Malware Labeling Practices

and what's wrong with them

Azqa Nadeem

PhD Student @ Cyber Security Group

TU Delft

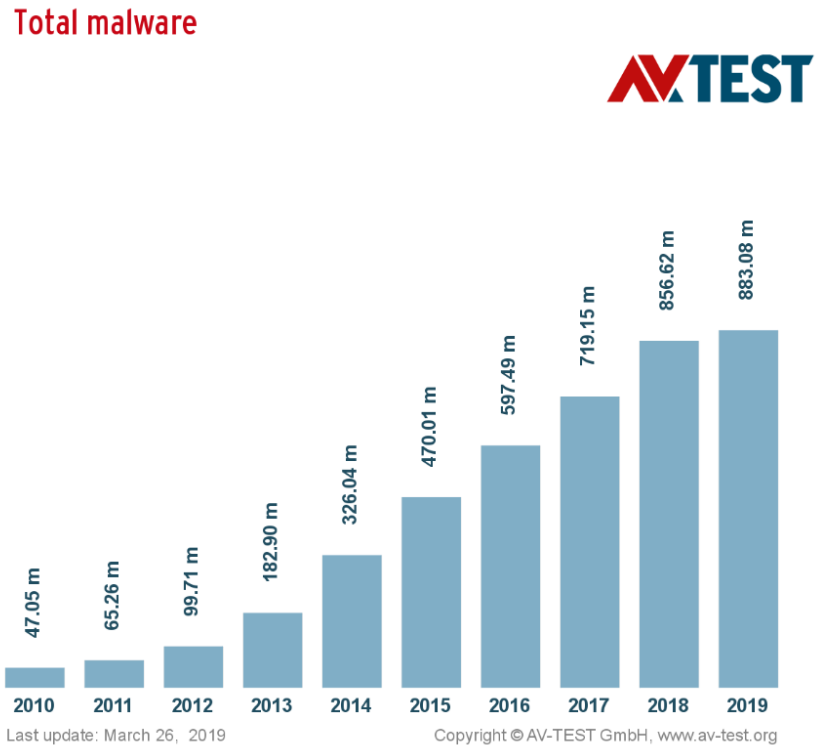
Agenda

- Introduction – Is malware a big deal?
- The role of malware family labels
- Problems with current family labelling practices
- Behavioural profiling as a potential solution
- Wrap-up

TU Delft

Introduction

Introduction



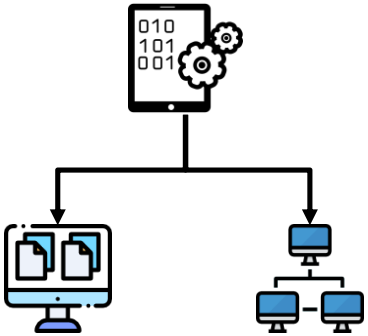
Introduction

- Growth of malware variants
  - Malware-as-a-service
  - DIY malware via leaked source code
  - Easy-to-use obfuscation tools

- Do we have a defense?
  - Anti-Virus and Anti-Malware vendors
  - Security companies
  - Security researchers

Introduction

- *How?*
  - *Static analysis*
  - *Dynamic analysis*
    - *System activity*
    - *Network traffic*



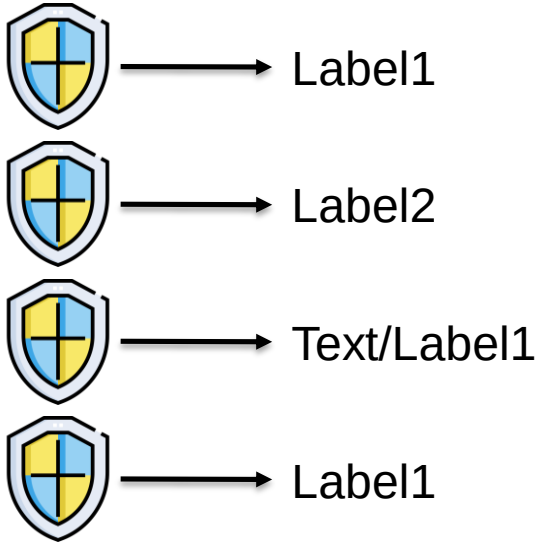
- *Research goals:*
  - *To distinguish malicious entities from benign ones*
  - *To dissect, analyze, and understand malware in order to categorize them in families*

