Online Extortion, Ransomware and other Cybercrimes: How to Protect Yourself and Your County

National Association of Counties
October 20, 2016

Stronger Counties. Stronger America.

Tips for viewing this webinar

- The questions box and buttons are on the right side of the webinar window.
- This box can collapse so that you can better view the presentation. To unhide the box, click the arrows on the top left corner of the panel.
- If you are having technical difficulties, please send us a message via the questions box on your right. Our organizer will reply to you privately and help resolve the issue.

Webinar recording and evaluation survey

- This webinar is being recorded and will be made available online to view later or review at www.naco.org/webinars.

- After the webinar, you will see a pop-up box containing a webinar evaluation survey. Thank you in advance for completing this survey – your feedback is very important to us!

Question & Answer instructions

- Type your question into the “Questions” box at any time during the presentation, and the moderator will read the question on your behalf during the Q&A session.

National Cybersecurity Awareness Month events at NACo

Learn more at http://www.naco.org/programs/cybersecurity

Today’s Speakers

FEDERAL BUREAU OF INVESTIGATION
CYBERCRIME DIVISION

Agent Edward Parmelee,
Federal Bureau of Investigations Cyber Division

Captain Todd Turpitt,
Hennepin County Sherriff’s Office, Detective Unit

Ben Spear,
Senior Intelligence Analyst, Multi-State Information Sharing and Analysis Center (MS-ISAC) .

Kevin Haley,
Director, Product Management for Security Response, Symantec

FEDERAL BUREAU OF INVESTIGATION
CYBERCRIME DIVISION

Agent Edward Parmelee,
Federal Bureau of Investigations Cyber
Division

Ransomware is malware that infects computers, networks, and services.

- Victim's computer is infected with malware.
- Malware encrypts victim's data and/or systems, making them unreadable.
- Actor demands payment to decrypt files or network.
- New variants

- Isolate infected computer.
- The U.S. government does **not** advocate paying.
  - Paying ransom emboldens the adversary.
  - Ransom payment funds illicit activity.
- Your primary contact should be your local FBI/Secret Service office.

- ✓ Focus on awareness and training.
- ✓ Keep patches updated.
- ✓ Set anti-virus and anti-malware to automatic update.
- ✓ Manage privileged (Administrator) accounts.
- ✓ Implement principle of least privilege.
- ✓ Disable MS Office macro and use Office Viewer software in e-mail.
- ✓ Implement software restriction policies (SRP).

Backups

Backups are critical; if infected, backups may be the best way to recover critical data.

✓Robust backup and restore procedures.

✓Secure backups offline.

UNCLASSIFIED

FBI

Cyber Task Forces

www.fbi.gov/contact-us/field

Internet Crime Complaint Center

www.ic3.gov

CyWatch

cywatch@ic.fbi.gov

Secret Service

Electronic Crimes Task Force

www.secretservice.gov/investigation/#field

Local Field Offices

www.secretservice.gov/contact

Additional resources can be found at:
www.fbi.gov
www.secretservice.gov

Other Resources - InfraGard

- Member-based information sharing program
- Member Benefits:
  - Access to InfraGard's secure portal
  - Timely intelligence briefings and analytical products
  - Unique Networking Opportunities
  - Training/Education Opportunities
- Membership Requirements
  - US Citizen, 18 yrs or older
  - Consent to FBI security/risk assessment and periodic re-certifications
  - Confidentiality and NDA
  - Agree to InfraGard Code of Ethics
- Contact: www.infragard.org

Cybercrime and Cyber Security Awareness

Captain Todd Turpitt
Hennepin County Sheriff's Office
Minneapolis, MN

What is Cyber Crime?

Cyber crime is an extremely fast growing area of crime. In essence, it is nothing new, it has only been transformed from criminal activity in person to criminal activity behind a computer screen. This has allowed the criminals to gain a sense of anonymity.

With the speed, convenience and globalization of the internet, criminals can commit almost any illegal activity anywhere in the world.

Examples of Cybercrimes

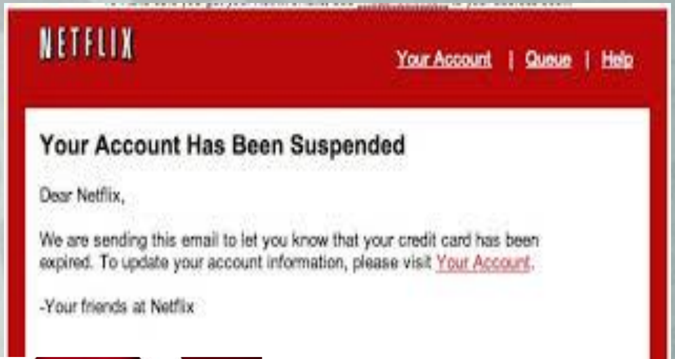
Source www.ic3.gov

- **<u>Identity Theft</u>:** The appropriation of your personal identifying information to commit fraud or theft.
- **<u>Credit and Debit Card Fraud</u>:** Fraudulent unauthorized charging of goods and services to a victim's credit/debit card
- **<u>Computer Crimes</u>:** Crimes that target computer networks or devices directly or crimes facilitated by computer networks or devices

Identity Theft

The appropriation of your personal identifying information to commit fraud or theft.

Personal identifying information (PII) can be obtained in a number of ways.



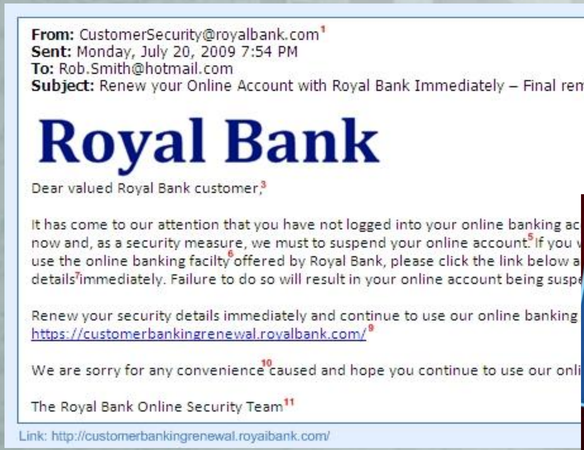
NETFLIX

Your Account Has Been Suspended

Dear Netflix,

We are sending this email to let you know that your credit card has been expired. To update your account information, please visit Your Account.

-Your friends at Netflix



From: CustomerSecurity@royalbank.com[1]
Sent: Monday, July 20, 2009 7:54 PM
To: Rob.Smith@hotmail.com
Subject: Renew your Online Account with Royal Bank Immediately – Final reminder[2]

Royal Bank

Dear valued Royal Bank customer,[3]

It has come to our attention that you have not logged into your online banking ac
now and, as a security measure, we must to suspend your online account.[5] If you v
use the online banking facilty[6] offered by Royal Bank, please click the link below a
details[7] immediately. Failure to do so will result in your online account being suspe

Renew your security details immediately and continue to use our online banking
https://customerbankingrenewal.royalbank.com/[9]

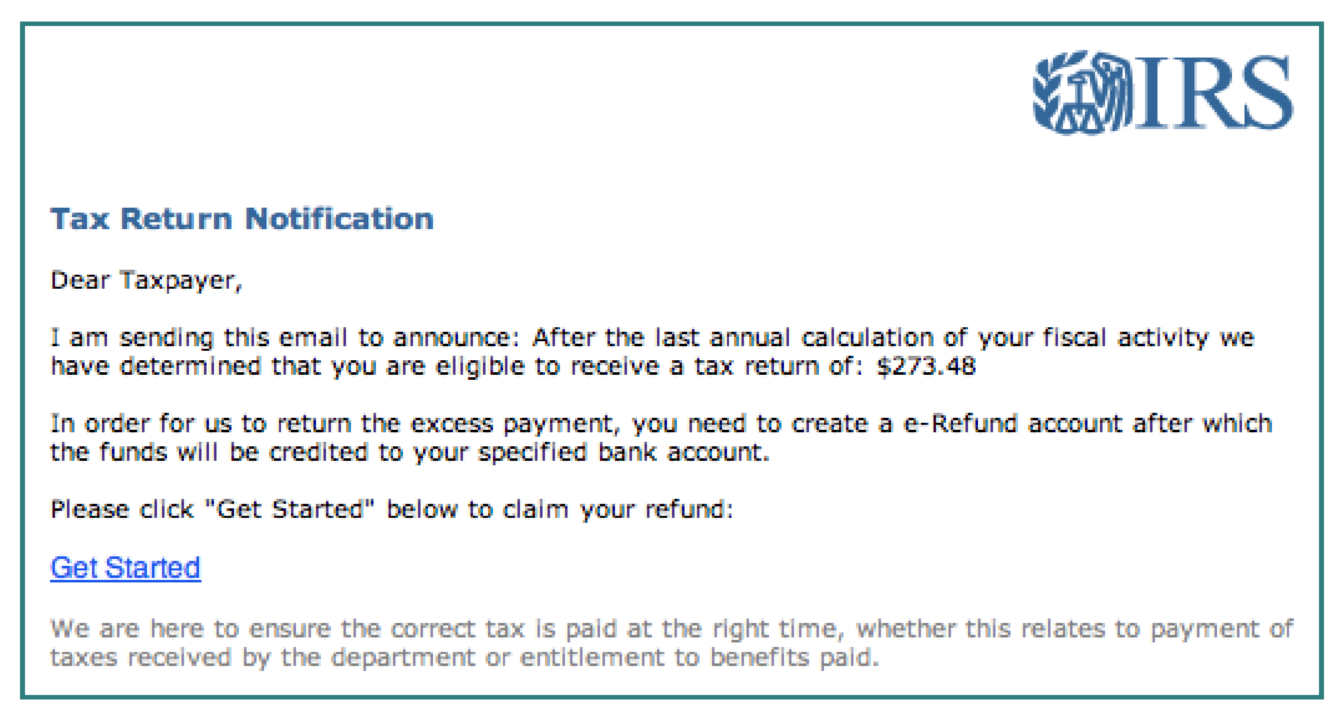
We are sorry for any convenience[10] caused and hope you continue to use our onli

The Royal Bank Online Security Team[11]

Link: http://customerbankingrenewal.royaibank.com/

Identity Theft Example

- Email notification for personal information



Tax Return Notification

Dear Taxpayer,

I am sending this email to announce: After the last annual calculation of your fiscal activity we have determined that you are eligible to receive a tax return of: $273.48

In order for us to return the excess payment, you need to create a e-Refund account after which the funds will be credited to your specified bank account.

Please click "Get Started" below to claim your refund:

Get Started

We are here to ensure the correct tax is paid at the right time, whether this relates to payment of taxes received by the department or entitlement to benefits paid.

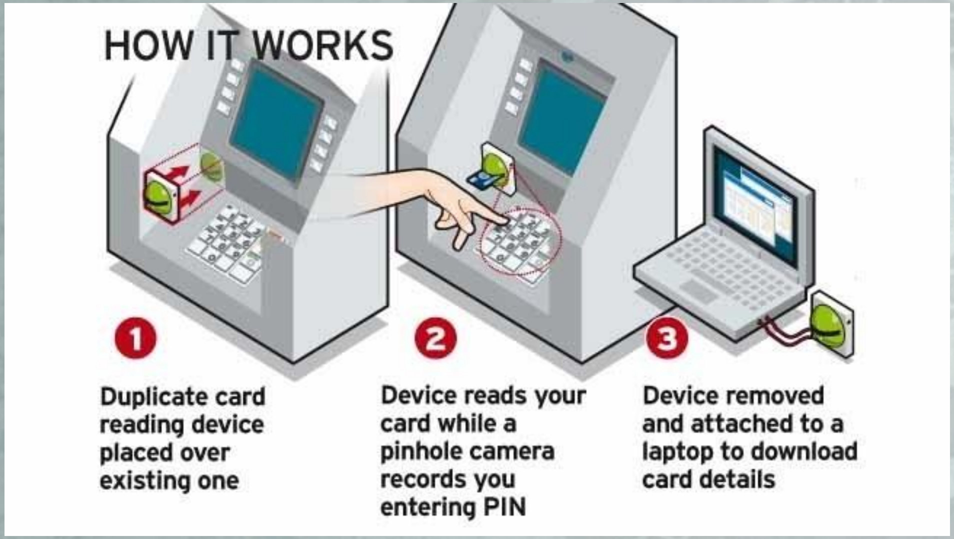
Credit and Debit Card Fraud

Fraudulent unauthorized charging of goods and services to a victim's credit/debit card- ***source ic3.gov.***

- Card info obtained through:
  - – Thievery
  - – Trash search
  - – Access to personal records
  - – Social media
  - – Change of address forms in banking statements
  - – Everyday use-skimming

