aronson LLC
ASSURANCE | TAX | CONSULTING
Expanding What's Possible

Ransomware Prevalence & Safeguards

July 21st, 2016

Agenda

- Describe ransomware characteristics
- Walkthrough different families of ransomware including CryptoWall
- Understand recent and potential ransomware targets
- Compare the advantages & disadvantages of potential payment
- Learn leading practices for prevention & mitigation

Ransomware Overview

- Ransomware is a form of malicious software or ‘malware’, where attackers demand payment in exchange for restored access
- An attack can render a computer, network, certain segments or files within it inaccessible to authorized users
- $18 million+ in losses caused by ransomware from April 2014 - June 2015 according to FBI reports; actual amount could be higher
- Impacts:
  - Temporary / permanent data loss
  - Disruption to operations / service delivery
  - Financial loss
  - Reputational damage

Ransomware Deployment

Ransomware can be deployed to a network or computer via various ways, such as:

- Visiting unsecure websites
- Opening emails from illegitimate senders
- Downloading deceptive attachments
- Clicking on malicious links in emails or social media
- Interacting with misleading spyware removal tools and anti-virus (AV)
- Activating drive-by downloads

Ransomware Deployment continued

Sophos 2015 – Anatomy of Ransomware

Ransomware Families

- Crypto Ransomware (Data locker): Prevents access to files or data via encryption
- Locker Ransomware (Computer locker): Denies access to a computer / device by disabling the user interface
- CryptoLocker Ransomware: (combination)

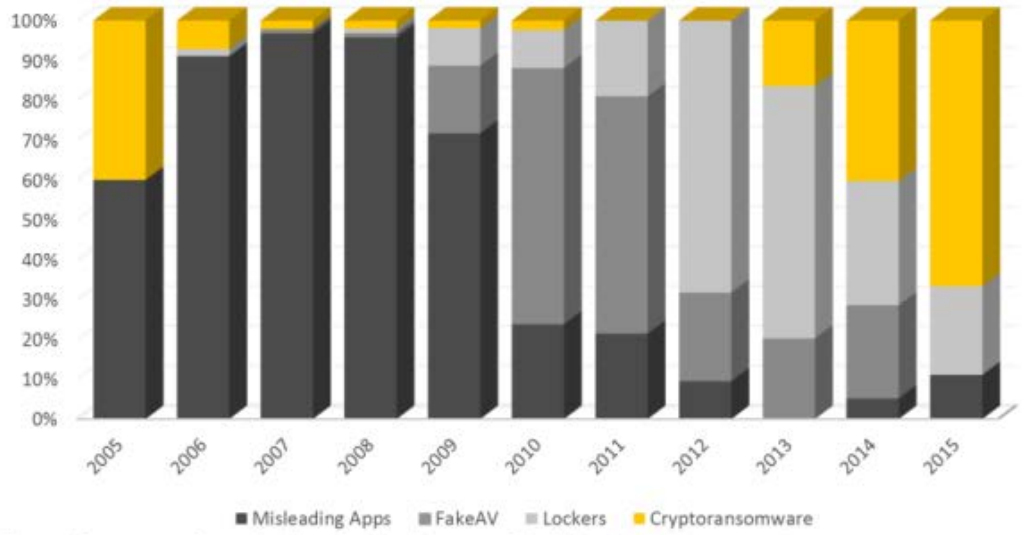


Figure 4. Percentage of new families of misleading apps, fake AV, locker ransomware and crypto ransomware identified between 2005 and 2015

