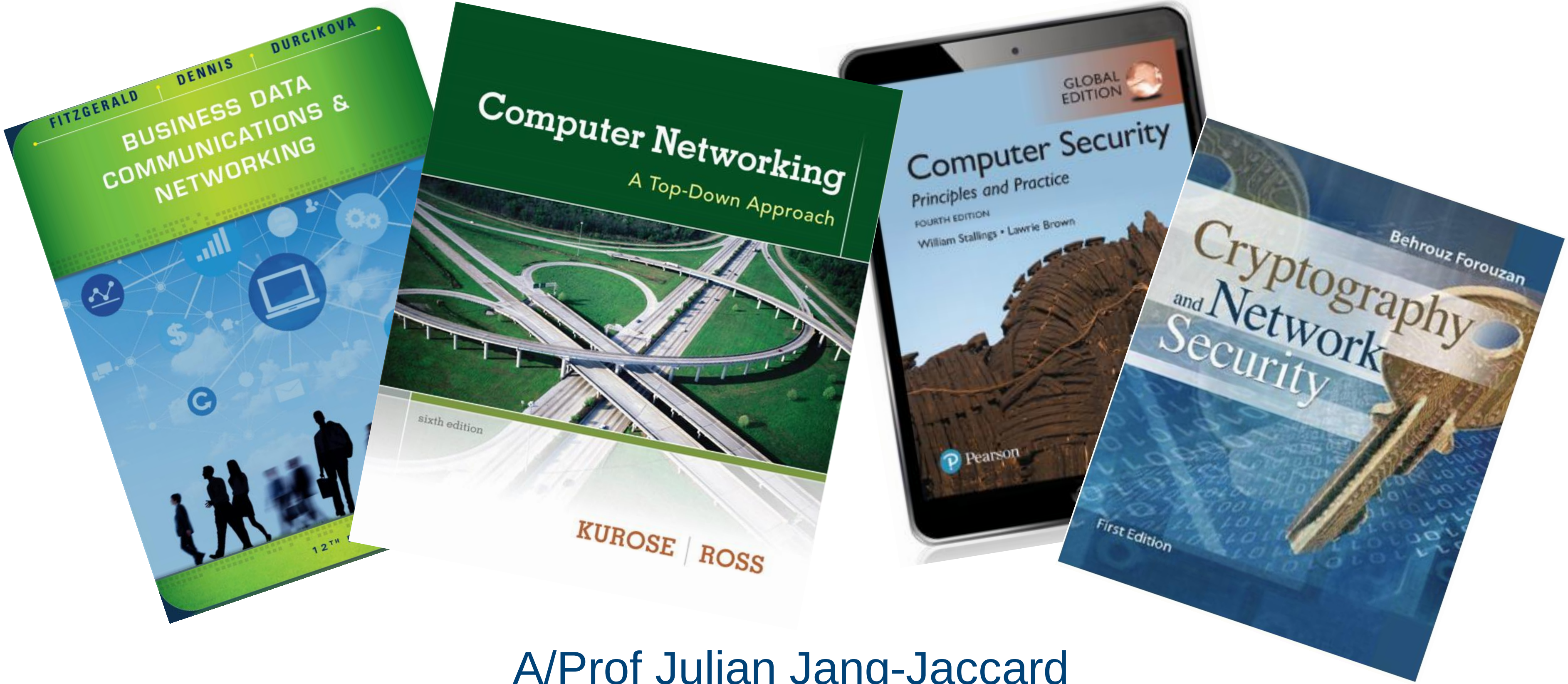
MASSEY UNIVERSITY
TE KUNENGA KI PŪREHUROA
UNIVERSITY OF NEW ZEALAND

Network, Security and Privacy

158.235



A/Prof Julian Jang-Jaccard

Introduction to Security

Why Security?

Why Need Security?

- Reliance on the use of electronic-based information processing, storage, and communication
- Day to day operations depend on the data and applications
- Data is now recognized as the most asset
  - Average value of organizational data and applications far exceeds cost of networks
- Organizations vulnerable due to dependency on computing and widely available Internet access to its resources

Difficulties in Defense

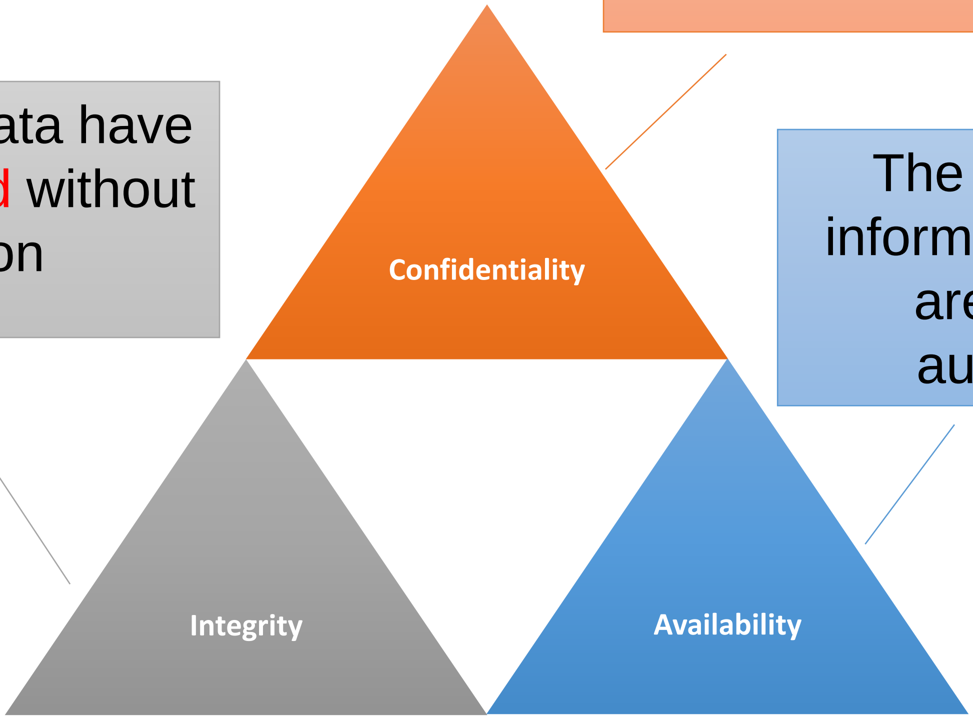
- Universally connected devices
  - Distributed Attacks
- Increased speed of attacks
  - Can scan millions devices to find weaknesses
  - Automated attack possible without human
- Greater sophistication of attacks
  - Complex and difficult (often exploiting internet protocols and applications) to detect and defense
- Availability and simplicity of attack tools
  - Cheap & easy to use attack tools
- Delays in security updating (patches)
  - Speed of new & modified virus spread is faster than security updates
- User confusion
  - Little or no information to guide users to make security decisions