Credit and Debit Card Fraud Example

- Skimmers



HOW IT WORKS

1 Duplicate card reading device placed over existing one

2 Device reads your card while a pinhole camera records you entering PIN

3 Device removed and attached to a laptop to download card details

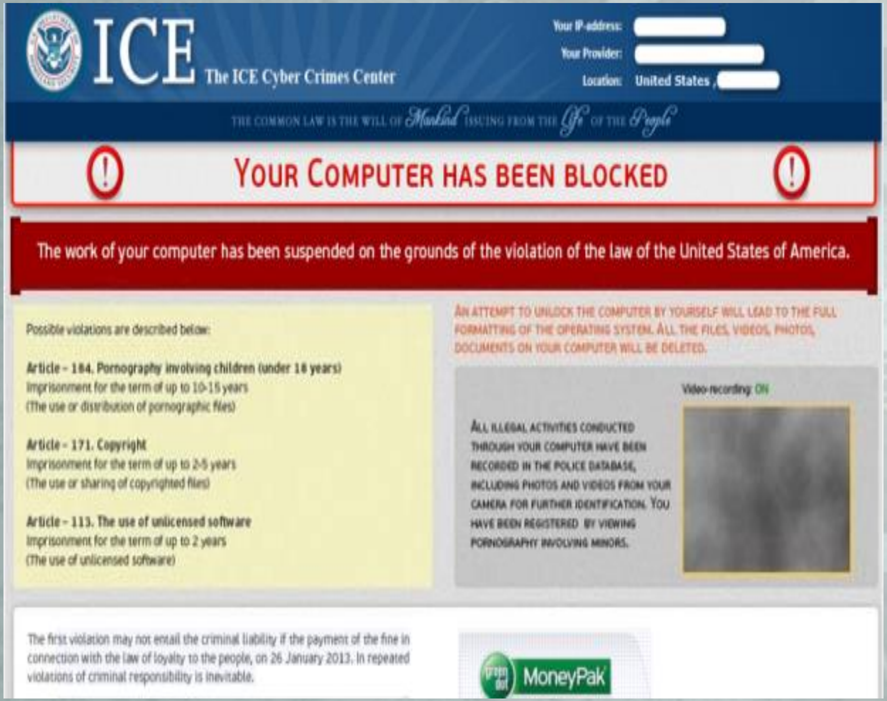
Computer Crimes

Crimes that target computer networks or devices directly or crimes facilitated by computer networks or devices ***– Source www.ic3.gov***

- <u>Cyber threats</u>
  - **Hacking-** The unauthorized intrusion into the computer system of another, often with malicious intent.
  - **Intrusion-** The unauthorized access or network usually with the intent to carry out malicious activity or obtain access to private information.
  - **Malware**- Software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems.

Computer Crimes

Cyber threat examples



ICE The ICE Cyber Crimes Center

Your IP-address: [redacted]

Your Provider: [redacted]

Location: United States , [redacted]

THE COMMON LAW IS THE WILL OF Mankind ISSUING FROM THE Life OF THE People

YOUR COMPUTER HAS BEEN BLOCKED

The work of your computer has been suspended on the grounds of the violation of the law of the United States of America.

Possible violations are described below:

Article - 184. Pornography involving children (under 18 years)
Imprisonment for the term of up to 10-15 years
(The use or distribution of pornographic files)

Article - 171. Copyright
Imprisonment for the term of up to 2-5 years
(The use or sharing of copyrighted files)

Article - 113. The use of unlicensed software
Imprisonment for the term of up to 2 years
(The use of unlicensed software)

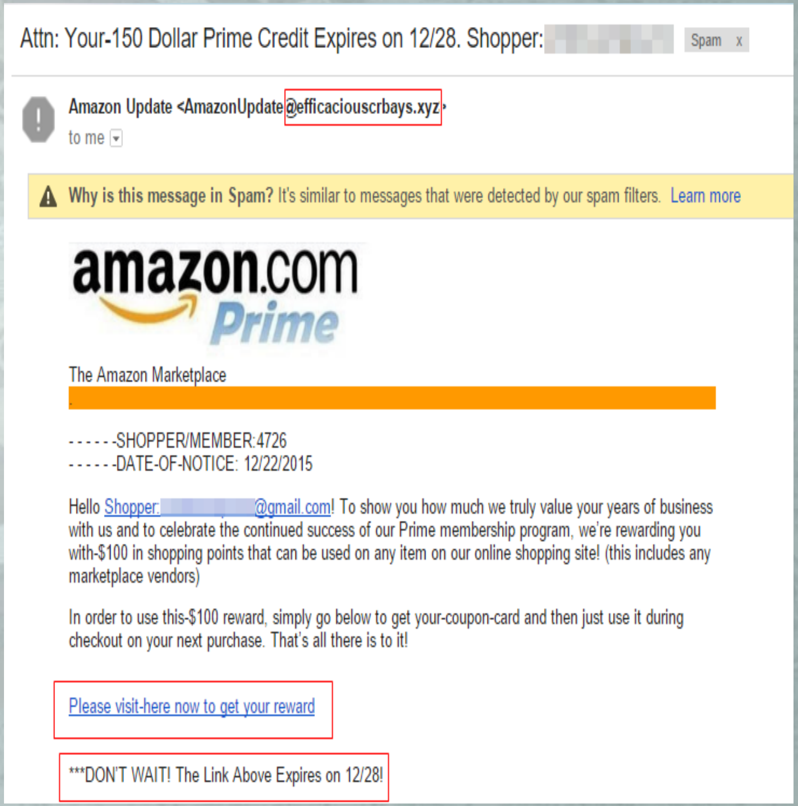
AN ATTEMPT TO UNLOCK THE COMPUTER BY YOURSELF WILL LEAD TO THE FULL FORMATTING OF THE OPERATING SYSTEM. ALL THE FILES, VIDEOS, PHOTOS, DOCUMENTS ON YOUR COMPUTER WILL BE DELETED.

Video-recording: ON

ALL ILLEGAL ACTIVITIES CONDUCTED THROUGH YOUR COMPUTER HAVE BEEN RECORDED IN THE POLICE DATABASE, INCLUDING PHOTOS AND VIDEOS FROM YOUR CAMERA FOR FURTHER IDENTIFICATION. YOU HAVE BEEN REGISTERED BY VIEWING PORNOGRAPHY INVOLVING MINORS.

The first violation may not entail the criminal liability if the payment of the fine in connection with the law of loyalty to the people, on 26 January 2013. In repeated violations of criminal responsibility is inevitable.

MoneyPak



Attn: Your-150 Dollar Prime Credit Expires on 12/28. Shopper: [redacted]

Amazon Update <AmazonUpdate@efficaciouscrbays.xyz>
to me

Why is this message in Spam? It's similar to messages that were detected by our spam filters. Learn more

amazon.com Prime

The Amazon Marketplace

-----SHOPPER/MEMBER:4726
-----DATE-OF-NOTICE: 12/22/2015

Hello Shopper:[redacted]@gmail.com! To show you how much we truly value your years of business with us and to celebrate the continued success of our Prime membership program, we're rewarding you with-$100 in shopping points that can be used on any item on our online shopping site! (this includes any marketplace vendors)

In order to use this-$100 reward, simply go below to get your-coupon-card and then just use it during checkout on your next purchase. That's all there is to it!

Please visit-here now to get your reward

***DON'T WAIT! The Link Above Expires on 12/28!

Doxing

What is it?

“Internet based practice of researching and broadcasting private or identifiable information about an individual or organization”.-Wikipedia

Concerns

Government officials may be targeted and personal information to include addresses, family members, and other private information published.

Prevention Strategies

- Check the mail daily and shred any documents that contain personal information.
- Be aware when bills are due and if a statement seems late
- Scrutinize all CC statements know what the charges are and question if it looks unusual
- Check your credit history at www.annualcreditreport.com. Look for unusual inquiries.
- Read emails, text messages, etc. carefully
  - Spelling errors, grammatical errors
  - Contact financial institution/other entity directly
  - Shred or destroy personal information

Prevention Strategies

- Utilize privacy settings on social media sites and avoid information on government or law enforcement activities.
- Minimize social media activities
- Explore options for privacy in your public records-ex: drivers license, vehicle registration, and property tax info.
- “Google” yourself. What is out there?
- For your network, engage your departmental IT services to develop strategies for security.

Prevention Strategies

- **Things to remember:**
- No legitimate bank or business requests personal information via email
- No law enforcement entity sends official legal notices via email
- No law enforcement or government entity will demand instant payment to avoid arrest, etc.
- No government entity takes unusual forms of payment such as gift cards, unusual wire transfers, etc.
- Back up files and hard drive frequently
- Use strong passwords and change them regularly
- If it seems too good to be true, it is.

If you are victimized

- Report to your local law enforcement agency
- File a complaint with the Internet Crime Complaint center @www.ic3.gov
- Submit a consumer complaint with the Federal Trade Commission @www.ftc.gov/complaint
- Notify your banking institution
- If you were scammed by someone claiming to represent a business, be sure to notify the actual business (bank, credit card company, etc.)

Source IACP Cybercenter.

Cybercrime and Security Awareness

Questions?

Captain Todd Turpitt

Hennepin County Sheriff’s Office-Minneapolis, MN

todd.turpitt@hennepin.us

MULTI-STATE
Information Sharing
& Analysis Center™

MS-ISAC

BEN SPEAR

SENIOR INTELLIGENCE ANALYST

Multi-State Information Sharing and Analysis Center

The U.S. Department of Homeland Security has designated the MS-ISAC as its key cybersecurity resource for cyber threat prevention, protection, response and recovery for all U.S. State, Local, Tribal and Territorial (SLTT) governments.

Who We Serve

MS-ISAC Members include:

- All 56 US States and Territories
- All 78 federally recognized fusion centers
- More than 1,000 local governments and tribal nations

State, Local, Tribal, and Territorial

Cities, counties, towns, airports, public education, police departments, ports, transit associations, and more

24 x 7 Security Operations Center

Central location to report any cybersecurity incident

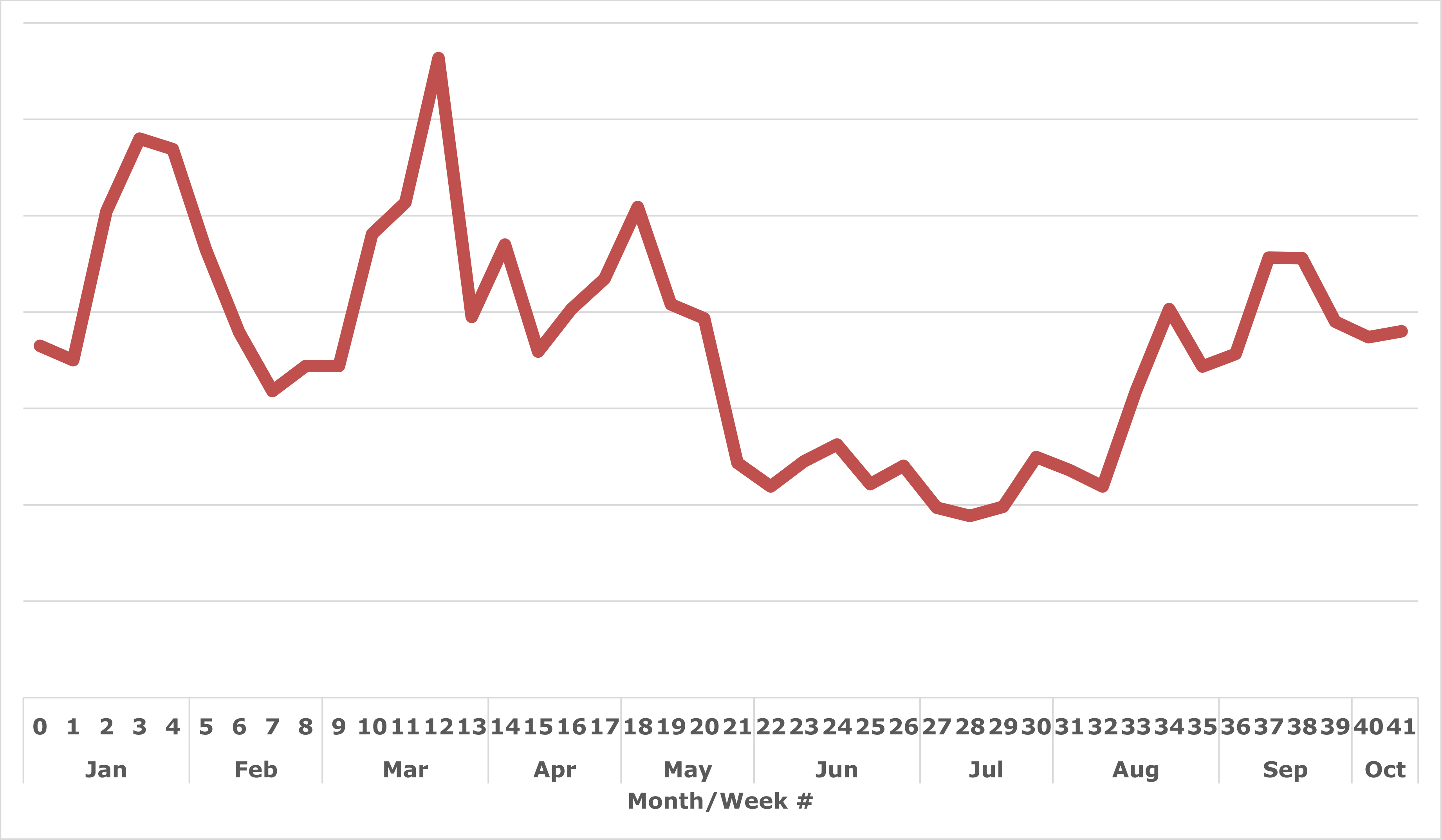
- **Support:**
  - Network Monitoring Services
  - Research and Analysis

