INFS 5115 Security Principles

Malware / Ransomware

University of South Australia

School of
Information Technology
and Mathematical Sciences

Malware / Ransomware

- In this seminar we will discuss a variety of contemporary malware including ransomware.
- We will also review the operation and practical effects of two different types of malware, and briefly discuss mitigation strategies.

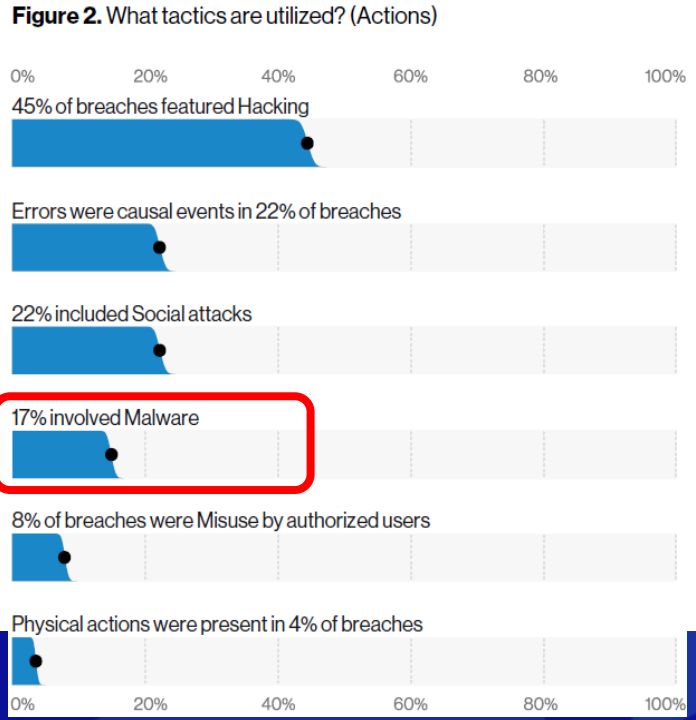
Malware

Definition

- Malware
  - *A program that is **inserted** into a system, usually **covertly**, with the intent of compromising the **confidentiality**, **integrity**, or **availability** of the victim's **data**, **applications**, or **operating system** or of otherwise annoying or disrupting the victim.*[1]

[1] SP 800-83 cited in Kissel, R., 2013. Glossary of Key Information Security Terms. NIST Interagency Reports, NISTIR 7298.

Malware as a tactic



Source: Verizon's 2020 Data Breach Investigations Report, p.7, https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf

Malware findings

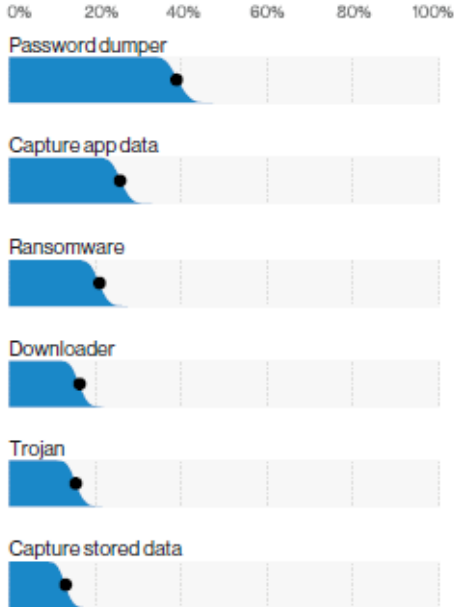


Figure 16. Top Malware varieties in breaches (n = 506)

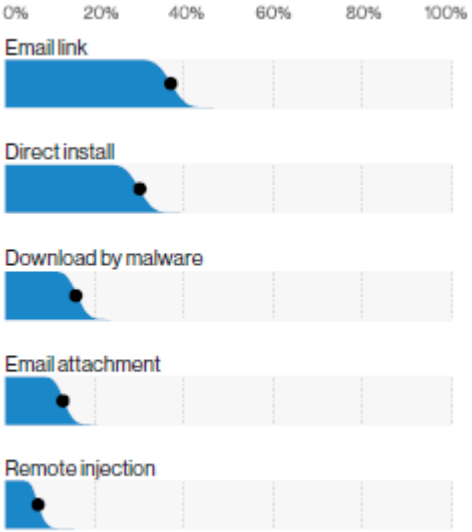


Figure 17. Top Malware vectors in breaches (n = 360)