Symantec 2015 – The Evolution of Ransomware

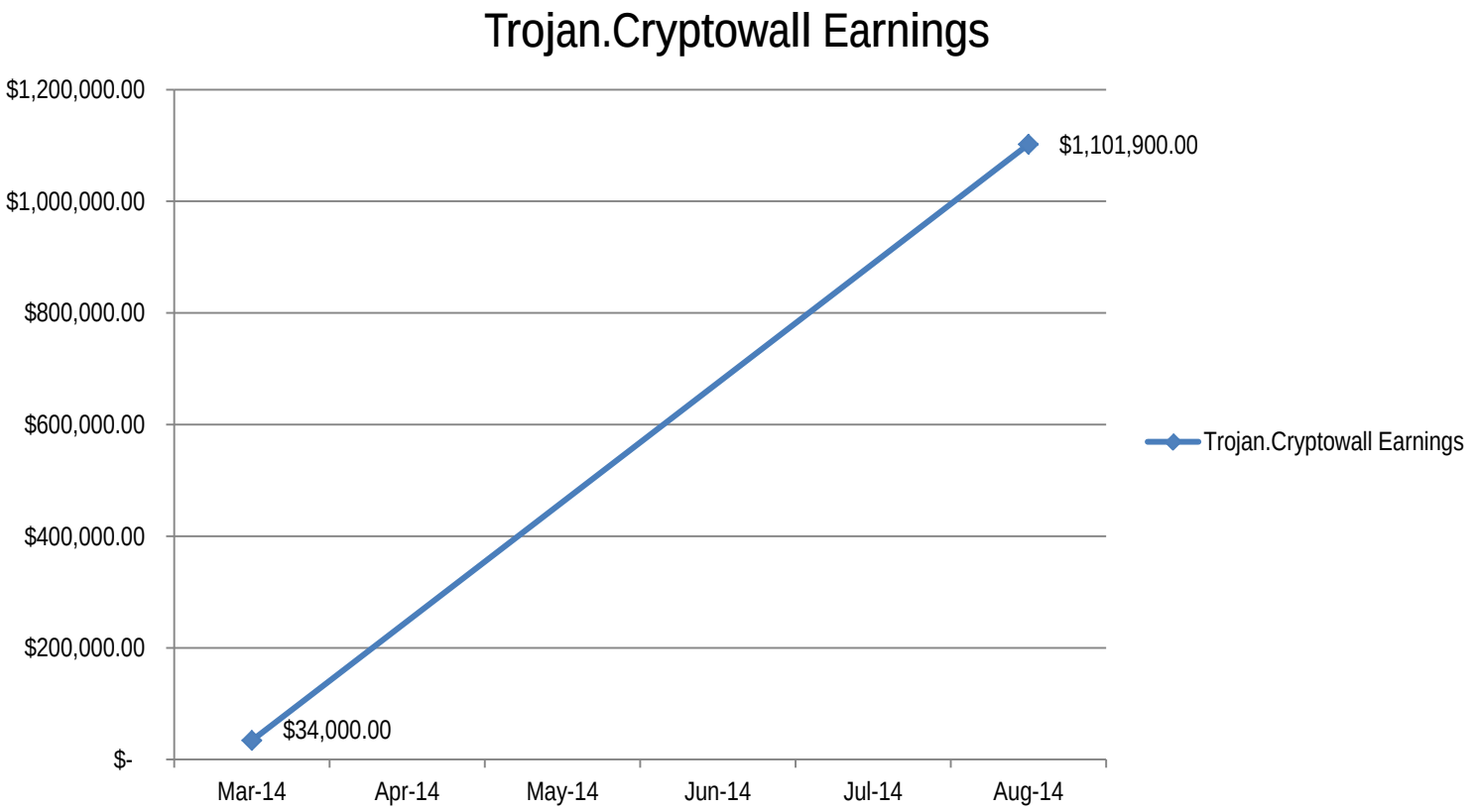
Crypto Ransomware

Locker Ransomware

CryptoLocker

CryptoWall

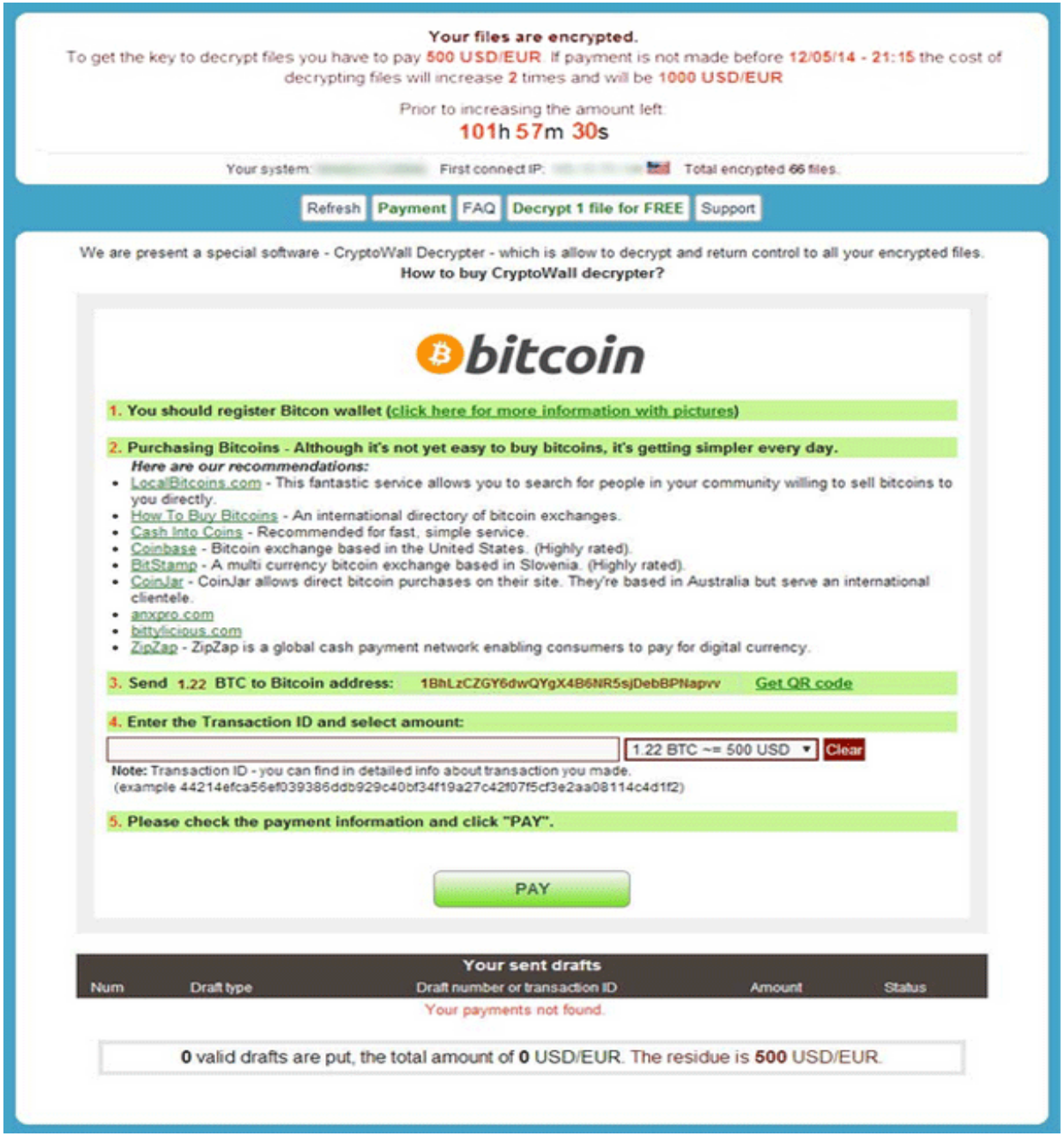
- "[CryptoWall is] the most current and significant ransomware threat targeting U.S. individuals and businesses." - FBI
- Includes all CryptoLocker capabilities



