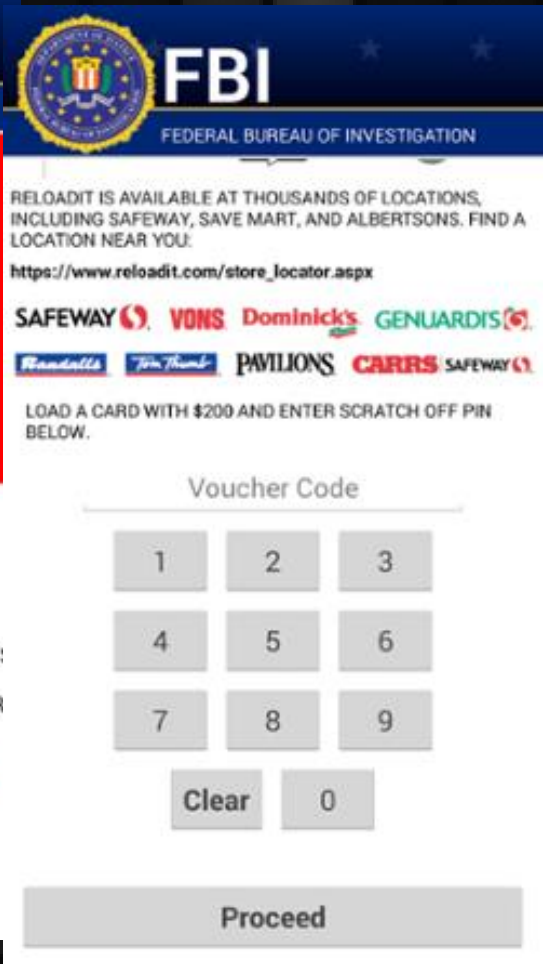
IOS “Ransomware”

- May 2014 Australian iPhone users were victims of Ransomware attack.
- Actually victims iCloud accounts were phished.
  - Devices were put in Lost (LOCKED) mode w/ ransom message.
  - Failure to pay resulted in wiped device.
- Russian Officials Arrested 2 People a month later.



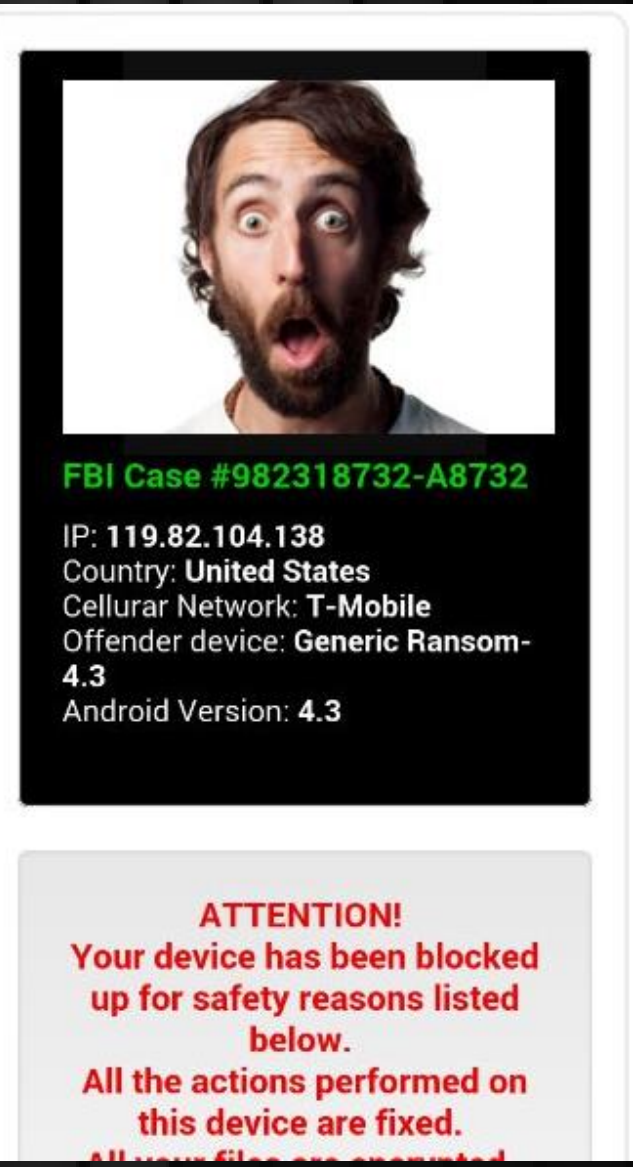
SIPLockr – 1st Android Encrypting Ransomware

