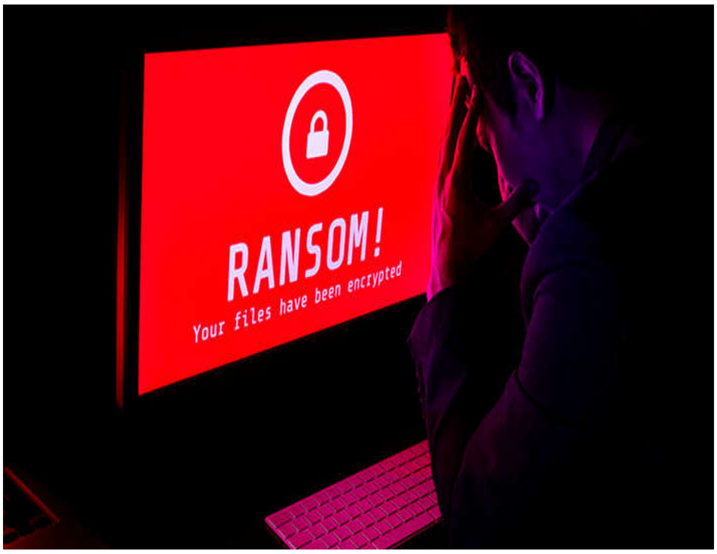
FOUNDATIONS IN IT SECURITY: UNDERSTANDING MALWARE

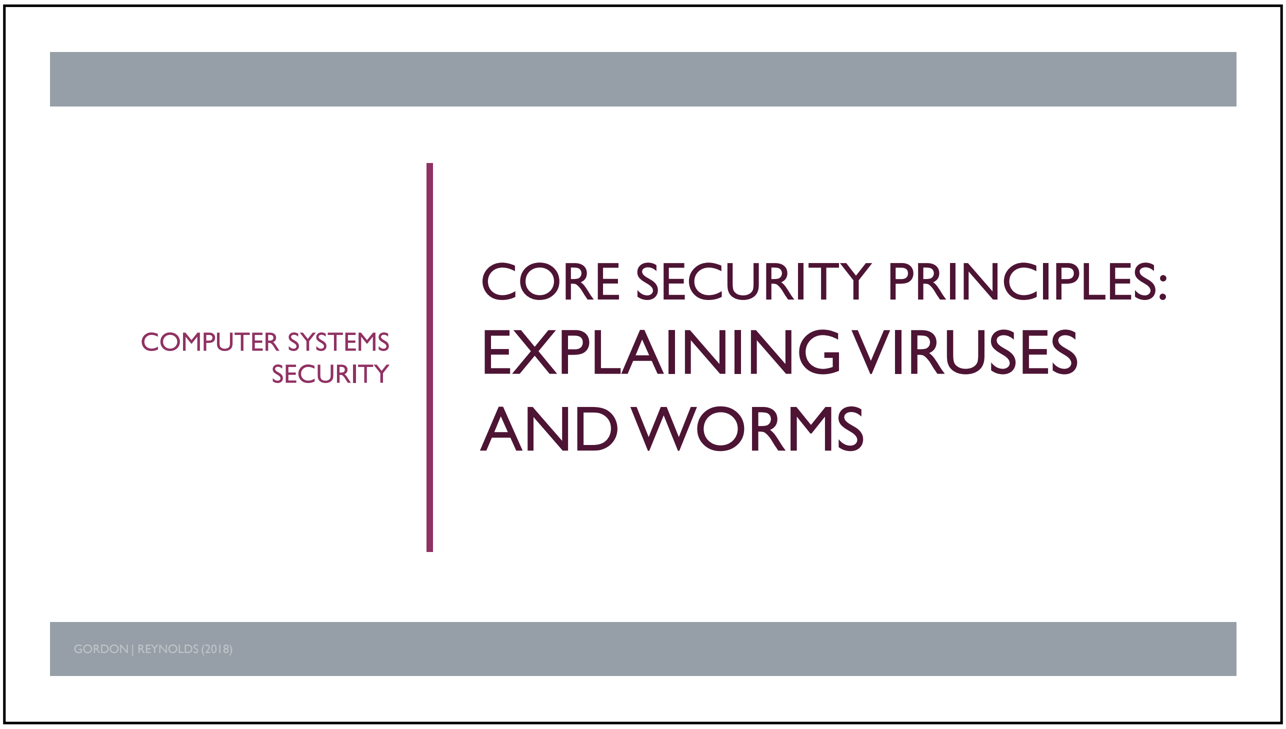
COMPUTER SYSTEMS SECURITY

TODAY ….

Today we will look at Core Security Principles, which includes:

- Explaining Viruses and Worms
- Eliminating unwanted surveillance
- Holding data hostage

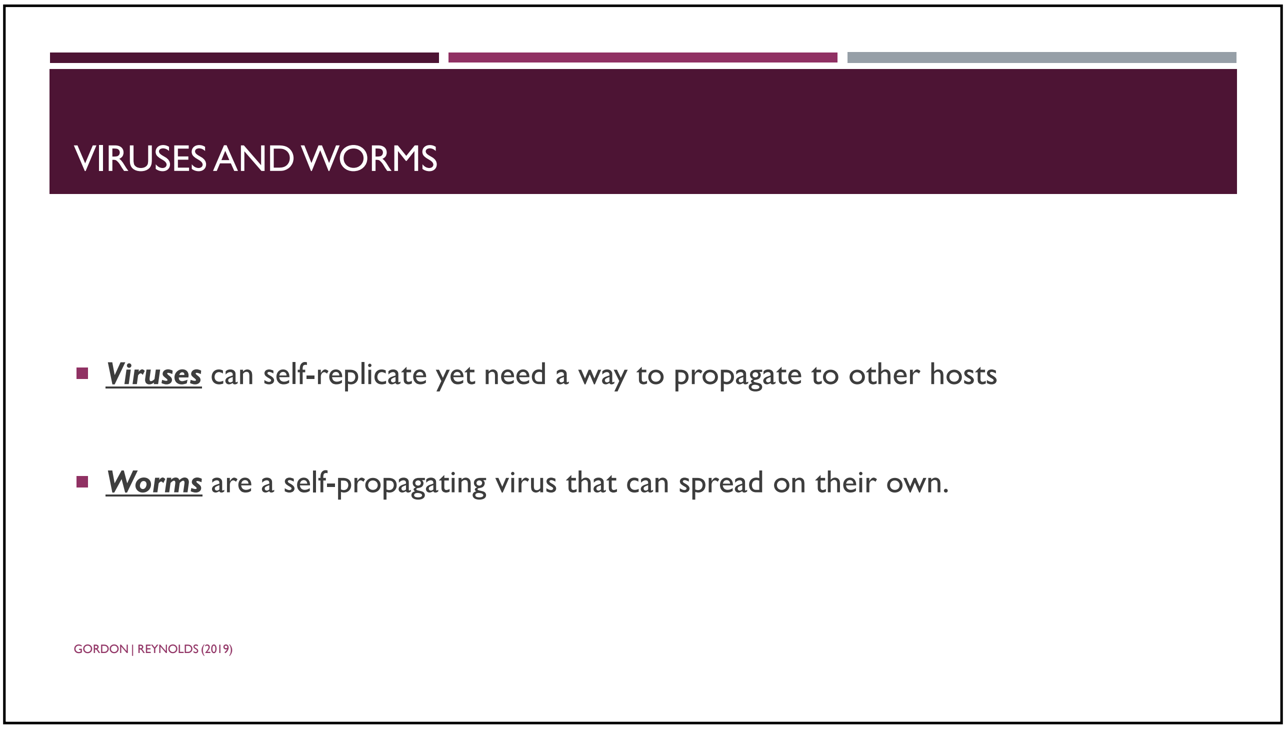




COMPUTER SYSTEMS SECURITY

CORE SECURITY PRINCIPLES: EXPLAINING VIRUSES AND WORMS

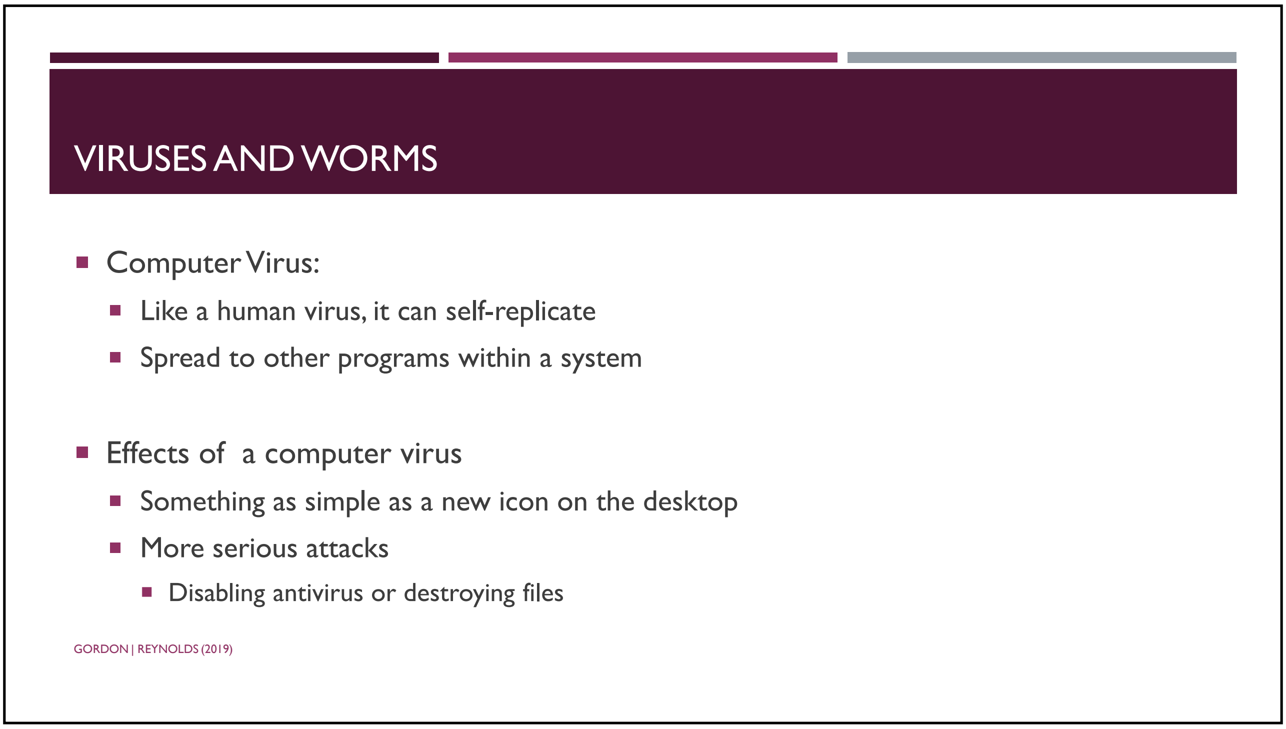
GORDON | REYNOLDS (2018)



VIRUSES AND WORMS

- ***Viruses*** can self-replicate yet need a way to propagate to other hosts
- ***Worms*** are a self-propagating virus that can spread on their own.

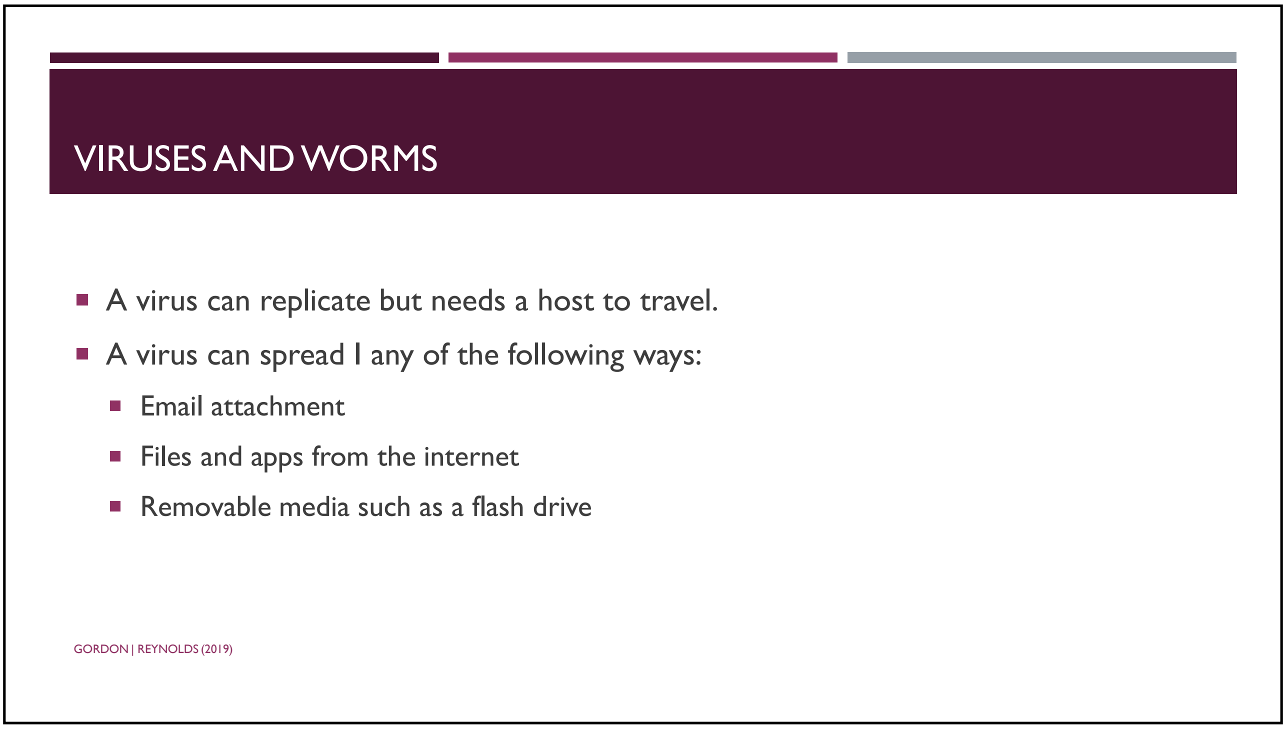
GORDON | REYNOLDS (2019)



