



How to Defeat Ransomware

Ed Cabrera, VP Cybersecurity Strategy

@Ed_E_Cabrera

Jon Clay

Cybersecurity Expert



Cyber-Safe

'Ransomware' crime wave growing

by David Fitzpatrick and Drew Griffin @CNNTech

April 4, 2016: 6:14 PM ET

Recommend 722



HOME | POLICY | CYBERSECURITY

DHS: Ransomware attacks widely targeting feds

SC Magazine > News > U.S., Canada issue ransomware alert



Doug Olenick, Online Editor

Follow @DougOlenick

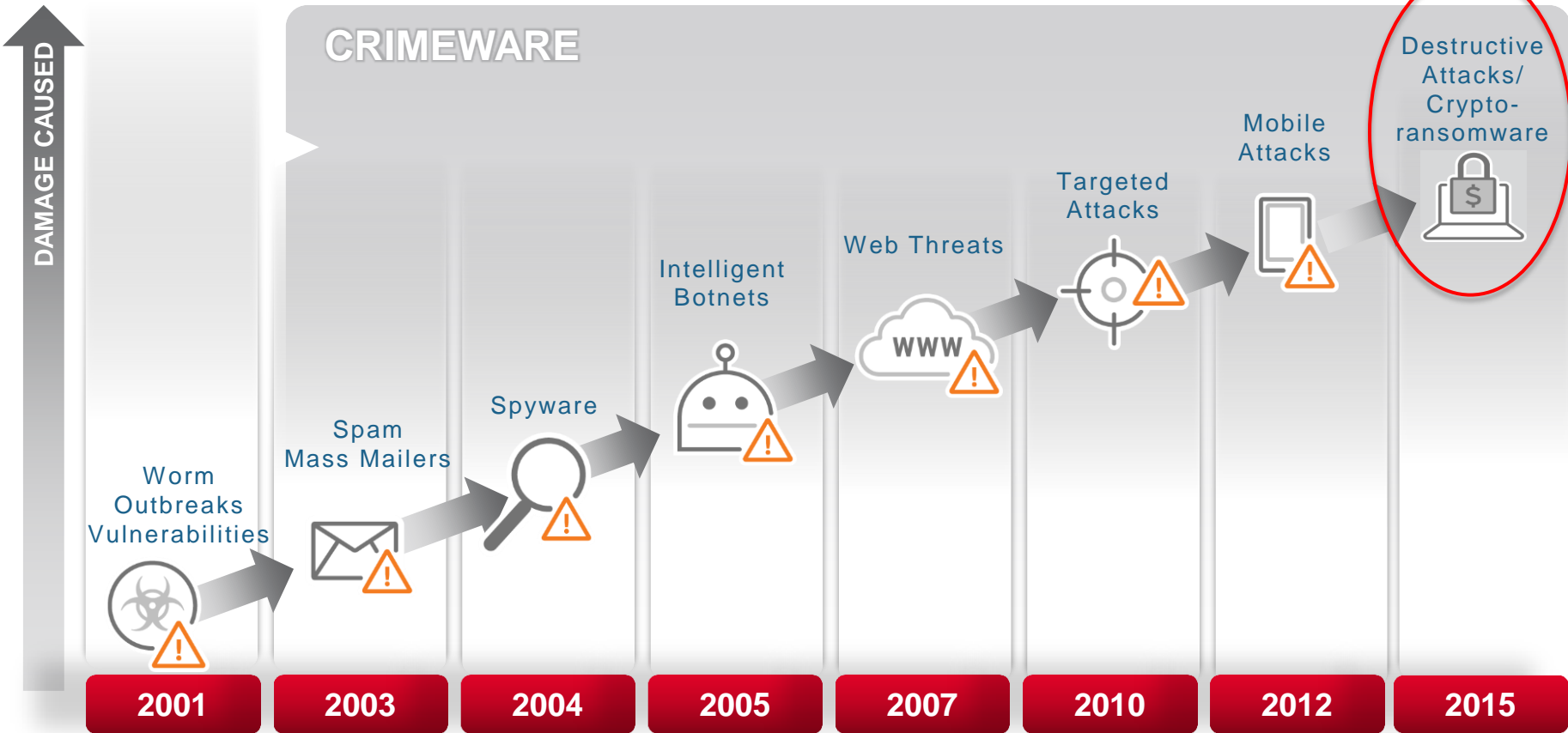
April 05, 2016

U.S., Canada issue ransomware alert

HOME \ NEWS \ SECURITY

