WannaCry and other Ransomware—Strategies and Approach for Preventing and Removing It

Presenter: George Sconyers, Omega ATC

CONEXXUS
solve forward

Agenda

- Housekeeping
- Presenters
- About Conexxus
- Presentation
- Q & A

Housekeeping

This webinar is being recorded and will be made available in approximately 30 days.

- YouTube (youtube.com/conexxusonline)
- Website Link (conexxus.org)

Slide Deck

- Survey Link – Presentation provided at end

Participants

- Ask questions via webinar interface
- Please, no vendor specific questions

Email: **info@conexxus.org**

Presenters

Conexxus Host & Moderator

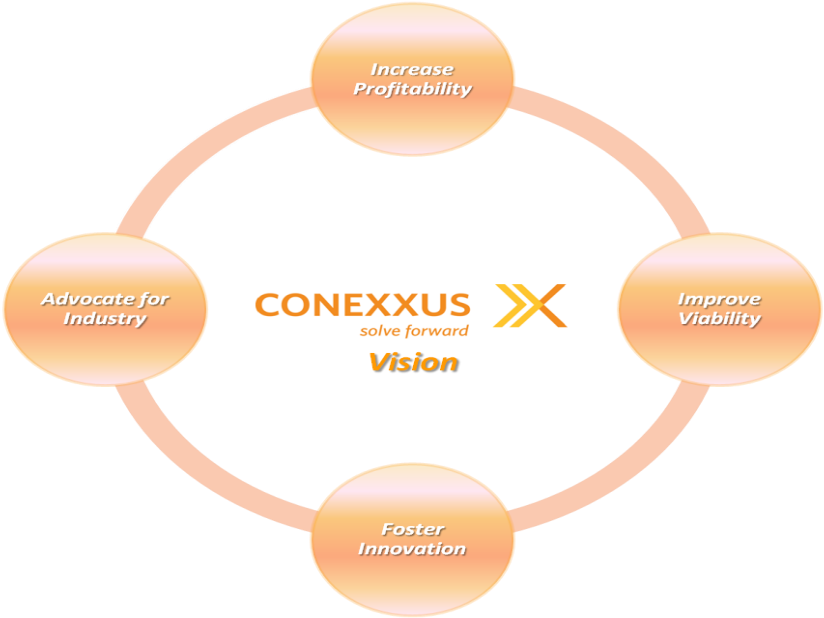
Allie Russell
Conexxus
arussell@conexxus.org

Speaker

George Sconyers
Senior Solutions Architect
Omega ATC
george.sconyers@omegasecure.com

About Conexxus

- We are an independent, non-profit, member driven technology organization
- We set standards…
  - Data exchange
  - Security
  - Mobile commerce
- We provide vision
  - Identify emerging tech/trends
- We advocate for our industry
  - Technology is policy



2017 Conexxus Webinar Schedule*

Month/Date	Webinar Title	Speaker	Company
June 29, 2017	WannaCry and other Ransomware—Strategies and Approach for Preventing and Removing It	George Sconyers	Omega ATC
July, 2017	Third Party Risk Management: How to Identify and Manage Data Security Risks from your Vendors	Sam Pfanstiel	Coalfire Systems
August, 2017	Using the NIST Cybersecurity Framework to Guide your Security Program	Chris Lietz	Coalfire Systems

TECHEDGE

In partnership with CONEXXUS

At the NACS Show
October 17-20, 2017
Chicago, IL
Booth 4584

CONEXXUS
solve forward

Ransomware Attacks are Everywhere

- Feb 2016, Hollywood Presbyterian Medical Center
  - Paid $17,000
  - Down 10 days
- Black Friday Nov 25th, San Francisco Muni Transport Agency
  - RW demands $73,000
  - 2 days to restore from backups, passengers rode free
- Dec 2016, Circle Sport-Leavine Family Nascar race team
  - Paid $500 ransom to get race car control files back so they could race
  - Dave Winston, crew chief, got bitcoin from ATM at suburban Charlotte, N.C. C-store
- Jan 2017, Cockrell Hill, TX police department
  - RW demanded $4000 in Bitcoin
  - Didn't pay based on FBI input and lost 8 years of video evidence and case files
- Two petro operators in the US also recently suffered RW attacks
  - Elected to pay the fines in order to get their data back
  - Don't want their names disclosed

CONEXXUS solve forward

RW Attacks Rates are Going Ballistic

- IBM Study – Emails with RW payload up 6000% in 2016
- RW payloads in 40% of all spam email
- 70% of RW victims payed ransom
- 50% paid > $10,000
- 20% paid > $40,000
- 40% consumers surveyed would pay > $100

CONEXXUS solve forward

Attacks on Businesses

- Datto Study – 1,100 IT service provider professionals
- 92% had clients that suffered RW attacks
- 40% had suffered >6 attacks
- 31% had multiple RW incidents in single day
- Less than 1 in 4 incidents reported to authorities

CONEXXUS solve forward

Ransomware Presentation Agenda

- What is Ransomware?
- Ransomware Families and Expansion
- What does it look like and what does it do exactly?
- How to Defend Against Ransomware
- To Pay or Not to Pay?
- What’s Next?
- Reporting to Authorities

CONEXXUS solve forward

What is Ransomware?

- Malware that blocks access to a victim's data or threatens to expose it publicly until a ransom is paid
- Some ransomware moves data to attacker's servers
- Delivered primarily via email attachment or malicious website
- Can migrate between systems once within an organization

