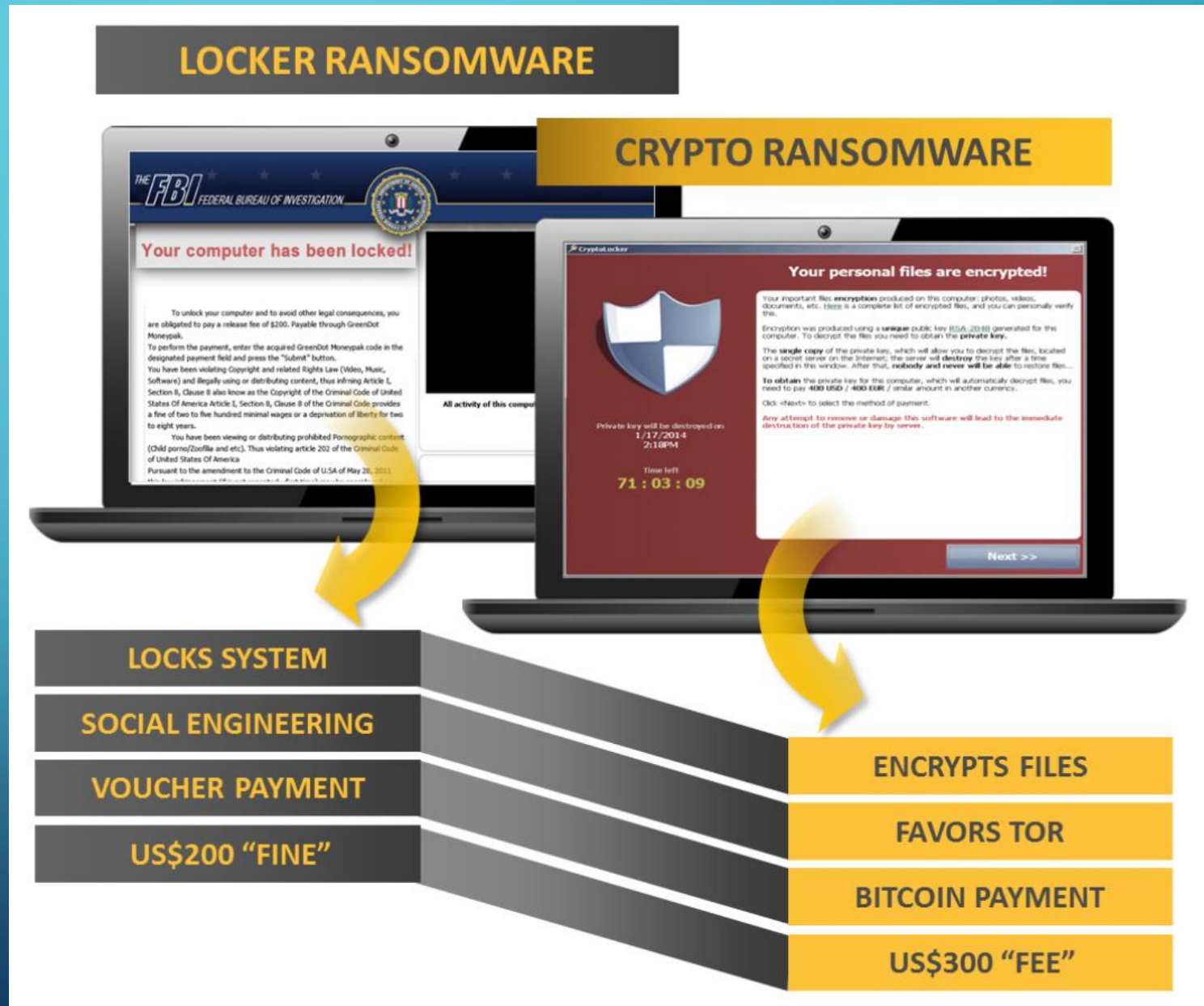
# RANSOMWARE EVOLUTION AND THE CURRENT LANDSCAPE

BY QIYANG CHEN, ERIC LIN

# WHAT IS RANSOMWARE

- Crypto ransomware