MedStar hackers exploited 9-year-old flaw to hold hospital data for ransom

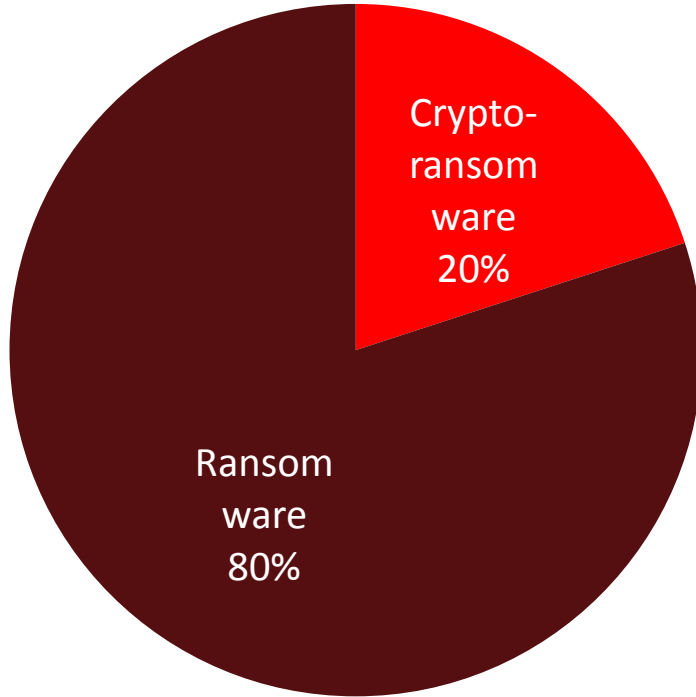
Threat Landscape Evolution



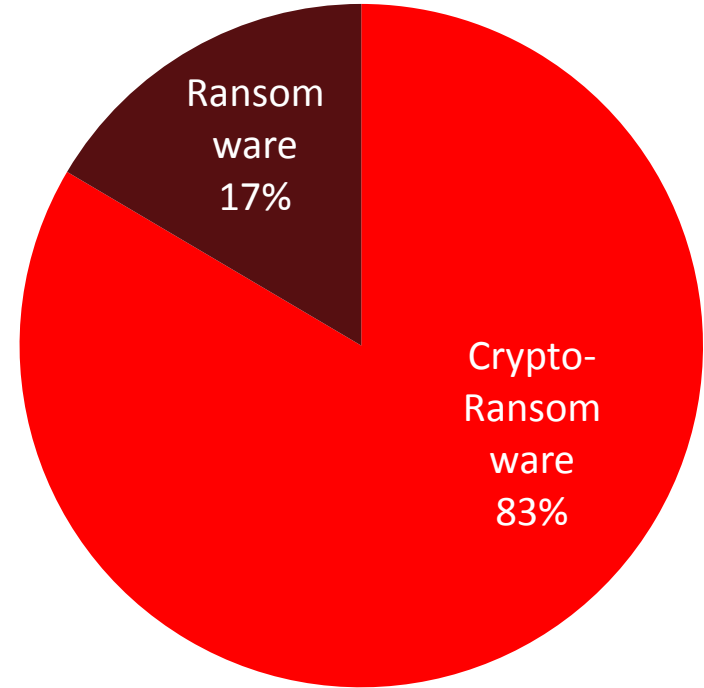
Ransomware Evolution



Q4'2014 Ratio of Ransomware vs Crypto-ransomware

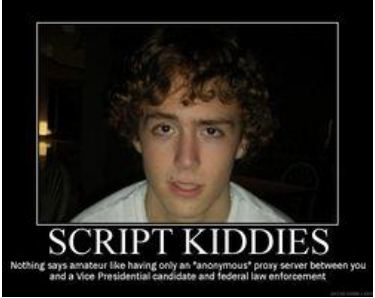


Q4'2015 Ratio of Ransomware vs Crypto-ransomware



Motivation: Return per Infection

 Spam bot \longrightarrow \$












 Banking Trojan \longrightarrow \$\$

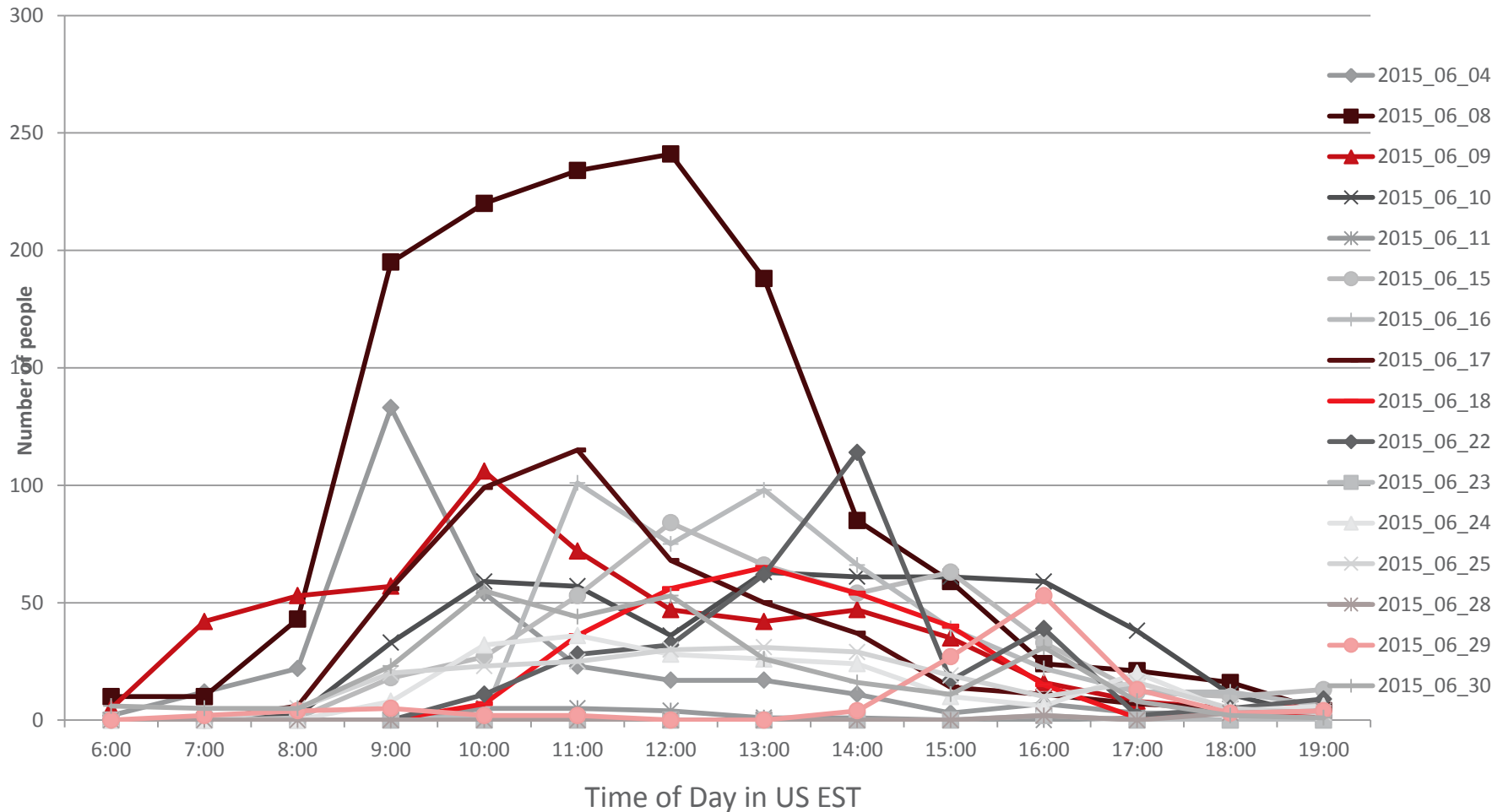
 Crypto-ransomware \longrightarrow \$\$\$



