ETH zürich

Discussion exercise sheet 9

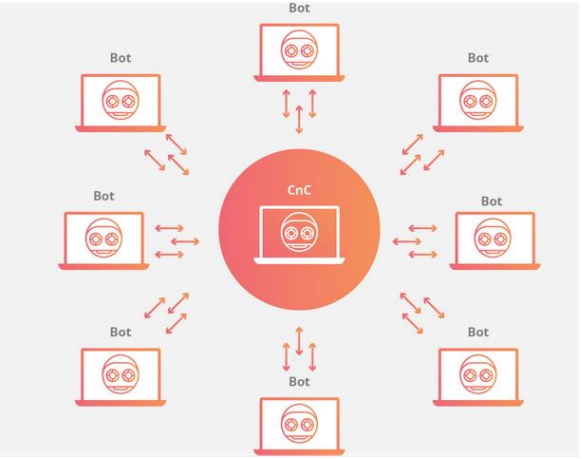
Marc-Philippe Bartholomä
Student Assistant for Network Security 2020
19 November 2020, At home

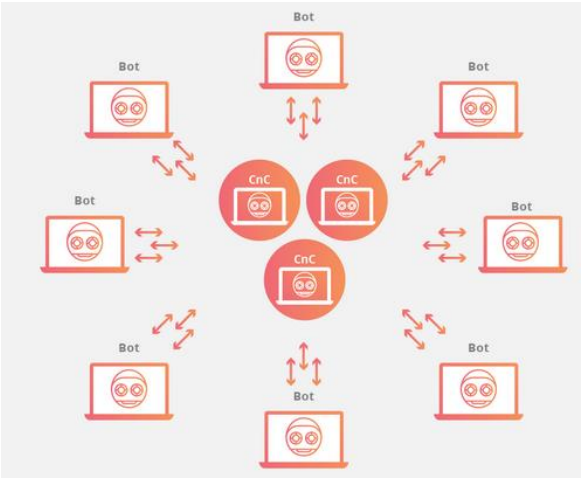
Question 1 - Mirai

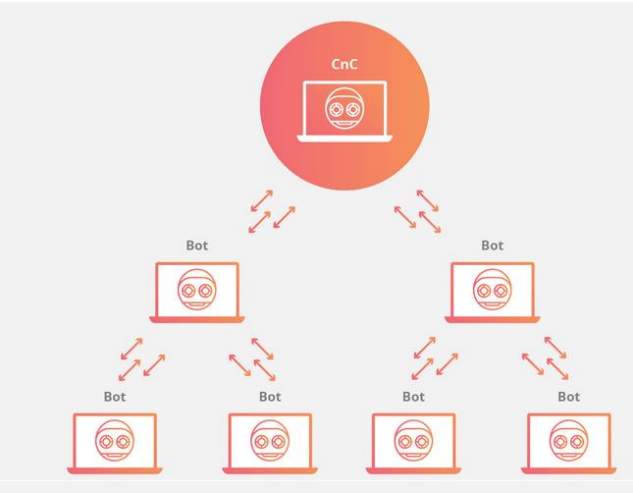
It just means future and the botnet was named after an anime series.

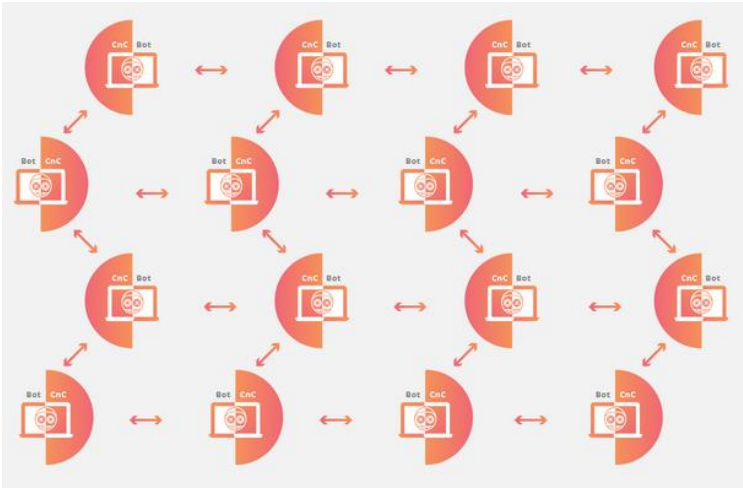
Question 1 – Mirai

- Related Material: 08-DDoS: slide 12-26
- Question: Botnet components









Rule of Thumb: Bot is more about the software, Zombie more about the machine.