- Locker ransomware



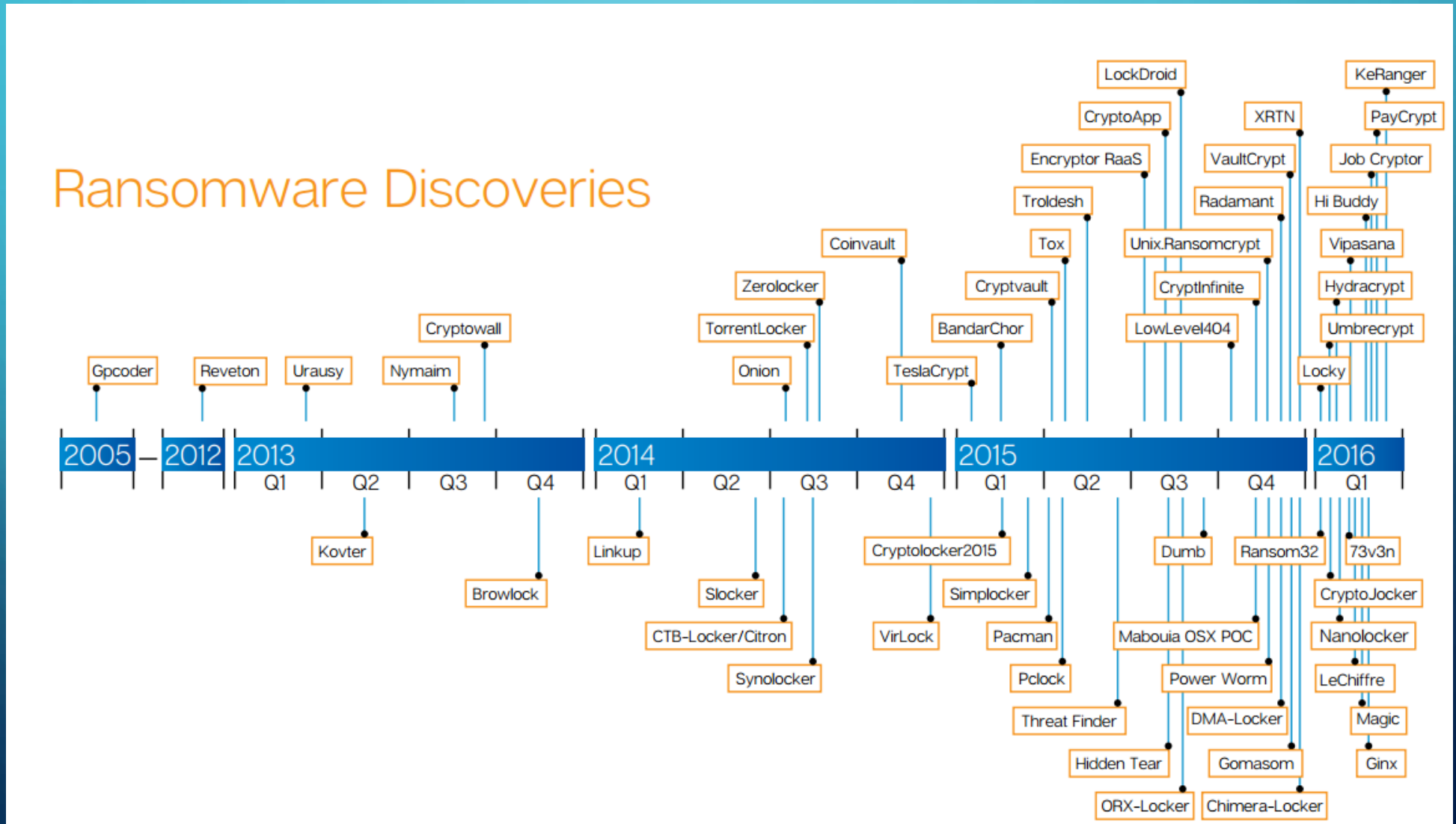
# THE HISTORY OF RANSOMWARE

- 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)



