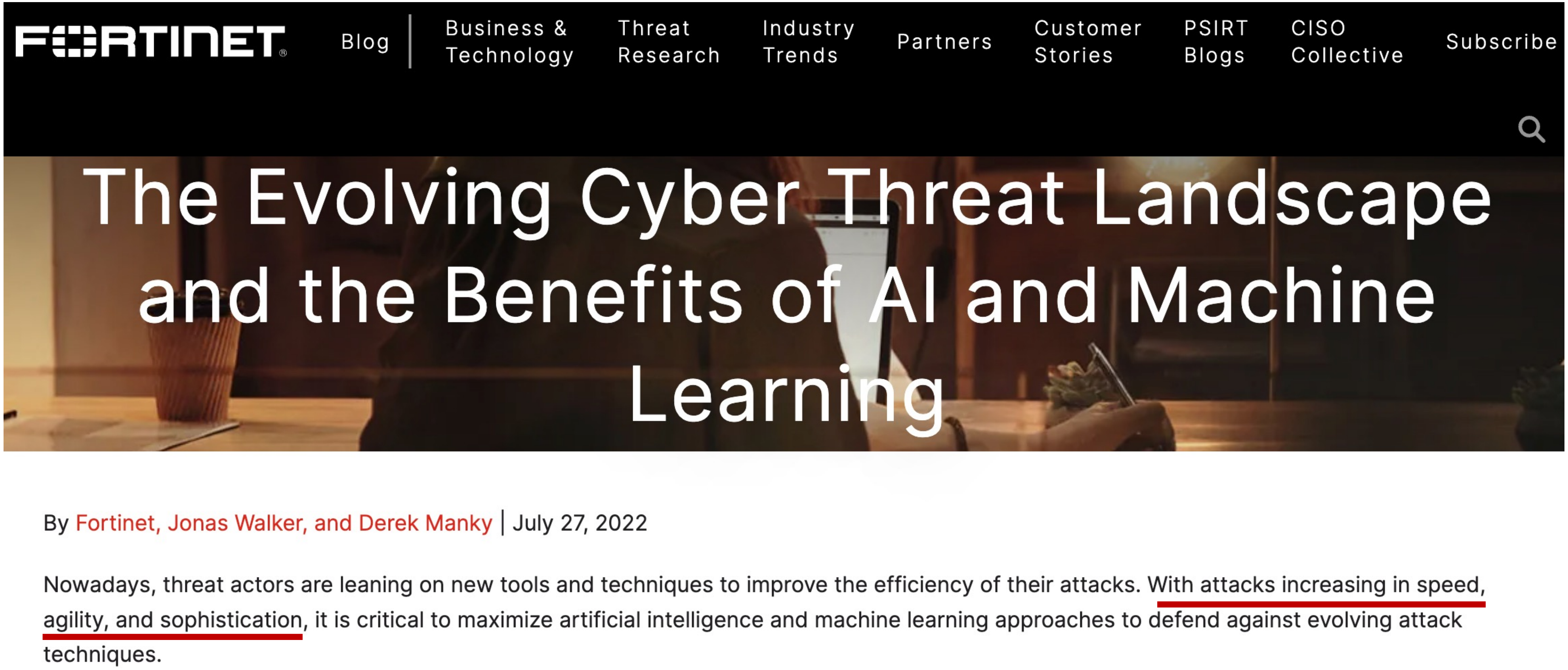
Annual Computer Security Applications Conference (ACSAC 2022)

Threats in Crowdsourcing Threat Intelligence for Practical Threat Triaging

Afsah Anwar, Yi Hui Chen, Roy Hodgman, Tom Sellers,
Engin Kirda, Alina Oprea

Evolving Threat Landscape

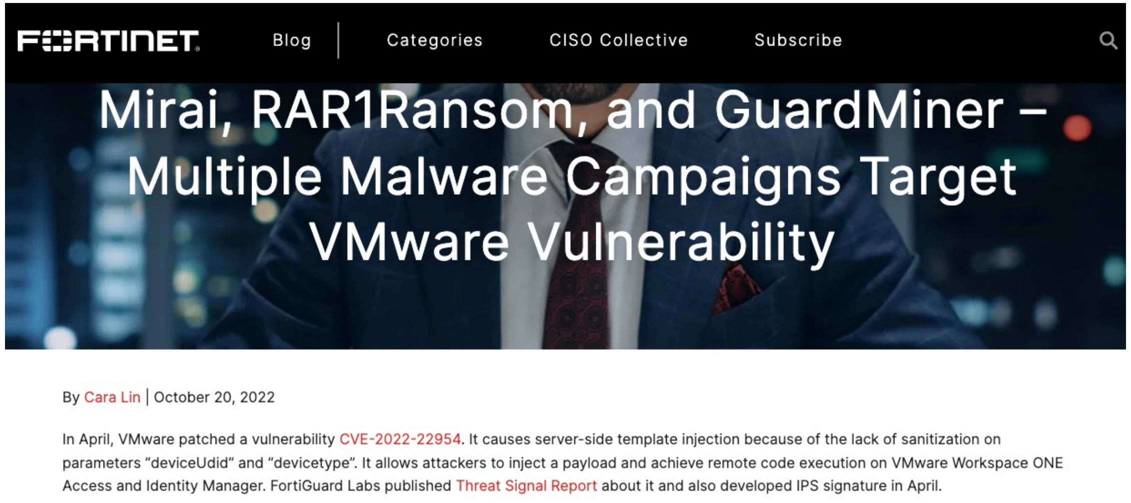


The Evolving Cyber Threat Landscape and the Benefits of AI and Machine Learning

By Fortinet, Jonas Walker, and Derek Manky | July 27, 2022

Nowadays, threat actors are leaning on new tools and techniques to improve the efficiency of their attacks. With attacks increasing in speed, agility, and sophistication, it is critical to maximize artificial intelligence and machine learning approaches to defend against evolving attack techniques.

Motivation



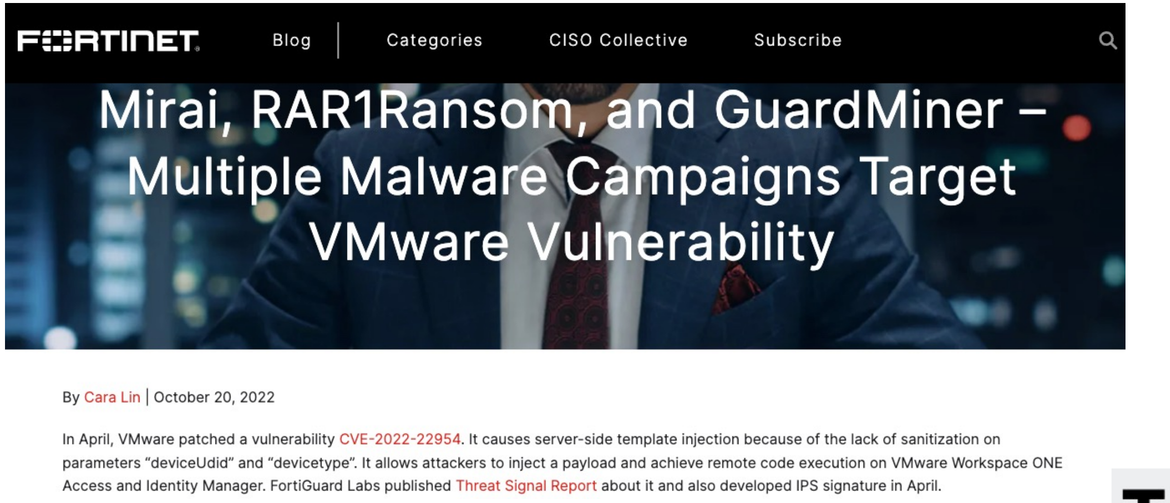
Mirai, RAR1Ransom, and GuardMiner – Multiple Malware Campaigns Target VMware Vulnerability

By Cara Lin | October 20, 2022

In April, VMware patched a vulnerability CVE-2022-22954. It causes server-side template injection because of the lack of sanitization on parameters “deviceUdid” and “devicetype”. It allows attackers to inject a payload and achieve remote code execution on VMware Workspace ONE Access and Identity Manager. FortiGuard Labs published Threat Signal Report about it and also developed IPS signature in April.

Vulnerabilities may be exploited as part of malware campaigns

Motivation

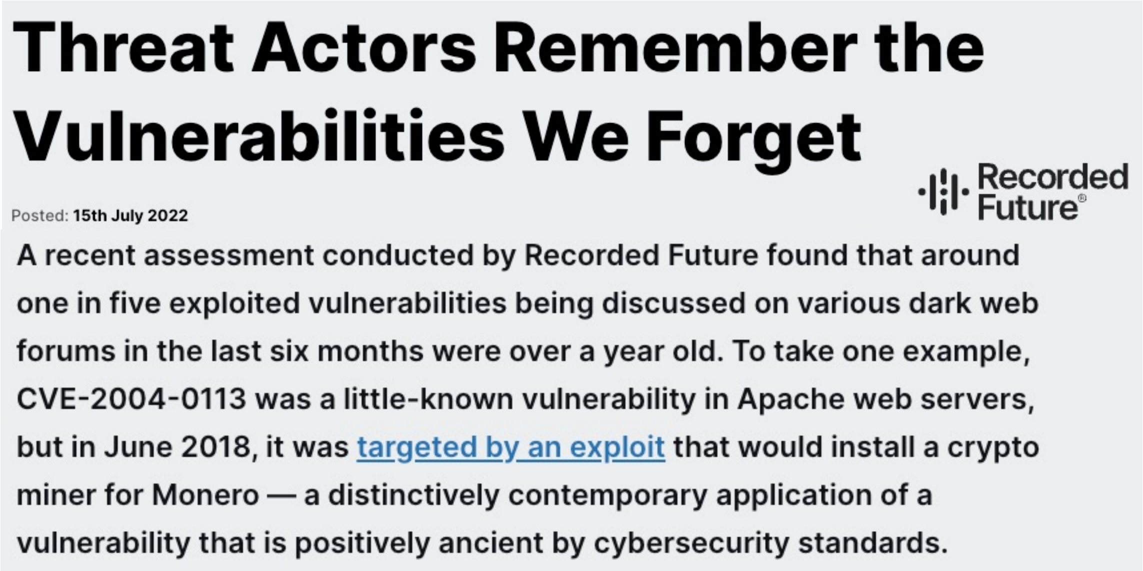


Mirai, RAR1Ransom, and GuardMiner – Multiple Malware Campaigns Target VMware Vulnerability

By Cara Lin | October 20, 2022

In April, VMware patched a vulnerability CVE-2022-22954. It causes server-side template injection because of the lack of sanitization on parameters “deviceUdid” and “devicetype”. It allows attackers to inject a payload and achieve remote code execution on VMware Workspace ONE Access and Identity Manager. FortiGuard Labs published Threat Signal Report about it and also developed IPS signature in April.

