



DYNAMITE

A N A L Y T I C S

Our Presenter



Jamin Becker

Chief Technology Officer
Dynamite Analytics

Jamin is a career network defender and creator of PacketTotal, the largest public PCAP analytic service in the world.

The Company

Originally
founded as Vlabs
in 2015

Small Business
Cybersecurity
Software

Network Traffic Analysis
Network Detection and Response

Winner of multiple federal R&D
awards related to Network Traffic
Analysis

HQ in Atlanta
Georgia



The Dynamite Family



The worlds largest public PCAP analysis
platform (over 100K PCAPs)
Thousands of users worldwide

Dynamite Agent

Commercial Network Sensor for NDR
Network Metadata and Security Alerts
API Integration and Web UI

PCAP Anonymizer

Free utility for sanitizing packet-capture files
Advanced packet transformation options

DynamiteNSM

Open-source Network Security Monitor
Full stack for network traffic analysis
Native integration of Zeek and Suricata
github.com/DynamiteAI/dynamite-nsm

Briefing and Demo

PACKETTOTAL

Design Goals

Simplify the process of PCAP analysis

Provide a platform for sharing network traffic samples

Prioritize the importance of search



DYNAMITE
ANALYTICS

+1-760-760-7014

7

Demos

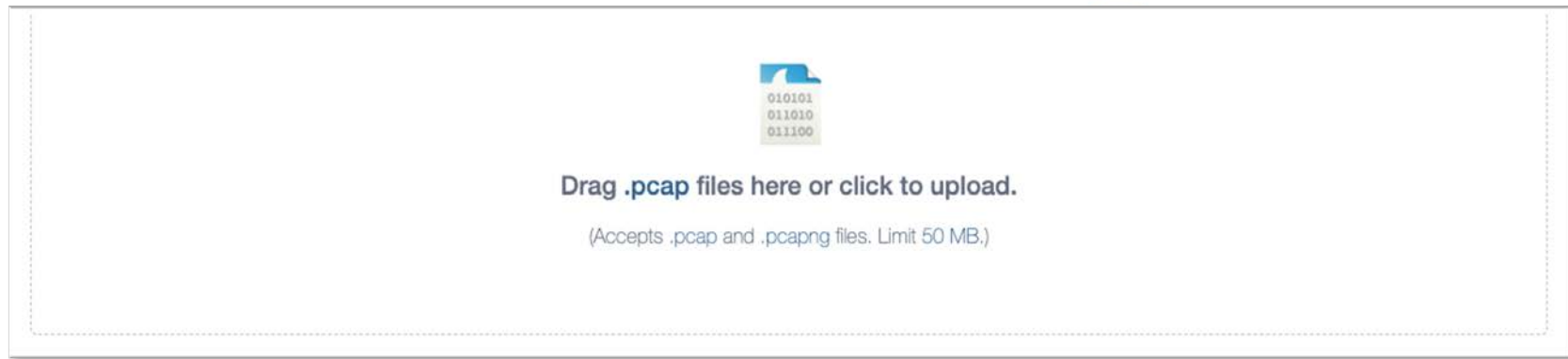
- ✓ Analyzing a Packet Capture File
- ✓ Locating Captures via Search
- ✓ Locating Captures via Similar Search

Be careful what you upload!

- ✓ Avoid uploading pcaps of home or work networks
- ✓ Avoid capturing traffic containing information about your environment
- ✓ Consider using capture filters, only capture the traffic you wish to analyze/share
- ✓ Consider capturing pcaps from sandboxed environment

Analyzing a Packet Capture File

- ✓ PacketTotal supports both pcap and pcapng file-types
- ✓ You can upload from any page on the site
- ✓ Once uploaded your PCAP will be queued for analysis
- ✓ Time to analyze varies



Console View

Submitter: Anonymous

Name: dB34f75V4W3DjBF0IL7M.pcap

MD5: 6f4a5f6d7b3c4af88577fa79f8aa105d

Size: 5.494046 MB

Submitted: Tue Feb 13 2018 16:17:11 GMT-0500

Download

Malicious Activity

Connections

DNS

HTTP

Kerberos

SSL Certificates

PKI (X.509)