MASSEY UNIVERSITY
TE KUNENGA KI PŪREHUROA
UNIVERSITY OF NEW ZEALAND

Introduction to Security

Security Goals

Goals of Security: CIA Triad



Protection of organizational data from unauthorized disclosure

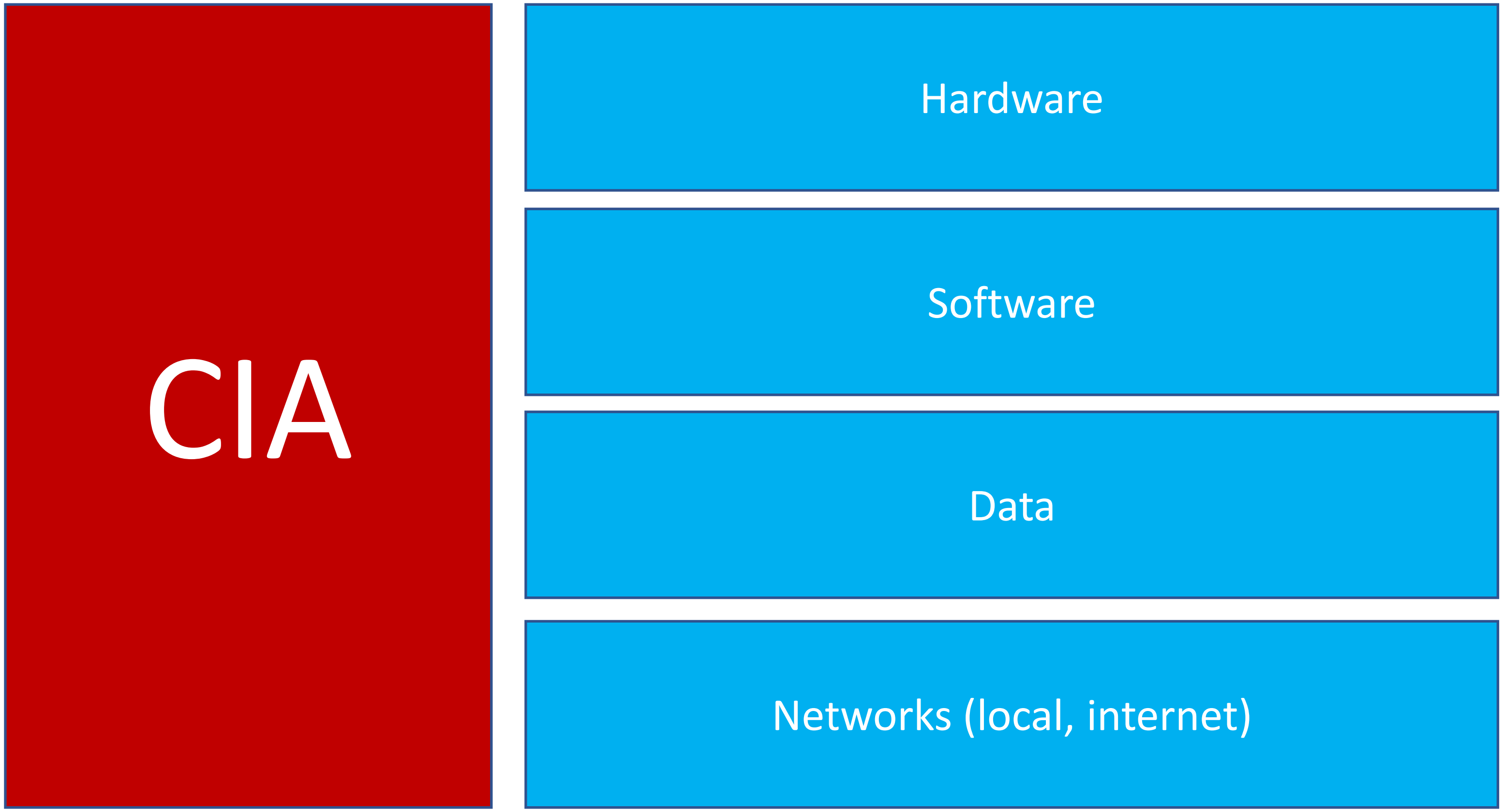
Assurance that data have not been modified without authorization

The degree to which information and systems are accessible to authorized users

Related Terms

- Authentication – proving who you are (did you send that message?)
- Authorization – checking if allowed to access an asset usually based upon who you are, something you know or something you possess (can I read Julian’s messages?)
- Non-repudiation -- cannot deny knowledge of an action done by a user (I never sent that message to Julian)

What are we trying to protect?



CIA

Hardware

Software

Data

Networks (local, internet)

Vulnerabilities, Threats and Attacks

- Categories of system resource vulnerabilities
  - Corrupted (loss of Integrity)
  - Leaky (loss of Confidentiality)
  - Unavailable or very slow (loss of Availability)
- Security threats
  - Capable of exploiting vulnerabilities
  - Represent potential security harm to an asset
- Security attacks
  - Passive – attempt to learn or make use of information from the system that does not affect system resources
  - Active – attempt to alter system resources or affect their operation
  - Insider – initiated by an entity inside the security parameter
  - Outsider – initiated from outside the perimeter

MASSEY UNIVERSITY
TE KUNENGA KI PŪREHUROA
UNIVERSITY OF NEW ZEALAND

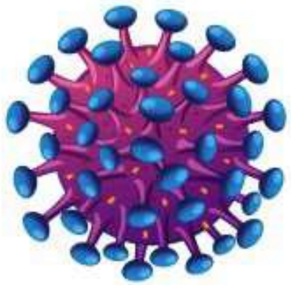
Introduction to Security

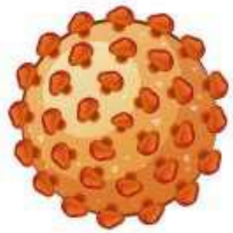
Security Attacks and Tools

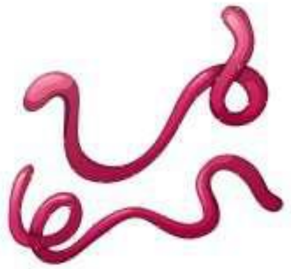
Malware

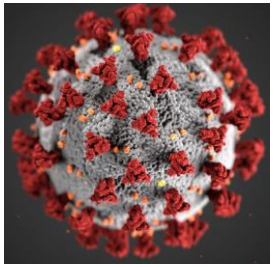
- Malware is short for "malicious software," also known as malicious code or "malcode.“
- Specifically designed to damage, disrupt, or gain unauthorized access to a computer system.
- Includes viruses, trojans, ransomware etc.,
- Can be distinguished from each other in terms of how they propagate and operate
- Most used attacking tool (APWG, 2017)