Vulnerabilities may be exploited as part of malware campaigns



Threat Actors Remember the Vulnerabilities We Forget

Posted: 15th July 2022

A recent assessment conducted by Recorded Future found that around one in five exploited vulnerabilities being discussed on various dark web forums in the last six months were over a year old. To take one example, CVE-2004-0113 was a little-known vulnerability in Apache web servers, but in June 2018, it was targeted by an exploit that would install a crypto miner for Monero — a distinctively contemporary application of a vulnerability that is positively ancient by cybersecurity standards.

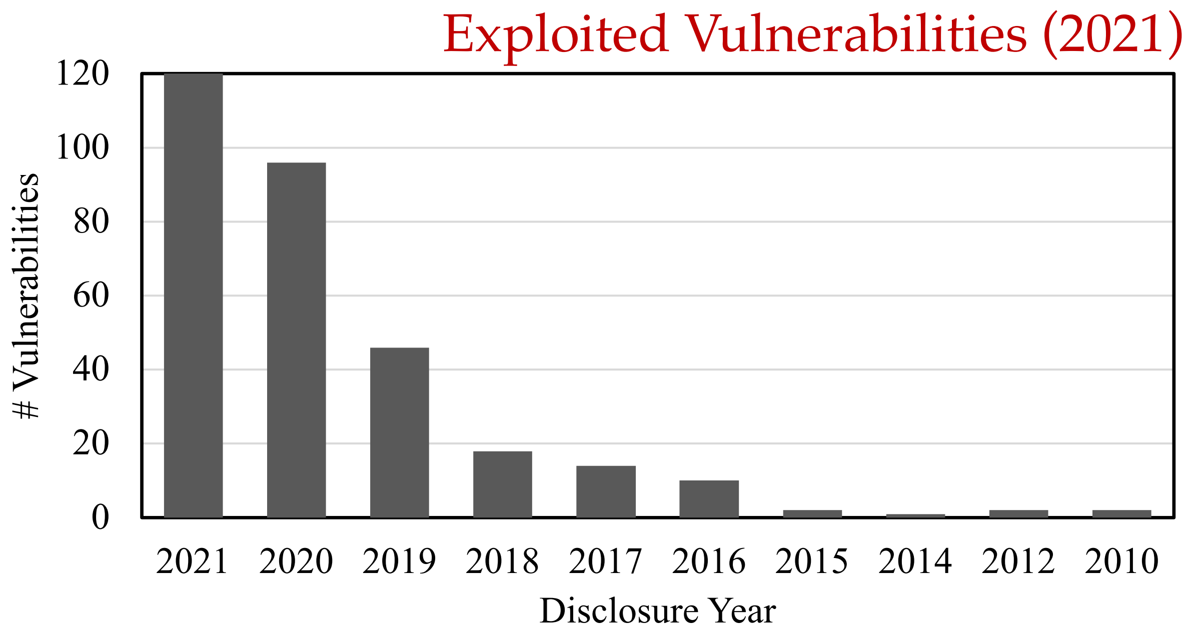
Older threats reappear as new attack vectors

Motivation

- Only a handful of vulnerabilities are exploited

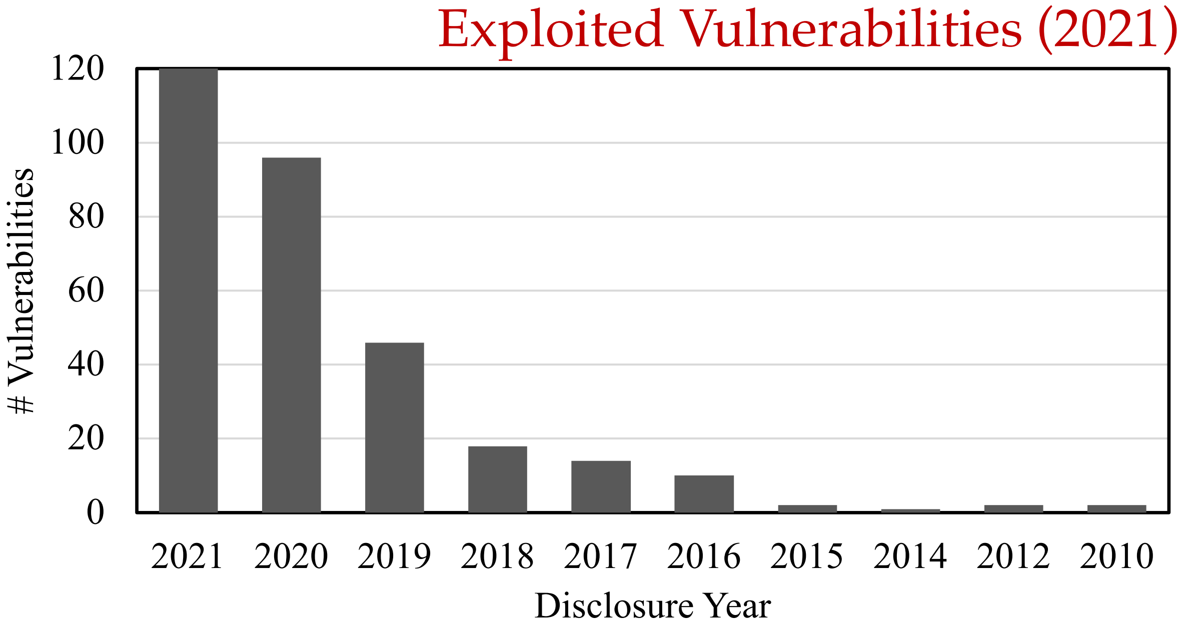
Motivation

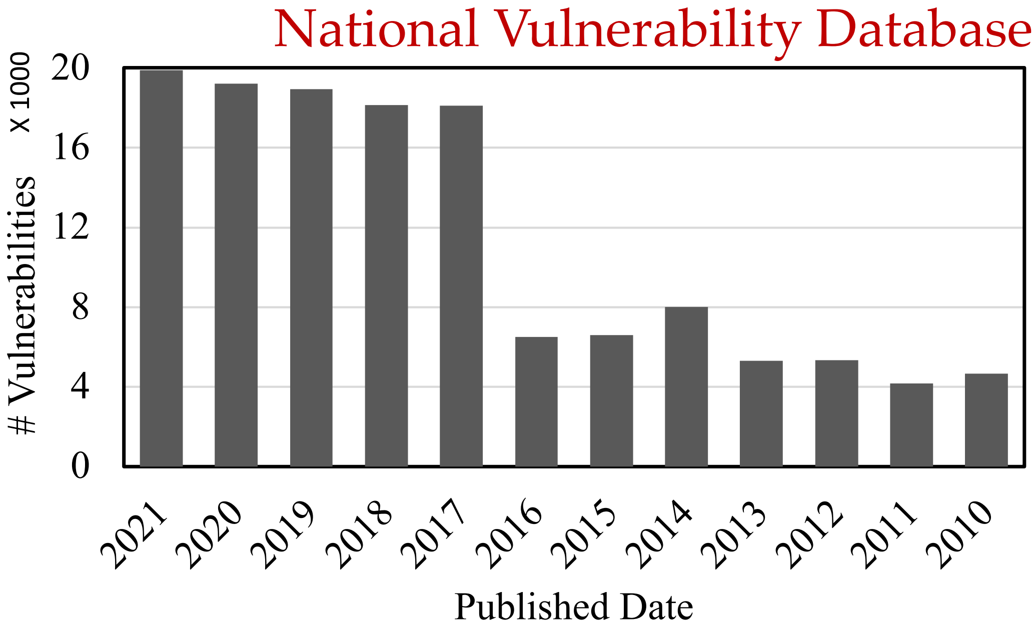
- Only a handful of vulnerabilities are exploited



Motivation

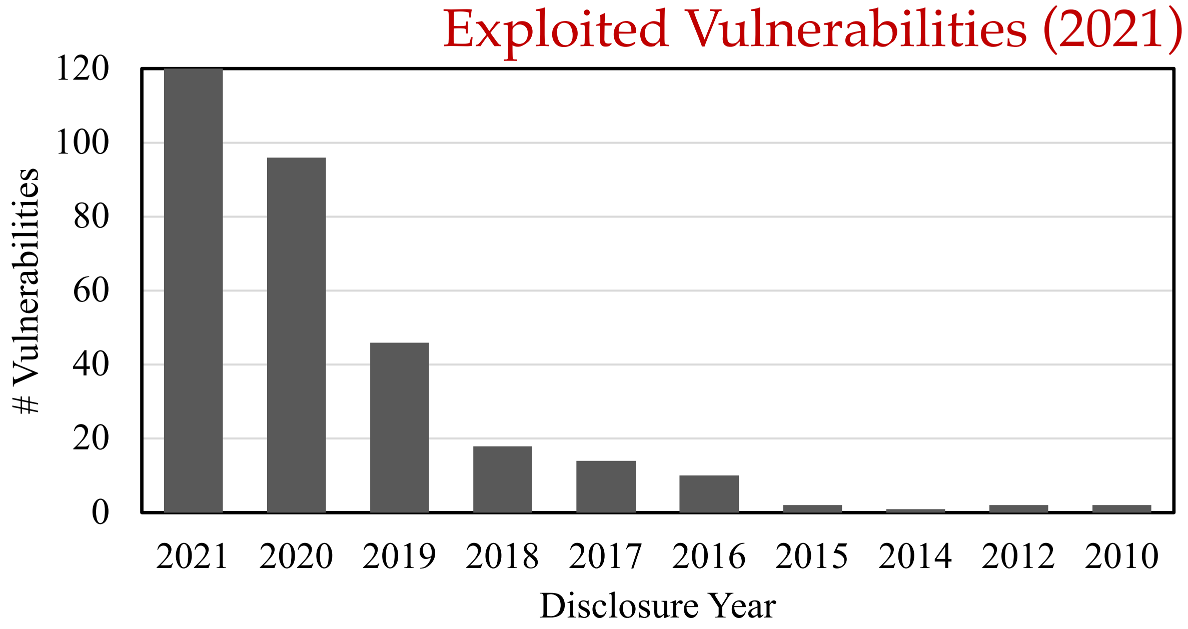
- Only a handful of vulnerabilities are exploited