# HOW RANSOMWARE WORKS

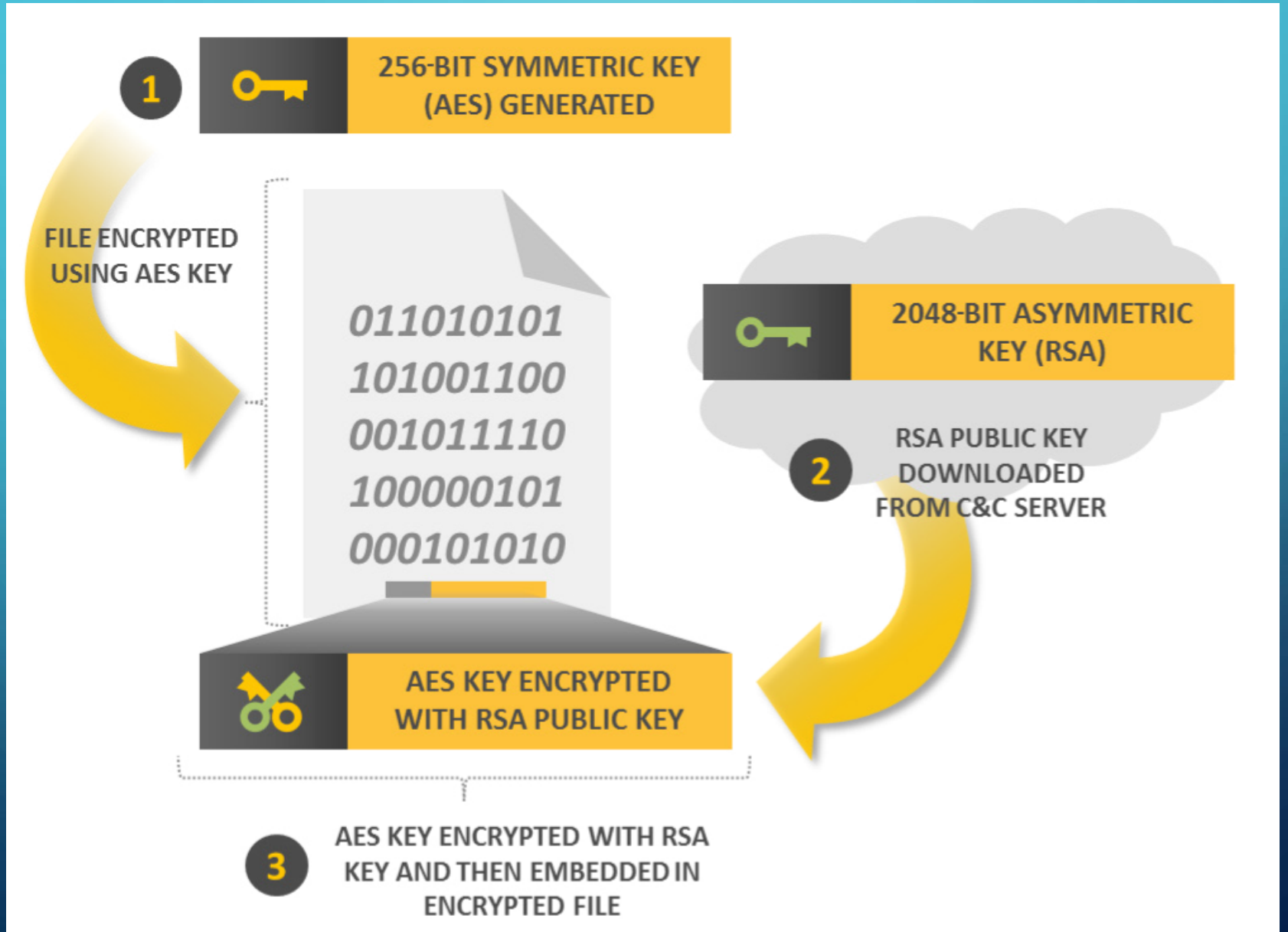
1. TARGETING
2. PROPAGATION
3. EXPLOIT
4. INFECTION
5. EXECUTION

