



Application of open-source firewall and intrusion detection and prevention systems in Taiwan Academic Network

Ming-Chang Cheng (鄭明彰)

Nantou County Education Network Center (南投縣教育網路中心)

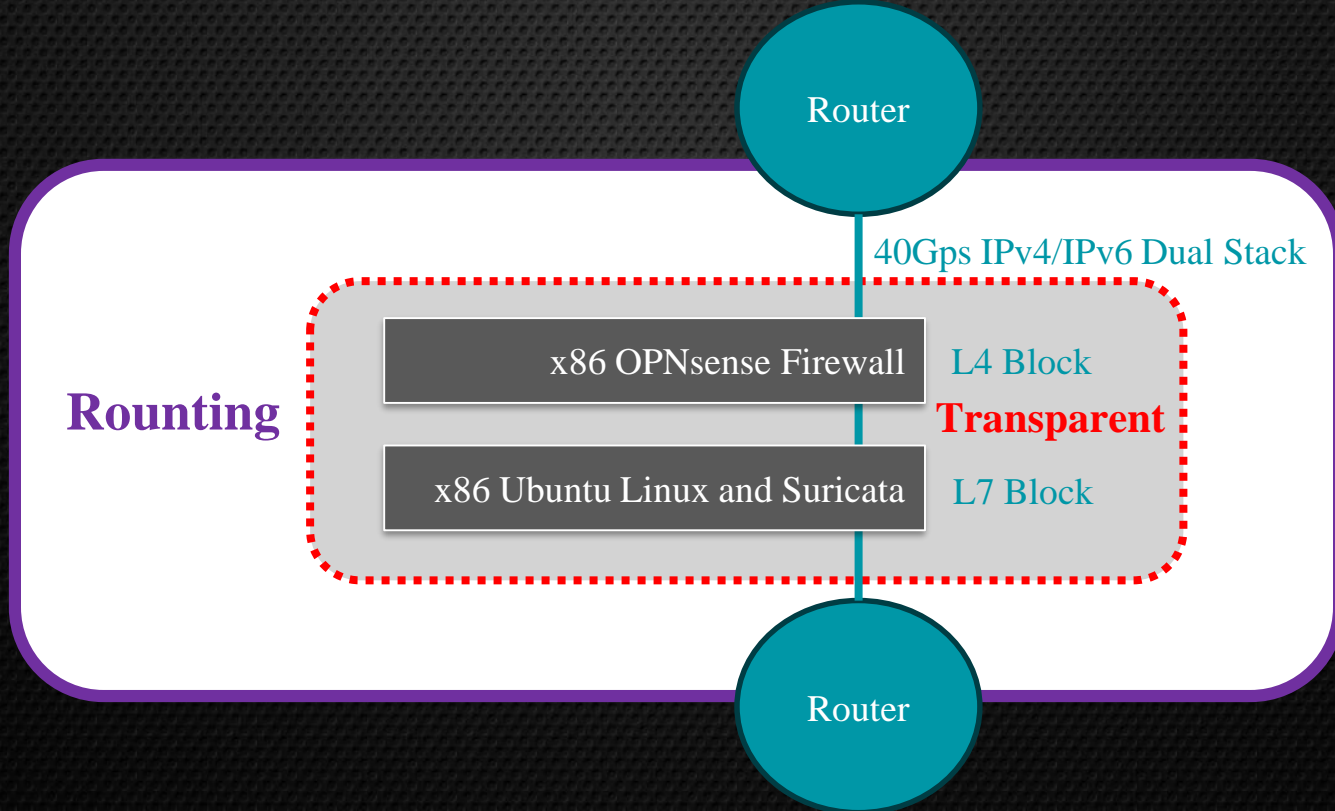


南投縣教育網路中心

Nantou County Education Network Center - TANet

AS number	1659 (TANet)
Traffic profile	Nantou Network Regional Center IPv4 and IPv6 dual stack 10Gx4
Traffic Volume	TANet: 40 Gbps https://www.ntrc.edu.tw/cacti/NTCT.html
Peering Policy	Restrictive
Peering Locations	Taiwan: Nantou County Education Network Center - TANet
Message	High performance and Cost-effectiveness open-source network security solution
Contact	everfree@ntct.edu.tw

