Malware Uncertainty Principle: an alteration of malware behavior by close observation

María José Erquiaga, Sebastián García and Carlos García Garino

Botconf 2018, Montpellier, France

Researcher, teacher, master student

MaryJo_E

Plan

- Motivation and contribution
- Background
- Nomad project
- HTTPs Dataset
- Analysis and discussion
- Conclusion and future work

Motivation

Study the **influence** of web **TLS** interceptor **proxies** for network malware analysis.

Contribution

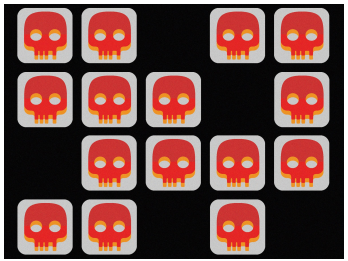
1. Creation of a network **malware capture dataset.**
   Goal → capture malware using **TLS, SSL** or port **443.**
   Two scenarios with and without MITM proxy interception.

2. **Publication** of the dataset

3. **Analysis** → malware network **behavior**.

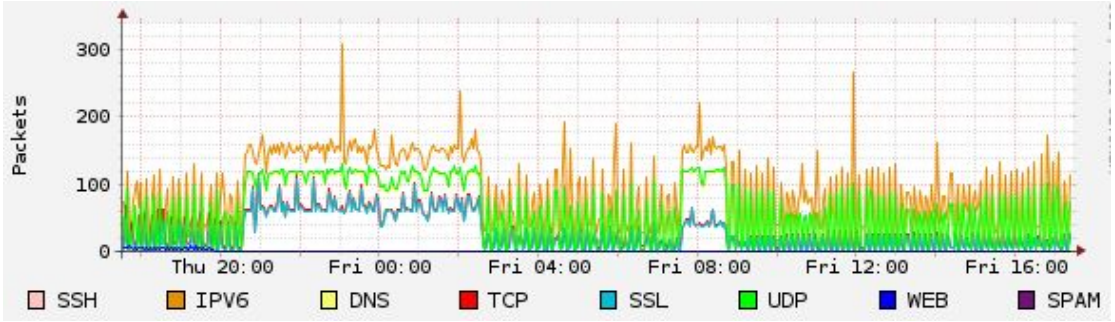
Background

- **TLS** (Transport Layer Security)
  - Security protocol for **encrypting** information
- **Malware** increases and **evolves**
  - Is hard to understand the **behavior** and to **detect**
- **Evolution** → **Malware uses HTTPS** (SSL, TLS).
  - Harder to detect (e.g. banking trojan, Zeus)



Nomad Project

- CISCO Systems CTA, CVUT University Prague, UNCuyo Argentina
- Goal: HTTPS Malware capture



HTTPs Malware dataset

Nomad Dataset → **150** network malware traffic **captures.**
Different types of malware (Botnet, trojans, adware, etc)

To obtain a good HTTPs malware captures we considered:

1. **Study the malware**: checking if it is **HTTPs based** malware
2. Keep the **infection running**.

Nomad Project (Lab Infrastructure)