Viruses

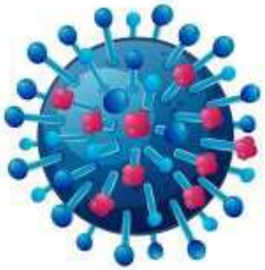

HIV


Hepatitis B


Ebola Virus


Covid-19

Adenovirus

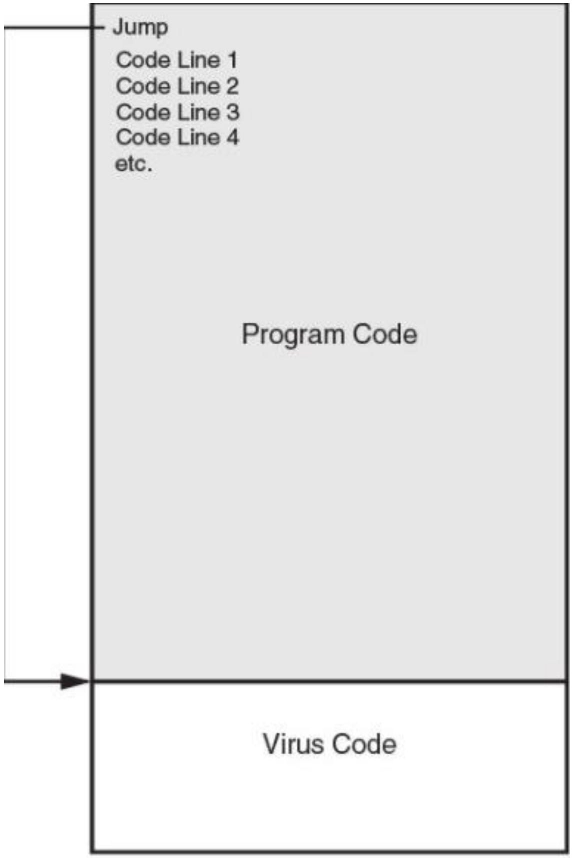

Influenza

Bacteriophage

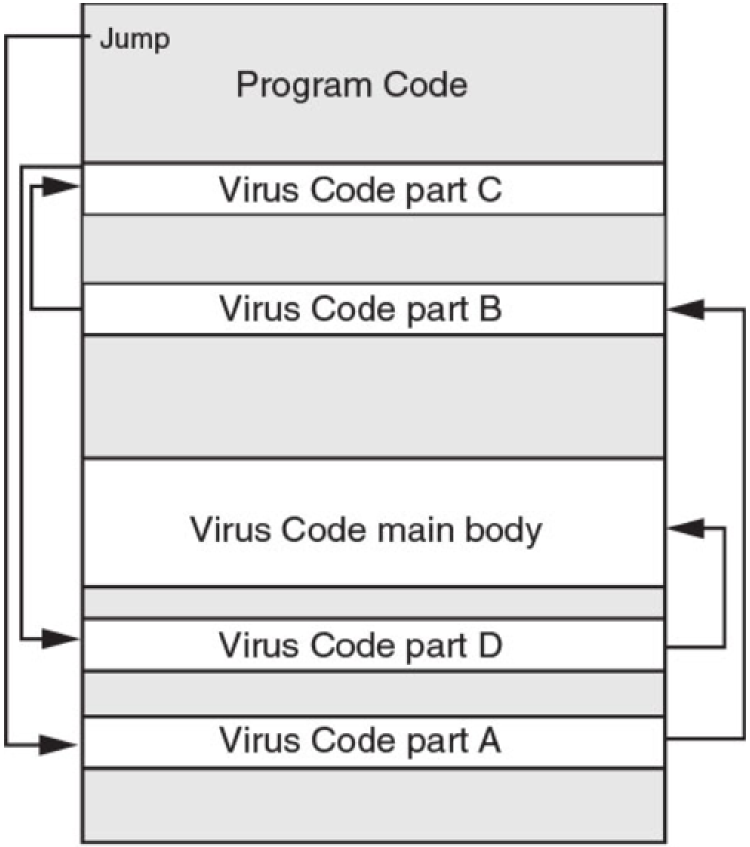
- Infective agent
- Multiplies within the living cells of a host
- Doesn’t have any purpose beyond replicating itself

Viruses

- Propagates by inserting a copy of itself into and becoming part of another program, (i.e., reproduce by infecting other files)
    - Insertion Phase is inserting itself into file
    - Execution phase is performing some (possibly null) action
    - Almost all viruses are attached to an executable file (and macros)
- Insertion phase must be present
    - Need not always be executed
- Require a host program for spreading