Source: Verizon's 2020 Data Breach Investigations Report, p.13, https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf

Malware delivery types

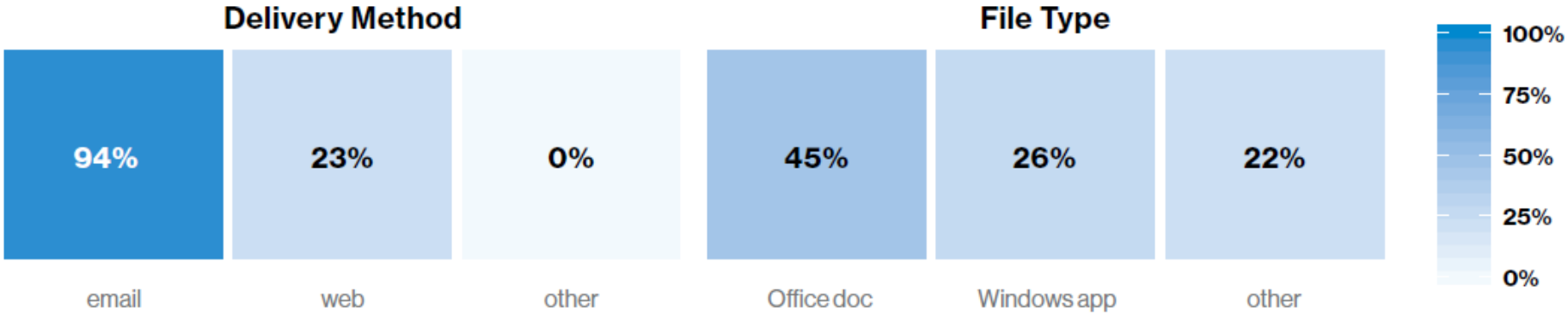


Figure 19. Malware types and delivery methods

Source: Verizon's 2019 Data Breach Investigations Report, p.13, https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf

Other malware delivery types

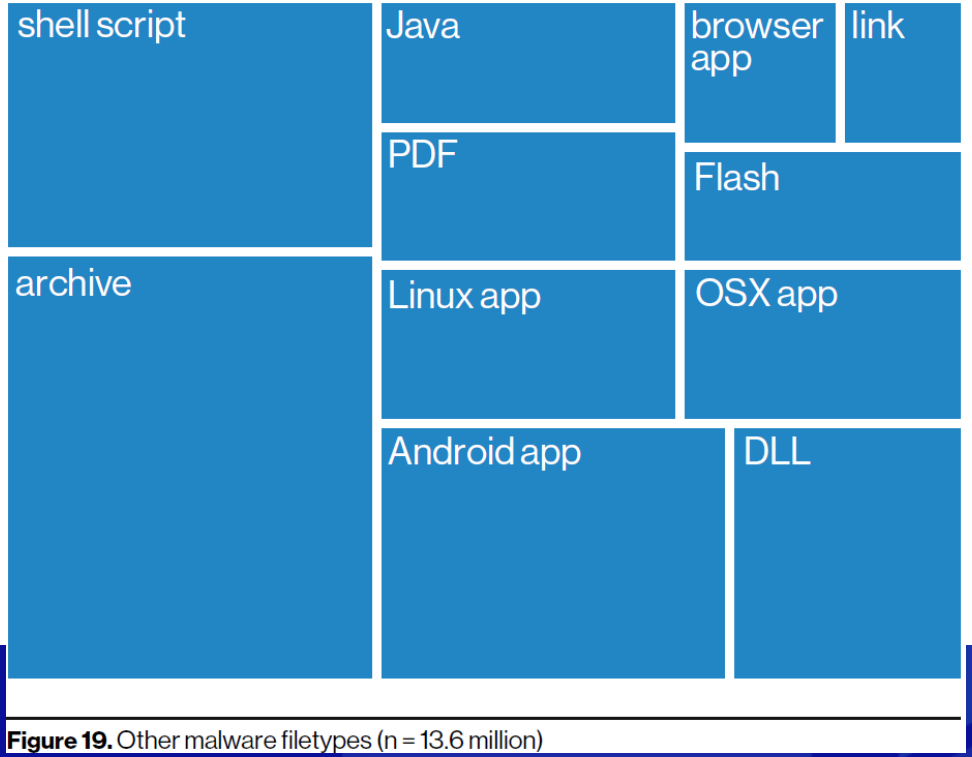


Figure 19. Other malware filetypes (n = 13.6 million)

Source: Verizon's 2020 Data Breach Investigations Report, p.13, https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf

Types of malware

Many types of malware have been classified in the last few decades.

