Cyberattack 1: Attack Classification

THE UNIVERSITY OF WESTERN AUSTRALIA

CITS3004
Jin Hong

Cyberattacks1: outline

- Attack trends
- Classification
  - Social engineering
  - Cracking
  - malware
  - Network layer attacks
  - Web-based attacks
  - (Distributed) DoS
  - Zero-day

How did it all start…

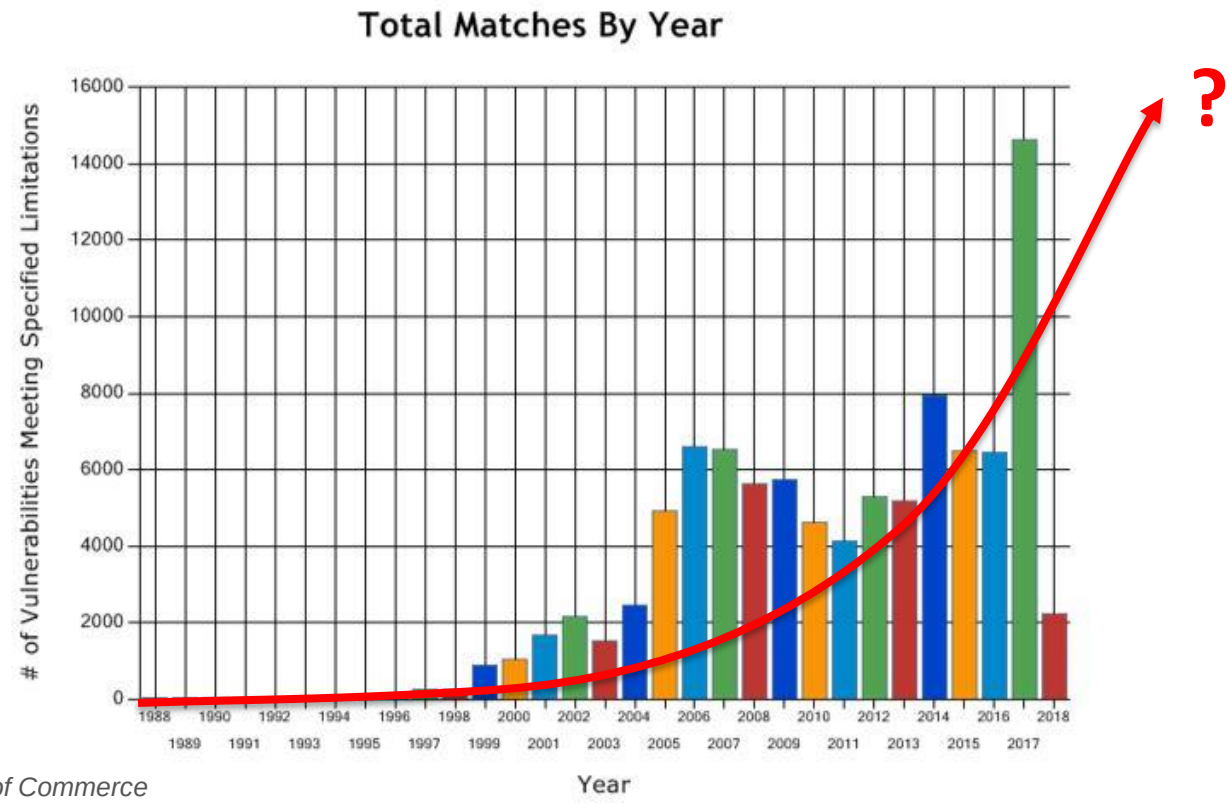
- Before the Internet, the only way to conduct "cyberattack" is via physical access
  - But the computational power at the time was lacking, did not store much things to steal
- TCP/IP was designed in early 1980s
  - IPv4
- Today, TCP/IP is used everywhere
  - LAN, MAN, WAN, etc
  - Various applications (voice, multimedia etc)

Attack Trends

THE UNIVERSITY OF WESTERN AUSTRALIA

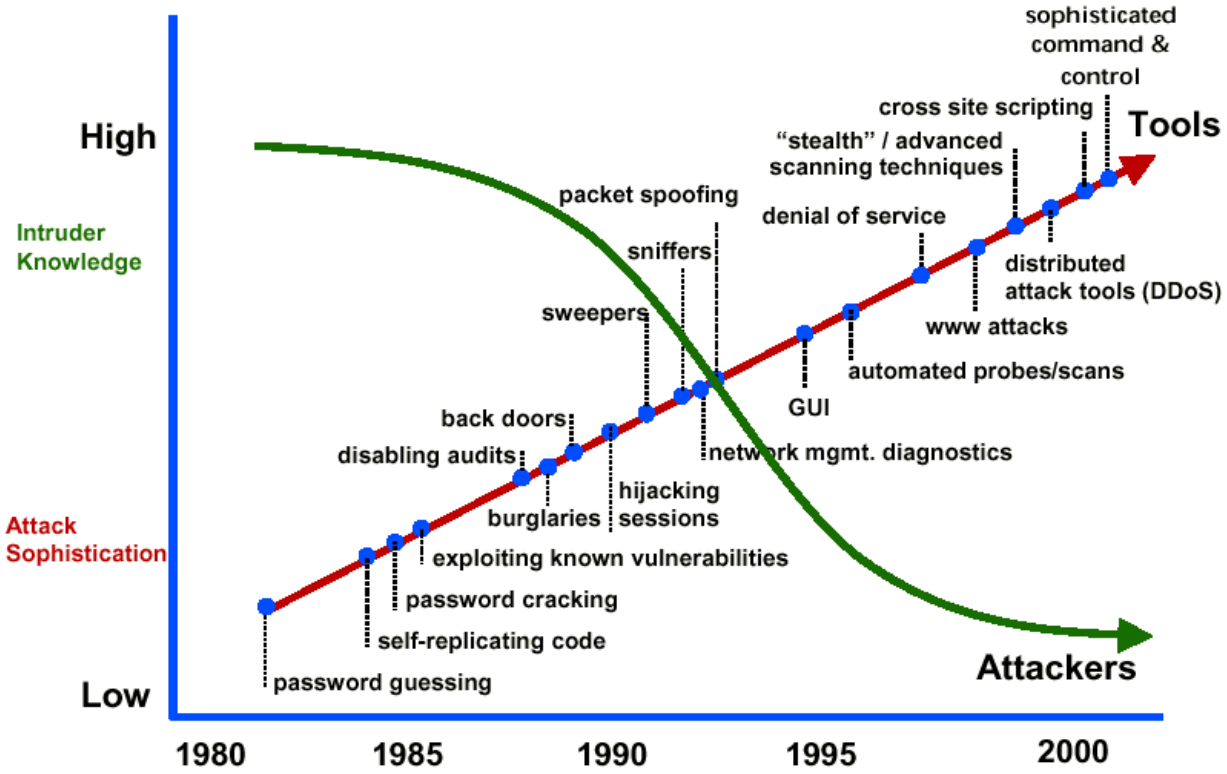
- There are many events that contribute toward attack trends
  - More people using the Internet
  - Increase in software complexity
  - Availability of attacking tools
  - Dependability on cyberspace
  - Lack of security implementation/deployment/adoption

Attack Trends



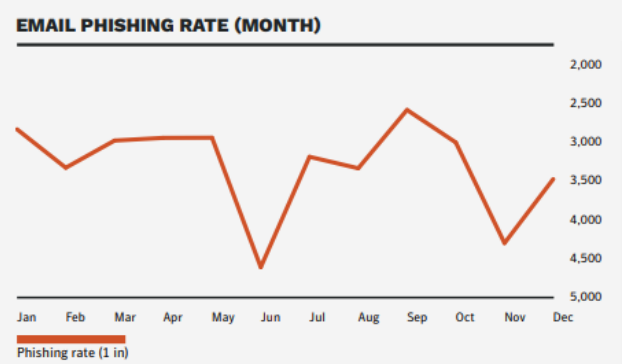
Source: NIST: US Department of Commerce

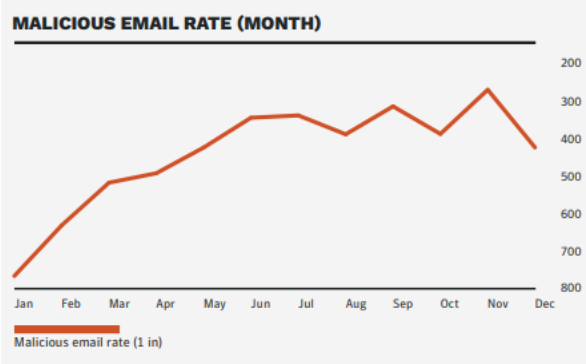
Attack Trends

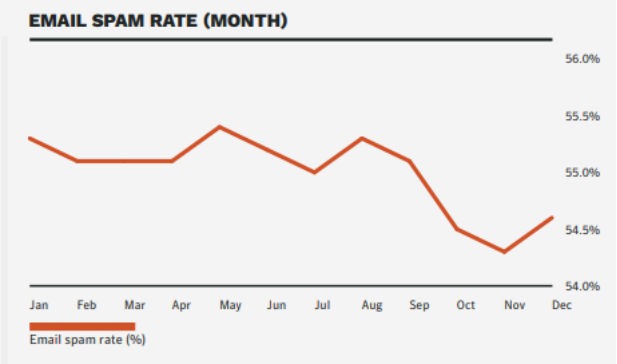


Howard Lipson. Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues. CERT Coordination Center. Nov. 2002

Attack Trends







Symantec Internet Security Threat report 2019 https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf

Attack Trends

- Attacks are evolving with time
  - Deepfakes
    - Deepfake image, voice etc.
  - AI-powered cyberattacks
  - Disinformation in Social Media
  - Vehicle cyberattacks
  - Cloud jacking
  - Etc…

https://us.norton.com/internetsecurity-emerging-threats-cyberthreat-trends-cybersecurity-threat-review.html

Attack Trend

- What issues do cyberattacks bring?