VIRUSES AND WORMS

- Computer Virus:
  - Like a human virus, it can self-replicate
  - Spread to other programs within a system
- Effects of a computer virus
  - Something as simple as a new icon on the desktop
  - More serious attacks
    - Disabling antivirus or destroying files

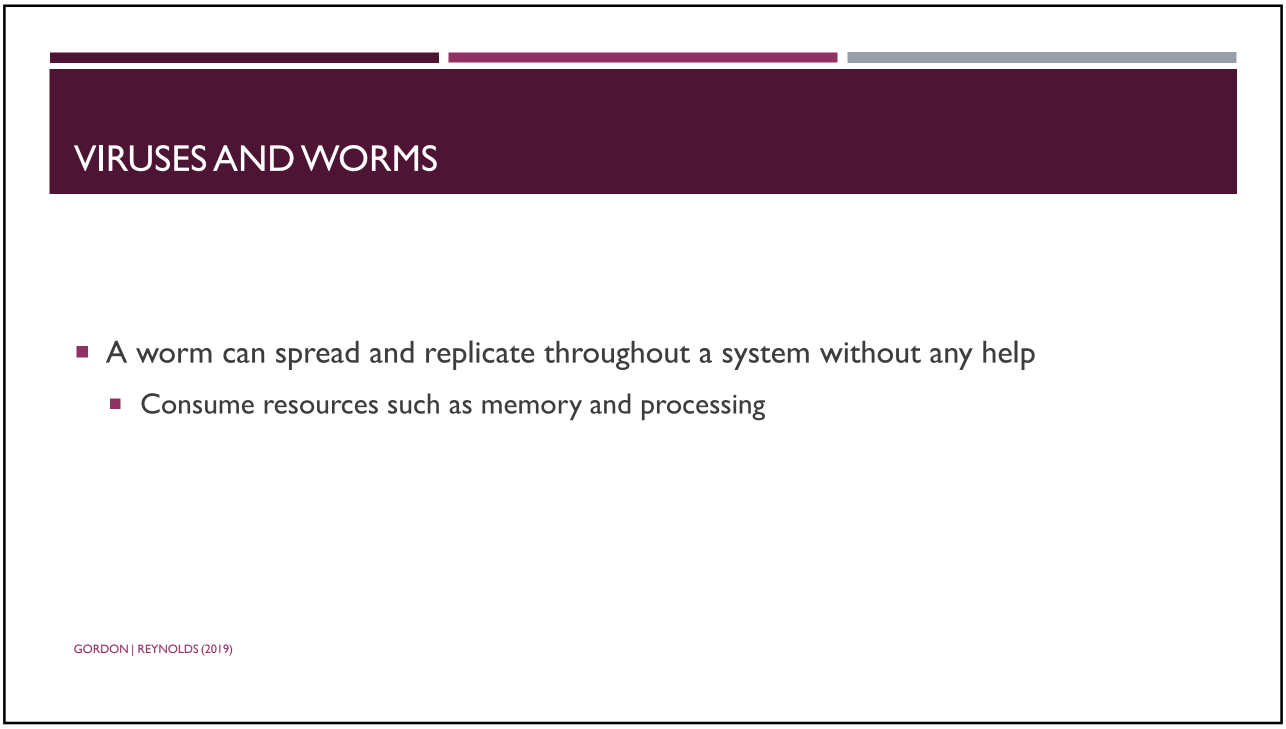
GORDON | REYNOLDS (2019)



VIRUSES AND WORMS

- A virus can replicate but needs a host to travel.
- A virus can spread I any of the following ways:
  - Email attachment
  - Files and apps from the internet
  - Removable media such as a flash drive

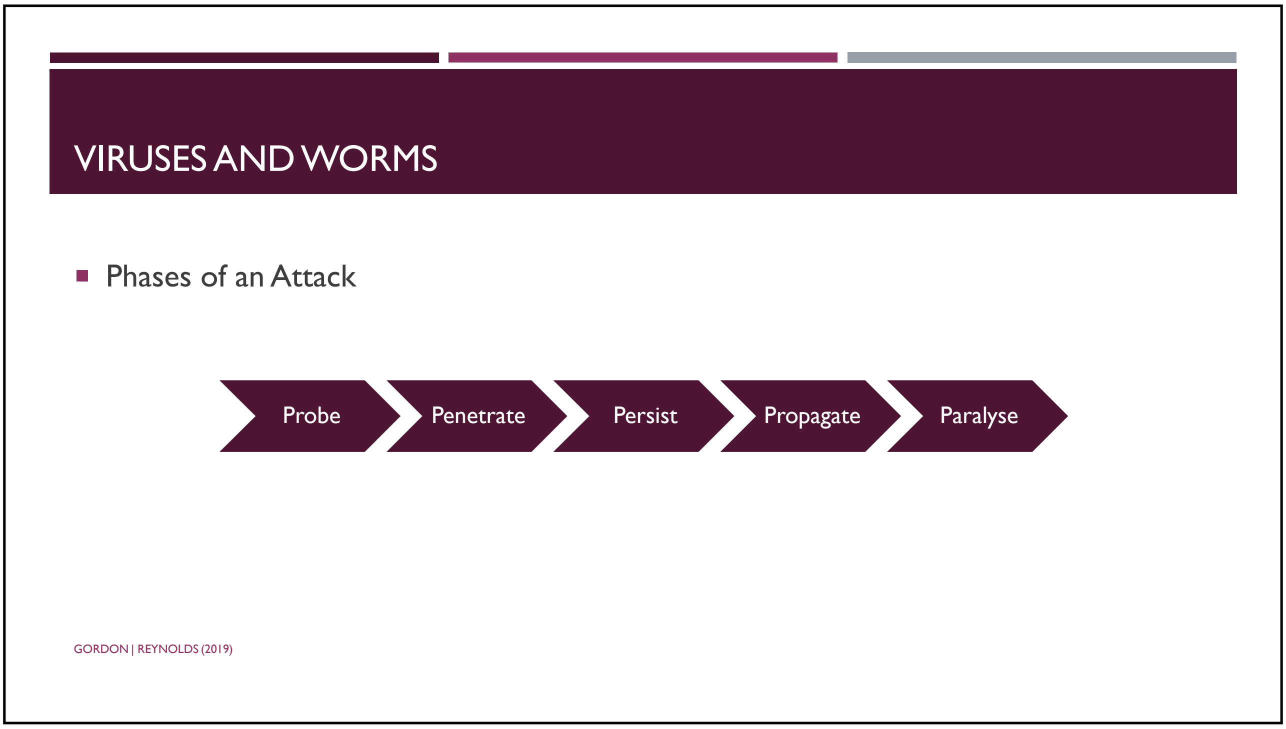
GORDON | REYNOLDS (2019)



VIRUSES AND WORMS

- A worm can spread and replicate throughout a system without any help
  - Consume resources such as memory and processing

GORDON | REYNOLDS (2019)



VIRUSES AND WORMS

- Phases of an Attack

GORDON | REYNOLDS (2019)

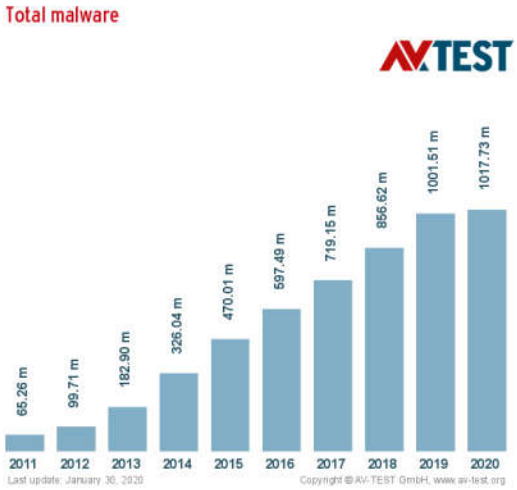
VIRUSES AND WORMS

- Viruses have been around a long time:
  - Search the free dictionary for: **Top 10 Worst Computer Worms of All Time**
    - Take note of the ***Storm Worm*** and ***Code Red***

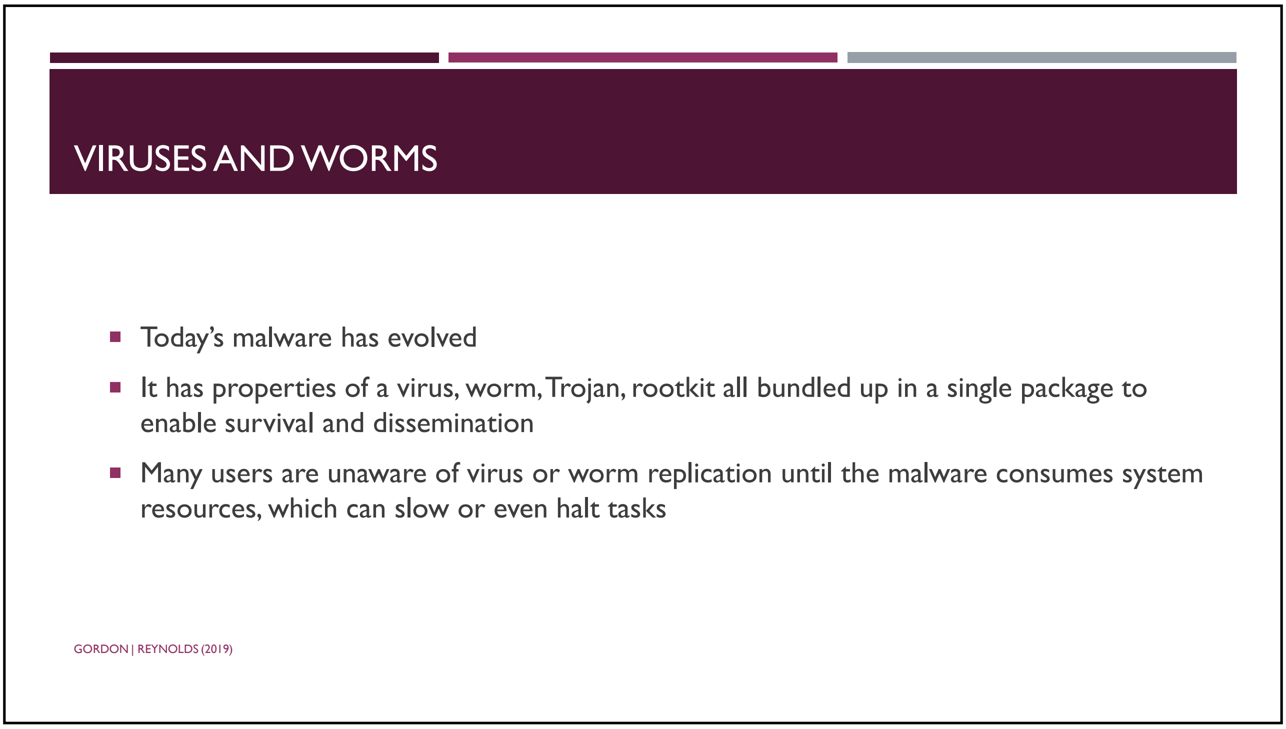
GORDON | REYNOLDS (2019)

VIRUSES AND WORMS

- Business have lost significate revenue due to viruses, worms, spyware and phishing attacks