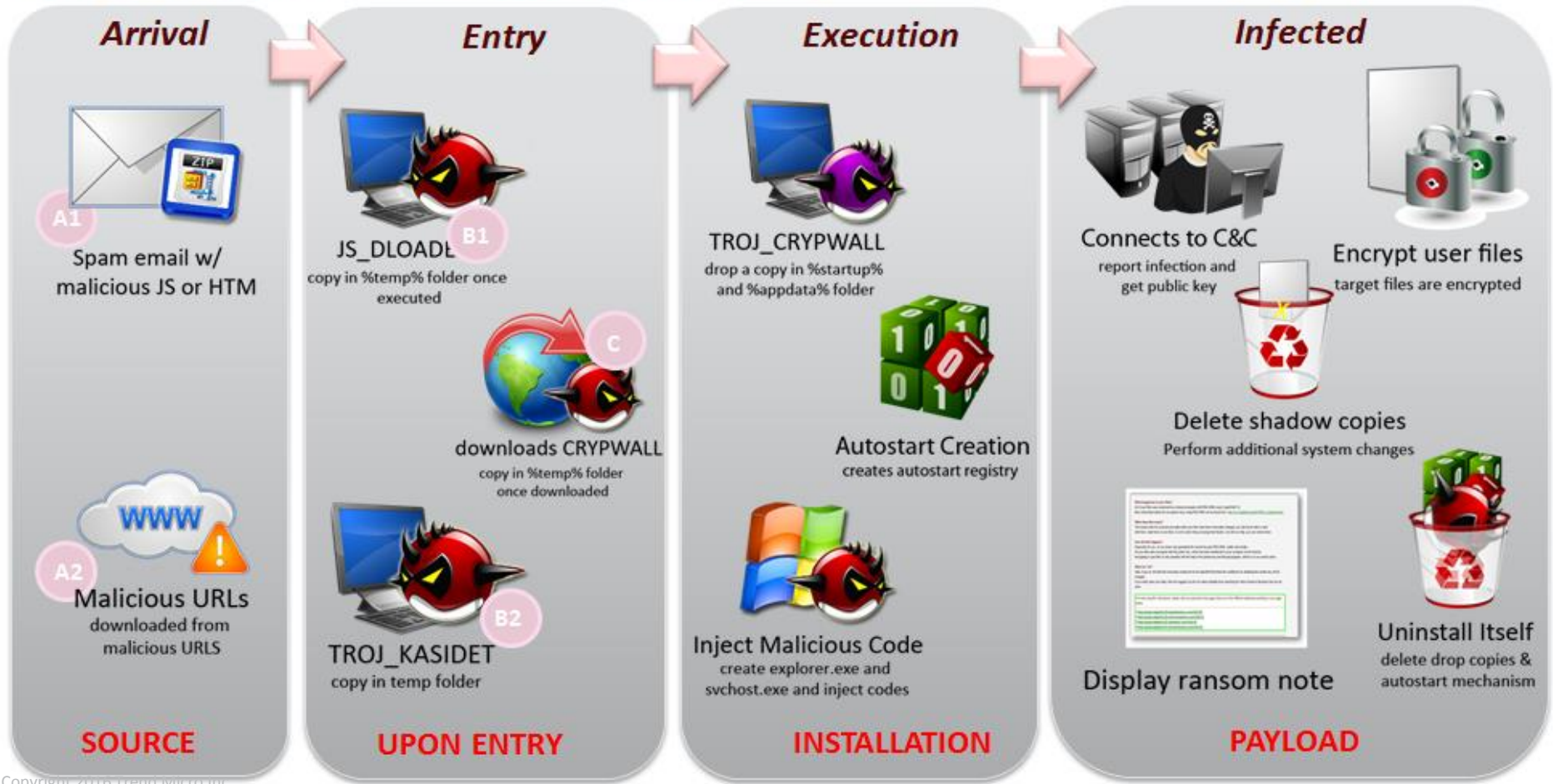
Jan 2016 Regional Ransomware Outbreaks

Sun	Mon	Tue	Wed	Thu	Fri	Sat
					1	2
3	4	5	6	7	8	9
10	11	12 	13	14	15	16
17	18	19 	20 	21 	22 	23
24	25	26 	27 	28 	29 	30
31						30

CryptoWall: Number of clicks on malicious URLs per hour on day of outbreak - June 2015