TU Delft

Icons by Freepik from www.flaticon.com

Problems with current approach

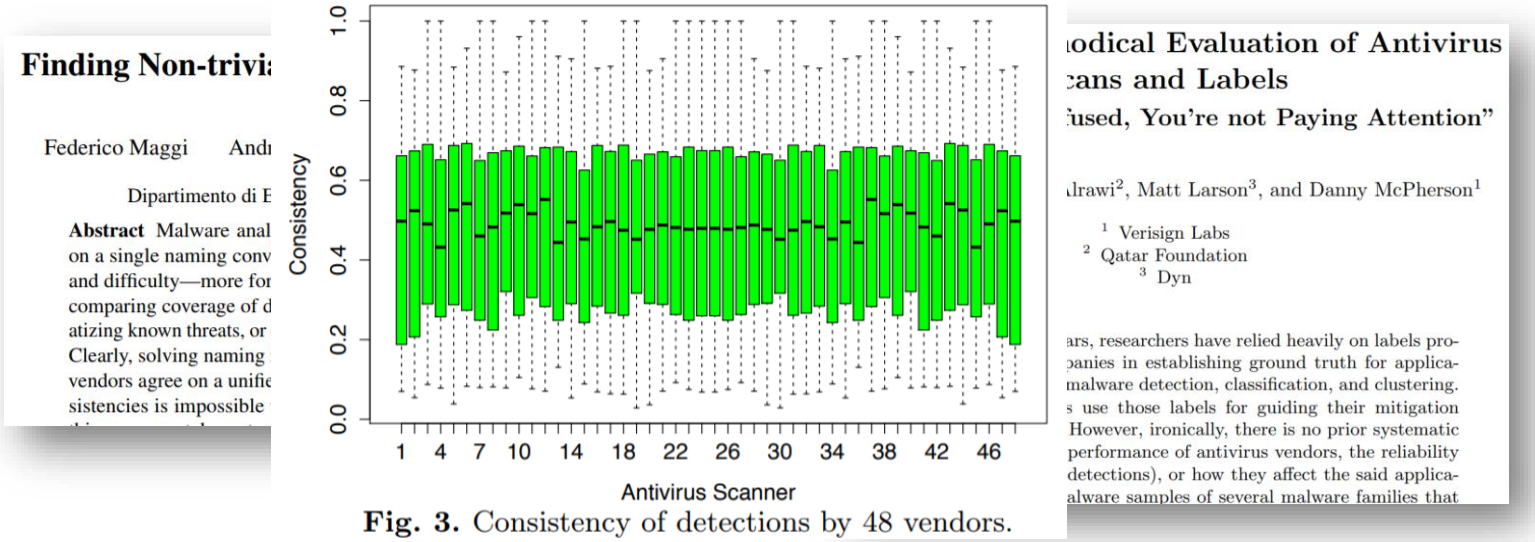
1. Inconsistent labeling
2. No consensus on common vocabulary