Transferred Files

Strange Activity

Community Tags

Similar Packet Captures

Search in results

Timestamp	Alert Description	Alert Signature	Severity	Sender IP	Sender Port	Target IP	Target Port	Transport Protocol
2018-02-13 05:08:28 Z	A Network Trojan was detected	ET TROJAN Backdoor.Win32.DarkComet Screenshot Upload Successful	1	10.25.1.205	49213	195.84.151.37	2200	TCP
2018-02-13 05:08:38 Z	A Network Trojan was detected	ET TROJAN Backdoor.Win32.DarkComet Screenshot Upload Successful	1	10.25.1.205	49213	195.84.151.37	2200	TCP
2018-02-13 05:08:49 Z	A Network Trojan was detected	ET TROJAN Backdoor.Win32.DarkComet Screenshot Upload Successful	1	10.25.1.205	49213	195.84.151.37	2200	TCP
2018-02-13 05:09:00 Z	A Network Trojan was detected	ET TROJAN Backdoor.Win32.DarkComet Screenshot Upload Successful	1	10.25.1.205	49213	195.84.151.37	2200	TCP
2018-02-13 05:09:08 Z	A Network Trojan was detected	ET TROJAN Backdoor.Win32.DarkComet Screenshot Upload Successful	1	10.25.1.205	49213	195.84.151.37	2200	TCP
2018-02-13 05:09:19 Z	A Network Trojan was detected	ET TROJAN Backdoor.Win32.DarkComet Screenshot Upload Successful	1	10.25.1.205	49213	195.84.151.37	2200	TCP
2018-02-13 05:09:28 Z	A Network Trojan was detected	ET TROJAN Backdoor.Win32.DarkComet Screenshot Upload Successful	1	10.25.1.205	49213	195.84.151.37	2200	TCP
2018-02-13 05:09:38 Z	A Network Trojan was detected	ET TROJAN Backdoor.Win32.DarkComet Screenshot Upload Successful	1	10.25.1.205	49213	195.84.151.37	2200	TCP
2018-02-13 05:09:48 Z	A Network Trojan was detected	ET TROJAN Backdoor.Win32.DarkComet Screenshot Upload Successful	1	10.25.1.205	49213	195.84.151.37	2200	TCP
2018-02-13 05:09:59 Z	A Network Trojan was detected	ET TROJAN Backdoor.Win32.DarkComet Screenshot Upload Successful	1	10.25.1.205	49213	195.84.151.37	2200	TCP

Locating Captures via Search

- ✓ Navigate to packettotal.com/app/search/ to get started
- ✓ Supported Query Types:
 - Free Text
 - Field/Value
 - Boolean



Free Text Queries

IP Addresses



8.8.8.8

URLs



https://evilsite.com/must/match/exactly

Domain Wildcards



evilsite.com

Field/Value Queries

IP Fields



id_orig_h: 192.168.0.5

Metadata Fields



tunnel_type: teredo

Protocol Fields



http_http_method: GET

Boolean Queries

OR



`_type: signature_alerts OR _type: intel`

AND



`Zeus AND GameOver`

Grouping



`dreambox OR smcadmin OR xc3511 OR (_type:intel OR _type: signature_alerts AND mirai)`

Malware Repository

- ✓ Maintained by Dynamite
- ✓ Locate common strains of malware
- ✓ Search related network indicators

packettotal.com/malware-archive.html

The screenshot displays a web interface for a malware repository. On the left, a dark sidebar titled 'Malware Categories' lists various types of malware: Botnets, Campaigns, Cryptojacking, Exploit Kits, Exploits, Ransomware, Trojans, and Worms. The 'Botnets' category is currently selected. The main content area on the right is titled 'Gameover ZeusS'. It includes a 'First Seen' date of 2012, a detailed description of the malware as a successor to the Zeus botnet, and a list of related Intel indicators. These indicators include entries from FBI and BlackHat, each with a unique hash and a 'View in search' button. The interface is clean and professional, with a focus on providing detailed information about the malware.

Locating Captures via Similar Search

- ✓ Can be thought of as a "reverse image search"
- ✓ "similar" pcaps have indicators in common
 - domain name, an IP, a file
- ✓ Go to "Similar PCAPs" tab

Similar Packet Captures

Analysis Completed	Matched Terms	Match Strength
2017-03-13T18:11:28.000Z	1d5dd76f52c11d3ebf9036a5a8bec2... 134.170.58.221 185.28.222.11 216.58.199.74 202.7.177.24 ⌵	56
2017-09-27T15:21:41.000Z	216.58.199.67 216.58.199.68 216.58.199.78 31.13.79.220 178f7e93a74ed73d88c29042220b9a...	5
2017-08-08T00:44:27.000Z	http://www.bing.com/ 40.74.117.114 /HPIImageArchive.aspx?format,id... 204.79.197.200 178f7e93a74ed73d88c29042220b9a...	5

Yes, There is an API!