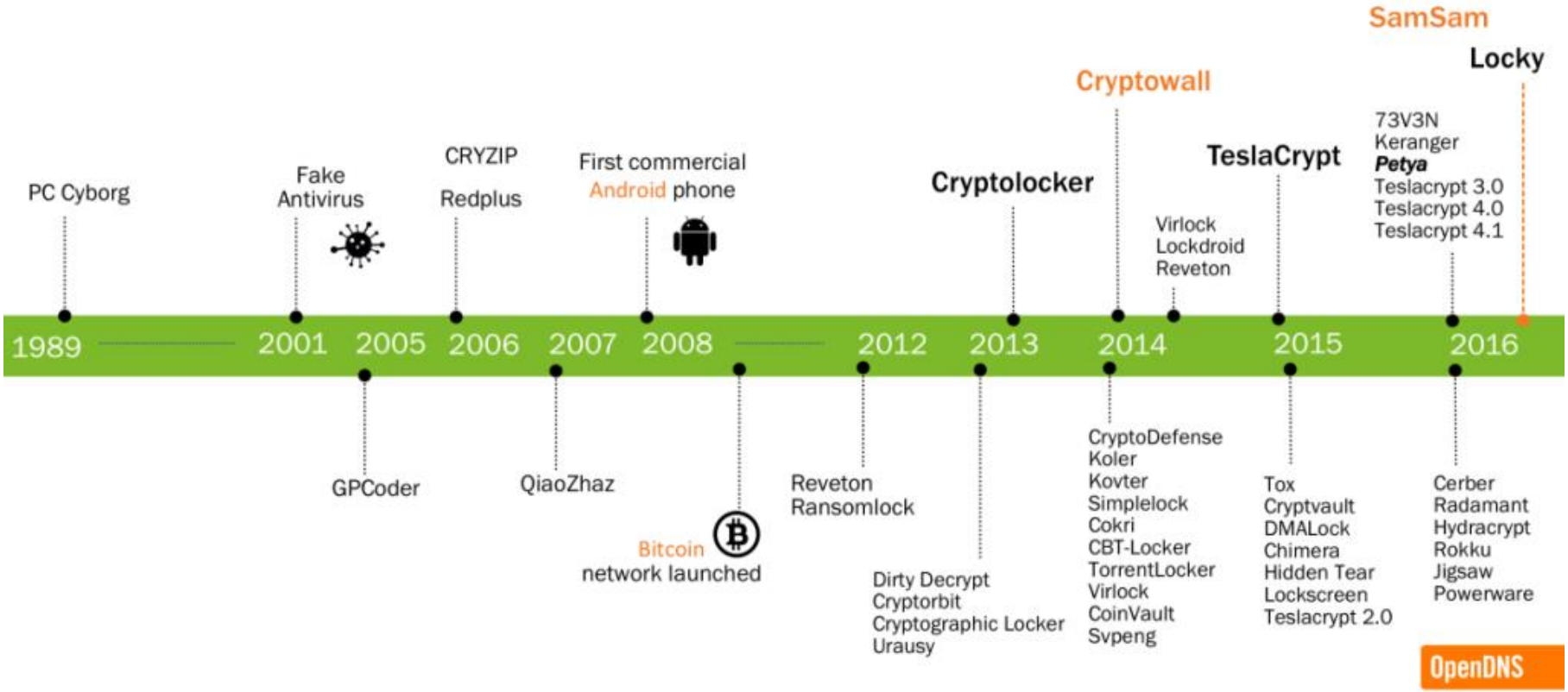
CONEXXUS solve forward

Recent Expansion of Ransomware Families

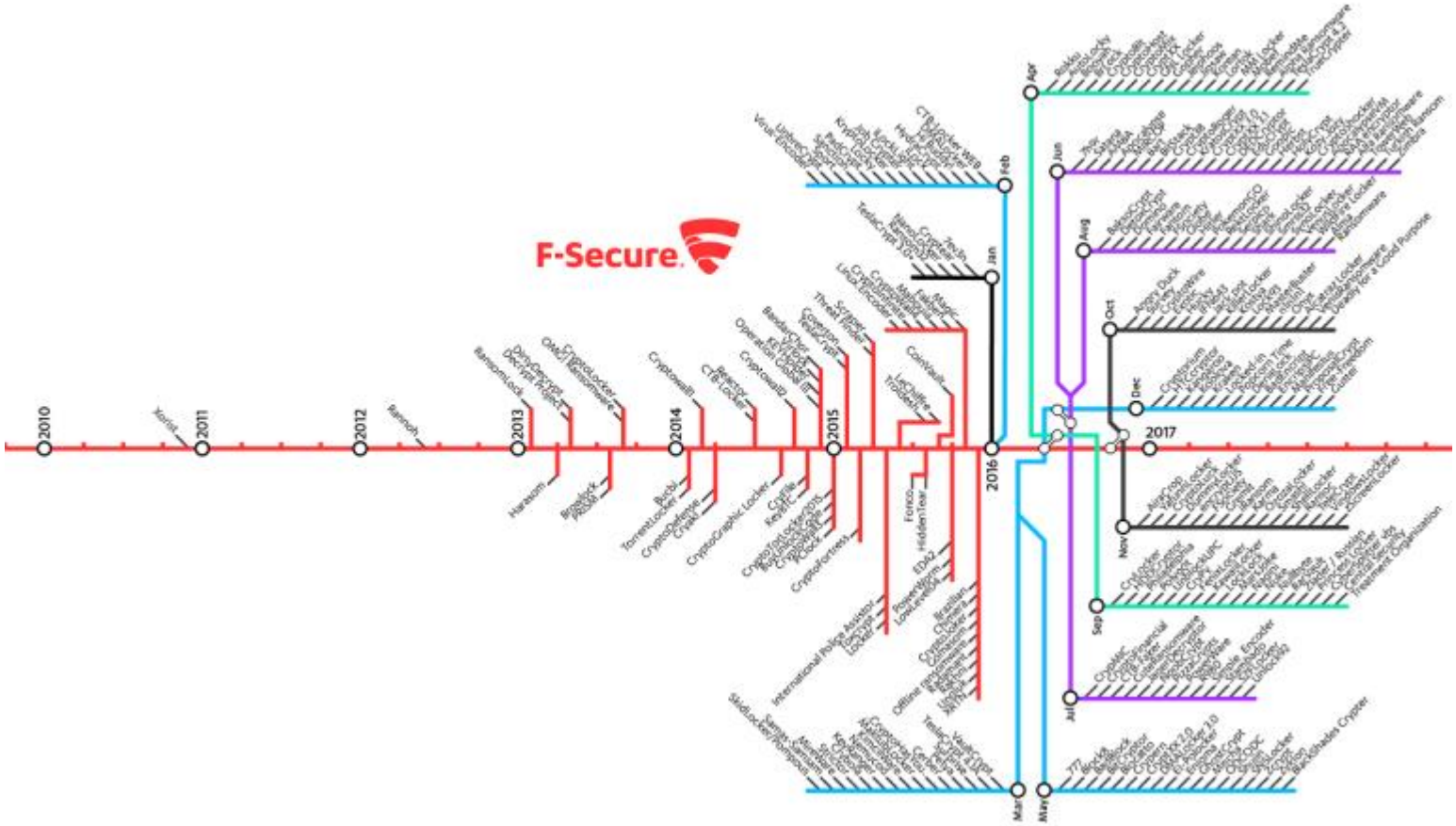
Family graph screen shots courtesy of:

OpenDNS / Cisco Systems Corp & F-Secure

CONEXXUS solve forward



CONEXXUS
solve forward



CONEXXUS solve forward

Exploit Kits and Ransomware as a Service

- On the Dark Web – reach with The Onion Router (TOR)
- Very little technical expertise needed use kits or service
- Simple Exploit Kits – provide email, RW payload, creates word document with embedded code - <$50
- RaaS Complete service – exploit, bot delivery, installation & trouble shooting, 24X7 support, purchase shopping carts, maintenance updates, consulting, ransom payment handling!
- Some offer revenue sharing arrangements with attackers

Ransomware Presentation Agenda

- What is Ransomware?
- Ransomware Families and Expansion
- What does it look like and what does it do exactly?
- How to defend against Ransomware
- To Pay or Not to Pay – and how
- What’s Next – MRW?
- Reporting to Authorities

CONEXXUS solve forward

Some Interesting Ransomware Families

- Locky
- Cerber
- Jigsaw
- CryptXXX
- Shade
- **WannaCry**
- **NotPetya**

CONEXXUS solve forward

Locky Ransomware – Most Active 2016

- Delivered via email / Necurs Botnet
- Encrypts & renames .locky, .zepto, .odin, .thor, .osiris
- Encrypts local files and network shares
- Deletes volume shadow copies to circumvent recovery
- No Decryption Tools (DTs) to date – but keep checking!
- New versions perform off-line encryption
- Observed recognizing and avoiding sandboxing
- Must restore from isolated backups or pay ransom

CONEXXUS solve forward

!!! IMPORTANT INFORMATION !!!!

All of your files are encrypted with RSA-2048 and AES-128 ciphers.
More information about the RSA and AES can be found here:
http://en.wikipedia.org/wiki/RSA_(cryptosystem)
http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.
To receive your private key follow one of the links:
1. http://[redacted]tor2web.org/[redacted]
2. http://[redacted]onion.to/[redacted]
3. http://[redacted]onion.cab/[redacted]
4. http://[redacted]onion.link/[redacted]

If all of this addresses are not available, follow these steps:
1. Download and install Tor Browser: https://www.torproject.org/download/download-easy.html
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: [redacted].onion/[redacted]
4. Follow the instructions on the site.

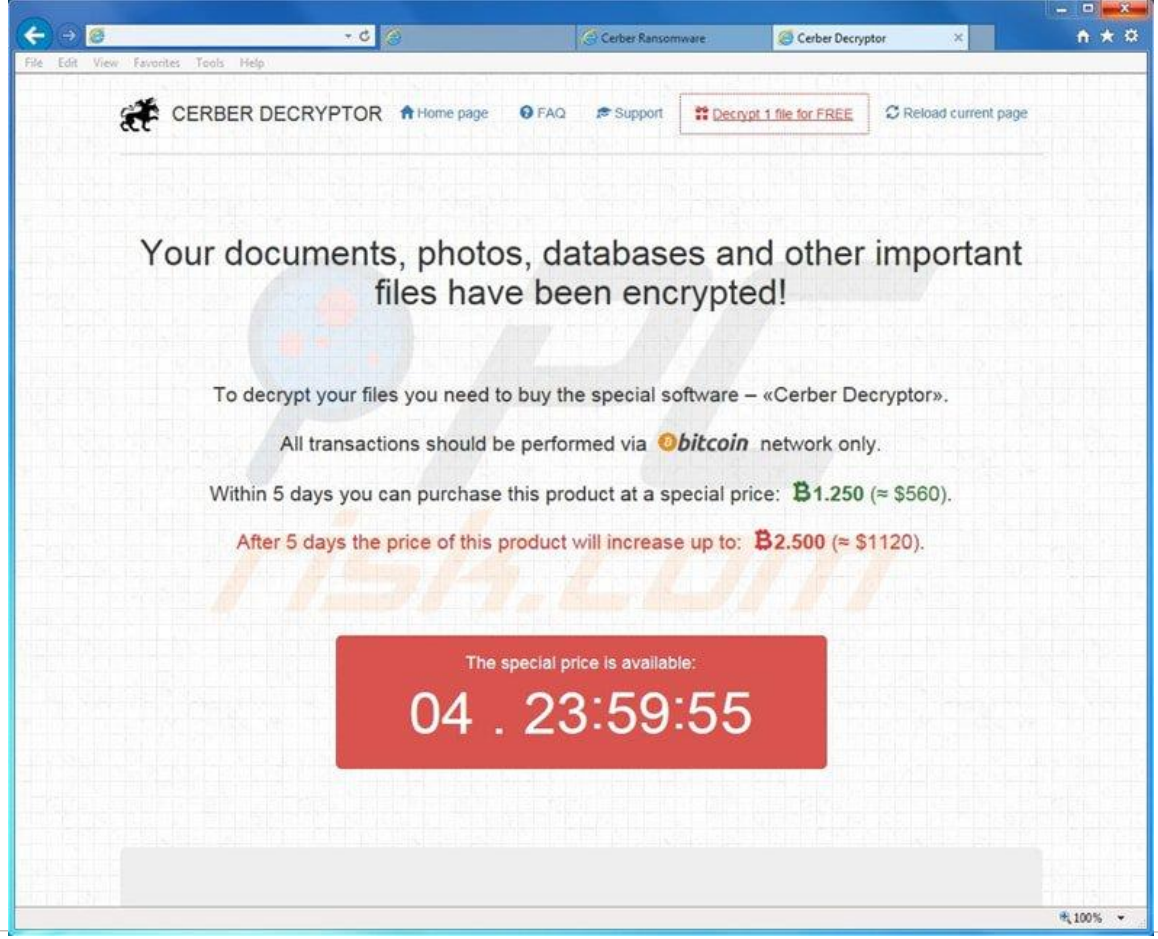
!!! Your personal identification ID: [redacted]!!!