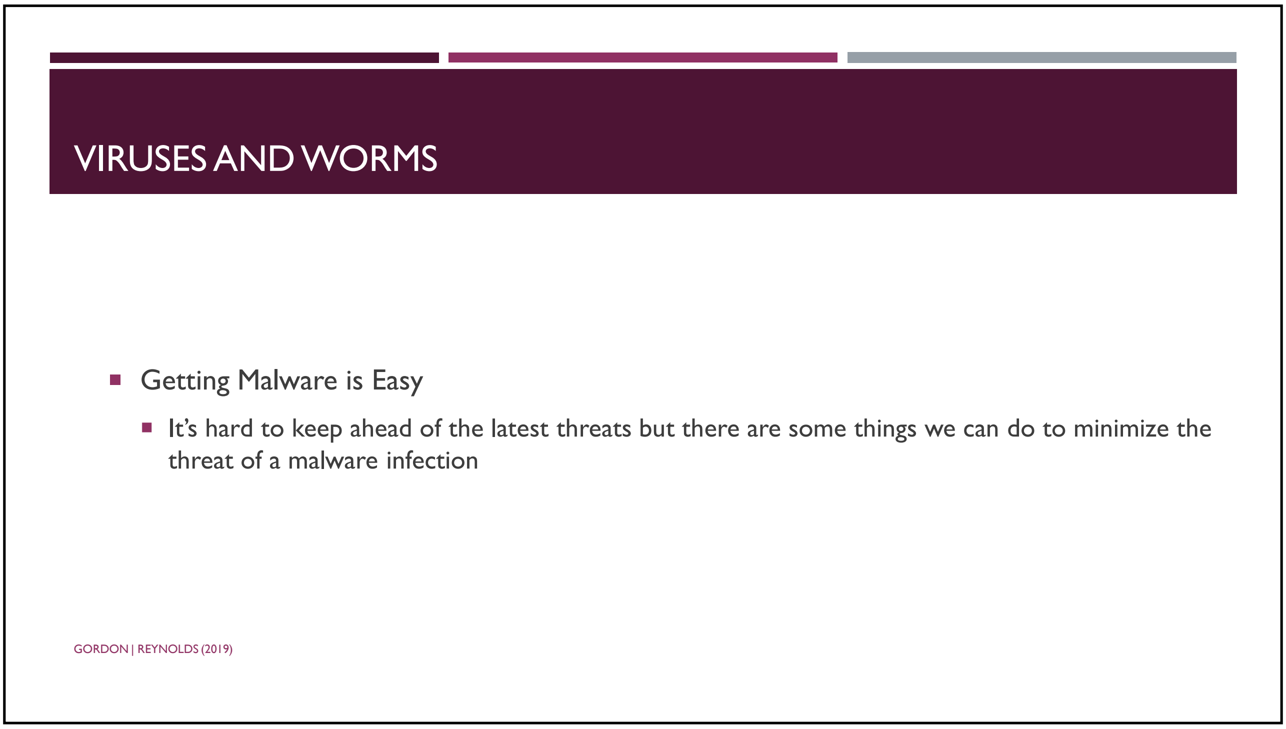
GORDON | REYNOLDS (2019)



VIRUSES AND WORMS

- Today's malware has evolved
- It has properties of a virus, worm, Trojan, rootkit all bundled up in a single package to enable survival and dissemination
- Many users are unaware of virus or worm replication until the malware consumes system resources, which can slow or even halt tasks

GORDON | REYNOLDS (2019)



VIRUSES AND WORMS

- Getting Malware is Easy
  - It's hard to keep ahead of the latest threats but there are some things we can do to minimize the threat of a malware infection

GORDON | REYNOLDS (2019)

VIRUSES AND WORMS

- Best Practices:
  - Use caution when opening attachments
  - Use Windows Defender (or equivalent)
  - Antimalware Protection
  - Stay away from risky websites
  - Think before you click

VIDEO

GORDON | REYNOLDS (2019)

COMPUTER SYSTEMS SECURITY

CORE SECURITY PRINCIPLES: ELIMINATING UNWANTED SURVEILLANCE

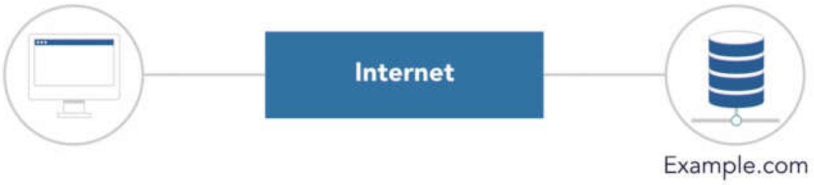
GORDON | REYNOLDS (2018)

ELIMINATING UNWANTED SURVEILLANCE

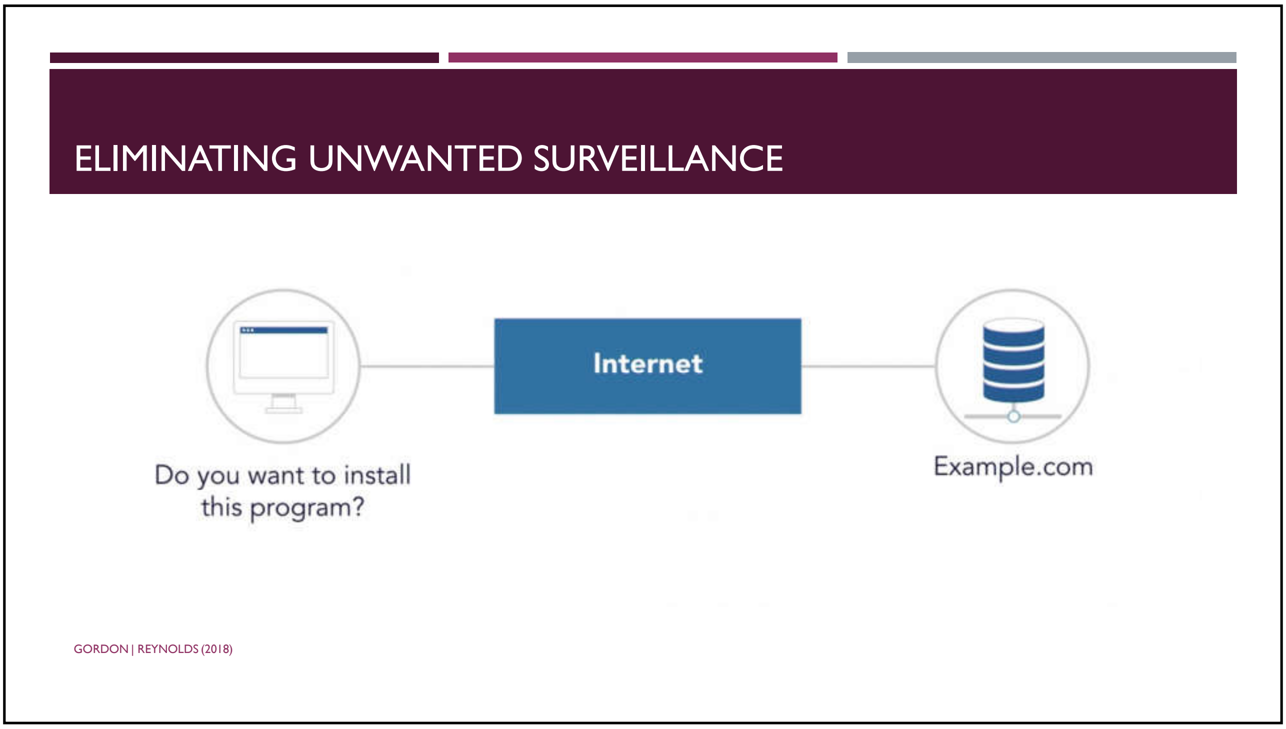
- Spyware
  - A type of malware that records keystrokes and other activity and sends the information to another site.
  - It tracks information on a user’s viewing habits while on the internet and sends that information to a remote computer without the user’s knowledge. (Adware)
  - Spyware is not illegal, but it is an unwanted program, nonetheless.

GORDON | REYNOLDS (2019)

ELIMINATING UNWANTED SURVEILLANCE



GORDON | REYNOLDS (2018)



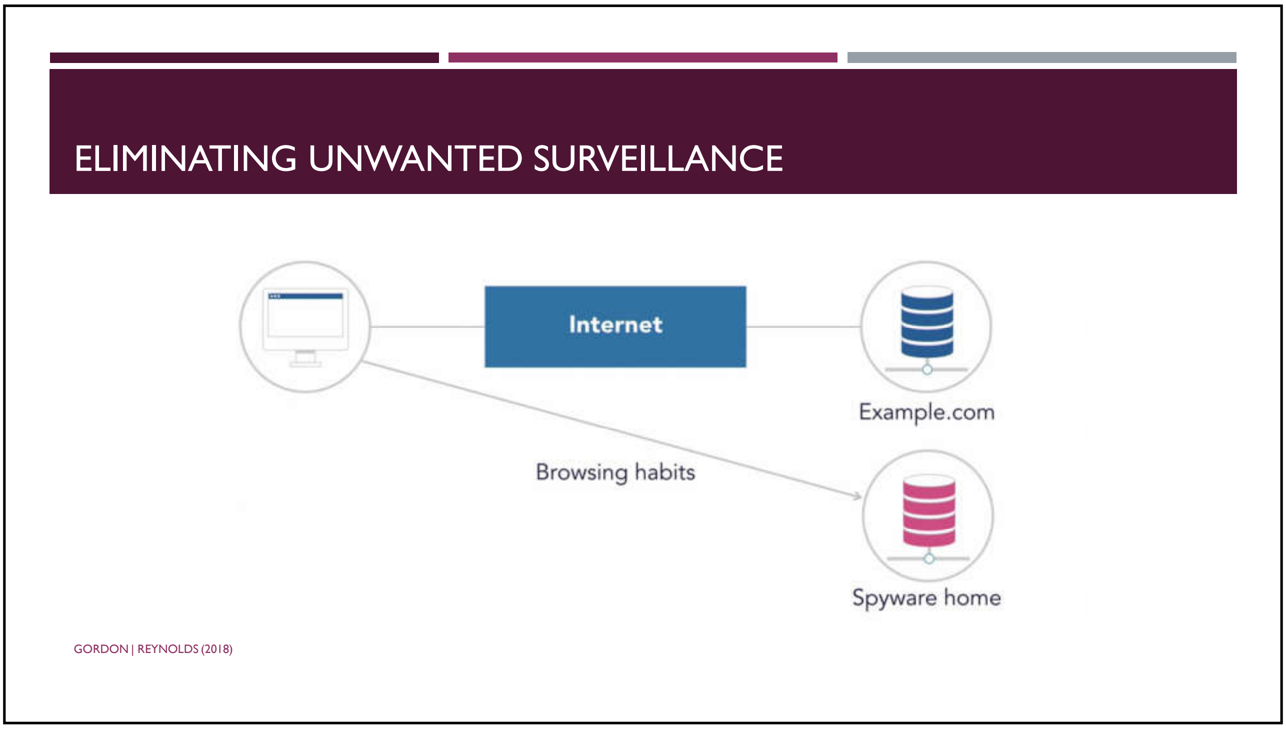
ELIMINATING UNWANTED SURVEILLANCE

Internet

Do you want to install this program?

Example.com

GORDON | REYNOLDS (2018)