- Virus
- Trojan (Horse)
- Worm
- Spyware
- Web-based malware
- Blended attacks

Graham, J, Olson, R, & Howard, R (eds) 2010, Cyber Security Essentials, CRC Press, Boca Raton. (Chapter 4 – Malicious Code)

Activity 1 – Types of malware

Open Activity 1 under Week 8 Malware/Ransomware

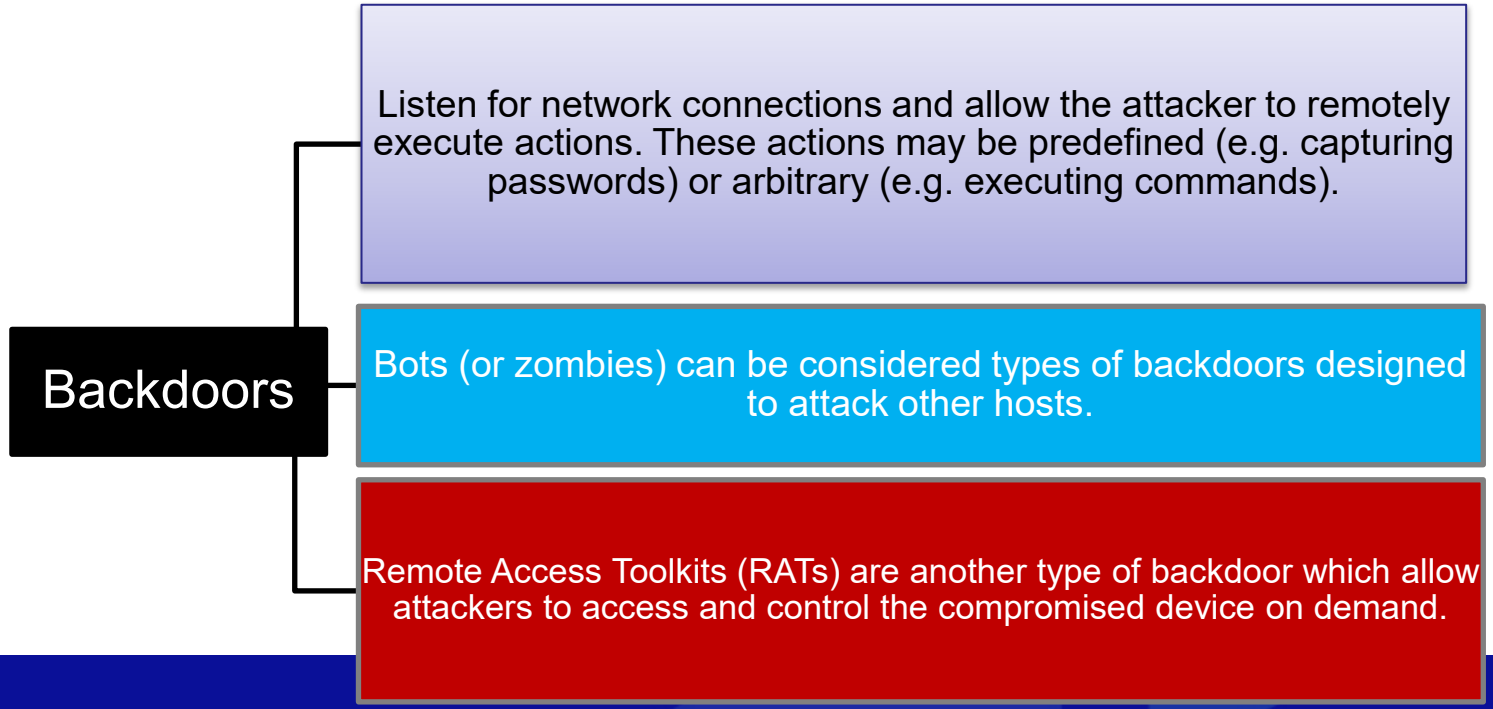
Malware attacker tools

- Once malware has infected a device, it generally tries to deploy one or more attacker tools.