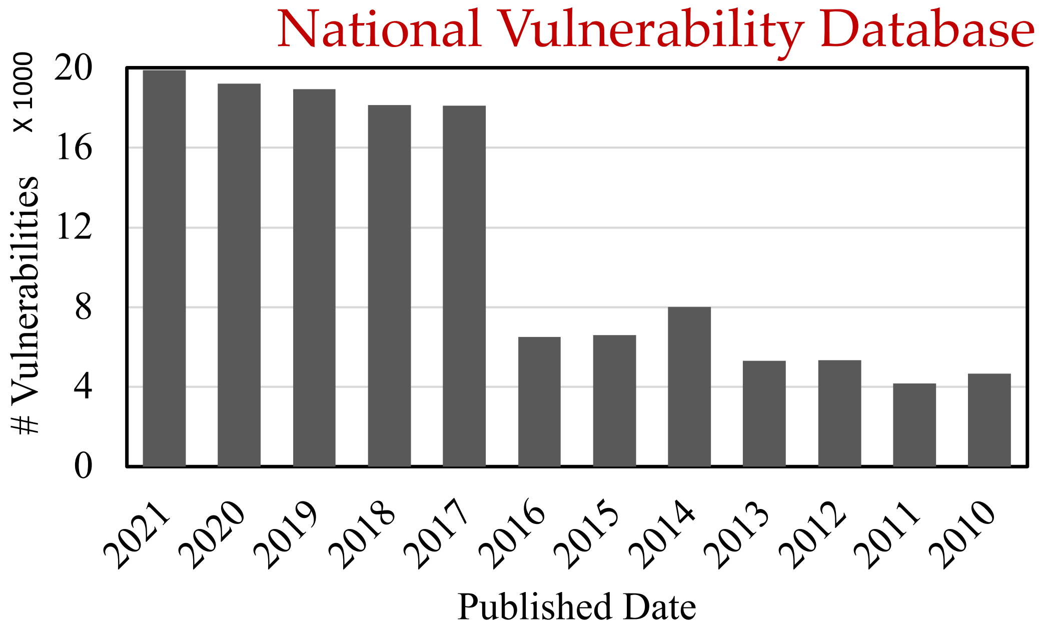




Motivation

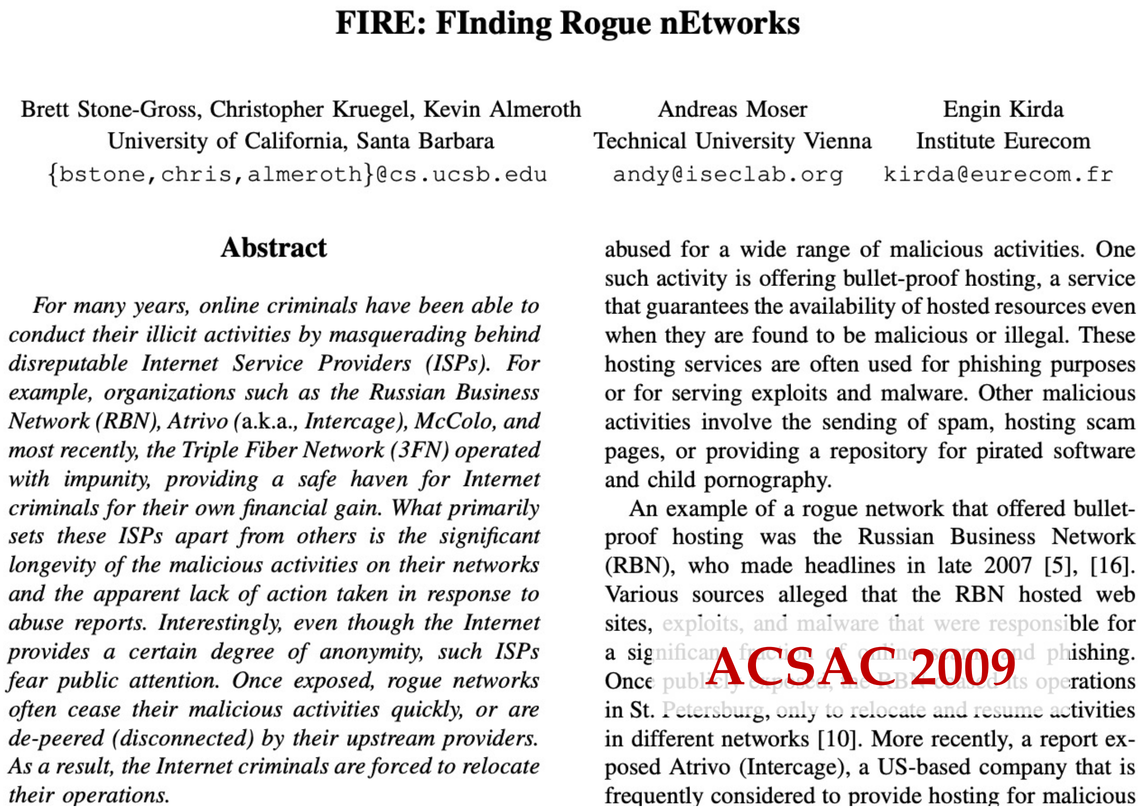
- Only a handful of vulnerabilities are exploited





Of all the vulnerabilities disclosed in 2021, only 0.9% of them have been exploited until November 2022

Honeypots to Monitor Active Threats



FIRE: FInding Rogue nEtworks

Brett Stone-Gross, Christopher Kruegel, Kevin Almeroth
University of California, Santa Barbara
{bstone,chris,almeroth}@cs.ucsb.edu

Andreas Moser
Technical University Vienna
andy@iseclab.org

Engin Kirda
Institute Eurecom
kirda@eurecom.fr

Abstract

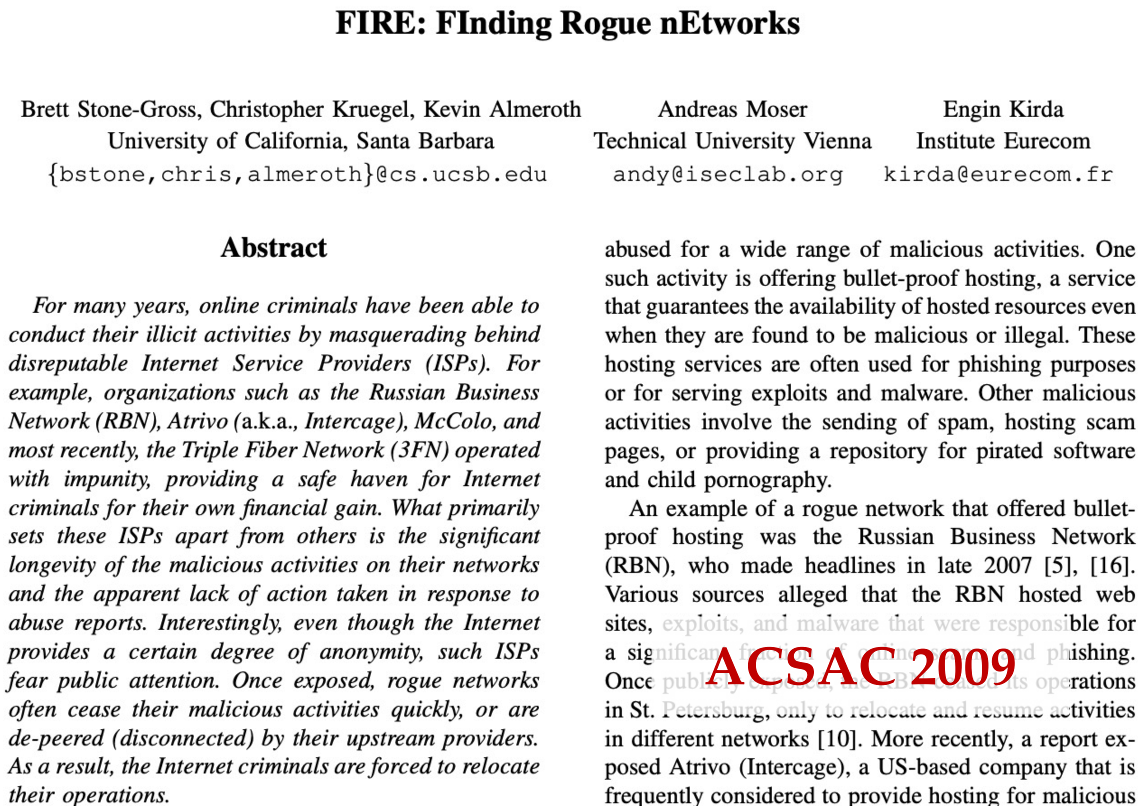
*For many years, online criminals have been able to conduct their illicit activities by masquerading behind disreputable Internet Service Providers (ISPs). For example, organizations such as the Russian Business Network (RBN), Atrivo (*a.k.a.*, Intercage), McColo, and most recently, the Triple Fiber Network (3FN) operated with impunity, providing a safe haven for Internet criminals for their own financial gain. What primarily sets these ISPs apart from others is the significant longevity of the malicious activities on their networks and the apparent lack of action taken in response to abuse reports. Interestingly, even though the Internet provides a certain degree of anonymity, such ISPs fear public attention. Once exposed, rogue networks often cease their malicious activities quickly, or are de-peered (disconnected) by their upstream providers. As a result, the Internet criminals are forced to relocate their operations.*

abused for a wide range of malicious activities. One such activity is offering bullet-proof hosting, a service that guarantees the availability of hosted resources even when they are found to be malicious or illegal. These hosting services are often used for phishing purposes or for serving exploits and malware. Other malicious activities involve the sending of spam, hosting scam pages, or providing a repository for pirated software and child pornography.

An example of a rogue network that offered bullet-proof hosting was the Russian Business Network (RBN), who made headlines in late 2007 [5], [16]. Various sources alleged that the RBN hosted web sites, exploits, and malware that were responsible for a significant fraction of online scams and phishing. Once publicly exposed, the RBN ceased its operations in St. Petersburg, only to relocate and resume activities in different networks [10]. More recently, a report exposed Atrivo (Intercage), a US-based company that is frequently considered to provide hosting for malicious

ACSAC 2009

Honeypots to Monitor Active Threats



FIRE: FInding Rogue nEtworks

Brett Stone-Gross, Christopher Kruegel, Kevin Almeroth
University of California, Santa Barbara
{bstone,chris,almeroth}@cs.ucsb.edu