https://www.cloudflare.com/learning/ddos/what-is-a-ddos-botnet/

Question 1 – Mirai

- Question: Victims

DYN

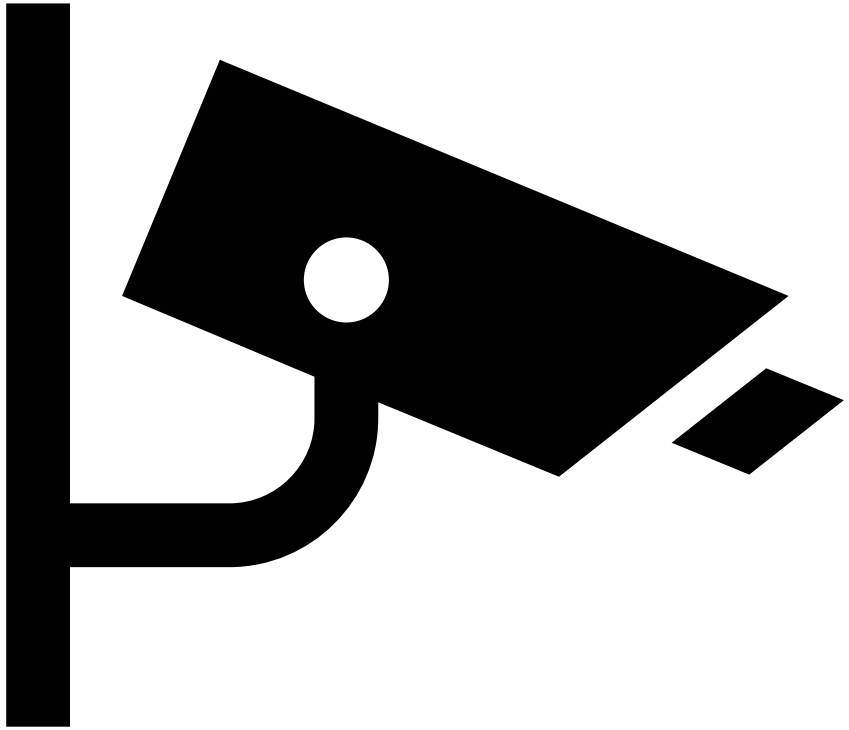