# How Ransomware Works?

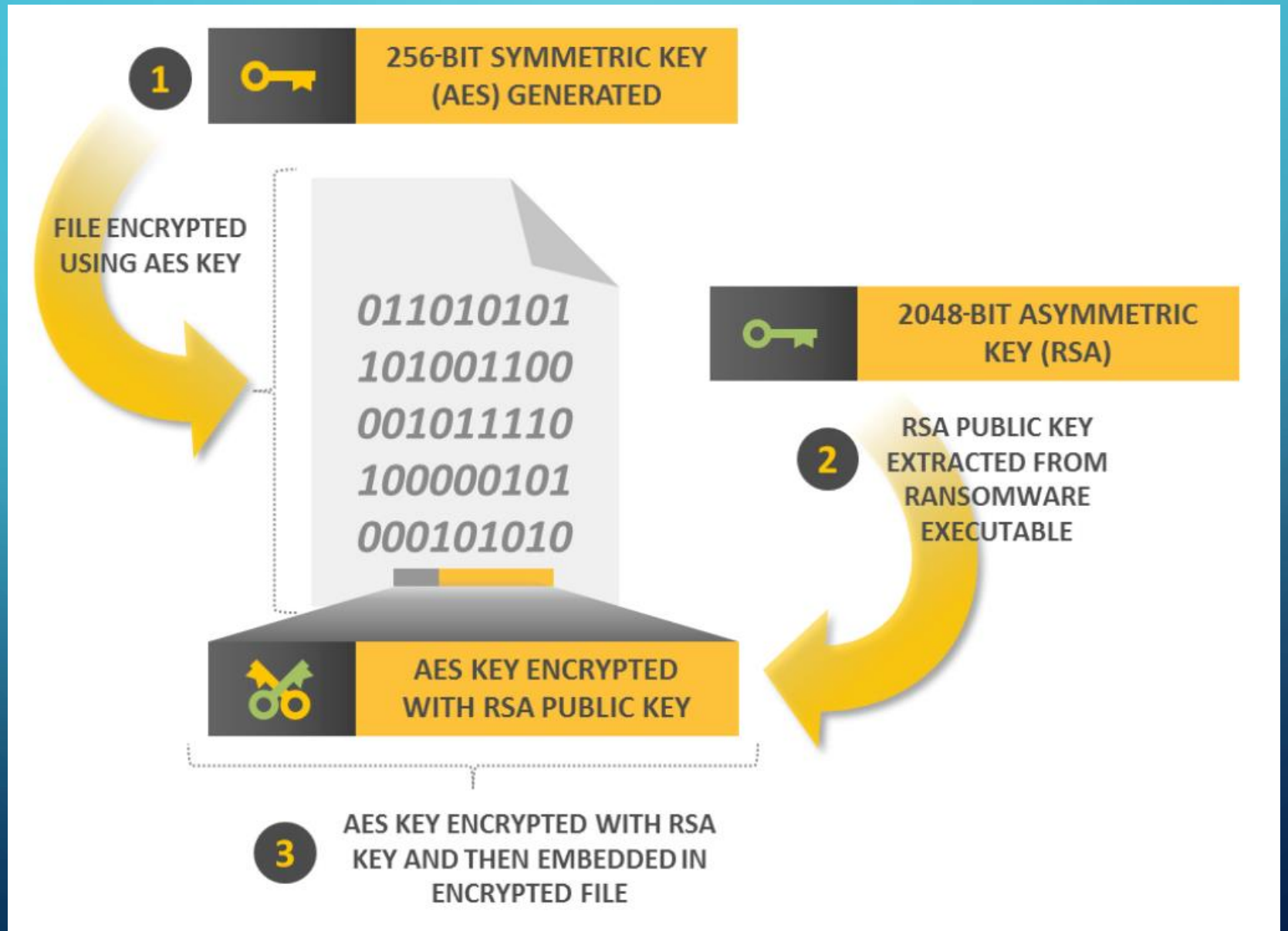
# RANSOM TECHNIQUES

- 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

# 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>
```