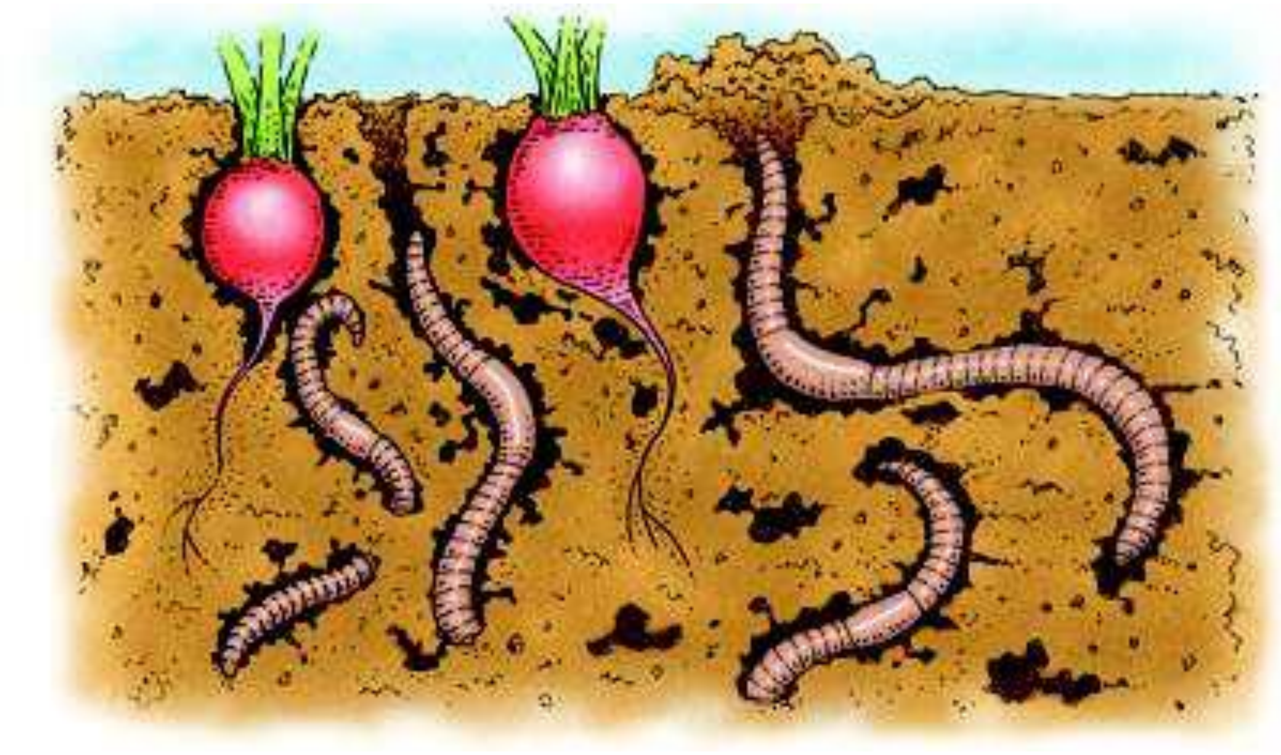


Appender Infection



Spilt Infection

Worms



- Worms follow tunnels
- Find vulnerable vegetables

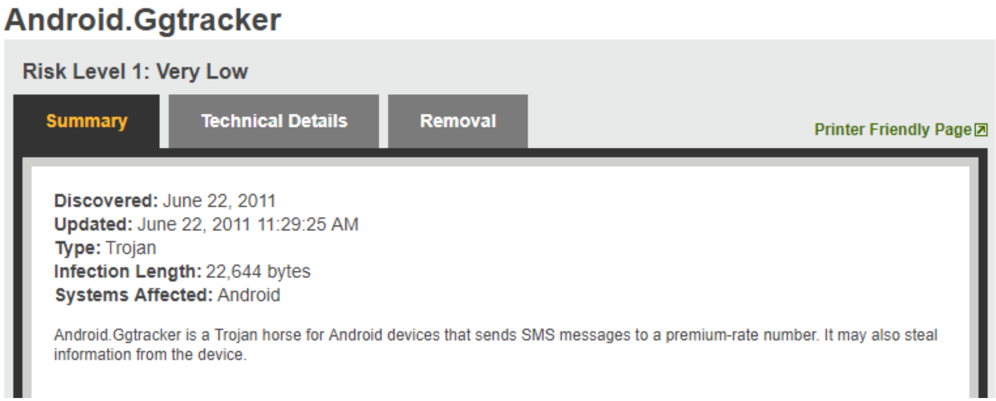
Worms

- Worms are standalone software and do not require a host program or human help to propagate
- worms either exploit a vulnerability on the target system or use some kind of social engineering to trick users into executing them
- A worm enters a computer through a vulnerability in the system and takes advantage of file-transport or information-transport features on the system, allowing it to travel unaided

MASSEY UNIVERSITY
TE KUNENGA KI PŪREHUROA
UNIVERSITY OF NEW ZEALAND

Trojan

- It is a harmful piece of software that looks legitimate
- Program with an overt purpose (known to user) and a covert purpose (unknown to user)
- Users are typically tricked into loading and executing it on their systems (e.g, video/audio files online)
- Example: Android malware (tracker for StarCraft 2 game)



Android.Ggtracker

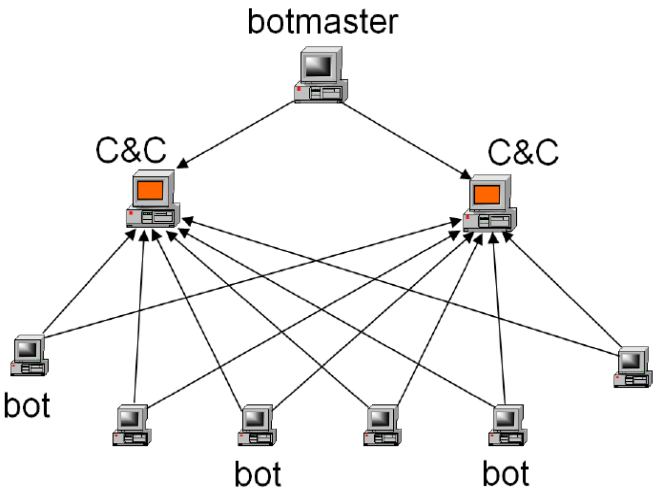
Risk Level 1: Very Low

Discovered: June 22, 2011
Updated: June 22, 2011 11:29:25 AM
Type: Trojan
Infection Length: 22,644 bytes
Systems Affected: Android

Android.Ggtracker is a Trojan horse for Android devices that sends SMS messages to a premium-rate number. It may also steal information from the device.

Bots

- "Bot" is derived from the word "robot" and is an automated process that interacts with other network services.
- A malicious bot is self-propagating malware designed to infect a host and connect back to a central server or servers that act as a command and control (C&C) center for an entire network of compromised devices, or "botnet."
- With a botnet, attackers can launch broad-based, "remote-control," flood-type attacks against their target(s).

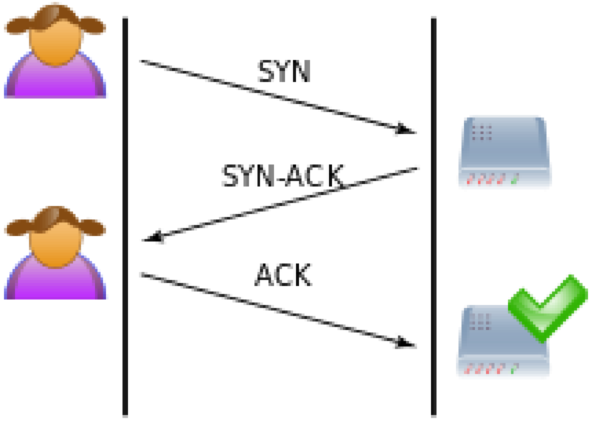


https://www.usenix.org/legacy/event/hotbots07/tech/full_papers/wang/wang_html/

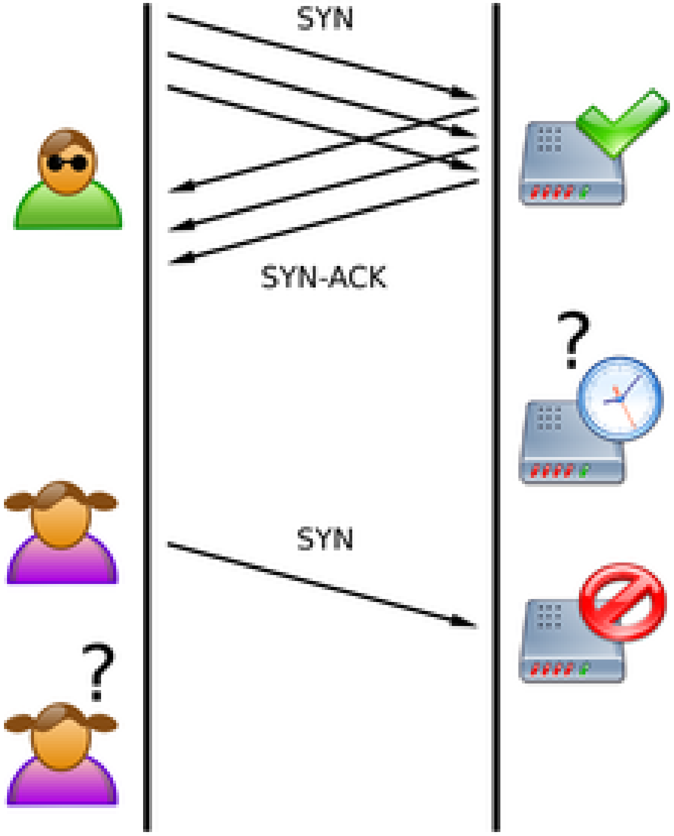
Distributed Denial-Of-Service (DDOS)