Attack Trend

- Why do people carry out cyberattacks?

Attack Classification

- Main techniques used are (but not limited to):
  - Port-based
  - Malicious email
  - Buffer overflow
  - Malicious web-based
  - (Distributed) Denial of Service

Attack Classification

- Attacks can be classified into
  1. Social Engineering — This week
  2. Cracking — Next week
  3. Malware — The week after
  4. Network Layer Attacks
  5. Web-based Attacks
  6. (Distributed) Denial of Service Attacks
  7. Zero-day

You can of course use other classification methods

Social Engineering

- Persuasion-type of an attack to disclose sensitive information
  - E.g., phishing attack
  - Persuade to install/execute malicious software
  - Links to bogus website (e.g., spoofed bank website)
  - Impersonating legitimate user to retrieve credentials
  - Impersonating technical support member

Social Engineering

- Is it effective?

*https://cofense.com/enterprise-phishing-susceptibility-report

Phishing

- Phishing attack is a mass distribution of a spoofed emails
  - Comes from what it seems to be **well known** organisations
    - Such as banks, insurance, retailers, credit card etc.
  - Looks legitimate, but leads to **fake** or **bogus** sites
  - Asking for personal credentials
  - They are **evolving**!
    - Less grammar/spelling mistakes
    - More in context
    - target-oriented contents
    - Focused targeting is called “Spear Phishing”

Phishing

Paula Peterson <paula.peterson@fresnocitycollege.edu> | Paula Peterson | 25/04/2018

IT Helpdesk! Treat Very Urgently!!!

Links and other functionality have been disabled in this message. To turn on that functionality, move this message to the Inbox.

Dear User,

Please take note of this important update that our new web-mail has been improved with a new messaging system from Microsoft Exchange\Outlook which also include faster usage on email, shared calendar,web-documents also with the new Anti-spam version.

Kindly use the link below to Switch to the New Microsoft Exchange/Outlook.

Click on Microsoft Exchange<http://2w0g99hp69vbla66jukqhmdtm.designmysite.pro/> to Switch immediately.

© IT Technical Support
Copyright 2018, Web-mail Maintenance,
All Rights Reserved.

Phishing

THE UNIVERSITY OF WESTERN AUSTRALIA

Google

paula peterson fresno college

All | Images | News | Maps | Videos | More | Settings | Tools

About 251,000 results (0.95 seconds)

Paula Peterson | Fresno City College
www.fresnocitycollege.edu/directory/counseling/peterson-paula.html
Paula Peterson. Counselor. Administrative. Student Learning Support Services. 559-443-8586. **paula.peterson@fresnocitycollege**.edu. Office location: ST-108.

Paula Peterson | Professional Profile - LinkedIn
https://www.linkedin.com/in/paula-peterson-83abb074
View **Paula Peterson's** profile on LinkedIn, the world's largest professional community. Paula has 3 jobs listed on their profile. See the ... **Fresno** City **College**.

Images for paula peterson fresno college

Phisl

THE UNIVERSITY OF WESTERN AUSTRALIA

Real or fake?

Australian Taxation Office

To: [redacted]

Your have received a tax refund

Australian Government

Australian Taxation Office

Dear citizen,

After the last annual calculations of your fiscal activity we have determined that you are eligible to receive tax refund of 680.33 AUD.
Please submit the tax refund request and allow us 3-5 days in order to process it.

To access your tax refund, please download and fill the Tax Refund Form attached to this email
- open it in a browser (recommended mozilla firefox or google chrome)

A refund can be delayed for a variety of reasons. For example :
-invalid records
-applying after the deadline

IMPORTANT:
If you find this email in Bulk, Spam or Junk
please move it to your inbox as not to
jeopardize the future our communication with you.
It is essential to receive all emails from us to be in touch.

Australian Taxation Office

Working for all Australians

You can help us provide you with the most relevant information by taking a moment to tell us your e-mail preferences.
And of course you can unsubscribe at any time.

Remember, ATO is committed to your security and protection.
To find out more, take a look at our Information Security section under Privacy and Security on the Web site.

Phishing

THE UNIVERSITY OF WESTERN AUSTRALIA

Real or fake?

Vice-Chancellor's Voice

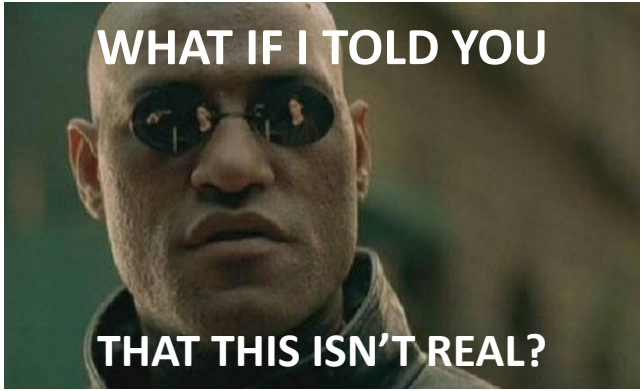
Good afternoon UWA Staff

Recently, we hosted 60 Year 12 students from high schools around WA in an online experience about the accessible and inclusive educational opportunities available through our Fairway UWA program. Fairway UWA provides academic, financial and personal support to Year 12 students facing challenging circumstances, to help prepare them for higher education. Please read more about this important program below.

We have now moved into the implementation phase of the Variations to the Enterprise Agreements for academic and professional staff covered by those Agreements. You will be able to book your purchased leave in the Employee Self Service system from 31 August 2020 and we ask that you book this leave by 30 September 2020. If you intend to submit an application for an exemption, you will find the relevant application form on the EAV Intranet Site. Further information is available at the EAV Intranet Site, or by contacting the EAV team at eav@uwa.edu.au

Pharming

- Attack that **redirects** a website's traffic to another website
- The browser may still display the web address you wanted, but the content may not be correct
- DNS tampering to **redirect** the traffic to a different website without users knowing
- What you are viewing is fake, even though it looks real

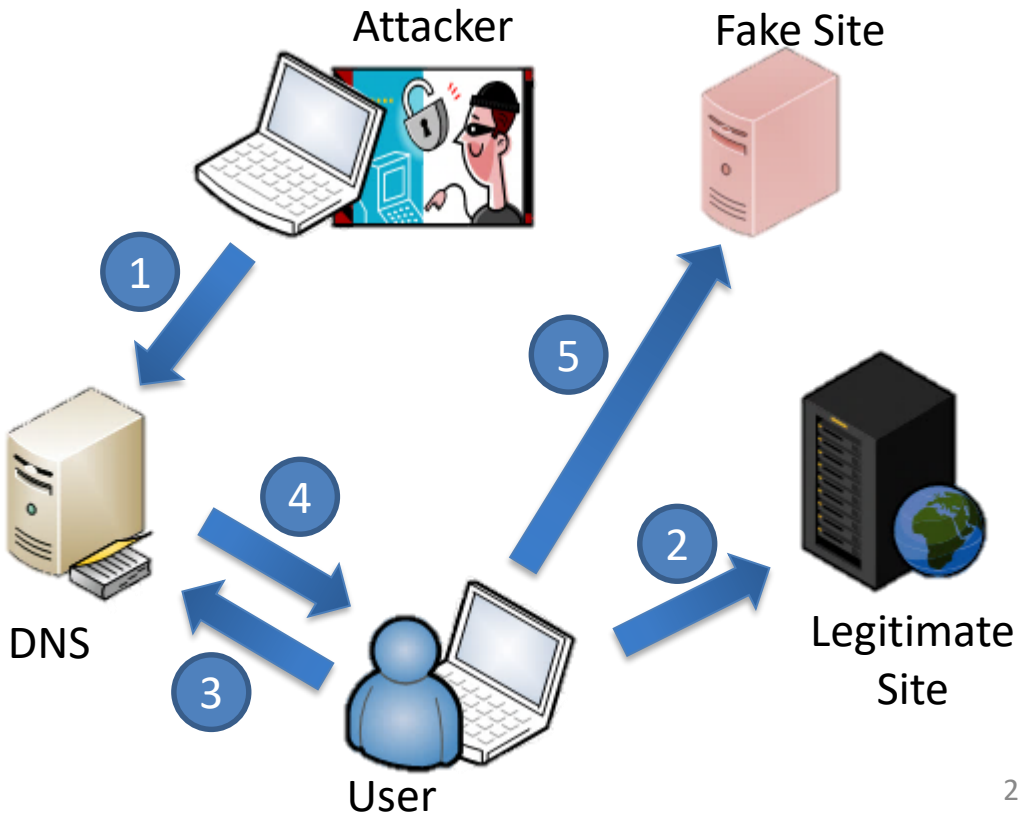


Pharming

- DSN server can be manipulated

Or

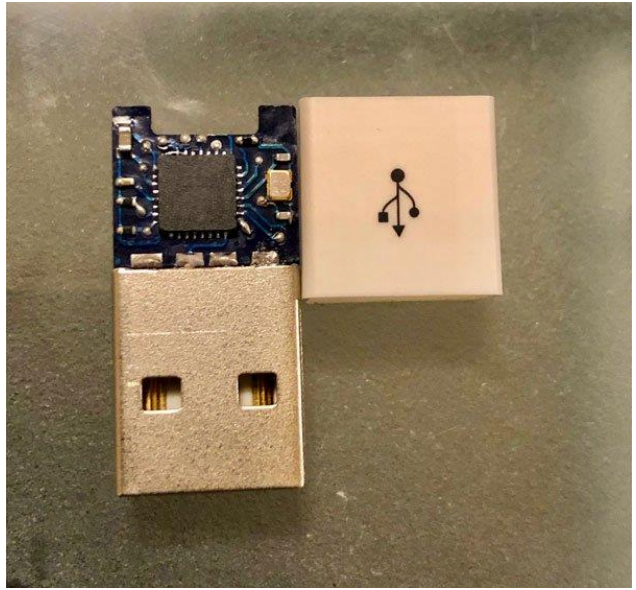
- DSN lookup table on the user's computer can be manipulated