- ✓ Search API is available to beta testers
- ✓ Automation with programmatic search
- ✓ Many other API-only features
- ✓ Request an API key at packettotal.com/api.html

Analyze Packet Captures
Programmatically upload and analyze .pcap/.pcapng files. View the results on PacketTotal.com, or explore through the API.
*6MB Upload Max

```
{  
  'id': '10fc81d13d6914b599f4299ab1dc51f4',  
  'queue': 'https://packettotal.com/app/queue?id=10fc81d13d6914b599f4299ab1dc51f4'  
}
```

Search by Indicators
Find packet captures containing any domain name, IP address, **malware strain**, protocol used (SSH, SMTP, etc.), and more.

Understand the Results in Context
Retrieve analysis of any pcap on PacketTotal, including malicious signatures, top-talkers, and connection stats.

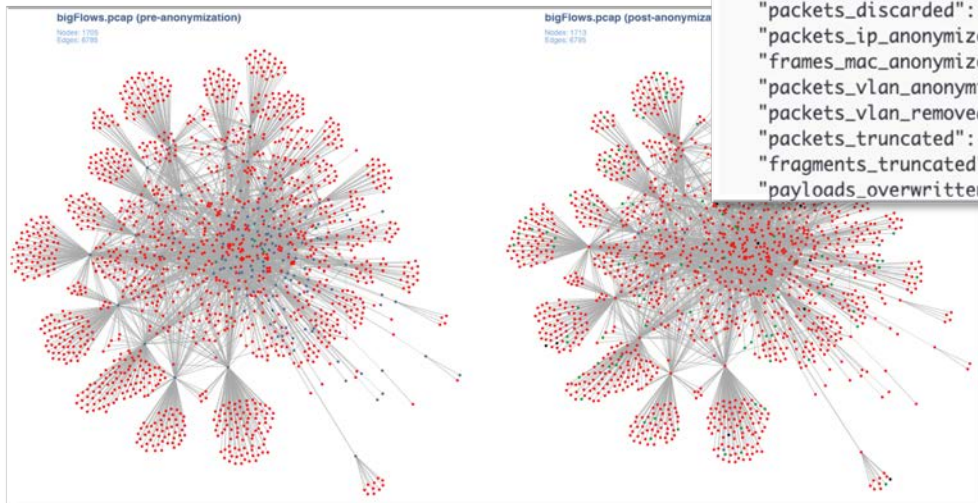
Download the Full Analysis
Download the packet capture, and any analysis files, including transferred files, signatures fired, logs generated, and external references.

APPENDIX

PCAP Anonymizer

- ✿ Highly Customizable via CLI or Options File
- ✿ Anonymize IP and MAC addresses
- ✿ Anonymize ARP, ICMP, VLAN

```
adam@mbp2 cmd % ./anonymizer -source ~/pcaps/bigFlows.pcap -ip full -mac full -store-mappings -graph {  
  "source_file": "bigFlows.pcap",  
  "output_file": "/tmp/bigFlows.pcap-anonymized",  
  "graph_file": "/tmp/bigFlows.pcap-anonymized-graph.html",  
  "ip_mapping_file": "/tmp/bigFlows.pcap-anonymized.ips",  
  "mac_mapping_file": "/tmp/bigFlows.pcap-anonymized.macs",  
  "packets_read": 791615,  
  "packets_analyzed": 791615,  
  "packets_written": 791581,  
  "packets_discarded": 0,  
  "packets_ip_anonymized": 787315,  
  "frames_mac_anonymized": 787315,  
  "packets_vlan_anonymized": 0,  
  "packets_vlan_removed": 0,  
  "packets_truncated": 0,  
  "fragments_truncated": 0,  
  "payloads_overwritten": 0,  
}
```



- ✿ Truncate and mask payloads
- ✿ Generate interactive graphs for visual analysis
- ✿ Packet filtering, CIDR support and more

Dynamite Agent

The screenshot displays the Dynamite Agent web interface. On the left is a dark sidebar with a user profile 'adam' and a menu including 'Local Agent Manager', 'Plugin Info', 'Network Interfaces', 'Network Environment', 'Rules & Scripts', 'Connectors', 'Processes', 'Advanced Configuration', and 'Documentation'. The main area has a top navigation bar with 'Home', 'API', 'Users', and 'Plugins'. Below this is a sub-header 'Local Agent Manager' with a dropdown. The main content area is titled 'Zeek Scripts' and 'Suricata Rules', with tabs for 'CONNECTIONS', 'DHCP', 'DNS', 'FTP', 'HTTP', 'KERBEROS', 'MODBUS', 'MYSQL', 'RDP', 'SMB', 'SMTP', 'SSH', 'FILES', 'SSL', 'X509', 'VALIDATIONS', 'DETECTIONS', 'NOTICES', and 'LOGGING'. The 'HTTP' tab is selected, showing a grid of detection rules. Each rule card includes a title (e.g., 'Detect Software', 'Extract URI Variables'), a status (e.g., 'enabled'), a protocol (e.g., 'http'), and a brief description. A callout box 'Intuitive Web UI and API' points to the top navigation. Another callout 'Built on Zeek and Suricata' points to the rule cards. A third callout 'Eliminates Complexity' points to the sidebar. A fourth callout 'Best in Class Network Visibility' points to the bottom right of the rule grid.