- **Analysis and Monitoring:**
  - Threats
  - Vulnerabilities
  - Attacks

- **Reporting:**
  - Cyber Alerts & Advisories
  - Web Defacements
  - Account Compromises
  - Hacktivist Notifications

To report an incident or request assistance:
Phone: 1-866-787-4722
Email: soc@msisac.org

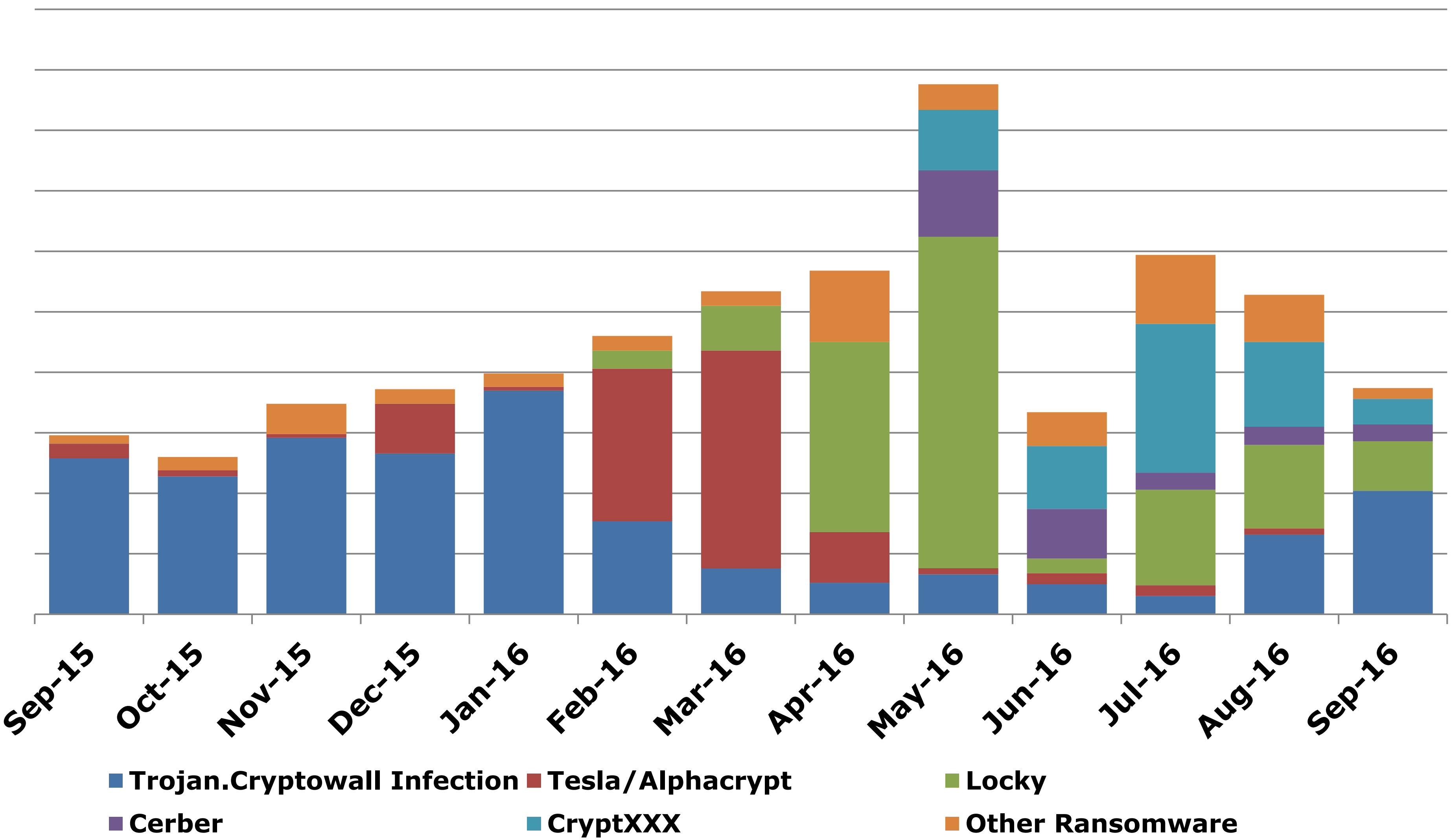
MS-ISAC Weekly Monitoring (2016)



Top Malware

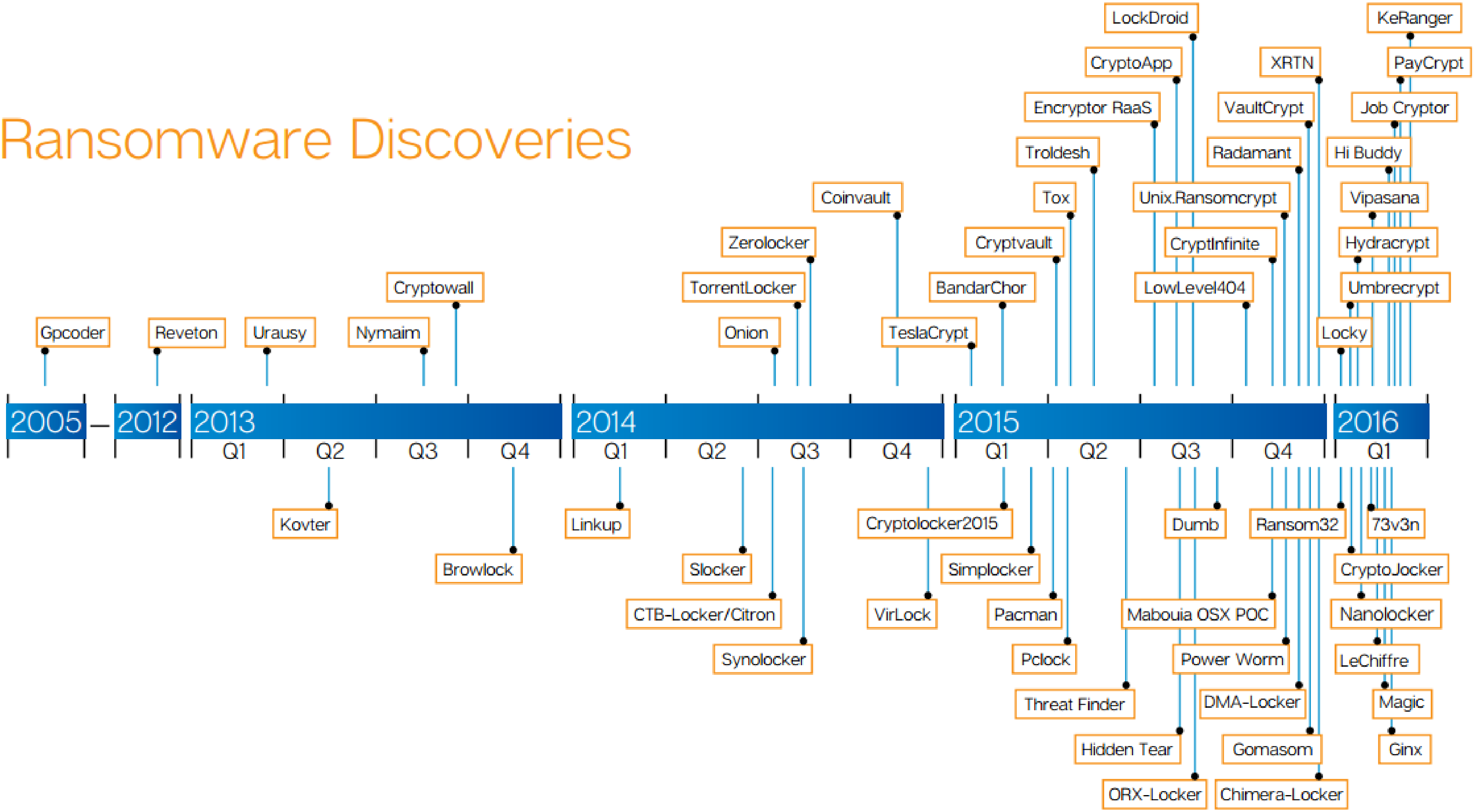
ZeuS
Kovter
Vawtrak/Neverquest
Locky
Dridex
Cryptowall
Tinba
Poweliks
Ponmocup
Nymaim

Ransomware Infections (Sep 15-16)



New Ransomware Variants Timeline

Ransomware Discoveries



2005 – 2012

2013 Q1 Q2 Q3 Q4

2014 Q1 Q2 Q3 Q4

2015 Q1 Q2 Q3 Q4

2016 Q1

Gpcoder

Reveton

Urausy

Kovter

Nymaim

Cryptowall

Browlock

Linkup

Onion

Slocker

CTB-Locker/Citron

TorrentLocker

Zerolocker

Synolocker

Coinvault

TeslaCrypt

Cryptolocker2015

VirLock

BandarChor

Simplocker

Cryptvault

Tox

Pacman

Pclock

Troldesh

Threat Finder

Encryptor RaaS

CryptoApp

Hidden Tear

LockDroid

ORX-Locker

Dumb

LowLevel404

Unix.Ransomcrypt

CryptInfinite

Mabouia OSX POC

Power Worm

Radamant

Ransom32

VaultCrypt

DMA-Locker

Gomasom

XRTN

Chimera-Locker

Locky

Umbrecrypt

Hydracrypt

Vipasana

Hi Buddy

73v3n

CryptoJocker

Nanolocker

LeChiffre

Job Cryptor

PayCrypt

KeRanger

Magic

Ginx

Ransomware

Ransomware Attack Vectors

1. Visiting a malicious site
2. Clicking on a malicious email attachment
3. Unpatched web servers

Recent Trends

1. New Variants / TTPs
2. Ransomware-as-a-service
1. Hospital targeting

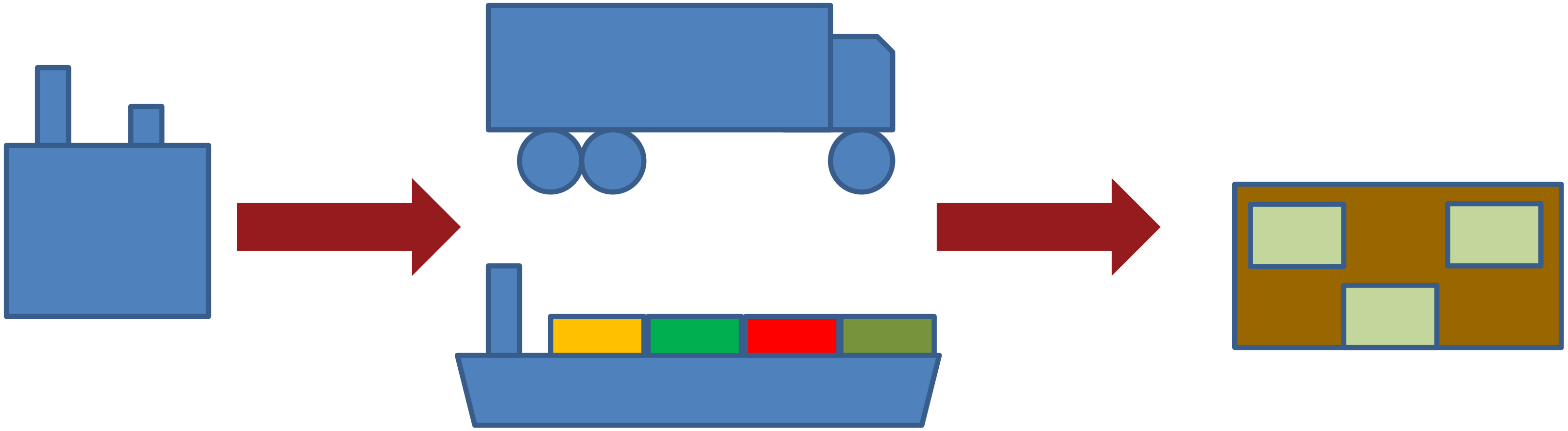
Prevention Mechanisms

1. Keep your systems patched – desktops and servers.
2. Email filtering
3. Keep your AV up to date
4. End user training and awareness

