SSHCURE

Flow-based Compromise Detection using NetFlow/IPFIX

Rick Hofstede

UNIVERSITY OF TWENTE.

REDSOCKS
malware threat defender

“51 percent of respondents admitted that their organizations have already been impacted by an SSH key-related compromise in the last 24 months.”

–Ponemon 2014 SSH Security Vulnerability Report

securityweek.com

DDoS Malware for Linux Distributed via SSH Brute Force Attacks

By Eduard Kovacs on February 09, 2015

Researchers at FireEye have been monitoring a campaign in which malicious actors use Secure Shell (SSH) brute force attacks to install a piece of DDoS malware on Linux and other types of systems.

The malware, dubbed XOR.DDoS, was first spotted back in September by the Malware Must Die research group, which linked it to a Chinese actor. XOR.DDoS is different from other DDoS bots because it's written in C/C++ and it uses a rootkit component for persistence.

FireEye started analyzing XOR DDoS in mid-November when it spotted SSH brute force attacks against its global threat research network coming from IP addresses belonging to Hee Thai Limited, an organization apparently based in Hong Kong. The security firm saw more than 20,000 SSH login attempts per server in the first 24 hours.

The second phase of the campaign took place between November 19 and November 30. By the end of November, FireEye had observed roughly 150,000 login attempts from almost every IP address belonging to Hee Thai Limited. The third phase, which according to researchers is more "chaotic" than the previous two, started on December 7 and continues even today. Nearly 1 million login attempts had been seen on each server by the end of

Most Recent | Most Read

» A Match Made in Heaven: Fraud and Social Media
» Researchers Bypass All Windows Protections by Modifying a Single Bit
» FBI Probes Newsweek Hack Following Threats
» Chinese Spy Team Hacks Forbes.com: Security Firms
» White House to Create New Cyber Security Agency
» Microsoft Patches Critical Windows, Internet Explorer Vulnerabilities in Patch Tuesday Update
» Cybercriminals Use DNS Poisoning in Brazilian Boleto Fraud Scheme
» Gas Pump Monitoring System Compromised in Attack: Trend Micro

Level(3) COMMUNICATIONS
Connecting and Protecting the Networked World℠

Beyond Bandwidth
Level 3 Communications Blog

It Takes a Village – Collaborative Steps to Breaking Botnets: How Level 3 and Cisco Worked Together to Improve the Internet's Security and Stop SSHPsychos

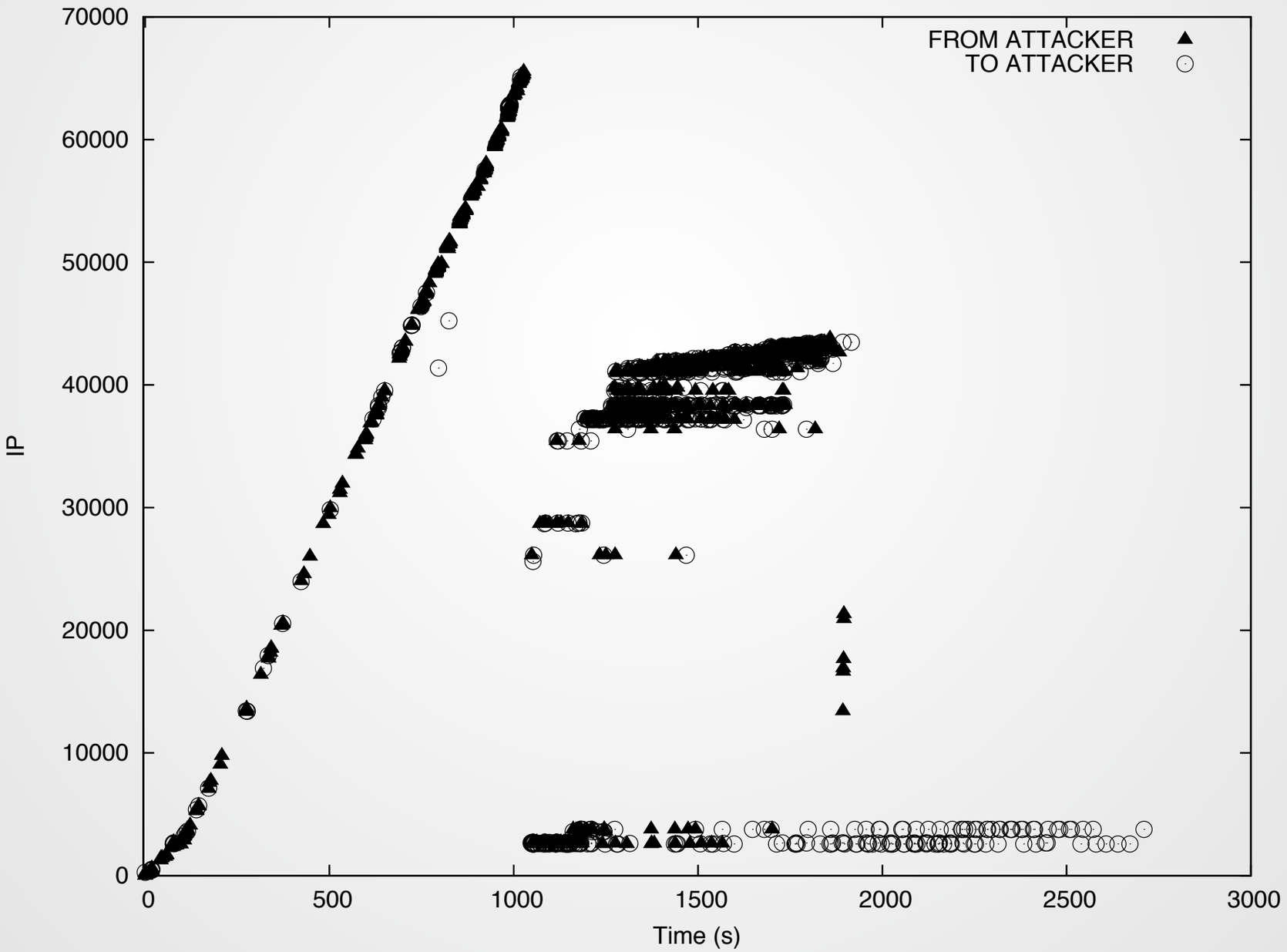
Level 3 Threat Research Labs / April 9, 2015

The information security community's ability to respond to threats and vulnerability discovery improves with each passing month. The collective reaction from the security community to a new file hash, new technique, or communication method has never been stronger. However, attackers are also keeping up, or even exceeding the security world's defenses.