"Locky" sets your wallpaper to make sure you know what to do next

CONEXXUS solve forward

Cerber – New in 2016

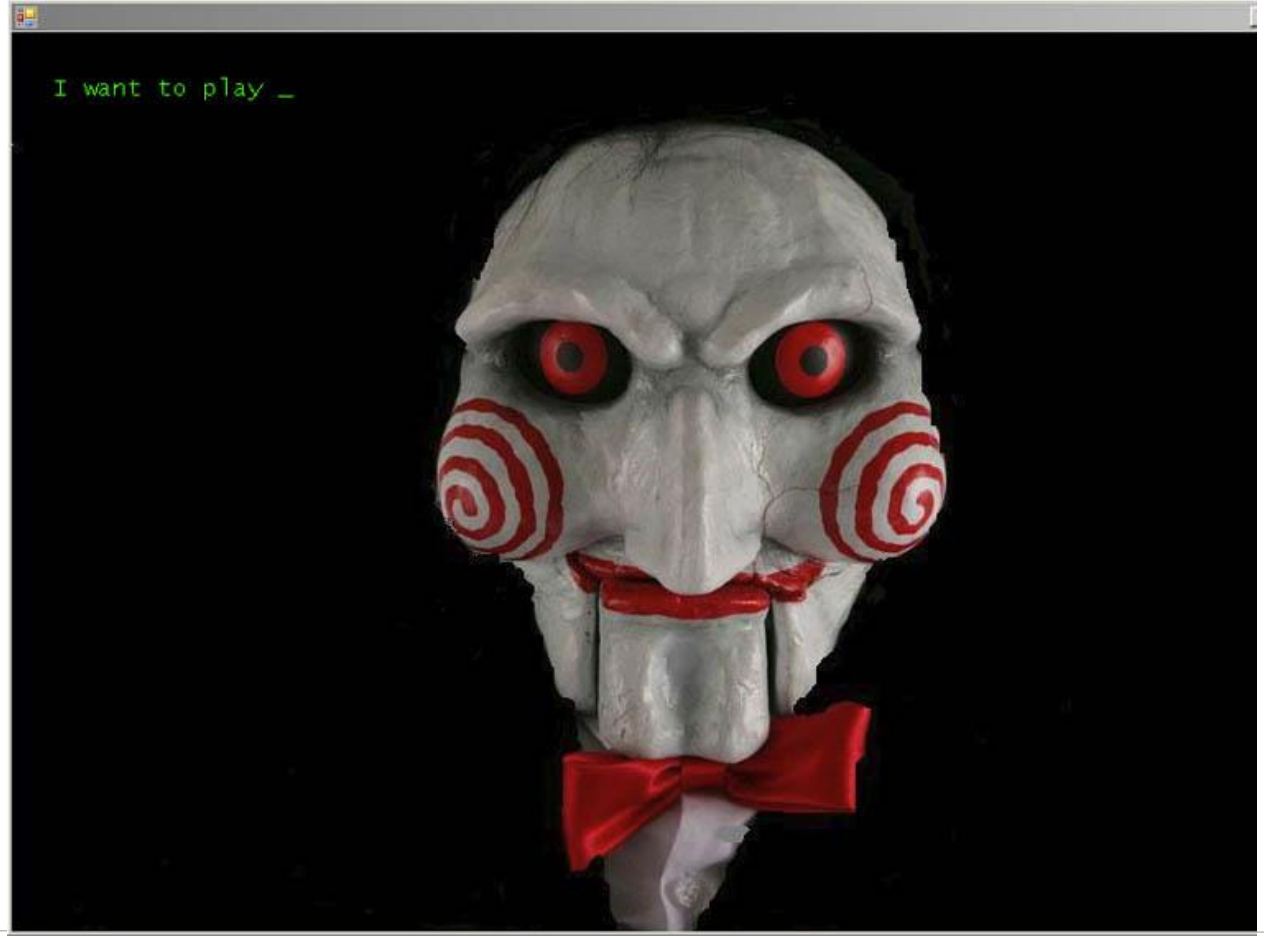
- Uses VBScript to “speak” to victims – talking head
- Launched as RaaS
- RaaS Partners share 40% of revenues with authors
- Early versions .cerber extension
- Newer variants use random extensions
- Can stop database operation to encrypt them
- Decrypt tool for .cerber files, no DT for new variants



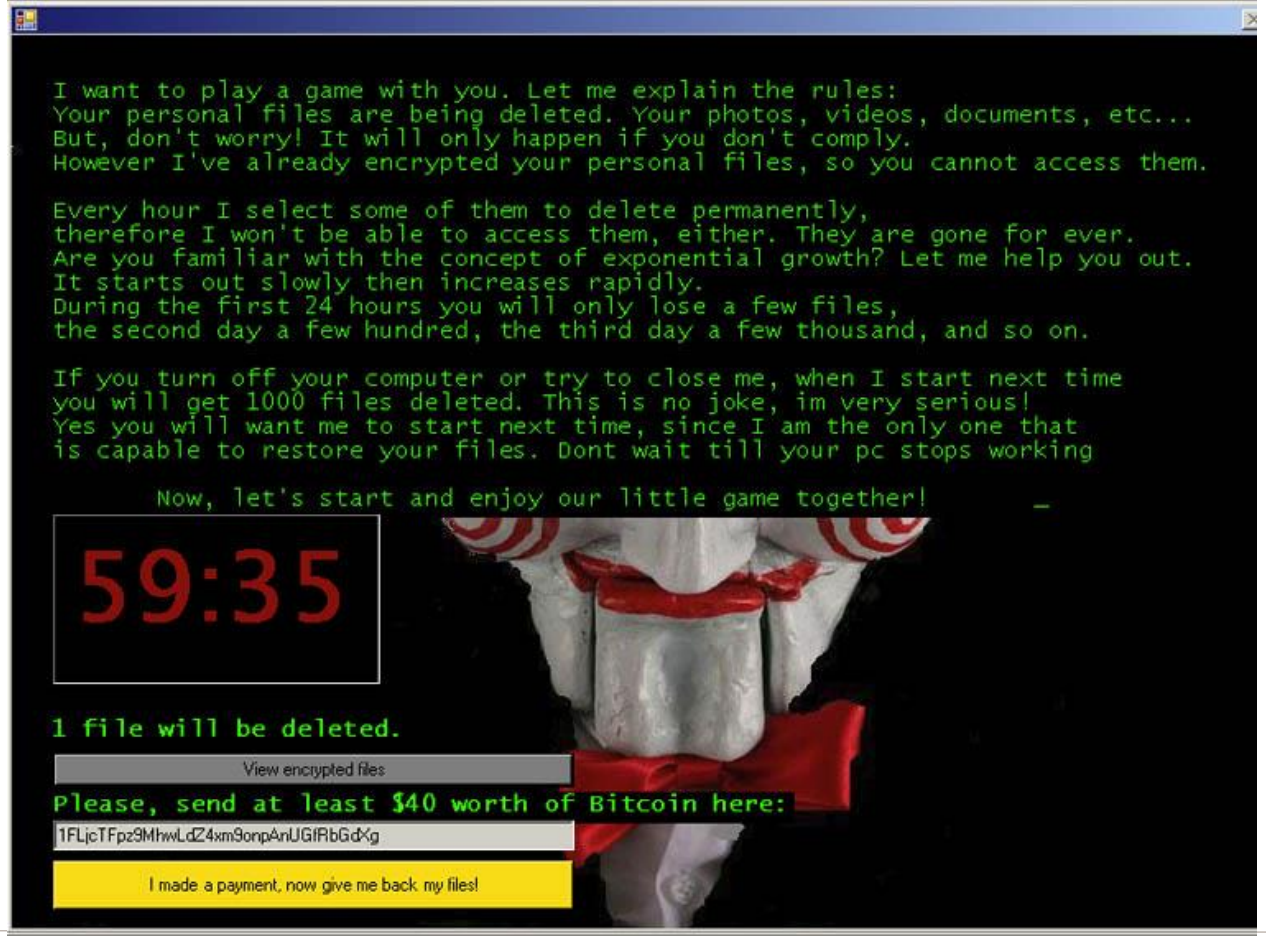
CONEXXUS solve forward

Jigsaw – You have to move fast!

- Extensions .payransom, .btc, .paybtcs, and many others
- Counts down one hour at a time
- Starts deleting files in one hour increasing the number each hour to 100, 1000 etc.
- If you reboot, it deletes 1,000 files upon startup
- Get your BitCoin ready!

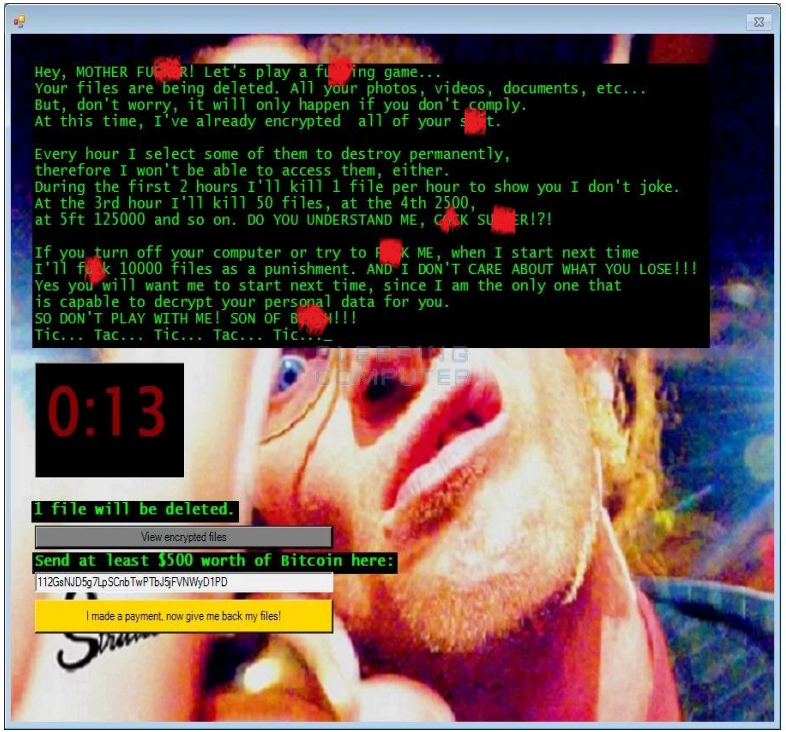


CONEXXUS
solve forward



CONEXXUS solve forward

Some Ransomware - More Bark Than Bite



- Not Jigsaw
- Stutterware – June 4th
- Doesn’t Actually Delete

CONEXXUS solve forward

CryptXXX

- Follow-on to TeslaCrypt, .crypt extension
- Delivered via Angler and Neutrino Exploit Kits, now?
- Steals credentials in addition to encrypting
- Some decryptor tools have been developed
  - https://support.kaspersky.com/viruses/disinfection/8547#block1
- CryptXXX developers have since written around many
- Determining specific version / proper tools can require help

NOT YOUR LANGUAGE? USE https://translate.google.com

What happened to your files?