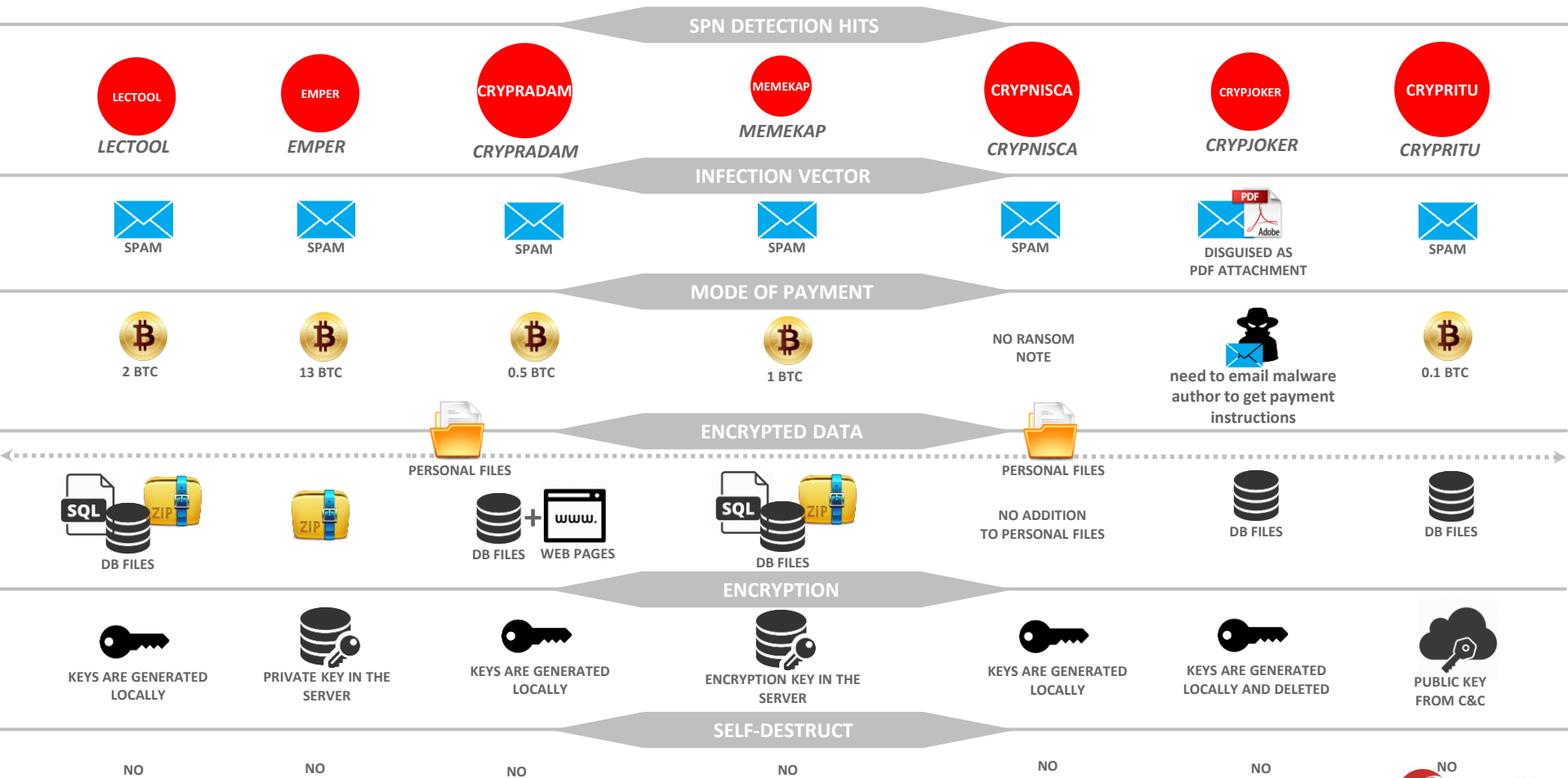


Infection Chain

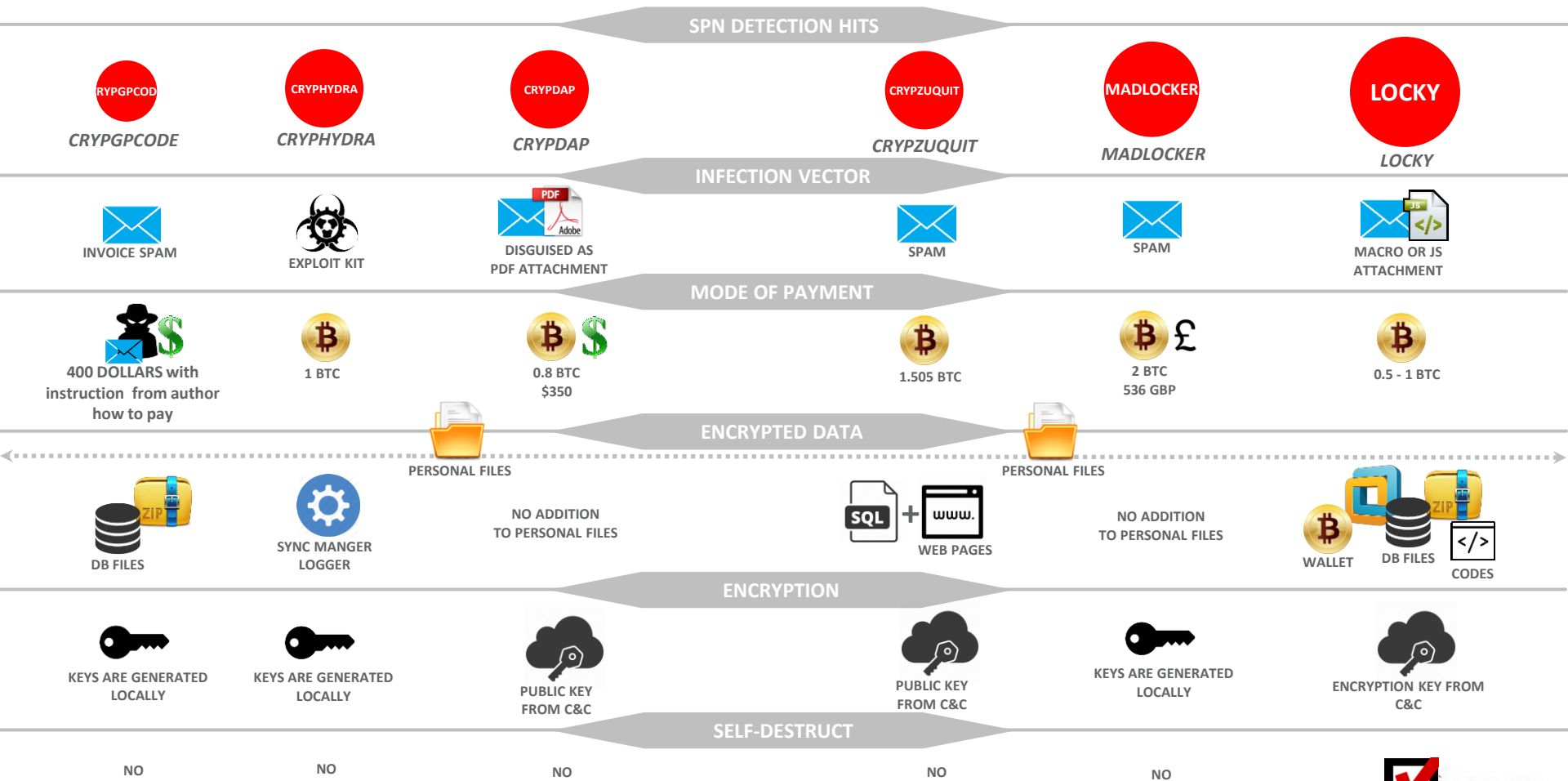


Recent Crypto Activity

Jan 2016 - Ransomwares
















Feb 2016 - Ransomwares



March 2016 - Ransomwares











 with customer case

SPN DETECTION HITS












 CERBER	 CRYPURA	 KeRanger	 TESLA 4.0	 MAKTUB	 SURPRISE	 PETYA	 Powerware	 CRIPOTOSO	 COVERTON	 CRYPTOHASU	 KIMCIL	 MRAWARE
---	---	--	---	--	--	---	---	---	--	--	--	---

Thought bubbles: "It speaks!!" (above Cerber), "Power shell script" (above Powerware), "Target: Magento eCommerce" (above MRAWARE)

INFECTION VECTOR

 EXPLOIT KIT	 SPAM	 APPSTORE	 MACRO OR JS ATTACHMENT	 EXPLOIT KIT	 TERMS-OF_SERVICE (TOS) SPAM	 TEAM VIEWER	 JOB APPLICATION WITH DROPBOX	 MACRO DOWNLOADER ATTACHMENT	<under reversing>	<under reversing>	 SPAM	 HACK	<under reversing>
---	---	---	---	--	--	--	---	--	-------------------	-------------------	---	---	-------------------

MODE OF PAYMENT








 1.24-2.48 BTC	<under reversing>	 1 BTC	 1.3 BTC	 1.4 - 3.9 BTC \$588 - \$1638	 0.5 to 25 BTC	 0.99 - 1.98 BTC \$431 - \$862	 1.18 - 2.37 BTC \$500 - \$1000	 1 BTC then increases by 1 BTC daily	 1 BTC	 1 BTC \$300 Increased /day	 1 BTC \$140	<under reversing>
--	-------------------	--	--	--	--	---	--	--	--	--	--	-------------------

ENCRYPTED DATA

 PERSONAL FILES	 DB FILES	 DB FILES	 CODES	 MACOS FILES	 GAMES	 GAMES	 WALLET	 ACCOUNTING/ FINANCE FILES	 OVERWRITES MBR & BSOD	 US TAX RETURN FILES	<under reversing>	 DB FILES	 SCRIPTS & PROGRAMS	 Website files	 PERSONAL FILES	<under reversing>
--	--	---	--	--	--	--	---	---	--	--	-------------------	---	---	--	---	-------------------

Thought bubble: "Tax fraud" (above US tax return files)