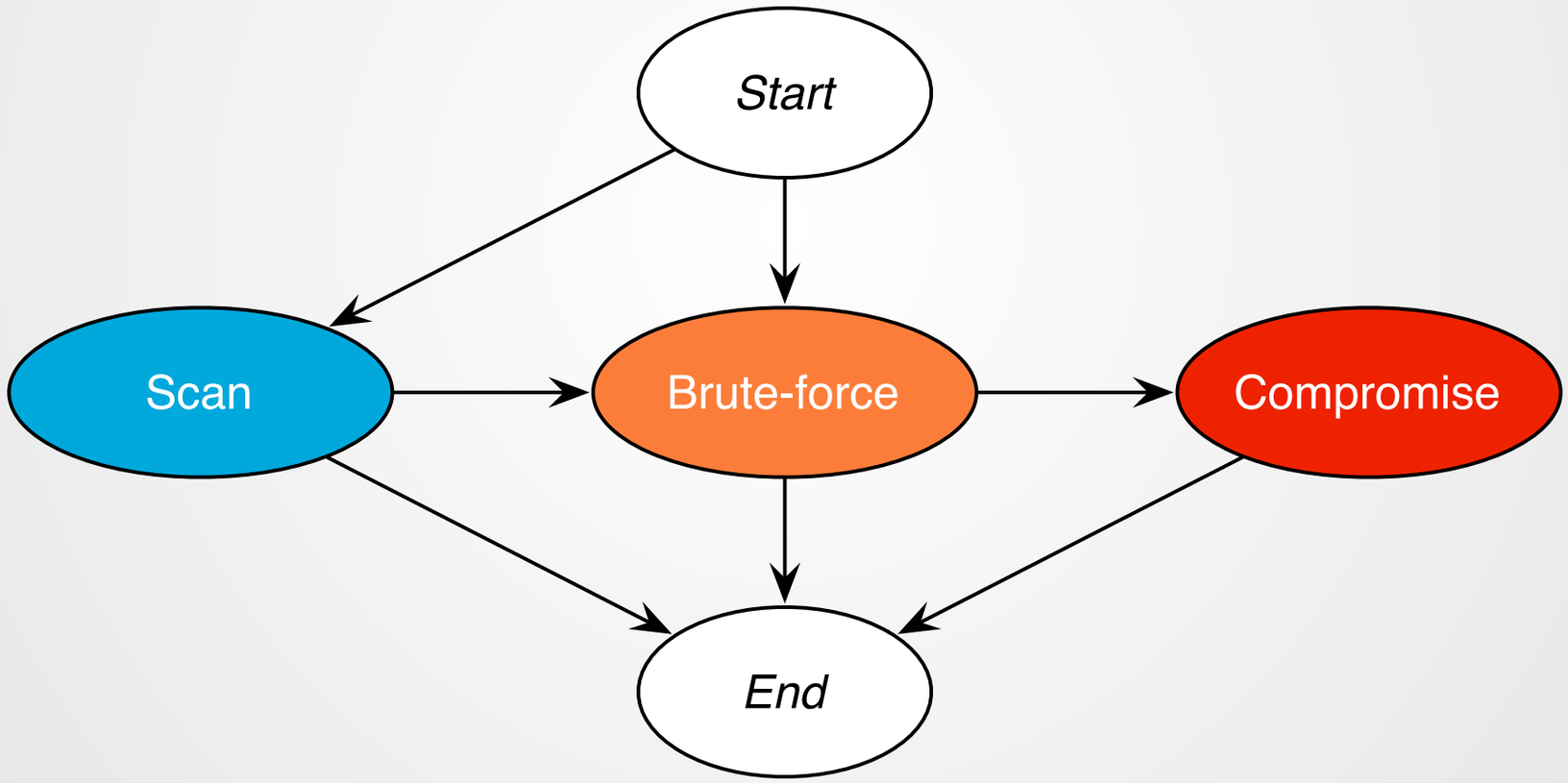
One way to balance this problem is to not only focus on identifying the threat, but also to find an effective method of removing it from the Internet. Too often problem identification is confused with problem removal, leaving attackers observed, yet still able to pursue their goals.

This is why Level 3's Threat Research Labs and Cisco's Talos Group worked together to investigate and mitigate the risk posed by an attacker's Internet-wide scanning and DDoS botnet, SSHPsychos.

SSH attacks


FROM ATTACKER
TO ATTACKER
IP
Time (s)
0
10000
20000
30000
40000
50000
60000
70000
0
500
1000
1500
2000
2500
3000

SSH attacks



SSH attacks

- SSH intrusion detection on end hosts is hardly scalable
- Network-based approaches exist, but only inform security operators about the presence of attacks

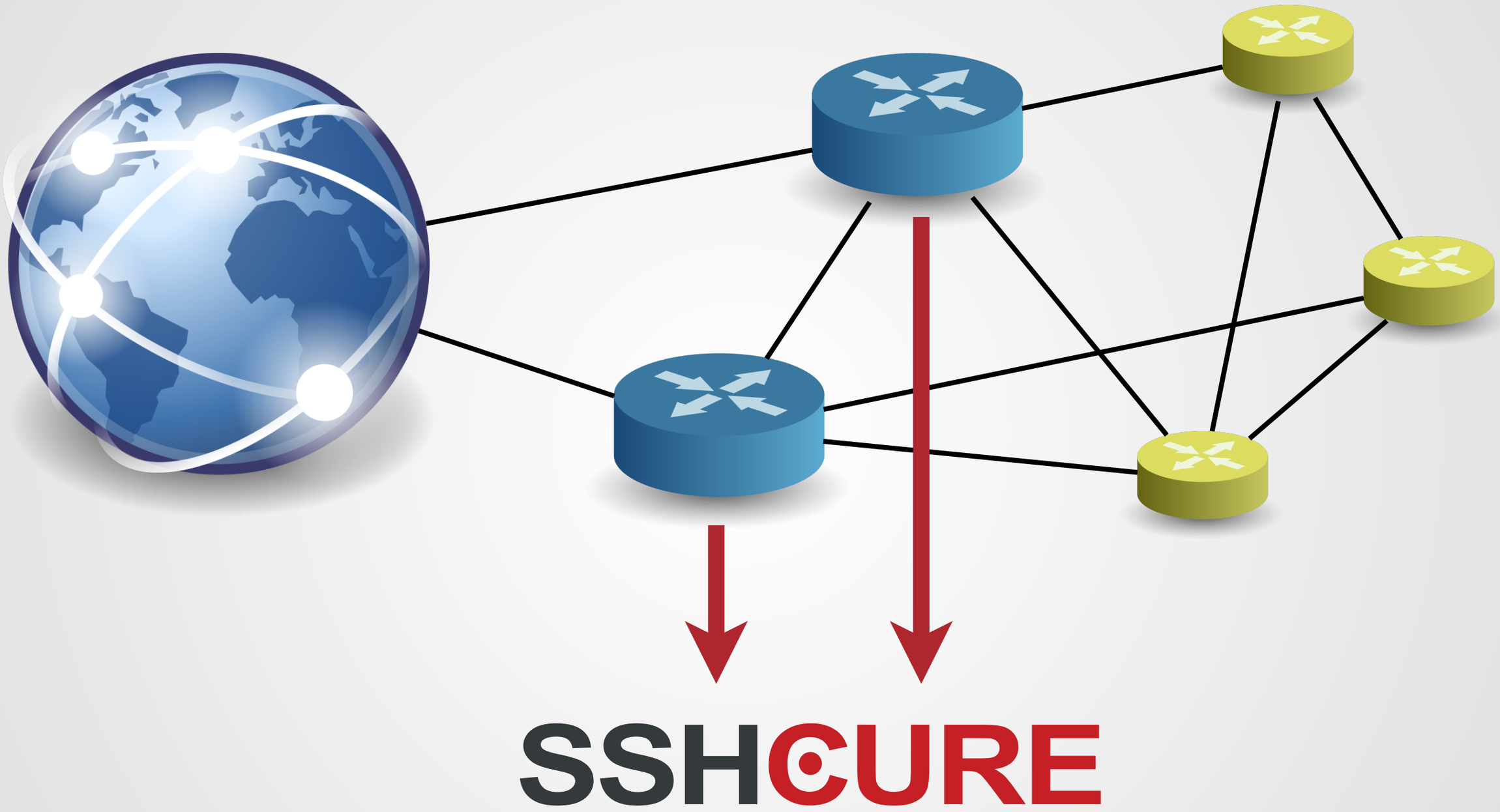
We perform compromise detection.

UNIVERSITY OF TWENTE.

REDSOCKS
malware threat defender

We perform compromise detection.

All flow-based.



UNIVERSITY OF TWENTE.