>= 1 Tbit/s

OVH.com

620 Gbit/s

Question 1 – Mirai

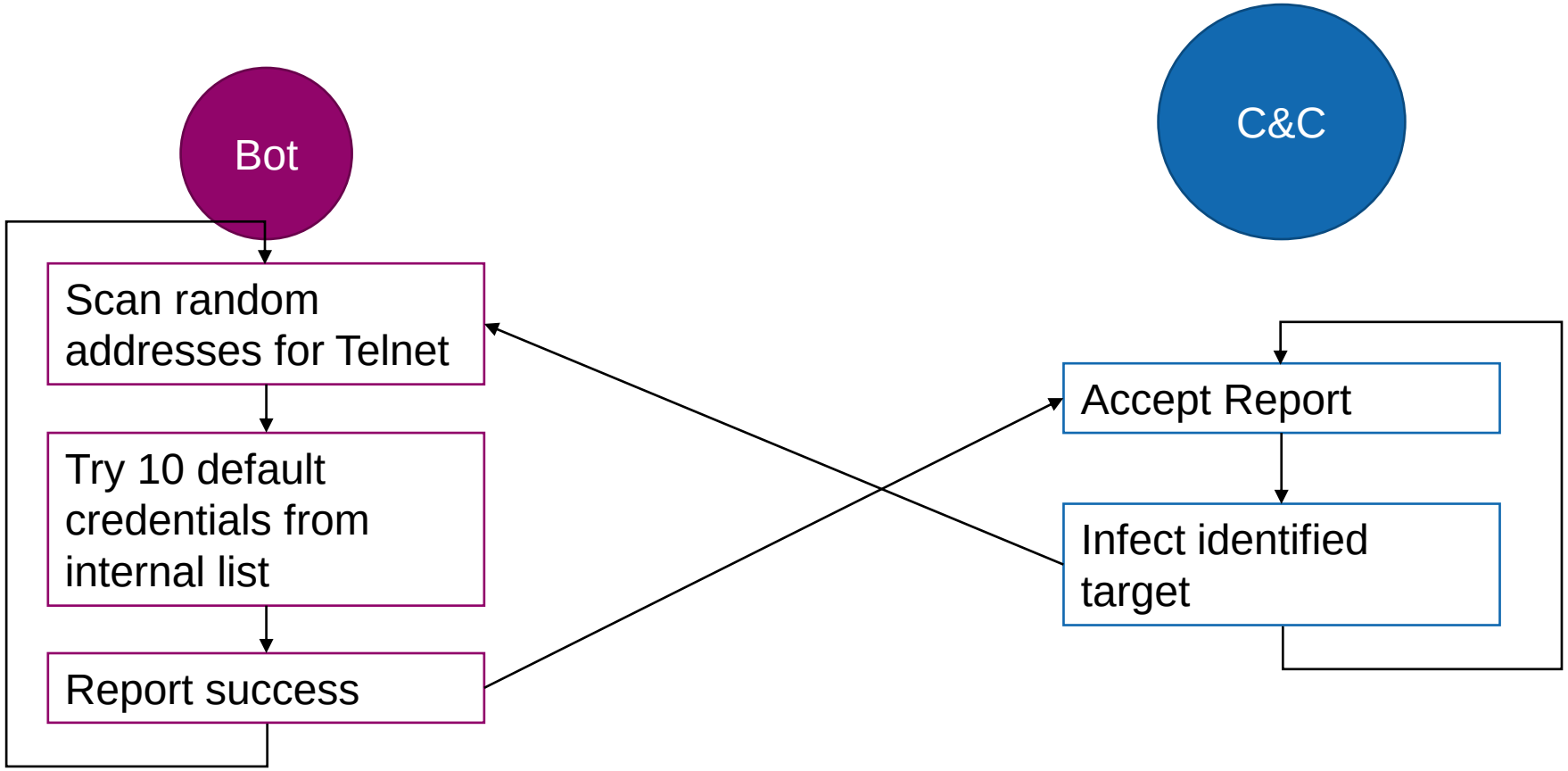
- Question: Spreading



```
User: admin
Password: admin
```