- Detected June 1st, 2014
- Lots of Android Screen Lockers, but this was the first file encrypter.
- Encrypts *.jpg, *.jpeg, & *.png to *.enc
- Communicates to C2 via Tor network
- Decrypter is currently available.



Adult Player – Extortion at its Finest

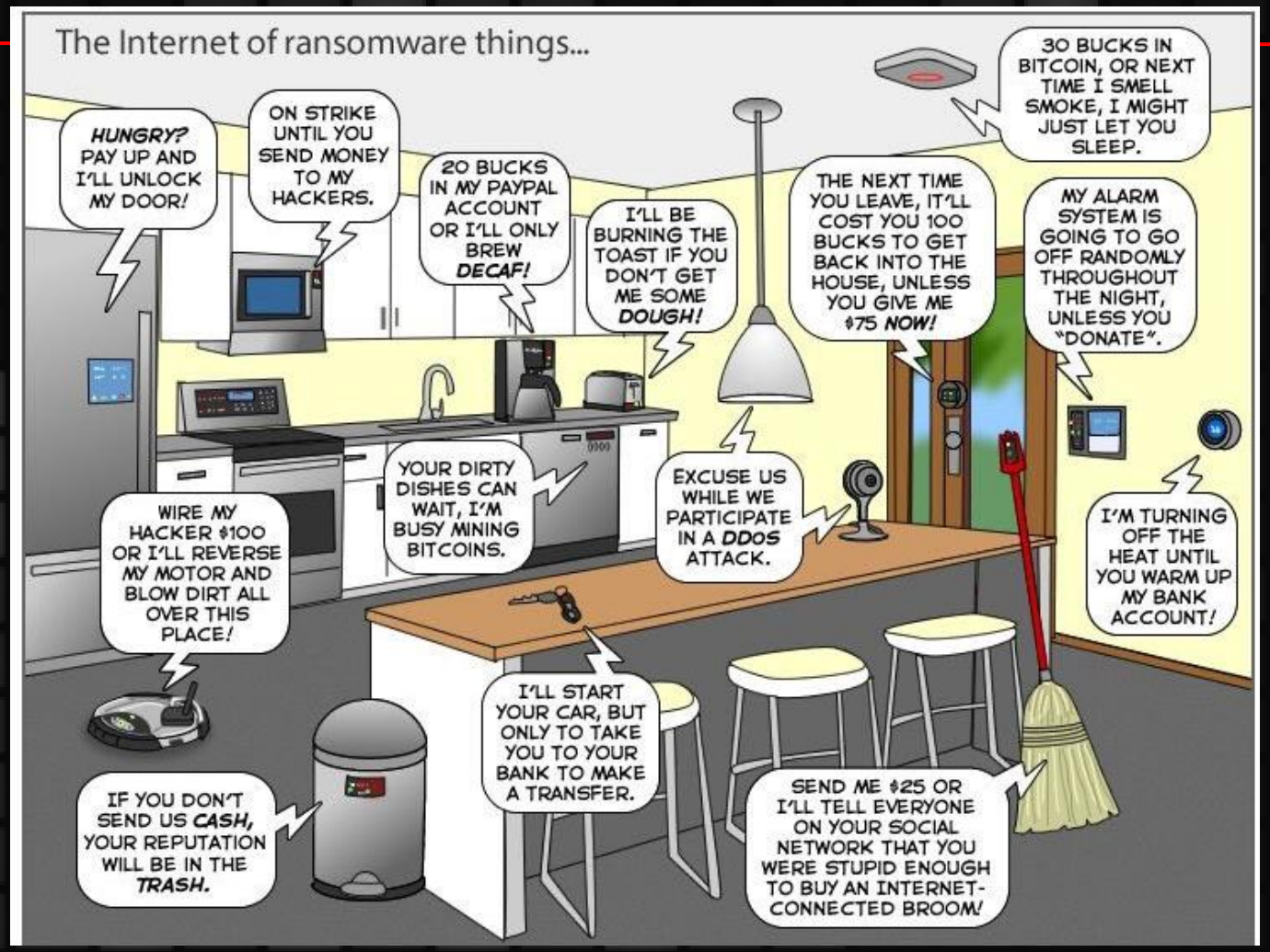
- Masquerades as a Porn Movie player.
- Takes photos using the front facing camera while in use.
- Initiate Lock screen with photos and ransom message.
  - If ransom is not paid, send message and photos to all contacts on phone.
- Easy to fix



