



# RANSOMWARE EVOLUTION AND THE CURRENT LANDSCAPE

BY QIYANG CHEN, ERIC LIN

# WHAT IS RANSOMWARE

- Crypto ransomware
- Locker ransomware



# THE HISTORY OF RANSOMWARE

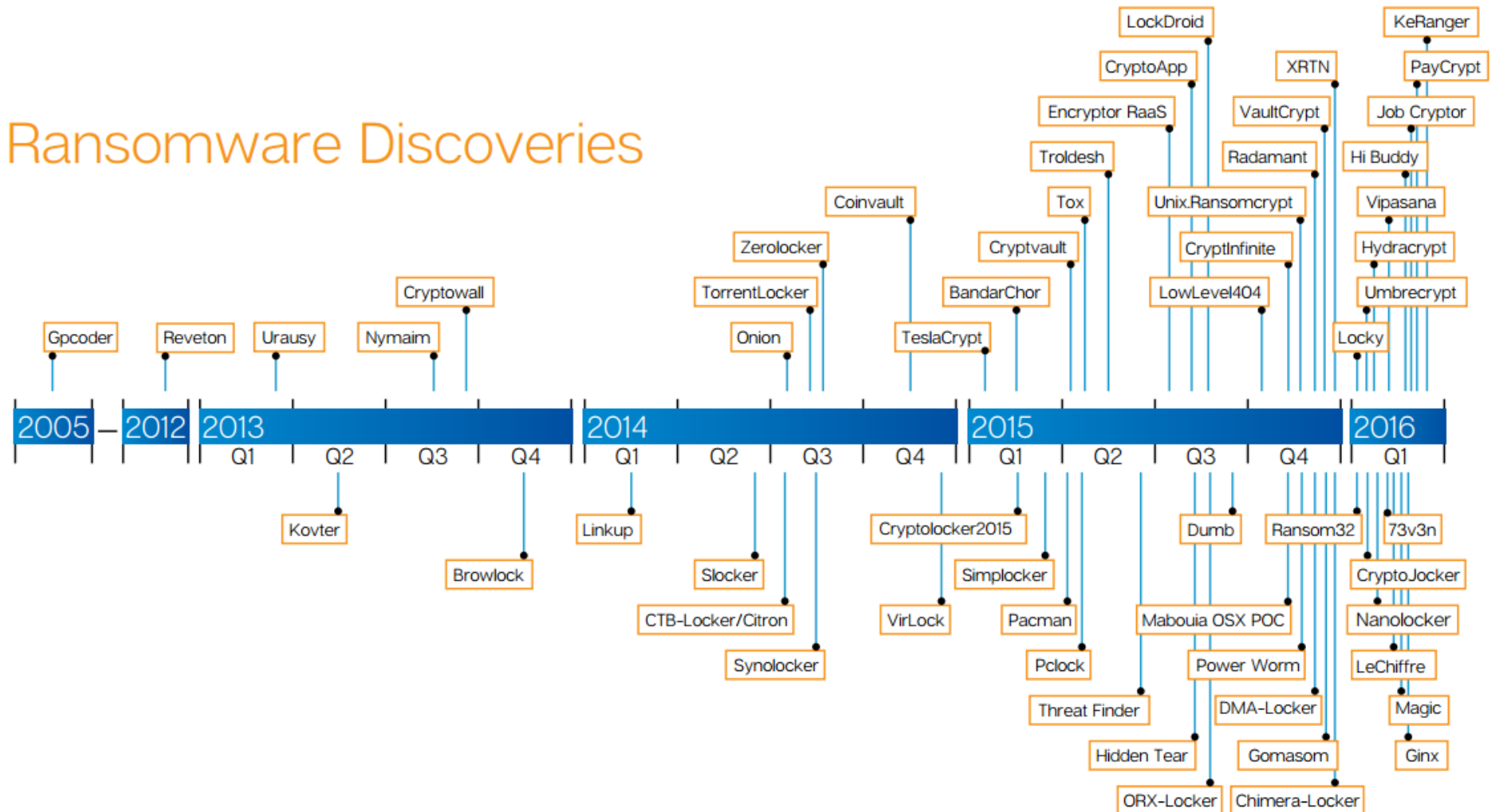
- Cases of ransomware infection were first seen in Russia between 2005 – 2006
- Ransomware Spreads Outside Russia (across Europe and North America 2012)
- The Rise of Reveton and Police Ransomware (2012)
- The Evolution to CryptoLocker and Crypto-ransomware (2013)
- The Foray into Cryptocurrency Theft: BitCrypt (2014)