ELIMINATING UNWANTED SURVEILLANCE

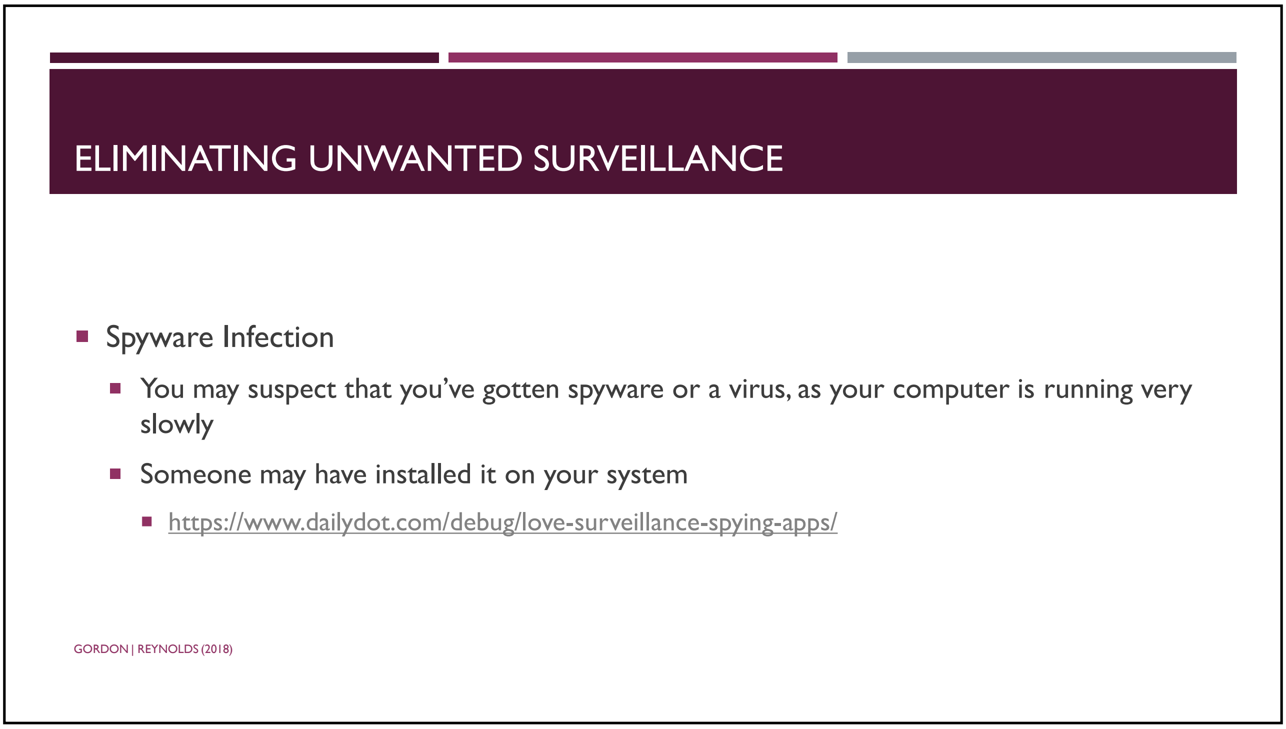
Internet

Example.com

Browsing habits

Spyware home

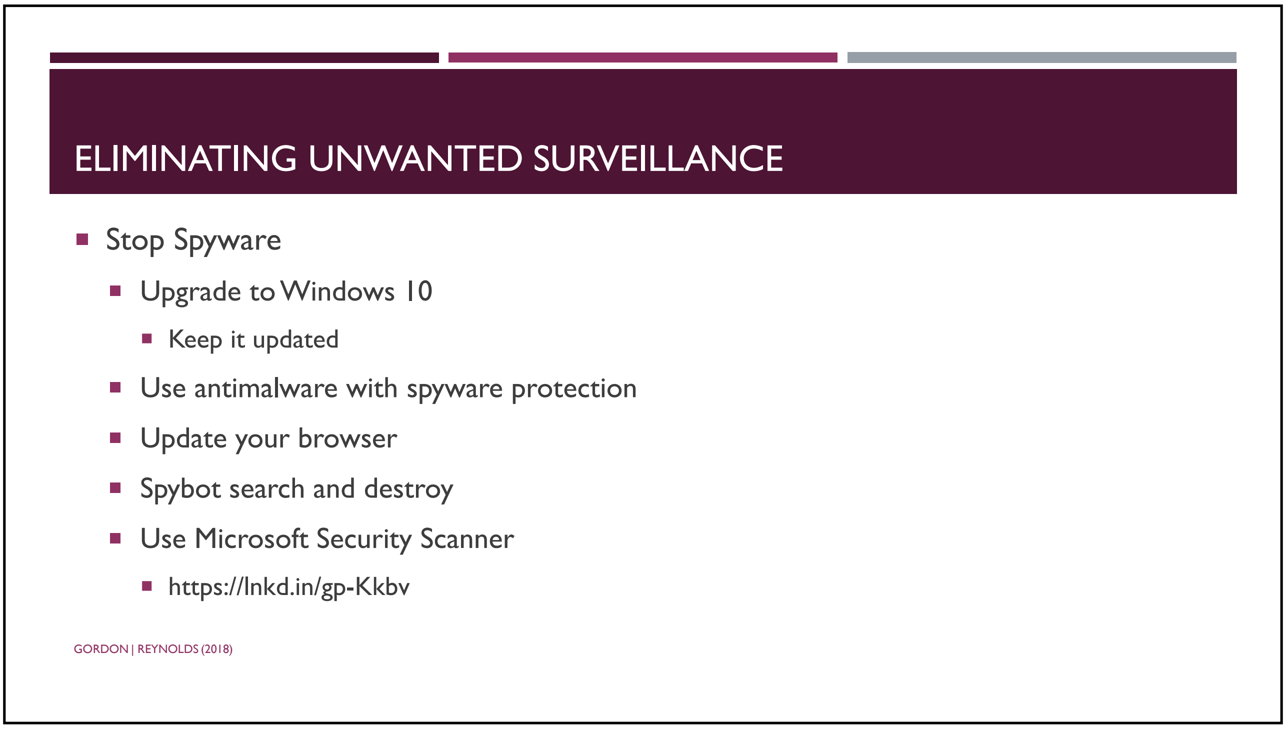
GORDON | REYNOLDS (2018)



ELIMINATING UNWANTED SURVEILLANCE

- Spyware Infection
  - You may suspect that you’ve gotten spyware or a virus, as your computer is running very slowly
  - Someone may have installed it on your system
    - https://www.dailydot.com/debug/love-surveillance-spying-apps/

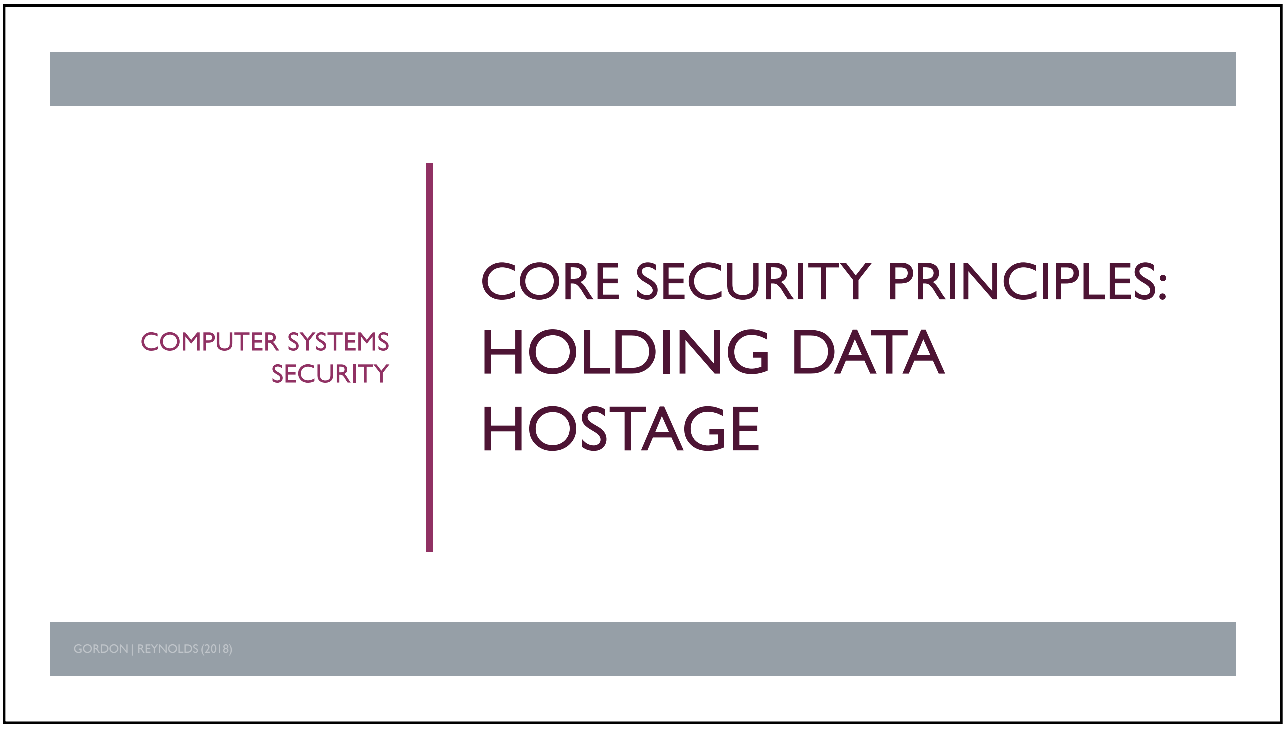
GORDON | REYNOLDS (2018)



ELIMINATING UNWANTED SURVEILLANCE

- Stop Spyware
  - Upgrade to Windows 10
    - Keep it updated
  - Use antimalware with spyware protection
  - Update your browser
  - Spybot search and destroy
  - Use Microsoft Security Scanner
    - https://lnkd.in/gp-Kkbv

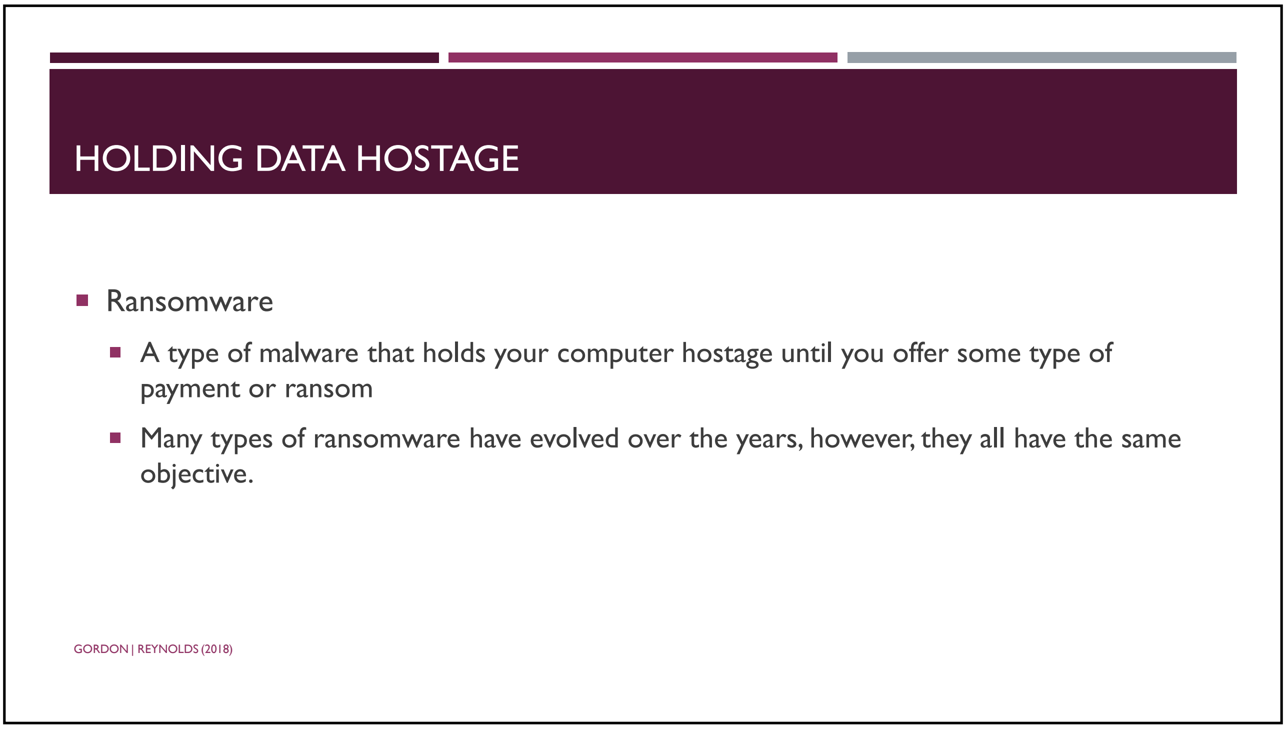
GORDON | REYNOLDS (2018)



COMPUTER SYSTEMS SECURITY

CORE SECURITY PRINCIPLES: HOLDING DATA HOSTAGE

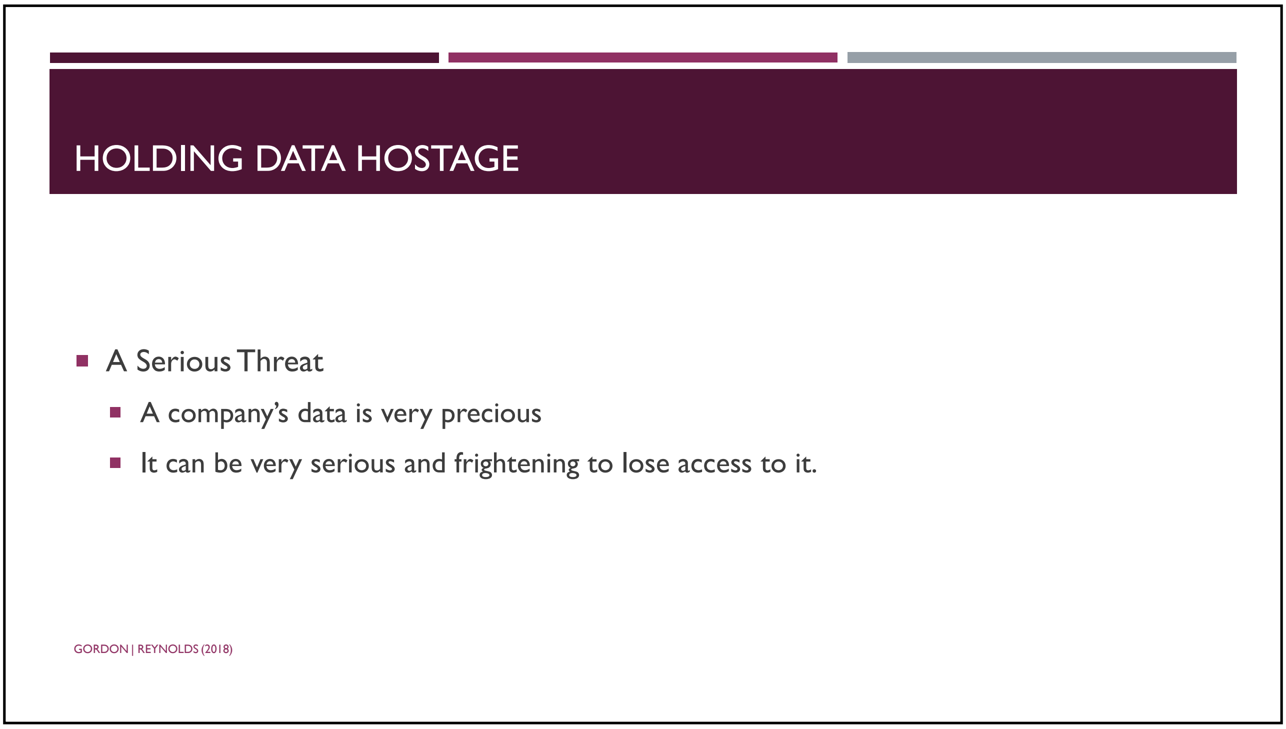
GORDON | REYNOLDS (2018)



HOLDING DATA HOSTAGE

- Ransomware
  - A type of malware that holds your computer hostage until you offer some type of payment or ransom
  - Many types of ransomware have evolved over the years, however, they all have the same objective.