Andreas Moser
Technical University Vienna
andy@iseclab.org

Engin Kirda
Institute Eurecom
kirda@eurecom.fr

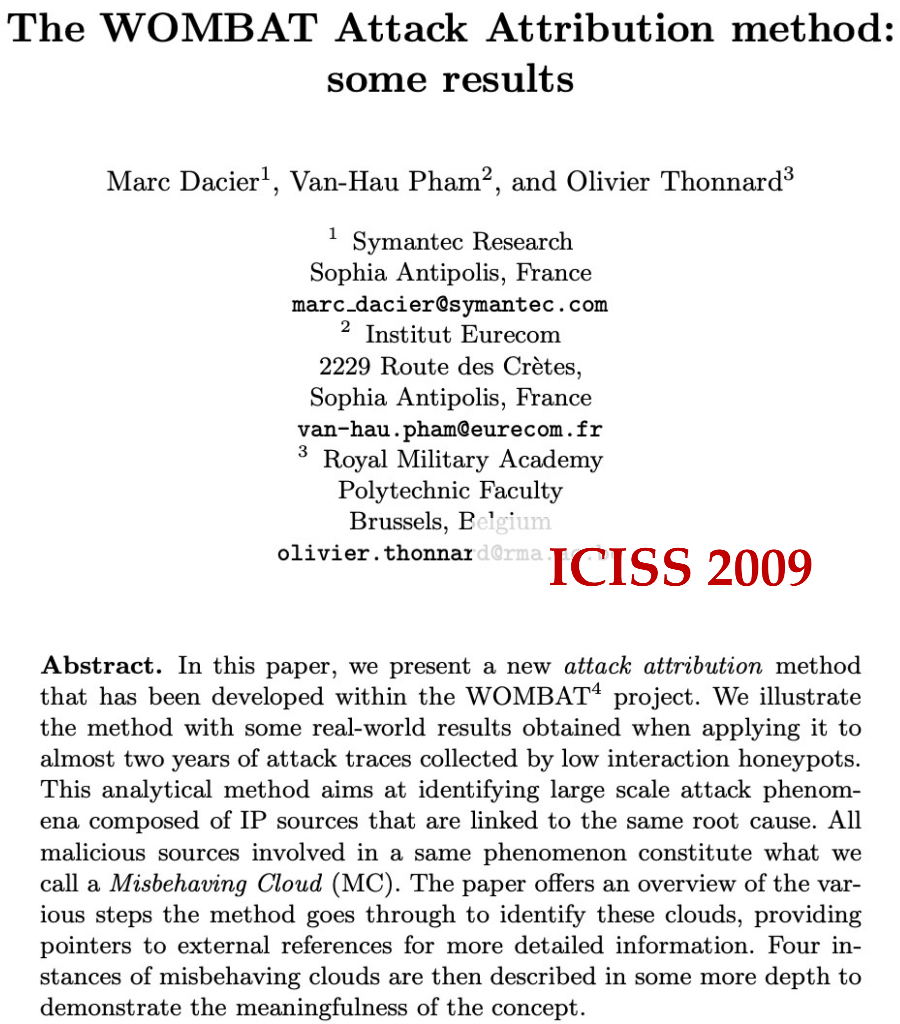
Abstract

For many years, online criminals have been able to conduct their illicit activities by masquerading behind disreputable Internet Service Providers (ISPs). For example, organizations such as the Russian Business Network (RBN), Atrivo (a.k.a., *Intercage), McColo, and most recently, the Triple Fiber Network (3FN) operated with impunity, providing a safe haven for Internet criminals for their own financial gain. What primarily sets these ISPs apart from others is the significant longevity of the malicious activities on their networks and the apparent lack of action taken in response to abuse reports. Interestingly, even though the Internet provides a certain degree of anonymity, such ISPs fear public attention. Once exposed, rogue networks often cease their malicious activities quickly, or are de-peered (disconnected) by their upstream providers. As a result, the Internet criminals are forced to relocate their operations.*

abused for a wide range of malicious activities. One such activity is offering bullet-proof hosting, a service that guarantees the availability of hosted resources even when they are found to be malicious or illegal. These hosting services are often used for phishing purposes or for serving exploits and malware. Other malicious activities involve the sending of spam, hosting scam pages, or providing a repository for pirated software and child pornography.

An example of a rogue network that offered bullet-proof hosting was the Russian Business Network (RBN), who made headlines in late 2007 [5], [16]. Various sources alleged that the RBN hosted web sites, exploits, and malware that were responsible for a significant fraction of online scams and phishing. Once publicly exposed, the RBN ceased its operations in St. Petersburg, only to relocate and resume activities in different networks [10]. More recently, a report exposed Atrivo (Intercage), a US-based company that is frequently considered to provide hosting for malicious

ACSAC 2009



The WOMBAT Attack Attribution method: some results

Marc Dacier[1], Van-Hau Pham[2], and Olivier Thonnard[3]

[1] Symantec Research
Sophia Antipolis, France
marc_dacier@symantec.com
[2] Institut Eurecom
2229 Route des Crètes,
Sophia Antipolis, France
van-hau.pham@eurecom.fr
[3] Royal Military Academy
Polytechnic Faculty
Brussels, Belgium
olivier.thonnard@rma.ac.be

ICISS 2009

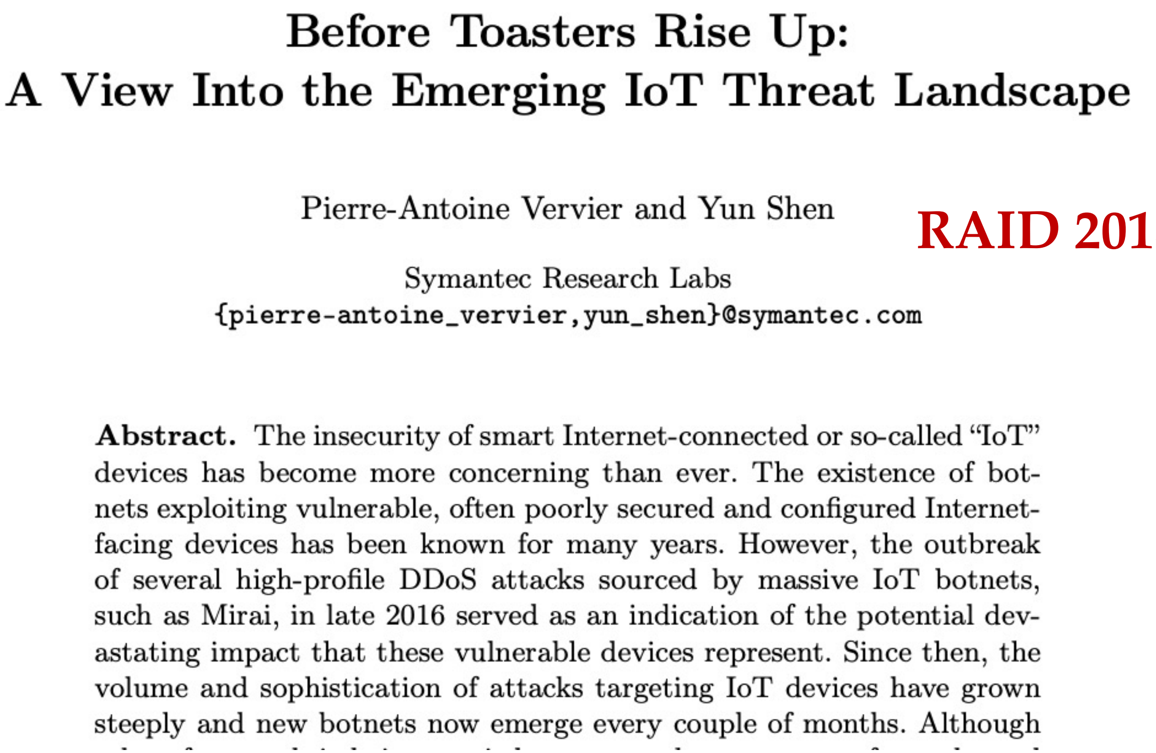
Abstract. In this paper, we present a new *attack attribution* method that has been developed within the WOMBAT[4] project. We illustrate the method with some real-world results obtained when applying it to almost two years of attack traces collected by low interaction honeypots. This analytical method aims at identifying large scale attack phenomena composed of IP sources that are linked to the same root cause. All malicious sources involved in a same phenomenon constitute what we call a *Misbehaving Cloud* (MC). The paper offers an overview of the various steps the method goes through to identify these clouds, providing pointers to external references for more detailed information. Four instances of misbehaving clouds are then described in some more depth to demonstrate the meaningfulness of the concept.

Narrowed Attention

- Recent works have leveraged honeypots with narrowed focus

Narrowed Attention

- Recent works have leveraged honeypots with narrowed focus



Before Toasters Rise Up: A View Into the Emerging IoT Threat Landscape

Pierre-Antoine Vervier and Yun Shen

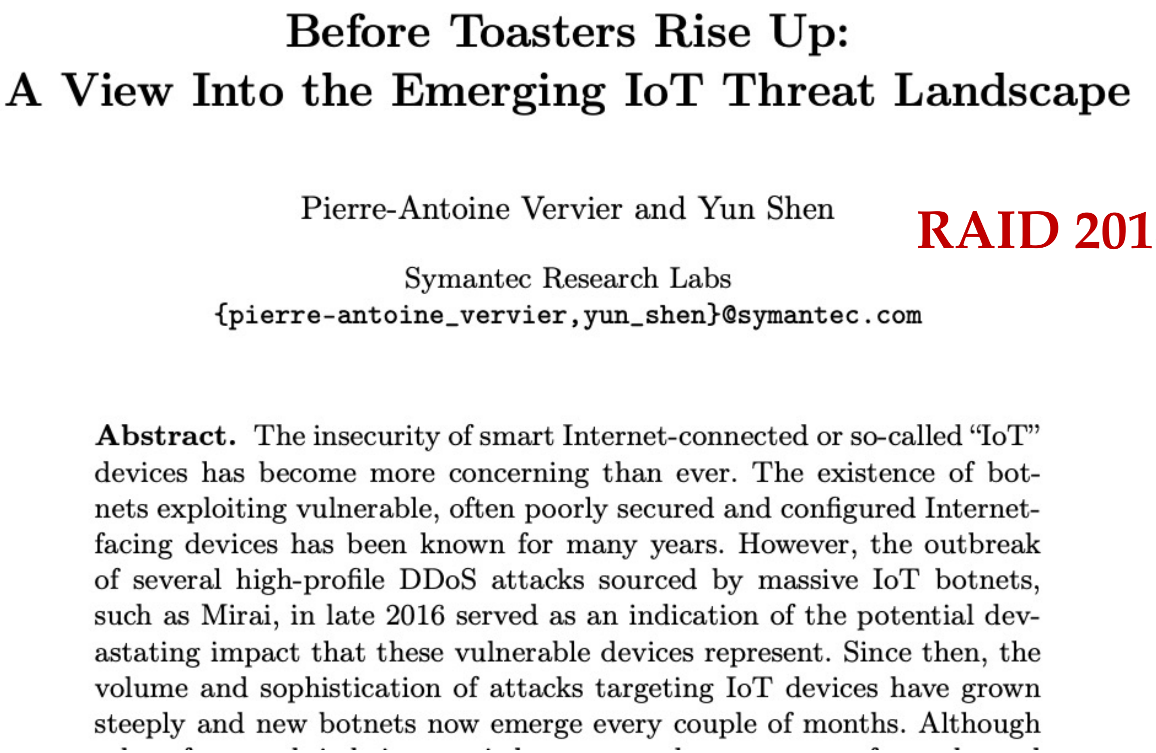
Symantec Research Labs
{pierre-antoine_vervier,yun_shen}@symantec.com