# THE HISTORY OF RANSOMWARE (CONTINUED)

- The Angler Exploit Kit (2015): popular exploit kits used to spread ransomware
- POSHCODER: PowerShell Abuse
- Ransomware Infects Critical Files
- Ransomware Evolved: Modern Ransomware

# THE HISTORY OF RANSOMWARE (TIMELINE)

## Ransomware Discoveries



# HOW RANSOMWARE WORKS

1. TARGETING
2. PROPAGATION
3. EXPLOIT
4. INFECTION
5. EXECUTION

# How Ransomware Works?

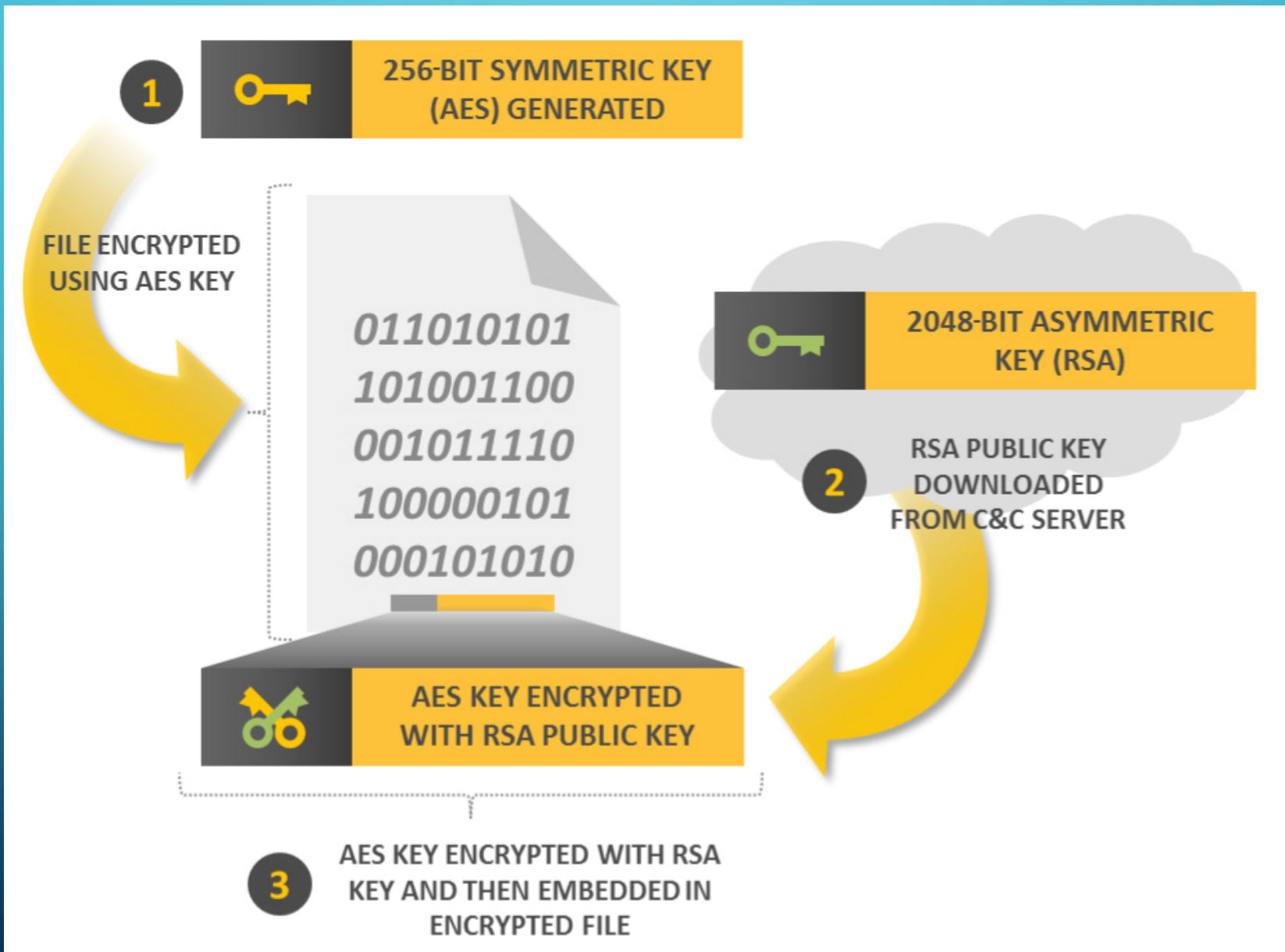


# RANSOM TECHNIQUES

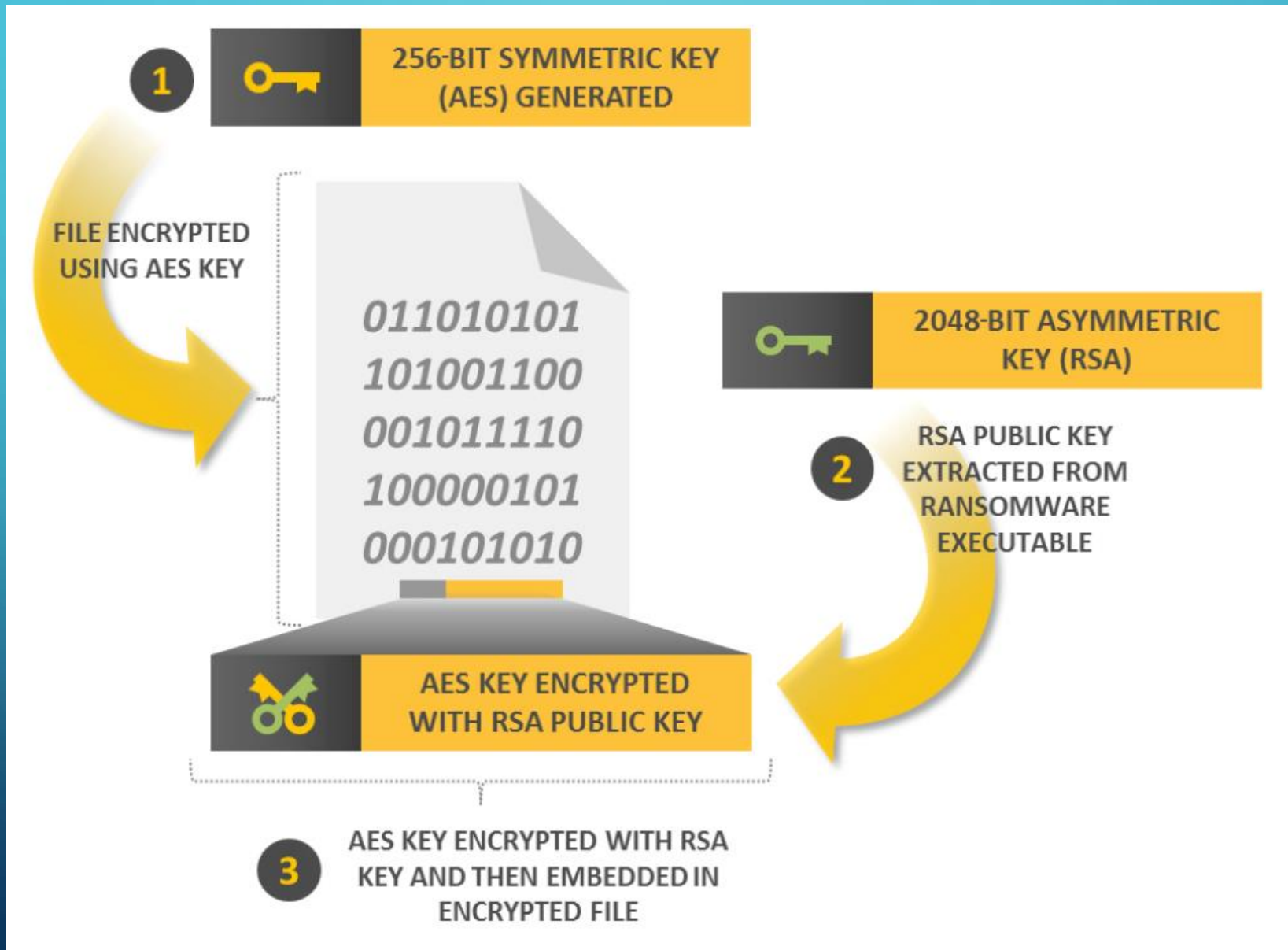
- File encryption: Downloaded public key, Embedded public key and Embedded symmetric key
- Screen locking: Windows locker ransomware, Browser locking and Android locker ransomware



# DOWNLOADED PUBLIC KEY



# EMBEDDED PUBLIC KEY



# WINDOWS LOCKER RANSOMWARE

THE **FBI** FEDERAL BUREAU OF INVESTIGATION  
CYBER DEPARTMENT



**All activities of this computer have been recorded**

**All your files are encrypted. Don't try to unlock your computer!**

Your browser has been blocked due to at least one of the reasons specified below.