All of your files were protected by a strong encryption with RSA4096
More information about the encryption keys using RSA4096 can be found here:https://en.wikipedia.org/wiki/RSA_(cryptosystem)

How did this happen?

!!! Specially for your PC was generated personal RSA4096 Key ,both 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 ?

So ,there are two ways you can choose:wait for a miracle and get your price doubled,or start obtaining BITCOIN NOW! ,and restore your data easy way If You have really valuable data,you better not waste your time,because there is no other way to get your files,except make a payment.

Your personal id

For more specific instructions,please visit your personal home page,
there are a few different addresses pointing to your page below:

1. http://7d7dkaulayebb3s3.onion.to
2. http://7d7dkaulayebb3s3.onion.cab
3. http://7d7dkaulayebb3s3.onion.city

If for some reasons the addresses are not available,follow these steps:

1. Download and install tor-browser:https://torproject.org/projects/torbrowser.html.en
2. After a successful installation,run the browser
3. Type in the address bar:http://7d7dkaulayebb3s3.onion
4. Follow the instructions on the site.

Be sure to copy your personal ID and the instruction link to your notepad not to lose them.

Shade

- Extra stages – scan, remote access, encrypt
- Scans for accounting or banking activity / content
- Installs remote access tools (RAT)
- Attackers use RAT to try an gain access to accounts
- DT available - possibly www.nomoreransom.org
- Encryption final stage – uses .xtbl, .ytbl extensions
- Shadow volume copies have been left in-tact


ВНИМАНИЕ!
Все важные файлы на всех дисках вашего компьютера были зашифрованы.
Подробности вы можете прочитать в файлах README.txt, которые можно найти на любом из дисков.
ATTENTION!
All the important files on your disks were encrypted.
The details can be found in README.txt files which you can find on any of your disks.

WannaCry Ransomware

- May 12, the WannaCry spread throughout the Internet
- Used exploit vector for missing Microsoft "Critical" patch MS17-010 released 3/14
- Infected over 200,000 computers in over 150 countries 20 different languages by May 14th
- Attackers only made approximately $100K total
- Demanded $300 or $600 per computer in Bitcoin

WannaCry Ransomware (con’t)

- Used NSA tool Eternal Blue that exploited SMB protocol
- Russian “Shadow Brokers” stole Eternal Blue in April
- “Malware Tech” researcher discovered kill switch based on URL, registered domain
- New variants have popped up with different kill switches
- Almost nobody got files decrypted by attackers – flaw in decryption process
- DT is available

Linguistic Analysis of Ransom Message and Identifying its source:

- In 28 Languages
- Accurate Simplified & Traditional different in content / tone
- English Google Translates ~95%

- Fluent in Chinese and English
- Likely dispels the idea of being Korean in origin

- Source: Flashpoint Researchers
  - Jon Condra
  - John Costello

CONEXXUS
solve forward

WannaCry Imitator!

- “Wana Decrypt0r 3.0”
- Doesn’t currently encrypt, verify
- Scareware Only

CONEXXUS solve forward

WannaCry Ransomware and Windows 10?

- Robert Lefferts, Dir of Program Management, Windows Enterprise and Security – Windows 10 not vulnerable, no customers affected.
- Not infected by WannaCry self-spreading worm
- Some got infected – they launched WannaCry by hand

WannaCry Ransomware Removal

- https://support.microsoft.com/en-us/help/890830/remove-specific-prevalent-malware-with-windows-malicious-software-removal-tool
- Also see DT slide for complete list

NotPetya (New this week!)

- Encrypts master file table of system
- Designed to do damage vs. make money
- May Likely require full system re-installation
- Posteo closed email account – can’t pay ransom
- Steals credentials first then spreads
- Spreads via Eternal Blue, PSExec and WMIC
- Appears to be a running (unrequested) chkdsk on your hard drive, then the lock screen appears – next slide…
- No DT available - c:\Windows\perfc kill switch

CONEXXUS
solve forward

Ransomware Presentation Agenda

- What is Ransomware?
- Ransomware Families and Expansion
- What does it look like and what does it do exactly?
- How to Defend Against Ransomware
- To Pay or Not to Pay?
- What’s Next?
- Reporting to Authorities

CONEXXUS solve forward

Think Like a Ransomware Attacker

Need a Hoodie!
Look the part!

CONEXXUS
solve forward

One Custom SoHoodie

~~$29.99~~ $14.99

Over 10 bought

50% off

QTY 1

Buy

Give as a Gift

Easy Returns & Exchanges! NEW

Buy with peace of mind! Learn More

Limited Time Remaining!

150+ viewed today

629 Ratings

SHARE THIS DEAL

CONEXXUS solve forward

Sorry, Just Kidding…

But Yea, Check It.

It is a thing!

CONEXXUS
solve forward

Ransomware Presentation Agenda

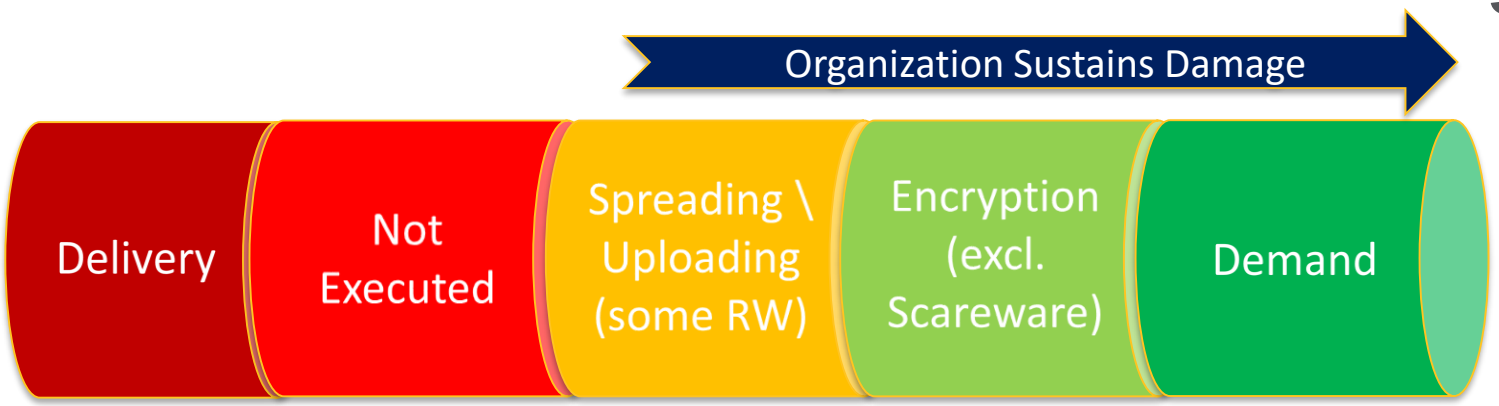
- What is Ransomware?
- Ransomware Families and Expansion
- What does it look like and what does it do exactly?
- How to Defend Against Ransomware
- To Pay or Not to Pay?
- What’s Next?
- Reporting to Authorities

CONEXXUS solve forward

Understand Ransomware Attack Stages

CONEXXUS solve forward

Understand Ransomware Attack Damage



CONEXXUS solve forward

Ransomware Attack HQ Damage

- Ransom Payment Cost – easy to understand, $10K, $20K
- Employee Lost Productivity – no computers
- Costs to re-create Lost Information – operations, store inventory, sales data, etc.
- Loyalty Program Customer Data Lost or Leaked
- HR Employee Data Leaked - Potential Legal Action!
- Vendor Relationship Impact - lost orders, payables, agreements, etc.
- Internal Corporate Plans Leaked – Value to Competitors

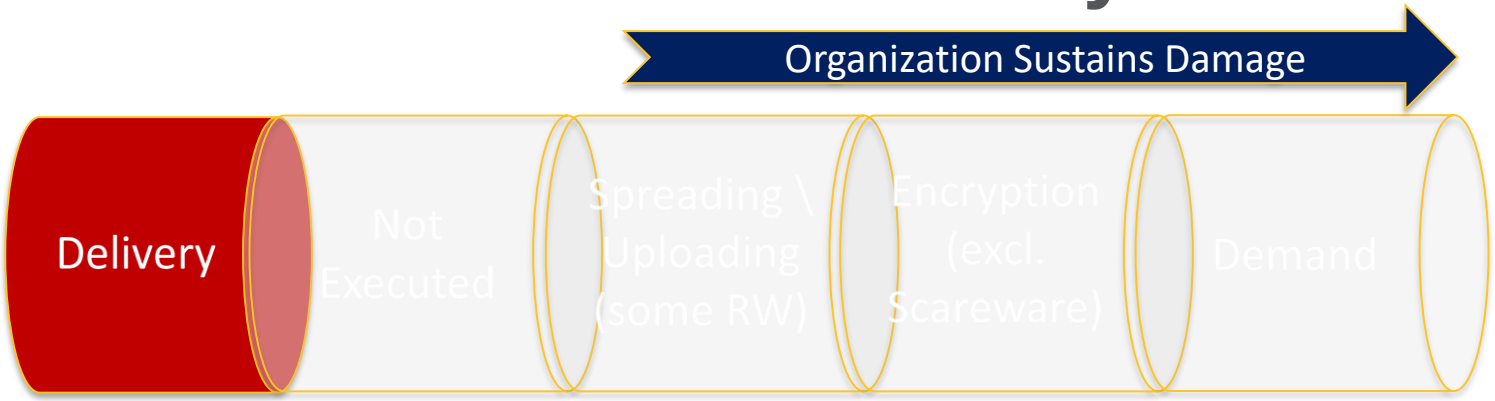
CONEXXUS solve forward

Ransomware Attack Retail Store Damage

- So your HQ gets Ransomware, handled, but wait?
- Have VPNs between HQ and store systems?
- VPN can be a Ransomware Highway right to your stores
- **All STORES POS DOWN** – Huge Revenue Hit!
- Customer PR Impact – **“Did all their stores close?”**
- **Monumental Restoration Effort** for your IT team
- **Days / weeks to recover all stores!**

