School of Computing – https://www.cs.kent.ac.uk/

RANSOMWARE DEPLOYMENT METHODS AND ANALYSIS: VIEWS FROM A PREDICTIVE MODEL AND HUMAN RESPONSES

Gavin Hull (hullgj@gmail.com), Henna John (henna_john@hotmail.com), and Budi Arief (b.arief@kent.ac.uk)

What is Ransomware?

- Preventing victims' access to their data
  - Locking out the victims
  - Encrypting some or all of their files
- Demanding ransom to be paid
  - A ransom note or splash screen
  - Payment via cryptocurrency
  - Contact information or multi-lingual support may be provided
  - May include extra pressure, e.g. timer

Our Research Aim

- To understand how various ransomware strains are being deployed
- To find out how (potential) victims may react to ransomware incidents

Methodology

- A predictive model of ransomware
- A user study (questionnaire + interview) of victims

Key findings

- Common infection vectors
  - Phishing and social engineering
  - Exploit kits
  - Downloader
  - Trojan botnets
  - Traffic distribution systems
- "Randep": Ransomware Deployment model
  - Mapping ransomware activities into higher and lower level stages (Figure 1)
- Applying the Randep model on some ransomware
  - TeslaCrypt, Cerber and WannaCry (Figure 2)
- Human responses: victims' perspective
  - Figure 3, Figure 4, Figure 5, and Table 1

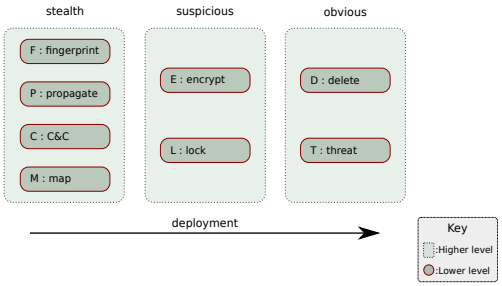

Figure 1: Predictive model of ransomware deployment methods

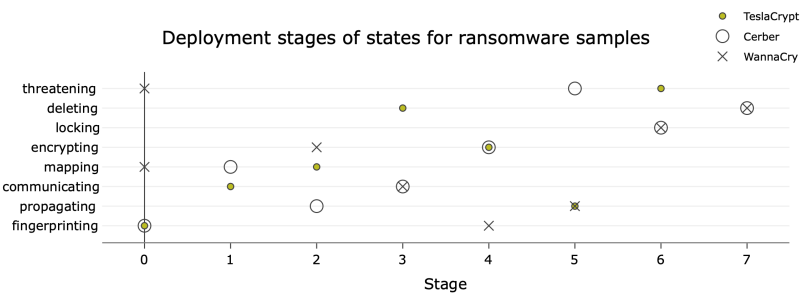

Figure 2: The stages of deployment for TeslaCrypt, Cerber and WannaCry according to the states of the Randep model

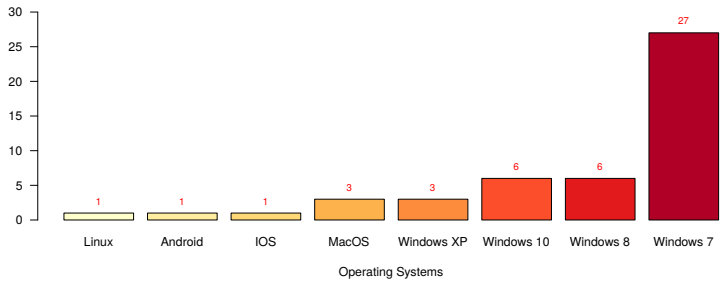

Figure 3: Operating Systems affected

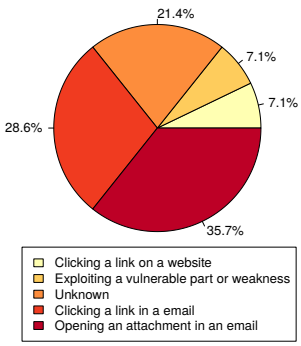

Figure 4: How ransomware got in

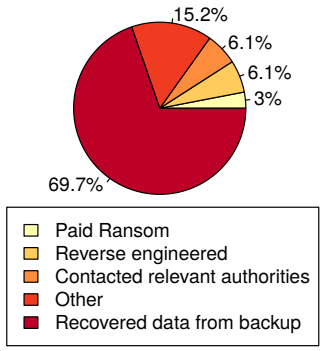

Figure 5: How data got recovered

Table 1: Common first signs of ransomware infection

Sign of infection	Number of occurrences
Desktop was locked	10
Some files went missing	10
Office software such as MS Word and Excel crashed or failed to open file	9
Starting up took much longer than usual	5
Computer crashed	4
Computer started to overheat and became very slow	4
Antivirus software was disabled or took longer to start up	2
Screen or display started to jitter	2
Computer restarted without my consent	1
Noticed files starting to encrypt on network share	1
Browser window popups appeared	1
Intrusion detection system sent alerts about connections to blacklisted IP addresses, vulnerable ports, or suspicious DNS queries	1
User reported system performance issue	1

Lessons Learned

- The most common attack vector is via email, more specifically through email attachments
- **Basic security hygiene** should be followed
  - Do backups
  - Be careful with links (especially on emails)
  - Perform software updates
  - Install protection software
  - Don't run everyday operations with admin privileges by default

Summary

- **Prevention** is better than remedy
- **Educating** users and implementing endpoint security measures are needed
- **Do not pay** the ransom demand!
  - There is no guarantee you would get your data back
  - By paying ransom, you could be funding cybercrime

QR Code for the article

Adapted from a published journal article:

Hull, G., John, H. & Arief, B. Ransomware deployment methods and analysis: views from a predictive model and human responses. *Crime Sci* **8**, 2 (2019). https://doi.org/10.1186/s40163-019-0097-9