SUPPLY CHAIN

Both opportunistic and targeted attacks

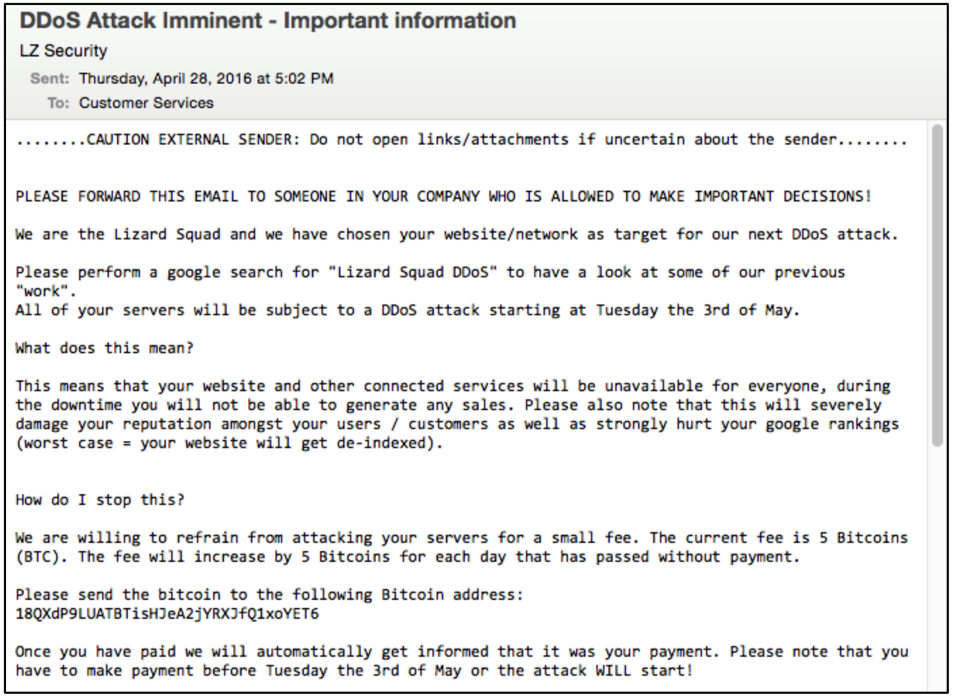
- Malicious actors gaining access to devices during manufacturing
- Exploitation of third-party connections



Consider these concerns when establishing business relationships and drafting agreements

Hoax DDoS Extortion Scheme

- Extortion demands
- Bitcoin Payment
- Known CTAs: Lizard Squad, Armada Collective, LulzSec, New World Hacking
- **HOAX!**



DDoS Attack Imminent - Important information

LZ Security

Sent: Thursday, April 28, 2016 at 5:02 PM

To: Customer Services

```
........CAUTION EXTERNAL SENDER: Do not open links/attachments if uncertain about the sender........


PLEASE FORWARD THIS EMAIL TO SOMEONE IN YOUR COMPANY WHO IS ALLOWED TO MAKE IMPORTANT DECISIONS!

We are the Lizard Squad and we have chosen your website/network as target for our next DDoS attack.

Please perform a google search for "Lizard Squad DDoS" to have a look at some of our previous
"work".
All of your servers will be subject to a DDoS attack starting at Tuesday the 3rd of May.

What does this mean?

This means that your website and other connected services will be unavailable for everyone, during
the downtime you will not be able to generate any sales. Please also note that this will severely
damage your reputation amongst your users / customers as well as strongly hurt your google rankings
(worst case = your website will get de-indexed).


How do I stop this?

We are willing to refrain from attacking your servers for a small fee. The current fee is 5 Bitcoins
(BTC). The fee will increase by 5 Bitcoins for each day that has passed without payment.

Please send the bitcoin to the following Bitcoin address:
18QXdP9LUATBTisHJeA2jYRXJfQ1xoYET6

Once you have paid we will automatically get informed that it was your payment. Please note that you
have to make payment before Tuesday the 3rd of May or the attack WILL start!
```

What Can You Do?

Low Hanging Fruit!

1. PATCH!
2. Use defensive software
3. Back-up
4. Train users
5. Enforce strong, complex, unique passwords

Critical Security Controls

1. Identify authorized and unauthorized devices
2. Inventory authorized and unauthorized software
3. Secure configurations for hardware and software
4. Continuous vulnerability assessment and remediation
5. Controlled use of admin privileges

MS-ISAC Contact Numbers

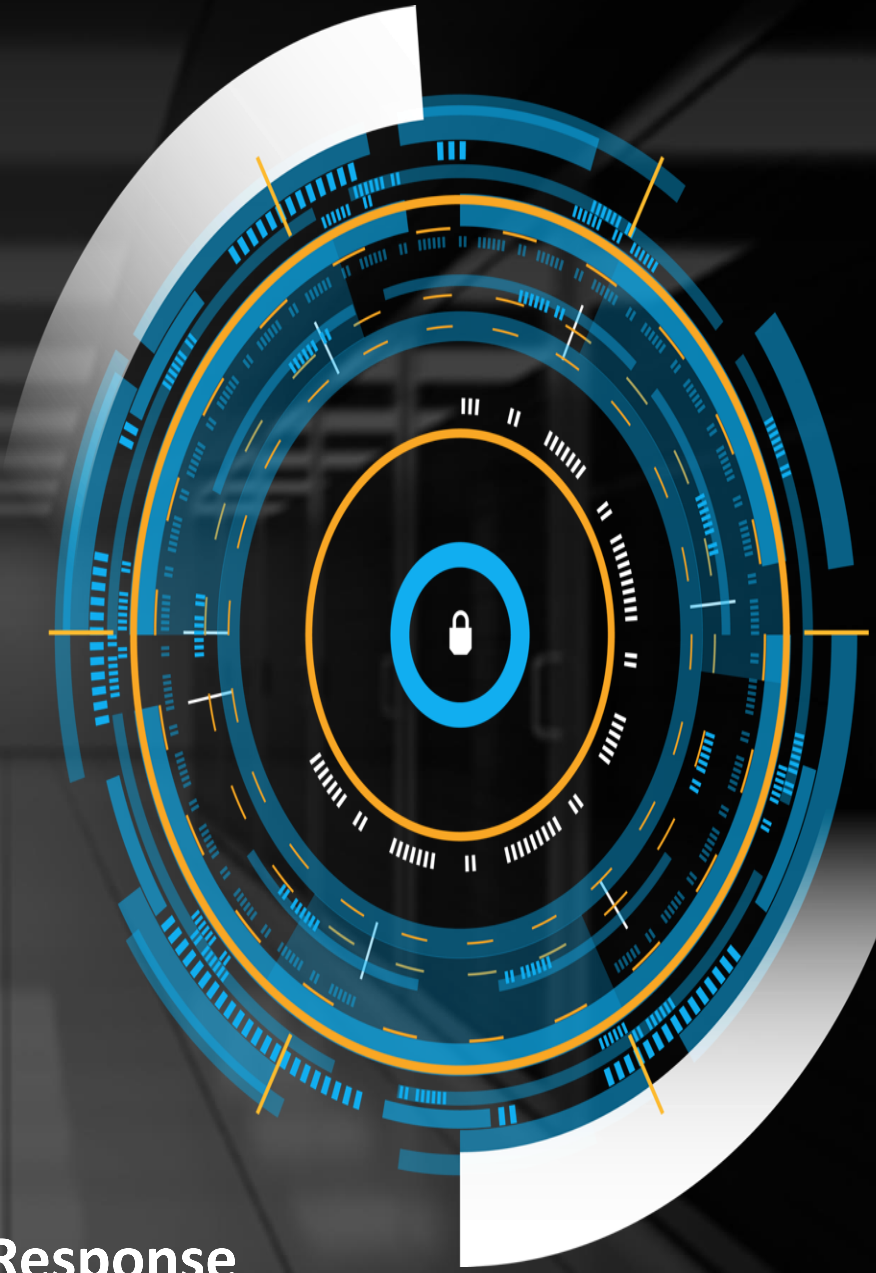
Thank You!

Ben Spear
ben.spear@cisecurity.org

Security Operations Center
24/7 Phone Number
1-866-787-4722
soc@msisac.org

MS-ISAC HQ
Front Desk
518-266-3460
info@msisac.org

Observations on Ransomware

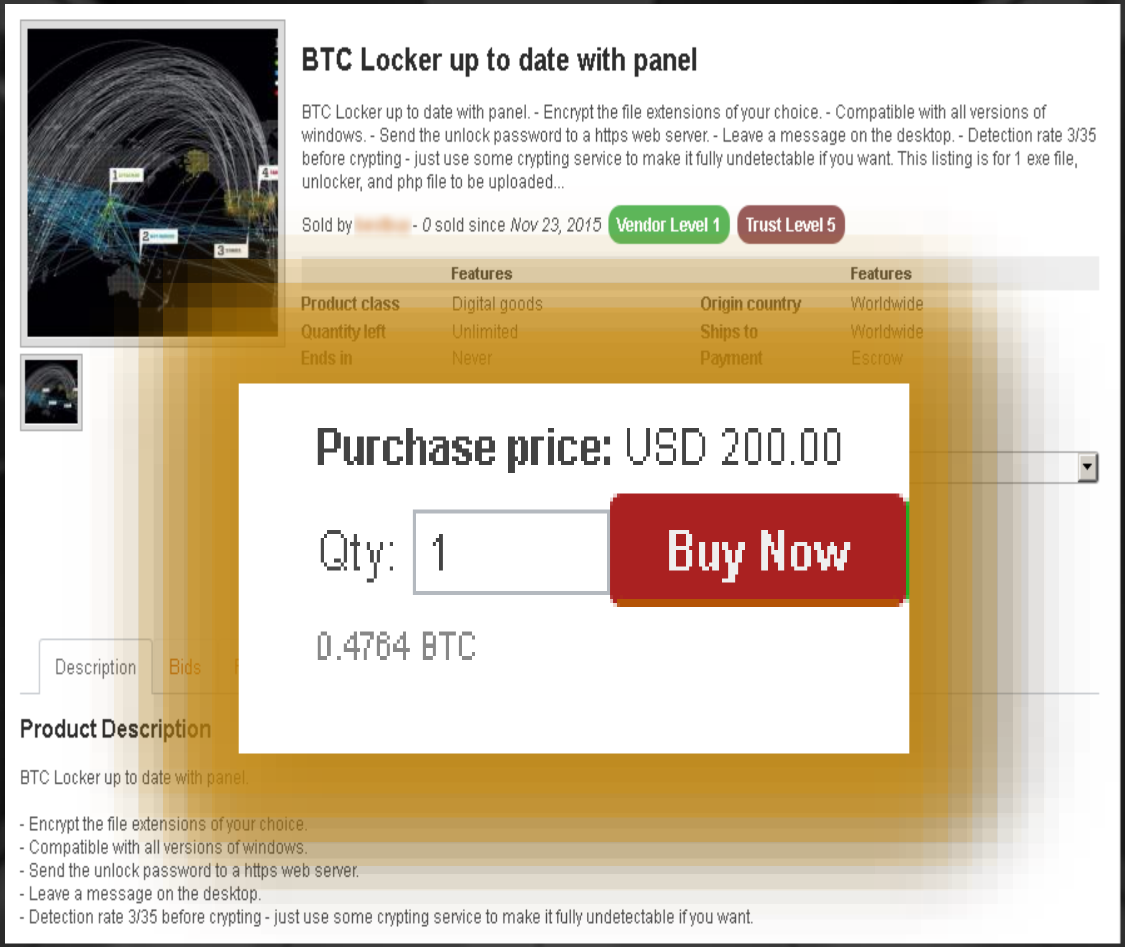


Kevin Haley
Director, Symantec Security Response

Ransomware Growth Factors

- High Profitability
- Effective Infection Vectors
- Easy Access to Encryption
- Low Barrier to Entry

Ransomware is Easy



BTC Locker up to date with panel

BTC Locker up to date with panel. - Encrypt the file extensions of your choice. - Compatible with all versions of windows. - Send the unlock password to a https web server. - Leave a message on the desktop. - Detection rate 3/35 before crypting - just use some crypting service to make it fully undetectable if you want. This listing is for 1 exe file, unlocker, and php file to be uploaded...