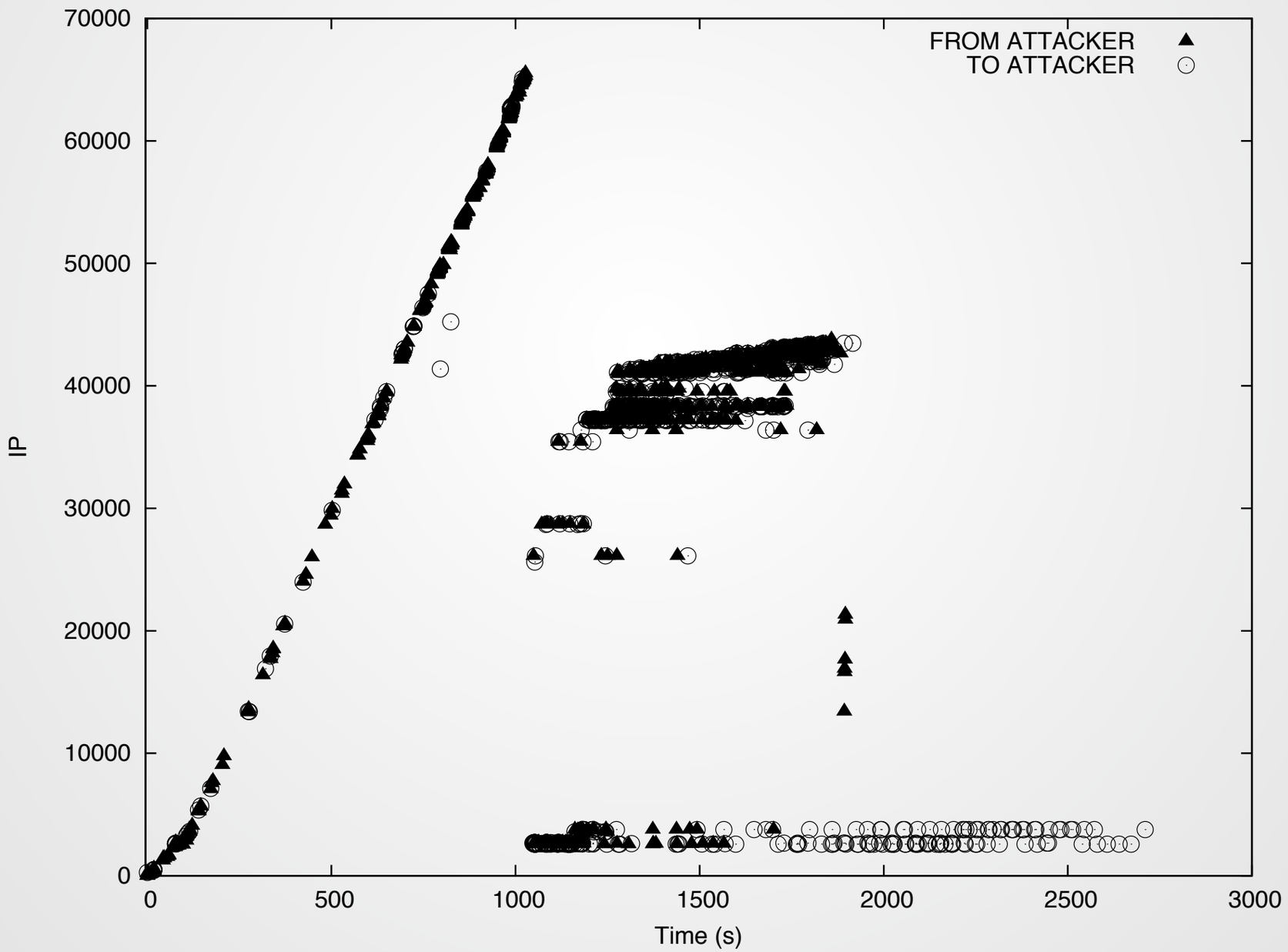
REDSOCKS
malware threat defender

NetFlow & IPFIX

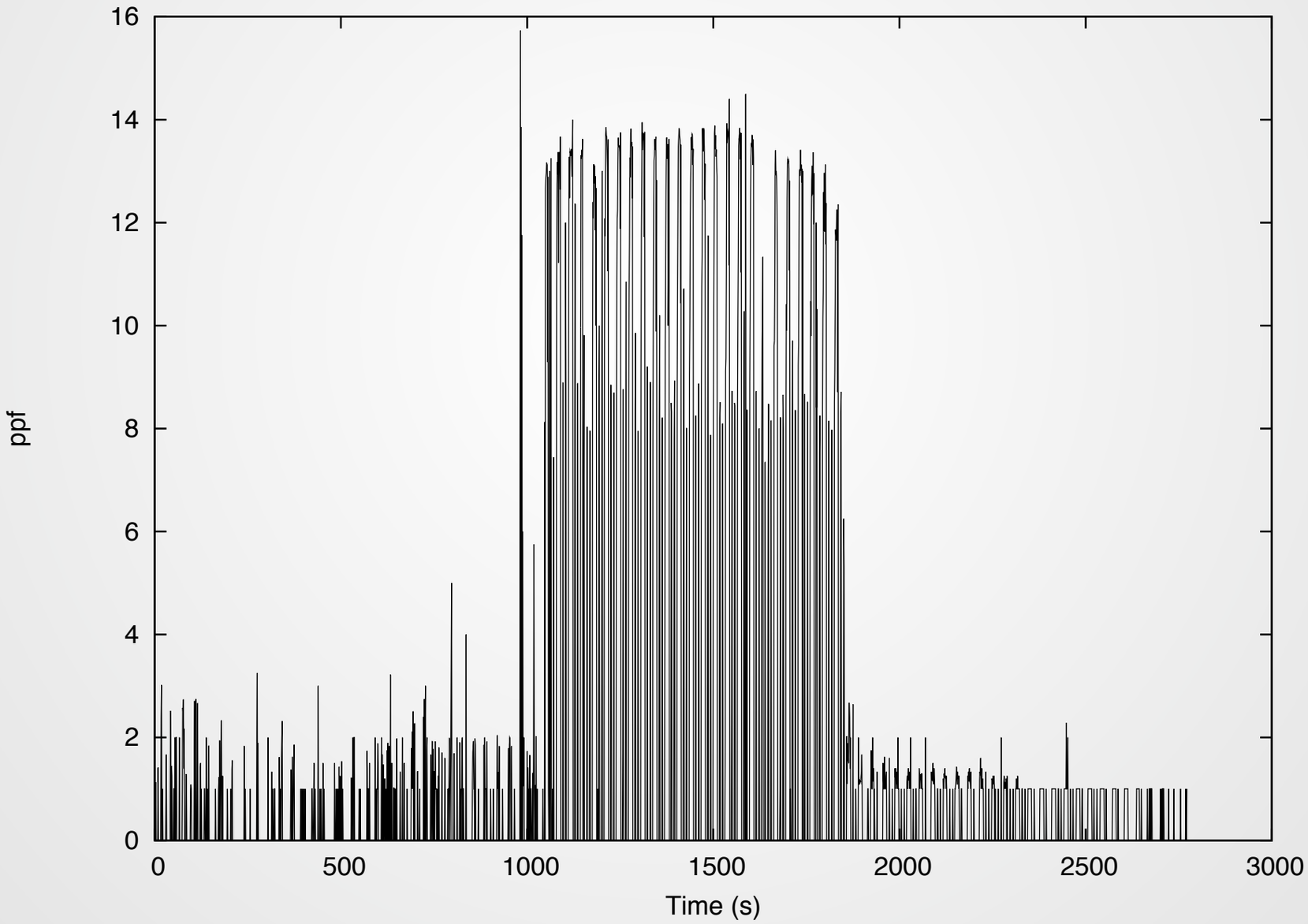
Start	Duration	Proto	SrcIP:Port	DstIP:Port	Packets	Bytes
2014-05-29 04:59:23	6.350	TCP	A:33038	B:22	11	1675
2014-05-29 04:59:26	4.950	TCP	A:33101	B:22	11	1675
2014-05-29 04:59:28	4.850	TCP	A:33126	B:22	11	1675

- Packets are aggregated into flows; aggregates are analyzed
  - ➤ Scalable, privacy-preserving
- NetFlow & IPFIX are available on most high-end networking devices
  - ➤ Easily deployable