- These tools are often designed to provide remote access to the device to receive further instructions, exfiltrate data and/or launch attacks on other devices.

Souppaya, M and Scarfone, K 2013, 'Guide to Malware Incident Prevention and Handling for Desktops and Laptops', National Institute of Standards and Technology, SP 800-83.

Malware examples of tools : NIST SP 800-83



Souppaya, M and Scarfone, K 2013, 'Guide to Malware Incident Prevention and Handling for Desktops and Laptops', National Institute of Standards and Technology, SP 800-83.

Malware

Attacker Tools

- Keystroke Loggers
  - Captures the keypresses on the device keyboard and either stores them locally for physical collection by the attacker or transmits them remotely via various means.
- Rootkit
  - Collection of files installed on a host to alter its standard functionality. Designed to provide stealth characteristics to help ensure persistence.
- Web Browser Plugins
  - Malicious web browser plugins are designed to allow an attacker to monitor and/or modify browser sessions.

Souppaya, M and Scarfone, K 2013, 'Guide to Malware Incident Prevention and Handling for Desktops and Laptops', National Institute of Standards and Technology, SP 800-83.

Malware

Attacker Tools

- Email Generators
  - Designed to send large quantities of spam email messages.
- Attacker Toolkit
  - A combination of various utilities and scripts that are useful as part of cyber intrusions, for example:
    - Packet sniffers
    - Port scanners
    - Vulnerability scanners
    - Password cracking or capturing tools
    - Other attack programs/scripts

Souppaya, M and Scarfone, K 2013, 'Guide to Malware Incident Prevention and Handling for Desktops and Laptops', National Institute of Standards and Technology, SP 800-83.

Malware

Malware Toolkits

- Malware toolkits have grown increasingly popular with adversaries either buying customised malware or building it using open source toolkits.
- Examples of malware toolkits include:
  - Metasploit Framework
  - Drovorub
  - XcodeGhost

- The colloquial concept of *Malware as a Service* is also often discussed.

Souppaya, M and Scarfone, K 2013, 'Guide to Malware Incident Prevention and Handling for Desktops and Laptops', National Institute of Standards and Technology, SP 800-83.

Malware

- NIST SP 800-83 provides an example of an attack executed by a malware toolkit:
  1. *The toolkit sends spam to users, attempting to trick them into visiting a particular website.*
  2. *Users visit the website, which has malicious content provided by the toolkit.*
  3. *The website infects the users' computers with Trojan horses (provided by the toolkit) by exploiting vulnerabilities in the computers' operating system.*
  4. *The Trojan horses install attacker tools, such as keystroke loggers and rootkits (provided by the toolkit).*

Souppaya, M and Scarfone, K 2013, 'Guide to Malware Incident Prevention and Handling for Desktops and Laptops', National Institute of Standards and Technology, SP 800-83, p. 4.

Activity 2 – Anatomy of a Malware Toolkit Attack

Open Activity 2 under Week 8 Malware/Ransomware

Ransomware

- Ransomware can cripple organisations that rely on computer systems to function, by encrypting all connected electronic devices, folders and files and rendering systems inaccessible.
- Cybercriminals will then demand a ransom in return for the decryption keys, often in the form of untraceable crypto currencies such as Bitcoin
- Recovering from ransomware is almost impossible without comprehensive backups.
- Over the last 12 months, ransomware has become one of the most significant cyber threats facing the operation of private sector organisations.

ACSC, 2020, ACSC Annual Threat report 2019-20

Ransomware

Emotet and Trickbot

- Emotet is a type of malware disseminated through phishing emails designed to provide an adversary with a foothold into a network from which additional attacks can be performed.
- Emotet is most commonly spread via emails containing MS Office attachments, usually Word documents , or PDF attachments.
- Once activated, Emotet commonly deploys Trickbot malware which infects a network and sits unobtrusively for a period while it collects user credentials and maps networks.

ACSC, 2020, ACSC Annual Threat report 2019-20

Ransomware

Ryuk

- Ryuk is a type of ransomware typically used to target enterprise environments.
- Initial compromise of devices or networks is generally obtained through use of Emotet or Trickbot malware, which provides a foothold by which adversaries can then execute Ryuk ransomware for financial gain.
- Ryuk is particularly effective because it encrypts almost all file types, unlike other variants of ransomware that typically contain extensive lists of file extensions that will not be encrypted.