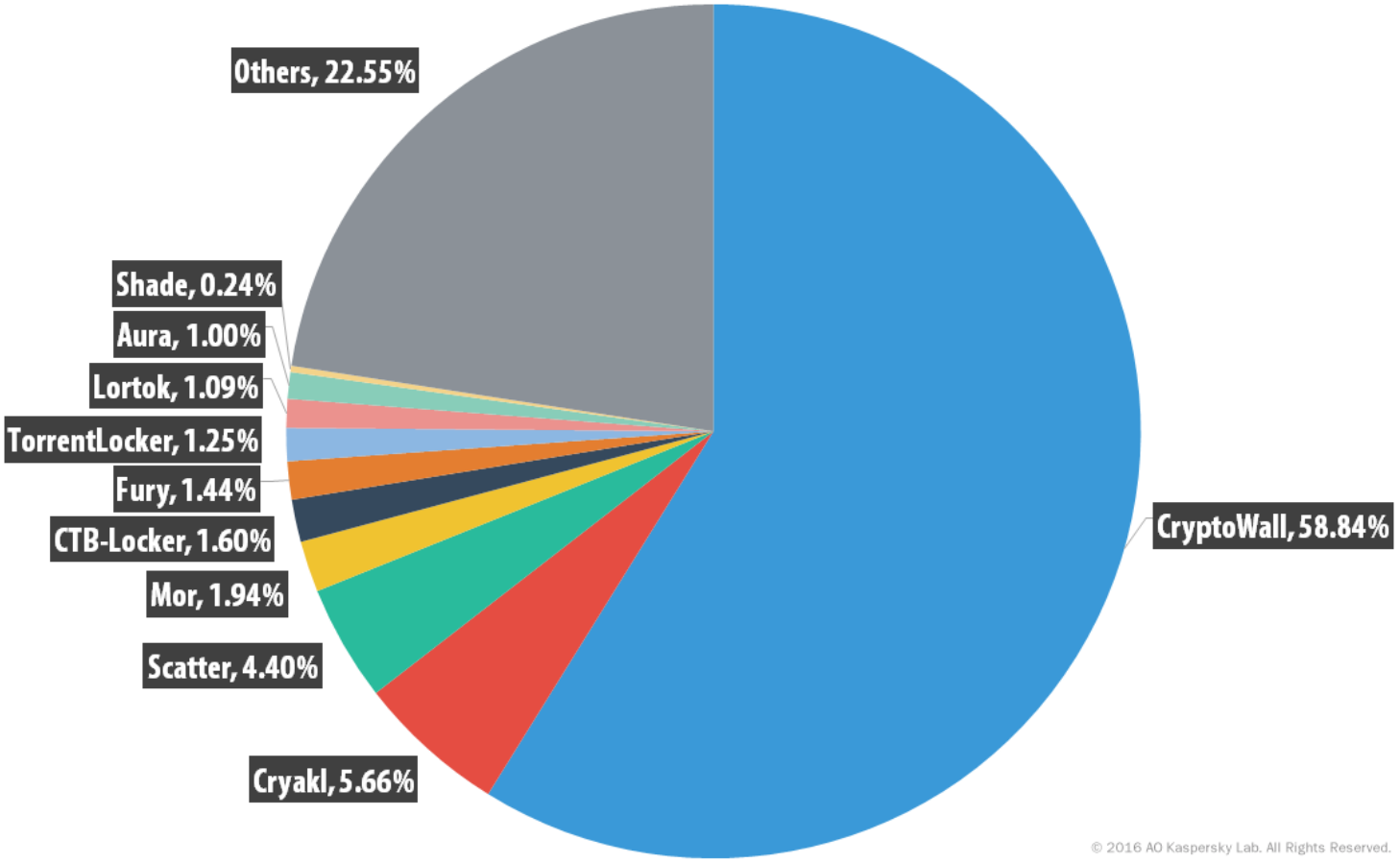
CryptoWall


CryptoLocker-v3
Your personal files are encrypted!
Your private key will be destroyed on:
3/5/2015
Your files have been safely encrypted on this PC: photos,videos, documents,etc. Click "Show encrypted files" Button to view a complete list of encrypted files, and you can personally verify this.
Encryption was produced using a unique public key RSA-2048 generated for this computer. To decrypt files you need to obtain the private key.
The only copy of the private key, which will allow you to decrypt your files, is located on a secret server in the Internet; the server will eliminate the key after a time period specified in this window.
Once this has been done, nobody will ever be able to restore files...
In order to decrypt the files open your personal page on site https://34r6hq26q2h4jkzj.tor2web.fi and follow the instruction.
Use your Bitcoin address to enter the site:
1K7Q5TrFxFqCZEmzocfxn8LfrxvdB39Uvm
Click to copy Bitcoin address to clipboard
if https://34r6hq26q2h4jkzj.tor2web.org is not opening, please follow the steps:
You must install this browser www.torproject.org/projects/torbrowser.html.en
After instalation,run the browser and enter address 34r6hq26q2h4jkzj.onion
Follow the instruction on the web-site. We remind you that the sooner you do, the more chances are left to recover the files.
Any attempt to remove or corrupt this software will result in immediate elimination of the private key by the server.
Show encrypted files
Check Payment
Enter Decrypt Key
Click to Free Decryption on site

CryptoWall


Your files are encrypted.
To get the key to decrypt files you have to pay 500 USD/EUR. If payment is not made before 12/05/14 - 21:15 the cost of decrypting files will increase 2 times and will be 1000 USD/EUR
Prior to increasing the amount left:
101h 57m 30s
Your system: First connect IP: Total encrypted 66 files.
Refresh
Payment
FAQ
Decrypt 1 file for FREE
Support
We are present a special software - CryptoWall Decrypter - which is allow to decrypt and return control to all your encrypted files.
How to buy CryptoWall decrypter?
bitcoin
1. You should register Bitcon wallet (click here for more information with pictures)
2. Purchasing Bitcoins - Although it's not yet easy to buy bitcoins, it's getting simpler every day.
Here are our recommendations:
LocalBitcoins.com - This fantastic service allows you to search for people in your community willing to sell bitcoins to you directly.
How To Buy Bitcoins - An international directory of bitcoin exchanges.
Cash Into Coins - Recommended for fast, simple service.
Coinbase - Bitcoin exchange based in the United States. (Highly rated).
BitStamp - A multi currency bitcoin exchange based in Slovenia. (Highly rated).
CoinJar - CoinJar allows direct bitcoin purchases on their site. They're based in Australia but serve an international clientele.
anxpro.com
bittylicious.com
ZipZap - ZipZap is a global cash payment network enabling consumers to pay for digital currency.
3. Send 1.22 BTC to Bitcoin address: 1BhLzCZGY6dwQYgX4B6NR5sjDebBPNapvv Get QR code
4. Enter the Transaction ID and select amount:
1.22 BTC ~= 500 USD
Clear
Note: Transaction ID - you can find in detailed info about transaction you made.
(example 44214efca56ef039386ddb929c40bf34f19a27c42f07f5cf3e2aa08114c4d1f2)
5. Please check the payment information and click "PAY".
PAY
Your sent drafts
Num
Draft type
Draft number or transaction ID
Amount
Status
Your payments not found.
0 valid drafts are put, the total amount of 0 USD/EUR. The residue is 500 USD/EUR.