Offensive USB

Phishing in physical domain

- Microchips can be embedded on USB lines.
- When plugged in, they are detected by the US as a human interface device (HID)
  - E.g. mouse, keyboard etc
- You can control those malicious USB lines via WiFi!



Link to the video in additional materials

Social Engineering - Mitigation

- Establishing frameworks
- Asset management
- Security protocol implementation and evaluation
- Security education
- Security review
- Trust establishment

Cracking

- Conducting malicious activities to guess, corrupt or steal information
- “Unethically exploits the highly sensitive information and uses the flaws in the security systems”*

Cracker – Uses the flaws in the security systems
Hacker – Finds and exploits flaws in the security systems

*https://www.educba.com/hackers-vs-crackers/

Cracking

- Password guessing or using Password cracking tools
  - Brute force and dictionary attacks
  - Use of tools such as
    - CRACK – www.pwcrack.com
    - L0phtcrack – www.l0phtcrack.com
    - John the Ripper www.openwall.com/john/
    - Other password (and bunch of other security) tools www.securityfocus.com/tools/

Cracking

- Packet Sniffers
  - Packet sniffing tools are used widely and legitimate tools for network analysis
    - E.g., Microsoft Protocol Analyser
    - E.g., Wireshark
  - Can also be used illegitimately
  - Usually for monitoring IP packets

Cracking

*Local Area Connection [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
56	8.102594	208.83.241.15	192.[redacted]	TCP	60	[TCP Window Update]
57	8.102652	192.[redacted]	208.83.241.15	HTTP	1189	POST /Authenticatic

```
⊟ Member Key: "handle"
    String value: dan.goodin@arstechnica.com
⊟ Member Key: "password"
    String value: secretpassword
```

```
0450  3a 22 64 61 6e 2e 67 6f  6f 64 69 6e 40 61 72 73   :"dan.go odin@ars
0460  74 65 63 68 6e 69 63 61  2e 63 6f 6d 22 2c 22 70   technica .com","p
0470  61 73 73 77 6f 72 64 22  3a 22 73 65 63 72 65 74   assword" :"secret
0480  70 61 73 73 77 6f 72 64  22 2c 22 65 6d 61 69 6c   password ","email
0490  22 3a 22 22 2c 22 72 65  6d 65 6d 62 65 72 22 3a   ":"","re member":
04a0  74 72 75 65 7d                                     true}
```

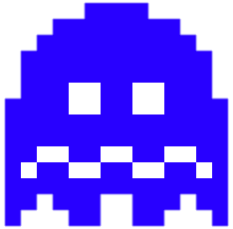
JSON string value (json.value.string), 16 bytes | Packets: 226 · Displayed: 226 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

Cracking - Mitigation

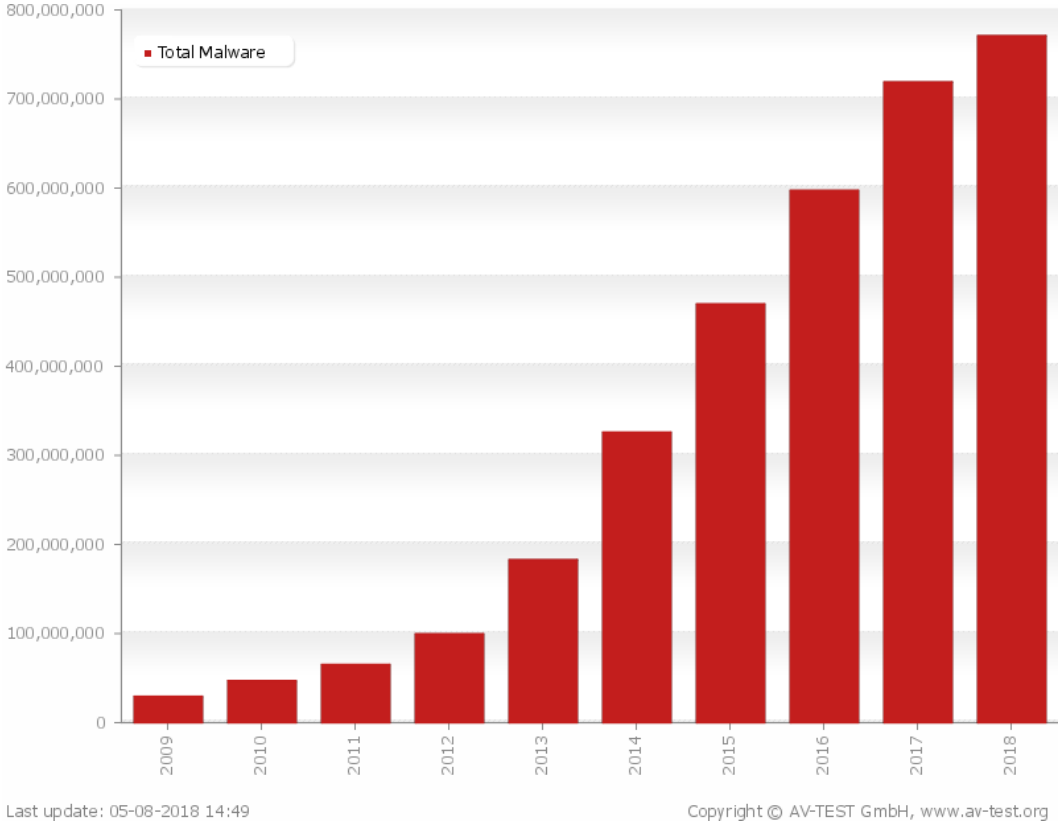
- Ensure your password is strong
  - https://howsecureismypassword.net/
- Store salted hash of the password
- Close unused ports
- Ensure secure programming
- Enforce encryption
- Security education
- Limited trial
- Multi-factor authentication

Malware

- Short for malicious software
- Includes
  - Viruses
  - Worms
  - Spyware
  - Trojan Horses
  - Rootkits
  - Ransomware
  - Etc…



Malware


Total Malware
800,000,000
700,000,000
600,000,000
500,000,000
400,000,000
300,000,000
200,000,000
100,000,000
0
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
Last update: 05-08-2018 14:49
Copyright © AV-TEST GmbH, www.av-test.org

