Week 5 ---

Malware

- **Lecture Content**

❑ **Malware Classification by Action (Payload)**

- ❑ **Adware, Spyware**
- ❑ **Browser hijackers**
- ❑ **Bots, RATs**
- ❑ **Ransomware**

Adware

❑ Adware is software which controls the downloading of advertisements onto web-browsers and "free" software. The distinction between adware and "spyware" is blurred. Few anti-spyware companies make a distinction.

- Ben Edelman has made extensive studies of the infection processes of spyware, and the ethics of companies making money from it (http://www.benedelman.org/archives/).

Spyware/Adware

❑ Spyware is persistent software that installs itself as a service, opens a TCP or UDP socket and sends information about the user's computer to some other party.

❑ Discovered during testing a new software firewall called ZoneAlarm. Unlike other firewalls at the time, ZoneAlarm monitored out-going connections as well as in-coming connections.

❑ Out-bound TCP connections can also be detected with Netstat.

Spyware/Adware

- ❑ Uses of spyware include keylogging, browser hijacking, theft of information such as passwords, user's surfing habits (cookies) and registry entries, push-advertising and other forms of un-ethical marketing.
- ❑ Social networking sites love spyware!
  - Nice description of an infection process here: http://isc.sans.org/diary.html?date=2004-11-24

Spyware/Adware

❑Spyware is persistent and difficult to remove.

- An infection will involve an installer, a downloader, scripts in *Temp* folders and *.ini* files, a *.dll* library, and entries including executable code in the registry.
- If one part of the spyware is deleted, the other parts re-create it. Some parts are locked by the OS and can't be easily deleted.
- Some spyware uses root-kits to evade detection and removal.

Browser Hijackers

❑ Various types of spyware which target the internet browser:

- BHO: browser helper objects. ActiveX controls and purpose written programs which attach themselves to your browser, usually in the form of toolbars or media players.
- ActiveX controls: Unlike Javascript, these programs do not run in a sandbox – they have access to the browser's DOM and the hard drives of the PC.
- Trojans and root-kits which install themselves as services or in auto-execute locations (startup folder, registry, ***.ini/bat/com/exe/sys/dll*** files).

Browser Hijackers

- These programs change the way the browser behaves. They may turn off security settings, open ports, add web sites to the favorites list, add or replace toolbars, change the default home page, download and install software.
- They are hard to get rid of – often storing self-executing and installing code in many places in the PC.
- Most browsers are susceptible because they support client-side scripting – both Javascript and VB script are used extensively.

Bots and Botnets

- ❑ AI or proxy malware designed to allow attacker remote control of “zombie” computer.
- ❑ Used for spying, DDOS attacks, relaying SPAM, anything the customer wants.

Bots

- Spider Bots (web spiders/crawlers)
  - Browse the web by hyperlinks with the objective of retrieving and indexing web content.
- Scraper Bots
  - Read data from websites with the objective of saving them offline and enabling their reuse
- Spam Bots
  - An Internet application designed to gather email addresses for spam mailing lists.

RATS

- Remote Access Trojan (RATs)
- Written for net admins (!?)
- Recognised as malware by A/V
- Undetectable, silent install, includes rootkit.
- Many features

gh0st-RAT

❑ Used in gh0st-NET
(BOT NET used for spying)

❑ Many features

❑ Can stream audio, video, keystrokes, documents.

❑ read and answer/compose e-mails (via desktop remote control).