SSH attacks

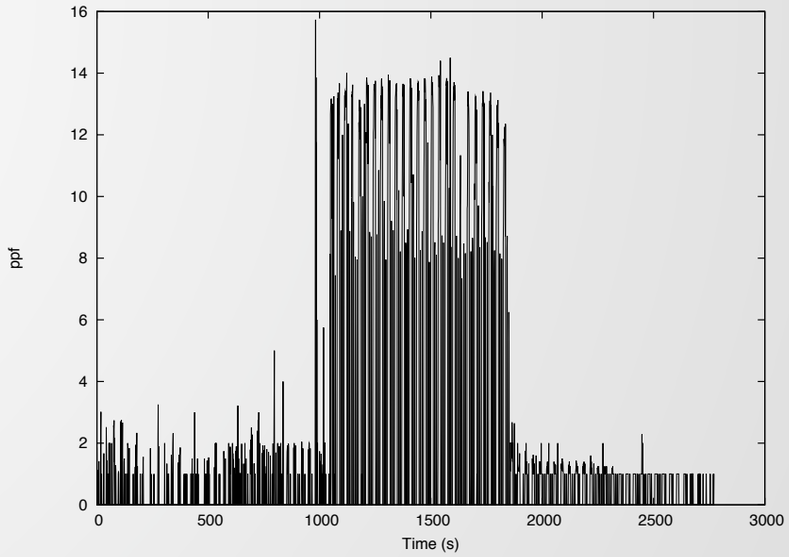

FROM ATTACKER
TO ATTACKER
IP
Time (s)
0
10000
20000
30000
40000
50000
60000
70000
0
500
1000
1500
2000
2500
3000

SSH attacks



Compromise detection

- Deviation-based approach yielded many false detections:
  - Retransmissions
  - Various acknowledgement schemes (e.g., depending on timing)
  - …

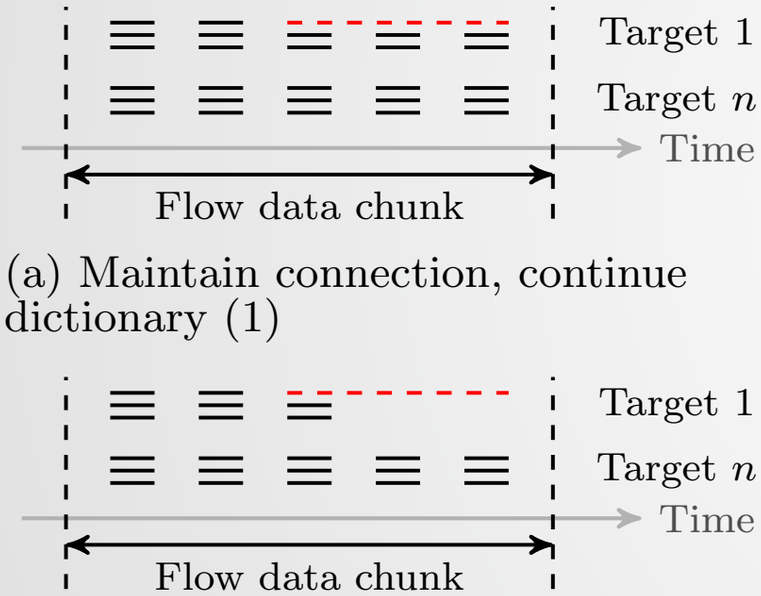


- Our approach: analyze and characterize attack tool behavior (action upon compromise)

Compromise detection

SSH Compromise Detection using NetFlow/IPFIX.
In: ACM SIGCOMM Computer Communication Review, October 2014

Compromise detection

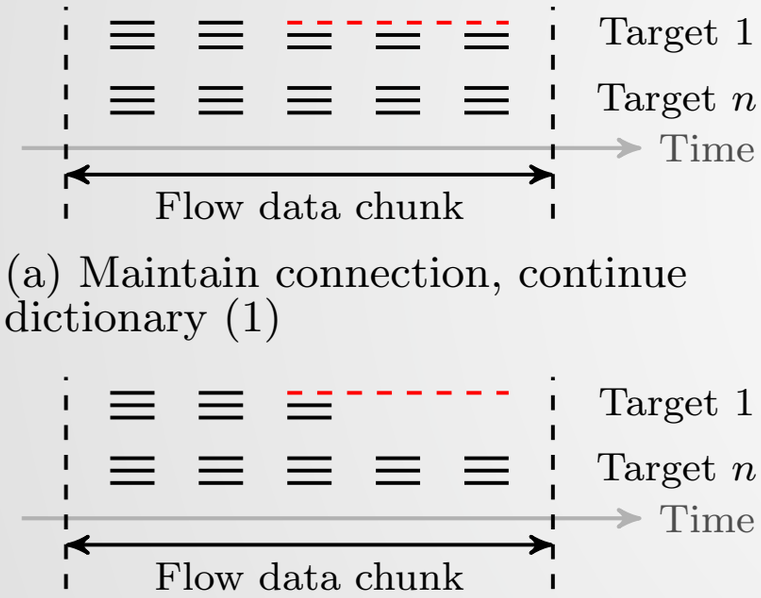


(a) Maintain connection, continue dictionary (1)

(d) Maintain connection, abort dictionary (1)

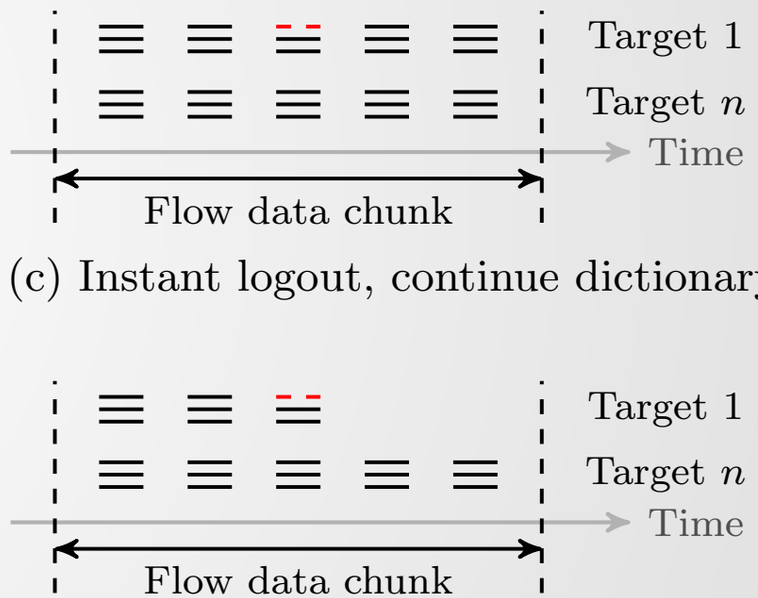
SSH Compromise Detection using NetFlow/IPFIX.
In: ACM SIGCOMM Computer Communication Review, October 2014

Compromise detection



(a) Maintain connection, continue dictionary (1)

(d) Maintain connection, abort dictionary (1)

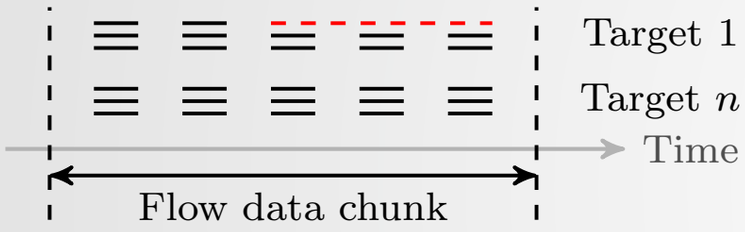


(c) Instant logout, continue dictionary

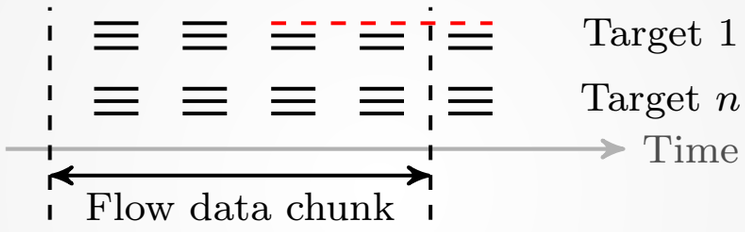
(f) Instant logout, abort dictionary

SSH Compromise Detection using NetFlow/IPFIX.
In: ACM SIGCOMM Computer Communication Review, October 2014

