An Empirical Study on the Blocking of HTTP and DNS Requests at Providers Level to Counter In-The-Wild Malware Infections

Marcus Botacin[1], Paulo Lício de Geus[2], André Grégio[1]

[1]Federal University of Paraná (UFPR) – {mfbotacin, gregio}@inf.ufpr.br

[2]University of Campinas (Unicamp) – paulo@lasca.ic.unicamp.br

SBSEG 2020

Agenda

1. Introduction
2. Experiments & Results
3. Concluding Remarks

Agenda

1. Introduction
2. Experiments & Results
3. Concluding Remarks

Malware Blocking Approaches

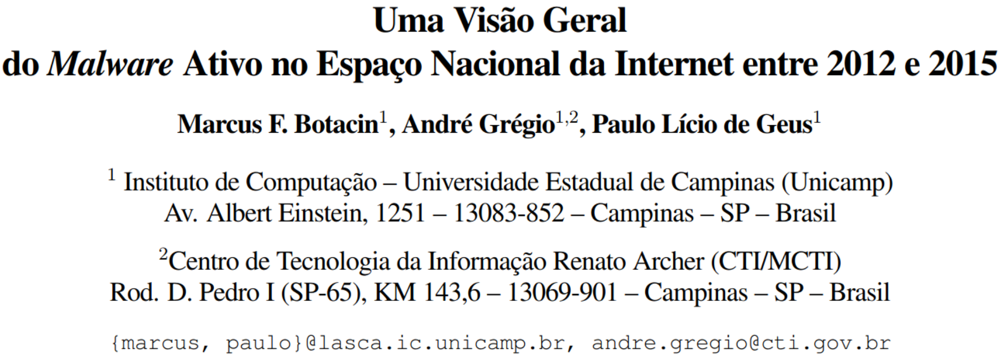
Endpoint Level

- **Pro:** Does not cause significant side-effects.
- **Con:** Needs to be applied to every infected host.

Network Level

- **Pro:** Affects all infected hosts.
- **Con:** False positives at large scale.

Previously...



Uma Visão Geral
do *Malware* Ativo no Espaço Nacional da Internet entre 2012 e 2015

Marcus F. Botacin[1], André Grégio[1,2], Paulo Lício de Geus[1]

[1] Instituto de Computação – Universidade Estadual de Campinas (Unicamp)
Av. Albert Einstein, 1251 – 13083-852 – Campinas – SP – Brasil

[2]Centro de Tecnologia da Informação Renato Archer (CTI/MCTI)
Rod. D. Pedro I (SP-65), KM 143,6 – 13069-901 – Campinas – SP – Brasil

`{marcus, paulo}@lasca.ic.unicamp.br, andre.gregio@cti.gov.br`

Figure: **SBSeg 2015.** Previous Work.

Network Discoveries

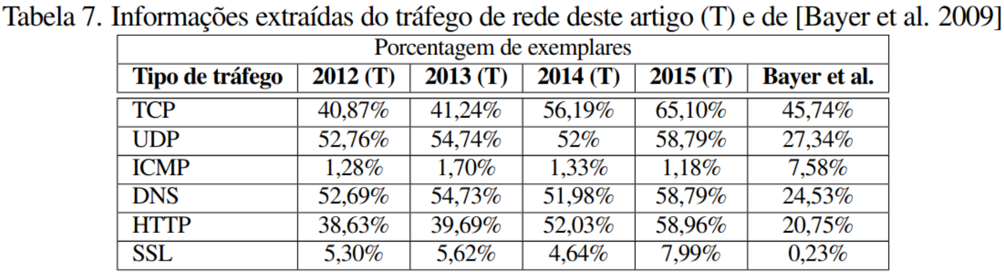


Tabela 7. Informações extraídas do tráfego de rede deste artigo (T) e de [Bayer et al. 2009]

	Porcentagem de exemplares				
Tipo de tráfego	**2012 (T)**	**2013 (T)**	**2014 (T)**	**2015 (T)**	**Bayer et al.**
TCP	40,87%	41,24%	56,19%	65,10%	45,74%
UDP	52,76%	54,74%	52%	58,79%	27,34%
ICMP	1,28%	1,70%	1,33%	1,18%	7,58%
DNS	52,69%	54,73%	51,98%	58,79%	24,53%
HTTP	38,63%	39,69%	52,03%	58,96%	20,75%
SSL	5,30%	5,62%	4,64%	7,99%	0,23%

Figure: **Previous Work.** Most used protocols.