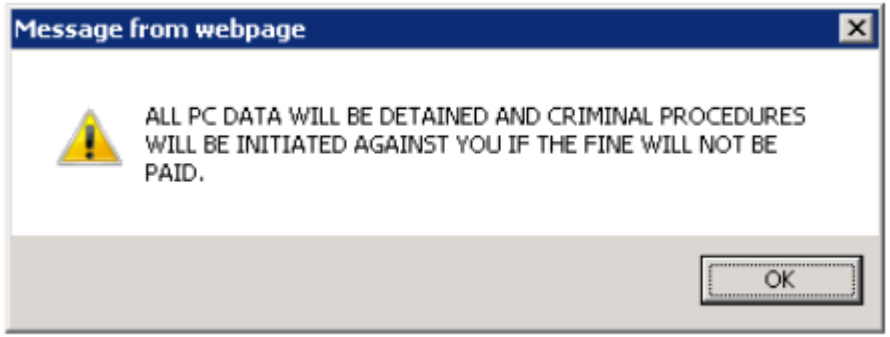



*Figure 22. First Browlock dialog box*

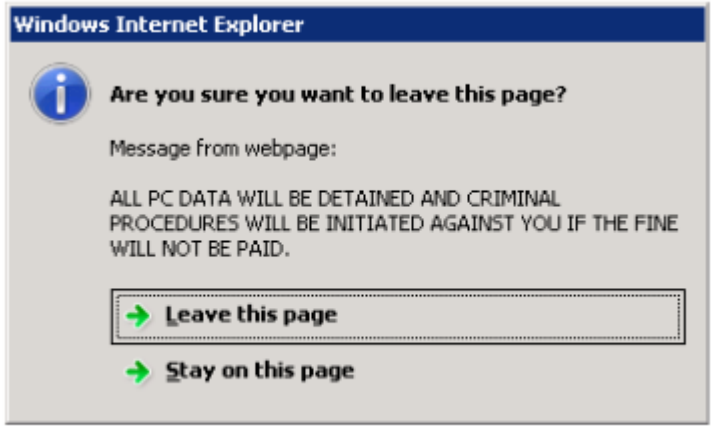



*Figure 23. Second Browlock dialog box*

# HOW WIDESPREAD IS THE PROBLEM OF RANSOMWARE?

- Top 12 countries impacted by ransomware