- DDoS attack
  - launched from multiple connected devices that are distributed across the Internet.
  - These multi-person, multi-device barrages are generally harder to deflect, mostly due to the sheer volume of devices involved.
- Command zombies(e.g., bots) to stage a coordinated attack on the victim
- Overwhelm victim with traffic arriving from thousands of different sources
- DDoS often exploits networking protocols
  - SYN flood: send lots of “open TCP connection” requests with spoofed source addresses
  - UDP flood: exhaust bandwidth by sending thousands of bogus UDP packets
  - Smurf: ICMP echo request to broadcast address with spoofed victim’s address as source
  - HTTP request flood: flood server with legitimate looking requests for Web content

Example: SYN flood



Normal scenario

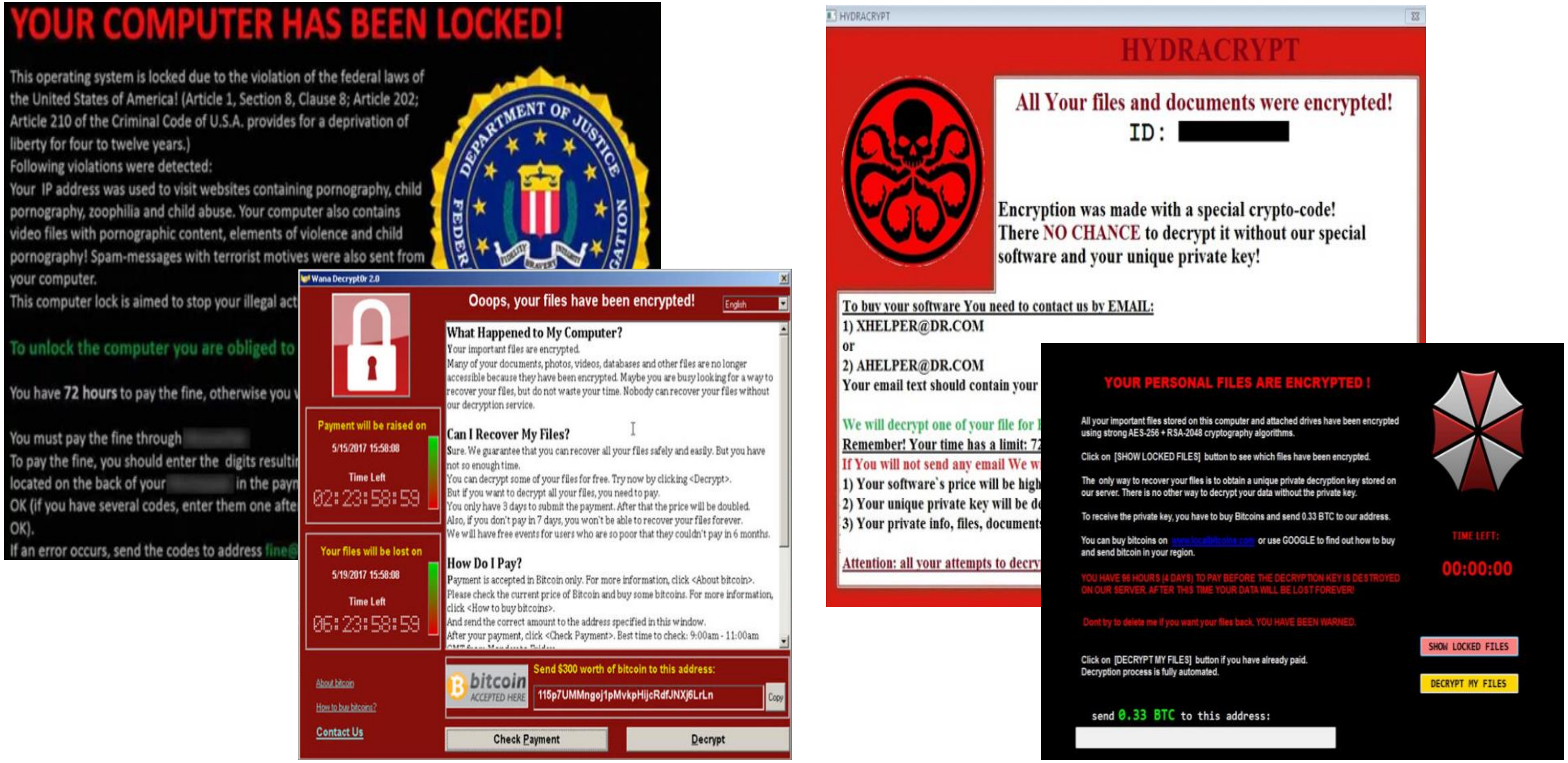


Attack scenario

https://en.wikipedia.org/wiki/SYN_flood

Ransomware

- A type of malicious software designed to block access to a computer system until a sum of money is paid.



YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)
Following violations were detected:
Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.
This computer lock is aimed to stop your illegal act

To unlock the computer you are obliged to

You have 72 hours to pay the fine, otherwise you

You must pay the fine through [redacted]
To pay the fine, you should enter the digits resulti
located on the back of your [redacted] in the payn
OK (if you have several codes, enter them one afte
OK).
If an error occurs, send the codes to address fine@

Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

Payment will be raised on
5/15/2017 15:58:08
Time Left
02:23:58:59

Your files will be lost on
5/19/2017 15:58:08
Time Left
06:23:58:59

What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

HYDRACRYPT

HYDRACRYPT

All Your files and documents were encrypted!
ID: [redacted]

Encryption was made with a special crypto-code!
There NO CHANCE to decrypt it without our special software and your unique private key!

To buy your software You need to contact us by EMAIL:
1) XHELPER@DR.COM
or
2) AHELPER@DR.COM
Your email text should contain your

We will decrypt one of your file for
Remember! Your time has a limit: 72
If You will not send any email We wi
1) Your software`s price will be high
2) Your unique private key will be de
3) Your private info, files, document

Attention: all your attempts to decry

YOUR PERSONAL FILES ARE ENCRYPTED !

All your important files stored on this computer and attached drives have been encrypted using strong AES-256 + RSA-2048 cryptography algorithms.

Click on [SHOW LOCKED FILES] button to see which files have been encrypted.

The only way to recover your files is to obtain a unique private decryption key stored on our server. There is no other way to decrypt your data without the private key.

To receive the private key, you have to buy Bitcoins and send 0.33 BTC to our address.

You can buy bitcoins on www.localbitcoins.com or use GOOGLE to find out how to buy and send bitcoin in your region.

YOU HAVE 96 HOURS (4 DAYS) TO PAY BEFORE THE DECRYPTION KEY IS DESTROYED ON OUR SERVER. AFTER THIS TIME YOUR DATA WILL BE LOST FOREVER!

Dont try to delete me if you want your files back. YOU HAVE BEEN WARNED.