Malware

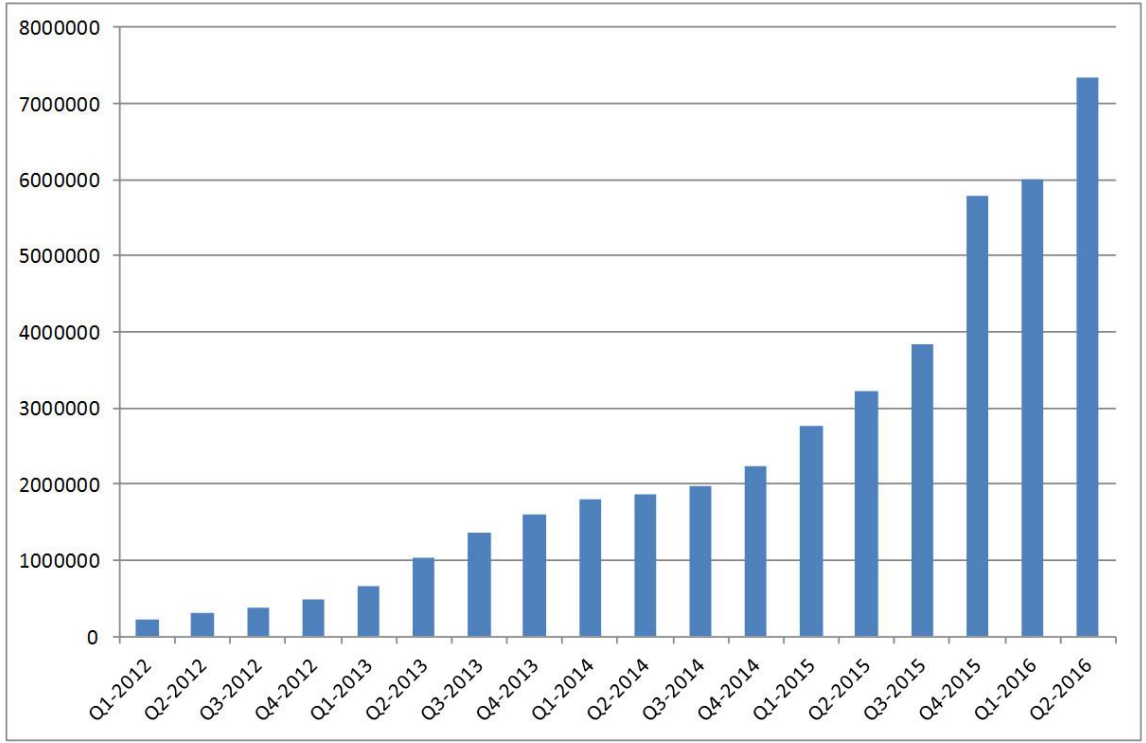


Figure 1 - The growth of incidences of Ransomware - Source Mcafee

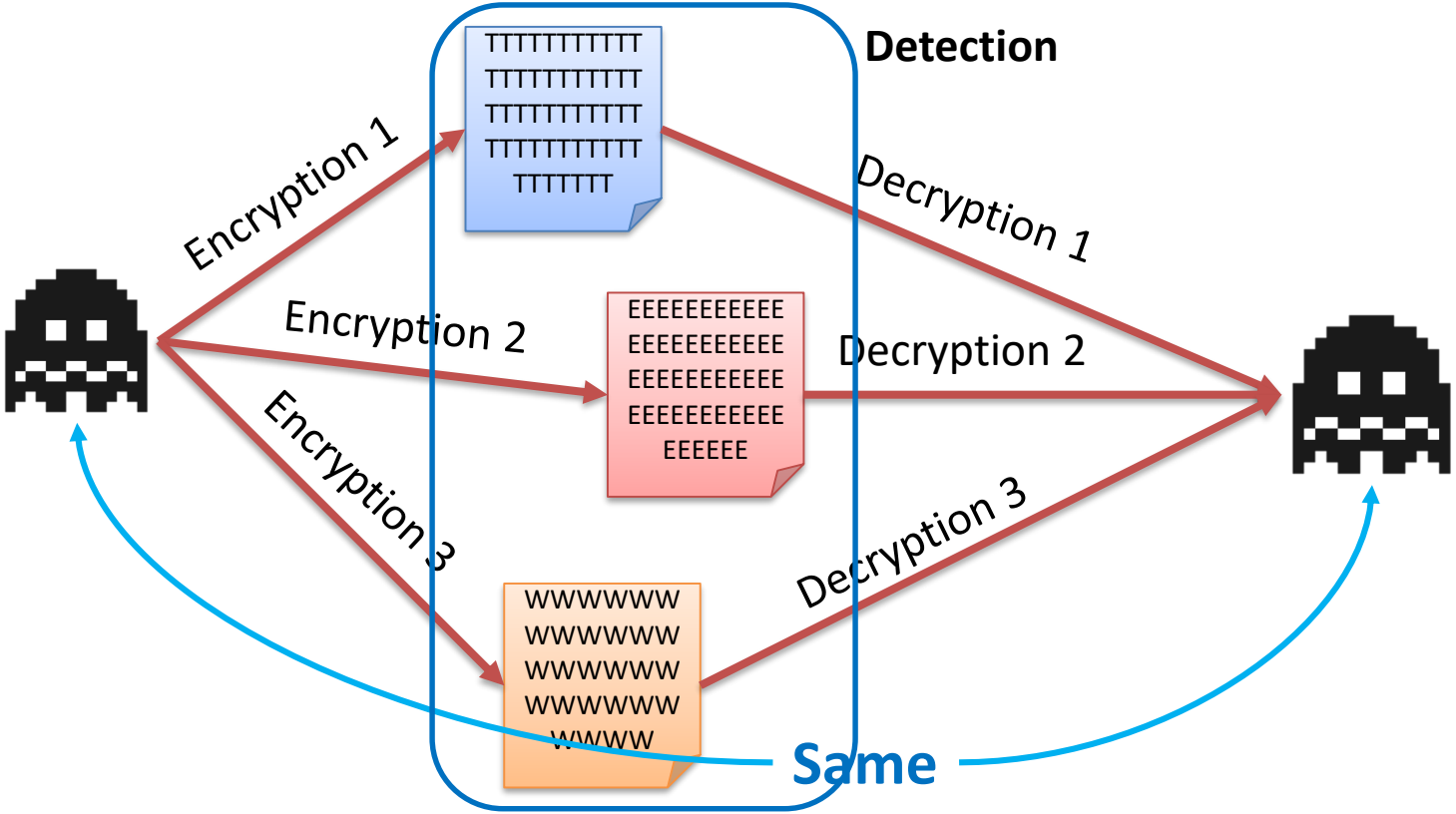
Virus

- Malicious program that spreads through the network by infecting various **files**
- Infected files will **execute** the malicious program without the user knowing first, and then run the normal program
- Viruses will also **replicate** itself by replacing other executable files by attaching the malicious program
- Many viruses spread through **file sharing**
  - E.g., email attachments, USB sharing, FTP, downloads etc.
  - Requires the infected files to be transferred to other hosts

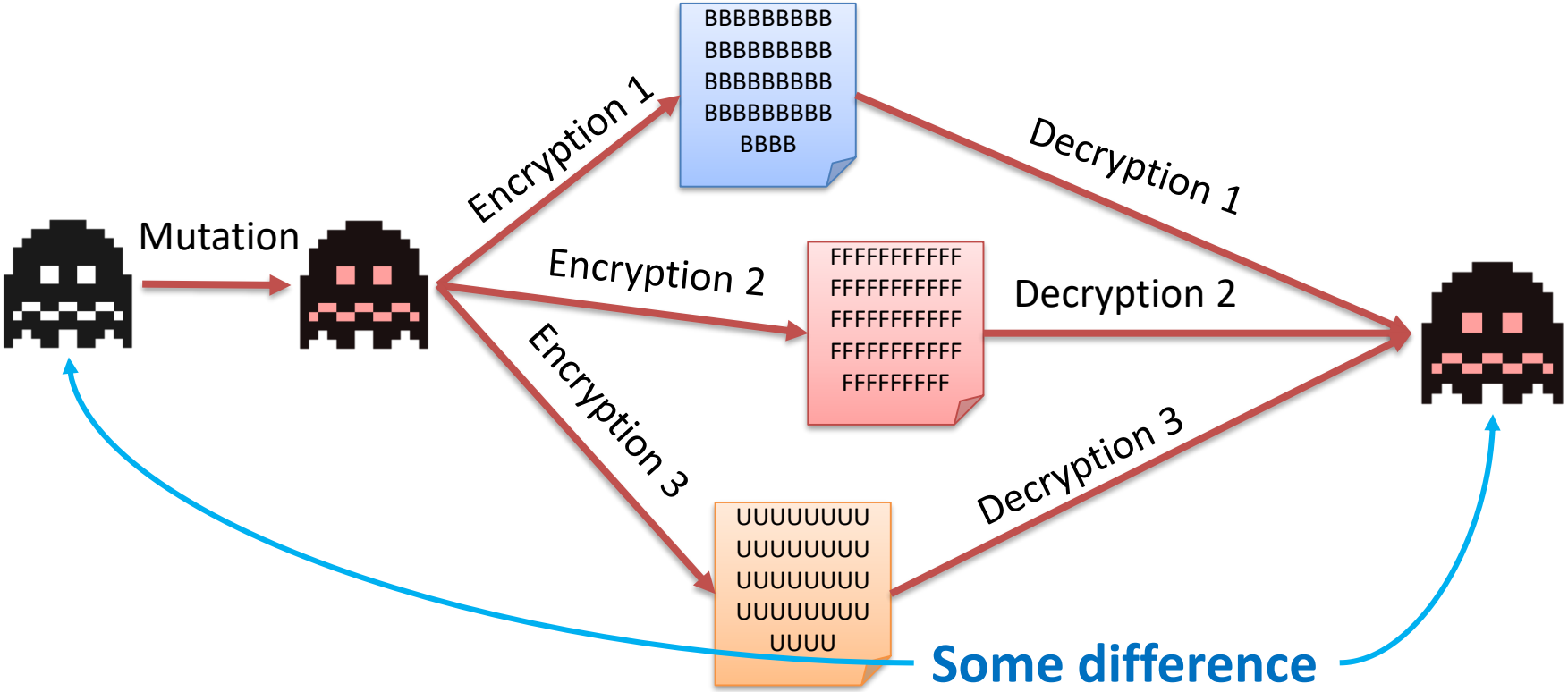
Virus

- Viruses come in many forms:
  - File infector viruses
  - Boot sector viruses
    - System area, memory area, or both
  - Macro viruses
- Viruses mutate:
  - Oligomorphic – using multiple decryptors. E.g., Whale
  - Polymorphic – mutate certain part of itself. E.g., Virut
  - Metamorphic – rewrites all (or most) of itself. E.g., Zmist, Virlock