**You have been subjected to violation of Copyright and Related Rights Law (Video, Music, Software) and illegally using or distributing copyrighted contents**, thus infringing Article 1, Section 8, Clause 8, also known as the Copyright of the Criminal Code of United States of America. Article 1, Section 8, Cause 8 of the Criminal Code provides for a fine of two to five hundred minimal wages or a deprivation of liberty for two to eight years.

**You have been viewing or distributing prohibited Pornographic content** (Child Porno photos and etc were found on your computer). Thus violating article 202 of the Criminal Code of United States of America, Article 202 of the Criminal Code provides for a deprivation of liberty for four to twelve years.

**Illegal access has been initiated from your PC without your knowledge or consent, your PC may be infected by malware**, thus you are violating the law on Neglectful Use of Personal Computer. Article 210 of the Criminal Code provides for a fine of up to \$100,000 and/or deprivation of liberty for four to nine years. Pursuant to the amendment to Criminal Code of United States of America of May 28, 2011, this law infringement (if it is not repeated - first time) may be considered as conditional in case you pay the fine of the States.

**To unlock your computer and avoid other legal consequences, you are obligated to pay a release fee of \$300, payable through GreenDot MoneyPak (you have to purchase MoneyPak card, load it with \$300 and enter the code). You can buy the code at any shop or gas station. MoneyPak is available at the stores nationwide.**

#### How do I pay the fine to unlock my PC?

1. Find a retail location of MoneyPak near to you:



- Pick up the MoneyPak at prepaid selection and load it with cash at the register.  
*A service fee of up to \$4.95 will apply*
- Enter your MoneyPak code and submit "UNLOCK YOUR PC NOW"



Your IP: 254.43

Location: Atlanta,  
Georgia, United States

green dot MoneyPak SECURE PAYMENT FORM

Enter the MoneyPak code

Please enter MoneyPak code  
using pin pad below.

1 2 3 4 5 6 7 8 9 0 Clear

**UNLOCK YOUR PC NOW!**

Your browser will be unblocked within 3-12 hours after the money is put into the State's account.

**Please note:** Fine must be paid within 12 hours. As soon as 12 hours elapse, the possibility to pay the fine expires. All PC data will be detained and criminal procedures will be initiated against you if the fine is not paid.

# BROWSER LOCKING

```
▼ <html xmlns="http://www.w3.org/1999/xhtml">
  ▶ <head>...</head>
  ▼ <body onkeypress="return catchControlKeys(event);">
    ▼ <iframe class="frame" width="0" height="0" src="us/close.html">
      ▼ #document
        ▼ <html>
          ▶ <head>...</head>
          ▼ <body style="margin:0px;padding:0px;width:100%;height:100%;">
            ▼ <script type="text/javascript">
              window.onbeforeunload = function(env){
                var str = 'YOUR BROWSER HAS BEEN LOCKED.\n\nALL PC DATA WILL BE D
                alert(str);
                return str;
              }
            </script>
          </body>
        </html>
      </iframe>
    ▼ <iframe class="frame" width="0" height="0" src="us/close.html">
      ▼ #document
        ▼ <html>
          ▶ <head>...</head>
          ▼ <body style="margin:0px;padding:0px;width:100%;height:100%;">
            ▼ <script type="text/javascript">
              window.onbeforeunload = function(env){
                var str = 'YOUR BROWSER HAS BEEN LOCKED.\n\nALL PC DATA WILL BE D
                alert(str);
                return str;
              }
            </script>
          </body>
        </html>
      </iframe>
    ▶ <iframe class="frame" width="0" height="0" src="us/close.html">...</iframe>
    ▶ <iframe class="frame" width="0" height="0" src="us/close.html">...</iframe>
    ▶ <iframe class="frame" width="0" height="0" src="us/close.html">...</iframe>
    ▶ <iframe class="frame" width="0" height="0" src="us/close.html">...</iframe>
```