Sold by [redacted] - *0* sold since *Nov 23, 2015* Vendor Level 1 Trust Level 5

	Features		Features
Product class	Digital goods	Origin country	Worldwide
Quantity left	Unlimited	Ships to	Worldwide
Ends in	Never	Payment	Escrow

Purchase price: USD 200.00

Qty: 1 Buy Now

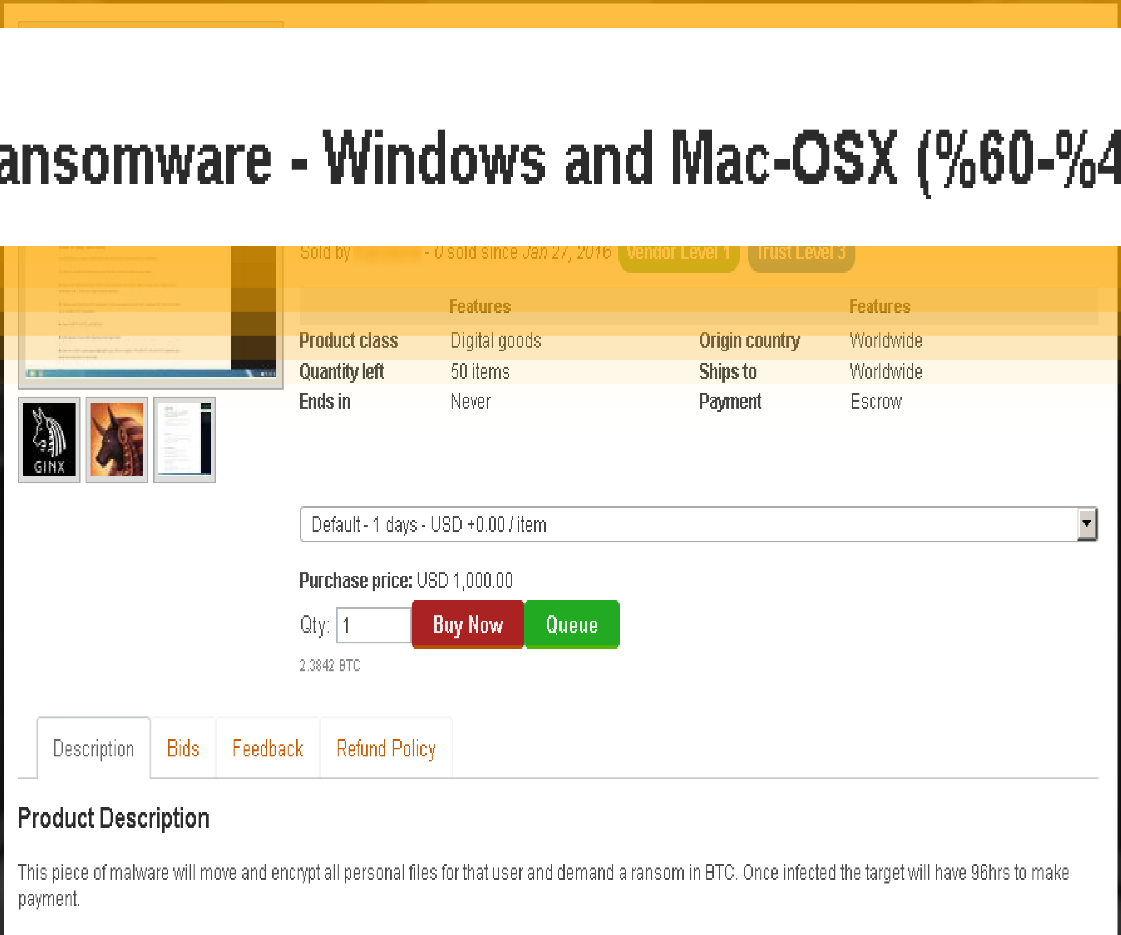
0.4764 BTC

Product Description

BTC Locker up to date with panel.

- Encrypt the file extensions of your choice.
- Compatible with all versions of windows.
- Send the unlock password to a https web server.
- Leave a message on the desktop.
- Detection rate 3/35 before crypting - just use some crypting service to make it fully undetectable if you want.

Ransomware is Easy



Ginx Ransomware - Windows and Mac-OSX (%60-%40 split)

Sold by [redacted] - 0 sold since Jan 27, 2016 Vendor Level 1 Trust Level 3

	Features		Features
Product class	Digital goods	Origin country	Worldwide
Quantity left	50 items	Ships to	Worldwide
Ends in	Never	Payment	Escrow

Default - 1 days - USD +0.00 / item

Purchase price: USD 1,000.00

Qty: 1 Buy Now Queue

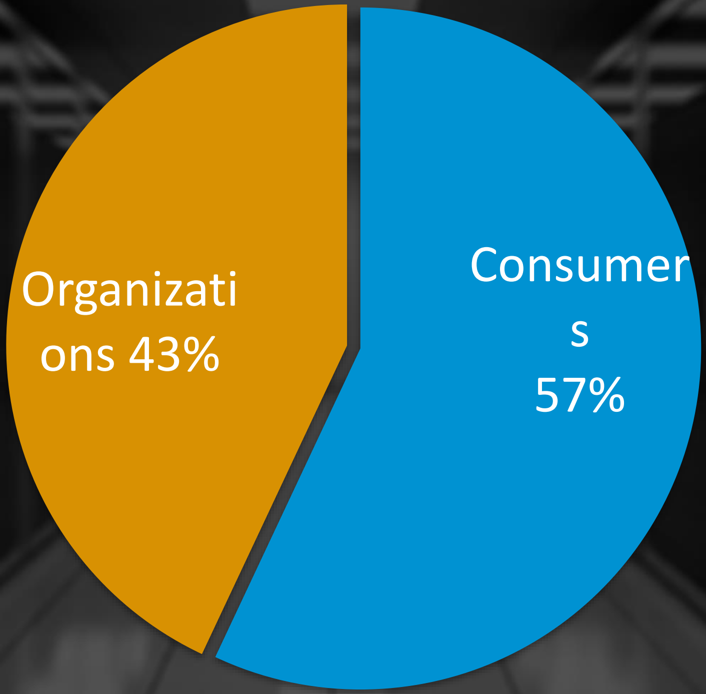
2.3842 BTC

Description Bids Feedback Refund Policy

Product Description

This piece of malware will move and encrypt all personal files for that user and demand a ransom in BTC. Once infected the target will have 96hrs to make payment.

Most Ransomware Does Not Care Who it Infects



How is Ransomware getting on machine?

Vectors

- Other malware
- Brute-force attacks
- Server-side vulnerabilities
- Worm techniques
- SMS messages and app stores (Android)

#10 Don’t Let Defenses Down at Mail Server

1 in 152

emails is

Malicious

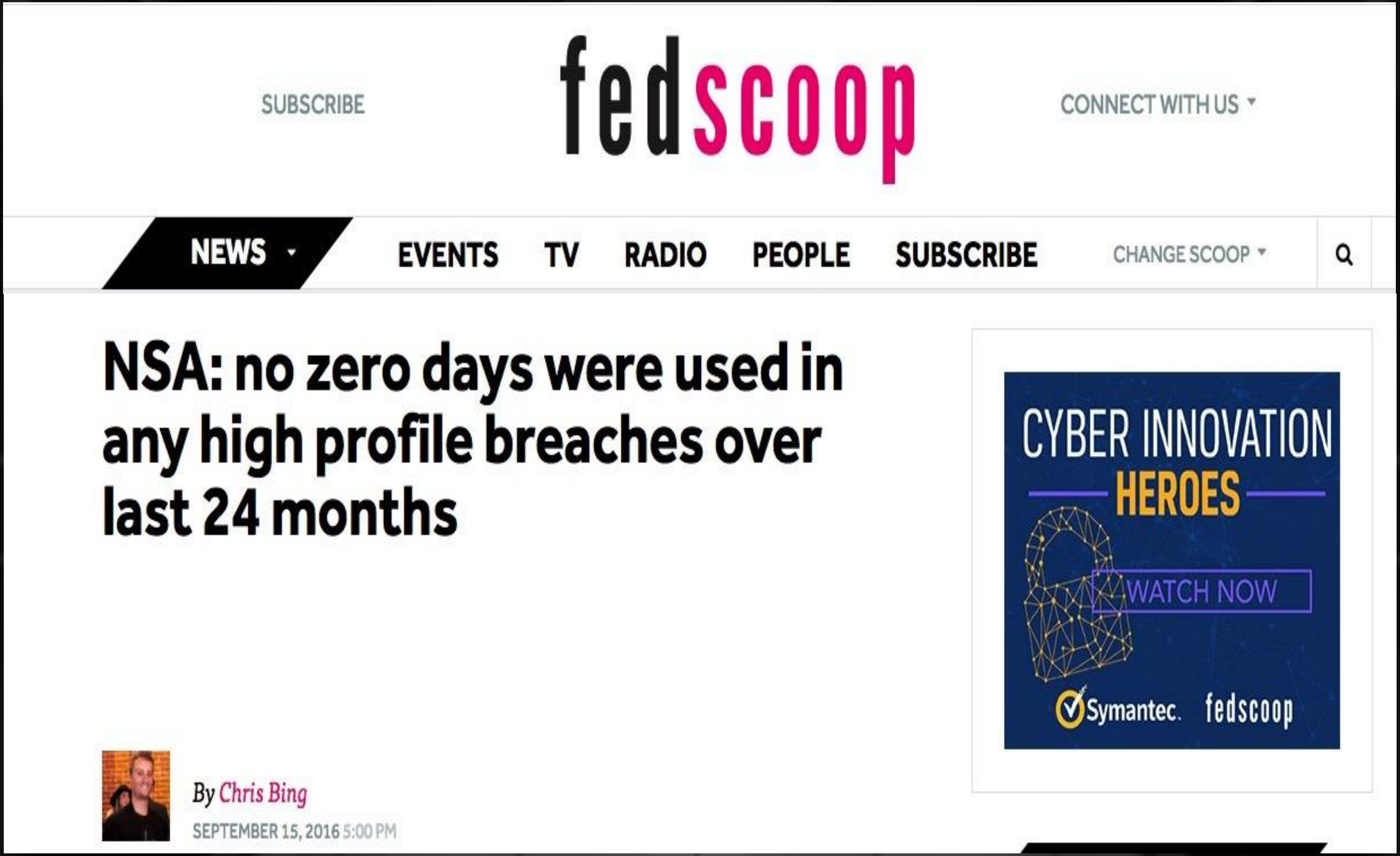
Symantec ISTR August 201

Review Your Email File Filtering Policy

- **Block these file extensions at the Mail Gateway**
  - **.js**
  - **.jse**
  - **.vbs**
  - **.vbe**
  - **.iso**
  - **.hta**
  - **.wsf**

- End-Users and Desktop Security is the ***last*** line of defense from these threats.

- See: http://www.symantec.com/connect/articles/support-perspective-w97mdownloader-battle-plan