RAID 2018

Abstract. The insecurity of smart Internet-connected or so-called "IoT" devices has become more concerning than ever. The existence of botnets exploiting vulnerable, often poorly secured and configured Internet-facing devices has been known for many years. However, the outbreak of several high-profile DDoS attacks sourced by massive IoT botnets, such as Mirai, in late 2016 served as an indication of the potential devastating impact that these vulnerable devices represent. Since then, the volume and sophistication of attacks targeting IoT devices have grown steeply and new botnets now emerge every couple of months. Although

Narrowed Attention

- Recent works have leveraged honeypots with narrowed focus



**Before Toasters Rise Up:
A View Into the Emerging IoT Threat Landscape**

Pierre-Antoine Vervier and Yun Shen

Symantec Research Labs
{pierre-antoine_vervier,yun_shen}@symantec.com

RAID 2018

Abstract. The insecurity of smart Internet-connected or so-called "IoT" devices has become more concerning than ever. The existence of botnets exploiting vulnerable, often poorly secured and configured Internet-facing devices has been known for many years. However, the outbreak of several high-profile DDoS attacks sourced by massive IoT botnets, such as Mirai, in late 2016 served as an indication of the potential devastating impact that these vulnerable devices represent. Since then, the volume and sophistication of attacks targeting IoT devices have grown steeply and new botnets now emerge every couple of months. Although

It is essential to look at the overall threat landscape

A Recent Year On the Internet

- The Internet ecosystem has changed in the last decade
  - ❖Increased Internet penetration
  - ❖Internet itself has evolved as well

A Recent Year On the Internet

- The Internet ecosystem has changed in the last decade
  - ❖Increased Internet penetration
  - ❖Internet itself has evolved as well

- This increase in volume of Internet connected population poses a more broadened threat

A Recent Year On the Internet

- The Internet ecosystem has changed in the last decade
  - ❖Increased Internet penetration
  - ❖Internet itself has evolved as well

- This increase in volume of Internet connected population poses a more broadened threat

- We again revisit honeypots to understand the threat landscape posed to Internet-connected systems

The Honeypot

RAPID7

[1] https://www.rapid7.com/research/project-heisenberg/

The Honeypot

- Deployed by Rapid7 as part of Project Heisenberg[1]
    - ❖Globally distributed network of honeypots
    - ❖Timeline – July 2020 to June 2021

[1] https://www.rapid7.com/research/project-heisenberg/

The Honeypot

- Deployed by Rapid7 as part of Project Heisenberg[1]
  - ❖Globally distributed network of honeypots
  - ❖Timeline – July 2020 to June 2021

RAPID7

- We analyze the exploitation events observed by the honeypots, as identified by Suricata
  - ❖7 billion connections raise 806 million alerts

[1] https://www.rapid7.com/research/project-heisenberg/

Suricata Alerts

- Suricata rules assign a short description to the alerts

Suricata Alerts

- Suricata rules assign a short description to the alerts

```
alert tcp any any -> any any (msg: "ATTACK CoronaBlue/SMBGhost
DOS/RCE Attempt (CVE-2020-0796)"; flow: established; content:
"|FC|SMB"; depth: 8; byte_test: 4, >, 0x800134, 8, relative,
little; reference: url,www.mcafee.com/blogs/other-blogs/mcafee-
labs/smbghost-analysis-of-cve-2020-0796; reference: cve, 2020-
0796; reference: url, github.com/ptresearch/AttackDetection;
classtype: attempted-admin; sid: 10005777; rev: 2;)
```

Suricata Alerts

- Suricata rules assign a short description to the alerts

```
alert tcp any any -> any any (msg: "ATTACK CoronaBlue/SMBGhost DOS/RCE Attempt (CVE-2020-0796)"; flow: established; content: "|FC|SMB"; depth: 8; byte_test: 4, >, 0x800134, 8, relative, little; reference: url,www.mcafee.com/blogs/other-blogs/mcafee-labs/smbghost-analysis-of-cve-2020-0796; reference: cve, 2020-0796; reference: url, github.com/ptresearch/AttackDetection; classtype: attempted-admin; sid: 10005777; rev: 2;)
```

Suricata Alerts

- Suricata rules assign a short description to the alerts

```
alert tcp any any -> any any (msg: "ATTACK CoronaBlue/SMBGhost
DOS/RCE Attempt (CVE-2020-0796)"; flow: established; content:
"|FC|SMB"; depth: 8; byte_test: 4, >, 0x800134, 8, relative,
little; reference: url,www.mcafee.com/blogs/other-blogs/mcafee-
labs/smbghost-analysis-of-cve-2020-0796; reference: cve, 2020-
0796; reference: url, github.com/ptresearch/AttackDetection;
classtype: attempted-admin; sid: 10005777; rev: 2;)
```

Suricata Alerts

- Suricata rules assign a short description to the alerts

```
alert tcp any any -> any any (msg: "ATTACK CoronaBlue/SMBGhost
DOS/RCE Attempt (CVE-2020-0796)"; flow: established; content:
"|FC|SMB"; depth: 8; byte_test: 4, >, 0x800134, 8, relative,
little; reference: url,www.mcafee.com/blogs/other-blogs/mcafee-
labs/smbghost-analysis-of-cve-2020-0796; reference: cve, 2020-
0796; reference: url, github.com/ptresearch/AttackDetection;
classtype: attempted-admin; sid: 10005777; rev: 2;)
```

Doesn’t say much on association with malicious campaigns or threat characteristics!