Icons by Freepik from www.flaticon.com

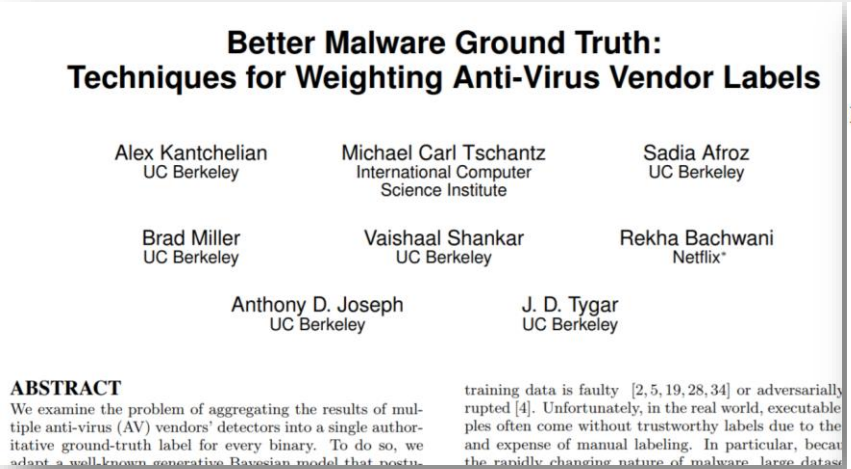
Problems with current approach

1. Inconsistent labeling
2. No consensus on common vocabulary



Problems with current approach

1. Inconsistent labeling
2. No consensus on common vocabulary



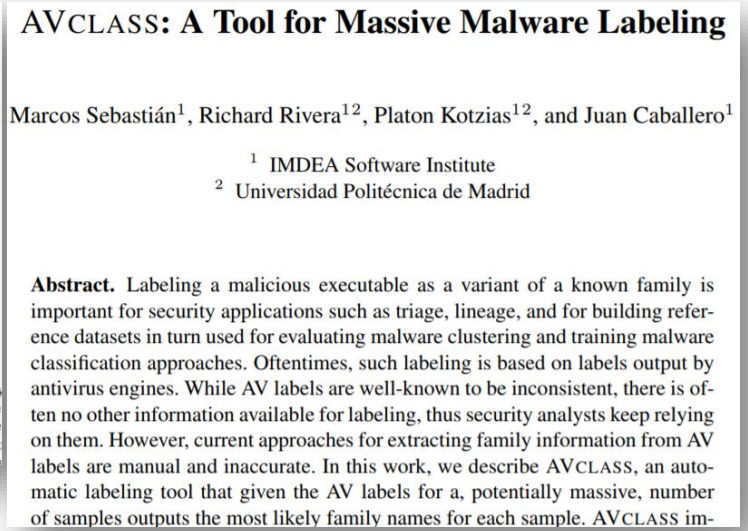
Better Malware Ground Truth: Techniques for Weighting Anti-Virus Vendor Labels

Alex Kantchelian, UC Berkeley
Michael Carl Tschantz, International Computer Science Institute
Sadia Afroz, UC Berkeley
Brad Miller, UC Berkeley
Vaishaal Shankar, UC Berkeley
Rekha Bachwani, Netflix*
Anthony D. Joseph, UC Berkeley
J. D. Tygar, UC Berkeley

ABSTRACT

We examine the problem of aggregating the results of multiple anti-virus (AV) vendors' detectors into a single authoritative ground-truth label for every binary. To do so, we adapt a well-known generative Bayesian model that postu-

training data is faulty [2, 5, 19, 28, 34] or adversarially rupted [4]. Unfortunately, in the real world, executable ples often come without trustworthy labels due to the and expense of manual labeling. In particular, becau the rapidly changing nature of malware, large datas



AVCLASS: A Tool for Massive Malware Labeling

Marcos Sebastián[1], Richard Rivera[1,2], Platon Kotzias[1,2], and Juan Caballero[1]

[1] IMDEA Software Institute
[2] Universidad Politécnica de Madrid

Abstract. Labeling a malicious executable as a variant of a known family is important for security applications such as triage, lineage, and for building reference datasets in turn used for evaluating malware clustering and training malware classification approaches. Oftentimes, such labeling is based on labels output by antivirus engines. While AV labels are well-known to be inconsistent, there is often no other information available for labeling, thus security analysts keep relying on them. However, current approaches for extracting family information from AV labels are manual and inaccurate. In this work, we describe AVCLASS, an automatic labeling tool that given the AV labels for a, potentially massive, number of samples outputs the most likely family names for each sample. AVCLASS im-