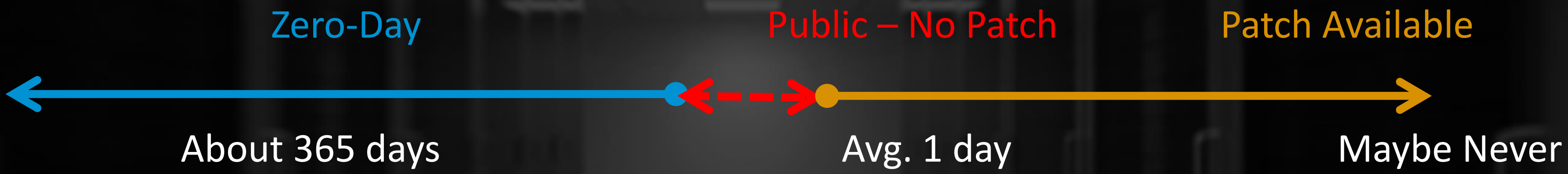


NSA: no zero days were used in any high profile breaches over last 24 months

By Chris Bing

SEPTEMBER 15, 2016 5:00 PM

Zero-Day Vulnerability Lifecycle



Zero-Day

Public – No Patch

Patch Available

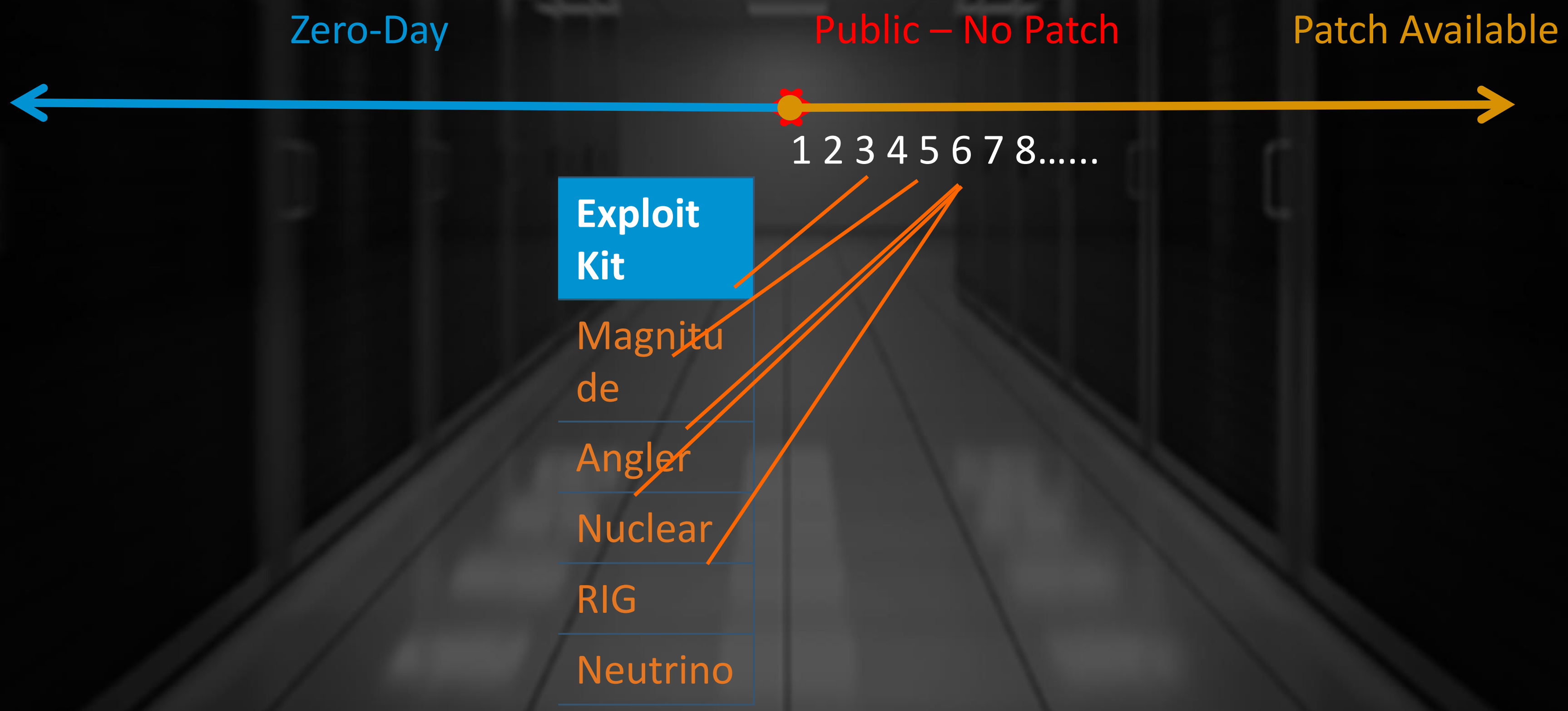
About 365 days

Avg. 1 day

Maybe Never

Adobe Releases Out-of-Band Patch For Flash Vulnerability

- On June 23, Adobe released an out-of-band patch for a critical zero day vulnerability, designated CVE-2015-3113



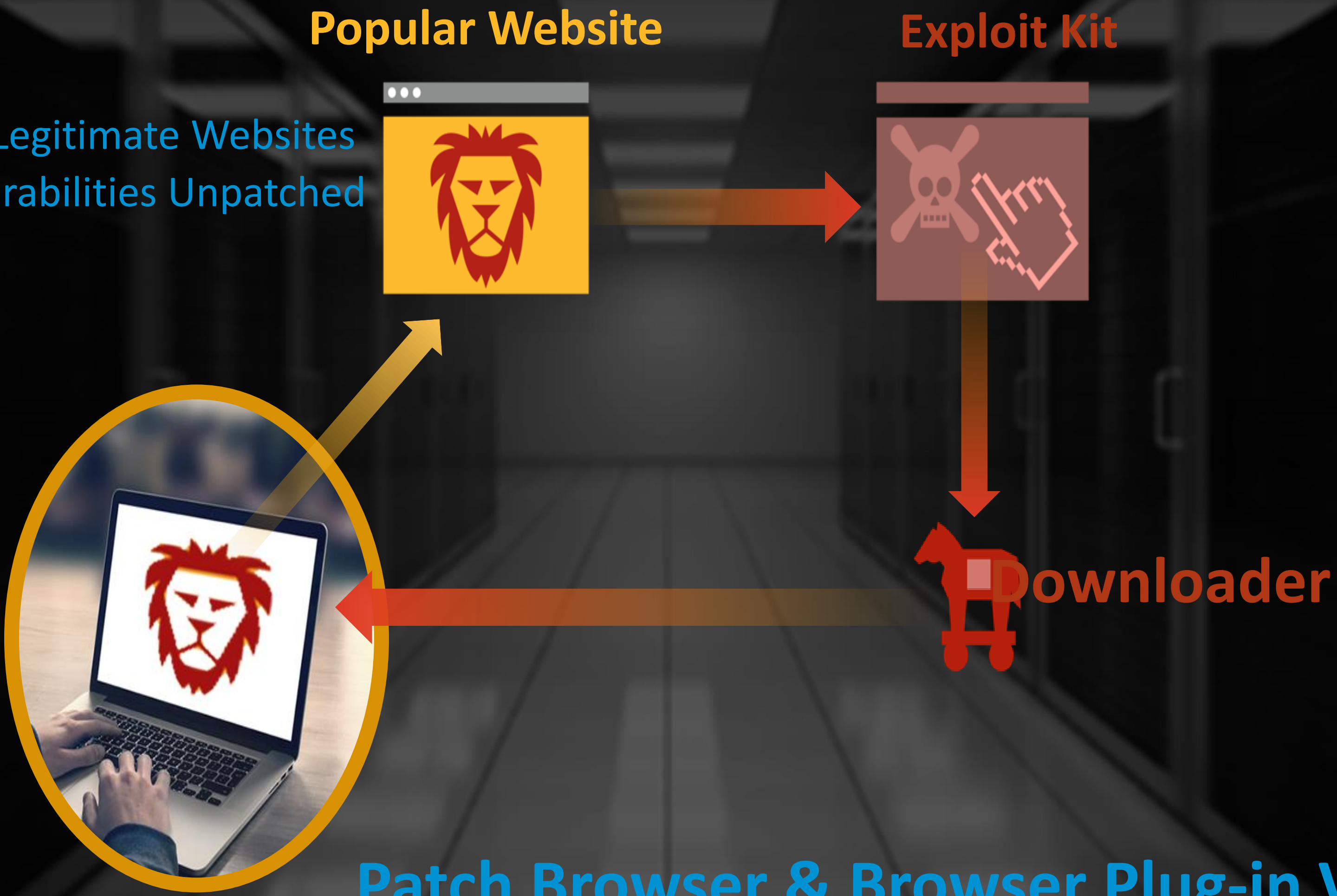
Exploit Kit
Magnitu de
Angler
Nuclear
RIG
Neutrino

Top 5 most Frequently Exploited Zero-Day Vulnerabilities in 2015

Rank	Name	2015 Percentage
1	Adobe Flash Player CVE-2015-0313	81%
2	Adobe Flash Player CVE-2015-5119	14%
3	Adobe Flash Player CVE-2015-5122	5%
4	Heap-Based Buffer Overflow aka ‘Ghost’ CVE-2015-0235	<1%
5	Adobe Flash Player CVE-2015-3113	<1%