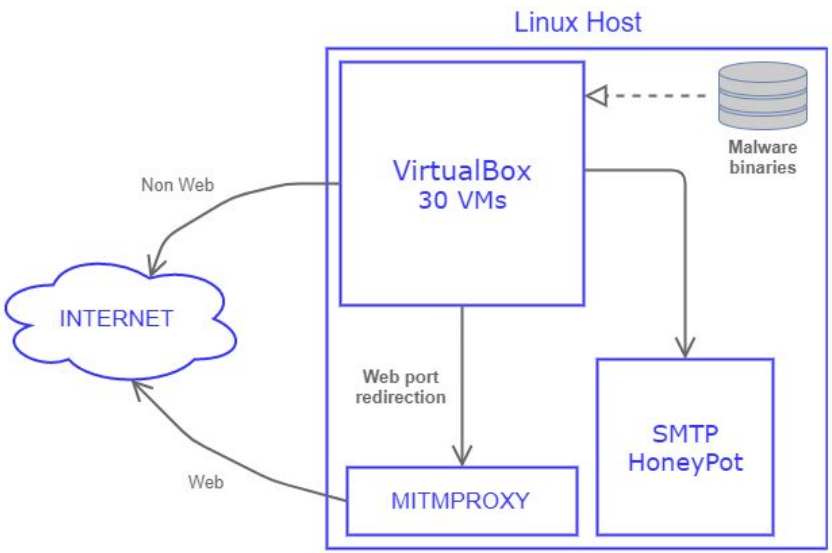


Fig 1. *First scenario, malware traffic with MITMproxy interception*

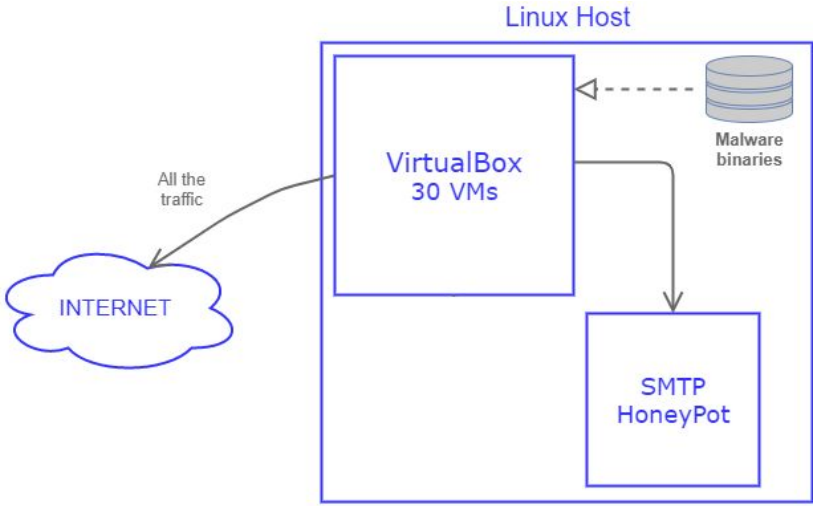


Fig 2. *Second scenario, malware traffic without proxy interception*

Capture methodology

1. **Find** malware binary in ***SSL Blacklist***
   a. Obtain it from Virus Total
2. **Copy** the binary to the server
3. **Start** the virtual machine and infect it
4. **Compute** the start date and the infection date and **monitoring** the machine
5. **Stop** the machine , **generate** output files and **publish** the capture. (twitter and blog [1])

SSL Certificate Information

Subject Common Name:	localhost
Subject:	C=GB, ST=Yorks, L=York, O=MyCompany Ltd., OU=IT, CN=localhost
Issuer Common Name:	localhost
Issuer:	C=GB, ST=Yorks, L=York, O=MyCompany Ltd., OU=IT, CN=localhost
SSL Version:	TLSv1
Fingerprint (SHA1):	2a5d840ba99228082bf70aa8ae416ffd4f868051
Status:	Blacklisted (Reason: Zeus C&C, Listing date: 2016-10-18 12:25:50)

[1]https://mcfp.felk.cvut.cz/publicDatasets/CTU-Malware-Capture-Botnet-188-1/

Analysis

- Malware capture analysis:
  - **pcap** and **mitm.out** files

- **Ports** and **IPs** contacted by the malware, check if the connection was **encrypted** or not.

Swrort (ID 188)