Whats next

Internet of Things

- Institute for Critical Infrastructure Technology – “IoT presents an Infinite attack surface”.
- What’s next?
  - Pacemakers/Insulin pumps
  - Automobiles
  - Your house

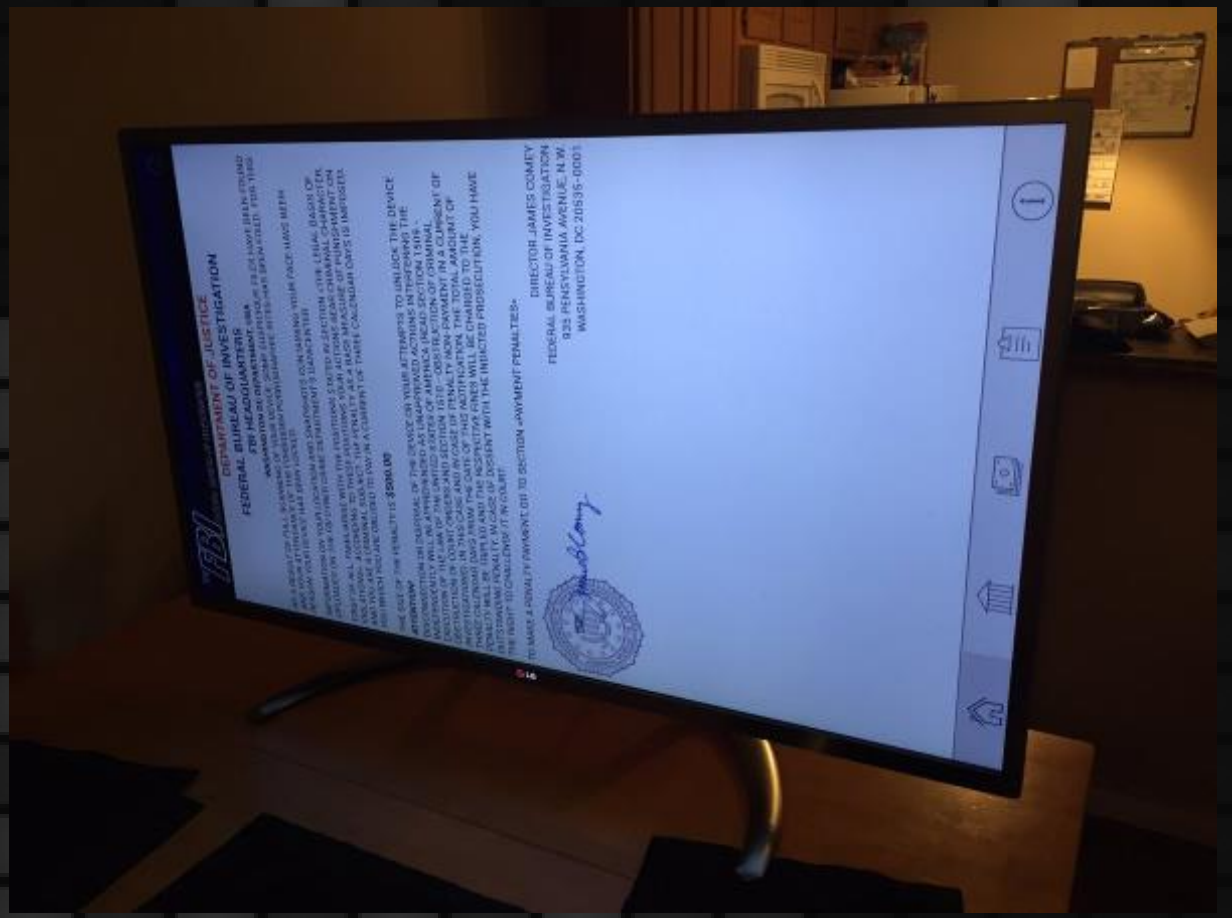


THE FUTURE IS NOW!