Do Your Fellow Man a Favor and Patch Your Website

15% of Legitimate Websites
Critical Vulnerabilities Unpatched



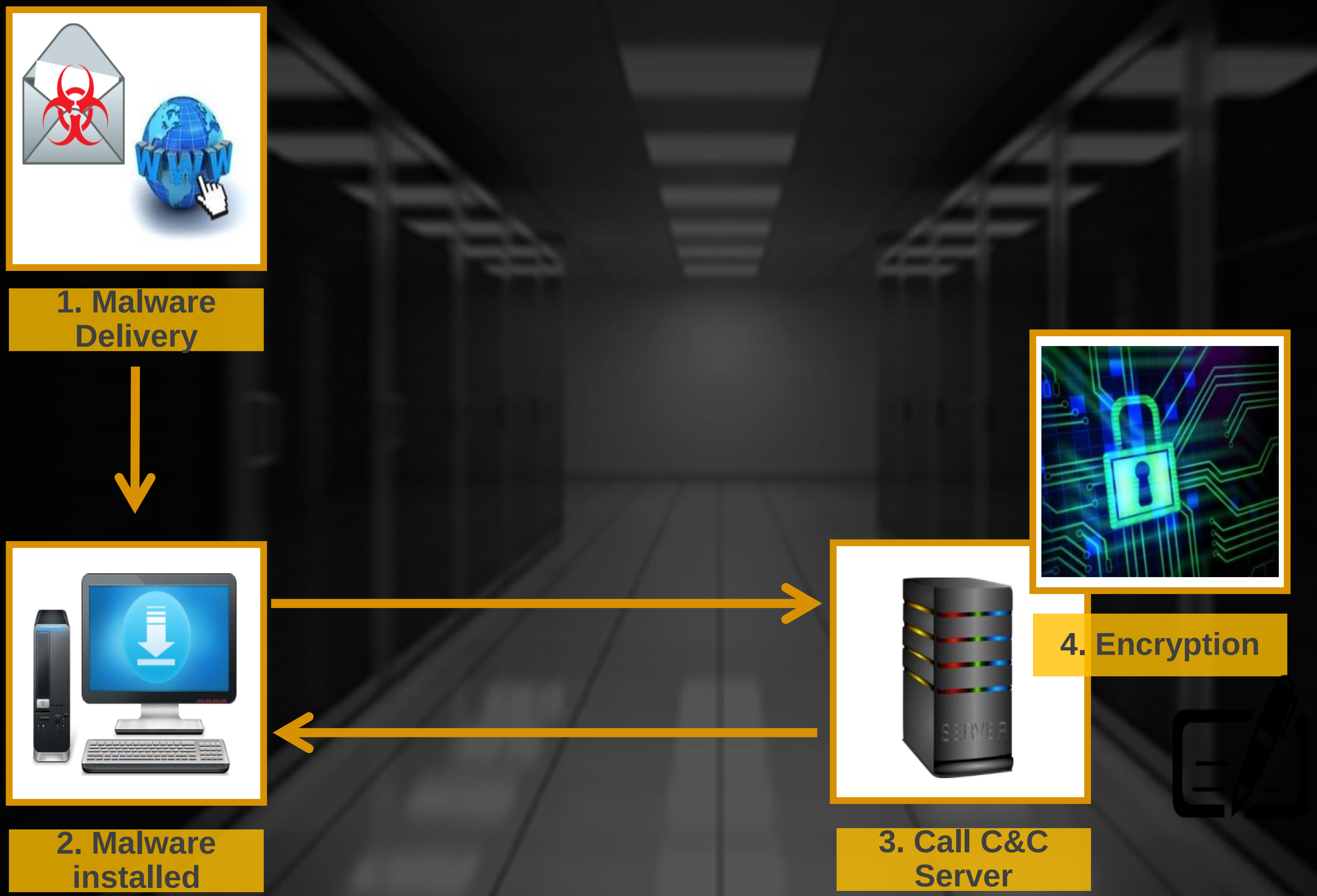
Popular Website

Exploit Kit

Downloader

Patch Browser & Browser Plug-in Vulnerab

Ransomware Attack Chain



1. Malware Delivery

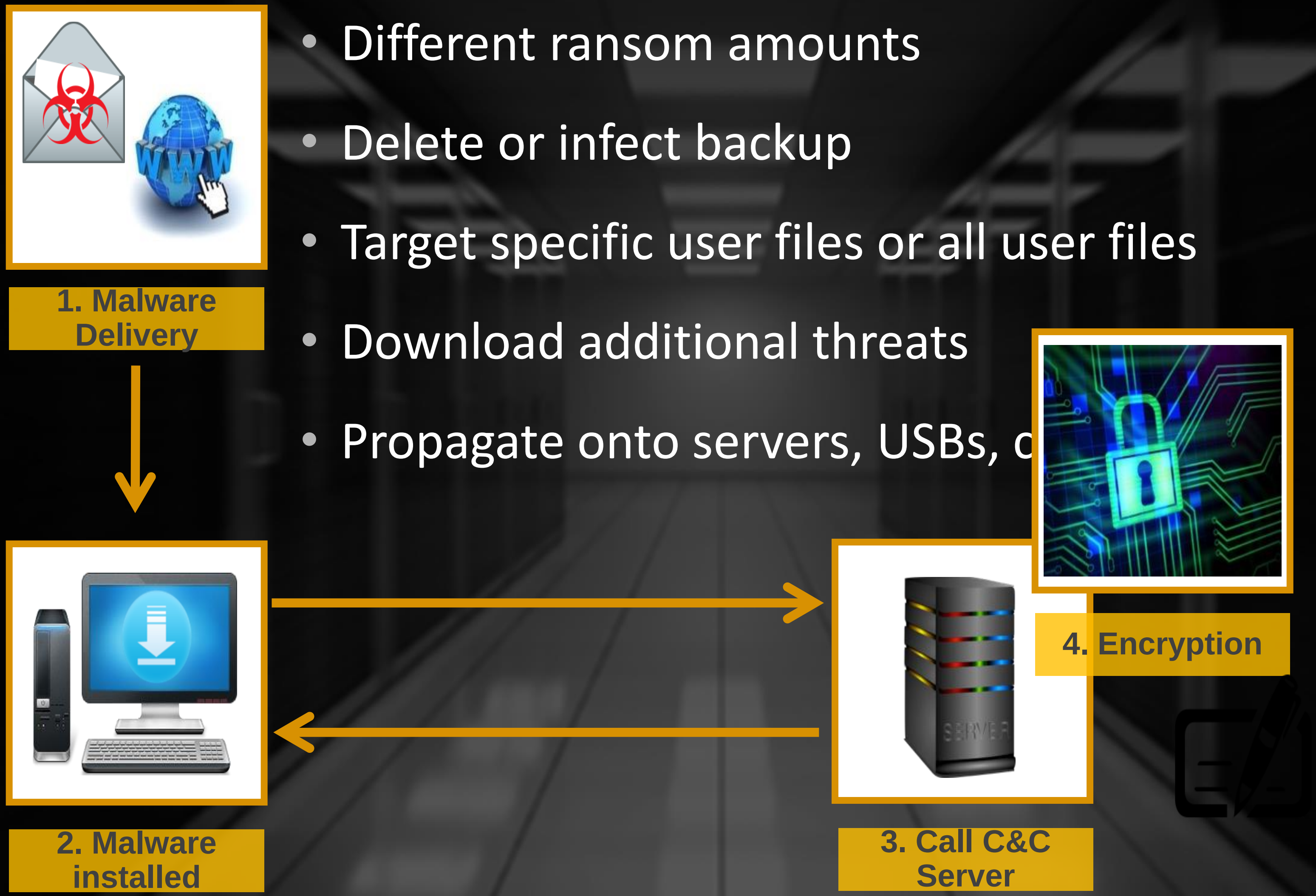
2. Malware installed

3. Call C&C Server

4. Encryption

Ransomware Attack Chain - Variations

- Different ransom amounts
- Delete or infect backup
- Target specific user files or all user files
- Download additional threats
- Propagate onto servers, USBs, c



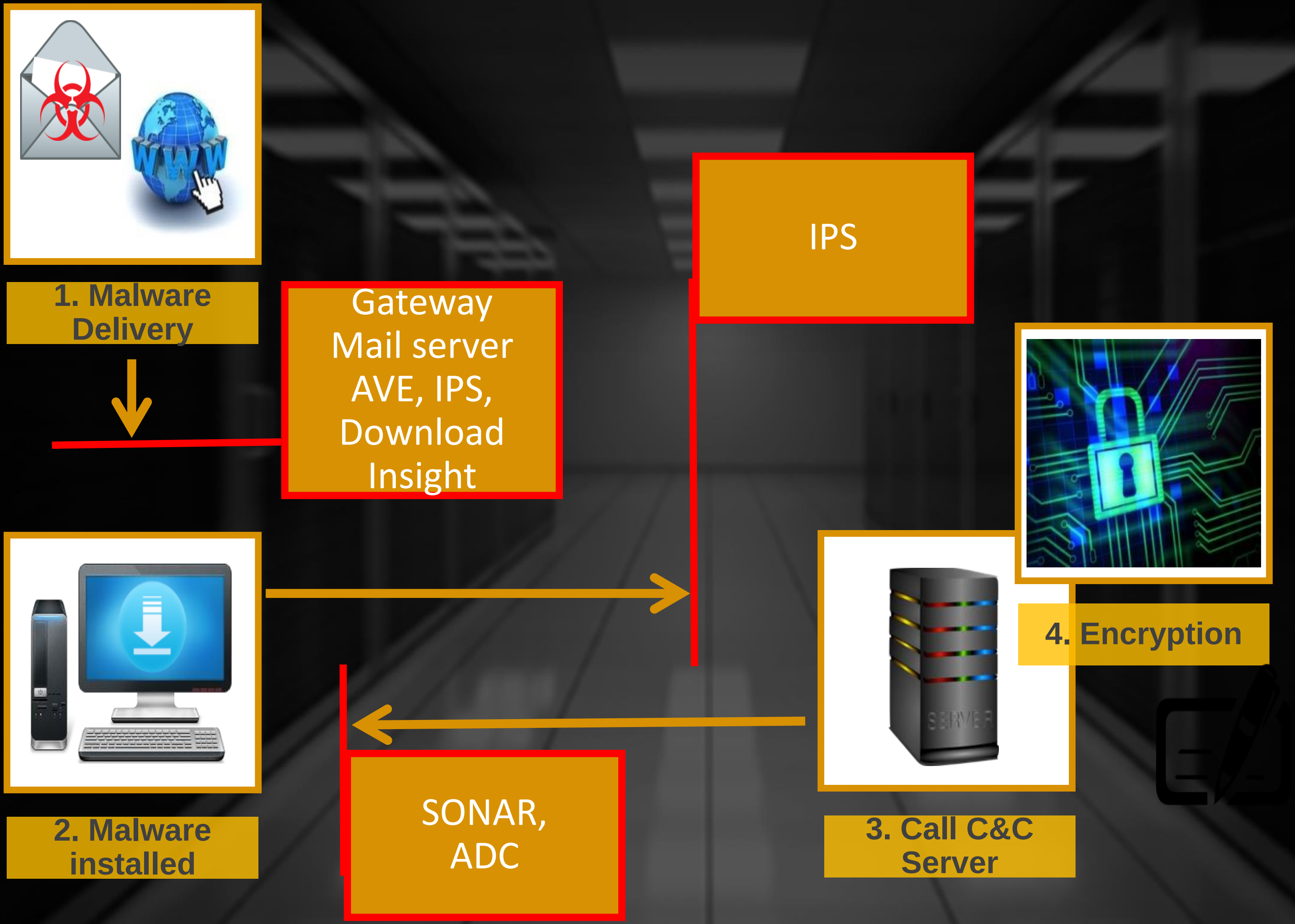
1. Malware Delivery

2. Malware installed

3. Call C&C Server

4. Encryption

If There Is An Attack Chain There Is A Kill Chain



1. Malware Delivery

Gateway
Mail server
AVE, IPS,
Download Insight

IPS

2. Malware installed

SONAR, ADC

3. Call C&C Server

4. Encryption

Protection Against Ransomware

- Install, configure and maintain an endpoint security solution
- User Education
- Employ content scanning and filtering on your mail servers
- Maintain a current patch level for any operating systems and applications that have known vulnerabilities
- Limit end user access to mapped drives – make read only and password protect
- Deploy and maintain a comprehensive backup solution
  - Make sure backup is not writeable by network workstations or servers

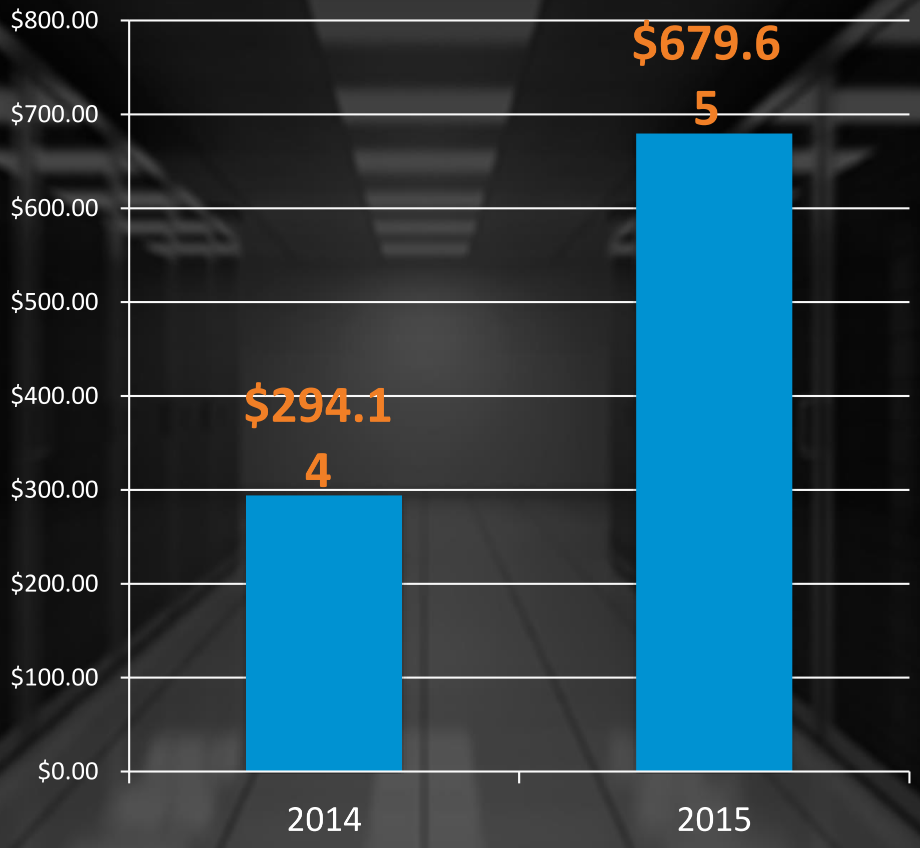
If You Get Infected

- Isolate the infected computer before the ransomware can attack network drives to which it has access
- Clean the machine
- Restore damaged files from a known good backup
- And…