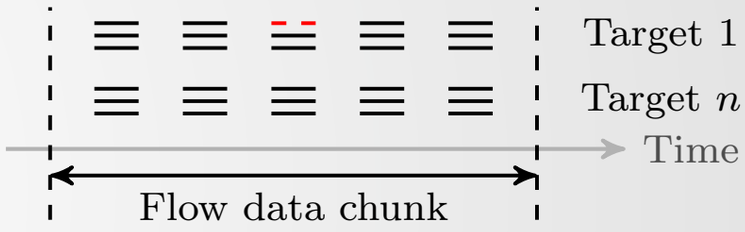
Compromise detection



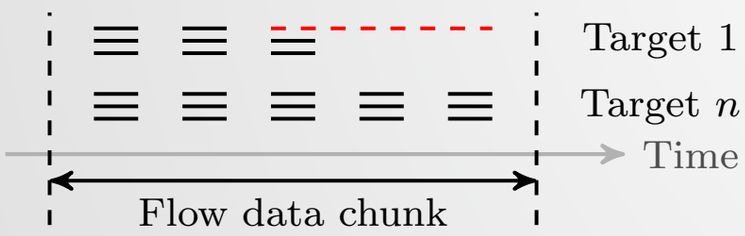
(a) Maintain connection, continue dictionary (1)



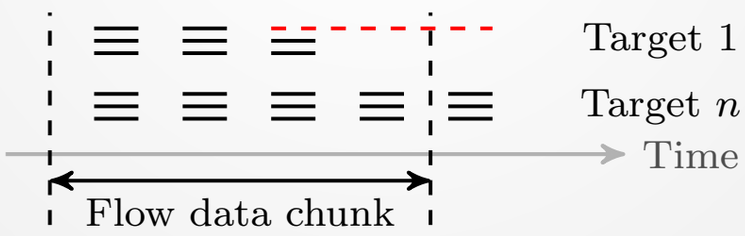
(b) Maintain connection, continue dictionary (2)



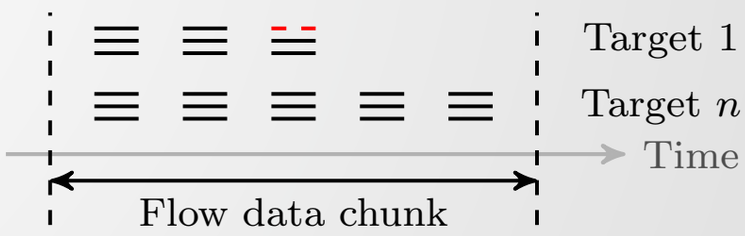
(c) Instant logout, continue dictionary



(d) Maintain connection, abort dictionary (1)



(e) Maintain connection, abort dictionary (2)



(f) Instant logout, abort dictionary

SSH Compromise Detection using NetFlow/IPFIX.
In: ACM SIGCOMM Computer Communication Review, October 2014

NFSEN – Profile live

https [redacted]/nfsen/nfsen.php?sub_tab=1

Home | Graphs | Details | Alerts | Stats | Plugins | live | Bookmark URL | Profile: | live ▼

SURFmap | SSHCure

Dashboard

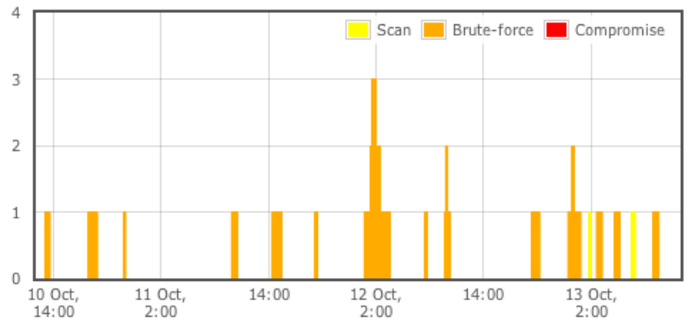
SSHCure Version 2.2 UNIVERSITY OF TWENTE.

Dashboard

Search Help About License

Time range: 3 days **from** Thu. Oct 10, 2013 12:00 **Thu. Oct 10, 2013 - Sun. Oct 13, 2013**

Attacks



Date	Ongoing	Phases	Attacker	Targets
Sun. Oct 13, 2013 09:01			[redacted]	65536
Sun. Oct 13, 2013 02:43			[redacted]	12089
Sat. Oct 12, 2013 23:58			[redacted]	437
Sat. Oct 12, 2013 19:29			[redacted]	16641
Sat. Oct 12, 2013 03:02			[redacted]	19905
Sat. Oct 12, 2013 01:38			[redacted]	10422
Sat. Oct 12, 2013 00:46			[redacted]	57856
Fri. Oct 11, 2013 09:57			[redacted]	4025
Thu. Oct 10, 2013 17:59			[redacted]	4562
Thu. Oct 10, 2013 13:06			[redacted]	8090
Sun. Oct 13, 2013 04:45			[redacted]	1
Sun. Oct 13, 2013 04:17			[redacted]	1

Top attackers - scan

Attacker	Attacks	Targets
[redacted]	3	4025
[redacted]	2	16641
[redacted]	1	65536
[redacted]	1	65536
[redacted]	1	65144
[redacted]	1	57856
[redacted]	1	32812
[redacted]	1	19905
[redacted]	1	16641
[redacted]	1	12089

Top attackers - brute-force & compromise

Attacker	Attacks	Targets
[redacted]	6	1
[redacted]	2	4025
[redacted]	1	65536
[redacted]	1	57856
[redacted]	1	19905
[redacted]	1	16641
[redacted]	1	12089
[redacted]	1	10422
[redacted]	1	8090
[redacted]	1	437

Top targets - brute-force

Target	Attacks	Attack blocked
[redacted]	8	✖
[redacted]	7	✖
[redacted]	7	✖
[redacted]	7	✖
[redacted]	7	✖
[redacted]	7	✖
[redacted]	7	✖
[redacted]	7	✖
[redacted]	7	✖
[redacted]	7	✖

Top targets - compromise

Target	Attacks	Compromises
No data available for selected time period...		

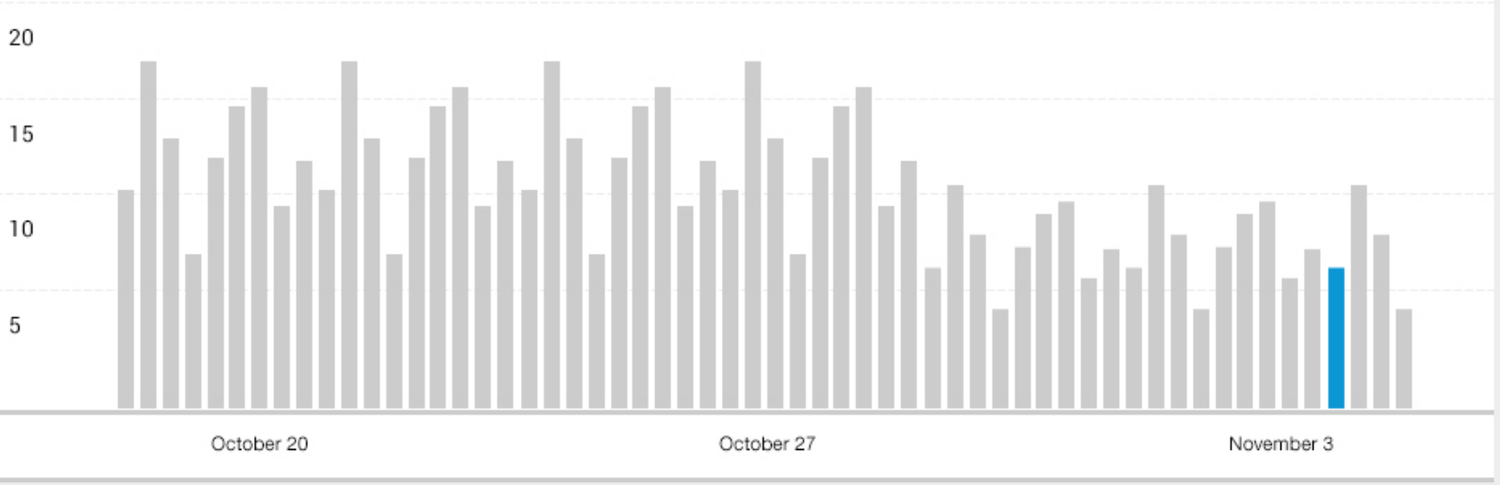
SSHCURE a flow-based intrusion detection system for NfSen. UNIVERSITY OF TWENTE.