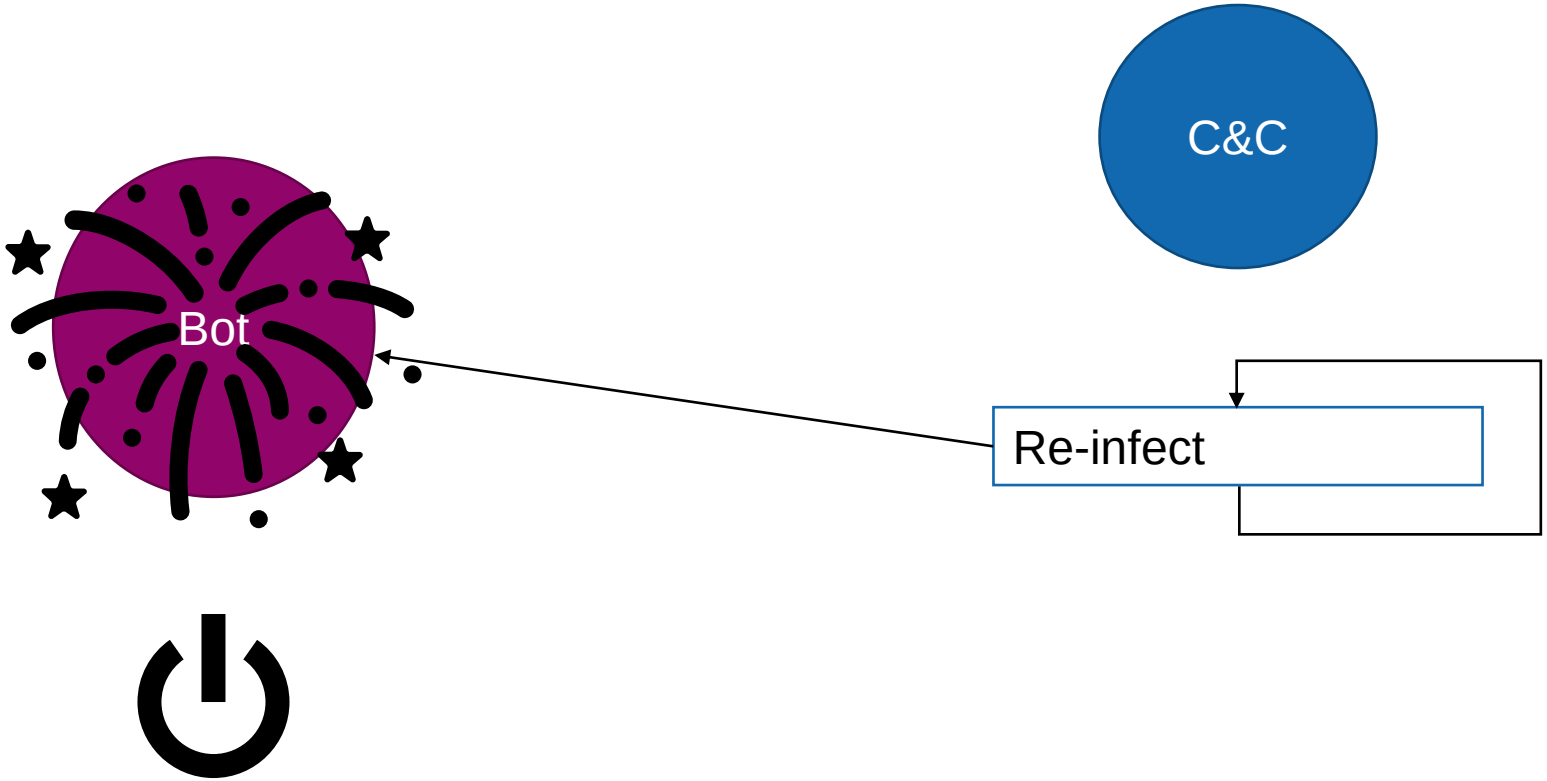
Question 1 – Mirai

- Question: Spreading in detail



Question 1 – Mirai

- Question: Persistence



Question 2 – Stuxnet

Question 2 – Stuxnet

- Question: AntiVirus

Injection Technique

Whenever an export is called, Stuxnet typically injects the entire DLL into another process and then just calls the particular export. Stuxnet can inject into an existing or newly created arbitrary process or a preselected trusted process. When injecting into a trusted process, Stuxnet may keep the injected code in the trusted process or instruct the trusted process to inject the code into another currently running process.

The trusted process consists of a set of default Windows processes and a variety of security products. The currently running processes are enumerated for the following:

- Kaspersky KAV (avp.exe)
- Mcafee (Mcshield.exe)
- AntiVir (avguard.exe)
- BitDefender (bdagent.exe)
- Etrust (UmxCfg.exe)
- F-Secure (fsdfwd.exe)
- Symantec (rtvscan.exe)
- Symantec Common Client (ccSvcHst.exe)
- Eset NOD32 (ekrn.exe)
- Trend Pc-Cillin (tmpproxy.exe)

Question 2 – Stuxnet

- Question: AntiVirus – Air-Gap
- Hard to update signatures
- Increases Attack Surface
- Might disrupt normal operation

Bitdefender kämpft mit schweren Sicherheitsproblemen

Bis zu vier Anläufe brauchte der Hersteller, um insgesamt 10 kritische Sicherheitslücken zu beseitigen.