Problems with current approach

1. Inconsistent labeling
2. No consensus on common vocabulary
   - Reliability of proposed malware analysis methods

Problems with current approach

1. Inconsistent labeling
2. No consensus on common vocabulary
3. Different aspects not taken into account
4. Current practices heavily use static and system-level

Problems with current approach

Variant 1:
TR/Dropper.Gen

File System Operations

```
Delete c:\docume~1\admini~1\locals~1\temp\tmp1.tmp
Read   \\?\globalroot\systemroot\system32\msvcrt.dll
Write  c:\docume~1\admini~1\locals~1\temp\tmp1.tmp
```

HTTP Traffic

```
[1249356561 192.168.14.2:1037 => 94.247.2.193:80]
POST /cgi-bin/generator HTTP/1.0
Content-Length: 45
[... DATA ...]

[1249356562 192.168.14.2:1038 => 94.247.2.193:80]
POST /extra.php HTTP/1.0
Content-Type: application/x-www-form-urlencoded
Content-Length: 44
[... DATA ...]
```

Variant 2:
DR/PCK.Tdss.A.21

File System Operations

```
Delete c:\docume~1\admini~1\locals~1\temp\tmp4.tmp
Delete c:\docume~1\admini~1\locals~1\temp\tmp5.tmp
Write  c:\docume~1\admini~1\locals~1\temp\tmp5.tmp
Read   \\?\globalroot\systemroot\system32\advapi32.dll
Write  c:\docume~1\admini~1\locals~1\temp\tmp4.tmp
Write  c:\docume~1\admini~1\locals~1\temp\nso3.tmp\modern-header.bmp
Delete c:\docume~1\admini~1\locals~1\temp\nso3.tmp
Write  c:\docume~1\admini~1\locals~1\temp\matrix329411.exe
Read   (MALWARE_PATH)
Delete c:\docume~1\admini~1\locals~1\temp\nsc1.tmp
```