Later…

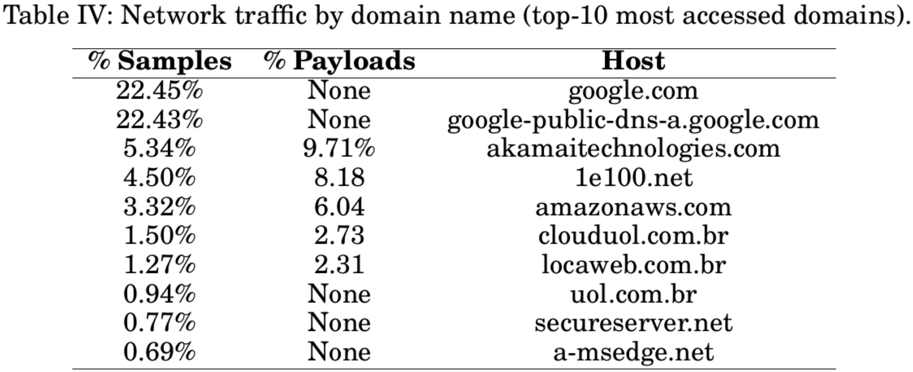


Table IV: Network traffic by domain name (top-10 most accessed domains).

% Samples	% Payloads	Host
22.45%	None	google.com
22.43%	None	google-public-dns-a.google.com
5.34%	9.71%	akamaitechnologies.com
4.50%	8.18	1e100.net
3.32%	6.04	amazonaws.com
1.50%	2.73	clouduol.com.br
1.27%	2.31	locaweb.com.br
0.94%	None	uol.com.br
0.77%	None	secureserver.net
0.69%	None	a-msedge.net

Figure: **Continuous Monitoring.** Most contacted hosts.

Now?

Let’s take a closer look on network.

Agenda

1. Introduction
2. Experiments & Results
3. Concluding Remarks

Experiments

Datasets

- **Brazil:** 20K Windows samples from a CSIRT.
- **World:** 11K Windows samples from MalShare.

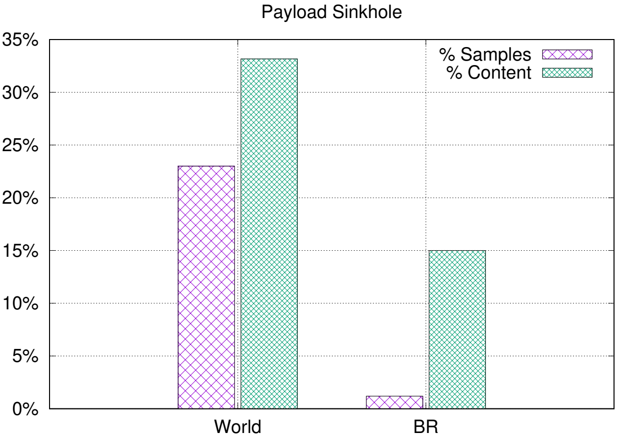
Methodology

- **Analysis:** Daily execution on a sandbox for 30 days.
- **Filtering:** Only HTTP and DNS.

Network Metric 1

Content Sinkhole

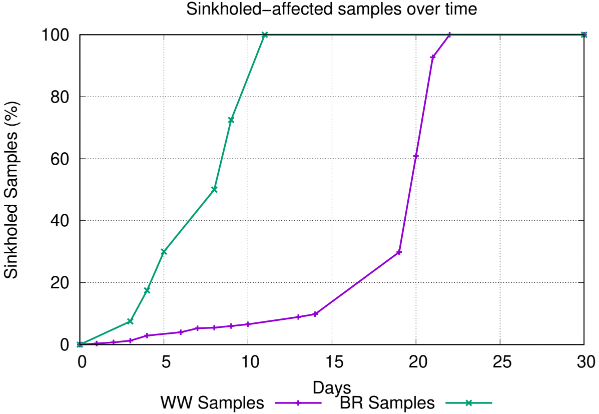
This metric evaluates whether the malicious payloads downloaded by given samples are removed from the hosting servers after some time or keep infecting users. This is particularly important in cases where AV solutions fail to detect a given threat and payload removal is the only defense available to protect users.