Lesezeit: 2 Min. 49

Bitdefende

UPDATE 11.11.2020 4:42 Uhr | Security

Von Jürgen Schmidt

Ein Informatikstudent hat gleich 10 Fehler in der Speicherverwaltung von Bitdefenders Antivirus-Software entdeckt. Die meisten davon dürften sich ohne allzu großen Aufwand dazu nutzen lassen, eigenen Code einzuschleusen und

Vulnerabilities were in unpacking compressed UPX files. Article (German) Original Blogpost

Question 2 – Stuxnet

- Question: Spreading
- USB-Drives for airgaps
- Network using various vulnerabilities

- New infection vectors

Question 2 – Stuxnet

TS//SI//REL) IRATEMONK provides software application persistence on desktop
ınd laptop computers by implanting the hard drive firmware to gain execution
hrough Master Boot Record (MBR) substitution.

- Question: Persistence

The driver file is a digitally signed with a legitimate Realtek digital certificate. The certificate was confirmed as compromised and revoked on July 16, 2010 by Verisign.

The driver scans the following filesystem driver objects:

- \FileSystem\ntfs
- \FileSystem\fastfat
- \FileSystem\cdfs

A new device object is created by Stuxnet and attached to the device chain for each device object managed by these driver objects. The MrxNet.sys driver will manage this driver object. By inserting such objects, Stuxnet is able to intercept IRP requests (example: writes, reads, to devices NTFS, FAT or CD-ROM devices).

Two types of files will be filtered out from a query directory result:

- Files with a ".LNK" extension having a size of 4,171 bytes.
- Files named "~WTR[FOUR NUMBERS].TMP", whose size is between 4Kb and 8Mb; the sum of the four numbers modulo 10 is null. For example, 4+1+3+2=10=0 mod 10

These filters hide the files used by Stuxnet to spread through removable drives, including:

- Copy of Copy of Copy of Copy of Shortcut to.lnk
- Copy of Copy of Copy of Shortcut to.lnk
- Copy of Copy of Shortcut to.lnk
- Copy of Shortcut to.lnk
- ~wtr4132.tmp
- ~wtr4141.tmp

Only IRATEMONKE survives OS reinstallation.

Question 2 – Stuxnet

- Question: Ways of getting a certificate

Answer in Zoom poll: What did they do and what would you do? Results integrated in slide!

- Steal it through cyber attack (Stuxnet way: 3, your way: 2)
- **Steal it physically by breaking in*** (Stuxnet way: 3, your way: 0)
- Steal an identity and buy the certificate (Stuxnet way: 0, your way: 1)
- Compromise a CA (Stuxnet way: 3, your way: 2)
- Force the CA to issue a certificate (Stuxnet: 3, your way: 3)
- Run your own CA (Stuxnet: 1, your way: 5)
- Don’t, abuse a vulnerability in certificate verification (Stuxnet: 0, your way: 0)

* This is what was most likely done for Stuxnet.

Question 2 – Stuxnet

- Question: Cost & Resource Requirements

Hacking Team Founder: 'Hacking Team is Dead'

The company's former CEO posted a bizarre obituary on LinkedIn saying the infamous surveillance firm is "definitely dead."