Ransomware Distribution 2014-2015



Kaspersky Labs – KSN Report

Ransomware Costs

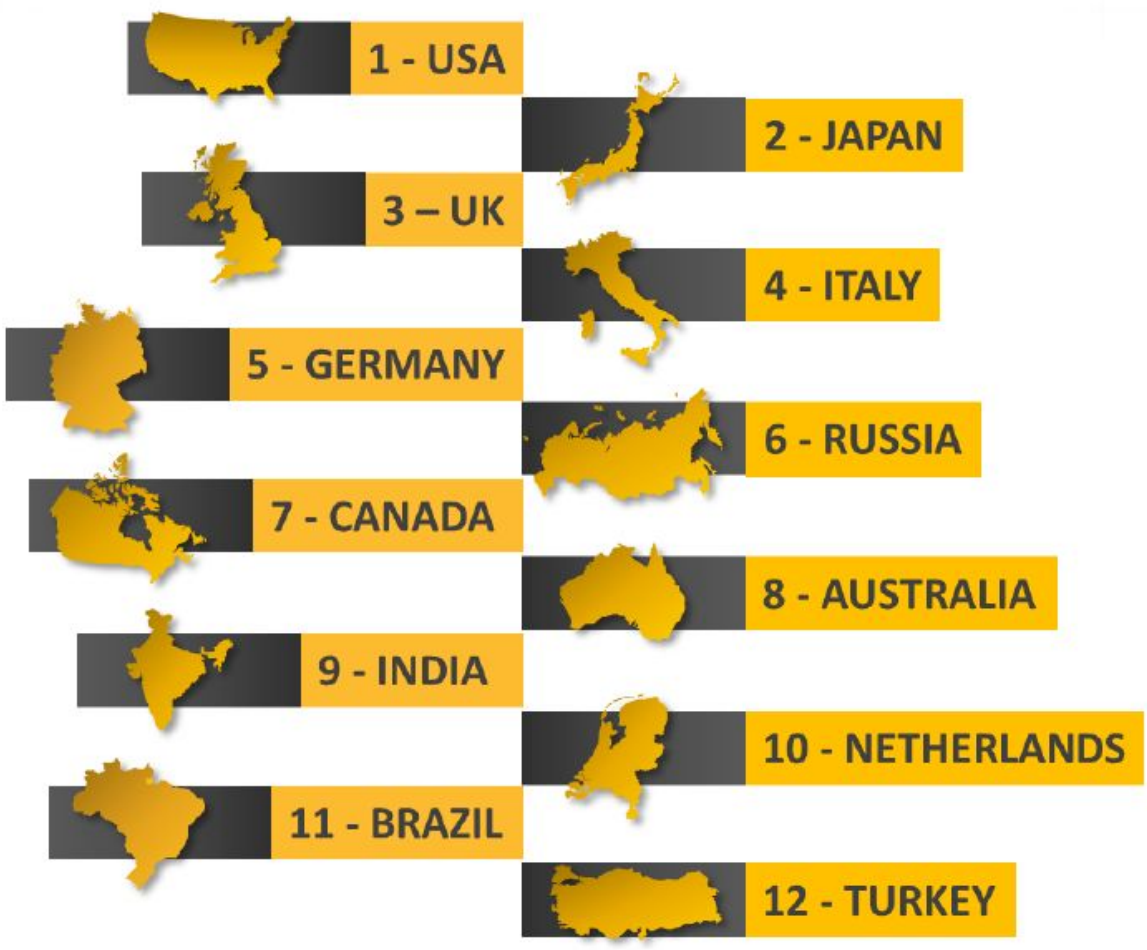
- FBI June 2015 alert stated the ransom fee range is $200 - $10,000
- 992+ CryptoWall-related complaints reported to the FBI April 2014 - June 2015 resulting in $18 million+ in losses
- The US Computer Emergency Readiness Team (US-CERT) does not support ransom payments
  - US CERT recommends prevention efforts, including business continuity plans
  - Report instances of fraud to the FBI at the Internet Crime Complaint Center or contact the CCIRC.
    - The FBI may recommend payment if no other solutions are possible

Payment

The popular payment method for ransomware is bitcoins.