ACSC, 2020, ACSC Annual Threat report 2019-20

Ransomware

Developments

- Contemporary ransomware is stronger than the initial developments in this field.
- For example, decryption keys are often stored on remote servers controlled by the attacker, rather than on the victim's device.
- This is facilitated by the use of asymmetric encryption which has separate public and private keys.
- Unique encryption keys per device are also now generally used.

Symantec 2016, 'An ISTR Special Report: Ransomware and Businesses 2016', Symantec Corporation, https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/ransomware-and-businesses-16-en.pdf

Ransomware

Developments

- Cryptocurrencies such as Bitcoin have also made it more feasible for adversaries to collect ransom payments.
- Ransomware as a Service (RaaS) allows non-skilled adversaries to buy a ransomware executable and a user interface to track their victims.
- The RaaS developers can take a proportion of the ransom profits as payment.

Symantec 2016, ‘An ISTR Special Report: Ransomware and Businesses 2016’, Symantec Corporation, https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/ransomware-and-businesses-16-en.pdf

ACSC 2017 Threat Report

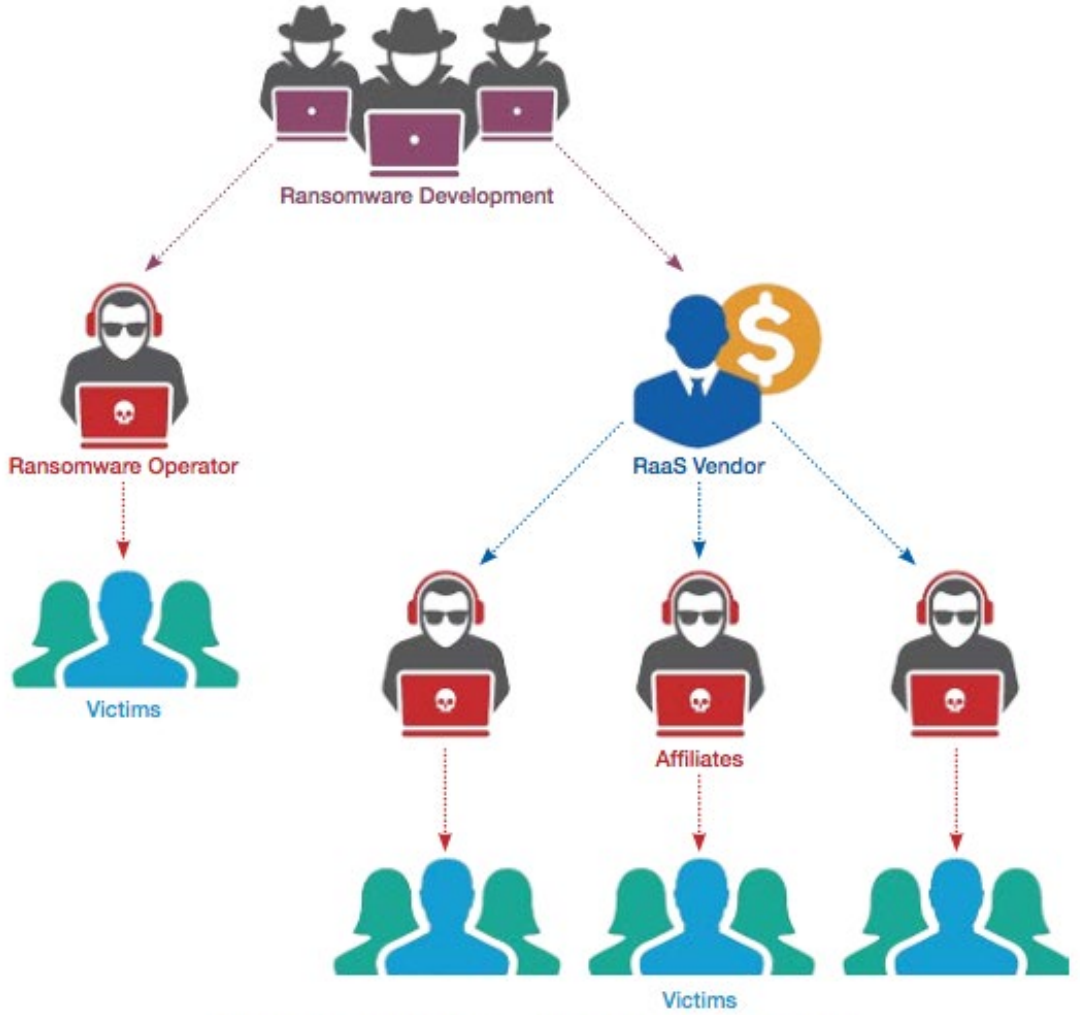


Figure 4: 'Ransomware-as-a-Service' operating model, ACIC

Ransomware

Infection Vectors

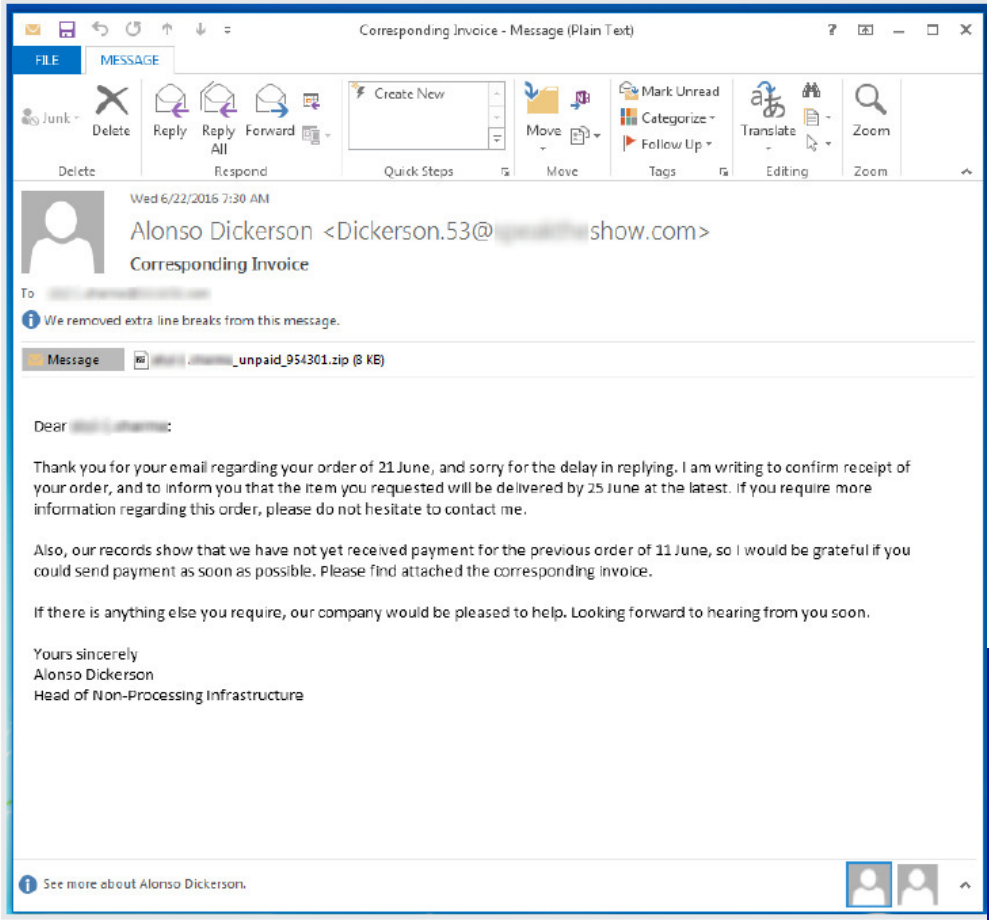
- Email
  - Malicious email is one of the most common methods for ransomware infections.
  - Common methods of email infection include:
    - Opening a malicious attachment that installs the ransomware.
    - Opening an attachment which installs the ransomware via another vector (e.g. a macro).
    - Following a link to an exploit kit which compromises the device and installs the malware.