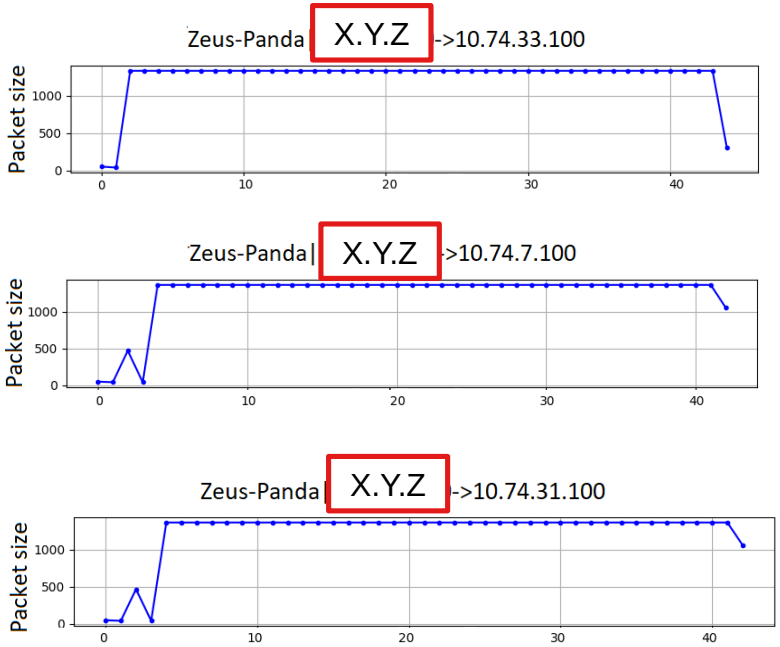
HTTP Traffic

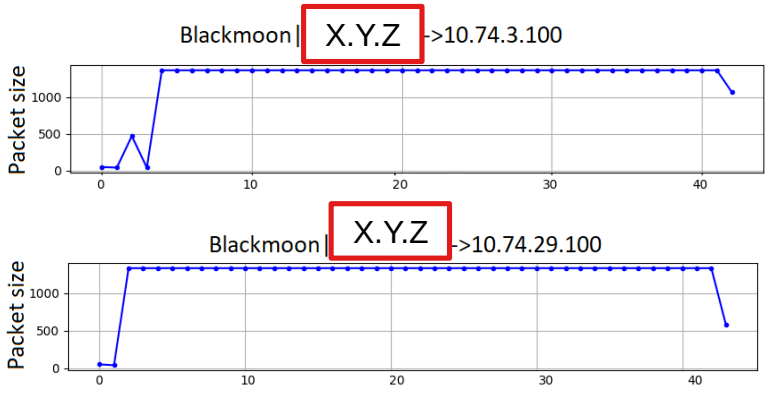
```
[1249345674 192.168.12.2:1034 => 94.247.2.193:80]
POST /cgi-bin/generator HTTP/1.0
Content-Length: 45
[... DATA ...]

[1249345674 192.168.12.2:1038 => 94.247.2.193:80]
POST /extra.php HTTP/1.0
Content-Type: application/x-www-form-urlencoded
Content-Length: 44
[... DATA ...]
```

Example from: *Perdisci, R., Lee, W., & Feamster, N. (2010, April). Behavioral Clustering of HTTP-Based Malware and Signature Generation Using Malicious Network Traces. In NSDI (Vol. 10, p. 14).*

Problems with current approach





Problems with current approach

1. Inconsistent labeling
2. No consensus on common vocabulary
3. Different aspects not taken into account
4. Current practices heavily use static and system-level
   - Interesting patterns missed because of different classification
   - Customized way of grouping

Problems with current approach

1. Inconsistent labeling
2. No consensus on common vocabulary
3. Different aspects not taken into account
4. Current practices heavily use static and system-level
5. Limited interpretability of labels

Problems with current approach

1. Inconsistent labeling
2. No consensus on common vocabulary
3. Different aspects not taken into account
4. Current practices heavily use static and system-level
5. Limited interpretability of labels
   - Impossible to derive information from family labels

Proposed Solution

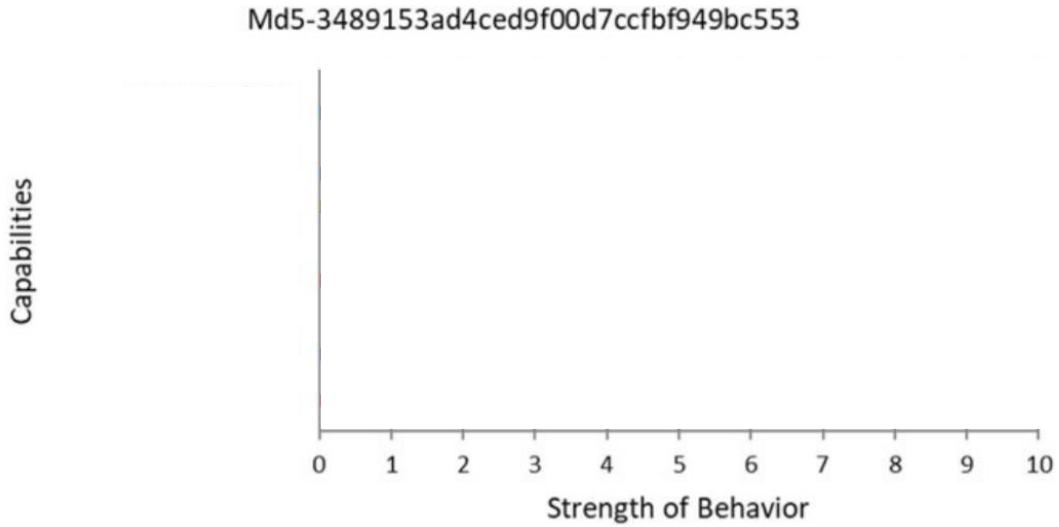
- Behavioral profiles instead of family labels