OSCTI for Alert Summarization

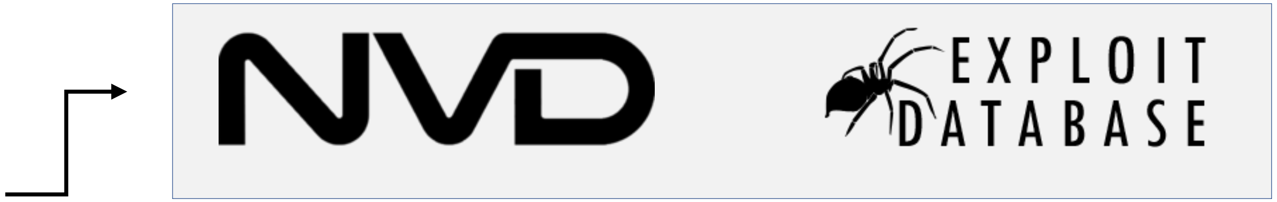
OSCTI for Alert Summarization

- Signature
- Category
- Reference

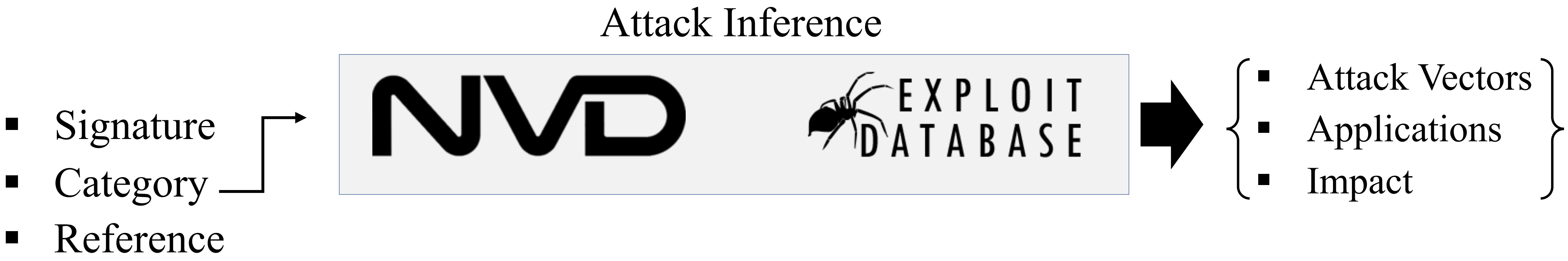
OSCTI for Alert Summarization

Attack Inference

- Signature
- Category
- Reference



OSCTI for Alert Summarization

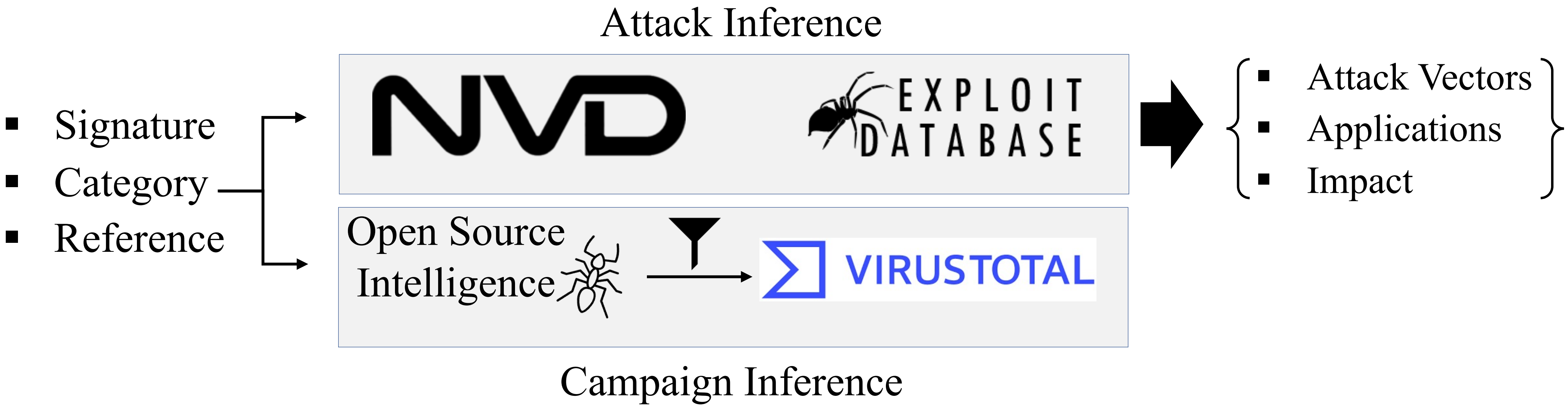


Attack Inference

- Signature
- Category
- Reference

- Attack Vectors
- Applications
- Impact

OSCTI for Alert Summarization



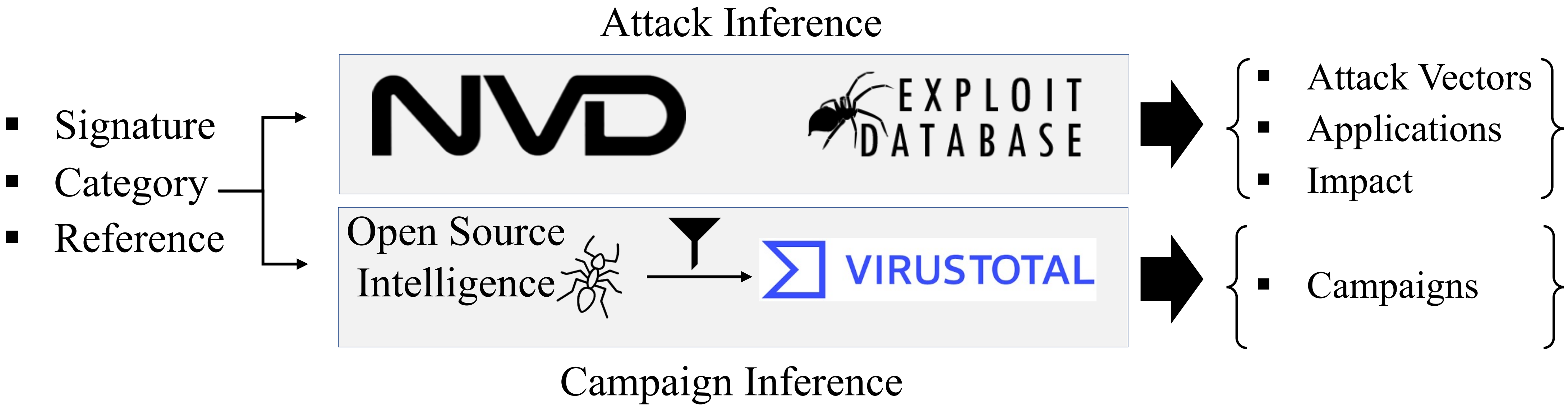
Attack Inference

- Signature
- Category
- Reference

- Attack Vectors
- Applications
- Impact

Campaign Inference

OSCTI for Alert Summarization



Attack Inference

- Signature
- Category
- Reference

- Attack Vectors
- Applications
- Impact

- Campaigns

Campaign Inference

Behavior Persistence

- We find that well-known malware behavior persist over time

Behavior Persistence

- We find that well-known malware behavior persist over time
  - ❖ Prevalence of known malware behavior after more than a decade
  - ❖ Implying, existing defenses such as blacklisting and threat intelligence sharing are insufficient at eradicating known threats

Persistence of Rogue Networks

AS (Alerts)		
AS16276 (3.9%)	AS174 (0.09%)	AS109290.0002%
AS4134 (0.5%)	AS26496 (0.09%)	AS48031 (0.0001%)
AS4837 (0.3%)	AS28753 (0.01%)	AS3595 (0.00003%)
AS3265 (0.2%)	AS35908 (0.003%)	AS44050 (0.000004%)
AS4812 (0.1%)	AS27715 (0.002%)	AS41665 (0.000001%)
AS36351 (0.1%)	AS41075 (0.002%)	

Persistence of Older Threats

- ~ 40.6M alerts due to vulnerabilities disclosed > 10 yrs. ago

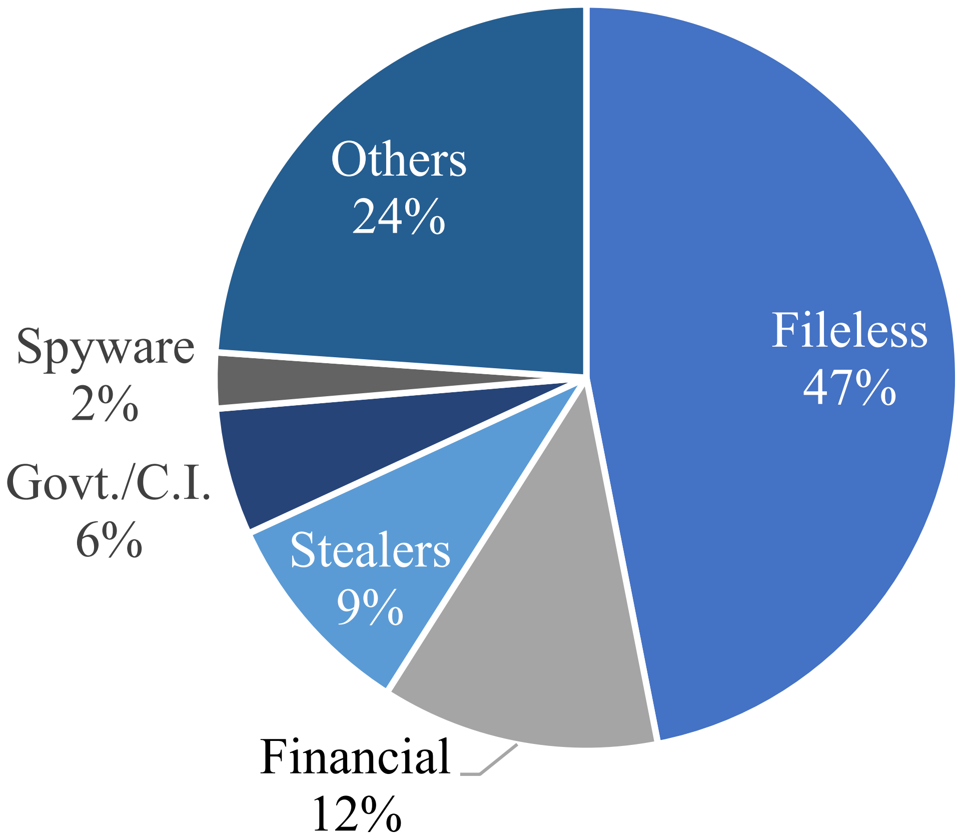
Vulnerability	Weakness	Product	Severity	Malware Campaign	Alerts
CVE-1999-0517	Unauthorized Access	SNMP	High	Gafgyt, RATs, Cobalt Strike	43.4K
CVE-2002-0012/13	Privilege Escalation	SNMP	High		
CVE-2001-0540	Memory Exhaustion	RDP - Windows NT	Medium	Fileless, Cobalt Strike, Zeus	2K
CVE-2003-0818	Remote Command Execution	Windows NT 4.0, 2000, and XP	High	Emotet, Qakbot, Trickbot	83
CVE-2002-0953	Code Injection	PHP - PHP Addr. before 0.2f	High	RATs	43

Campaign Trends

- We identified 118 campaigns in total
  - ❖Mapped them to six attributes

Campaign Trends

- We identified 118 campaigns in total
  - ❖Mapped them to six attributes



Collaborative Exploitation

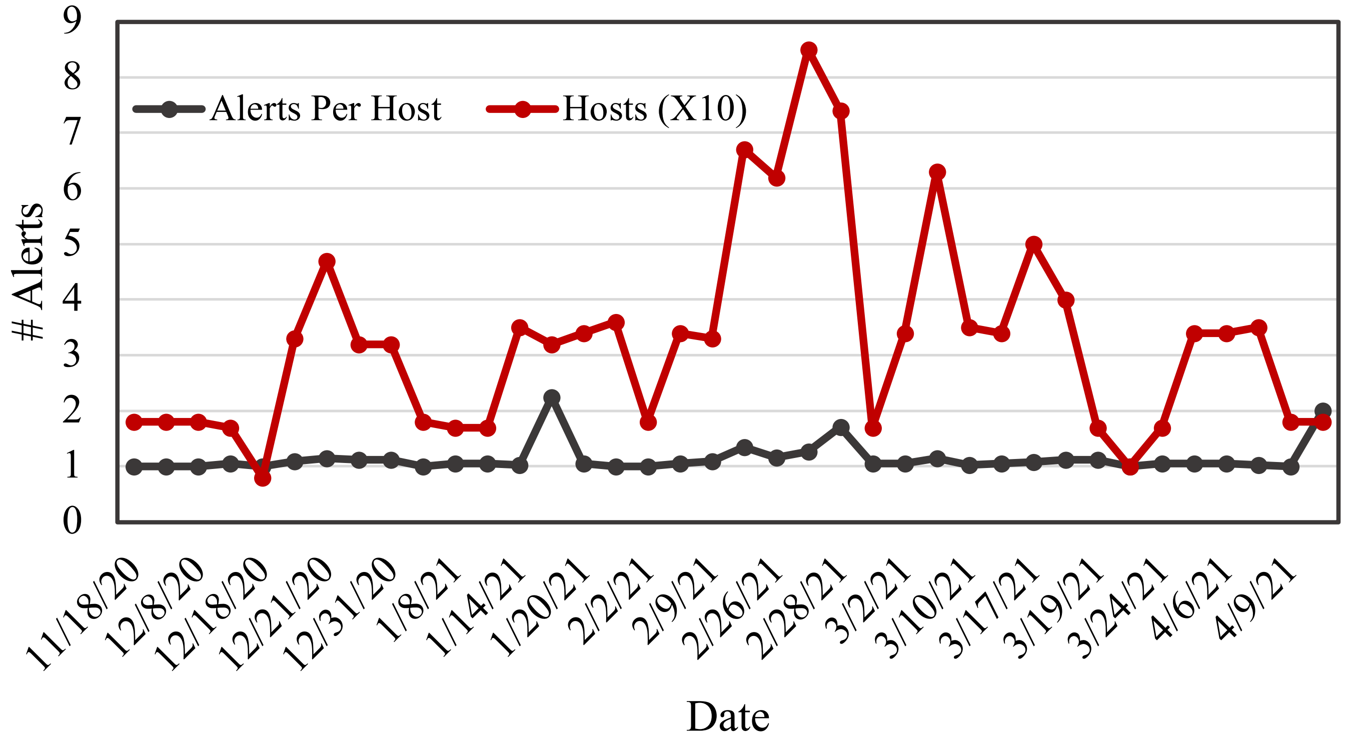
- Example: The SMBGhost vulnerability

Collaborative Exploitation

- Example: The SMBGhost vulnerability
  - ❖53% of alerts arise from subnets that use multiple hosts
  - ❖6 subnets use 100 or more hosts each

Collaborative Exploitation

- Example: The SMBGhost vulnerability
  - ❖53% of alerts arise from subnets that use multiple hosts
  - ❖6 subnets use 100 or more hosts each