Network Architecture

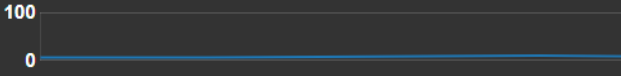


About OPNsense

- Open Source
- Easy-to-use (Web-GUI)
- FreeBSD based firewall
- Most of the features
- Zarmor plugin (NGFW)
- Offers weekly security.
- 2 major releases each year

Versions: OPNsense 24.1.5_3-amd64)

Versions: OPNsense 23.7.6-amd64)

System Information	
Name	
Versions	OPNsense 24.1.5_3-amd64 FreeBSD 13.2-RELEASE-p11 OpenSSL 3.0.13
Updates	Click to check for updates.
CPU type	Intel(R) Xeon(R) CPU E5-2699 v4 @ 2.20GHz (44 cores, 44 threads)
CPU usage	100 
Load average	4.97, 4.36, 4.40
Uptime	4 days 15:40:31
Current date/time	Wed Apr 10 9:32:17 CST 2024
Last config change	Mon Apr 1 11:21:33 CST 2024

IP and Blocklist

- pfSense (pfBlockerNG), OPNsense Forum, X(twitter), Reddit, Google, Blog
- Source data must be regularly verified for periodic updates
- Use IP and DNS Blocklist on OPNsense (L4)
- Inbound or Outbound
- Based on practical application experience, it is known that those lists are less false positives

- <https://threatview.io/> Website
- <https://cinsscore.com/list/ci-badguys.txt> IP
- <https://urlhaus.abuse.ch/downloads/hostfile/> DNS

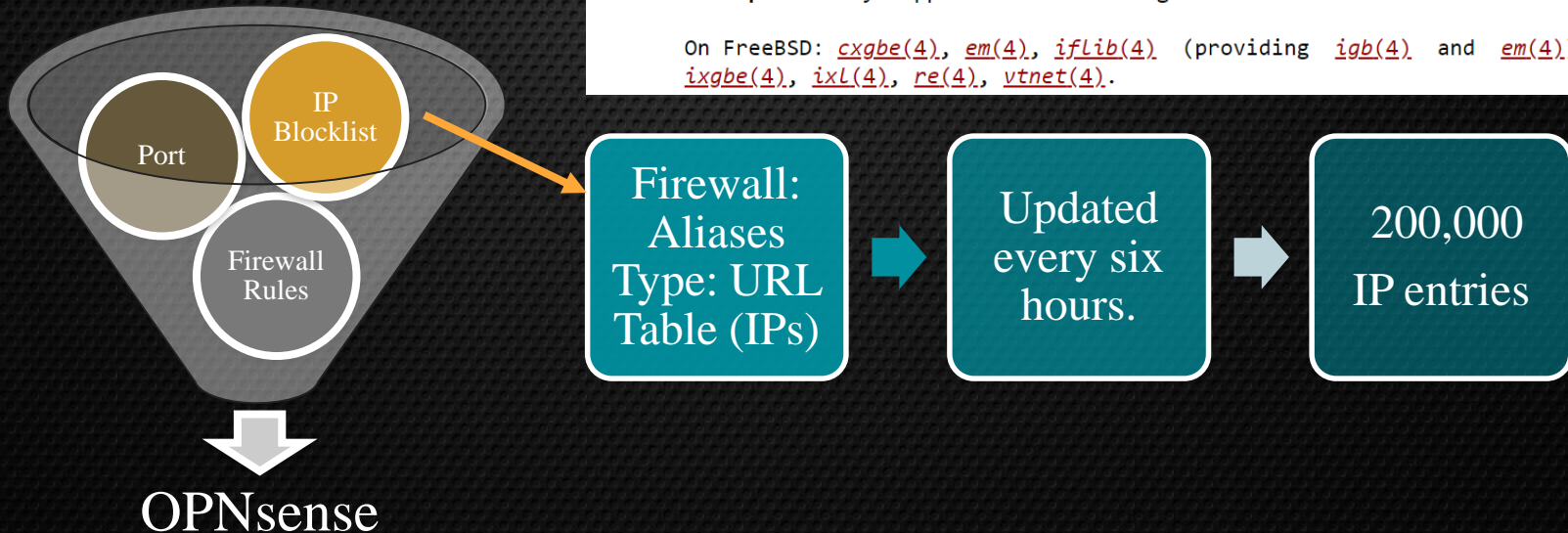
OPNSense is deployed in the backbone network