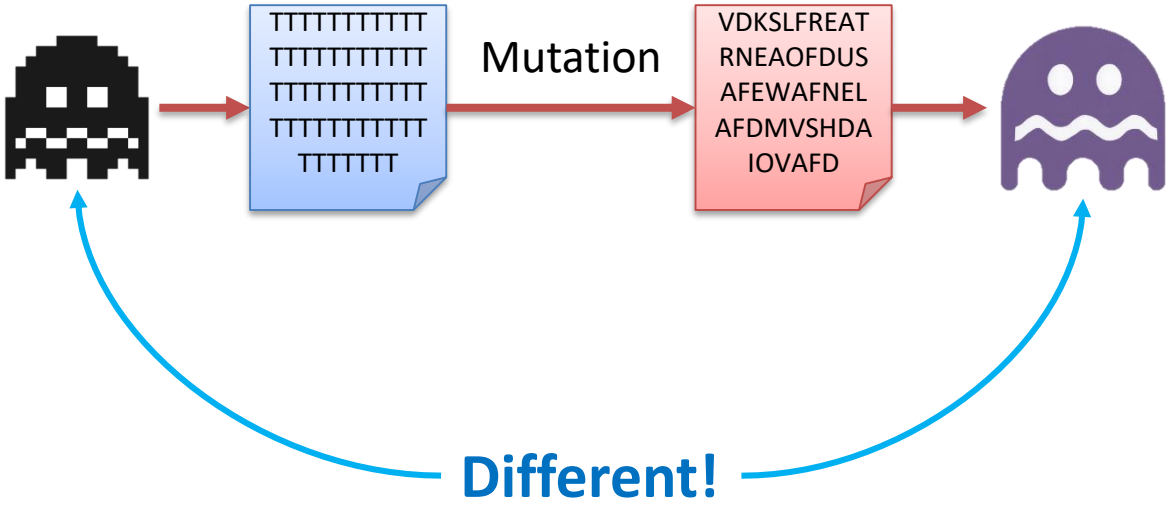
Oligomorphic Virus



Polymorphic Virus



Metamorphic Virus



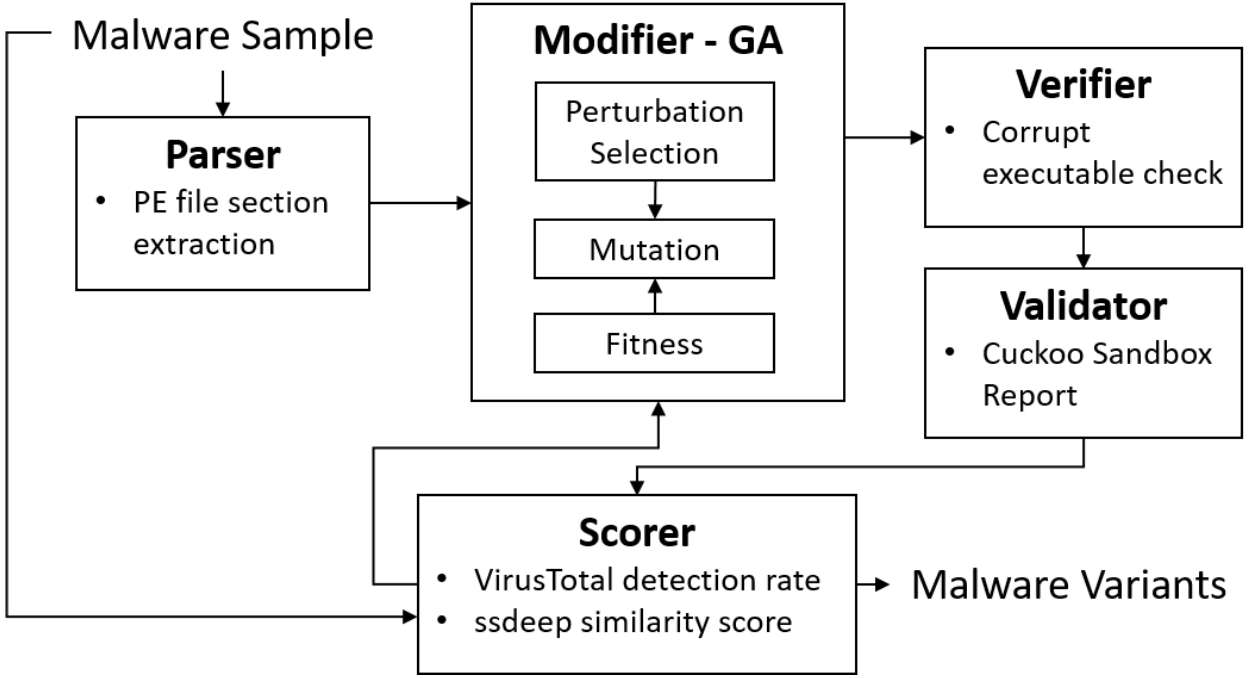
Virus - Silex

- New version of Silex released 2019 targeting IoT devices
  - So far, bricked over 2000 IoT devices
- What does it do?

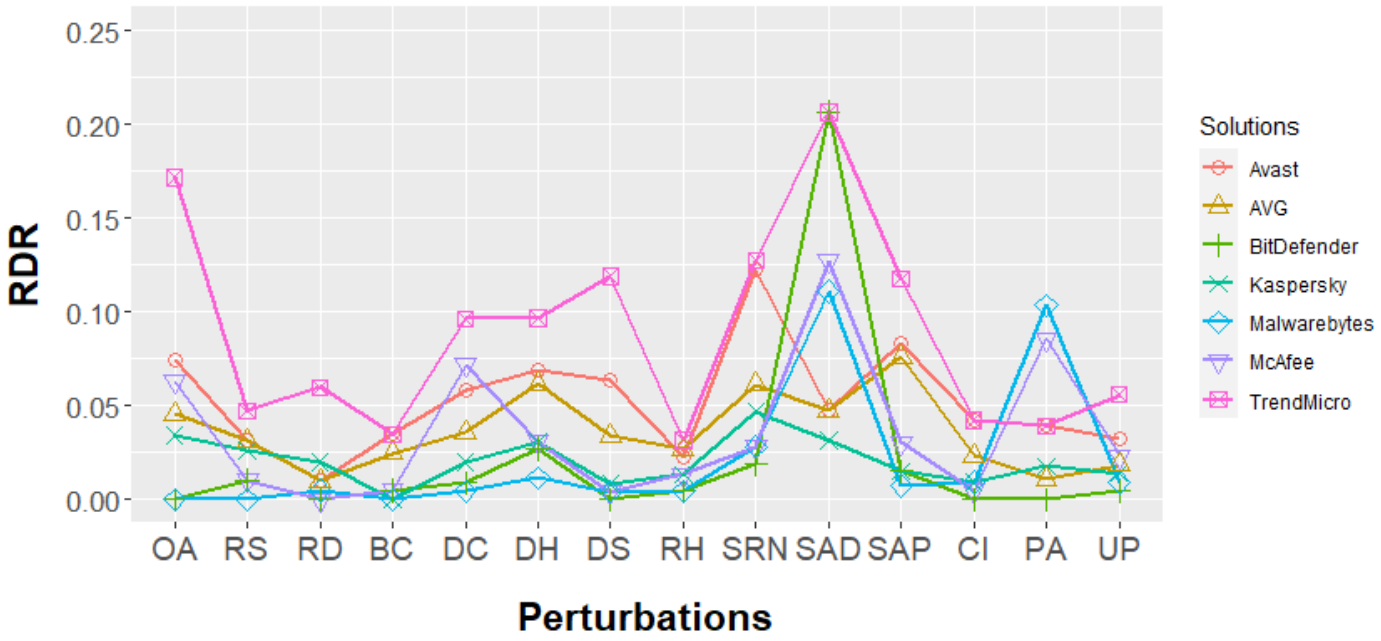
Virus - Silex

- Steps taken in the attack
  1. Enumerate accessible IP addresses
  2. Identify all Unix-like systems
  3. Attempt default login credentials
  4. Access all disk partitions via `fdisk -l`
  5. Then delete network config
  6. Next, run `rm -rf /` to delete everything else
  7. Finally, flush all iptables and add `DROPS` to all connections.