- Uses 254 of 256 hosts
- Daily Average: 1 alert/day

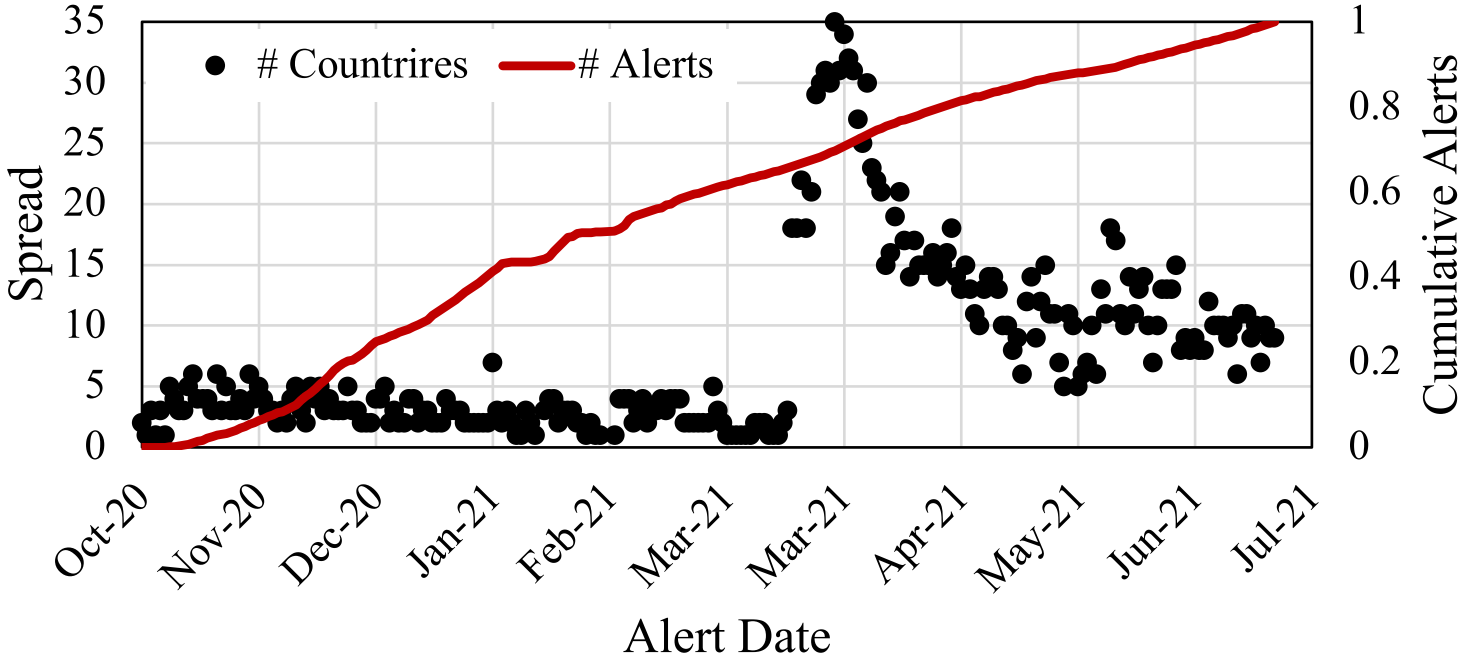
Geographical Movement of Exploits

- Example: Oracle WebLogic Vulnerability (CVE-2020-14882)
  - ❖322K alerts in a span of 240 days

Geographical Movement of Exploits

- Example: Oracle WebLogic Vulnerability (CVE-2020-14882)
  - ❖322K alerts in a span of 240 days

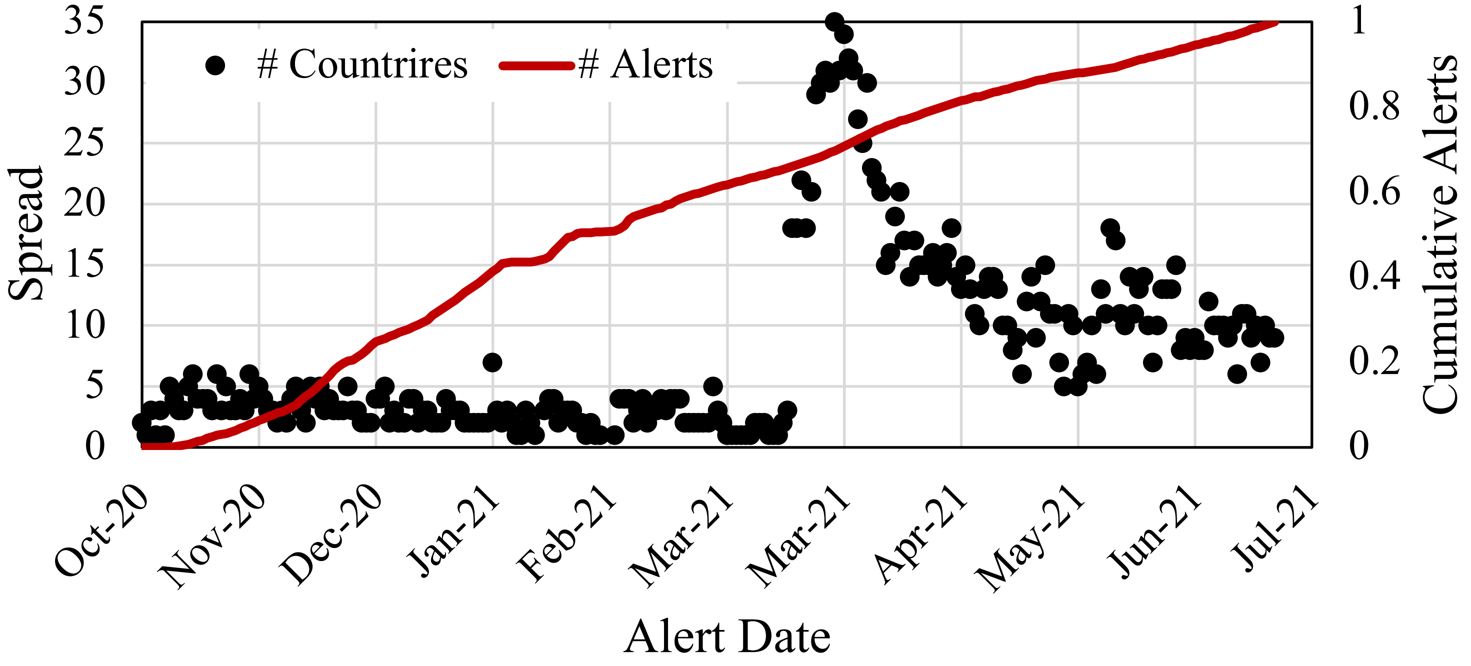
- First: Oct. 31st, 8:30 pm - China



Northeastern University
Khoury College of
Computer Sciences

Geographical Movement of Exploits

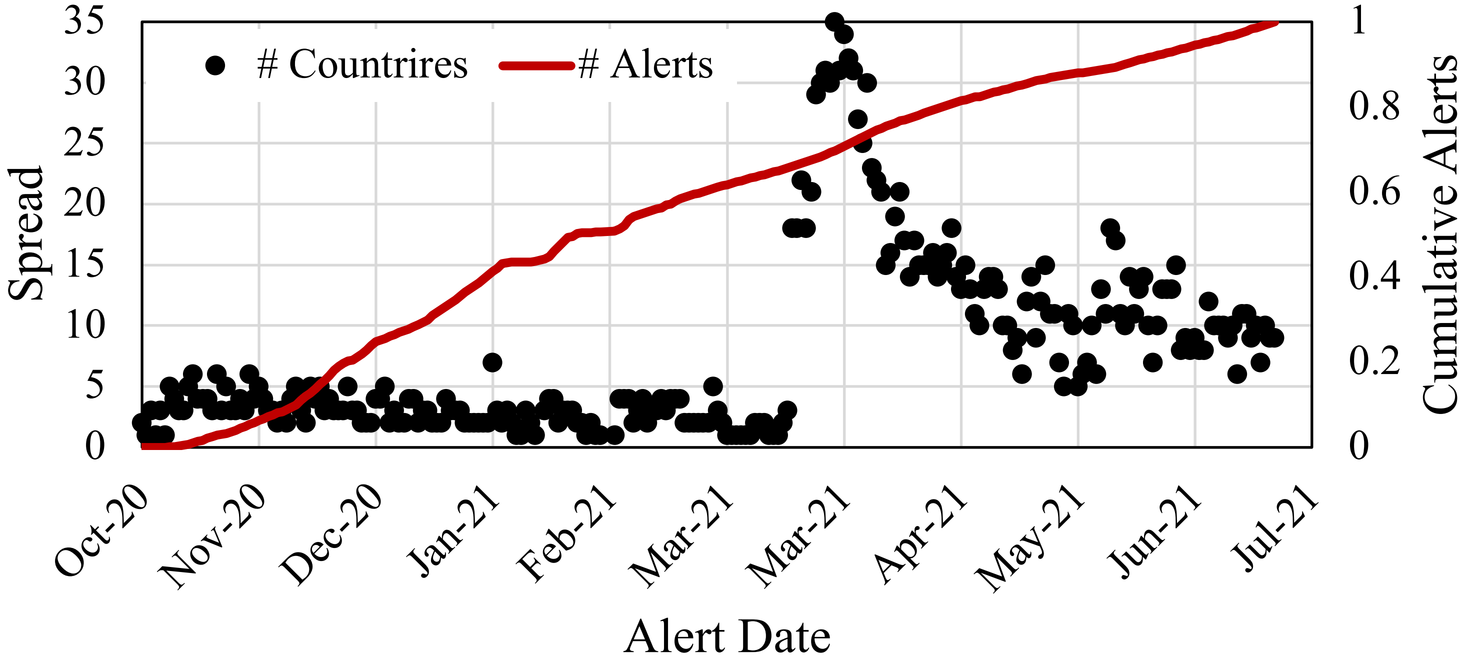
- Example: Oracle WebLogic Vulnerability (CVE-2020-14882)
  - ❖322K alerts in a span of 240 days