ENCRYPTION

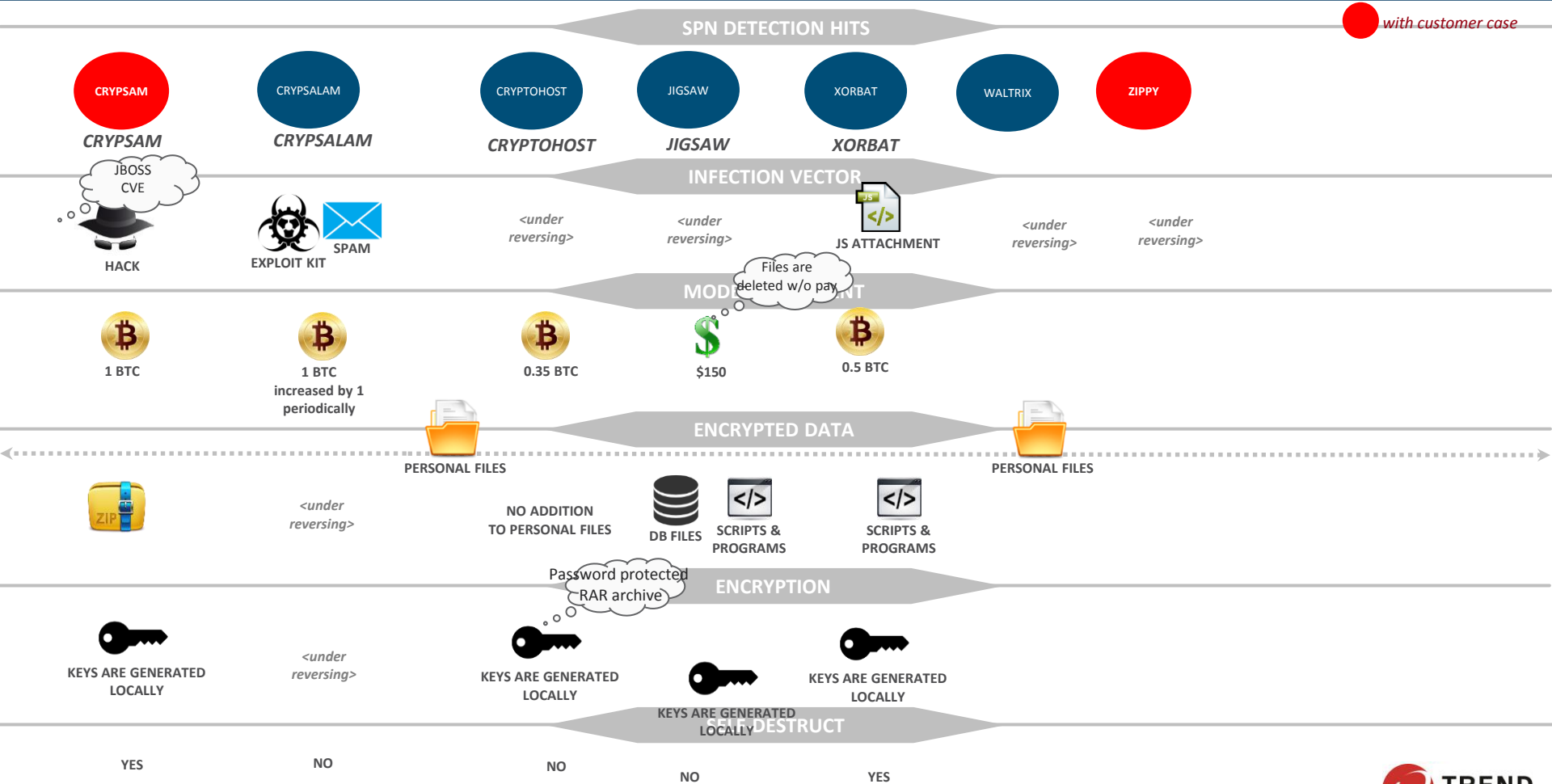
 PRIVATE KEY IS OBTAINED AFTER PAYMENT	 PUBLIC KEY FROM C&C	 PUBLIC KEY FROM C&C	 5 KEY PAIRS GENERATED LOCALLY 1 KEY REQUIRES RSA KEY	 PRIVATE KEY IS OBTAINED AFTER PAYMENT	 PRIVATE KEY IS OBTAINED AFTER PAYMENT	 PRIVATE KEY IS OBTAINED AFTER PAYMENT	 AES KEY GENERATED LOCALLY	<under reversing>	 PRIVATE KEY IS OBTAINED AFTER PAYMENT	 PRIVATE KEY IS OBTAINED AFTER PAYMENT	<under reversing>	<under reversing>
---	--	--	--	--	--	--	--	-------------------	--	--	-------------------	-------------------

SELF-DESTRUCT

NO	NO	NO		NO	NO	NO		<under reversing>	NO	NO	NO	NO
----	----	----	--	----	----	----	--	-------------------	----	----	----	----

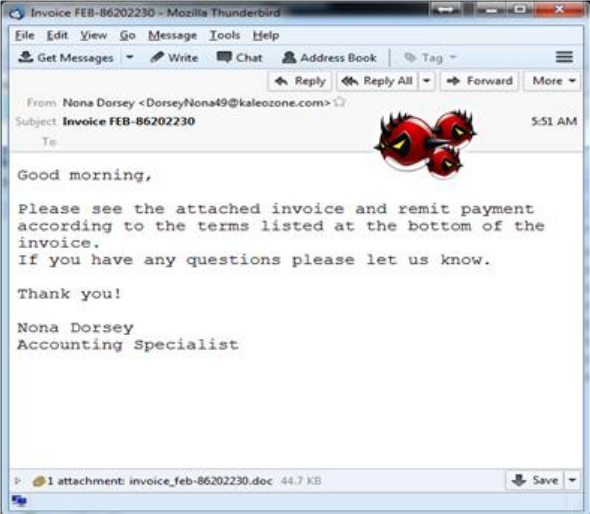
April 2016 - Ransomwares

 with customer case



Locky Ransomware – Malicious Macros

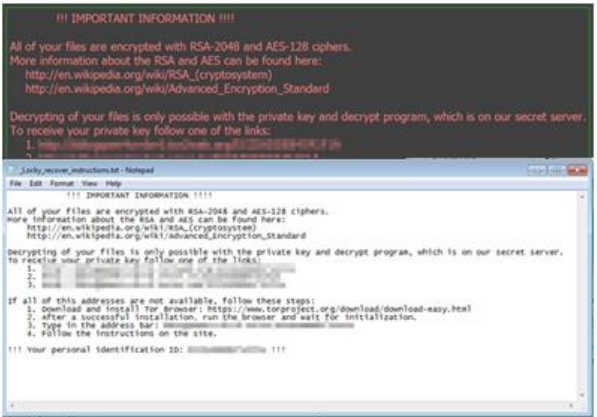
Arrival



Ransom_LOCKY was seen as downloaded by a malicious attachment in spam mails detected as:

- JS_LOCKY.A
- W2KM_LOCKY.BQS
- W2KM_LOCKY.A
- W2KM_LOCKY.D
- W2KM_LOCKY.B
- X2KM_LOCKY.A

Installation

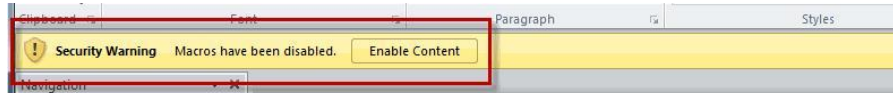


- Drops copy of itself
Note: deletes itself after encryption of files
- Drops component
- Creates autostart registry
- Encrypts and renames the encrypted files to {unique ID per victim}{identifier}.locky
- Modified the Internet Explorer Zone Settings.

Payload



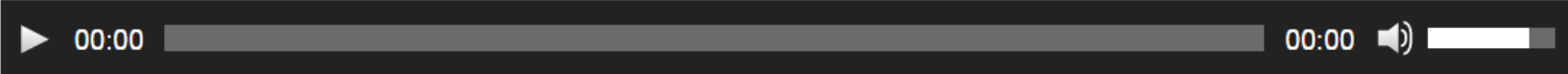
Extorts money by asking payment for decryption of files
Ransom_LOCKY is requesting 0.5 Bitcoin ransom (\$209.27)



Petya Ransomware – Overwrite MBR



CERBER Ransomware – Talk to Me



```
# DECRYPT MY FILES #txt - Notepad
File Edit Format View Help

          C E R B E R
          -----

Your documents, photos, databases and other important files have been encrypted!
To decrypt your files follow the instructions:

-----+-----

1. Download and install the "Tor browser" from https://www.torproject.org/
2. Run it
3. In the "Tor browser" open website:
   [REDACTED]
4. Follow the instructions at this website

-----

<...Quod me non necat me fortiores facit.>
```



Maktub Ransomware – Graphic Artists?