Virus – Malware Generator

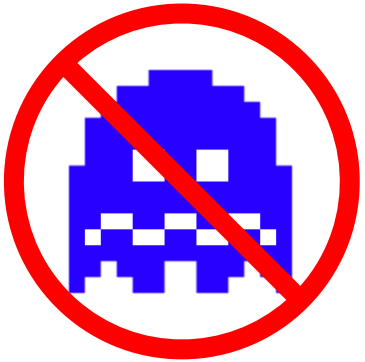


Virus – Malware Generator



Virus - Protection

- Antiviruses
  - Scanning email attachments
  - Checking virus activities (signatures and/or anomaly detection)
  - Examples include Norton, McAfee, Trend Micro, Symantec, Sophos etc.
  - Incorporate sandboxing, AI, data mining, machine learning etc.
- Access restriction
  - Remote access control
  - Firewalls
  - Email filtering



Worm

- Focuses on **spreading** through the network
- Exploits various **network vulnerabilities** to spread itself
  - Unprotected shared drives
  - FTP vulnerabilities (typically buffer overflow)
  - E.g., Ramen, Lion, Code-Red, Conficker
- May also release viruses upon opening
  - E.g., MyDoom.A -> backdoor and DoS
  - E.g., MyDoom.B -> MyDoom.A + block access to antivirus sites

Worm vs Virus

- “Virus does not intentionally try to spread itself from that computer to other computers. In most cases, that's where humans come in”

- “Worm is a program that is designed to copy itself from one computer to another over a network (e.g., by using e-mail). The worm spreads itself to many computers over a network”

http://www.symantec.com/avcenter/reference/worm.vs.virus.pdf

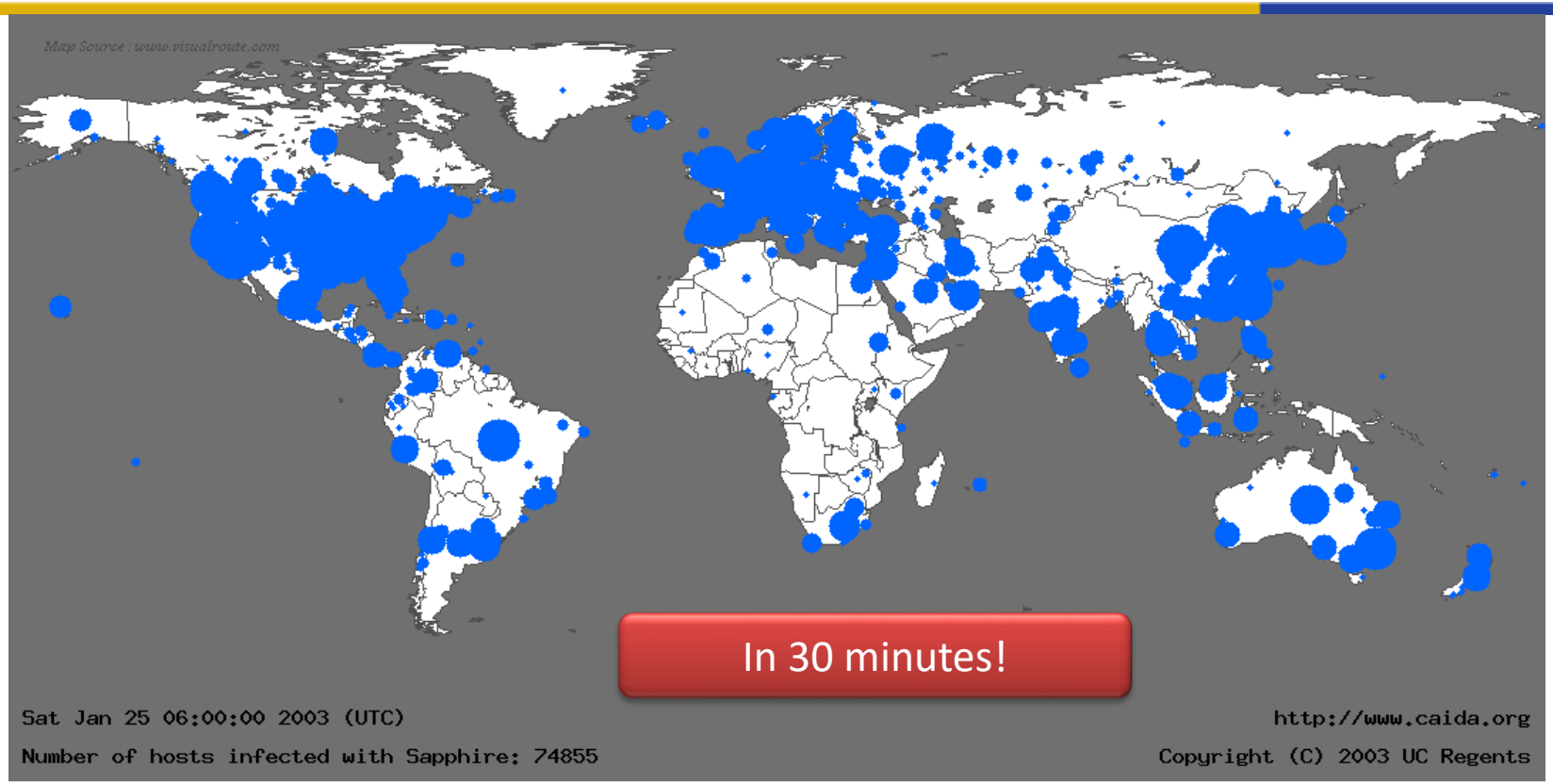
Worm - Slammer

- Slammer worm
  - Aliases: SQL Slammer, Saphire, W32.SQLExp.Worm
  - January 25 2003, approx. 5.30am (GMT)
  - Infected 75,000 victims
  - Spread world-wide in under 10 minutes
  - Doubled infections every 8.5 seconds
  - 376 bytes long
  - Buffer overflow in Microsoft SQL Server and Desktop Engine products
  - DoS on some Internet hosts, general Internet slow down
  - Patch was released 6 months before the worm, but many did not applied

Worm - Slammer

- Propagation technique
  - A single UDP packet (only 376 byte payload)
  - Target port 1434 (Microsoft SQL monitor)
  - Keep sending itself to random IP addresses
  - Once host identified running unpatched MS SQL server, it is infected immediately

Worm - Slammer



Worm - Protection

- Patching up-to-date
  - Applications and operating systems
- Security education
  - do not click suspicious links
  - Run executable files or programs
- Antivirus and anti-spyware software
- Firewall

Malvertising

- Malicious advertising
- Spread of malware through advertising
- Sometimes, just viewing can affect your system
- About 10 billion ads were malvertisement in 2012*
- In 2017, Google blocked 79 million ads with redirection and removed 48 million ads trying to install unwanted software#

*Online Trust Alliance (2012-07-29). "Anti-Malvertising Resources". Online Trust Alliance. Retrieved 2013-05-25.
#https://www.csoonline.com/article/3373647/what-is-malvertising-and-how-you-can-protect-against-it.html

Malvertising

- Many different ways they can get in:
  - Pop-up ads
  - Web widgets
  - Hidden iframes
  - Malicious banners
  - Third-party advertisement
  - Etc.

Malvertising

THE UNIVERSITY OF WESTERN AUSTRALIA

http://www.theage.com... | ASADA issues 12,000 pages...

7:05AM Saturday Oct 18, 2014 4474 online now Do you know more about a story? Fairfax Media Network

MY NEWS | MY CLIPPINGS | MY COMMENTS | MY BENEFITS | TODAY'S PAPER | SUBSCRIBE | LOG IN | REGISTER

THE AGE REAL FOOTY

One subscription for both of you

News Ladder Fixtures Clubs Experts Grand Final Brownlow Medal Supplements Saga VFL Ultimate Footy

You are here: Home » AFL » News » AFL Search

ASADA issues 12,000 pages of evidence against 34 Essendon players

October 17, 2014 - 5:35PM 7 reading now Read later

Jon Pierik
Sports writer with The Age
View more articles from Jon Pierik
Follow Jon on Twitter Email Jon

Tweet 3 Recommend 2 Share 1 Share submit
Email article Print Reprints & permissions

The 34 Essendon players re-issued with show-cause notices have been given 350 pages of evidence alleging they were administered a banned peptide during the club's 2012 supplements program.

The Australian Sports Anti-Doping Authority on Friday revealed it had issued amended notices to the players, alleging the use of the banned drug, thymosin beta-4.

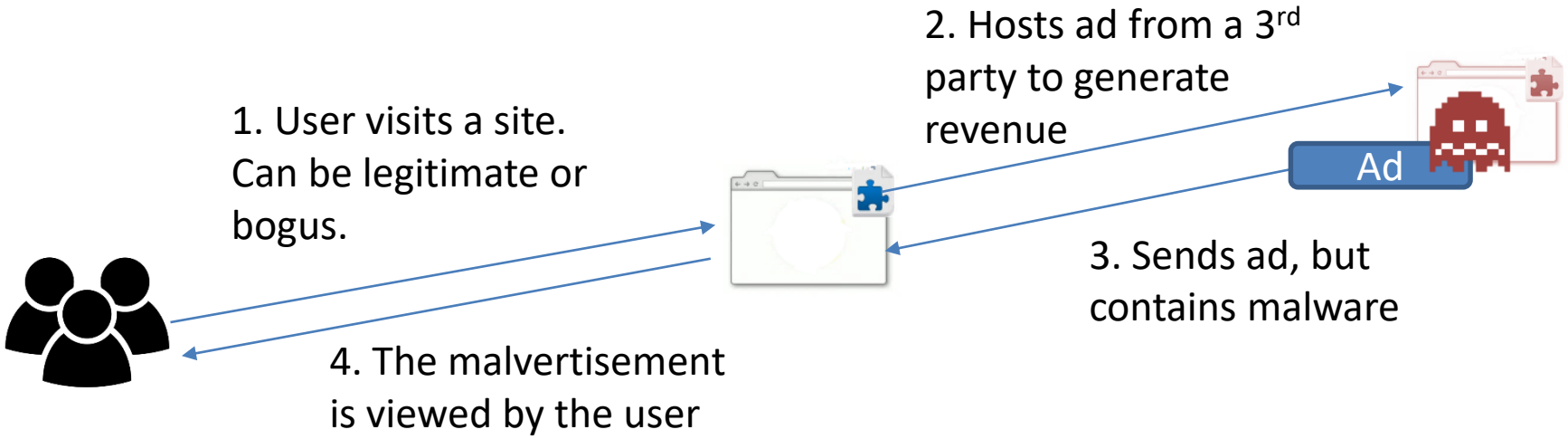
The players, of which about 18 are still with the Bombers, have until October 31 to respond to