Network Metric 2

Content Survival Time

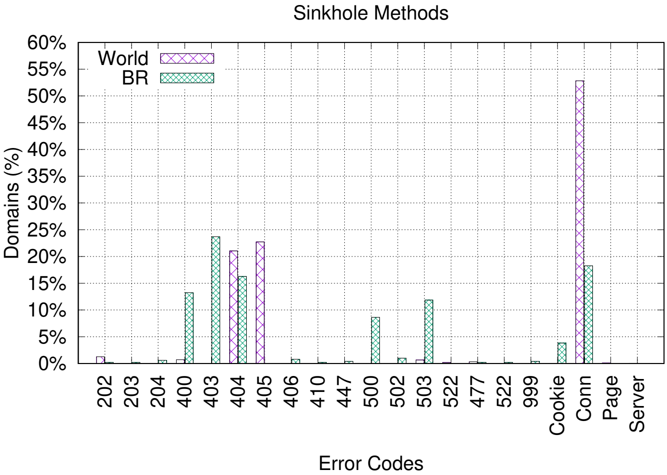
This metric evaluates how long the domains contacted by the malware samples remain active before being taken down. This metric helps evaluating whether removal procedures occur in reasonable time. Early removals are desired because AV solutions might take some time to develop signatures to new threats, thus network hosting providers might help reducing the attack opportunity window.



Network Metric 3

Sinkhole Method

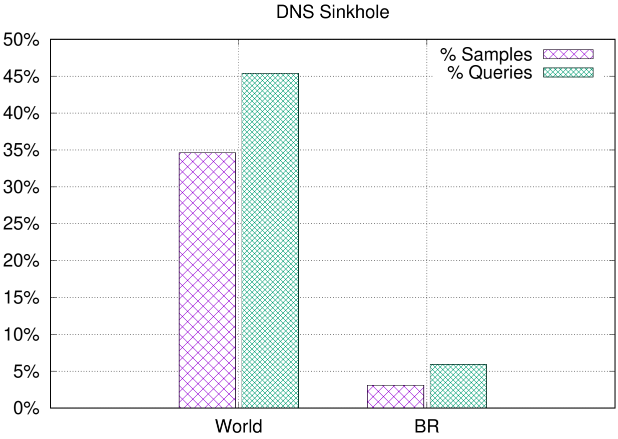
This metric evaluates how content hosts and/or providers act to remove malicious payloads. The removal method indicates which security scope is affected/involved.



Network Metric 4

DNS Takeover

This metric evaluates how many DNS records stop being resolved by the DNS requests performed by the malware samples within the evaluated period. This metric evaluates whether network administrators are blocking identified malicious traffic or not.



Network Metric 5

DNS/IP Rotation

This metric evaluates how many distinct IP addresses are resolved to the same DNS queries. This metric evaluates whether attackers rotate domains to make removal harder.

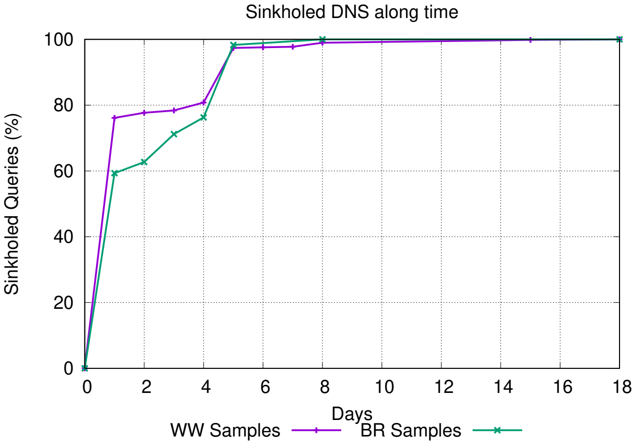
Characterization

1. **Content Deliver Networks (CDNs)**: Query to: `load.s3.amazonaws.com` resolves to `54.231.AA.BBB` and `52.216.CC.DD`.
2. **Dynamic IP services**: Query to: `iutf.dyndns.org` resolves to `216.146.EE.FF` and `91.198.GG.HH`.
3. **Registered Domains**: Query to: `xlscgpqghsxopwceausfyif.ru` resolves to `198.105.II.JJ` and `104.239.KKK.L`.

Network Metric 6

DNS Takeover Time

This metric evaluates for how long a given DNS query keeps being resolved until blocking. It impacts the attack opportunity of early-launched threats.



Agenda

1 Introduction

2 Experiments & Results

3 Concluding Remarks

Discussion

Many payloads stored in the Cloud

- How to inspect privacy servers with privacy guarantees?

DNS is the most effective way to block malware payloads

- How to automatically block suspicious queries?

Malicious domains must be reported

- Few providers have an easy mechanism to report abuse.

The context matters

- The Brazilian scenario is different and our security solutions should be too.

Questions & Comments.

Contact

- **mfbotacin@inf.ufpr.br**
- **twitter.com/MarcusBotacin**
- **secret.inf.ufpr.br**