Click on [DECRYPT MY FILES] button if you have already paid.
Decryption process is fully automated.

send 0.33 BTC to this address:

TIME LEFT:
00:00:00

Ransomware

Factsheet

- Appeared May 2017
- Affected more than 230,000 computers across 150 countries
- Indirect losses reach USD$4 billion

- Affected: Airlines (Boeing, LATAM), Railways (Germany, Russia), Telcom (Portugal, Saudi Arabia, Spain, Hungary, South Africa), Cars (Japan), Government Bodies (Russia, China, Russia), Hospitals (National Health Services, UK

Factsheet

- Year active 2016 – 2017
- Said to be most destructive cyberattack ever
- Most affected countries: Ukraine (80% hit), Germany (9%)
- Politically motivated

- Affected: Several Ukrainian ministries, banks and metro systems, including nuclear power plant
- Put the whole nation of Ukraine on hold for a few days

Phases of Ransomware

1. Infection and installation

- 97% of phishing emails deliver ransomware

2. Command and control

- Often utilizes botnet to infect as many computers as possible

3. Selection of file targets

- Family photos, business documents

4. Encryption

- Difficult to decrypt without super (or quantum) computer

5. Extortion

- 70% of infected businesses have paid the ransom, range from $200 – 10,000

Cyber Warfare

- May 2007: DDoS attacks on Estonia after government relocated Soviet-era war monument
- Aug 2008: similar attack on Georgia during the war between Russia and Georgia
- June 2017: DDoS + Ransomeware Petya targeting Ukrainian organizations (banks, ministries, newspapers, and electricity firms etc.,)

AP

MASSEY UNIVERSITY
TE KUNENGA KI PŪREHUROA
UNIVERSITY OF NEW ZEALAND

Introduction to Security

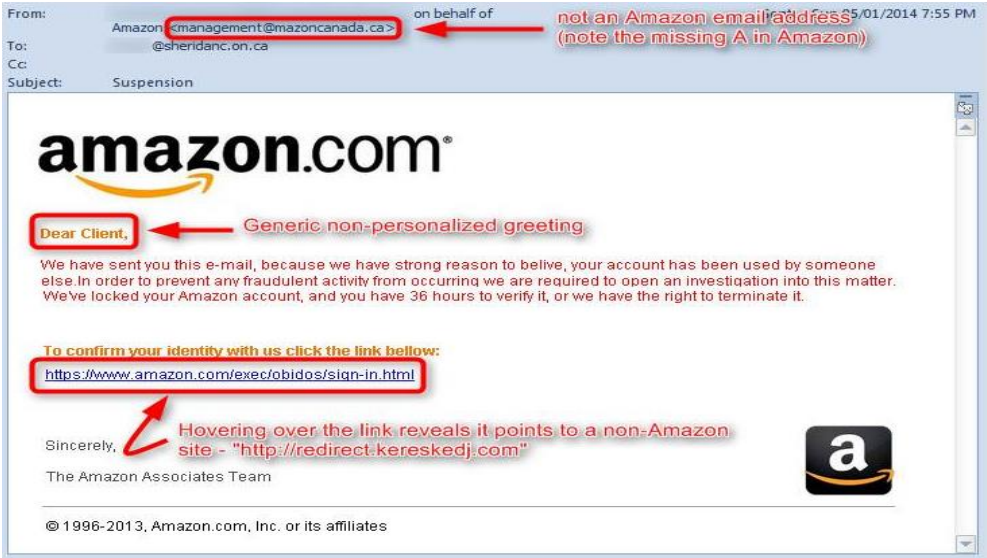
Attack Propagation

Spam

- Act of sending irrelevant, inappropriate and unsolicited messages
- Prolific due to low barrier to entry
- Estimated figure for spam messages is around seven trillion (APWG, 2011)
  - (e.g., lost productivity and fraud, and extra capacity needed to cope with the spam)
- Between 88–92% of email messages carried spam*
- Unsolicited Electronic Messages Act 2007 (NZ)
  - IMG ordered to pay $120 000 for sending spam via email and text messages to half million new Zealander

Phishing

- Act of attempting to acquire sensitive information by masquerading as a trustworthy entity
- Deceives users into visiting a malicious web site claiming to be from legitimate businesses and agencies
- Unsuspecting user enters private information in the malicious web site which is then subsequently used by malicious criminals.



From: [redacted] on behalf of Amazon <management@mazoncanada.ca>
To: [redacted] @sheridanc.on.ca
Cc:
Subject: Suspension

not an Amazon email address (note the missing A in Amazon)

25/01/2014 7:55 PM

amazon.com

Dear Client,

Generic non-personalized greeting

We have sent you this e-mail, because we have strong reason to belive, your account has been used by someone else.In order to prevent any fraudulent activity from occurring we are required to open an investigation into this matter. We've locked your Amazon account, and you have 36 hours to verify it, or we have the right to terminate it.

To confirm your identity with us click the link bellow:

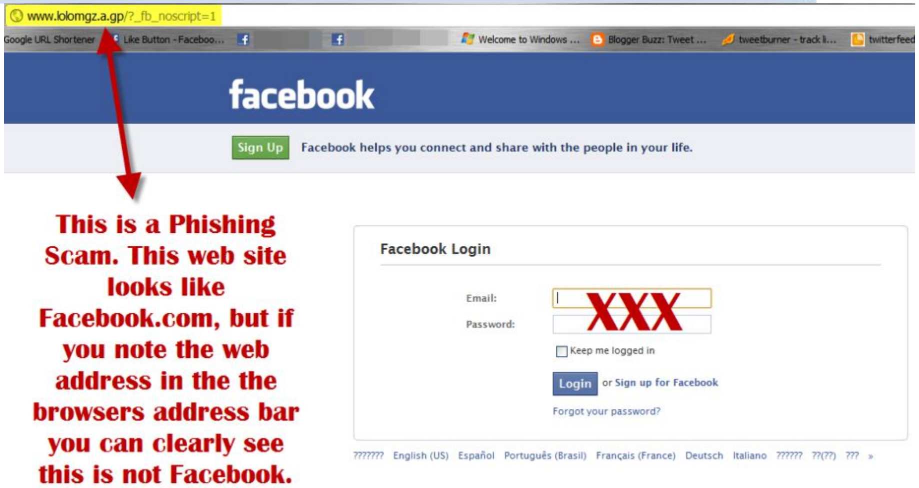
https://www.amazon.com/exec/obidos/sign-in.html

Hovering over the link reveals it points to a non-Amazon site - "http://redirect.kereskedj.com"

Sincerely,

The Amazon Associates Team

© 1996-2013, Amazon.com, Inc. or its affiliates



www.lolomgz.a.gp/?_fb_noscript=1

facebook

Sign Up Facebook helps you connect and share with the people in your life.

This is a Phishing Scam. This web site looks like Facebook.com, but if you note the web address in the the browsers address bar you can clearly see this is not Facebook.

Facebook Login

Email: XXX
Password:

□ Keep me logged in

Login or Sign up for Facebook

Forgot your password?