Most popular

1 AFL trade and free agency 2014: a club-by-club ... 42

2 ASADA issues fresh

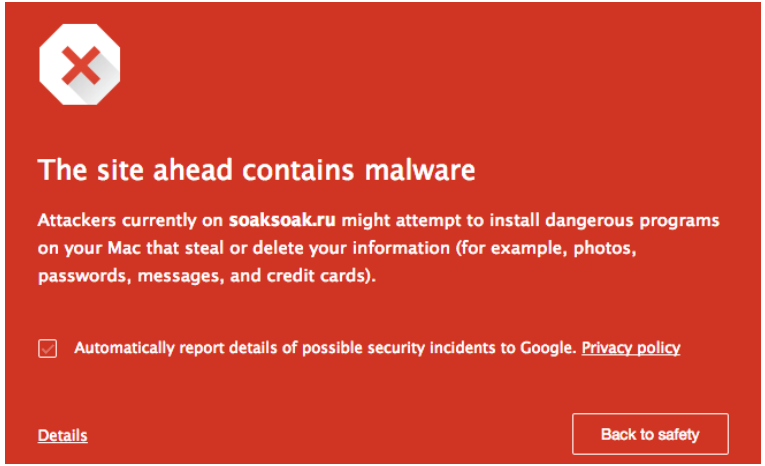
Malvertising



Malvertising can be “hidden” from the user by creating invisible boxes

Malvertising – Protection

- Keeping up-to-date software and OS
- Antivirus and other malware protection methods
- Browser extensions alerting malvertising campaigns



Spyware

- Variety of meanings including key loggers unsolicited commercial software, scumware, Trojan horses etc.

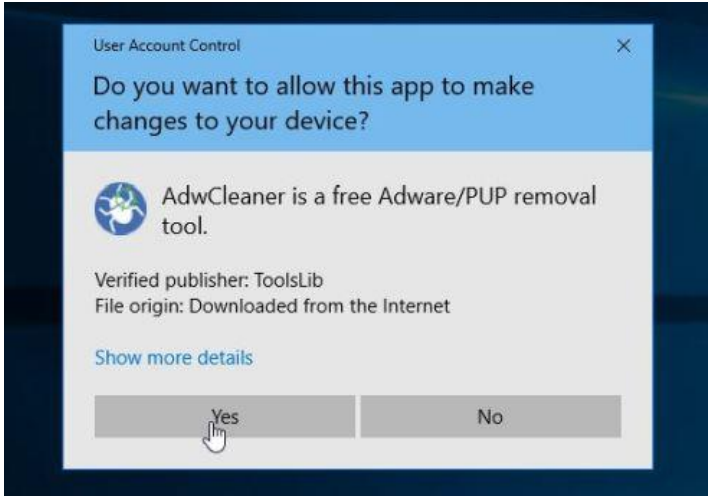
Spyware – Key Loggers

- Actions on computer is **monitored** and **captured** by adversaries
- Can be software or hardware
- Strong passwords are **no longer** effective

- Use:
  - Anti keyloggers, antivirus, anti-spyware
  - Monitor malicious network traffic
  - Security tokens
  - Automatic form fillers etc.

Spyware – Unsolicited Software

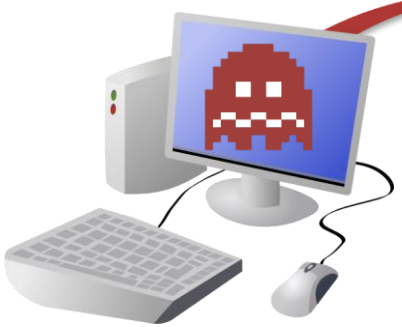
- Unsolicited commercial software are installed without user's intensions
  - E.g., Piggyback software
- May contain spyware to snoop user activities
- Always check what you are agreeing to install



Spyware – Scumware

- Refers to any malicious code that entered the system without the user's consent or permission
- Scumware can significantly changes the appearance and functions of websites without permission
  - Guiding to bogus websites for further malware infection
- Use anti-spyware and network filtering

Harvesting Personal Information



Name
Address/geography
Place of work
Name of bank
Ebay/PayPal
Family information
Friend information

Highly focused customised social engineering attack

Harvesting Personal Information

- We just trust them too much
  - Chrome Incognito mode still allow third parties to collect data
    - https://www.wired.co.uk/article/google-chrome-incognito-mode-privacy
  - Facebook listening in on user conversations (up to very recently)
    - https://www.scmp.com/news/world/united-states-canada/article/3022682/facebook-admits-listening-transcribing-users
  - Microsoft listening on Skype calls
    - https://www.scmp.com/news/world/united-states-canada/article/3021896/microsoft-admits-its-workers-listen-your-skype
  - Apps collect your data even you deny permissions
    - https://www.cnet.com/news/more-than-1000-android-apps-harvest-your-data-even-after-you-deny-permissions/

Trojan

- Trojan, or Trojan Horse, is different to viruses and worms
  - Do not infect files
  - Do not spread
- Allow attackers to access user's device remotely
- Has client and server applications
- User can unintentionally download and install on the system
  - E.g., email attachments, file sharing, free software online etc.
- Attackers can also directly install
  - E.g., physical access

Trojan

- Example: Zeus (2009)
  - Stole banking information using **keylogger**
  - Affected systems through downloads and phishing
  - Compromised over 74,000 FTP accounts on websites of companies (June 2009)
    - Such as Bank of America (BoA), NASA, Oracle, Cisco, Amazon etc.
  - Zeus botnet estimated millions of compromised computers
    - **Largest** botnet on the Internet
  - Also used for installing **CryptoLocker** ransomware

Trojan - Mitigation

- Best defence is safe computing practices
  - Don't trust what you get from the **Internet**
- Trojan Horses can come from unsolicited executable e-mail attachments from recognised senders
  - do **not** open if you are not sure
- Use IDS or file integrity monitoring systems
  - E.g., Tripwire

Rootkits

- Looks legitimate, but conducts **malicious** behaviours
- Used to obtain the **root** privilege
  - But also hide its elements such as processes, files, and network connections
- Have access to **modify** existing software
  - Including tools to remove it
- Rootkit types include:
  - **Firmware** (Persistent) – hides in firmware
  - **Kernel-mode** – hide from kernel list of active processes
  - **User-mode** – runs along with other applications

Rootkits - Mitigation

THE UNIVERSITY OF WESTERN AUSTRALIA

- Possible to hide spyware or virus that will not be detected by traditional antivirus products
- F-Secure BlackLight Rootkit Eliminator
  - www.f-secure.com/blacklight
  - www.systernals.com
- Published Rootkits
  - www.rootkit.com, eg AFX, Vanquish, HackerDefender

Botnet

- A bot is an application that runs automated tasks over the Internet
  - E.g., web crawlers
- A botnet is a collection of connected devices that runs one or more bots
- Botnet can deploy various types of attacks
  - E.g., DDoS, spamming
  - But also stealing data and accessing bots

Botnet

1. A botnet operator infects users
2. The bot on the infected PC communicate back to the command-and-control server
3. A spammer purchases the services of the botnet from the operator
4. (a) The spammer provides the spam messages to the operator
   (b) The botnet operator uses bots to send out the spam message