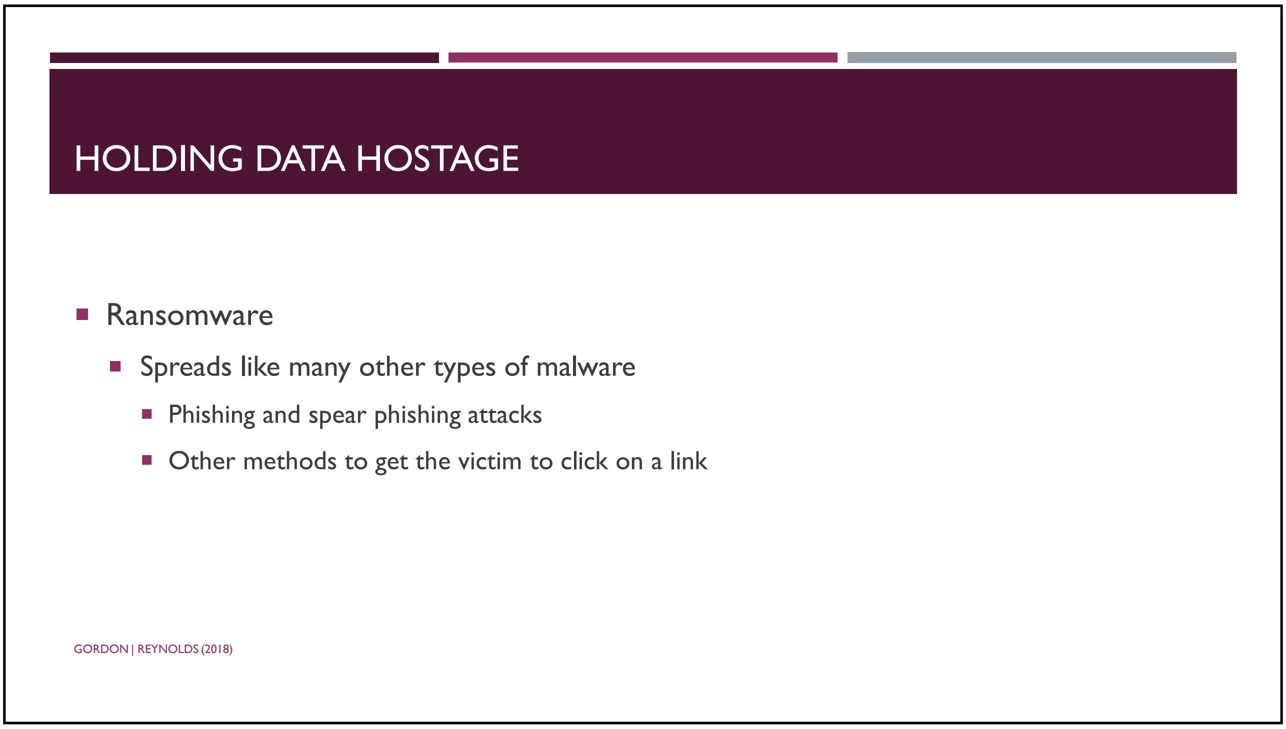
GORDON | REYNOLDS (2018)



HOLDING DATA HOSTAGE

- A Serious Threat
  - A company’s data is very precious
  - It can be very serious and frightening to lose access to it.

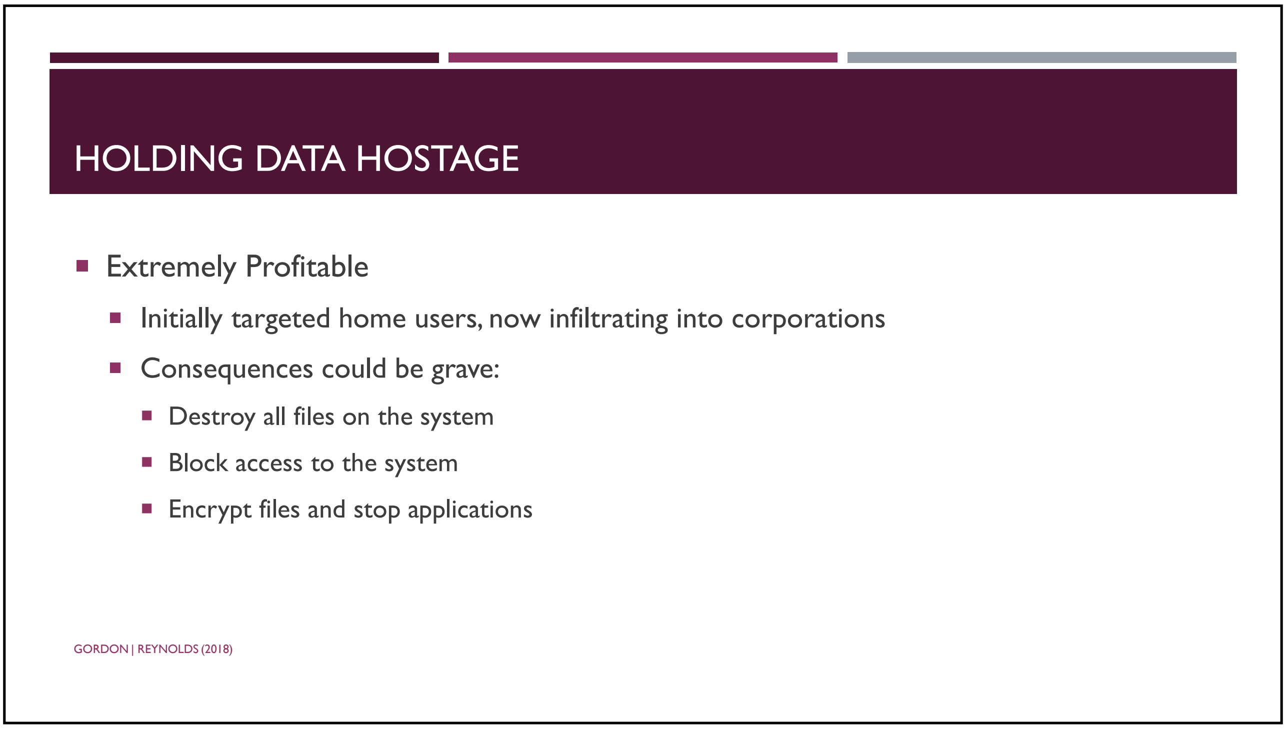
GORDON | REYNOLDS (2018)



HOLDING DATA HOSTAGE

- Ransomware
  - Spreads like many other types of malware
    - Phishing and spear phishing attacks
    - Other methods to get the victim to click on a link

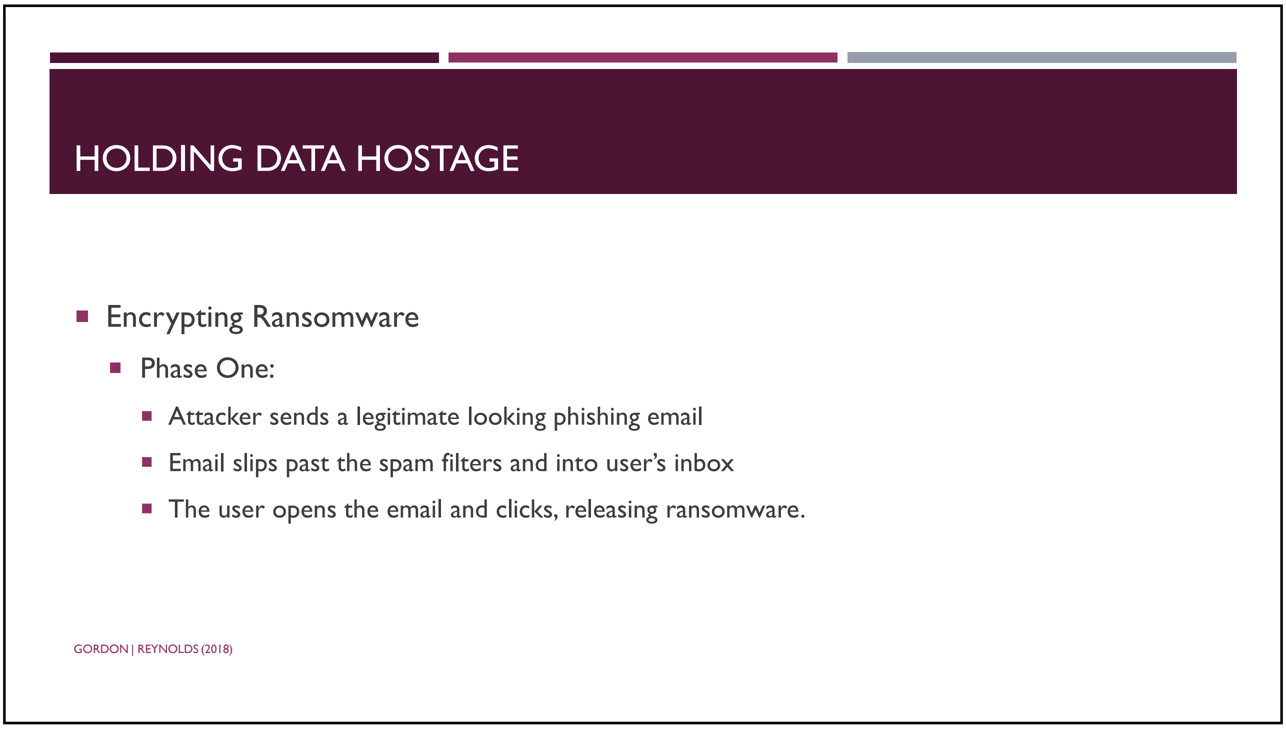
GORDON | REYNOLDS (2018)



HOLDING DATA HOSTAGE

- Extremely Profitable
  - Initially targeted home users, now infiltrating into corporations
  - Consequences could be grave:
    - Destroy all files on the system
    - Block access to the system
    - Encrypt files and stop applications

GORDON | REYNOLDS (2018)



HOLDING DATA HOSTAGE

- Encrypting Ransomware
  - Phase One:
    - Attacker sends a legitimate looking phishing email
    - Email slips past the spam filters and into user's inbox
    - The user opens the email and clicks, releasing ransomware.

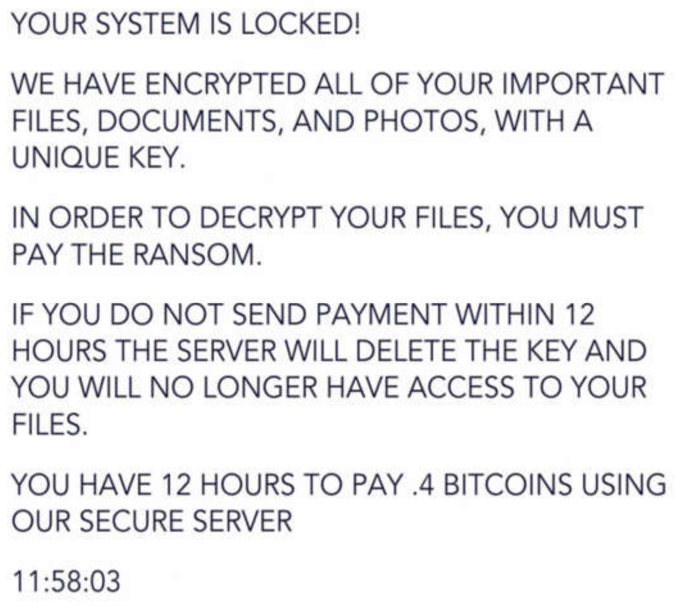
GORDON | REYNOLDS (2018)

HOLDING DATA HOSTAGE

- Encrypting Ransomware
  - Phase Two:
    - The ransomware attempts to execute and spawn child processes
    - Encrypts files and then communicates with C&C
    - Send encryption key and awaits further instruction
    - A message is then send from the C&C server

GORDON | REYNOLDS (2018)

HOLDING DATA HOSTAGE



YOUR SYSTEM IS LOCKED!

WE HAVE ENCRYPTED ALL OF YOUR IMPORTANT FILES, DOCUMENTS, AND PHOTOS, WITH A UNIQUE KEY.