Storm

❑ Grew to a very big (>10,000,000) BOT NET

❑ Details: http://en.wikipedia.org/wiki/Storm_Worm

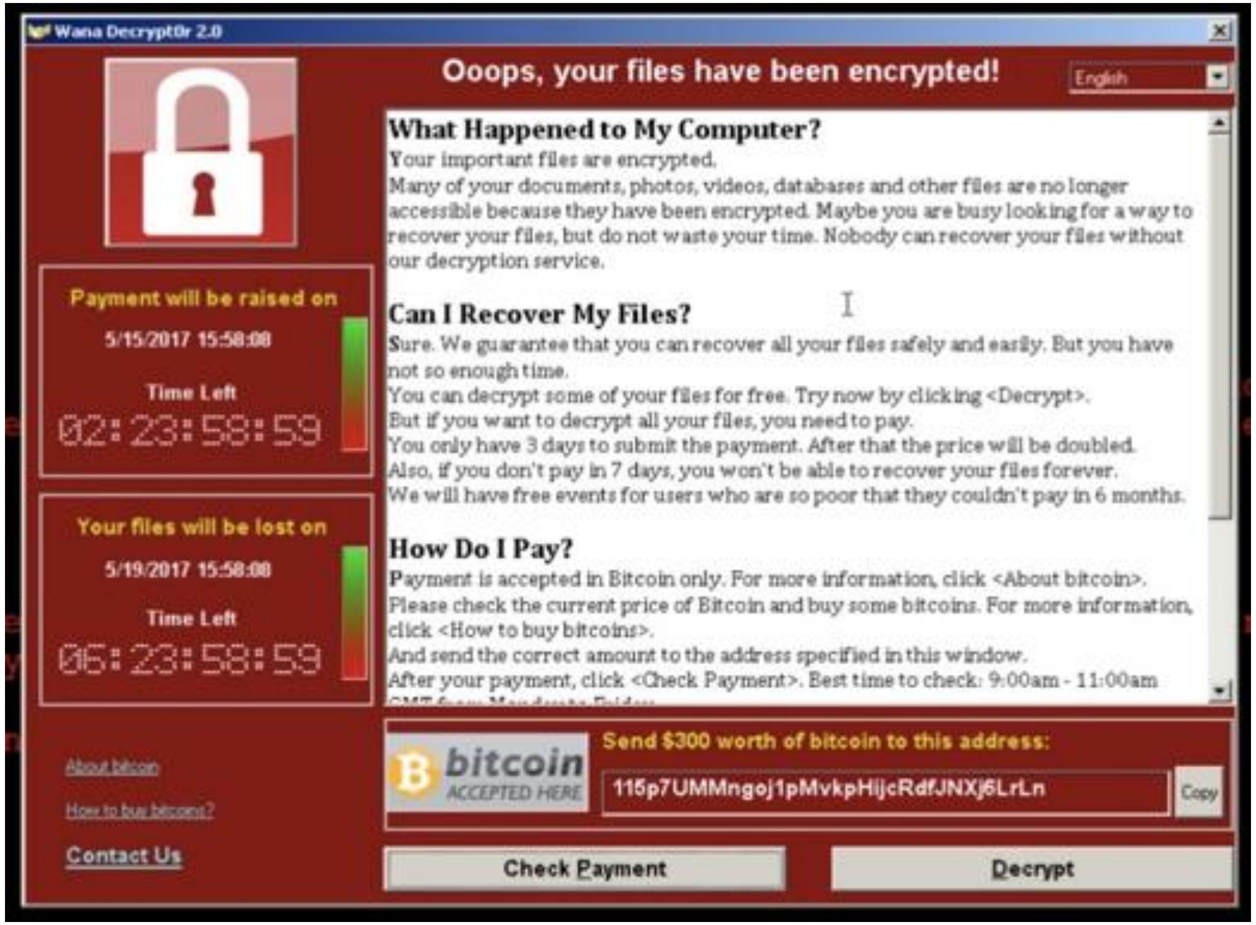
❑ Reduced by Microsoft MSRT:

https://www.computerworld.com/article/2536783/microsoft--we-took-out-storm-botnet.html

❑ and poisoned updates:

https://www.computerworld.com/article/2786943/researchers--poison--storm-botnet.html

WannaCry



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 GMT from Monday to Friday.

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

WannaCry

- 12-15 May 2017
- Infected >250,000 computers in the first day
- Spread to >150 countries
- Suspected to have been stolen from the NSA's cache or weaponised malware.
- Security researcher (Darien Huss) found "Kill Switch" by analysing code – 3 URLs which if successfully contacted by worm would cause it to shut down.

WannaCry

❑ EternalBlue (CVE-2017-0145) vulnerability in SMB version 1.

❑ Microsoft initially declares it won’t fix the bug

- Win10 not affected. XP-Win8 vulnerable
- Trojan dropper drops WannaCrypt ransomware
- Changes wallpaper

WannaCry

- ❑ Creates the mssecsvc2.0 service to ensure persistence of mssecsvc.exe
  - Changes registry keys
- ❑ Encrypts a massive number of data file types
  - Deletes volume shadow copies (backups)
  - Demands $300, $600 in Bitcoin
  - Spreads throughout LAN on port 445
  - Uses DOUBLEPULSAR shellcode to spread infection
  - 32 and 64-bit OS support

Detection / Removal

❑ Detection of malware is patchy. Relying on a single security product is unwise. You should keep several products in use

- keep them updated with the latest virus / spyware signatures.

❑ Be prepared to boot into safe mode – this disables many drivers and may disable the spyware long enough for you to remove it.

❑ Boot into another OS – Live CD running Linux – and scan / remove malware from there.

Detection / Removal

- Use the internet (on a different PC) to search for tools / procedures for removing specific threats
- Some may be impossible to remove by normal means.
- If all else fails, reformat the hard disk and install everything fresh.

- The best protection is NOT TO GET INFECTED!

Detection / Removal

❑ To prevent re-infection, reduce risky practices:

- Use a limited account.
- Never go on the internet while logged on as admin/root.
- Spyware will not be able to write to the registry or *system32* folder.
- Be cautious of what you install – many games (including some versions of Warcraft) and amusing toys (are trojans) install malware along with the intended application.
- Never install anything that you didn’t go looking for.
- Test suspect programs in a sandbox, VM or test machine

Android Malware Intelligence: Attack and Defence

- Bhat, Parnika, and Kamlesh Dutta. "A Survey on Various Threats and Current State of Security in Android Platform." *ACM Computing Surveys (CSUR)* 52, no. 1 (2019): 21.
- Xiao Chen, Chaoran Li, Derui Wang, Sheng Wen, Jun Zhang, Surya Nepal, Yang Xiang, and Kui Ren, “Android HIV: A Study of Repackaging Malware for Evading Machine-Learning Detection,” IEEE Transactions on Information Forensics and Security, vol. 15, no. 1, pp. 987-1001, 2020. [**Swinburne Cybersecurity Lab**]