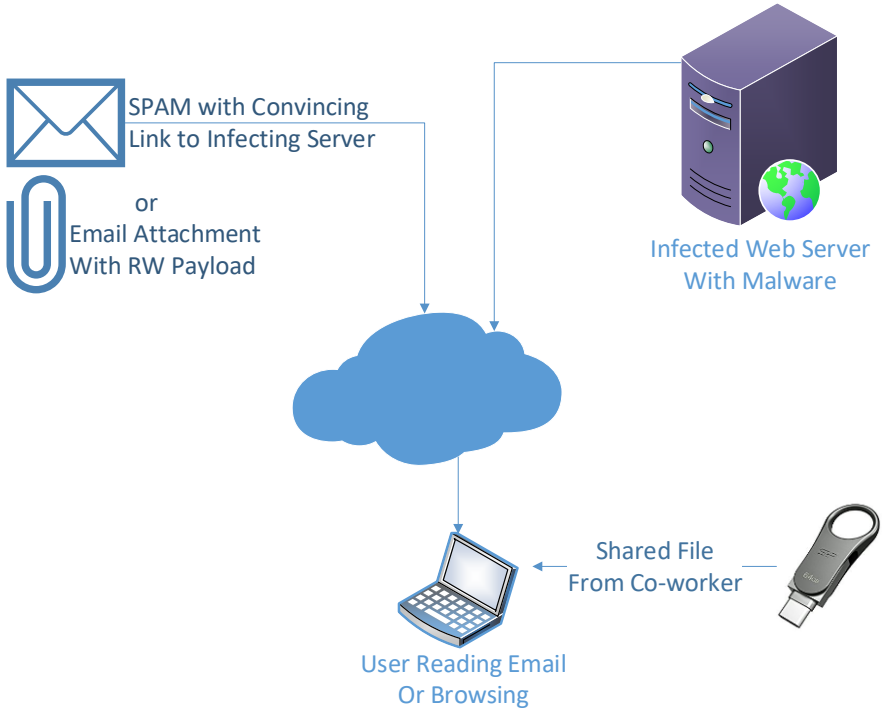
CONEXXUS solve forward

Ransomware Attack Multi-Layer Defense

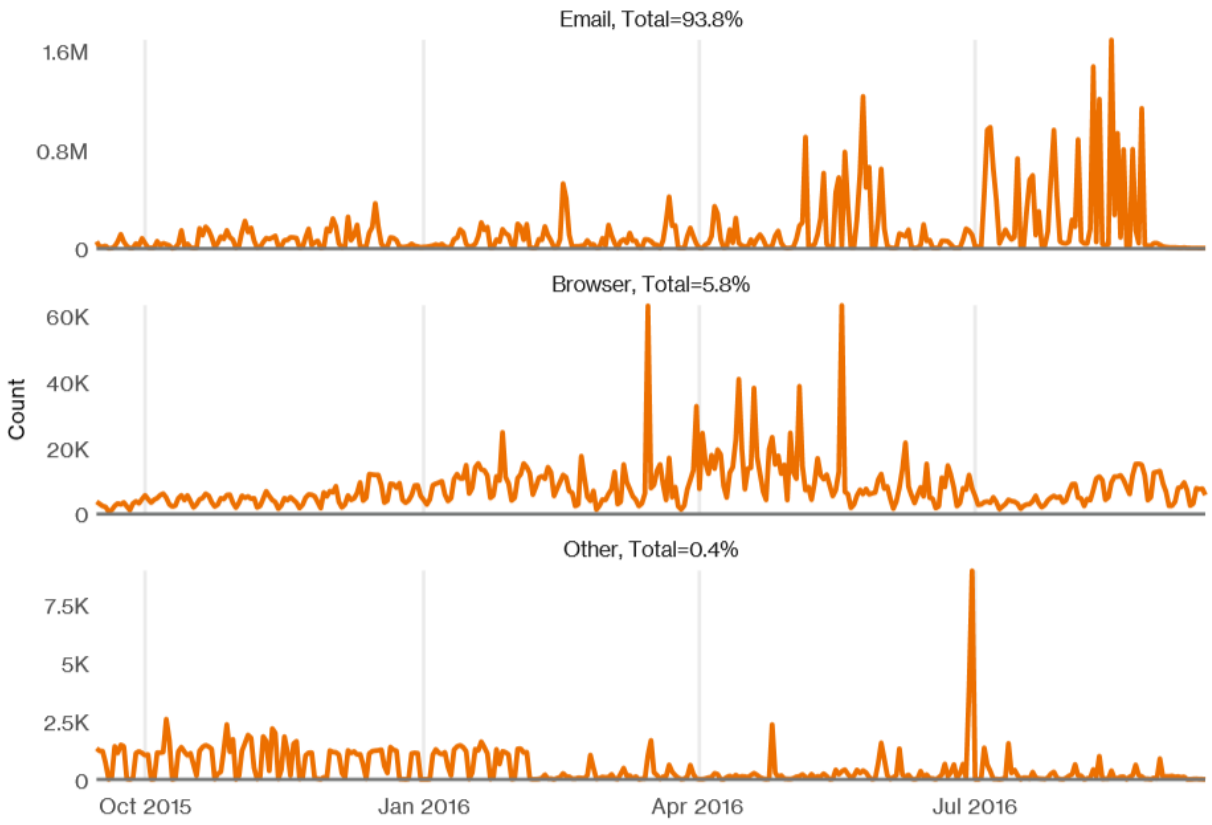


CONEXXUS solve forward

How Systems Get Infected - Delivery



CONEXXUS
solve forward



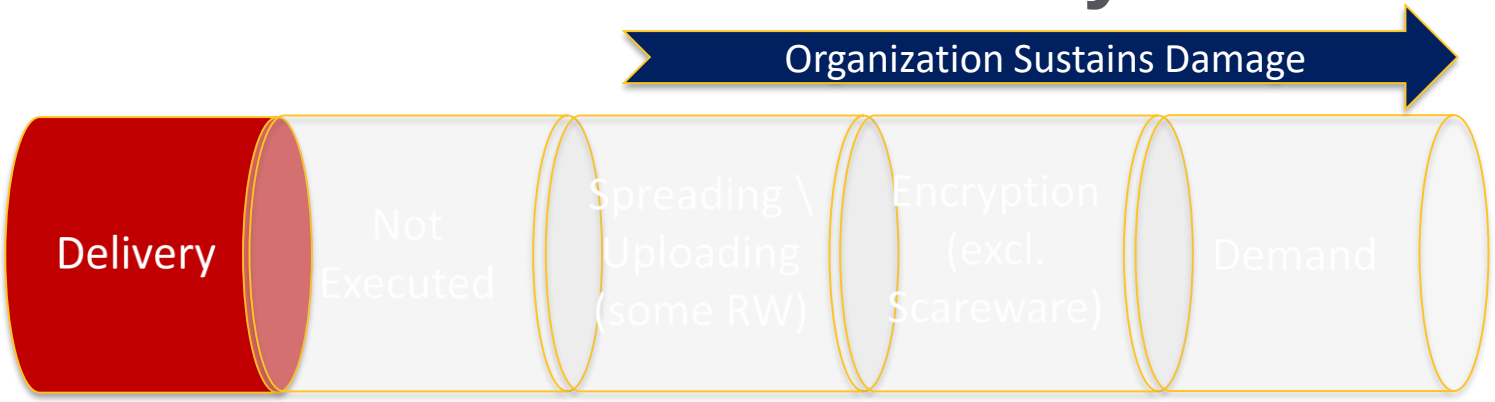
- 50 million on-the-wire detection samples
- Over 99% of malware is delivered using email or via web browsing
- Source: Verizon 2017 Data Breach Investigations Report

CONEXXUS solve forward

Why Ransomware is so Stealth

- Signature based Anti-virus doesn’t fully detect it
- Pre-execution based Defense Strategies are not reliable
- Exploit Actions slow and persistent
- Need Live / Behavior-based detection
- Machine Learning / fuzzy logic to recognize mutants
- Injects code into existing files
- Moves from file to file

Ransomware Attack Multi-Layer Defense



Firewall ATP / UTM
Centralized Email Filtering
Security Info / Event Mgmt
Security Awareness Training
Patching
Anti-Virus File Examination