- Pen Test Partners at DEF CON 24 successfully compromised a connected thermostat
- Locked out of device until ransom paid
- Can also turn up/turn down temperature as part of the extortion process

No, Really…the future is NOW

- December 29, 2016
  - LG TV's are now vulnerable to ransomware.
- Ransom charges $500
- LG charges $340 for help.



Mitigation

Mitigation Techniques

- Backup often
  - Keep disconnected when not in use
- Review and restrict access to shared resources
- Disconnect from Network Shares when not in use.
- Train end-users about social engineering techniques.
  - Phishing
  - PHISHING
  - **PHISHING!**

More Mitigation Techniques

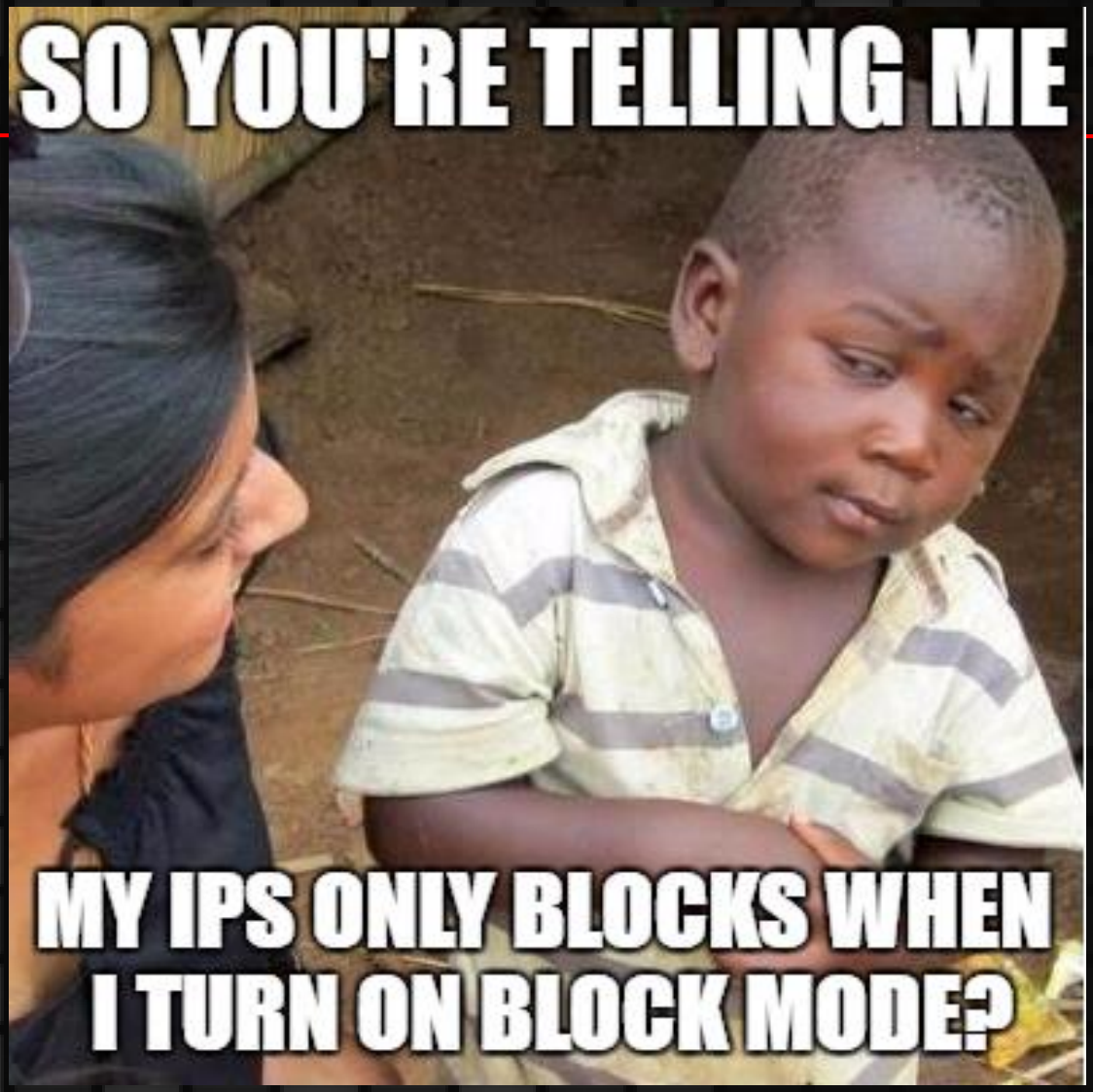
- Antivirus
  - Actually keep it updated.
- Patch the OS and software.
  - Can’t exploit vulnerabilities that have been patched.
- Prevent Malvertising/injection
  - Adblock/ublock Orgin/AdFender
  - Noscript
  - Sandboxie
- End of Life – It’s called that for a reason