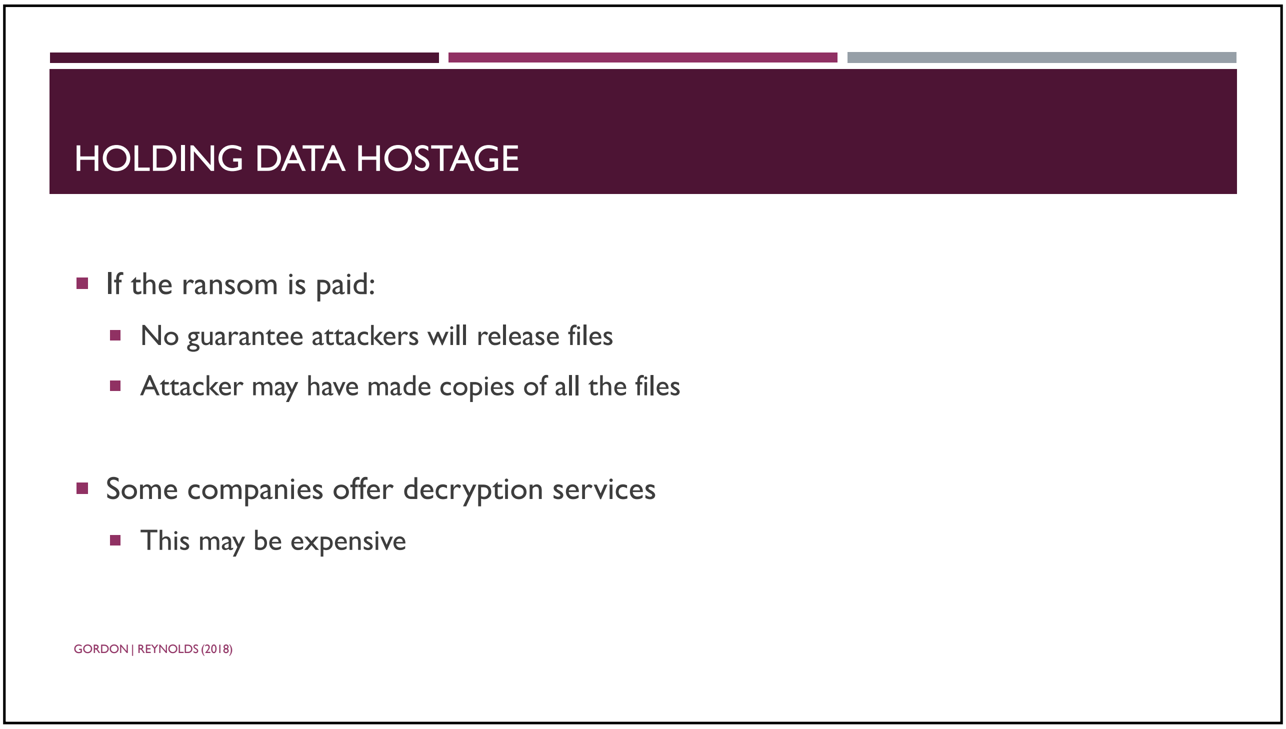
IN ORDER TO DECRYPT YOUR FILES, YOU MUST PAY THE RANSOM.

IF YOU DO NOT SEND PAYMENT WITHIN 12 HOURS THE SERVER WILL DELETE THE KEY AND YOU WILL NO LONGER HAVE ACCESS TO YOUR FILES.

YOU HAVE 12 HOURS TO PAY .4 BITCOINS USING OUR SECURE SERVER

11:58:03

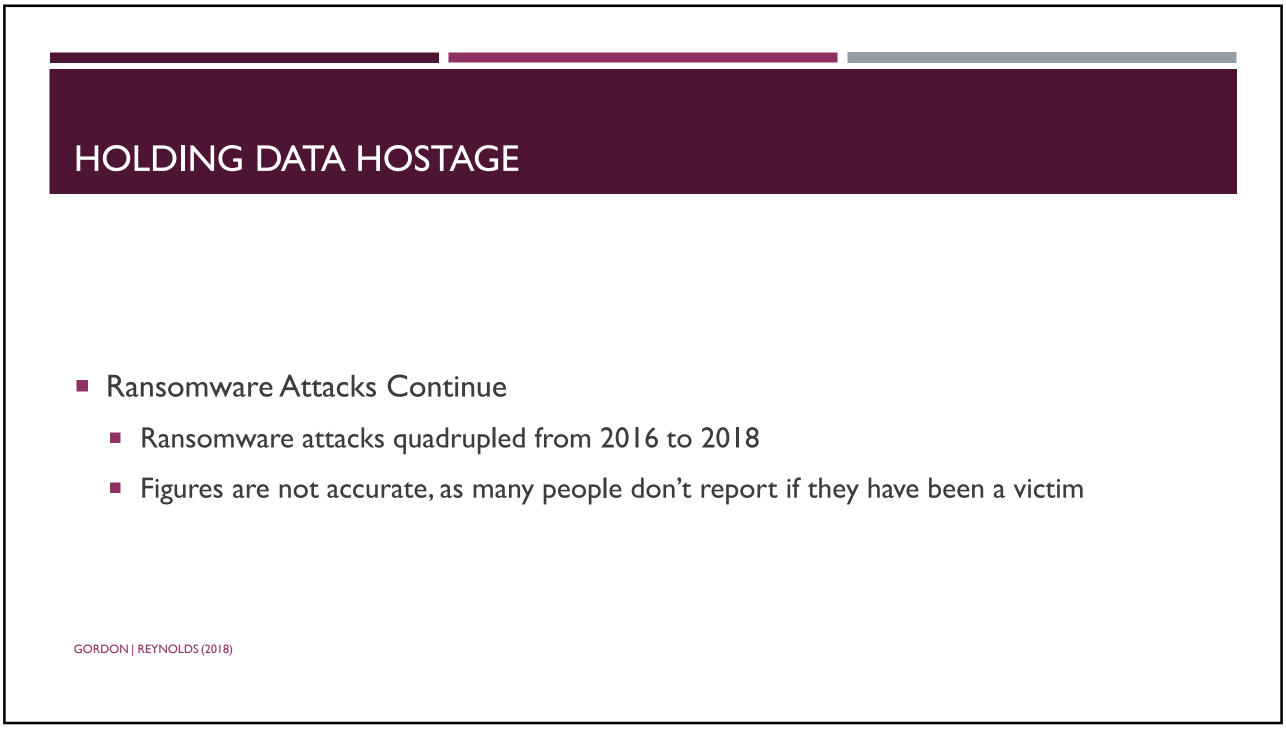
GORDON | REYNOLDS (2018)



HOLDING DATA HOSTAGE

- If the ransom is paid:
  - No guarantee attackers will release files
  - Attacker may have made copies of all the files
- Some companies offer decryption services
  - This may be expensive

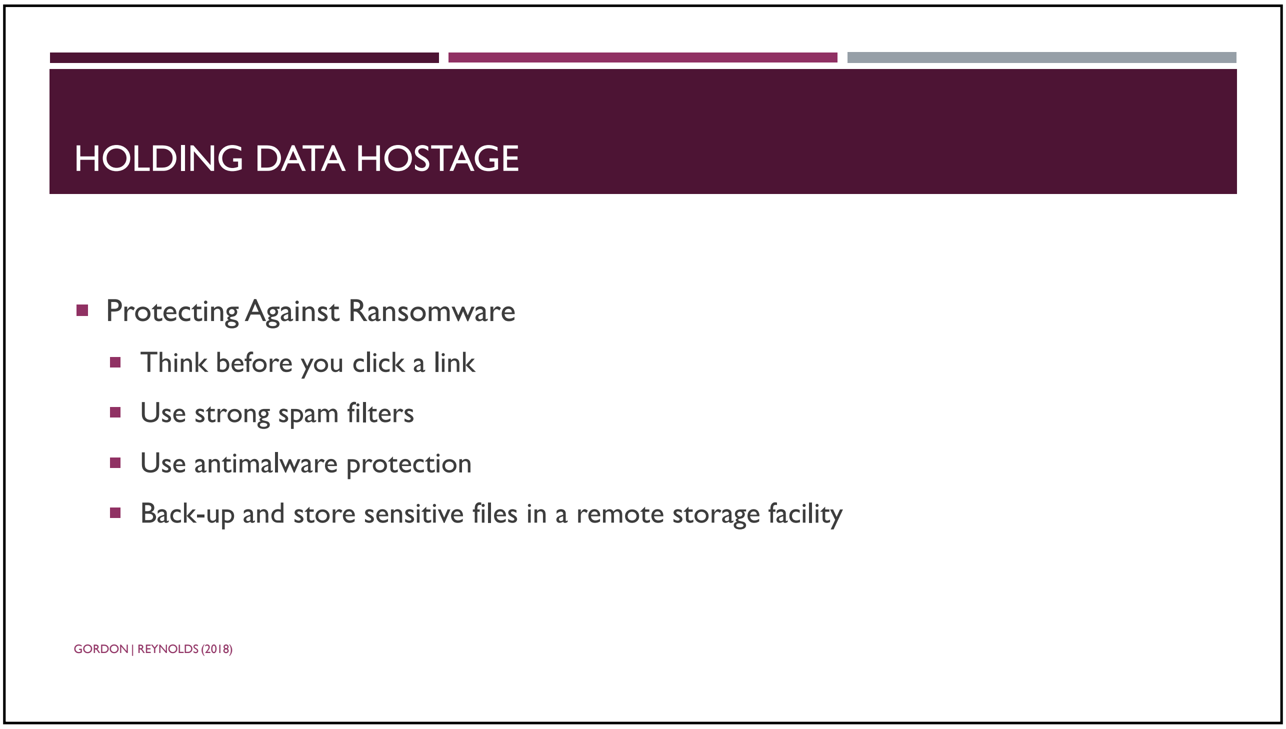
GORDON | REYNOLDS (2018)



HOLDING DATA HOSTAGE

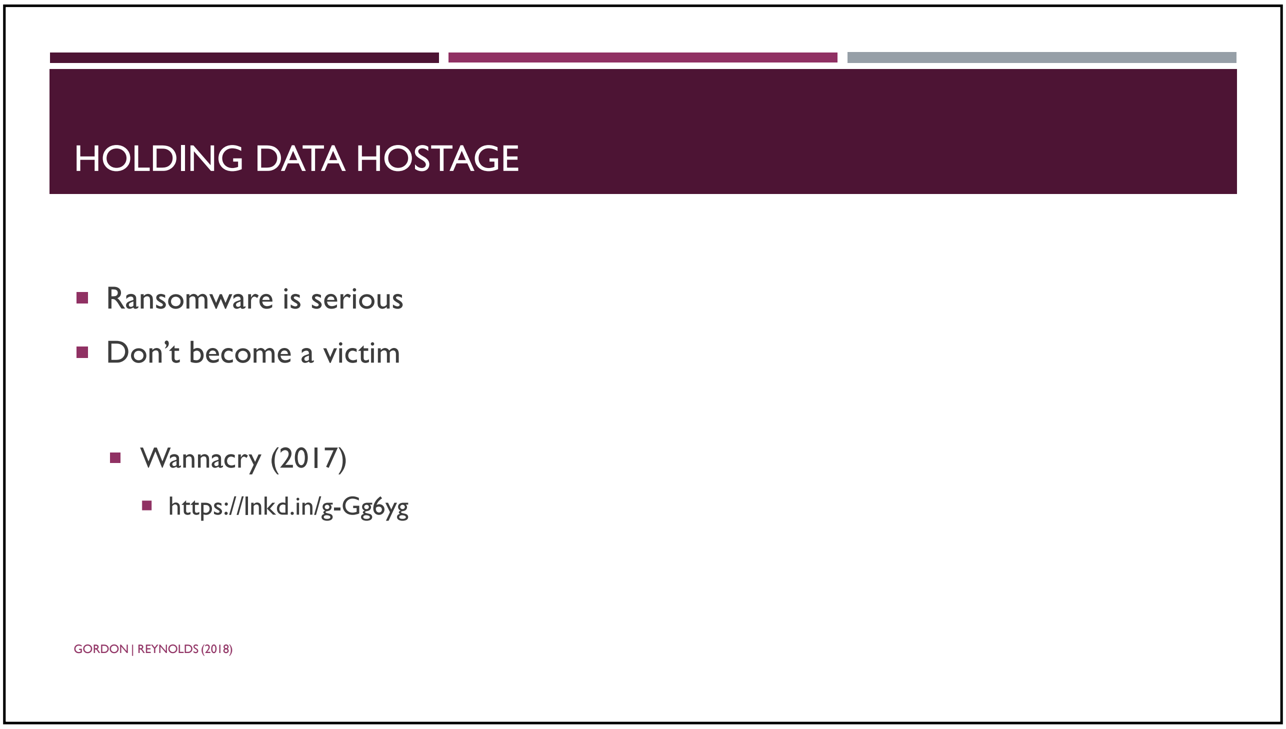
- Ransomware Attacks Continue
  - Ransomware attacks quadrupled from 2016 to 2018
  - Figures are not accurate, as many people don’t report if they have been a victim

GORDON | REYNOLDS (2018)