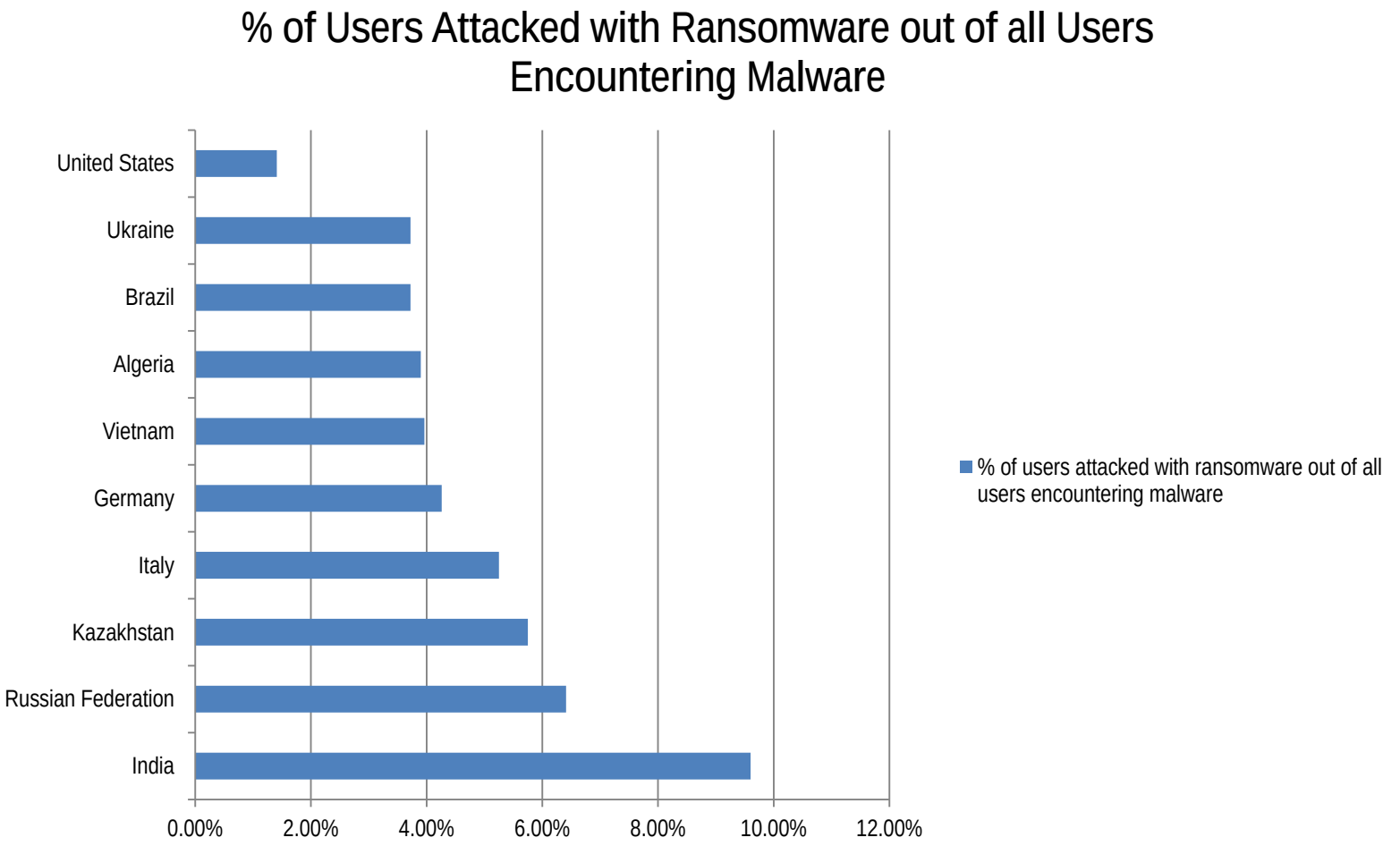
- Bitcoin is a form of “cryptocurrency,” involving completely digital fund transfers with user identity privacy
- It is powered by its users with no central authority or financial institutions
- Software program where currency is stored as credits and fund transfers are facilitated via user private keys
- Other options include payment voucher systems e.g., MoneyPak & UKash.