HOW MUCH DOES IT COST?

We hope that you are convinced that we can do an important thing! The faster you transfer the money every stage of payment, you get 3 days or 72 hours right top corner. After the clock shows 00:00:00 and the price automatically increases. We only accept form of payment. Here is a table that shows the current stage is marked in yellow.

Stage	Time of payment	Price
1	During the first 3 days	0.00000000 BTC
2	From 3 to 6 days	0.00000000 BTC
3	From 6 to 9 days	0.00000000 BTC
4	From 9 to 12 days	0.00000000 BTC
5	From 12 to 15 days	0.00000000 BTC
6	More than 15 days	0.00000000 BTC

After 15 days of no payment, we do not guarantee that you can be disconnected at any moment and you will be disconnected. Please take this seriously.

71:58:13
During this time you need to make a payment or the price will be increased.

BITCOIN PURCHASE 5

If this is the first time you heard about Bitcoin, don't despair! Simply google this word and you will find all the answers. We can just recommend a few sites that will be of use to you.

Buying Bitcoins - This page aims to be the best resource for new users to understand how to buy Bitcoins

Localbitcoins (WU) - Buy Bitcoins with Western Union

Coincafe.com - Recommended for fast, simple service. Payment Methods: Western Union, Bank of America, Cash by FedEx, Moneygram, Money Order. In NYC: Bitcoin ATM, In Person

LocalBitcoins.com - Service allows you to search for people in your community willing to sell bitcoins to you directly

btcdirect.eu - THE BEST FOR EUROPE

coinrrr.com - Another fast way to buy bitcoins

bitquick.co - Buy Bitcoins Instantly for Cash

How To Buy Bitcoins - An international directory of bitcoin exchanges

Cash Into Coins - Bitcoin for cash

CoinJar - CoinJar allows direct bitcoin purchases on their site

ZipZap - Global cash payment network enabling consumers to pay for digital currency

71:58:42
During this time you need to make a payment or the price will be increased.

WHERE DO I PAY? 4

Payment is automated! You won't have to wait while making payment. As soon as you send the money, we will automatically count them and create the transaction.

After a couple of hours, you will receive the decryption key.

Send the Bitcoin to the following address:

1A1zP1eP5QGefi2DMPTfTL5SLmv7nfz

SamSam Ransomware – Threat to Servers

CVE-2010-0738

The MITRE CVE dictionary describes this issue as:

The JMX-Console web application in JBossAs in Red Hat JBoss Enterprise Application Platform (aka JBoss EAP or JBEAP) 4.2 before 4.2.0.CP09 and 4.3 before 4.3.0.CP08 performs access control only for the GET and POST methods, which allows remote attackers to send requests to this application's GET handler by using a different method.

Find out more about CVE-2010-0738 from the [MITRE CVE dictionary](#) dictionary and [NIST NVD](#).

CVSS v2 metrics

NOTE: The following CVSS v2 metrics and score provided are preliminary and subject to review.

Impact: **Critical**
Public Date: 2010-04-26
CWE: [CWE-284](#)

Bugzilla:
[574105](#): CVE-2010-0738 JBoss EAP jmx authentication bypass with crafted HTTP request

CVE Details

The ultimate security vulnerability datasource

[Log In](#) [Register](#) [Reset Password](#) [Activate Account](#)

(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

Vulnerability Feeds & WidgetsNew

[www.itsecdb.com](#)



[Switch to https://](#)
[Home](#)

Browse :

[Vendors](#)

[Products](#)

[Vulnerabilities By Date](#)

[Vulnerabilities By Type](#)

Vulnerability Details : [CVE-2007-1036](#) (2 Metasploit modules)

The default configuration of JBoss does not restrict access to the (1) console and (2) web management interfaces, which allows remote attackers to bypass authentication and gain administrative access via direct requests.

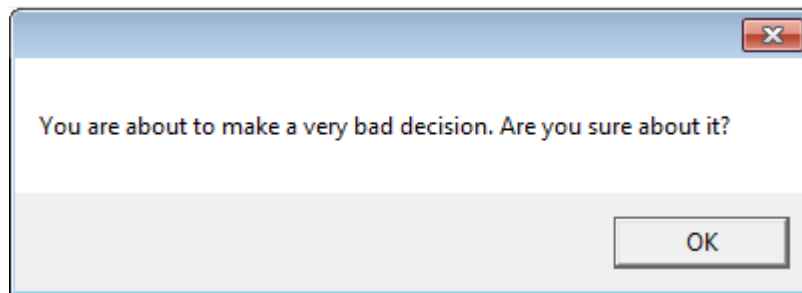
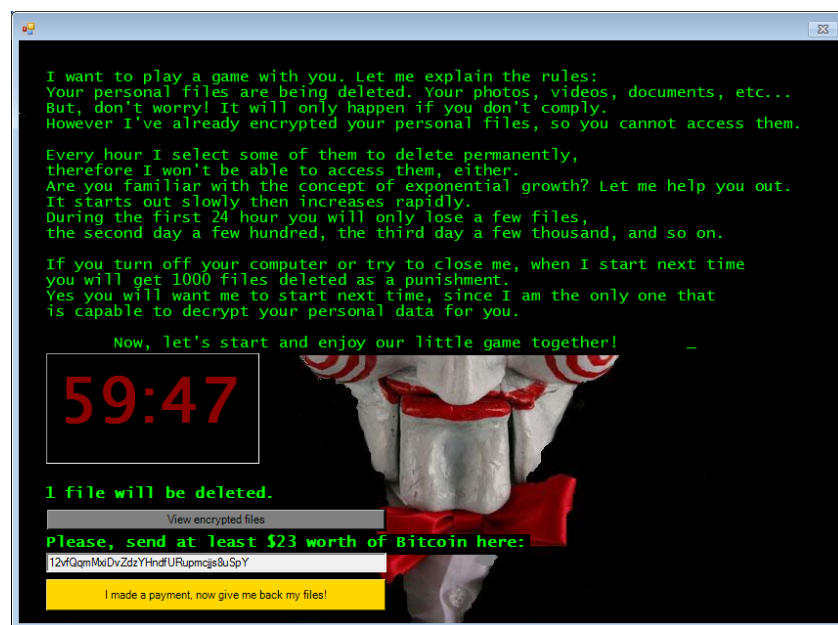
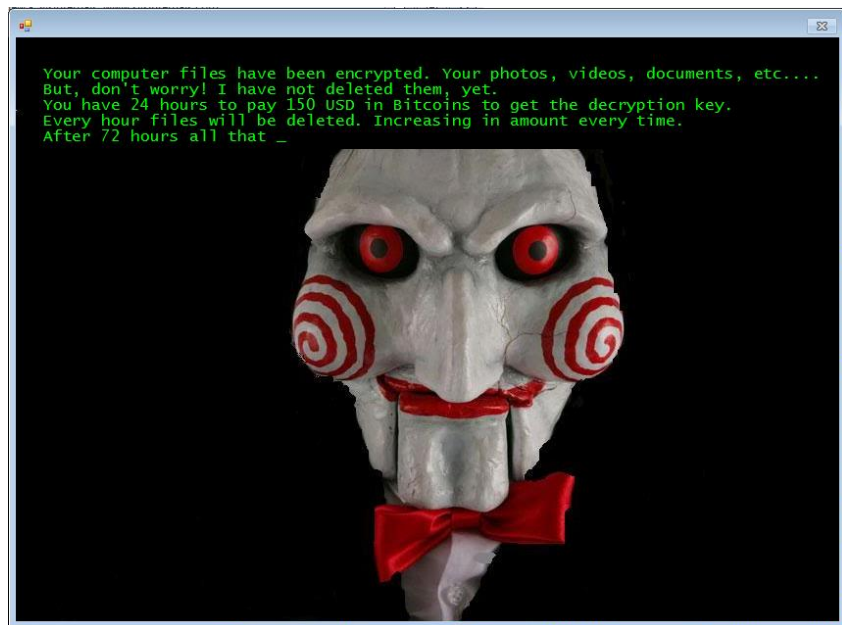
Publish Date : 2007-02-21 Last Update Date : 2009-03-16