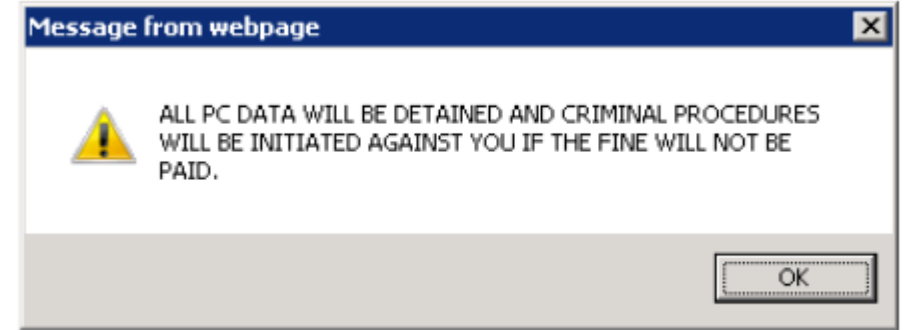


Figure 22. First Browlock dialog box

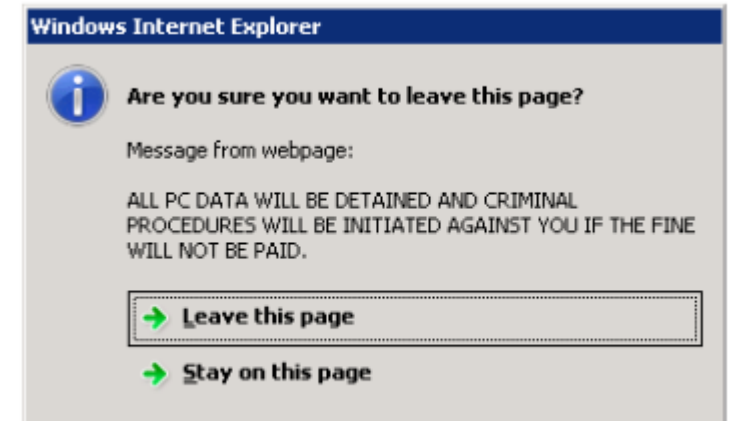


Figure 23. Second Browlock dialog box