Symantec 2016, 'An ISTR Special Report: Ransomware and Businesses 2016', Symantec Corporation, https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/ransomware-and-businesses-16-en.pdf

Ransomware

Infection Vectors

- Common *ostensible* email subjects include fake:
  - Shipping notifications
  - Overdue bills
  - Tax return notifications
  - Invoices



Symantec 2016, 'An ISTR Special Report: Ransomware and Businesses 2016', Symantec Corporation, https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/ransomware-and-businesses-16-en.pdf

Image Source: ibid, p. 10.

Ransomware

Infection Vectors

- Exploit Kits (/Malware Toolkits)
  - Vulnerabilities are another common malware delivery method.
- Malvertising
  - Malicious ads can be an infection vector, often when combined with exploit kits.
- Brute forcing server passwords/exploiting server vulnerabilities
- SMS messages and third party apps on mobile platforms

Symantec 2016, 'An ISTR Special Report: Ransomware and Businesses 2016', Symantec Corporation, https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/ransomware-and-businesses-16-en.pdf

Ransomware

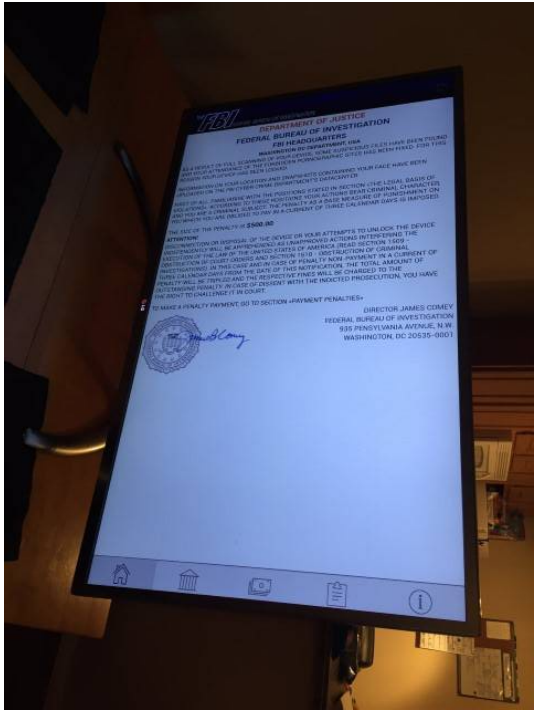
Platforms

- Windows
  - Windows is currently the primary target for prevalent ransomware.
- Mac OS/Linux
  - Mac OS and Linux are also targets of various malware variants.
- Mobile Platforms
  - Locker type ransomware has been deployed on Android devices. Crypto-ransomware is more difficult to deploy on mobile devices due to app sandboxing.

Symantec 2016, 'An ISTR Special Report: Ransomware and Businesses 2016', Symantec Corporation, https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/ransomware-and-businesses-16-en.pdf

Ransomware

- Future Targets
  - Internet of Things devices (such as smart TVs) have already been targeted by ransomware.
  - Industrial control systems are a concerning potential future target for ransomware.



Platforms

Image Source: https://www.theregister.co.uk/2017/01/03/programmer_finds_way_to_liberate_ransomwared_google_smart_tvs/

Symantec 2016, 'An ISTR Special Report: Ransomware and Businesses 2016', Symantec Corporation, https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/ransomware-and-businesses-16-en.pdf

Malware / Ransomware

Case Studies

- Three case studies are highlighted in the ACSC's Ransom in Australia, October 2020 report available here. https://www.cyber.gov.au/sites/default/files/2020-10/Ransomware%20in%20Australia%20%28October%202020%29.pdf
- Chose one of the case studies and attempt the following questions
  - Why was this organisation attacked?
  - What was their response?
  - Suggest possible mitigations for safeguarding the organisation against future attacks.

Malware Mitigations

- ASD recommends implementation of mitigation strategies in the following order to mitigate against *ransomware and external adversaries who destroy:*
  1. *Implement "essential" mitigation strategies to:*
     a. *recover data and system availability*
     b. *prevent malware delivery and execution*
     c. *limit the extent of cyber security incidents*
     d. *detect cyber security incidents and respond.*
  2. *Repeat step 1 with "excellent" mitigation strategies.*
  3. *Repeat step 1 with less effective mitigation strategies until an acceptable level of residual risk is reached.*

Australian Signals Directorate 2017, 'Strategies to Mitigate Cyber Security Incidents', https://www.asd.gov.au/infosec/top-mitigations/mitigations-2017-table.htm