https://commons.wikimedia.org/wiki/File:Botnet.svg

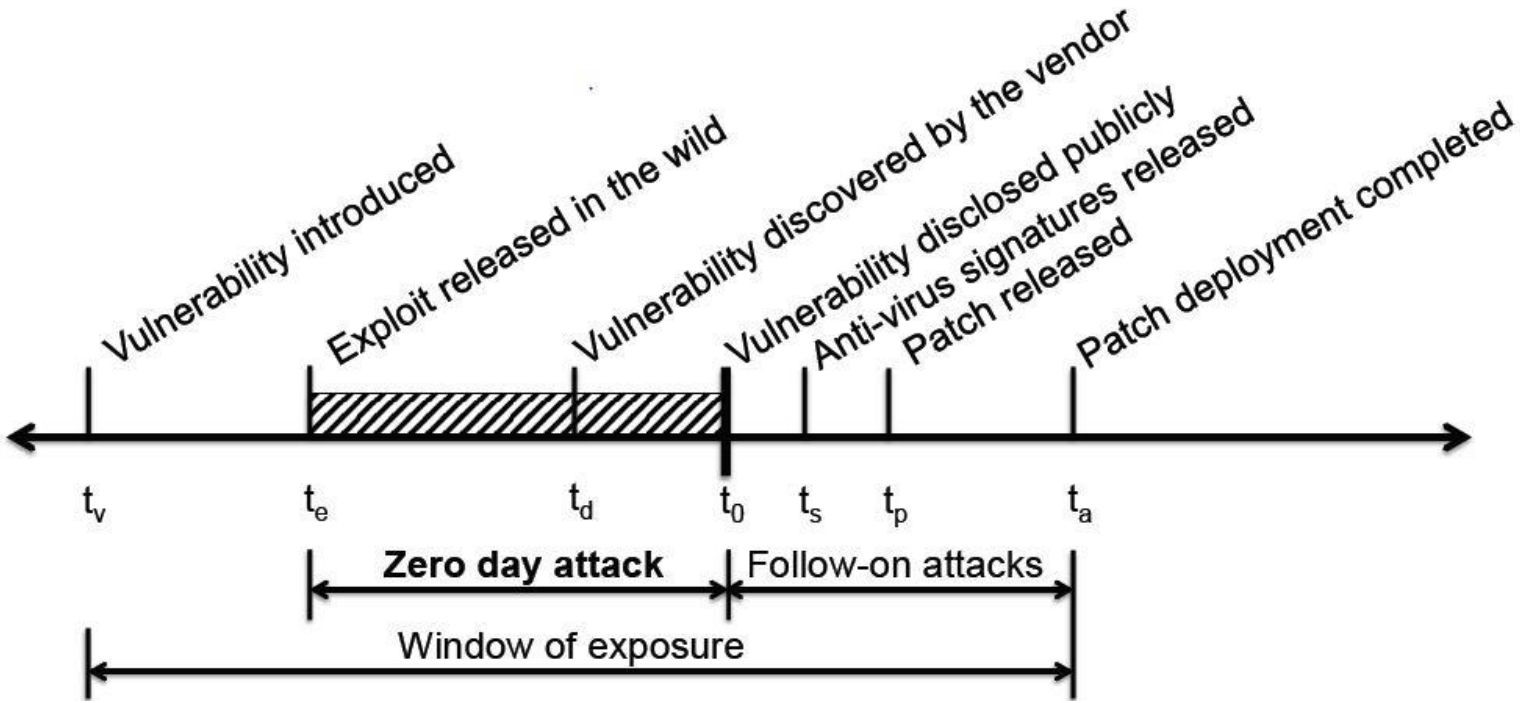
Zero-day

- Zero-day attacks take advantage of software vulnerability for which there are **no available fixes**
- Attacks take advantage of flaws before software makers can fix them
- Has become significant issue from 2008 on
- Emphasises importance of safe configuration policies and good incident reporting systems

Zero-day

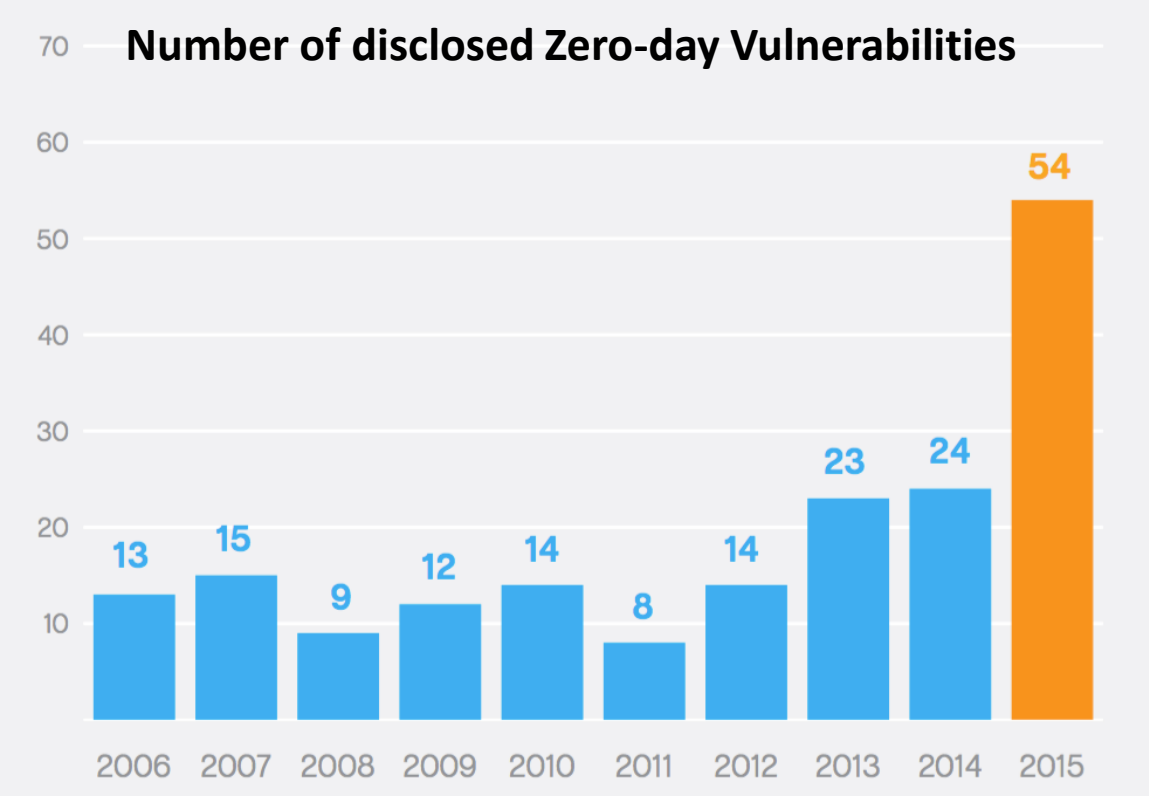
- Attackers are getting faster at discovering and exploiting flaws
- For example: the Blaster worm (2003)
  - Released August 2003, patch released January 2004
  - Used buffer overflow, and also launched DDoS against windowsupdate.com (but not very successful as it was redirected to windowsupdate.microsoft.com)

Zero-day



http://securityaffairs.co/wordpress/wp-content/uploads/2013/12/zero-day-vulnerability-life-cycle.jpg

Zero-day



Internet Security Threat Report – Symantec (2015)

Zero-day

- According to the **Zero Day Initiative**, 135 vulnerabilities were discovered in Adobe products during the first 11 months of 2016 and 76 in Microsoft products. Meanwhile, the number of zero-day flaws in Apple products doubled over the previous year, to 50 from 25.

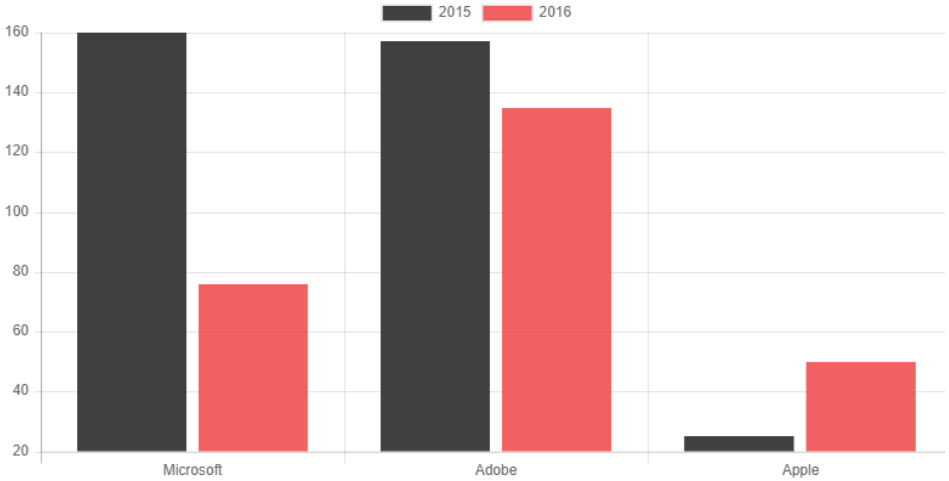


Figure 5: Microsoft, Adobe, and Apple vulnerabilities disclosed by the ZDI

https://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2017

Zero-day: detection

- A few techniques exist to detect zero-day attacks:
  - **Statistical-based:**
  - **Signature-based:**
  - **Behaviour-based:**
  - **Hybrid-based:**

Keeping Up-to-Date

- www.cert.org (main index by year)
- www.securityfocus.com (bugtraq)
- www.symantec.com
- www.caida.org (analysis of propagation etc)
- technet.microsoft.com/en-us/security/bulletin

CERT

- Computer Emergency Response Team
  - www.auscert.org.au (Australia)
  - www.nzcert.org.nz (New Zealand)
  - www.apcert.org (Asia-Pacific)
  - www.cert.org/advisories (US)
  - www.singcert.org.sg (Singapore)
  - www.hkcert.org (Hong Kong)
  - www.krcert.or.kr/english_www/ (South Korea)
  - www.ccert.edu.cn/about_us/index_en.htm (China)
  - www.jpcert.or.jp/english (Japan)

Summary

- Overview of attack trends
  - And attacker motivations
- A few categories of attack classification reviewed
  - Given the complex system we use, there are various ways they can be exploited
  - Need to be aware of different attack strategies in order to protect our systems

Next Week

- Cyberattacks 2: Network attacks and BOF
  - Network oriented attacks
    - Spoofing, hijacking, etc.
  - Buffer overflow

Additional Items

- Common Attack Pattern Enumeration and Classification
  - https://capec.mitre.org/index.html
- USB hacking video
  - https://twitter.com/i/status/1094389042685259776
- Virus Timeline
  - https://en.wikipedia.org/wiki/Timeline_of_computer_viruses_and_worms#2010%E2%80%93present
- 8 famous viruses
  - https://uk.norton.com/norton-blog/2016/02/the_8_most_famousco.html
- Zeus phishing email
  - http://www.salisbury.edu/helpdesk/security/latest/phishing_attempt__4122012_VariousZeusbot.html
- Document analysis cheat sheet
  - https://zeltser.com/analyzing-malicious-documents/?fbclid=IwAR3d2de5lJfacOaHBtR5RbtPCW7QFccv18LOjAHGAPW4N99PubT951EGRSc