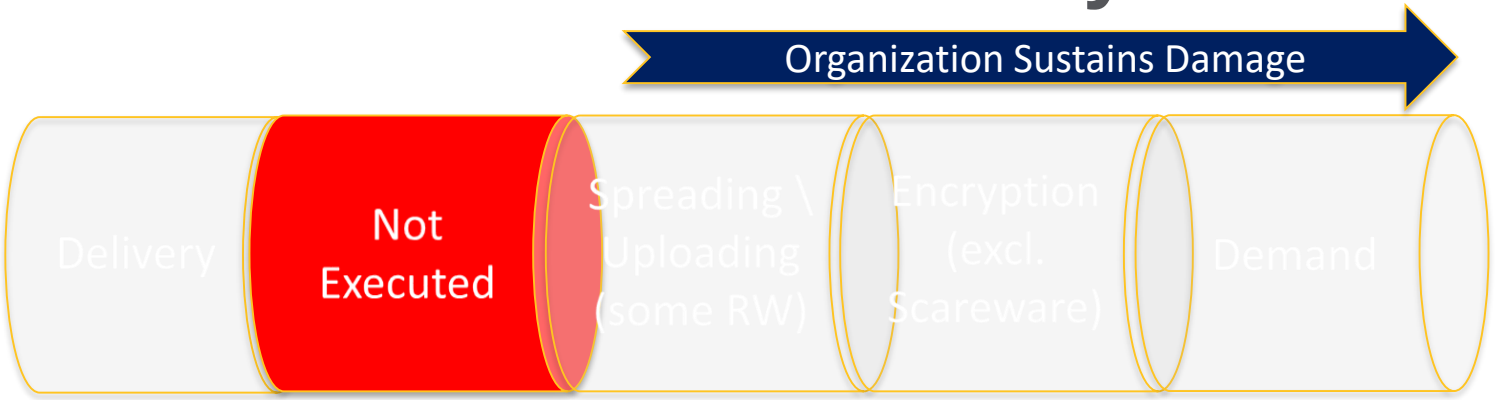
CONEXXUS solve forward

User Security Awareness Training

- Tools to assess employees – simulated phishing emails
- Assessment of where the problems are and with which employees
- Targeted Training based on assessment / analysis
- Teach employees how to detect phishing attempts
- Teach proper password management, Wi-Fi use, USB use etc.

CONEXXUS solve forward

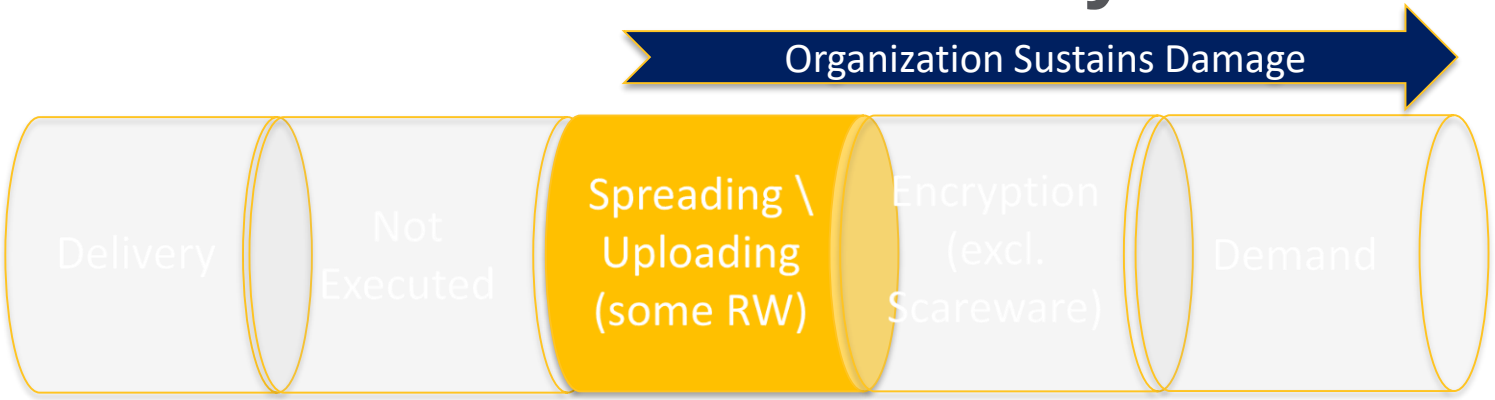
Ransomware Attack Multi-Layer Defense



Anti-Virus & Anti-Malware
Scheduled Scanning
Configuration / Change Management

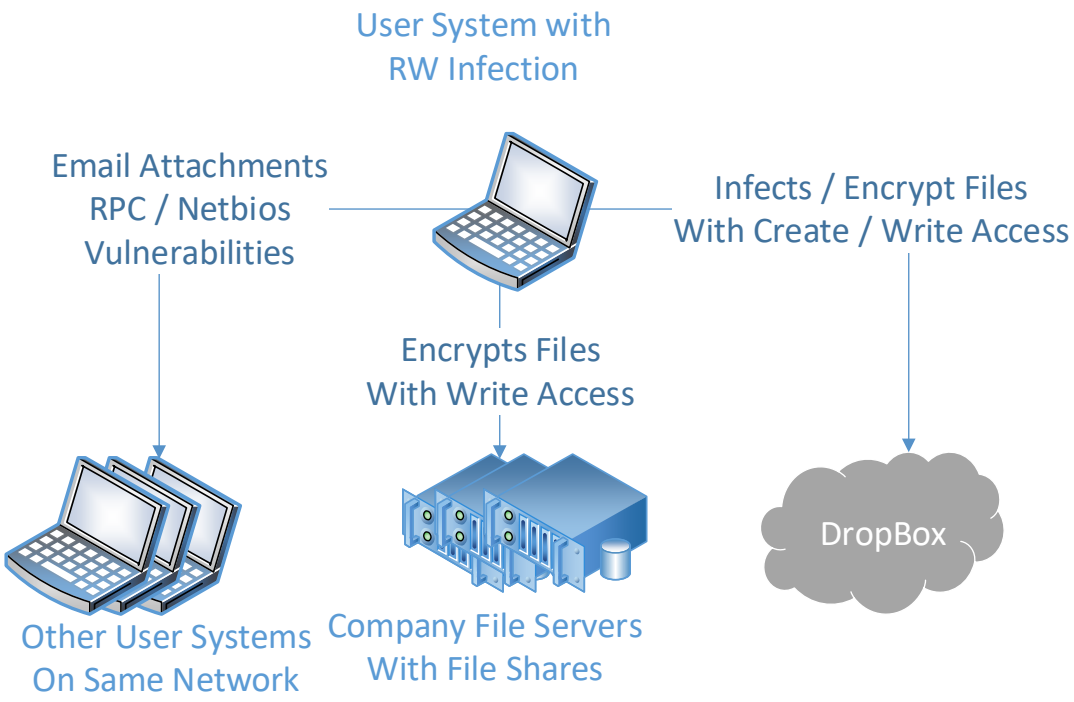
CONEXXUS solve forward

Ransomware Attack Multi-Layer Defense



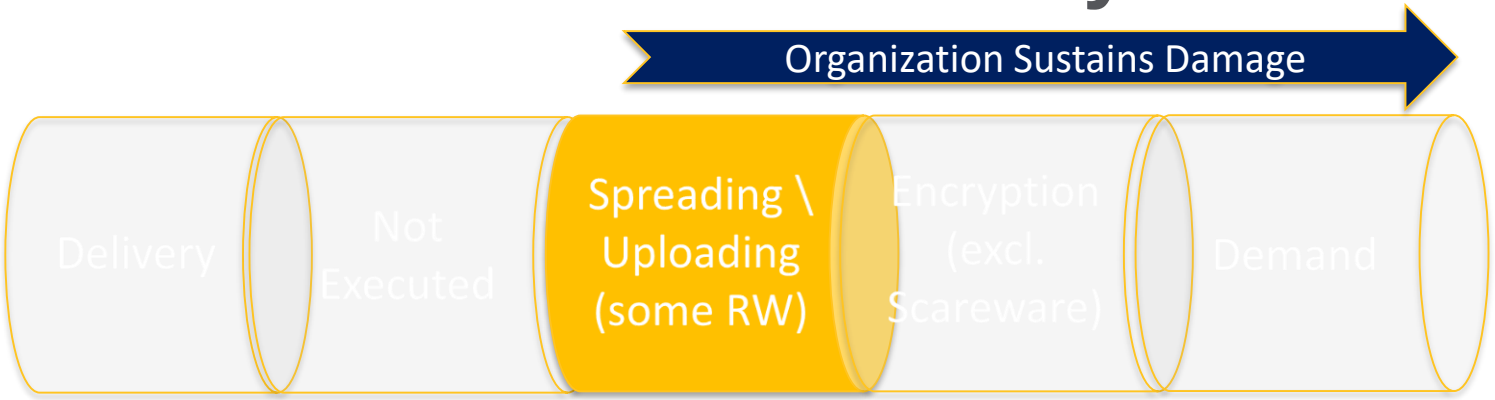
CONEXXUS solve forward

How Ransomware Spreads



CONEXXUS
solve forward

Ransomware Attack Multi-Layer Defense



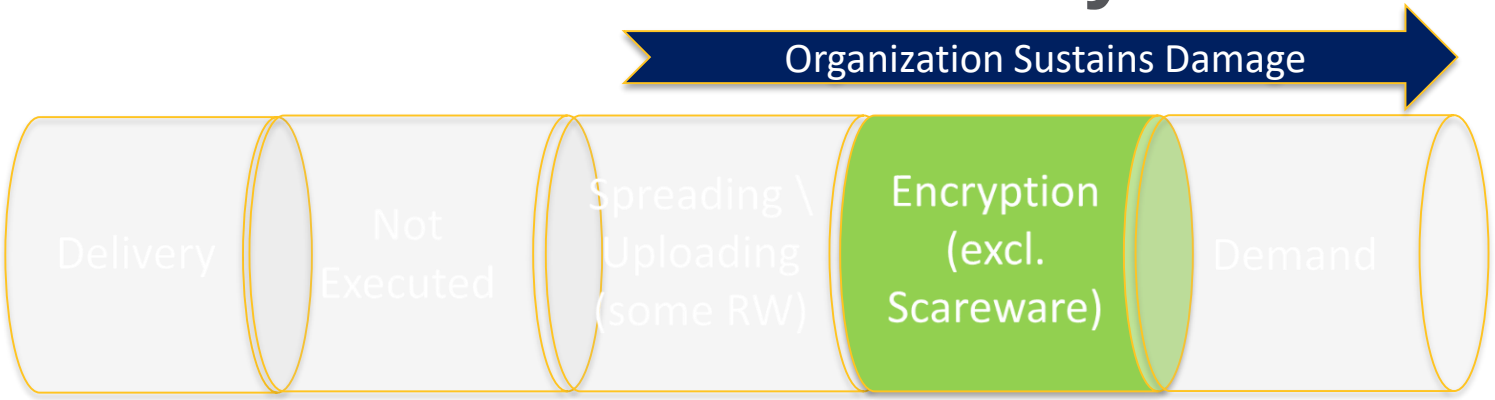
Anti-Malware Behavior Analysis
Executable White Listing
Network Segmentation
Data-Loss Prevention Tools
Internal Vulnerability Scanning
Firewall UTM (C2 blocking)