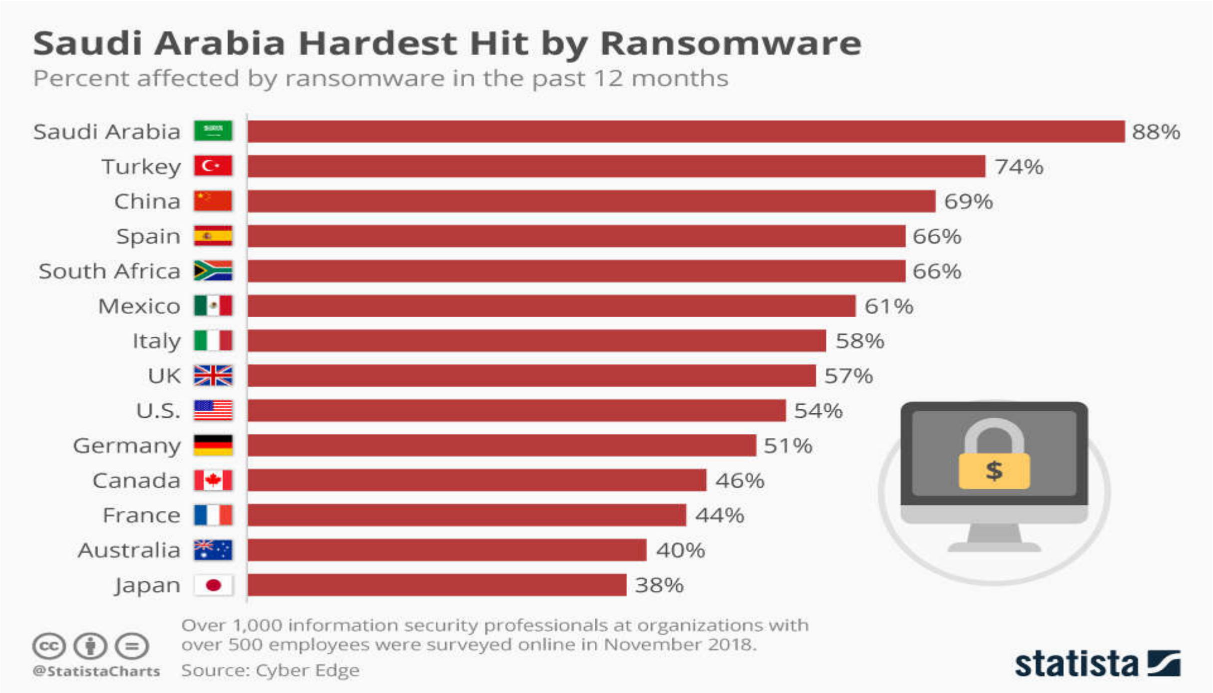
HOLDING DATA HOSTAGE

- Protecting Against Ransomware
  - Think before you click a link
  - Use strong spam filters
  - Use antimalware protection
  - Back-up and store sensitive files in a remote storage facility



HOLDING DATA HOSTAGE

- Ransomware is serious
- Don’t become a victim
  - Wannacry (2017)
    - https://lnkd.in/g-Gg6yg



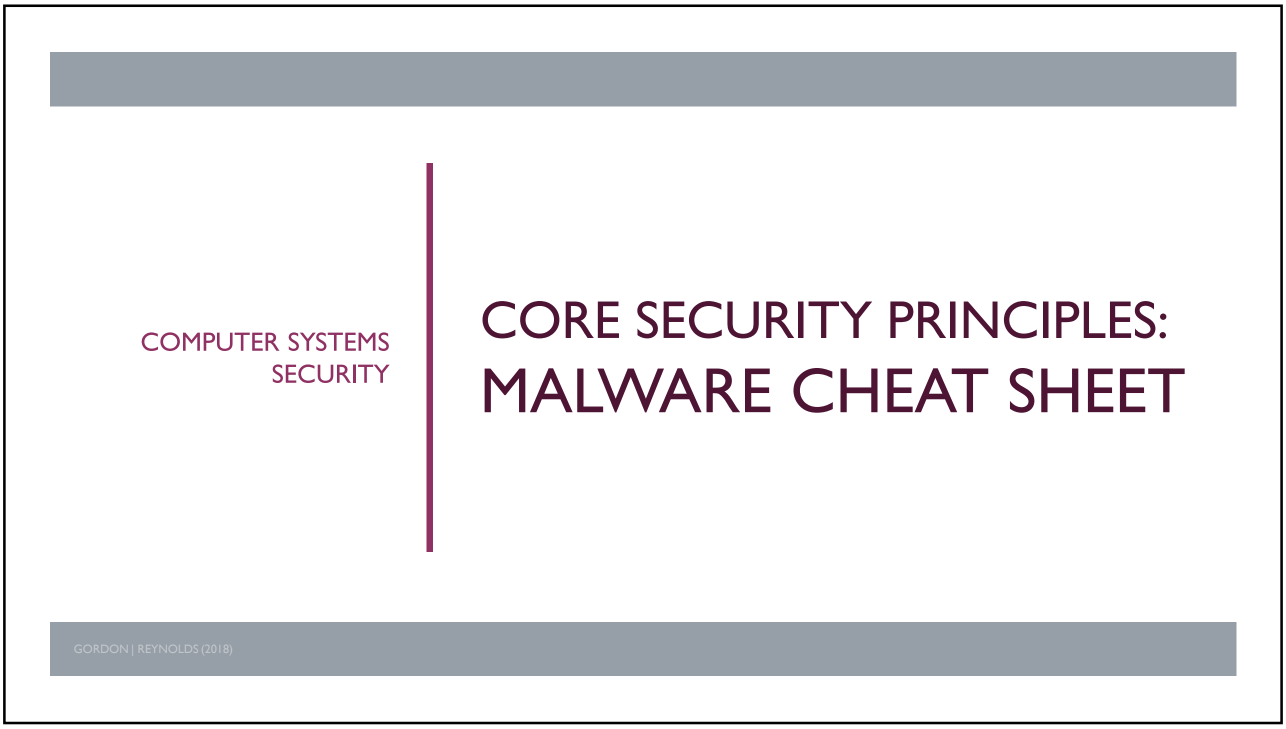
Over 1,000 information security professionals at organizations with over 500 employees were surveyed online in November 2018.

Source: Cyber Edge

HOLDING DATA HOSTAGE

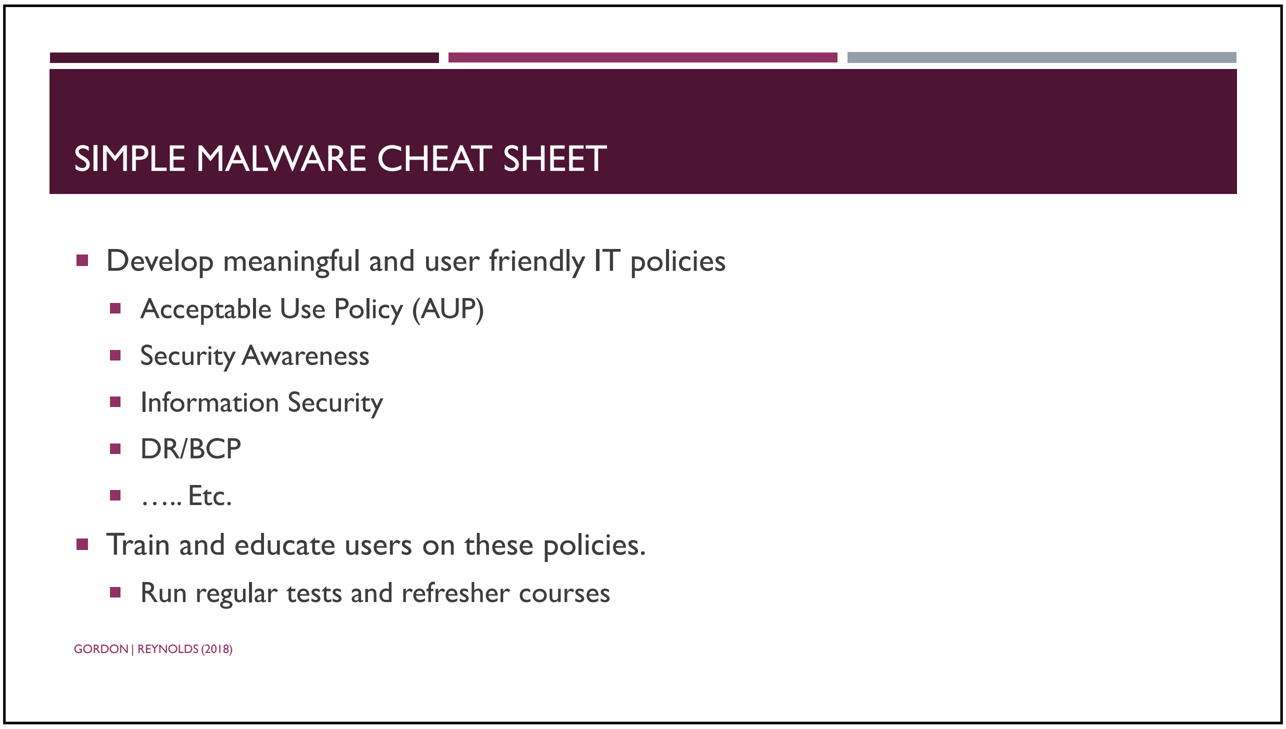
- Statistics on Ransomware
  - https://www.statista.com/topics/4136/ransomware/

GORDON | REYNOLDS (2018)