Ransomware Attacks by Country: 2014 – 2015



Symantec 2015 – The Evolution of Ransomware

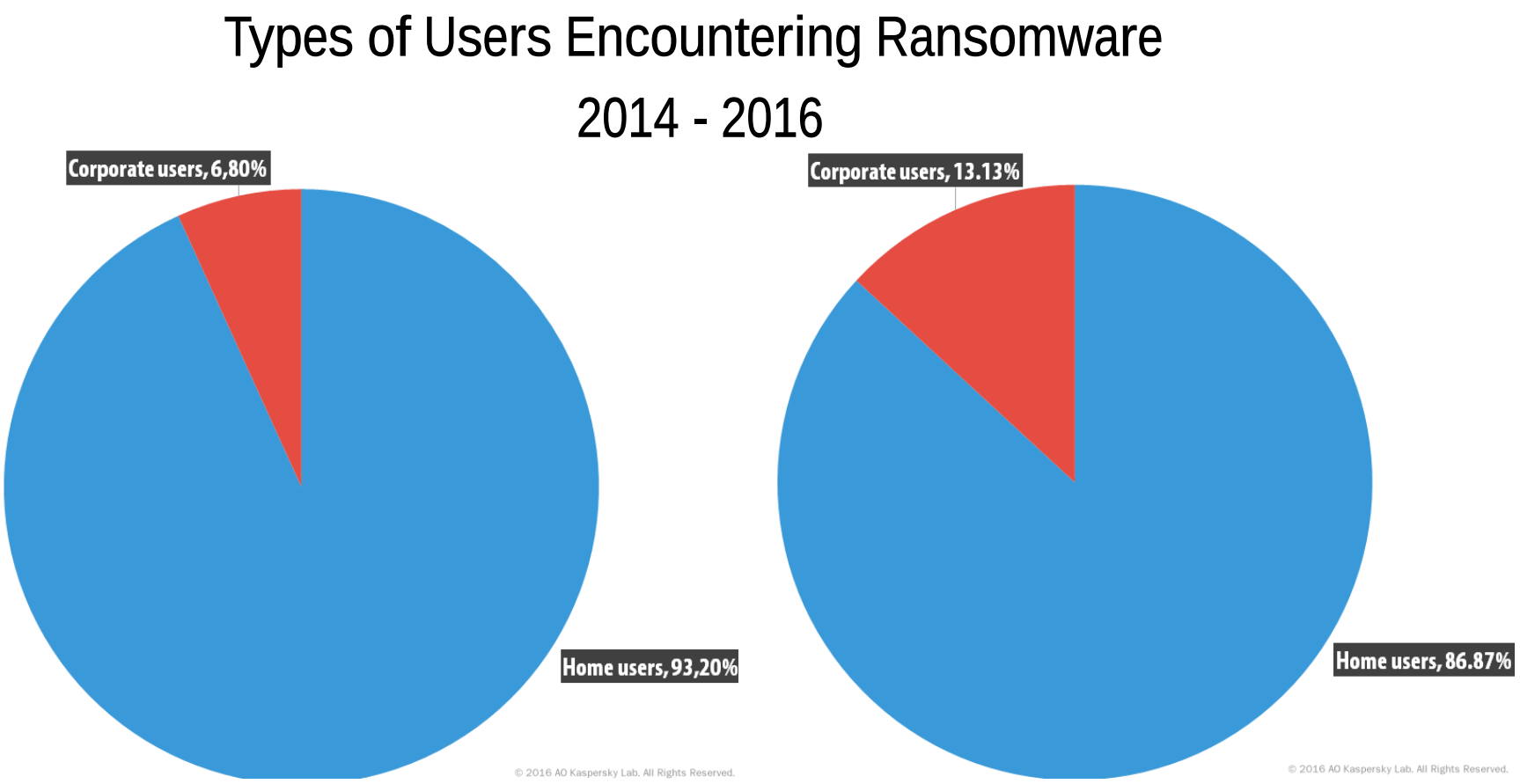
Ransomware Attacks by Country: 2015 – 2016



Countries with the biggest share of users attacked with ransomware 2015-2016, Kaspersky Labs – KSN Report

Potential Targets

Targets include: Home Users, Businesses, & Public Institutions.



Type of users encountering ransomware in 2014-2016, Kaspersky Labs – KSN Report

Case Study – Police Department

Tewksbury Police Department	
Location & Date	Tewksbury, Massachusetts, US December 2014
Ransomware Type	CryptoLocker
Ransom	$500 US (.77 Bitcoin)
Analysis	• The most recent backup was 18 months old • Most recent backup on an external hard drive was also corrupted • Two private security firms were unable to decipher the encryption
Response & Result	Paid ransom & regained access
Impact	Delayed operations

Case Study – Medical Institution

Hollywood Presbyterian Medical Center	
Location & Date	Los Angeles, California, US February 2016
Ransomware Type	CryptoLocker
Ransom	$17,000 U.S. (40 Bitcoins)
Analysis	• Inaccessible patient and related data • Potential operational setbacks and diminished patient care
Response & Result	Paid ransom & regained access
Impact	• Business operations resorted to manual processes • Service delivery delays