vs. ZeuS

- Behavioral profiles build on capability assessment

Icons by Smashicons from www.flaticon.com

Behavioral Profiling



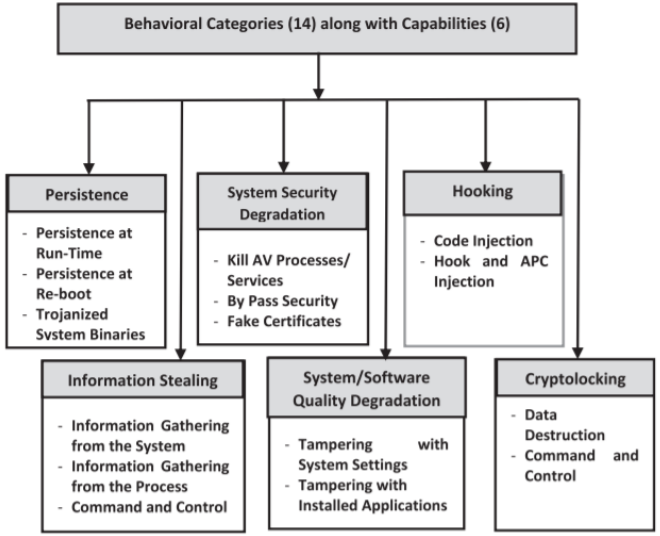
Malware Capability Assessment using Fuzzy Logic. Sharma, A., Gandotra, E., Bansal, D., & Gupta, D. (2019). Cybernetics and Systems, 1-16.

Manual Capability Assessment

Table 2 – MAEC capabilities and the behaviours used in this paper.

MAEC Capability	Behaviour Name
Command and Control	Configuration
Remote Machine manipulation	
Privilege escalation	
Data theft	Info Stealing, Injection
Spying	Screenshot, Video Capture
Secondary Operation	
Anti-detection	Anti-Analysis
Anti-code analysis	Anti-Analysis
Infection/Propagation	
Anti-behavioural analysis	Anti Analysis
Integrity violation	Process Injection
Data Exfiltration	Network Communications
Probing	
Anti-removal	Persistence
Security degradation	Info Stealing, Injection
Availability violation	
Destruction	
Fraud	Configuration, Info Stealing, Injection
Persistence	Persistence
Machine access/control	Backconnect, Network Communications

From: A survey of similarities in banking malware behaviors. Black, P., Gondal, I., & Layton, R. (2018). Computers & Security, 77, 756-772.



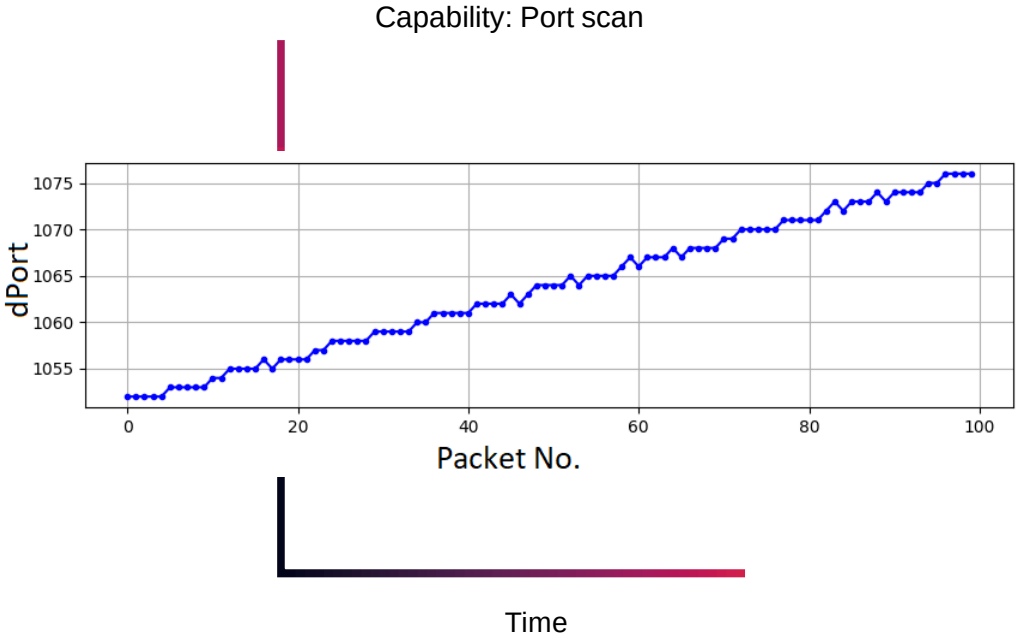
From: Malware Capability Assessment using Fuzzy Logic. Sharma, A., Gandotra, E., Bansal, D., & Gupta, D. (2019). Cybernetics and Systems, 1-16.