Intuitive Web UI and API

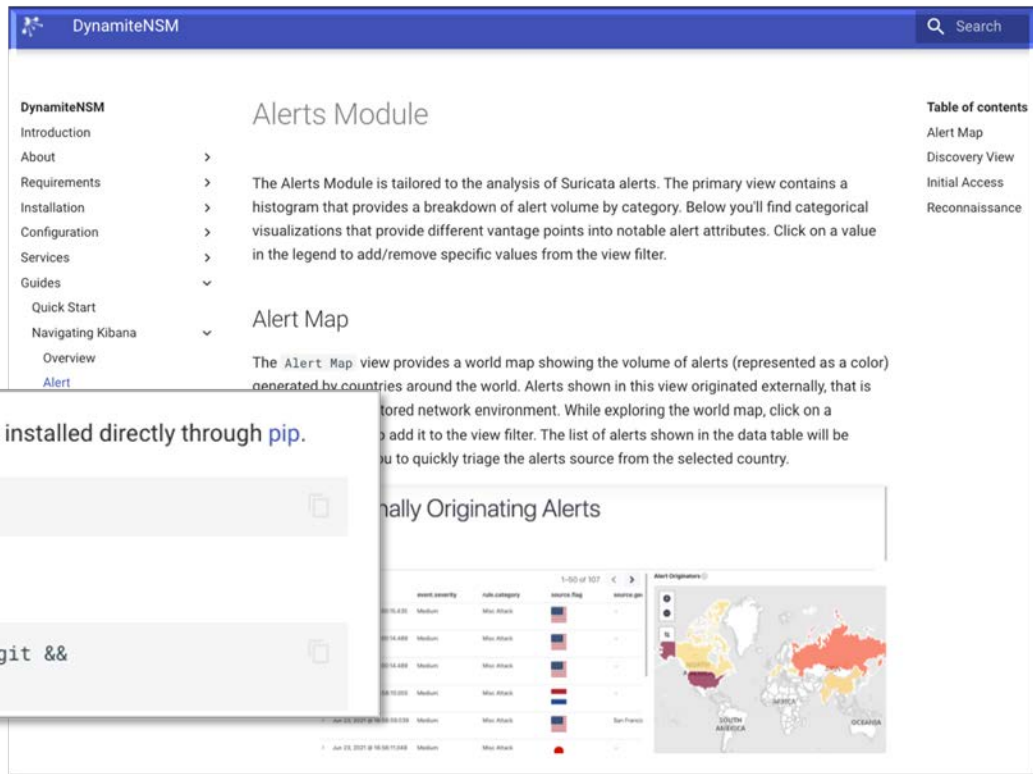
Built on Zeek and Suricata

Eliminates Complexity

Best in Class Network Visibility

DynamiteNSM

- ✿ Open-source Network Security Monitor
- ✿ Full Network Monitoring Stack + SDK
- ✿ Simple Zeek and Suricata Management
- ✿ Full Data Ingest Pipeline
- ✿ Many Analysis and Hunting Dashboards

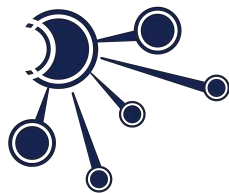


dynamite-nsm is a [Python3.7+](#) compatible package that can be installed directly through [pip](#).

```
sudo pip install dynamite-nsm
```

Alternatively, developers may also wish to build from source.

```
git clone https://github.com/DynamiteAI/dynamite-nsm.git &&  
sudo pip install dynamite-nsm/
```



DYNAMITE
A N A L Y T I C S

Thank You!

Jamin Becker

info@dynamite.ai

dynamite.ai

github.com/DynamiteAI

Check out Free Dynamite Agent Starter on AWS Marketplace

"Any opinions, findings, conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Networking and Information Technology Research and Development Program."

The Networking and Information Technology Research and Development
(NITRD) Program

Mailing Address: NCO/NITRD, 2415 Eisenhower Avenue, Alexandria, VA 22314

Physical Address: 490 L'Enfant Plaza SW, Suite 8001, Washington, DC 20024, USA Tel: 202-459-9674,
Fax: 202-459-9673, Email: nco@nitrd.gov, Website: <https://www.nitrd.gov>