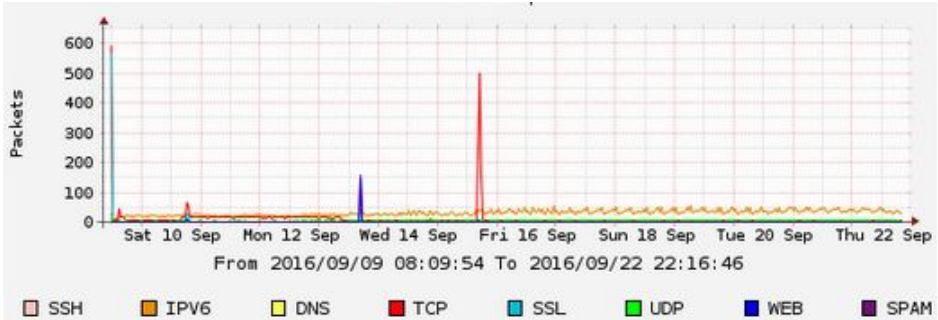


Fig 3. *Without mitmproxy interception [2]*

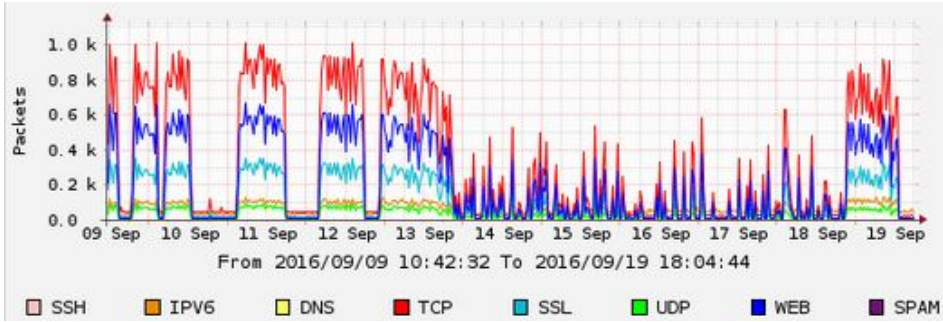


Fig 4 *With mitmproxy interception [1]*

[1] https://mcfp.felk.cvut.cz/publicDatasets/CTU-Malware-Capture-Botnet-188-1/
[2] https://mcfp.felk.cvut.cz/publicDatasets/CTU-Malware-Capture-Botnet-188-2/

Vawtrak (189)

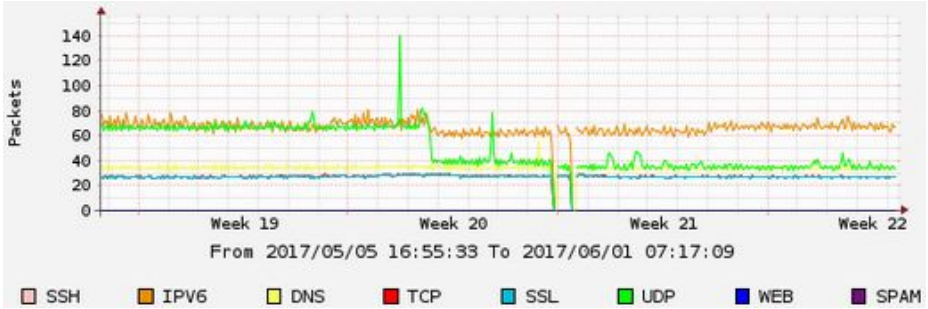


Fig 5. *Without mitmproxy interception [3]*

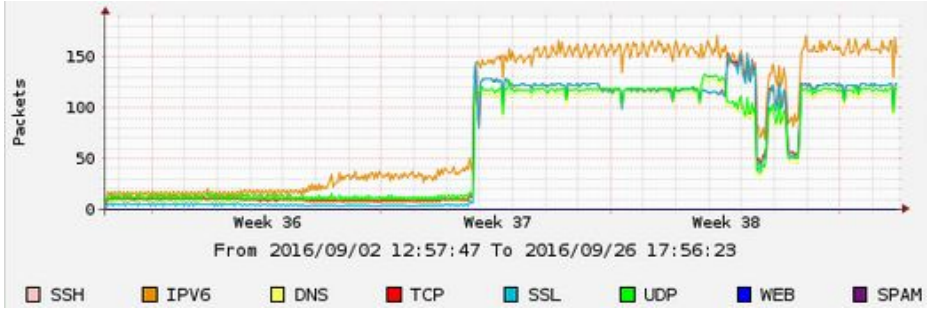


Fig 6. *With mitmproxy interception [4]*

[3] https://mcfp.felk.cvut.cz/publicDatasets/CTU-Malware-Capture-Botnet-189-2/
[4] https://mcfp.felk.cvut.cz/publicDatasets/CTU-Malware-Capture-Botnet-189-1/

Discussion I

1. In some cases, the malware was **not able** to **communicate** with the **Internet** at all!!!

Discussion I

1. In some cases, the malware was **not able** to **communicate** with the **Internet** at all!!!

↓

Custom protocol

Discussion I

1. In some cases, the malware was **not able** to **communicate** with the **Internet** at all!!!

↓

Custom protocol

↓

MITMProxy interception

```
HttpSyntaxException('Bad HTTP request line: HTTP/1.1 005',)
```

Discussion II

2. **Behaviors:**

   a) Tried to **reconnect** continually

   b) Seek **another way** to connect
   - Different **ports**
   - Other **servers**

Conclusion

- Some **malware** used a **custom protocol** on ports reserved for **HTTPs/HTTP (443, 80, 8080)**.
  - Blocking (MITMProxy) → **different** malware **behaviors.**
- Malware's **behavior** can **change** → intercepting **proxy**.
  - Proxy implementation should be **carefully considered** when analysing malware **behavior** in the **network**.
- **Dataset available** at stratosphere web site:
  - https://stratosphereips.org/category/dataset.html

Future work

Analyze other **features**

Malware using HTTPs

→ **IoT Lab**

Thank You!

 mariajoseerquiaga@gmail.com

 Maria_Erquiaga2

 MaryJo_E