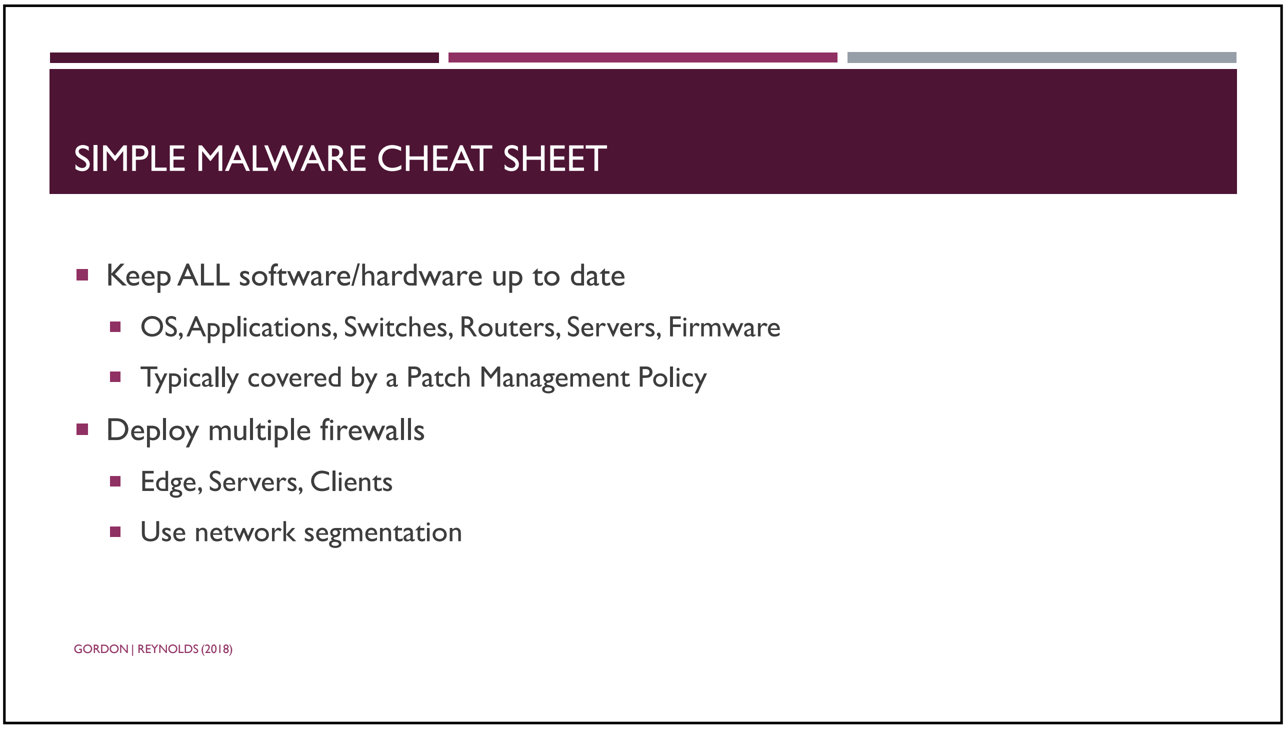
COMPUTER SYSTEMS SECURITY

CORE SECURITY PRINCIPLES: MALWARE CHEAT SHEET



SIMPLE MALWARE CHEAT SHEET

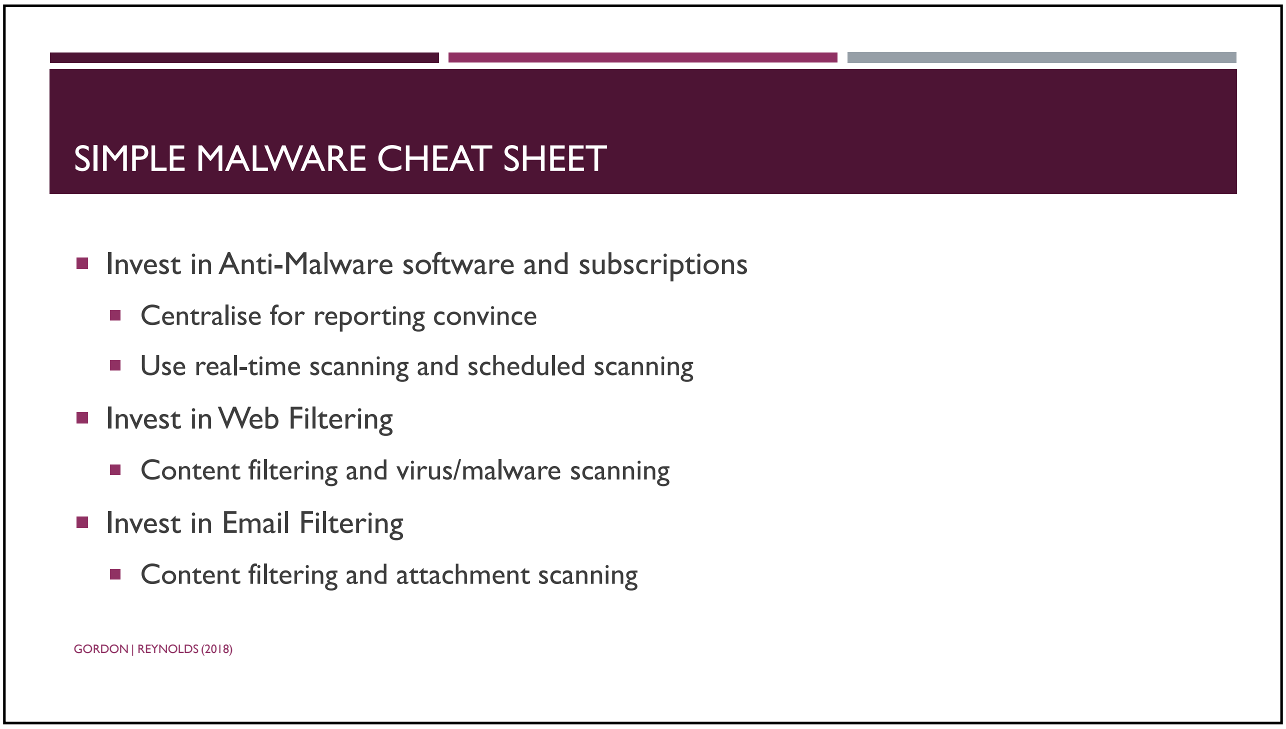
- Develop meaningful and user friendly IT policies
  - Acceptable Use Policy (AUP)
  - Security Awareness
  - Information Security
  - DR/BCP
  - ….. Etc.
- Train and educate users on these policies.
  - Run regular tests and refresher courses



SIMPLE MALWARE CHEAT SHEET

- Keep ALL software/hardware up to date
  - OS, Applications, Switches, Routers, Servers, Firmware
  - Typically covered by a Patch Management Policy
- Deploy multiple firewalls
  - Edge, Servers, Clients
  - Use network segmentation

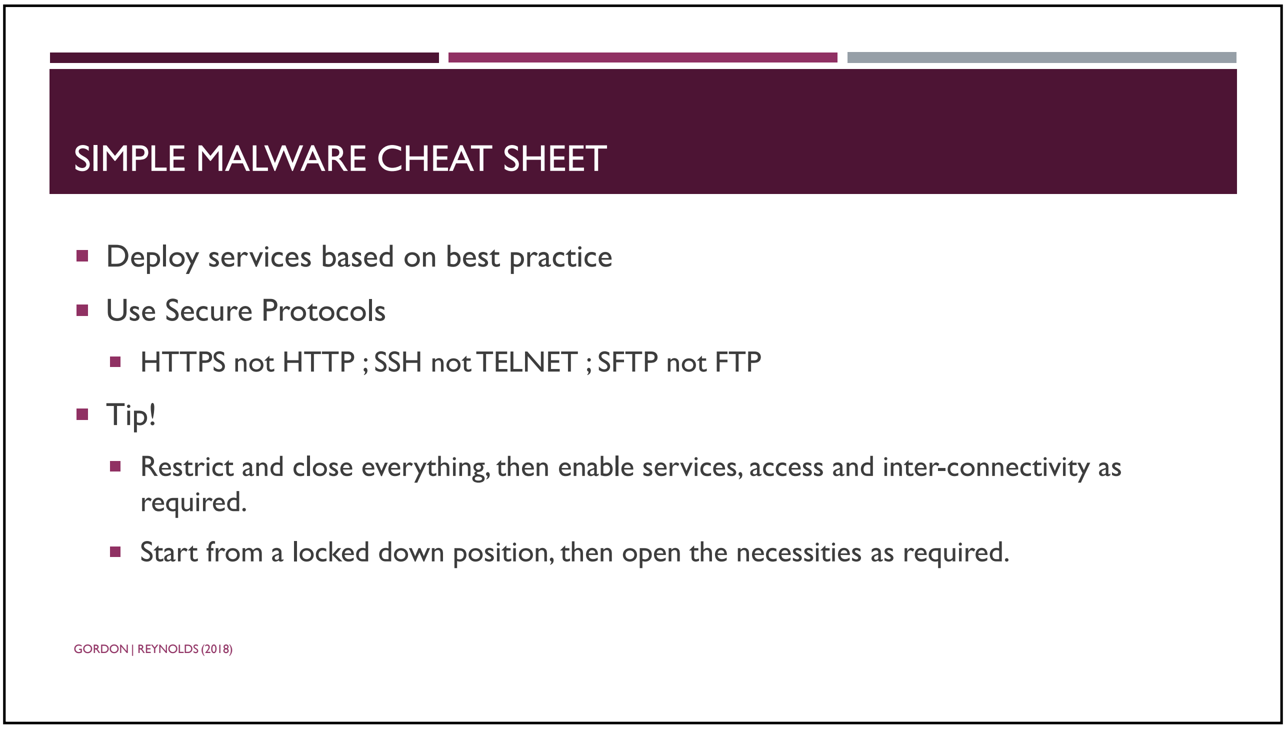
GORDON | REYNOLDS (2018)



SIMPLE MALWARE CHEAT SHEET

- Invest in Anti-Malware software and subscriptions
  - Centralise for reporting convince
  - Use real-time scanning and scheduled scanning
- Invest in Web Filtering
  - Content filtering and virus/malware scanning
- Invest in Email Filtering
  - Content filtering and attachment scanning

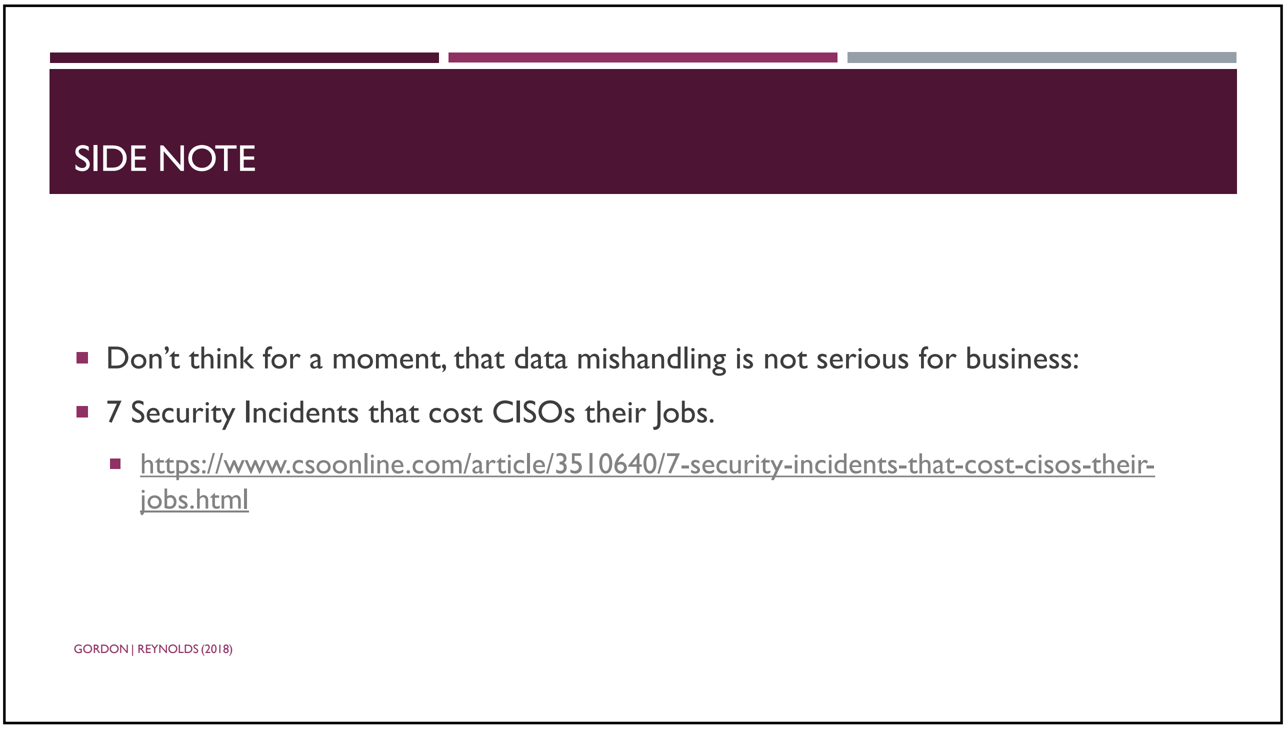
GORDON | REYNOLDS (2018)



SIMPLE MALWARE CHEAT SHEET

- Deploy services based on best practice
- Use Secure Protocols
  - HTTPS not HTTP ; SSH not TELNET ; SFTP not FTP
- Tip!
  - Restrict and close everything, then enable services, access and inter-connectivity as required.
  - Start from a locked down position, then open the necessities as required.

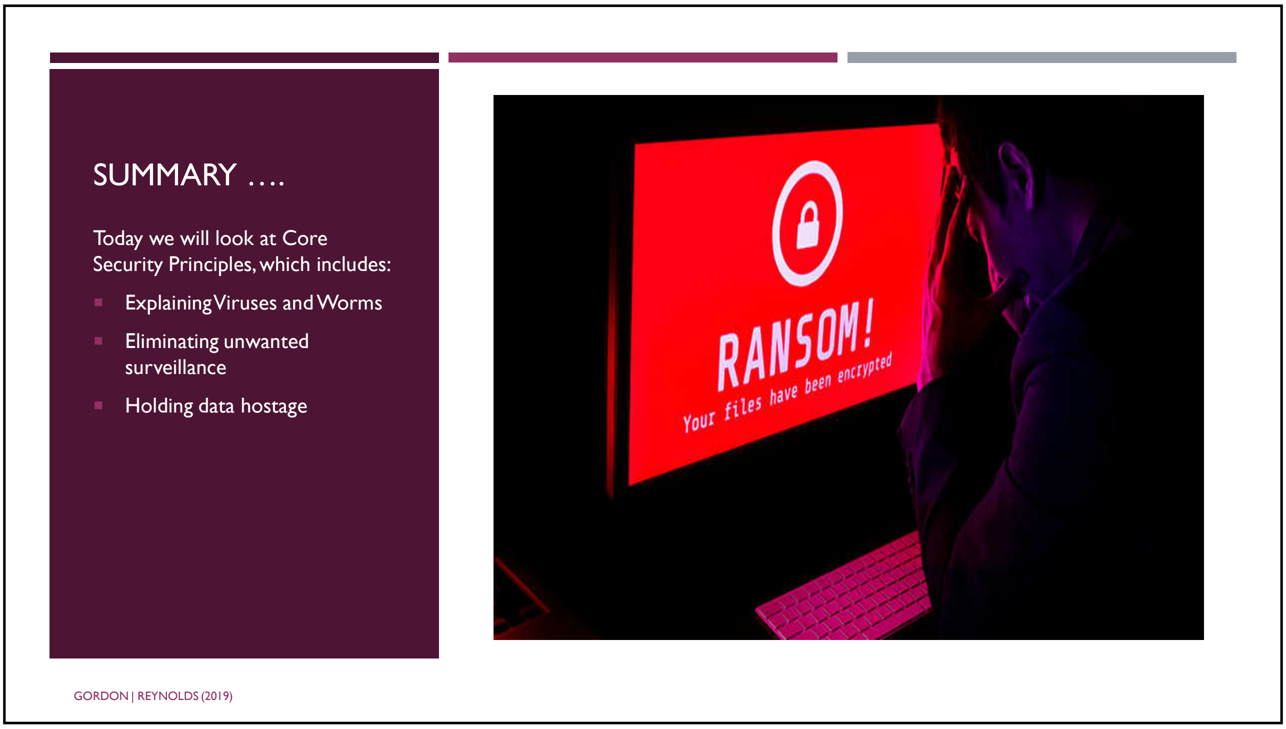
GORDON | REYNOLDS (2018)



SIDE NOTE

- Don't think for a moment, that data mishandling is not serious for business:
- 7 Security Incidents that cost CISOs their Jobs.
  - https://www.csoonline.com/article/3510640/7-security-incidents-that-cost-cisos-their-jobs.html

GORDON | REYNOLDS (2018)



SUMMARY ….

Today we will look at Core Security Principles, which includes:

- Explaining Viruses and Worms
- Eliminating unwanted surveillance
- Holding data hostage

RANSOM!
Your files have been encrypted

GORDON | REYNOLDS (2019)