Automated Capability Assessment

Clus	# families	Behavior	Clus	# families	Behavior
c1	***9 (Common)***	SSDP traffic	c10	2	HTTPs traffic
c2	***9 (Common)***	Broadcast traffic	c11	2	C&C Reuse
c3	4	LLMNR traffic	c12	4	HTTPs traffic
c4	5	Systematic port scan	c13	5	Misc.
c5	5	Randomized port scar	c14	3	Misc.
c6	***1 (Rare)***	Connection spam	c15	3	Misc.
c7	***1 (Rare)***	Connection spam	c16	3	Misc.
c8	***1 (Rare)***	Malicious subnet	c17	3	Misc.
c9	***1 (Rare)***	Connection spam	c18	4	Misc.

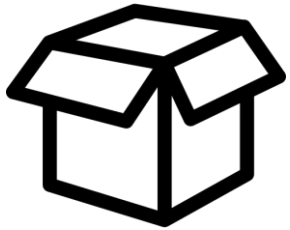
From: MalPaCA: Malware Packet Sequence Clustering and Analysis. Nadeem A., Hammerschmidt C., Ganan C. H., & Verwer S. Manuscript submitted for publication.

Automated Capability Assessment



Automated Capability Assessment

Network traces from malware families



	B	C	D	DL	GE	GI	R	Z	ZP	ZPa	Zv1	ZVA
SSDP traffic	X	X	X	X	X	X	X	X	-	X	-	X
Broadcast traffic	X	X	-	X	-	X	X	-	X	-	X	X
LLMNR traffic	X	X	-	X	-	X	-	-	-	-	-	-
System. port scan	X	X	-	-	-	X	X	-	-	-	-	X
Random. port scan	X	X	-	-	-	X	X	-	-	-	-	X
In conn spam	-	-	-	-	-	X	-	-	-	-	-	-
Out conn spam	-	-	-	-	-	X	-	-	-	-	-	-
Malicious Subnet	-	-	-	-	-	-	-	-	-	-	-	X
In HTTPs	-	X	-	X	-	X	-	-	-	X	-	-
Out HTTPs	-	-	-	-	-	X	-	-	-	X	-	-
C&C reuse	X	-	-	-	-	-	-	-	-	X	-	-
Misc.	X	X	-	X	-	X	-	X	-	X	-	X

Icons by Freepik from www.flaticon.com

Behavioral Profiling

- Higher confidence in labeling
- Solution to the interpretability problem
- Free to customize profiles

Capabilities	Blackmoon	Citadel
SSDP traffic	100%	100%
Port scan	90%	0%
Reuse C&C	70%	0%
Cryptolocking	20%	50%
Persistence	100%	100%
Connection spam	0%	100%
Subnet	0%	80%

* Scale: 0 (min) – 10 (max)

Collective behavioral profile

Wrap up

- Inconsistent and uninterpretable malware family labels
- Yet, used as ground truth
- Inconvenient for researchers
- Cause unreliable accuracy assessment of proposed solutions

- Use Behavioral profiling instead
- Profiles based on automated capability assessment
- Easy to interpret and encourages white box analysis

TU Delft

Questions?

TU Delft