Even More Mitigation Techniques

- Only install software from trusted sources
  - Follow the pack
  - Apple store is safe
    - Bad code still falls through
  - Android marketplace still iffy
    - You have to trust the developer
- Avoid Open Source Software
  - Validate Hashes from external sites

Will this guy ever stop?

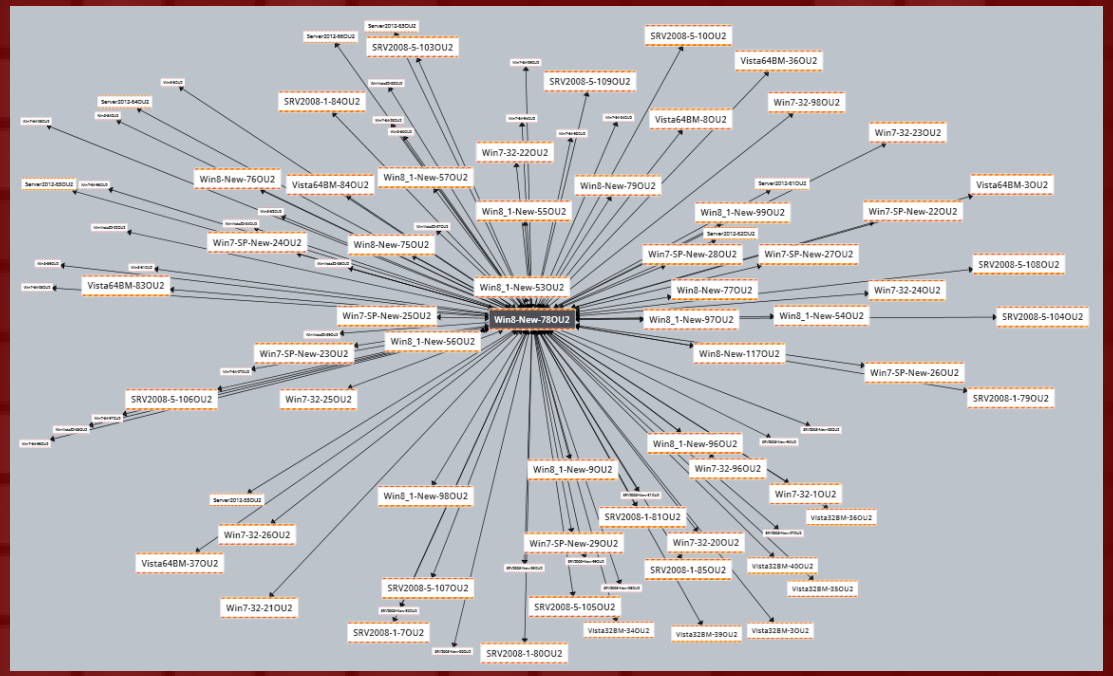
- Intrusion Prevention Systems
  - Actually implement block mode.
- Web Content Providers host their own ad content
  - Probably unrealistic, but it's a real possibility for small/medium businesses.
- Macros.
  - Do I really have to say it?
- Disassociate Dangerous Extensions.
  - js,jse,wsf,wsh,hte,lng,ps1,cmd,bat, vbs,vbe



Advanced Mitigation Techniques

Ransomware no longer wants to infect a single machine. Isolate the infection.