# HOW WIDESPREAD IS THE PROBLEM OF RANSOMWARE?

- Top 12 countries impacted by ransomware

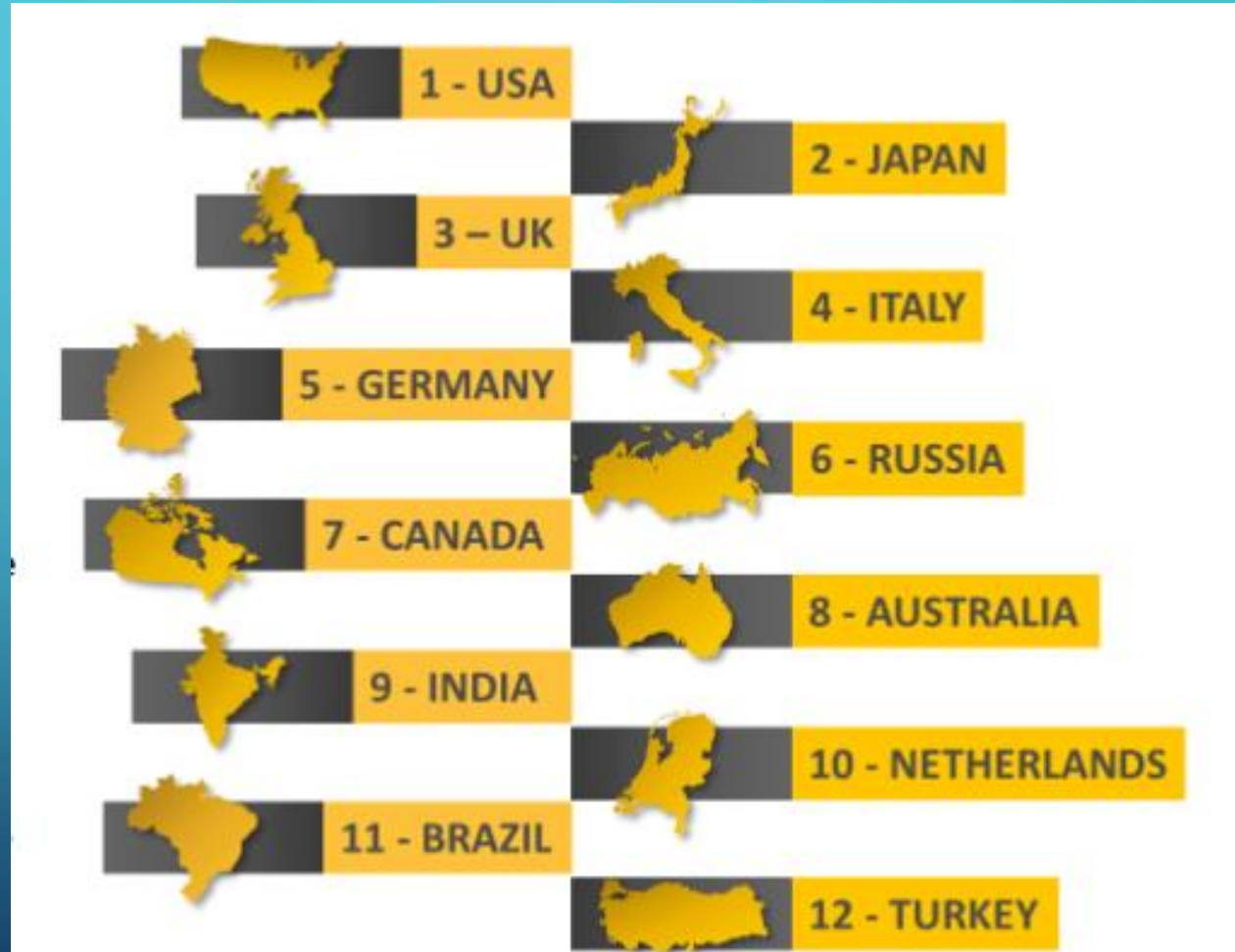
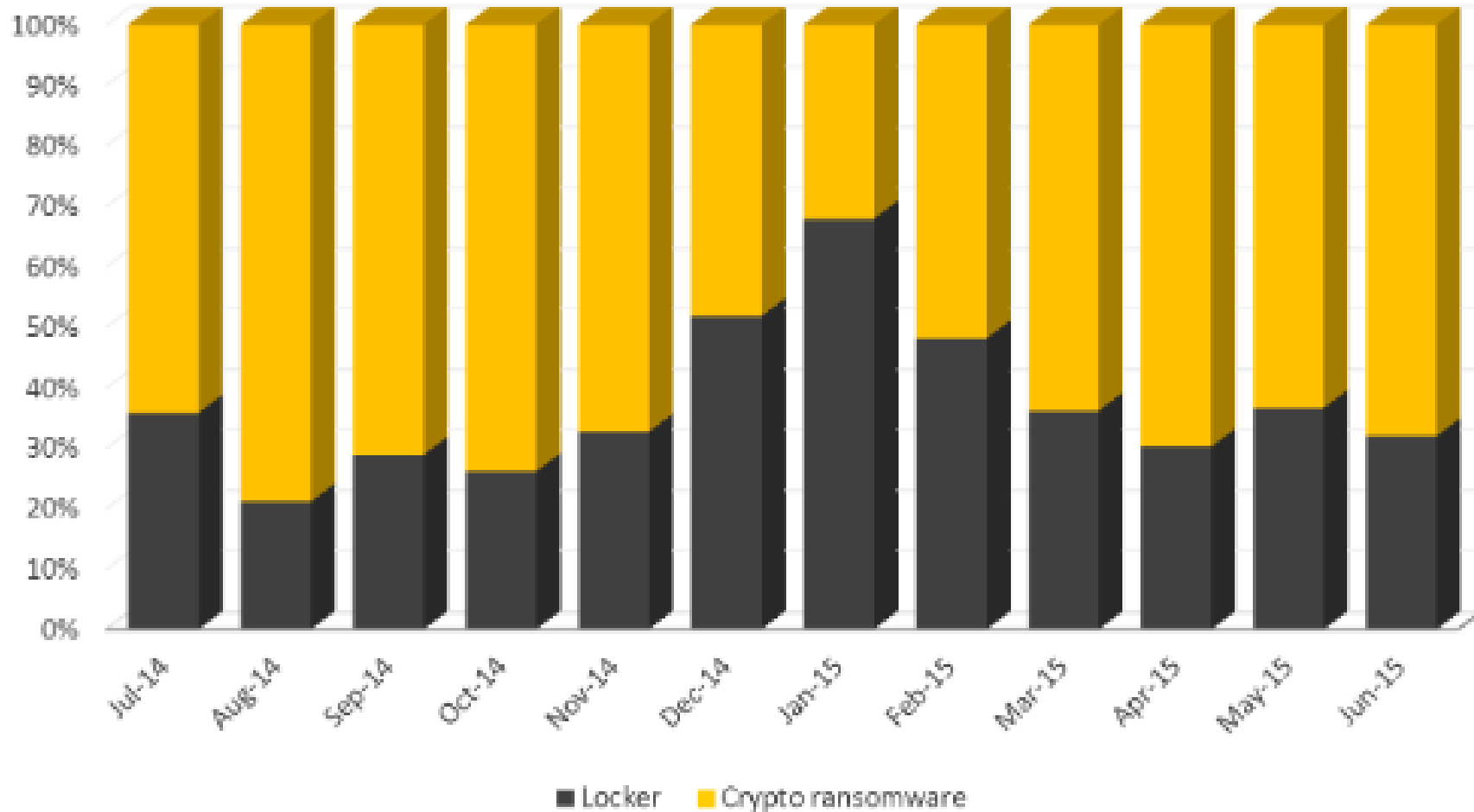