- Dashboard
- Incoming
- Outgoing
- Hosts
- Search
- Status
- Help
- Settings

Incoming attacks

Visits — Scan — Brute force — Compromise

Day | Week | Month



Incoming attacks

Phases	Active	Attacker	Date	Targets
	⚡	123.123.123.123	Mon. Jun 30, 2014 19:57	12
		123.123.123.123	Mon. Jun 30, 2014 19:57	456
		130.89.148.136	Mon. Jun 30, 2014 19:57	32
	⚡	123.123.123.123	Mon. Jun 30, 2014 19:57	7455
		123.123.123.123	Mon. Jun 30, 2014 19:57	64

Top targets - Compromise

Target	Attacks	Compromise
123.123.123.123	12	2
123.123.123.123	456	3
130.89.148.136	32	5
123.123.123.123	7455	64
123.123.123.123	64	78

Outgoing attacks

Phases	Active	Attacker	Date	Targets
	⚡	123.123.123.123	Mon. Jun 30, 2014 19:57	12
		123.123.123.123	Mon. Jun 30, 2014 19:57	456
		130.89.148.136	Mon. Jun 30, 2014 19:57	32
	⚡	123.123.123.123	Mon. Jun 30, 2014 19:57	7455
		123.123.123.123	Mon. Jun 30, 2014 19:57	64

Top targets - Brute Force

Target	Attacks	Compromise
123.123.123.123	12	2
123.123.123.123	456	3
130.89.148.136	32	5
123.123.123.123	7455	64
123.123.123.123	64	78

SSHCure

Validation approach

- Ground truth: `sshd` logs from 93 honeypots, servers and workstations, divided over two datasets:
  - Dataset 1 — easy targets
  - Dataset 2 — more difficult targets

	Honeypots	Servers	Workstations	Attacks
Dataset 1	13	0	0	636
Dataset 2	0	76	4	10353

SSHCure

Validation results

- Evaluation metrics:
  - TP / FP — correct / false identification of incident
  - TN / FN — correct / false identification of non-incident
- Detection accuracy close to 100%

	TPR	**TNR**	**FPR**	**FNR**	***Acc***
Dataset 1	0,692	0,921	0,079	0,308	0,839
Dataset 2	—	0,997	0,003	—	0,997

SSHCure

Deployment

- **SSHCURE** is open-source and actively developed
  - Download counter SourceForge (Jan. ’15): 3.1k
  - Recently moved to GitHub (summer ’14)
- Tested in several nation-wide backbone networks
- Many successful deployments already:
  - Web hosting companies
  - Campus networks
  - National Research and Education Networks (NRENs)
  - Governmental CSIRTs/CERTs

What is hidden in *non-flat* traffic…

Unveiling Flat Traffic on the Internet: An SSH Attack Case Study
Mattijs Jonker, Rick Hofstede, Anna Sperotto and Aiko Pras
In: 2015 IFIP/IEEE International Symposium on Integrated Network Management, May 2015

TCP measurements

- Retransmissions
- Control information types (~10):
  - Duplicate ACK
  - Window update
  - KeepAlive Probe/Response
  - …

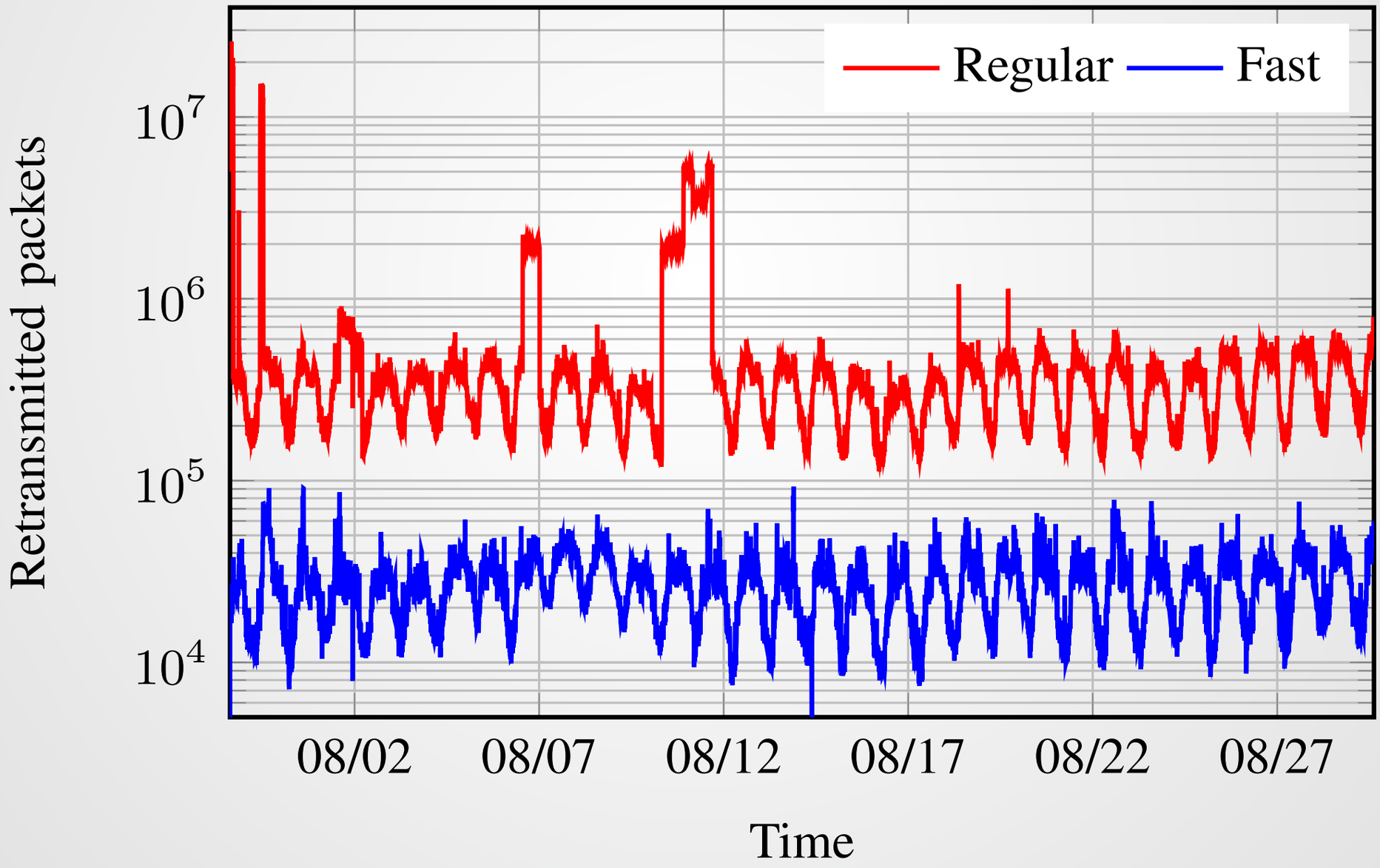
TCP measurements

- Retransmissions
- Control information types (~10):
  - Duplicate ACK
  - Window update
  - KeepAlive Probe/Response
  - …