Android Malware Statistics

# of malware samples at 2017: 22 millions

# of apps in Google Play at 2017: 3.6 millions

Android Malware Detection in Academia

- ❑ Researchers claimed that with machine-learning, the detection rate are very high:
  - *E.g.* Drebin [NDSS 2014, cited by 987] 94%
  - MaMaDroid [NDSS 2017, cited by 98] 99%
- ❑ However, they have a hidden assumption – training and testing data has the same distribution, which is unlikely to be true in real world.
- ❑ What if an adversary exists, and tries to evade the detection of these systems?
  (e.g. malware variants, malware evolution)

Attack Targets --- Machine learning detections

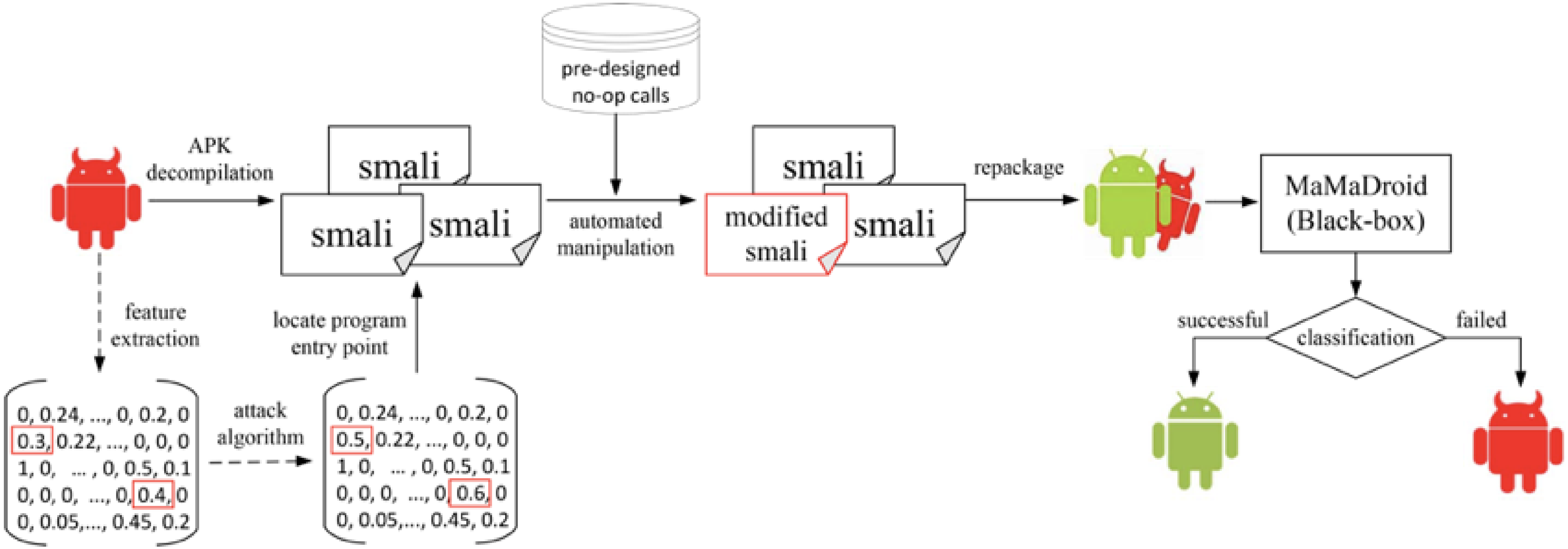
❑ Drebin [NDSS 2014]

- Use syntactic features
- Binary features extracted from *manifest* and *dexcode*
- *E.g.* permissions, APIs, components, *etc.*

❑ MaMaDroid [NDSS 2017]

- Use semantic features
- Markov chains generated from Control-Flow-Graphs
- Use transition probabilities as features *(e.g. android_to_android; self-defined_to_google, etc.)*

Attack Methodology Overview



$$\left(\begin{array}{l} 0, 0.24, \dots, 0, 0.2, 0 \\ \boxed{0.3,} 0.22, \dots, 0, 0, 0 \\ 1, 0, \quad \dots, 0, 0.5, 0.1 \\ 0, 0, 0, \quad \dots, 0, \boxed{0.4,} 0 \\ 0, 0.05, \dots, 0.45, 0.2 \end{array}\right) \xrightarrow{\text{attack algorithm}} \left(\begin{array}{l} 0, 0.24, \dots, 0, 0.2, 0 \\ \boxed{0.5,} 0.22, \dots, 0, 0, 0 \\ 1, 0, \quad \dots, 0, 0.5, 0.1 \\ 0, 0, 0, \quad \dots, 0, \boxed{0.6,} 0 \\ 0, 0.05, \dots, 0.45, 0.2 \end{array}\right)$$

Our Malware Dataset

❑ We have collected Android malware samples from VirusShare from 2012 to 2019, we excludes the ones cannot be processed by reverse engineering tools

- approx. 90,000 malware samples
- 485GB in size