Figure 25. Top countries impacted by binary-based ransomware

- The Ransomware Mix



**Figure 26. Detections for binary-based crypto ransomware dominate the ransomware threat landscape for past 12 months.**

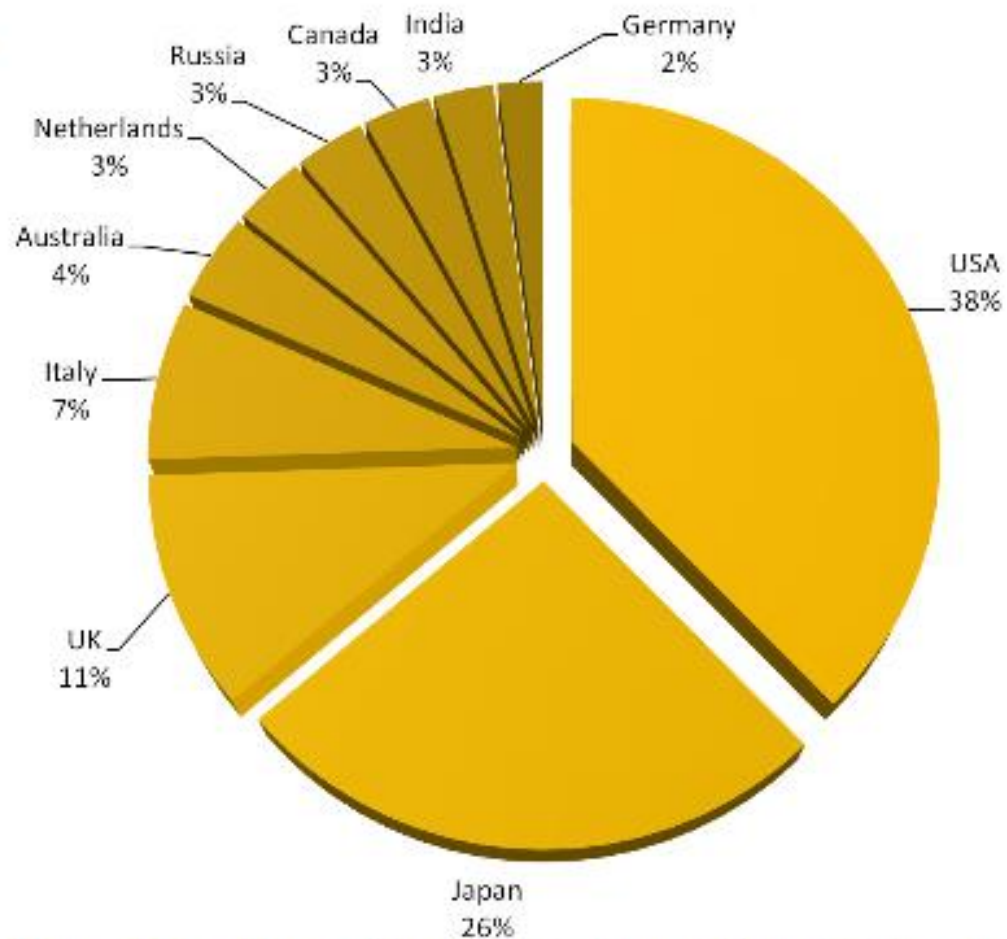


Figure 27. Top 10 countries for detections of binary file based crypto ransomware