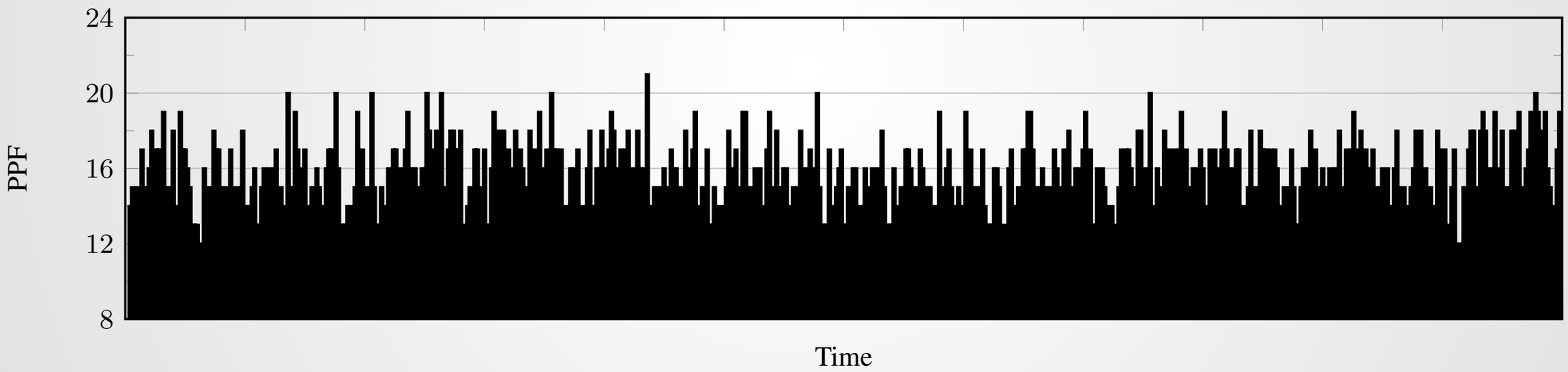
Dataset	Period	Duration	Packets	Bytes	Flows	Retransmissions		Control Information	
						Packets	*Bytes*	*Packets*	*Bytes*
UT	July / August 2014	31 days	370.73 G	291.64 TiB	7.35 G	5.30 G (1.43%)	2.83 TiB (0.97%)	100.50 G (27.11%)	4.30 TiB (1.47%)
CESNET	August / September 2014	31 days	257.38 G	227.67 TiB	3.57 G	8.29 G (3.22%)	2.78 TiB (1.22%)	83.61 G (32.48%)	3.48 TiB (1.53%)

Retransmissions?

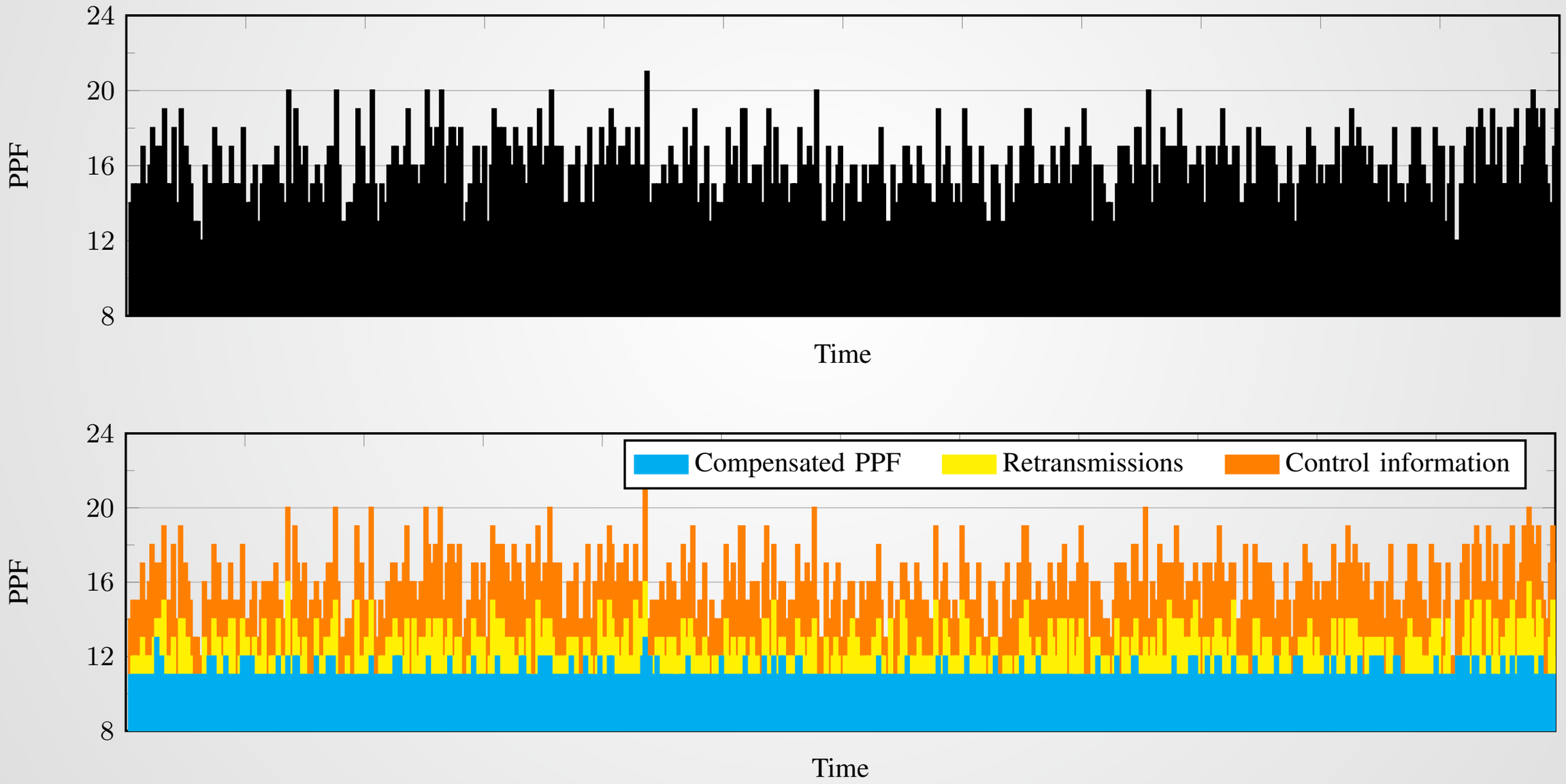
Retransmissions?