– CVSS Scores & Vulnerability Types

CVSS Score	7.5
Confidentiality Impact	Partial (There is considerable informational disclosure.)
Integrity Impact	Partial (Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited.)
Availability Impact	Partial (There is reduced performance or interruptions in resource availability.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	User
Vulnerability Type(s)	Bypass a restriction or similar
CWE ID	264



Jigsaw Ransomware -



Data Exfiltration as a 2nd Extortion Request

Chimera® Ransomware



You are victim of the Chimera
encrypted and can not
Maybe some prog

Please transfer Bitco
yo

Address: 1HqoNf

Amount: 0,9394

For the decryption prog

<https://mega.nz/Chime>

If you don't pay your private data, which include pictures and
videos will be published on the internet in relation on your
name.

Take advantage of our affiliate-program!
More information in the source code of this file.

If you don't pay your private data, which include pictures and videos will be published on the internet...

Use of Compromised Sites

- Infection Vector – Distributes Malware
- Redirect Site – Embedded URLs connect to these sites, which redirect to malicious servers
- Command & Control Sites
- Captcha Sites

CTB-Locker for Websites

Protection Best Practices & Solutions

Protecting Against Ransomware



Back-up and Restore

Automated: 3 copies, 2 formats, 1 air-gapped from network



Access Control

Limit access to business critical data & shared drives



Keep Current with Patching

Minimize exploits of vulnerabilities



Don't Pay the Ransom

Pay-off encourages further attacks, no guarantee of data recovery



Employee Education on Phishing

Awareness, best practices, simulation testing



Improve Security Posture

Follow best practices for current solution, additional technology

Trend Micro Protection Against Ransomware



Research and Development

- Active data scientists & threat researchers work to enhance capabilities (based on the campaign data and malware/URL samples we are collecting)
 - Smart patterns
 - Machine Learning
 - Advanced Detection Analytics
 - Behavioral analysis
 - Correlating the Threat Lifecycle

Ransomware Targets

Fewer attacks against servers BUT, may be more destructive

Most ransomware targets known vulnerabilities

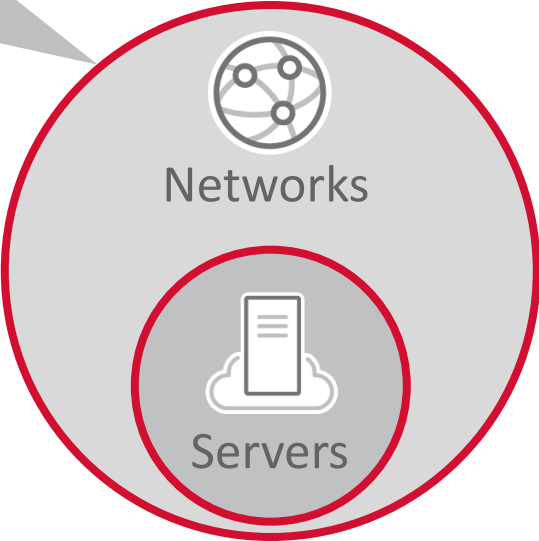
Can spread via lateral movement



Ransomware Targets

Possible point of entry

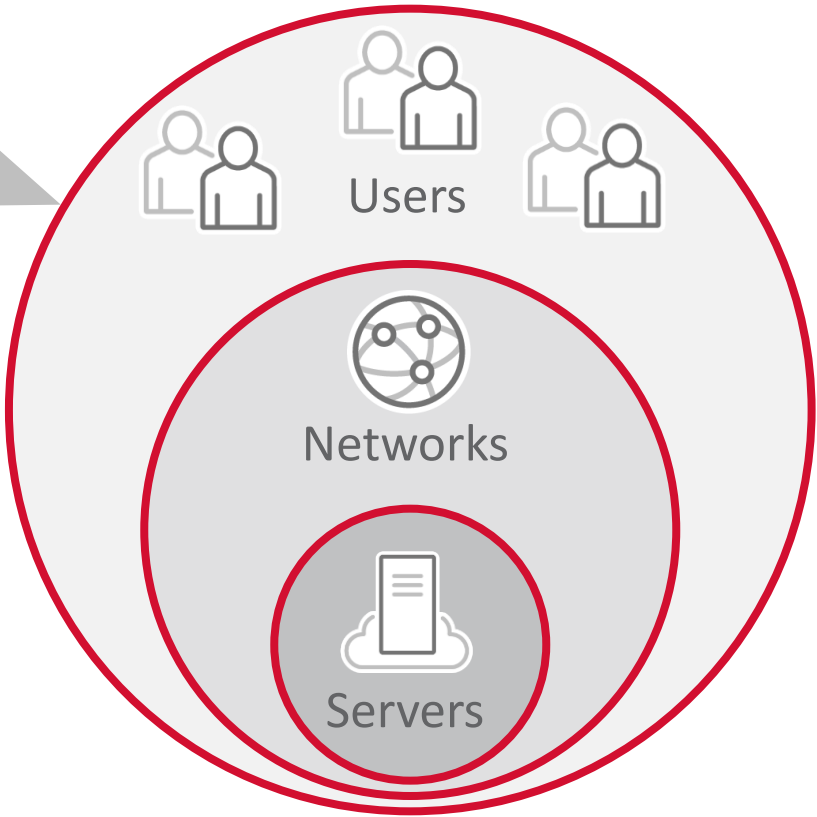
Malware spreads to other users and servers