??????? English (US) Español Português (Brasil) Français (France) Deutsch Italiano ?????? ??(??) ??? »

Phishing Variations

- Spear Phishing
  - Targets only specific users
  - Customized to the recipients including their names and personal info to make it appear legitimate
- Whaling
  - Going after “big fish” e.g., wealthy individuals or senior executives
  - Highly tuned message
- Vishing (also known as “Voice Phishing”)
  - Attacker calls a victim masquerading to be from a trusted third party e.g., bank manager

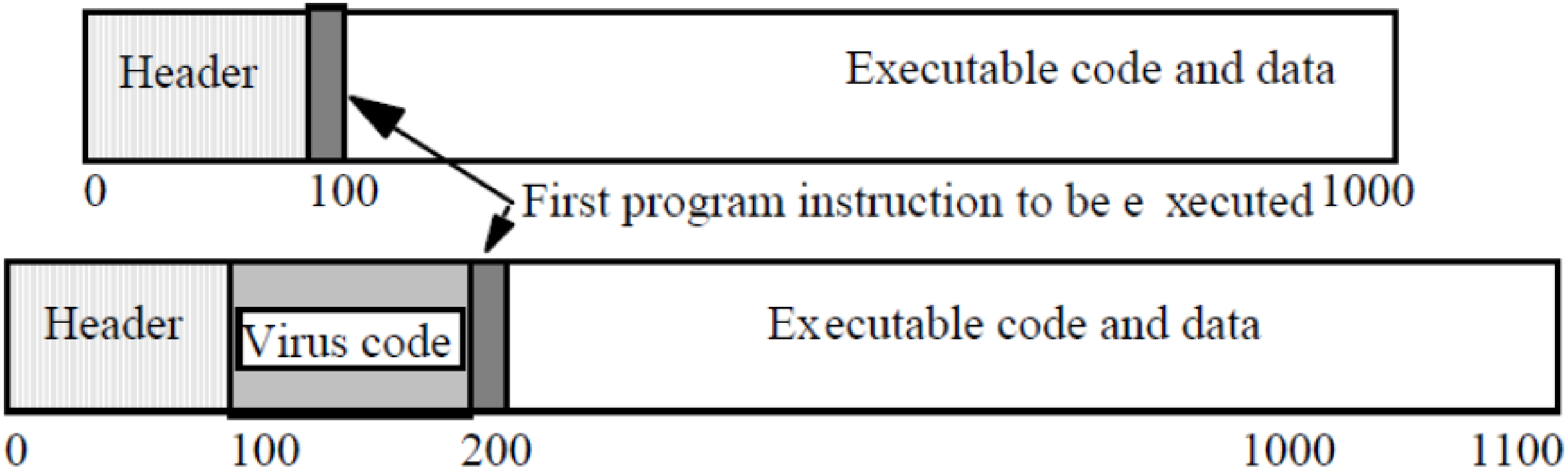
Drive-by-download

- Visit a website
  - Legitimate site that has been hacked
  - Evil site arrived at via a link
- Websites with popular content
  - Games: 60% of websites contain executable content, one-third contain at least one malicious executable
  - Celebrities, adult content, everything except news
- Code on site exploits vulnerability in web browser
- Drops malware onto your machine

Introduction to Security

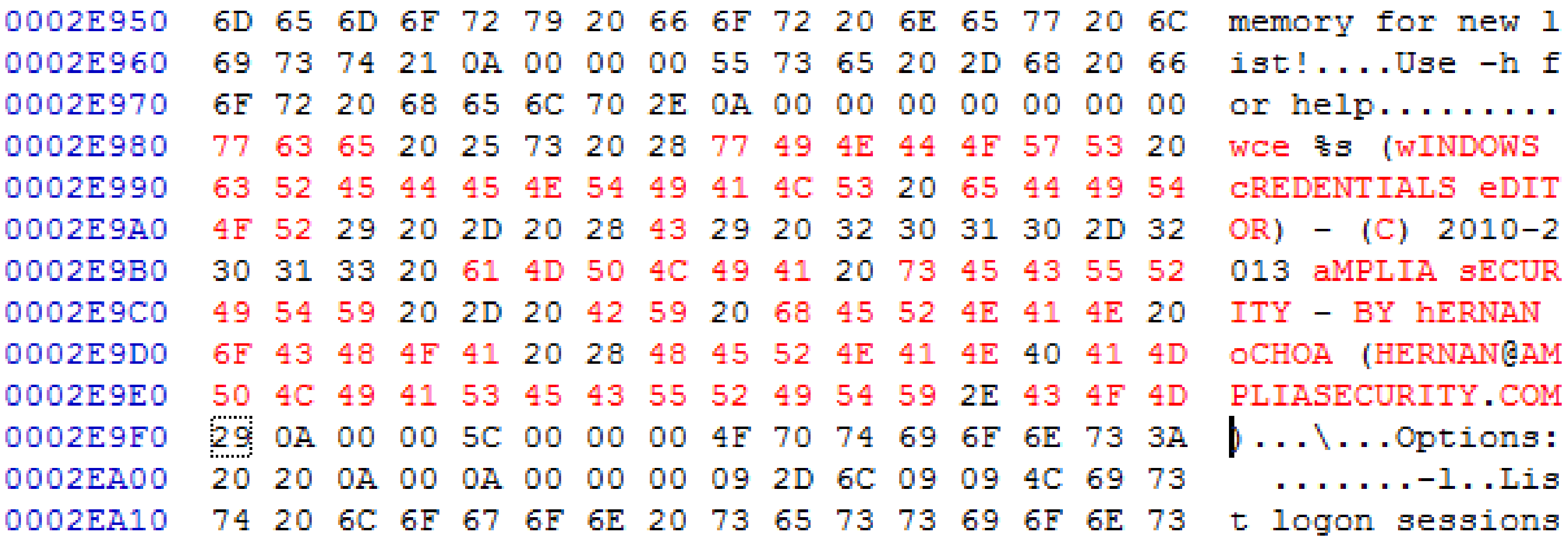
Anti-malware

Integrity Checkers



- Viruses make size of file grow
- Computer keeps a list of the lengths
- Periodically checks against the list
- Any unexpected change indicates a problem