- Hardware: HP DL380 Gen9 44Core + 96G RAM + **Chelsio SmartNICs**
- Best compatibility with high performance on FreeBSD system
- <https://www.chelsio.com/>

SUPPORTED DEVICES

netmap natively supports the following devices:

On FreeBSD: [cxgbe\(4\)](#), [em\(4\)](#), [iflib\(4\)](#) (providing [igb\(4\)](#) and [em\(4\)](#)), [ixgbe\(4\)](#), [ixl\(4\)](#), [re\(4\)](#), [vtnet\(4\)](#).



Zenarmor

- Zenarmor is a plugin for the OPNsense firewall which provides state-of-the-art next-generation features. Zenarmor is developed by Sunny Valley Cyber Security Inc.

Configuration	Security	App Controls	Web Controls	Exclusions
Essential Security				
Category name	Status			
DNS over HTTPS	Allowed <input type="checkbox"/>			
Malware/Virus	Blocked <input checked="" type="checkbox"/>			
Phishing	Blocked <input checked="" type="checkbox"/>			
Hacking	Allowed <input type="checkbox"/>			
Spam sites	Blocked <input checked="" type="checkbox"/>			
Potentially Dangerous	Blocked <input checked="" type="checkbox"/>			
Parked Domains	Allowed <input type="checkbox"/>			
Firstly Seen Sites	Allowed <input type="checkbox"/>			

Recent Malware/Phishing/Virus Outbreaks	Blocked <input checked="" type="checkbox"/>
Botnet C&C NEW	Blocked <input checked="" type="checkbox"/>
Botnet DGA Domains NEW	Blocked <input checked="" type="checkbox"/>
DNS Tunneling NEW	Blocked <input checked="" type="checkbox"/>
Compromised Website	Blocked <input checked="" type="checkbox"/>
Spyware and Adware	Blocked <input checked="" type="checkbox"/>
Keyloggers and Monitoring	Allowed <input type="checkbox"/>
Proxy	Allowed <input type="checkbox"/>
Dead Sites	Allowed <input type="checkbox"/>
Dynamic DNS Sites	Allowed <input type="checkbox"/>
Newly Registered Sites	Allowed <input type="checkbox"/>
Newly Recovered Sites	Allowed <input type="checkbox"/>
Malformed DNS Packet NEW	Blocked <input checked="" type="checkbox"/>

Suricata

- Suricata is a high performance, open source network analysis and threat detection software used by most private and public organizations, and embedded by major vendors to protect their assets.