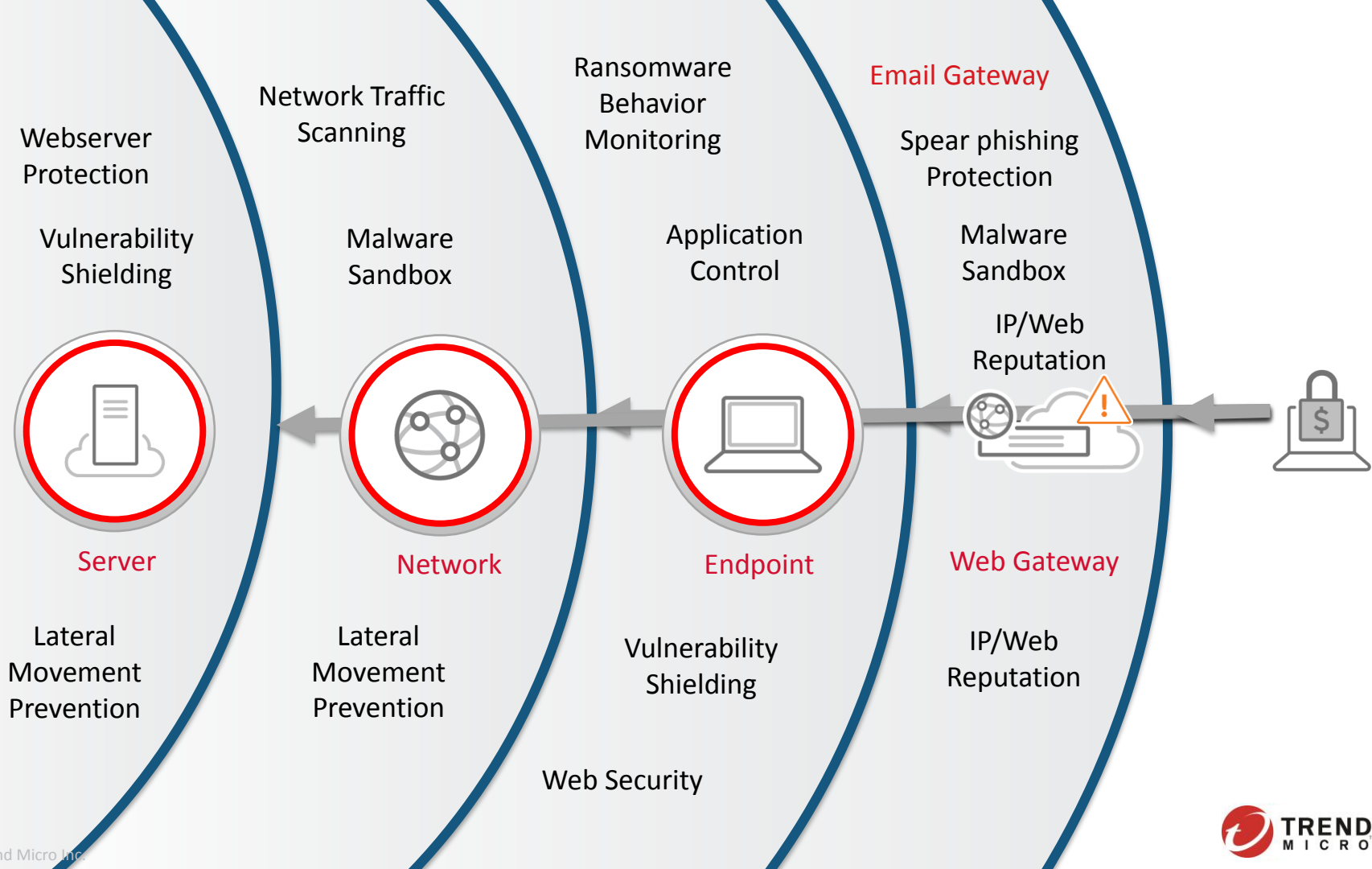


Ransomware Targets

Endpoints are most common target

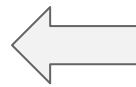
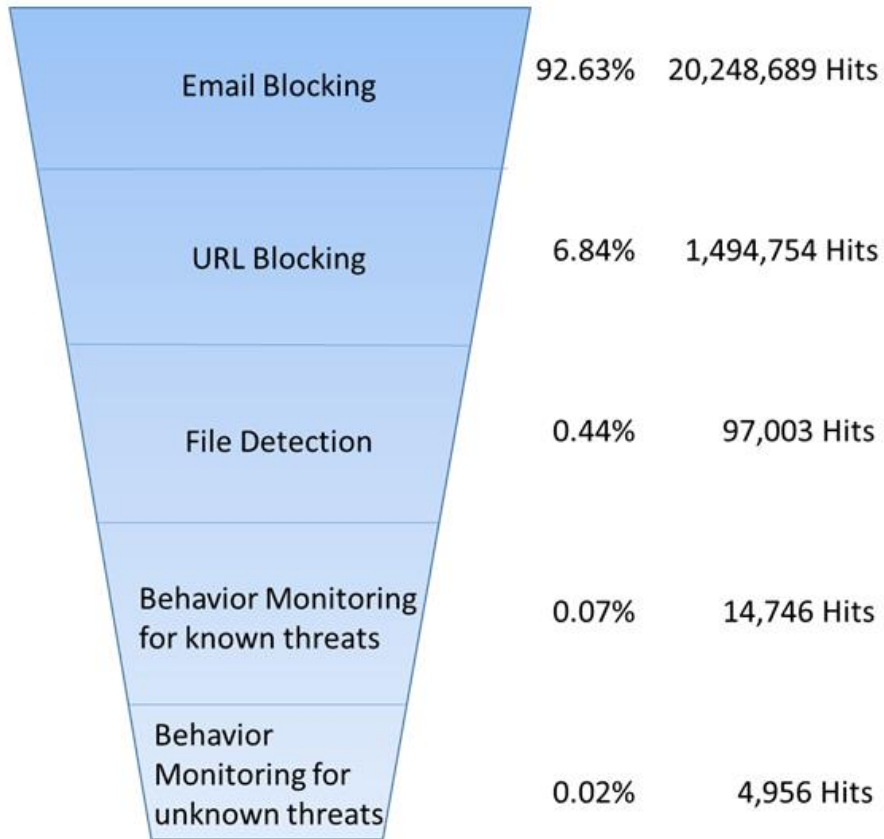
Web and spearphishing the most common attack vectors



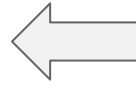


Effective Layered Protection

SPN feedback of Ransomware detection



Most ransomwares can be stopped on gateway level



The last defense is Anti-Ransomware feature to proactively detect & block ransomware execution

Time Period: 3/13 ~ 3/26



TREND
MICRO™

A world **safe** for exchanging digital information

A major pure-play security software company

Founded 1988, United States
Headquarters Tokyo, Japan
2013 Sales \$1.1B USD
Customers 500,000 businesses,
Millions of consumers

5000+ Employees in 50+ Countries



96% of the top
50 global
corporations.



100% of the
top 10 automotive
companies.



100% of the
top 10 telecom
companies.



80% of the top
10 banks.



90% of the top
10 oil companies.



TREND
MICRO™

Next Steps – Contact Trend Micro

- Determine if your security strategies address today's threats by speaking with a Trend Micro representative today.
 - Contact Sales – access this link by clicking on the attachments tab.
 - Or call 1-888-762-8736
 - Or email sales@trendmicro.com