CONEXXUS solve forward

Store Internal Vulnerability Scanning

- Required quarterly for PCI
- Verify the protection of your CDE
- Look for high risk vulnerabilities
- Scan centrally over VPN from HQ scanner or locally
- Watch for false sense of security due to timeouts
- You may miss the path RW can move from HQ to Stores
- Minimize CDE footprint based on scan results - Remediate

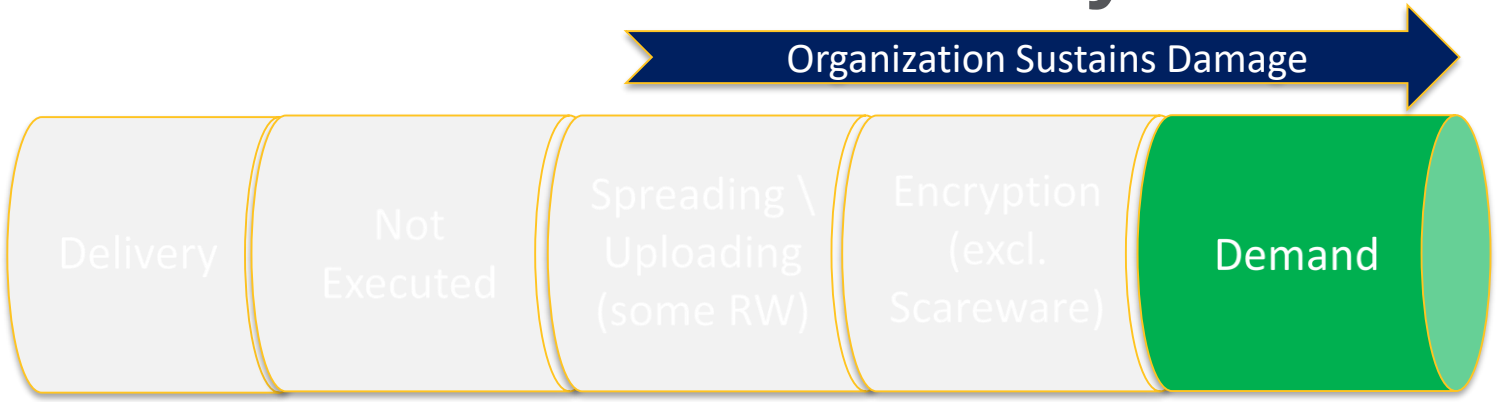
Ransomware Attack Multi-Layer Defense



File Integrity Monitoring
Shared File Server Access Controls

CONEXXUS solve forward

Ransomware Attack Multi-Layer Defense



Safe Mode Decryption Tools

File Backups

Pay Ransom

CONEXXUS solve forward

Decryption Tool Links – Caution Please!

- http://www.thewindowsclub.com/list-ransomware-decryptor-tools
  - 40+ links to decryption tools, RW identifiers, other handy RW- related utilities
  - Many of these require **strong** systems skills to use / have little documentation
  - Trust links to **commercial software companies** over others

- WannaCry Decryptor Tool:

https://success.trendmicro.com/solution/1114221-downloading-and-using-the-trend-micro-ransomware-file-decryptor#collapseSix

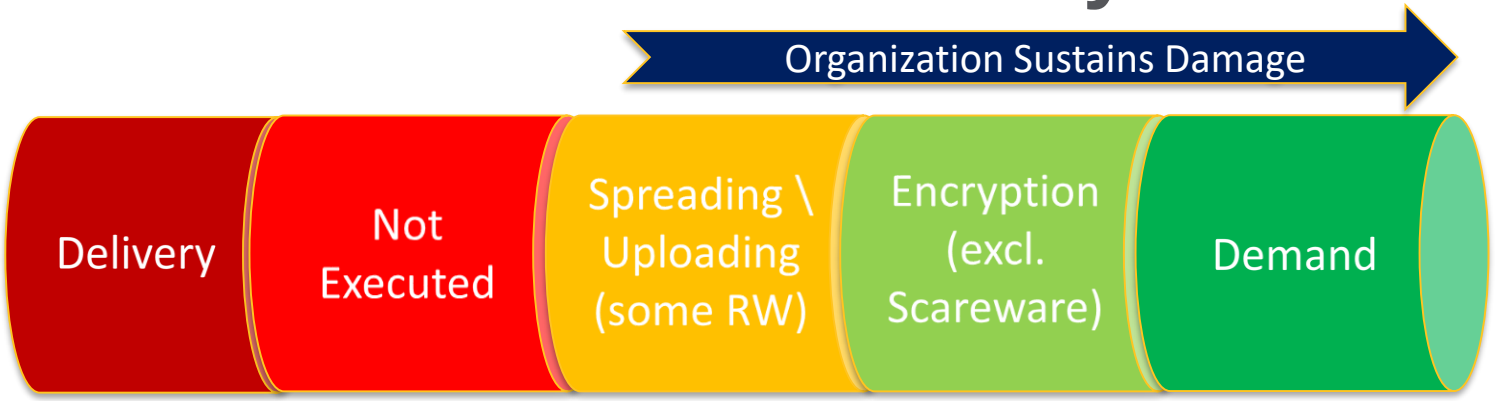
CONEXXUS solve forward

Ransomware Backup / File Sharing Issues

- USB attached backup drives with file level access get encrypted and possibly injected with malware
- Windows file share contents with continual write access get encrypted
- RW searches out all drives / folders for possible encryption targets
- Better to use cloud based backup solutions or those with proprietary backup drive access

CONEXXUS solve forward

Ransomware Attack Multi-Layer Defense



FW ATP / UTM	Anti-Virus	Behavior	File Integrity	**Decryption Tools**
SIEM	Scheduled	Whitelisting	Monitoring	**File Backups**
Email Filtering	Scanning	Net Segment	Server Access	**Pay Ransom**
User Training	Chg Mgmt	DLP Tools	Controls	
Patching		IVS		
AV File Exam		FW UTM (C&C)		

CONEXXUS solve forward

Ransomware Presentation Agenda

- What is Ransomware?
- Ransomware Families and Expansion
- What does it look like and what does it do exactly?
- How to defend against Ransomware
- To Pay or Not to Pay?
- What’s Next?
- Reporting to Authorities

CONEXXUS solve forward

To Pay or Not to Pay?

Yes or No?

CONEXXUS
solve forward

To Pay or Not to Pay?

- Can you tell what RW is demanding the ransom?
- Can you tell what has been encrypted?
- What confidential data could be exposed?
- Is a DT available from trusted company / service?
- Do you have RELIABLE backups?
- How much is the demand?
- Can you get required crypto-currency fast enough?
- Can you live with subsidizing the attackers?

Paying Ransom - What’s In Your Wallet?

1BTC ~ $2600

CONEXXUS solve forward

CONEXXUS solve forward

Paying the Ransom in Bitcoin

- Bitcoin is the most accepted crypto-currency for RW
- Get a Bitcoin Wallet – CoinPay, breadwallet, Armory
- Buy some BTC from an a BTC Exchange
- Be ready if you feel there is a possibility you will need it
- Takes too long to get it after an attack
- You might make money too!