Case Study – Medical Institution

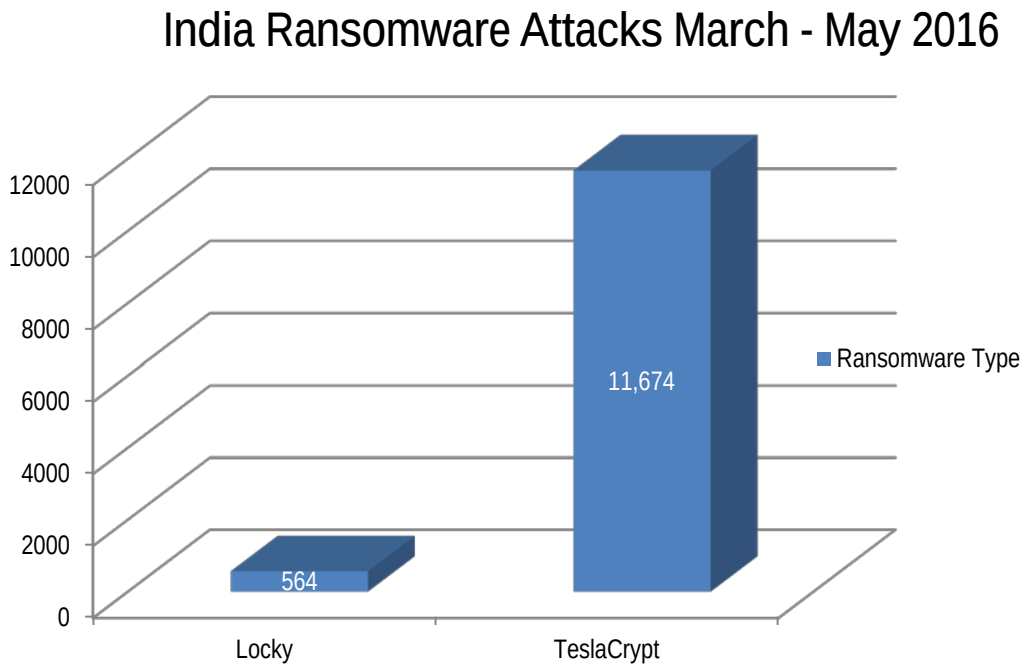
MedStar Health	
Location & Date	Washington DC Metropolitan Area March 2016
Ransomware Type	CryptoLocker
Ransom	$19,000 US (45 Bitcoins)
Analysis	TBD – Investigation on-going
Response & Result	TBD – Investigation on-going
Impact	• Business operations resorted to manual processes • Cancelled appointments & treatments • Inappropriate care due to unavailable data

Case Study – Educational Institution

Horry County School District	
Location & Date	Conway, South Carolina, US February 2016
Ransomware Type	CryptoLocker
Ransom	$10,000 (15 Bitcoin)
Analysis	• Breach may have occurred in an older server containing outdated applications • Remained locked out of 25 servers despite backup recovery efforts
Response & Result	Paid ransom & regained access
Impact	• Servers were shut down and disrupted online services to prevent further damage • Hours lost on recovery and alternative solution analysis

Forecast & Trends

- Financial Institutions - Locky Ransomware
- Public Sector Infrastructure & Organizations
- India Incidents - Locky & TeslaCrypt Ransomware
  - 3 Financial Institutions & 1 Pharmaceutical Co. via LeChiffre
  - LeChiffre needs to be run manually on the compromised system



Advantages & Disadvantages of Ransom Payment

Pay Ransom	Forego Payment
Pros: • Ransom amount could be affordable or a relatively nominal value • Timely restoration of access / data • Minimized adverse publicity	Pros: • No financial losses • Potential alternative recovery solutions could restore partial access / data • Discourages attackers from continuing such attacks
Cons: • No guarantee for access / data to be restored • Offers an incentive to continue such attacks	Cons: • Data could be lost and access could be withheld indefinitely • Business operation disruptions • Reputational harm • Unsuccessful recovery efforts

Prevention & Mitigation Measures

Contingency Planning

- ✓ Conduct frequent backups
- ✓ Periodically restore backups
- ✓ Develop a business continuity / contingency plan and test it periodically

Security Management & Access Control

- ✓ Use a defense-in-depth approach
- ✓ Maintain awareness of evolving ransomware characteristics and similar attacks
- ✓ Review and restrict access to public file sharing spaces e.g., shared drives
- ✓ Practice consistent cyber hygiene

Prevention & Mitigation Measures (continued)

Patch Management

- ✓ Maintain current antivirus software and system patches

Security Awareness & Training (SAT)

- ✓ Conduct Security Awareness Training periodically
- ✓ Exercise caution when opening links from email, websites, or social media
- ✓ Communicate IT security tips and refreshers year-round

Summary

- Any industry, organization or individual could become a target
- Ransomware attacks will continue to be profitable & prevalent
- Security Awareness & Training Programs are crucial
  - Maintain awareness of trends and developments
- Preventive measures should be taken before resorting to payment
  - Implement business continuity and data recovery measures

Aronson Technology Risk Services Group

Cyber Security Services

- Security Strategy
- Security Assessments & Remediation
- Security Architecture
- Security Awareness & Training
- Business Continuity Planning
- Vulnerability Assessments

Presenter Contact Information

Payal Vadhani

pvadhani@aronsonllc.com

Direct Line: 301.231.6259

Natasha Barnes

nbarnes@aronsonllc.com

Direct Line: 301.231.6236