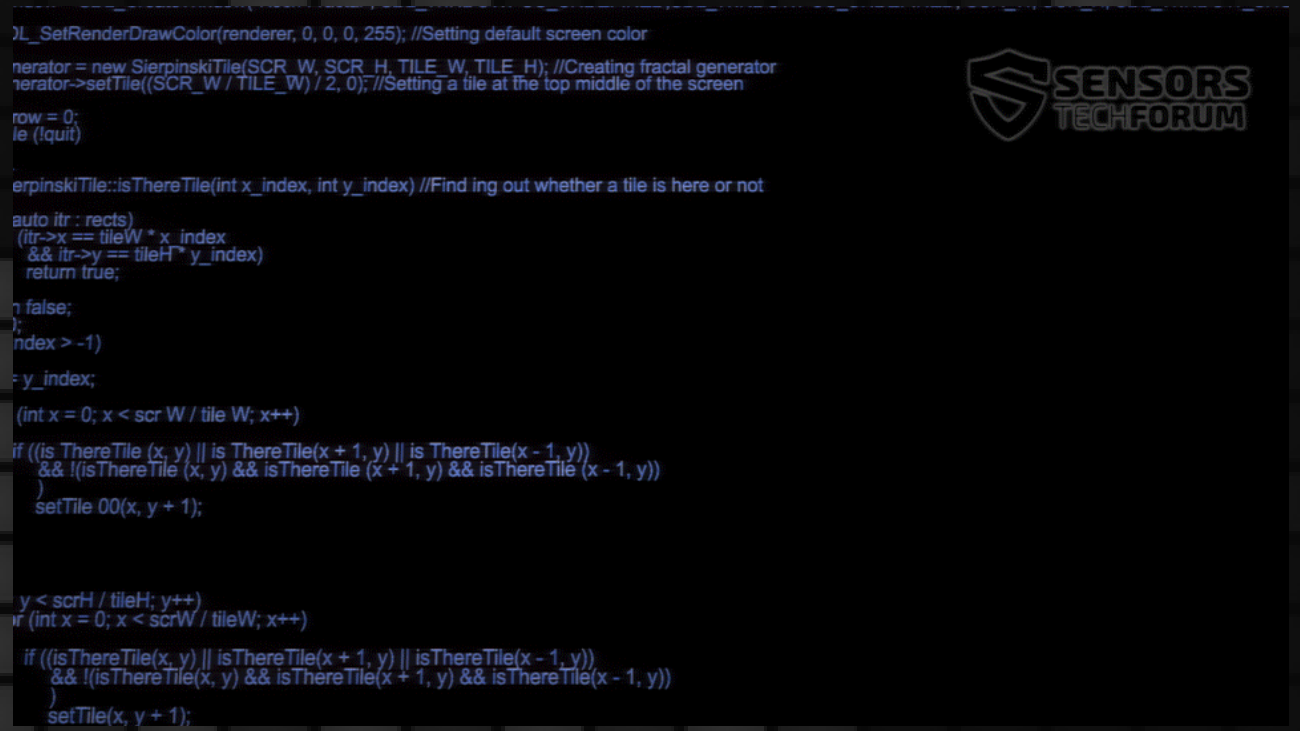
- Prevent Lateral Movement in your environment.
  - No password reuse.
  - Frequent Password Rotation.
- Enable Least Privilege
  - Not everyone needs administrative rights.
  - Even better, implement Application Control
    - Restrict the binaries from ever executing
    - **<u>AC can prevent ransomware entirely</u>**
- Isolate your Critical Resources



Final Thoughts

Reasons why you SHOULD pay.

- You get your files back. (maybe)
  - It’s in their best interest to deliver.
- FBI previously stated, “easiest path is to pay”.
- It might be cheaper.



Reasons why you Shouldn't pay.

- US-CERT & FBI clearly say no.
- It might be cheaper, but it's really not.
  - Disclosure is not cheap.
- There's a target on your back.
  - Copycat attacks are real.
- No guarantee you get your files back.
- The Criminals win.