CONEXXUS solve forward

Merchant Services that Manage Bitcoin Txs

1. Bitaps.com 2. BitBayPay 3. Bitcoin Transaction Coordinator 4. BitcoinPay 5. Bitcoinpaygate 6. BitKassa . 7. BitPagos 8. BitPay 9. BitPOS 10. BitStraat SiteCite: 11. Luno API 12. Blockchain.info 13. Blockonomics 14. **Coinbase** 15. CoinBox 16. Cashila 17. CoinCorner 18. CoinGate 19. Coinify 20. CoinPip 21. Coinsnap 22. Cryptopay 23. Cubits 24. Gourl.io . 25. Lavapay 26. OKPAY 27. PayFast 28. Paxful 29. Rocketr 30. SpectroCoin . 31. SpicePay 32. XBTerminal – source Unitrends

Ransomware Presentation Agenda

- What is Ransomware?
- Ransomware Families and Expansion
- What does it look like and what does it do exactly?
- How to Defend Against Ransomware
- To Pay or Not to Pay?
- What’s Next?
- Reporting to Authorities

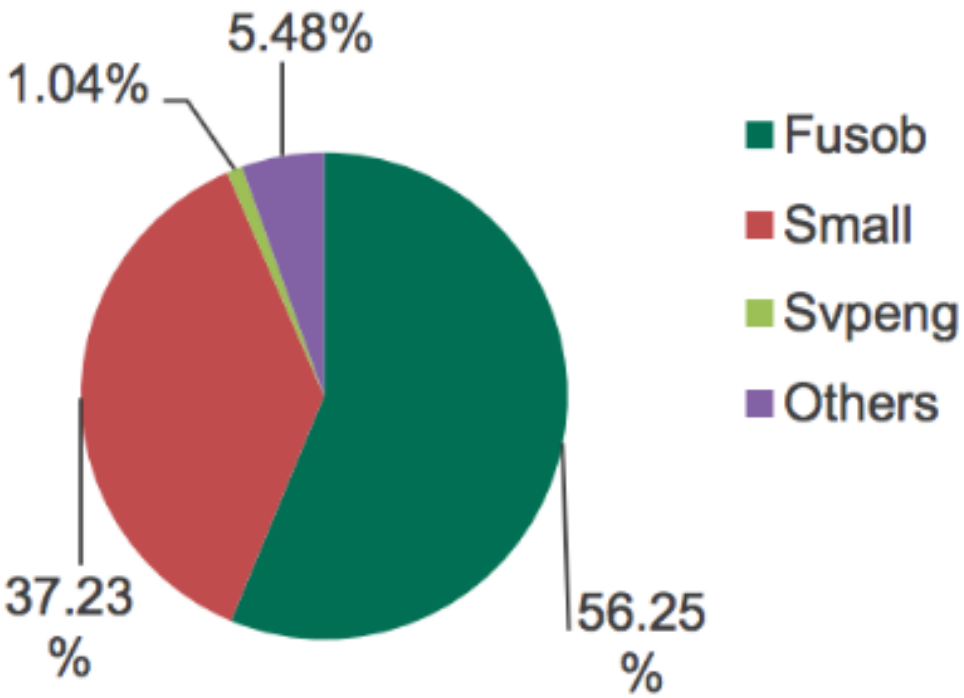
CONEXXUS solve forward

Mobile Ransomware!

*I used to have a girlfriend but she **ran som ware.***

*Makes you **wanna cry**, huh…*

CONEXXUS
solve forward



- Android RW Mid 2016
- Fusob + Small > 93%
- Fusob – iTunes Cards
- Small – Money Pak
- Locks user out of Phone
- Source: Kaspersky Labs

CONEXXUS solve forward

Fusob

Small

CONEXXUS solve forward

Android WannaCry - Kinda

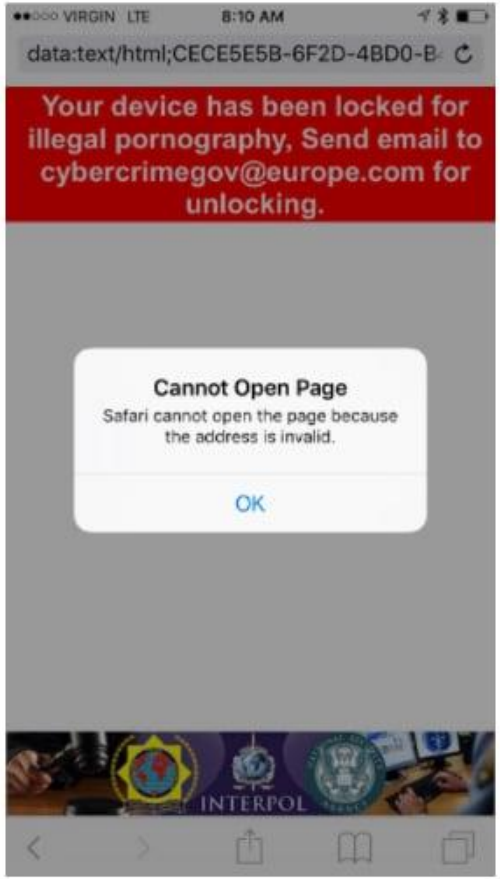
- Spotted in China June 5th
- Encrypts Files < 10K with AES-256
- Doesn't encrypt files starting with "."
- Stays out of system folders, targeting external storage

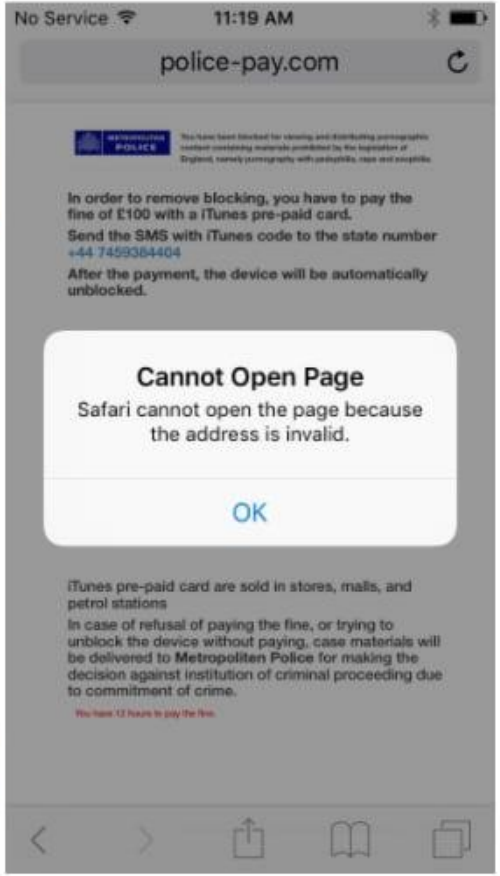
Source: Nikolaos Chrysaidos, Avast
Named: WannaLocker

CONEXXUS solve forward

Android RW – Attacks the Router

- Cybercriminals leverage IoT in 2016
- Use Wi-Fi and attached Android Device
- Guesses the router password
- Changes the DNS settings / entries
- All the other devices get re-directed to exploit sites vs. real sites





- Pre iOS 10.3 release
- Hijacked Safari
- Leverages JavaScript
- Endless pop-up loop
- Before pop-ups - browser modal
- Now pop-ups – separate tabs
- Source: Lockout

CONEXXUS solve forward

Stopping Mobile Ransomware

- Treat mobile phones like other systems on network
- Apply OS updates as they become available
- Update applications or delete them
- Only load applications from Google Play or Apple Store
- **BEST SOLUTION - Use Microsoft Mobile device instead**

CONEXXUS solve forward

Stopping Mobile Ransomware

- Treat mobile phones like other systems on network
- Apply OS updates as they become available
- Update applications or delete them
- Only load applications from Google Play or Apple Store
- **Use Microsoft Mobile device instead**

Sorry Just Kidding, Again!

CONEXXUS solve forward

Ransomware Presentation Agenda

- What is Ransomware?
- Ransomware Families and Expansion
- What does it look like and what does it do exactly?
- How to Defend Against Ransomware
- To Pay or Not to Pay?
- What’s Next?
- Reporting to Authorities

CONEXXUS solve forward

Report Ransomware to FBI Internet Crime Complaint Center – www.IC3.gov

1. Date of Infection
2. Ransomware Variant (identified on the ransom page or by the encrypted file extension)
3. Victim Company Information (industry type, business size, etc.)
4. How the Infection Occurred (link in e-mail, browsing the Internet, etc.)
5. Requested Ransom Amount
6. Actor's Bitcoin Wallet Address (may be listed on the ransom page)
7. Ransom Amount Paid (if any)
8. Overall Losses Associated with a Ransomware Infection (including the ransom amount)

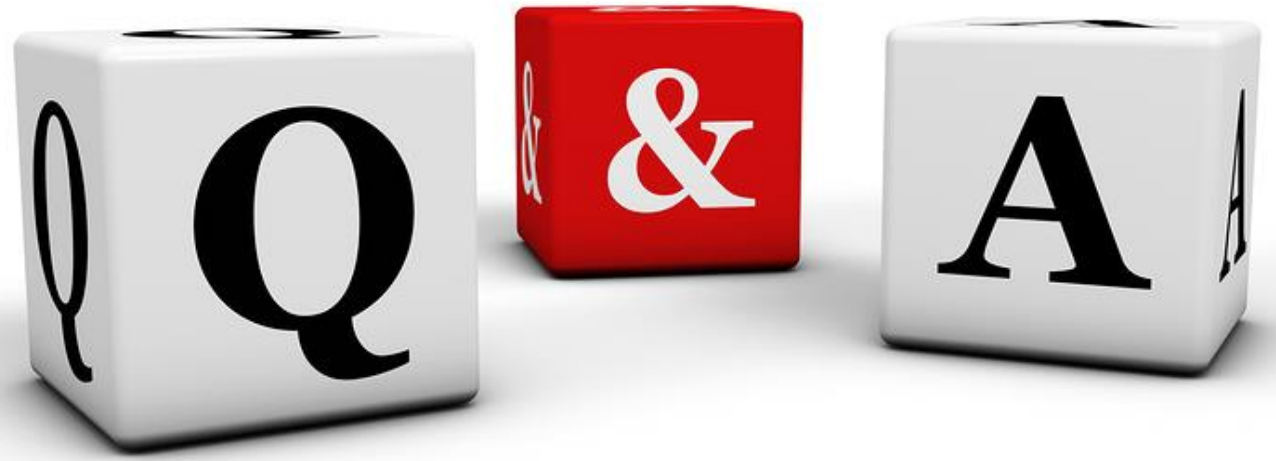
Security is founded on the sharing of ideas and awareness of threats – we all better pitch in!

Discuss or share data security issues or helpful ideas you have discovered?

Conexxus Links at the end of presentation

or

george.sconyers@omegasecure.com



CONEXXUS
solve forward

- Website: www.conexxus.org
- Email: info@conexxus.org
- LinkedIn Group: Conexxus Online
- Follow us on Twitter: @Conexxusonline