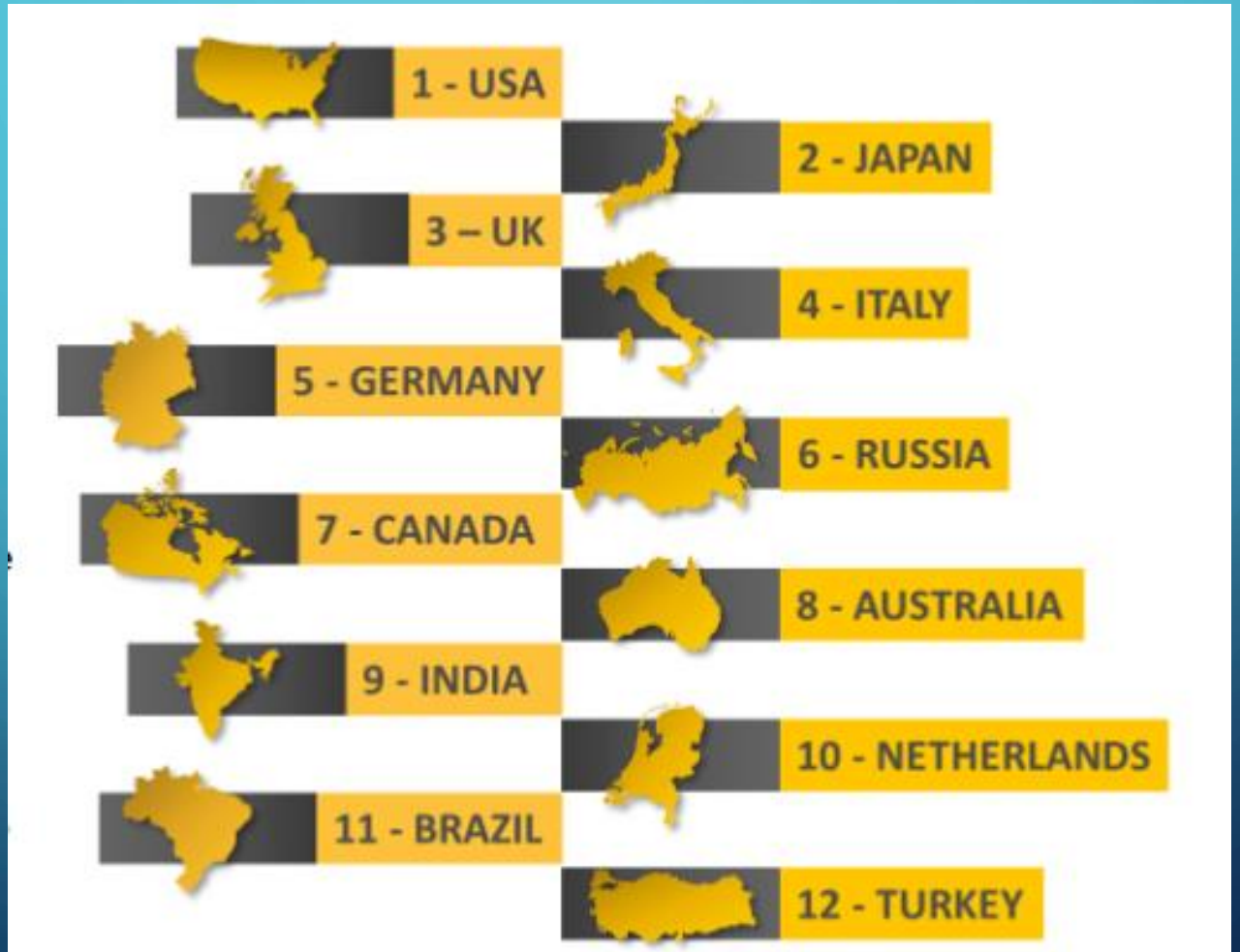



*Figure 25. Top countries impacted by binary-based ransomware*

- The Ransomware Mix

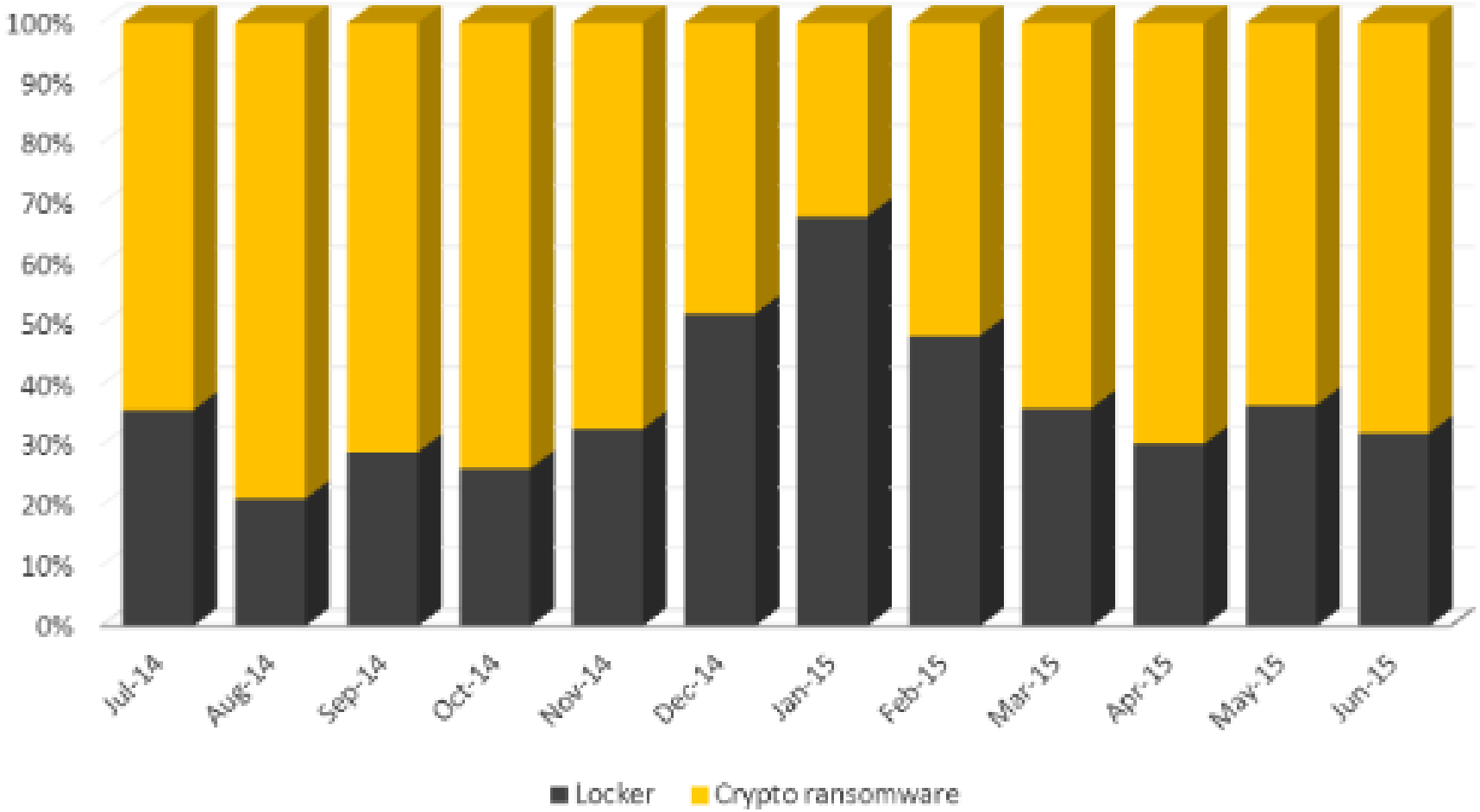