"The FBI does not condone payment of ransom, as payment of extortion monies may encourage continued criminal activity ... or be used to facilitate serious crimes."

- Chris Stangl, a section chief in the FBI's cyber division

Help! I've been ransomwared! What do you recommend?

- Contact your friendly neighborhood hacker.
- Research the variant.
- Take the machine offline.
- Change ALL the passwords!
- Wait…wait as long as you have to.

Last slide…I swear

"An ounce of prevention is worth a pound of cure."

THANK YOU

Andy Thompson

- **Email:**
  Andy@MeteorMusic.com
- **Twitter:**
  @R41nM4kr
- **Website:**
- www.MeteorMusic.com

References

- http://thehackernews.com/2016/03/what-is-malvertising.html
- https://en.wikipedia.org/wiki/AIDS_(Trojan_horse)
- http://www.coindesk.com/fbi-malware-victims-should-pay-bitcoin-ransoms/
- https://nakedsecurity.sophos.com/2013/10/12/destructive-malware-cryptolocker-on-the-loose/
- https://blog.kaspersky.com/ransomware_targets_ios_osx/4903/
- https://threatpost.com/alleged-oleg-pliss-iphone-hackers-arrested-in-russia/106570/
- http://thehackernews.com/2016/01/linux-ransomware-decryption.html
- http://www.securityweek.com/os-x-ransomware-keranger-based-linuxencoder
- http://www.virusradar.com/en/Android_Simplocker.A/description
- http://thehackernews.com/2013/07/Android-Ransomware-malware-mohit-kumar-hacker.html
- http://www.doynews.com/tags/adult-player-android
- http://www.ibtimes.co.uk/adult-player-android-porn-app-blackmailing-users-secret-photos-demands-ransom-1518808
- https://labs.bitdefender.com/2016/03/keranger-is-actually-a-rewrite-of-linux-encoder/
- https://blog.avast.com/2015/02/10/mobile-crypto-ransomware-simplocker-now-on-steroids/
- https://nakedsecurity.sophos.com/2012/08/29/reveton-ransomware-exposed-explained-and-eliminated/
- http://arstechnica.com/security/2016/03/big-name-sites-hit-by-rash-of-malicious-ads-spreading-crypto-ransomware/
- https://en.wikipedia.org/wiki/Malvertising
- http://www.tripwire.com/state-of-security/latest-security-news/half-of-american-ransomware-victims-have-paid-the-ransom-reveals-study/
- http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html
- http://go.cyphort.com/rs/181-NTN-682/images/Malvertising-Report-15-RP.pdf
- https://www.bostonglobe.com/business/2015/04/06/tewksbury-police-pay-bitcoin-ransom-hackers/PkcE1GBTOfU52p31F9FM5L/story.html
- https://securityledger.com/2015/10/fbis-advice-on-cryptolocker-just-pay-the-ransom/
- http://www.pcworld.com/article/3046626/security/petya-ransomware-overwrites-mbrs-locking-users-out-of-their-computers.html
- http://www.bleepingcomputer.com/news/security/teslacrypt-4-0-released-with-bug-fixes-and-stops-adding-extensions/
- http://www.newsweek.com/how-counter-ransomware-attack-442779
- https://www.kent.edu/is/secureit/april-2015-victims-ransomware
- http://blog.talosintel.com/2016/03/samsam-ransomware.html?m=1
- https://threatpost.com/new-server-side-ransomware-hitting-hospitals/117059/
- http://thehackernews.com/2015/01/police-ransomware-suicide.html
- https://www.us-cert.gov/ncas/alerts/TA16-091A
- https://threatpost.com/locky-variant-changes-c2-communication-found-in-nuclear-ek/117196/
- https://en.m.wikipedia.org/wiki/Ransomware
- http://mobile.reuters.com/article/idUSKCN0X502K
- http://www.csoonline.com/article/3101863/security/report-only-3-percent-of-u-s-companies-pay-attackers-after-ransomware-infections.html
- https://www.herjavecgroup.com/hackerpocalypse-cybercrime-report
- http://virusguides.com/free-decrypter-philadelphia-ransomware-available/