- First: Oct. 31st, 8:30 pm - China
- 1.5 hrs. later – Russia

Geographical Movement of Exploits

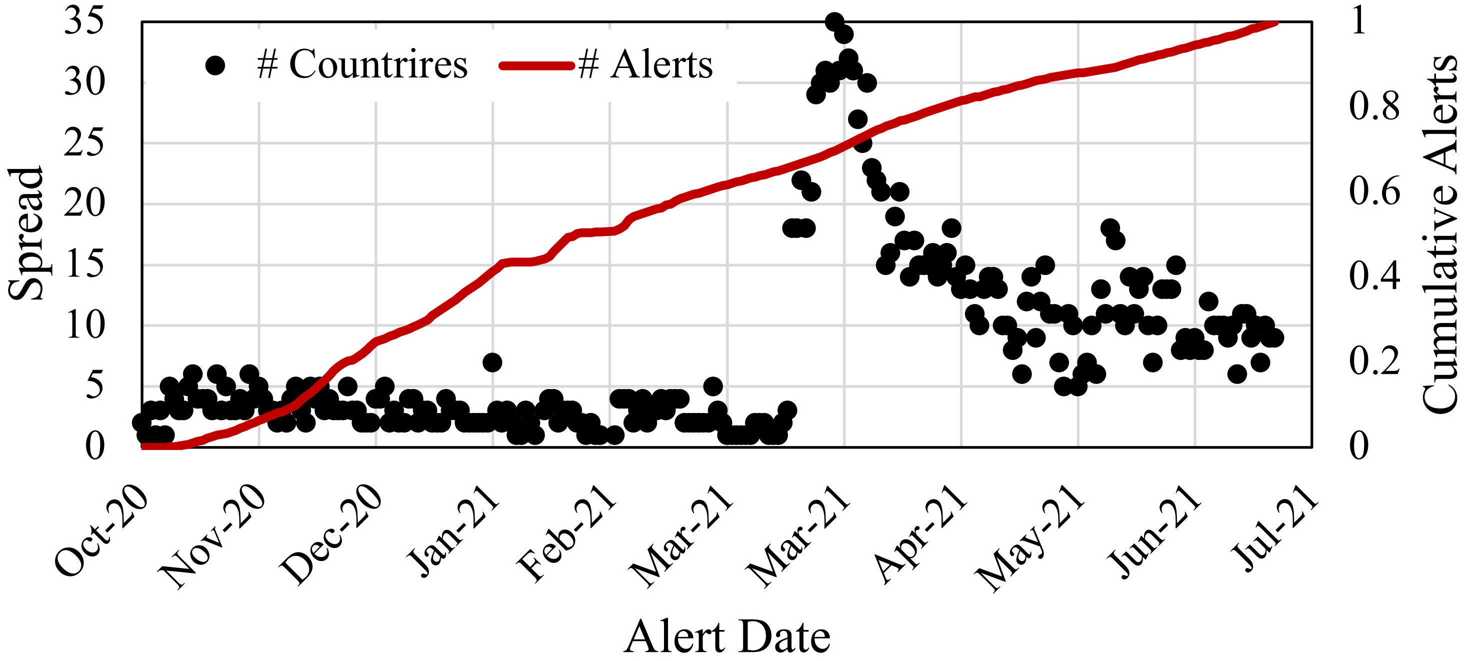
- Example: Oracle WebLogic Vulnerability (CVE-2020-14882)
  - ❖322K alerts in a span of 240 days



- First: Oct. 31st, 8:30 pm - China
- 1.5 hrs. later – Russia
- Day 3 - Hong Kong, Germany, and Netherlands

Geographical Movement of Exploits

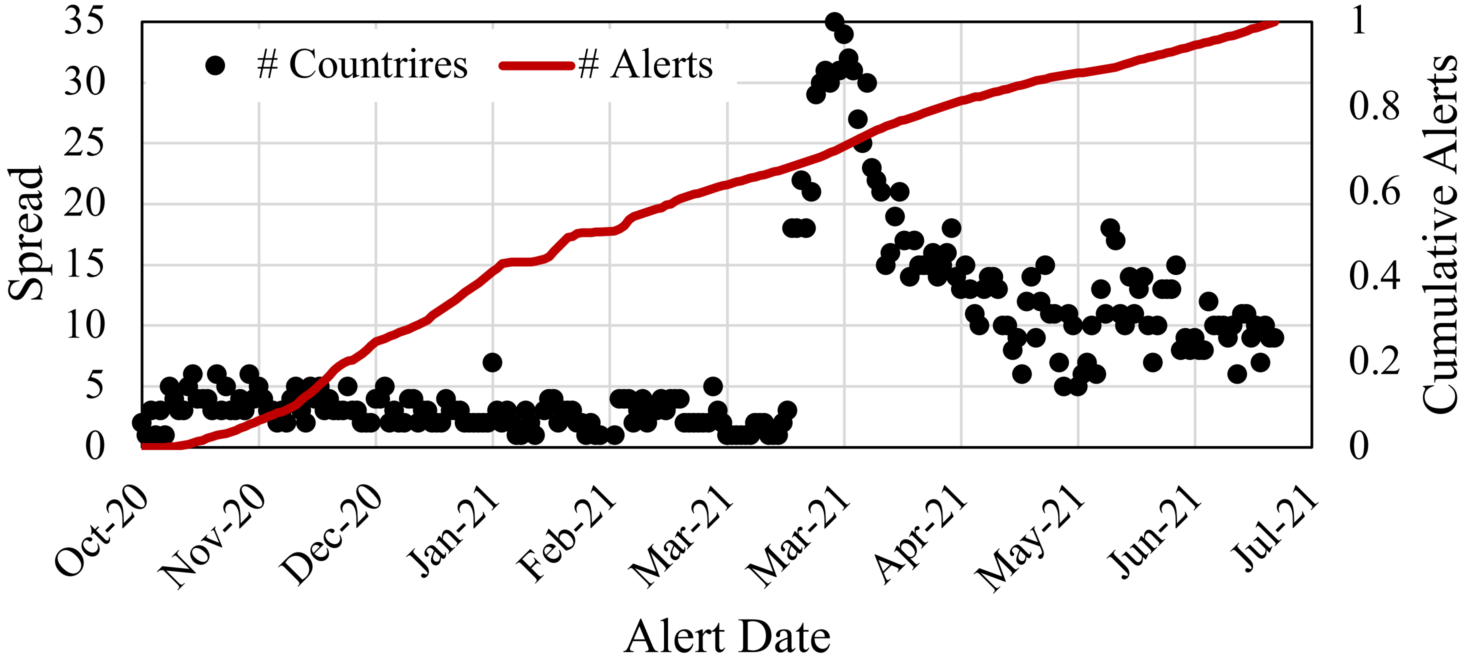
- Example: Oracle WebLogic Vulnerability (CVE-2020-14882)
  - ❖322K alerts in a span of 240 days



- First: Oct. 31st, 8:30 pm - China
- 1.5 hrs. later – Russia
- Day 3 - Hong Kong, Germany, and Netherlands
- A week later – 9 countries

Geographical Movement of Exploits

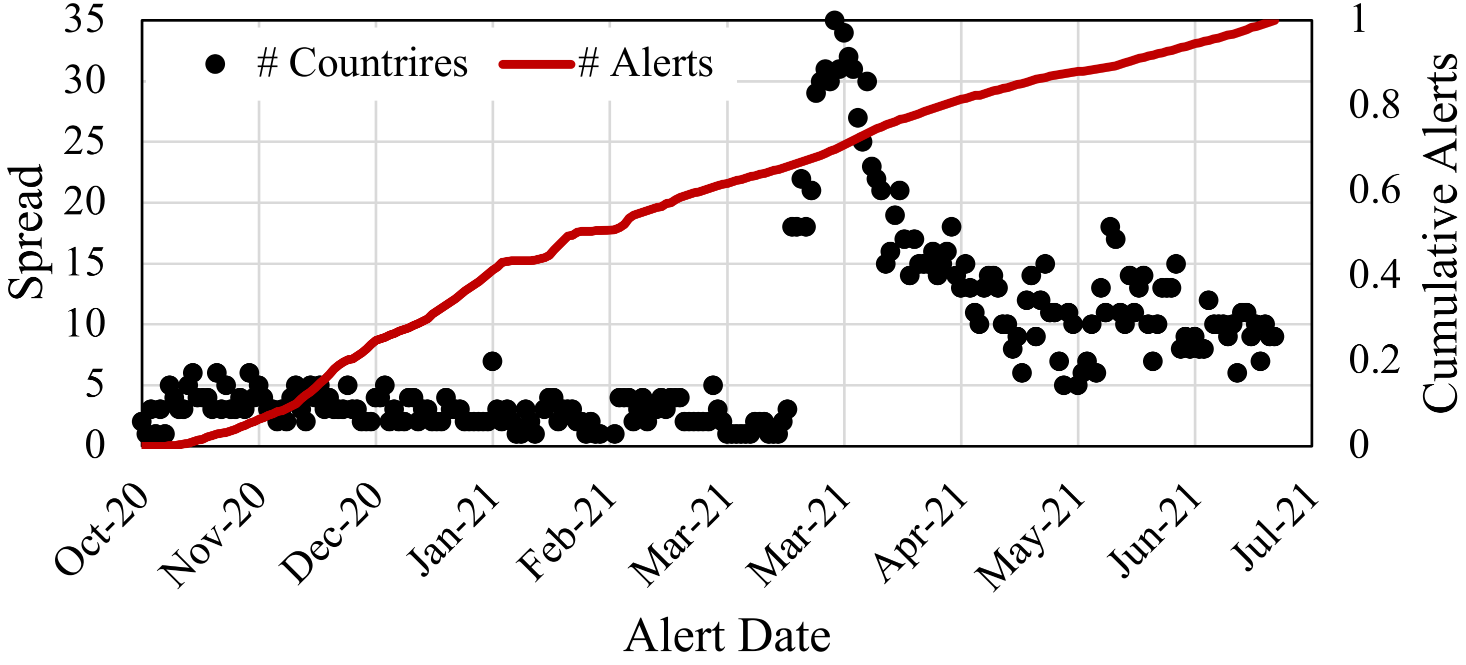
- Example: Oracle WebLogic Vulnerability (CVE-2020-14882)
  - ❖322K alerts in a span of 240 days



- First: Oct. 31st, 8:30 pm - China
- 1.5 hrs. later – Russia
- Day 3 - Hong Kong, Germany, and Netherlands
- A week later – 9 countries
- Until March 18th – 5 countries per day (but, 65% of alerts)
- In the next 18 days, 59 countries are added

Geographical Movement of Exploits

- Example: Oracle WebLogic Vulnerability (CVE-2020-14882)
  - ❖322K alerts in a span of 240 days



- First: Oct. 31st, 8:30 pm - China
- 1.5 hrs. later – Russia
- Day 3 - Hong Kong, Germany, and Netherlands
- A week later – 9 countries
- Until March 18th – 5 countries per day (but, 65% of alerts)
- In the next 18 days, 59 countries are added
- Overall - 85 countries targeted

Conclusion

- We analyze a dataset of 806 million alerts from 7 billion connections made by 662 honeypots

Conclusion

- We analyze a dataset of 806 million alerts from 7 billion connections made by 662 honeypots
- We design an OSCTI framework and gather attack and campaign inferences from the alerts

Conclusion

- We analyze a dataset of 806 million alerts from 7 billion connections made by 662 honeypots
- We design an OSCTI framework and gather attack and campaign inferences from the alerts
- We find that 17 networks involved in malware campaigns today overlap with the 24 rogue networks reported > 10 yrs. Ago
- Vulnerabilities disclosed >10 yrs. ago are still being actively exploited by various campaigns, e.g., APTs, RATs, and Emotet

Conclusion

- We analyze a dataset of 806 million alerts from 7 billion connections made by 662 honeypots
- We design an OSCTI framework and gather attack and campaign inferences from the alerts
- We find that 17 networks involved in malware campaigns today overlap with the 24 rogue networks reported > 10 yrs. Ago
- Vulnerabilities disclosed >10 yrs. ago are still being actively exploited by various campaigns, e.g., APTs, RATs, and Emotet
- We find empirical evidence of shared strategies among campaigns, shared infrastructure among campaigns and collaborative exploitation to amplify impact

Thank you!

Get in touch:

Afsah Anwar

afsahanwar@gmail.com

https://www.afsah.org/