Signature Detection

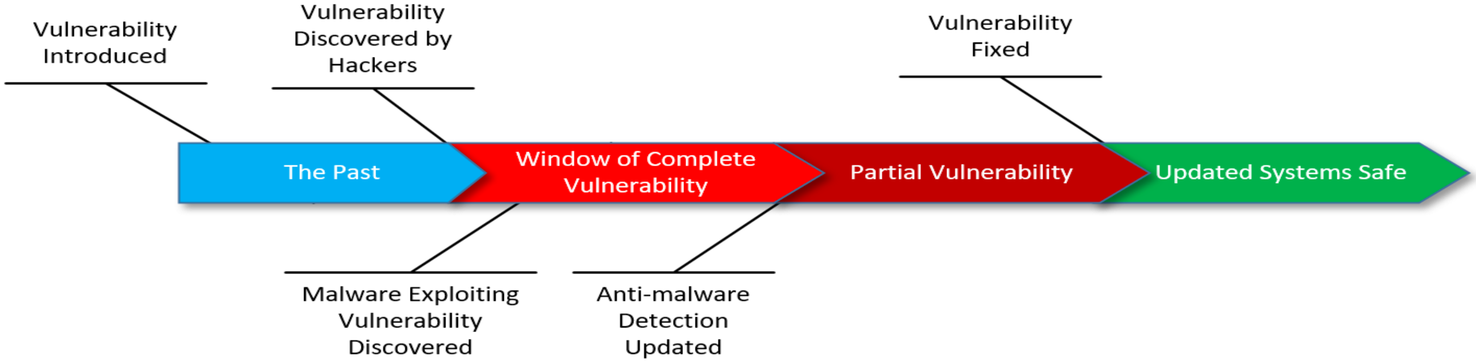


```
0002E950   6D 65 6D 6F 72 79 20 66 6F 72 20 6E 65 77 20 6C   memory for new l
0002E960   69 73 74 21 0A 00 00 00 55 73 65 20 2D 68 20 66   ist!....Use -h f
0002E970   6F 72 20 68 65 6C 70 2E 0A 00 00 00 00 00 00 00   or help.........
0002E980   77 63 65 20 25 73 20 28 77 49 4E 44 4F 57 53 20   wce %s (wINDOWS 
0002E990   63 52 45 44 45 4E 54 49 41 4C 53 20 65 44 49 54   cREDENTIALS eDIT
0002E9A0   4F 52 29 20 2D 20 28 43 29 20 32 30 31 30 2D 32   OR) - (C) 2010-2
0002E9B0   30 31 33 20 61 4D 50 4C 49 41 20 73 45 43 55 52   013 aMPLIA sECUR
0002E9C0   49 54 59 20 2D 20 42 59 20 68 45 52 4E 41 4E 20   ITY - BY hERNAN 
0002E9D0   6F 43 48 4F 41 20 28 48 45 52 4E 41 4E 40 41 4D   oCHOA (HERNAN@AM
0002E9E0   50 4C 49 41 53 45 43 55 52 49 54 59 2E 43 4F 4D   PLIASECURITY.COM
0002E9F0   29 0A 00 00 5C 00 00 00 4F 70 74 69 6F 6E 73 3A   )...\...Options:
0002EA00   20 20 0A 00 0A 00 00 00 09 2D 6C 09 09 4C 69 73     .......-l..Lis
0002EA10   74 20 6C 6F 67 6F 6E 20 73 65 73 73 69 6F 6E 73   t logon sessions
```

- Database of malware signatures (sometimes called DAT files).
- Search for bit pattern.
- Requires regular updates.
- Limited to detection of known malware.

Zero Day Exploits

- A zero-day exploit is an attack that exploits a previously unknown security vulnerability


Vulnerability Introduced
Vulnerability Discovered by Hackers
Vulnerability Fixed
The Past
Window of Complete Vulnerability
Partial Vulnerability
Updated Systems Safe
Malware Exploiting Vulnerability Discovered
Anti-malware Detection Updated

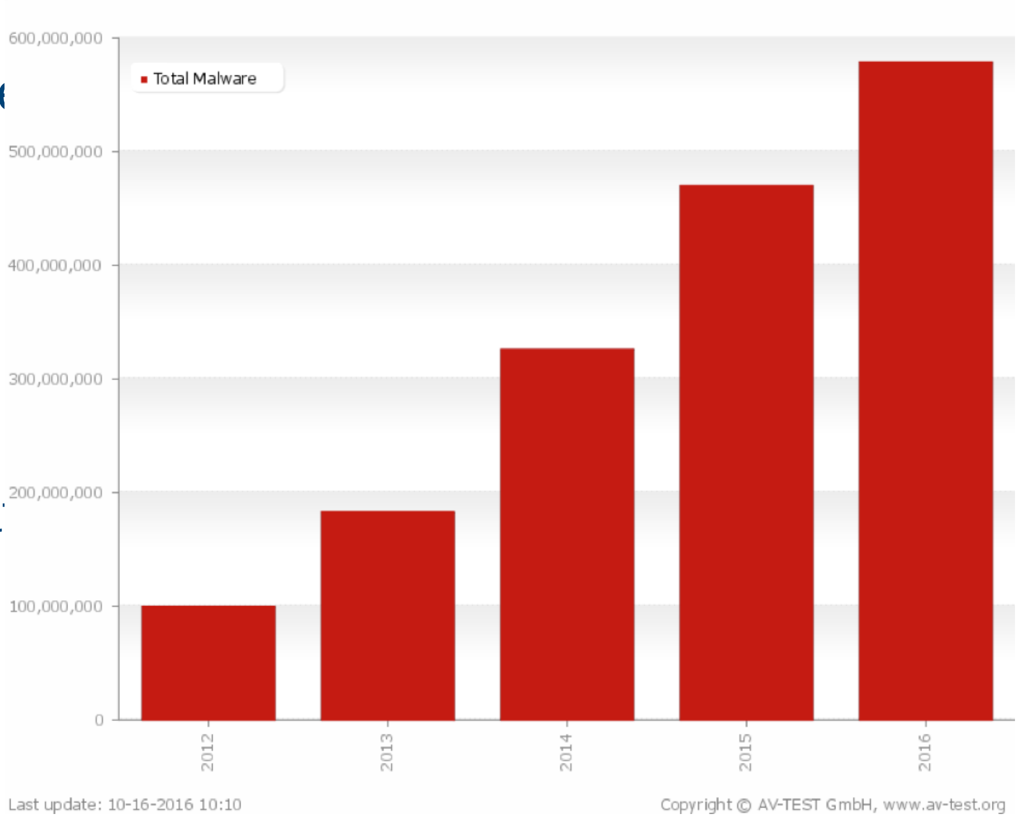
- Especially vulnerable to Encrypted and Polymorphic Viruses
  - These both change their code as they spread.
  - This means our signature no longer will work.
  - For example, every file with “BAD” in it is a virus.
  - Virus mutates and changes this to “ADB”, it will no longer be detected.

Anti-malware

- Anti-malware = marketing term mostly (= anti-virus)
- Anti virus+
  - Detect and locate the malware.
  - Identify specific malware.
  - Automatic removal.
- What if that fails?
- Restore from backups (better hope those are clean).
- Reimage whole machine (useful if no user data stored there).

Anti-malware

- Fails to keep up with malware
- 40 – 60% effective
- Challenges:
- Rapid growth of Malware
- Ease of mutation
- Speed of distribution of upda



Prevention as an alternative

- Prevention = don’t get infected or at least limit the damage.
- Strategies for Organizations
  - Policy: manage the implementation of countermeasures.
  - Awareness: influence individual behavior to practice “safe computing” or “cyber hygiene”.
  - Vulnerability mitigation: patching/updates, access controls on access to files .
  - Threat mitigation: least privilege assigned to users

MASSEY UNIVERSITY
TE KUNENGA KI PŪREHUROA
UNIVERSITY OF NEW ZEALAND

END