*Figure 26. Detections for binary-based crypto ransomware dominate the ransomware threat landscape for past 12 months.*

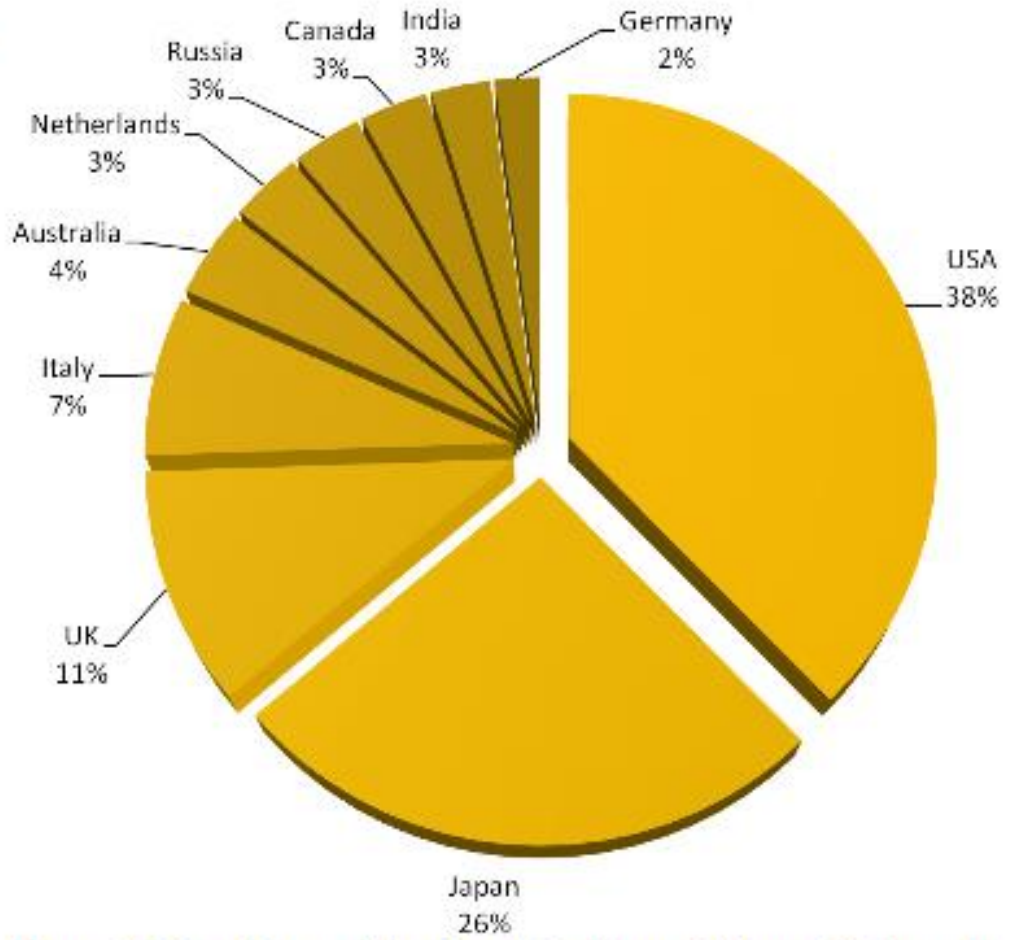



*Figure 27. Top 10 countries for detections of binary file based crypto ransomware*