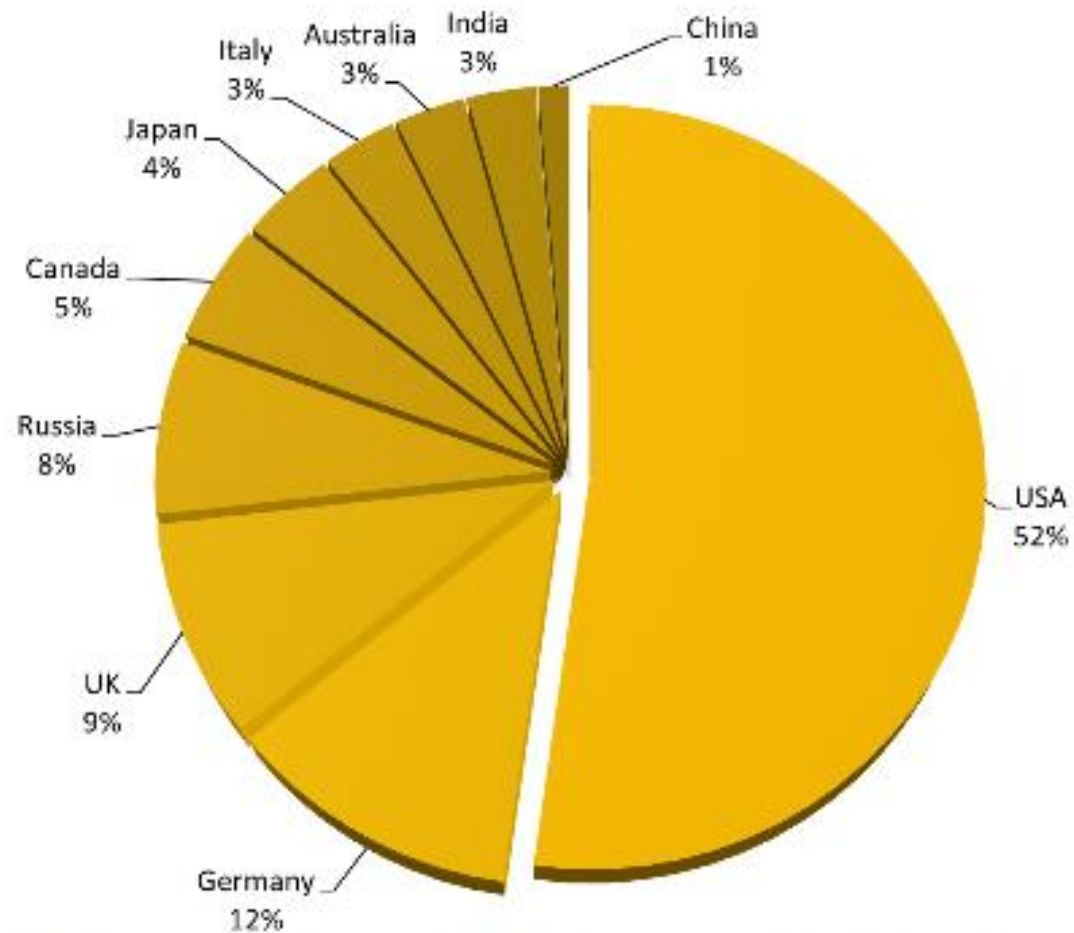


Figure 28. Top countries for detections of binary-based locker ransomware

# RANSOMWARE DEFENSE, PREVENTION, AND REMOVAL

- Using anti-ransomware tools
- Avoid unknown websites
- Avoid opening unverified emails





THANK YOU

# QUESTIONS

- Q1. What's a simple way to protect your data in case hackers successfully encrypt your files?
- A) Install antivirus software
- **B) Back up your data**
- C) Password protect your files
- D) Disable macro scripts in Microsoft Word

# QUESTIONS

- Q2. New types of ransomware developed last year helped make attacks more effective. What's the latest advance in how ransomware works?
- A) Locks users out of their files with an industry-grade encryption algorithm
- B) Sets up your computer to send viruses to other users
- C) Corrupts your hard drive, rendering it useless
- D) Defaces your personal website and social media profiles

# QUESTIONS

- Q3. What's the most common way that users get infected with ransomware?
- A) Phishing emails and malicious websites
- B) Fake two-factor authentication messages
- C) Infected USB drives
- D) Malicious computer hardware

# REFERENCE

- [http://www.symantec.com/content/en/us/enterprise/media/security\\_response/whitepapers/the-evolution-of-ransomware.pdf](http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-evolution-of-ransomware.pdf)
- <http://integranetworks.com/wp-content/uploads/2016/07/Integra-Networks-Ransomware-White-Paper.pdf>
- <https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/iSight-Ransomware-Threat-Landscape-Overview.pdf>
- <https://www.sans.org/reading-room/whitepapers/incident/enterprise-survival-guide-ransomware-attacks-36962>
- <https://en.wikipedia.org/wiki/Ransomware>
- <http://www.wikihow.com/Get-Rid-of-Ransomware>
- <https://www.welivesecurity.com/2013/12/12/11-things-you-can-do-to-protect-against-ransomware-including-cryptolocker/>
- <https://www.trendmicro.com/vinfo/us/security/definition/Ransomware>
- <https://community.sophos.com/kb/en-us/120797>
- <https://www.theatlantic.com/business/archive/2016/09/ransomware-us/498602/>
- <http://www.pcmag.com/news/343547/the-growing-threat-of-ransomware>