PPF compensation

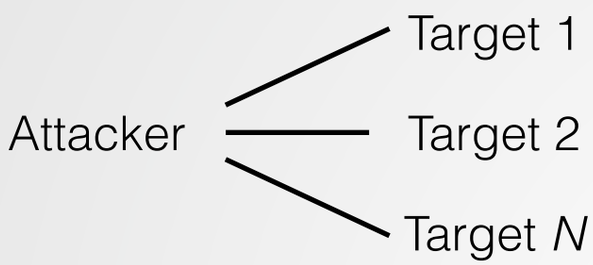


PPF compensation

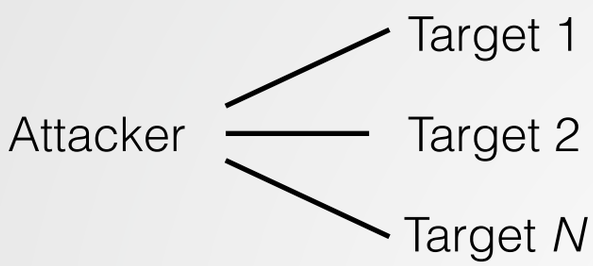


Detection results

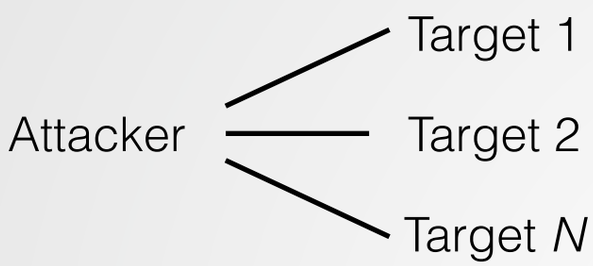
Detection results



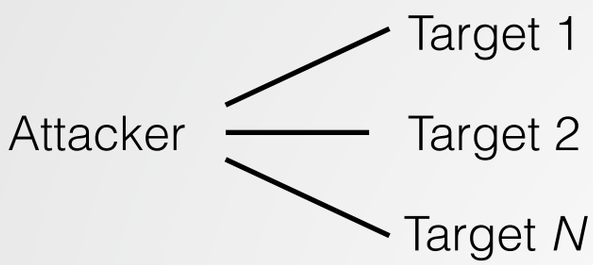
Detection results

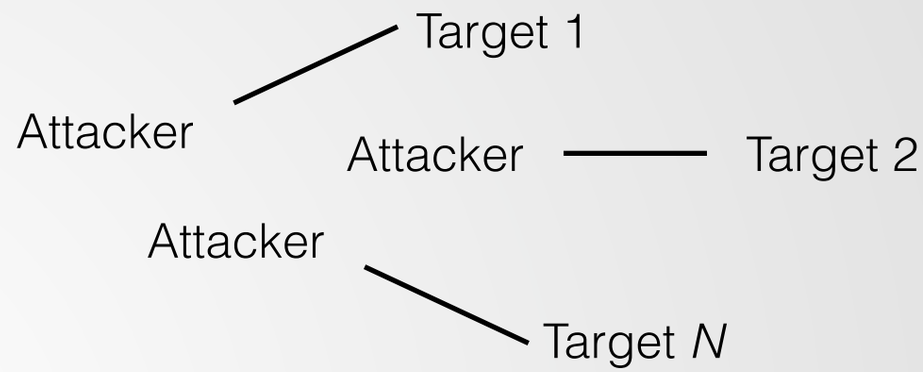


Detection results



Detection results





Detection results

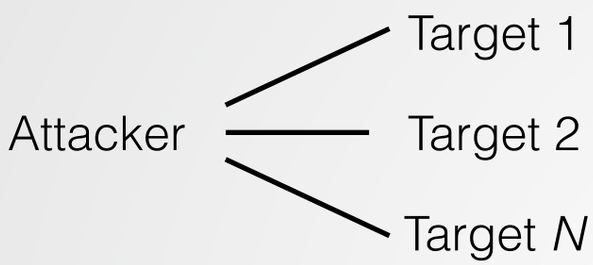


TABLE VII
TOP FIVE ATTACK ORIGINS – ATTACKS

Dataset	Country	Non-compensated	Compensated
UT1	China	370	494 (+34%)
	Netherlands	63	72 (+14%)
	Russian Federation	42	45 (+7%)
	Other	142	159 (+12%)
	Total	**617**	**774 (+25%)**
CESNET1	Canada	5	49 (+880%)
	France	3	30 (+900%)
	Germany	4	5 (+25%)
	Other	14	19 (+36%)
	Total	**26**	**99 (+281%)**

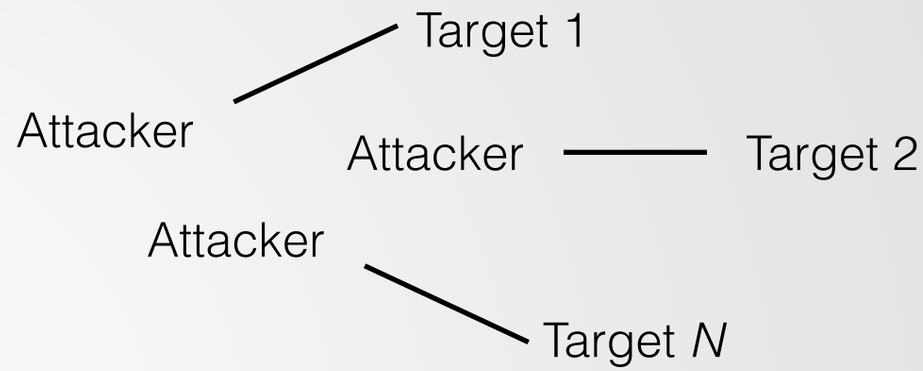


TABLE VIII
TOP FIVE ATTACK ORIGINS – TUPLES

Dataset	Country	Non-compensated	Compensated
UT1	China	6137	10040 (+64%)
	Vietnam	1048	1056 (+1%)
	United States	638	658 (+3%)
	Other	2027	8346 (+311%)
	Total	**9850**	**14074 (+43%)**
CESNET1	Poland	1186	2365 (+99%)
	France	10	613 (+6030%)
	Canada	19	520 (+2637%)
	Other	369	487 (+32%)
	Total	**1584**	**3985 (+152%)**

Detection results

TABLE VIII
DETECTION PERFORMANCE – ATTACKS

Dataset	Logged attacks	TPR	FPR	TNR	FNR	*Acc*
UT	812	0.644	0.087	0.913	0.356	0.788
compensated		0.784	0.096	0.904	0.216	0.849

TABLE X
DETECTION PERFORMANCE – TUPLES

Dataset	Logged tuples	TPR	FPR	TNR	FNR	*Acc*
UT	4562	0.430	0.081	0.919	0.570	0.689
compensated		0.585	0.090	0.910	0.415	0.758

What’s next?

Danielle Walker, Senior Reporter
Follow @daniellewlkr

February 26, 2015

Botnet of Joomla servers furthers DDoS-for-hire scheme

Researchers have uncovered a distributed denial-of-service (DDoS) attack campaign that takes advantage of Joomla servers with a vulnerable Google Maps plug-in installed.

A vulnerable Google Maps plug-in for Joomla allowed attackers to spoof the source of DDoS attacks.

Akamai's Prolexic Security Engineering & Research Team (PLXsert) worked with PhishLabs' Research, Analysis, and Intelligence Division (R.A.I.D) to analyze malicious traffic coming from multiple Joomla websites, a threat advisory (PDF) issued Wednesday said.

Through analysis, the teams found that attackers were able to use servers as DDoS zombies due to a vulnerability in a Google Maps plug-in that allows the plug-in to act as a proxy, masking the origin of DDoS attacks.

"Attackers spoof the source of the request, causing the results to be sent from the proxy to someone else – their denial of service target," a release from Akamai explained. This year, the company has observed eight Joomla-based DDoS attacks against its customer base, six of which were targeted at the education sector.

wptavern.com

WP TAVERN

EST 2009

100,000+ WordPress Sites Compromised Using the Slider Revolution Security Vulnerability

Sarah Gooding December 15, 2014 31

photo credit: Ravages – cc

Over the weekend, the security team at Sucuri discovered that more than

★ CURRENTLY ON TAP


XSS Vulnerability Affects More Than a Dozen Popular WordPress Plugins

Zero Day XSS Vulnerability in WordPress 4.2 Currently Being Patched

WordPress 4.2.1 Released to Patch Comment Exploit Vulnerability

Poll: How Often Do You Read a WordPress Plugin's Changelog Before Updating?

18 Free WordPress Themes Built With Bootstrap

RECENT COMMENTS

https://nl.linkedin.com/in/rhofstede/

www http://rickhofstede.nl

@ r.j.hofstede@utwente.nl,
rick.hofstede@redsocks.nl

Questions?

https://github.com/SSHCure/SSHCure