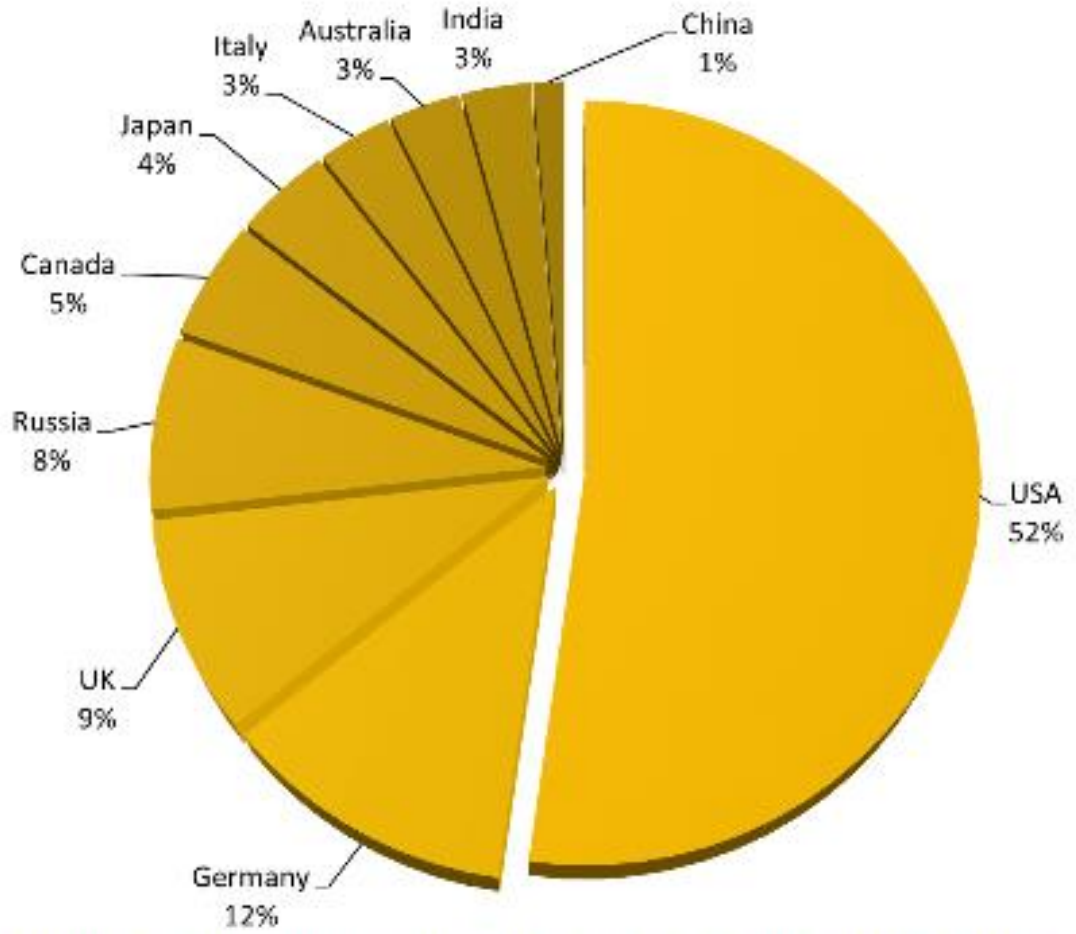



*Figure 28. Top countries for detections of binary-based locker ransomware*

# 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://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