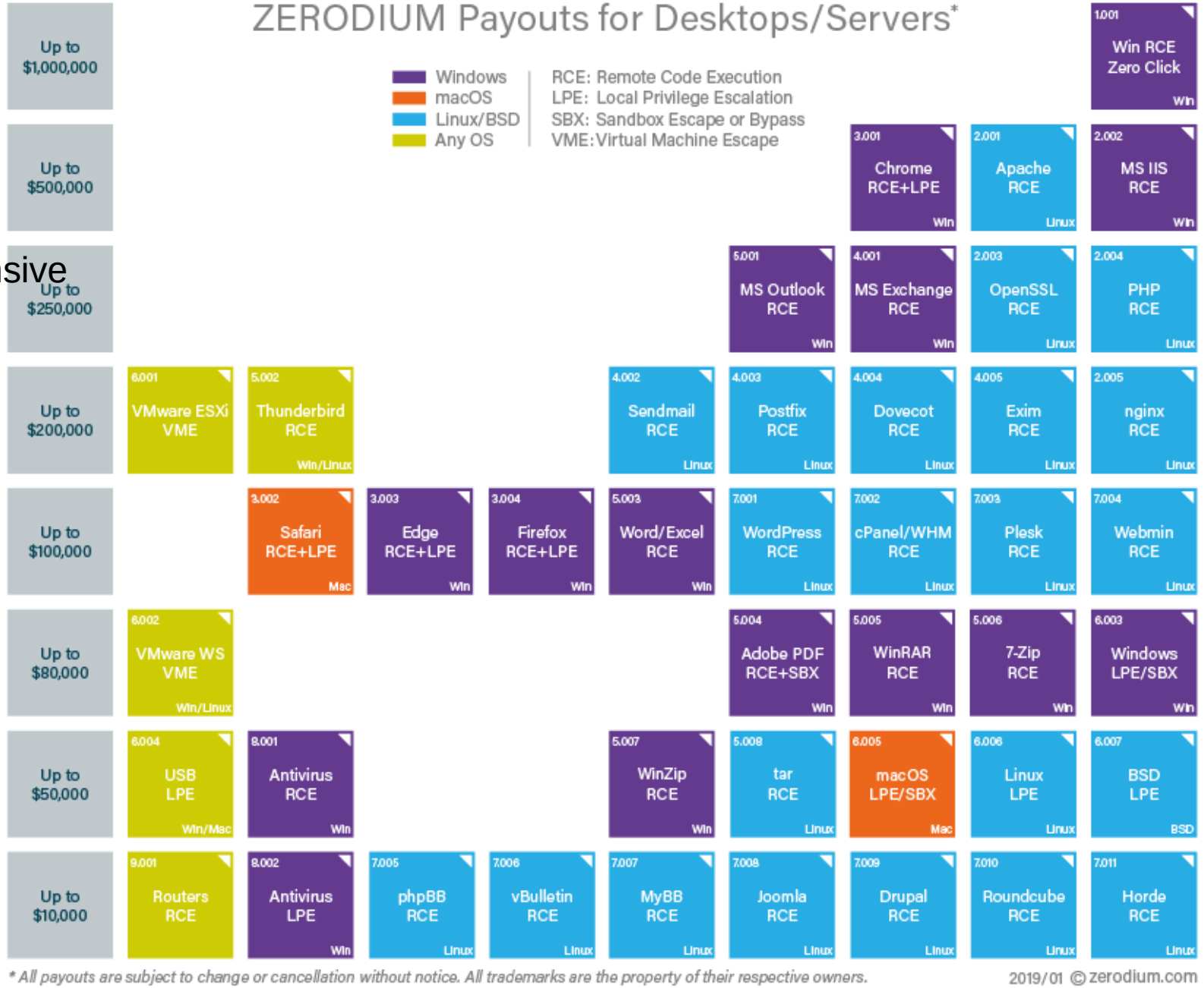
By Lorenzo Franceschi-Bicchierai

May 26, 2020, 8:31pm

https://www.vice.com/en/article/n7wbnd/hacking-team-is-dead

Question 2 – Stuxnet

- Question: Cost
- 0day vulnerabilities are expensive



Question 2 – Stuxnet

- Question: Counter-measures

Pick 2-4 promising countermeasures in the Zoom poll
Results integrated in slide!

- Run security OS (e.g. SEL4) instead of Windows (Picked: 7)
- Physically block USB ports (Picked: 7)
- Guard with Machine Gun and EMP (Picked: 2)
- Only trust internal CA (Picked: 9)
- Setup honeypots (e.g. fake centrifuge) (Picked: 1)
- Virtualize centrifuge programming to visualize it before carrying it out (Picked: 5)
- Insert all changes to your system into a blockchain (Picked: 2)
- Use Machine Learning to capture usual behavior (Picked: 1)
- Add independent sensors to analyze accidents after the fact (Picked: 2)
- Develop cyberweapons for deterrence (Picked: 2)

Your Questions