If You Get Infected

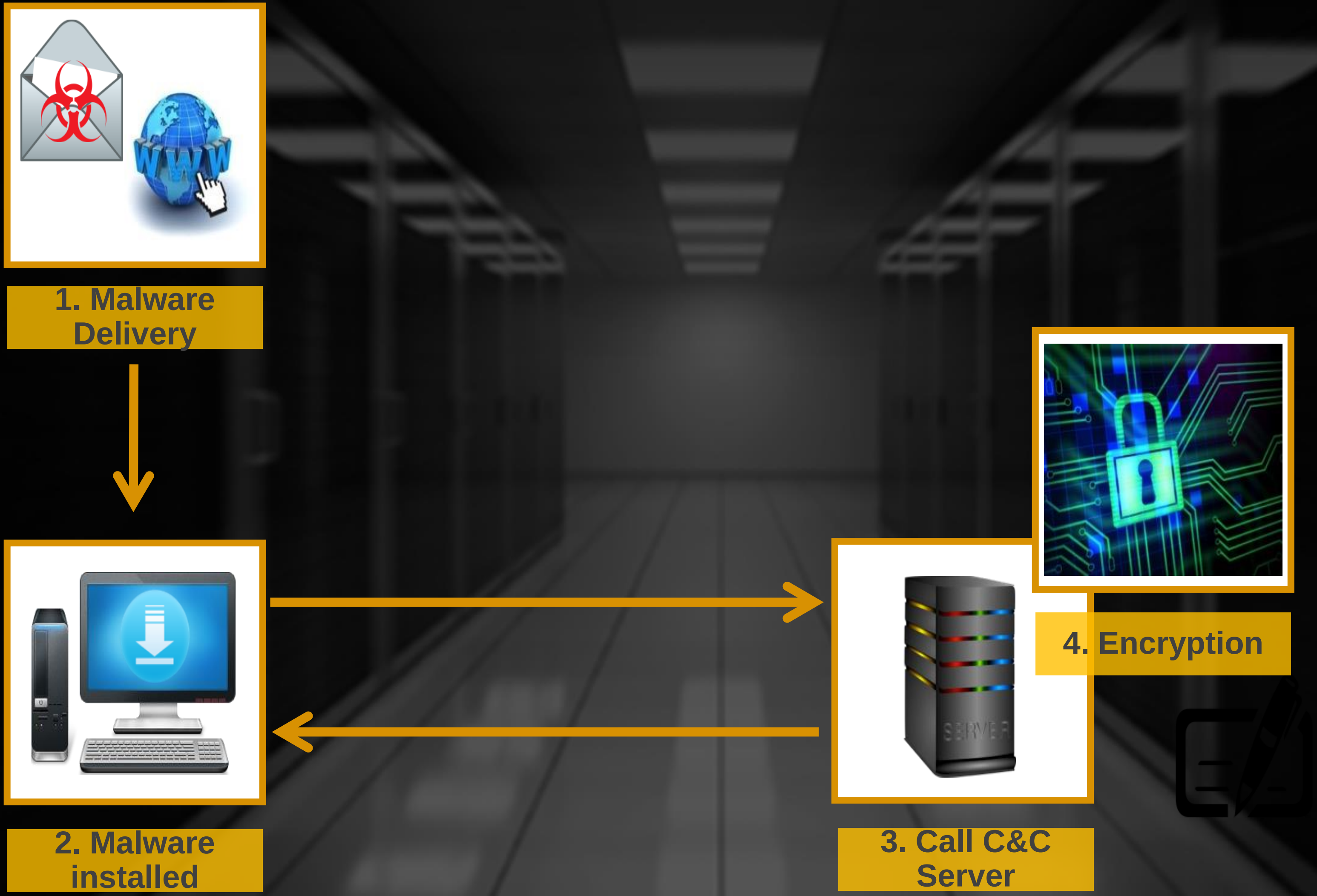
Do not pay the ransom

Willingness To Pay Is Driving Up The Cost Of The Ransom



Paying The Ransom Puts a Notch on Your Gate

Ransomware Attack Chain



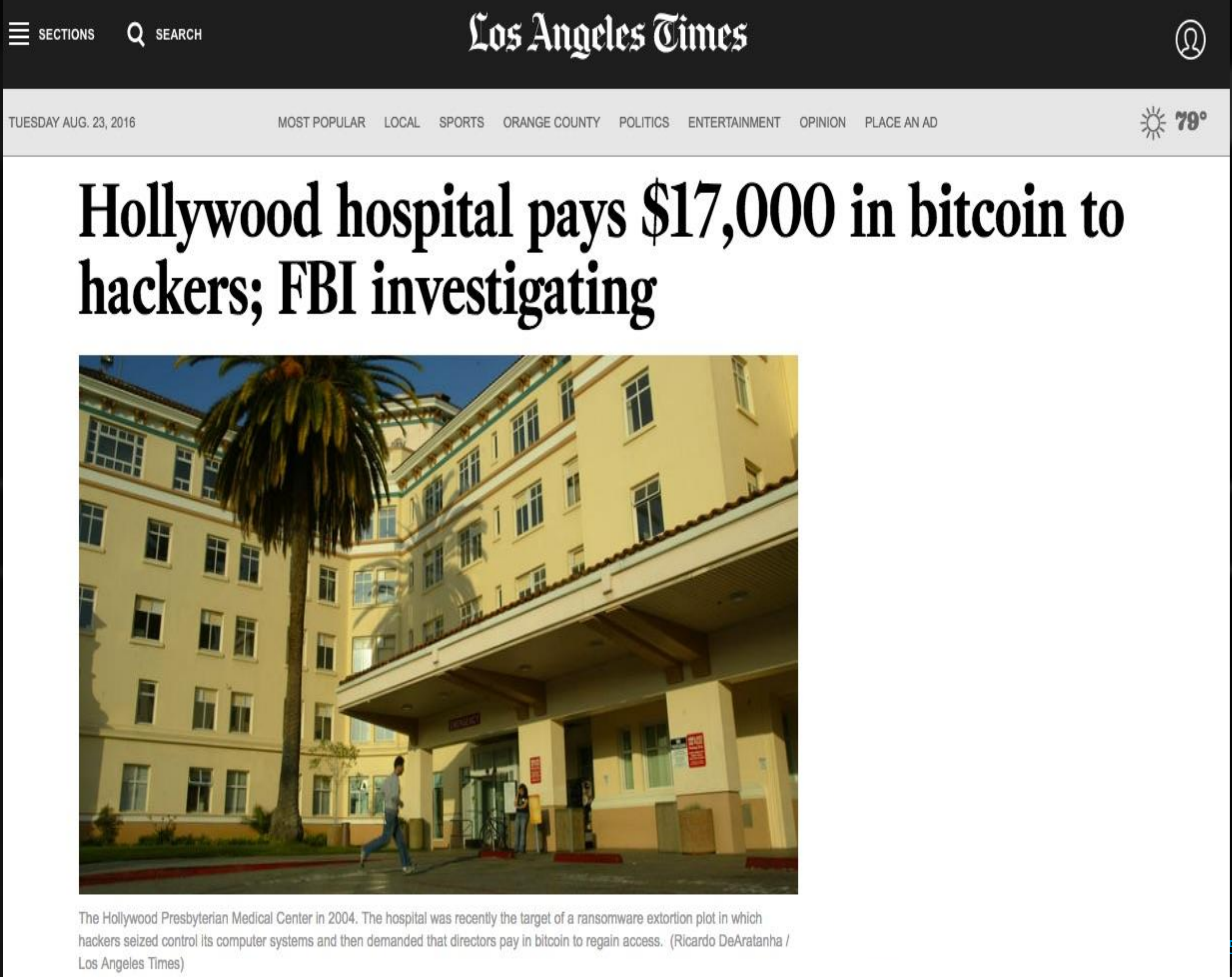
1. Malware Delivery

2. Malware installed

3. Call C&C Server

4. Encryption

Paying The Ransom Puts a Notch on Your Industry’s Gate



SECTIONS SEARCH

Los Angeles Times

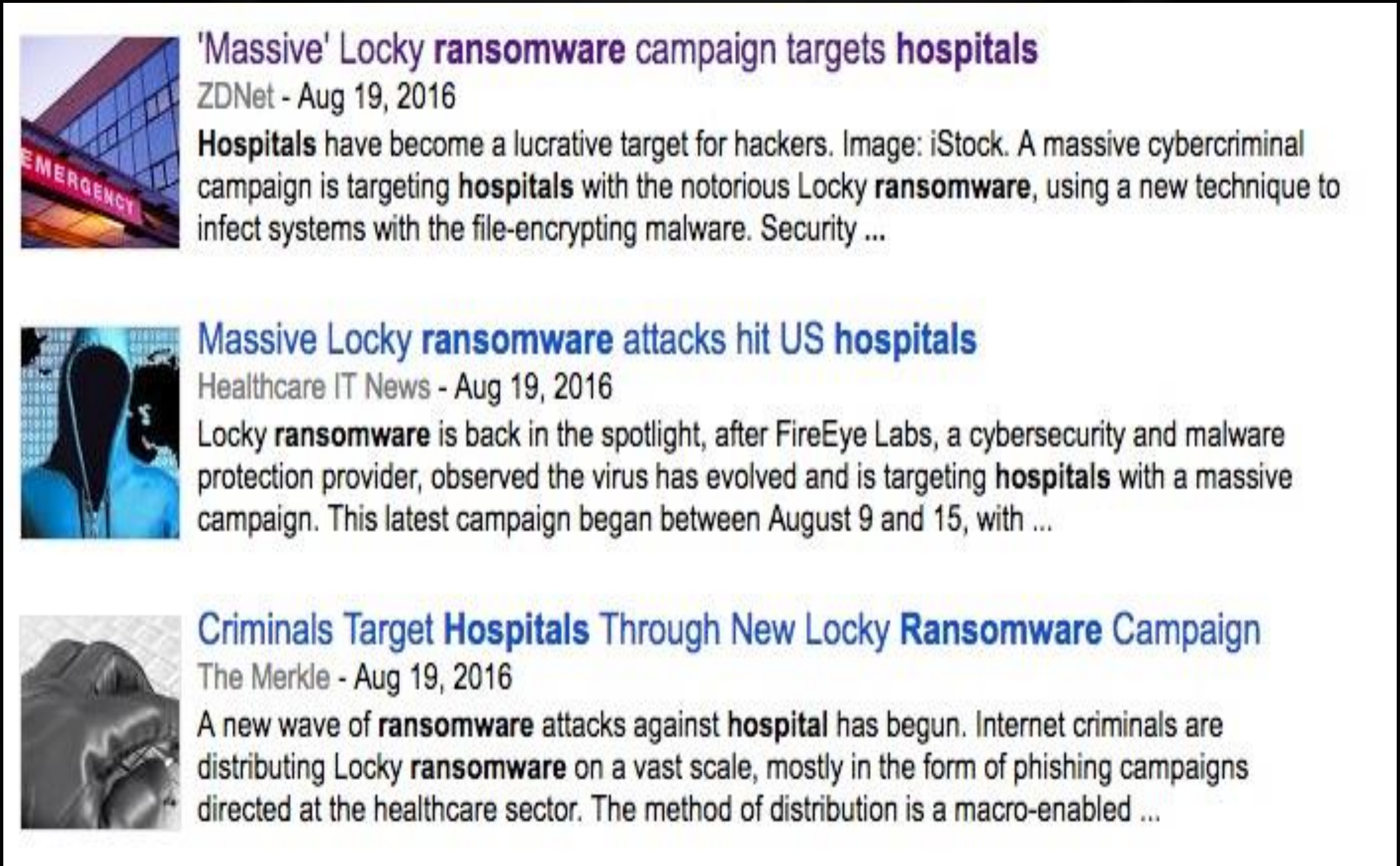
TUESDAY AUG. 23, 2016

MOST POPULAR LOCAL SPORTS ORANGE COUNTY POLITICS ENTERTAINMENT OPINION PLACE AN AD

☼ 79°

Hollywood hospital pays $17,000 in bitcoin to hackers; FBI investigating

The Hollywood Presbyterian Medical Center in 2004. The hospital was recently the target of a ransomware extortion plot in which hackers seized control its computer systems and then demanded that directors pay in bitcoin to regain access. (Ricardo DeAratanha / Los Angeles Times)



'Massive' Locky **ransomware** campaign targets **hospitals**

ZDNet - Aug 19, 2016

Hospitals have become a lucrative target for hackers. Image: iStock. A massive cybercriminal campaign is targeting **hospitals** with the notorious Locky **ransomware**, using a new technique to infect systems with the file-encrypting malware. Security ...

Massive Locky **ransomware** attacks hit US **hospitals**

Healthcare IT News - Aug 19, 2016

Locky **ransomware** is back in the spotlight, after FireEye Labs, a cybersecurity and malware protection provider, observed the virus has evolved and is targeting **hospitals** with a massive campaign. This latest campaign began between August 9 and 15, with ...

Criminals Target **Hospitals** Through New Locky **Ransomware** Campaign

The Merkle - Aug 19, 2016

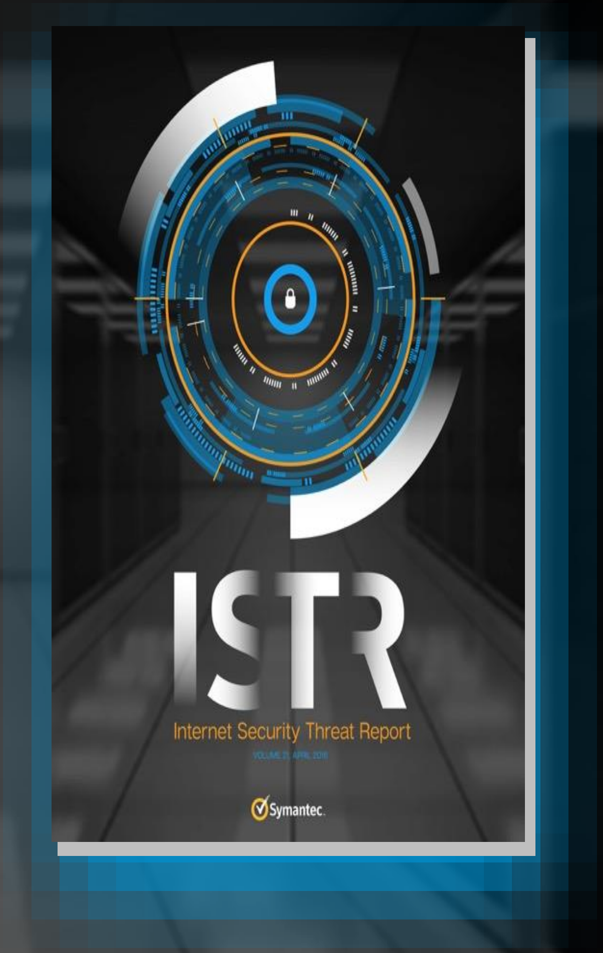
A new wave of **ransomware** attacks against **hospital** has begun. Internet criminals are distributing Locky **ransomware** on a vast scale, mostly in the form of phishing campaigns directed at the healthcare sector. The method of distribution is a macro-enabled ...

Kevin Haley

khaley@symantec.com

@kphaley

Thank you!



This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.

Question & Answer session

- Type your question into the “Questions” box and the moderator will read the question on your behalf.

THANK YOU!

Additional questions or feedback?
Contact Jerryl Guy at jguy@naco.org