Suricata is far more than an IDS/IPS

 IDS Alerts

 Protocol Transactions

 Network Flows

 PCAP Recordings

 Extracted Files

Source: Stamus Networks



```

0[|17.8%] 6[|147.0%] 12[|12.8%] 18[|20.0%] 22[|9.6%] 28[|14.9%] 34[|15.8%] 40[|34.0%]
1[|9.0%] 7[|14.0%] 13[|6.7%] 19[|28.0%] 23[|18.2%] 29[|100.0%] 35[|13.4%] 41[|16.9%]
2[|30.4%] 8[|6.7%] 14[|9.5%] 20[|49.3%] 24[|15.1%] 30[|12.4%] 36[|36.7%] 42[|16.4%]
3[|14.8%] 9[|14.2%] 15[|7.3%] 21[|20.9%] 25[|21.2%] 31[|10.0%] 37[|11.6%] 43[|20.7%]
4[|35.1%] 10[|7.6%] 16[|14.3%]
5[|24.2%] 11[|12.2%] 17[|15.7%]

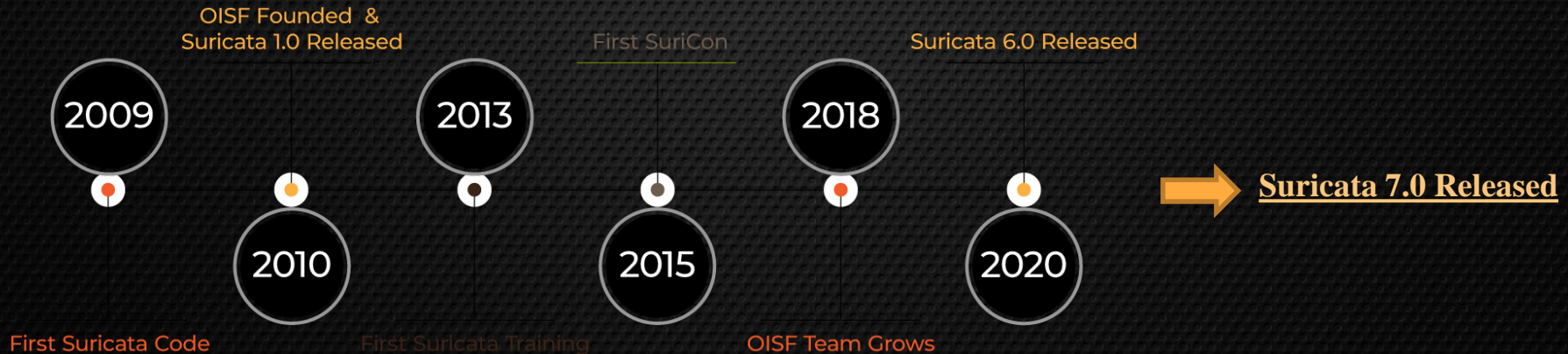
Mem[|||||] 7.56G/126G Tasks: 34, 261 thr: 14 running
Swp[|||||] 0K/8.00G Load average: 8.73 8.29 8.07
Uptime: 142 days (1), 00:15:25

PID USER PRI NI VIRT RES SHR S CPU% MEM% TIME+ Command
77792 root 20 0 8714M 5160M 13356 S 836. 4.0 504h /usr/bin/suricata -v -c /etc/suricata/suricata.yaml --napatec
10744 root 20 0 2415M 364M 40800 S 107. 0.3 231h /opt/napatech3/bin/ntservice -d -f /opt/napatech3/config/ntse
10771 root 20 0 2415M 364M 40800 R 100. 0.3 218h /opt/napatech3/bin/ntservice -d -f /opt/napatech3/config/ntse
78021 root 18 -2 8714M 5160M 13356 R 67.9 4.0 13h17:12 /usr/bin/suricata -v -c /etc/suricata/suricata.yaml --napatec
78030 root 18 -2 8714M 5160M 13356 R 54.5 4.0 13h24:33 /usr/bin/suricata -v -c /etc/suricata/suricata.yaml --napatec
78034 root 18 -2 8714M 5160M 13356 S 42.4 4.0 13h50:16 /usr/bin/suricata -v -c /etc/suricata/suricata.yaml --napatec
78011 root 18 -2 8714M 5160M 13356 S 41.0 4.0 12h55:11 /usr/bin/suricata -v -c /etc/suricata/suricata.yaml --napatec
78016 root 18 -2 8714M 5160M 13356 S 35.6 4.0 13h24:46 /usr/bin/suricata -v -c /etc/suricata/suricata.yaml --napatec
78037 root 18 -2 8714M 5160M 13356 R 32.3 4.0 13h08:08 /usr/bin/suricata -v -c /etc/suricata/suricata.yaml --napatec
78047 root 18 -2 8714M 5160M 13356 R 32.3 4.0 13h48:44 /usr/bin/suricata -v -c /etc/suricata/suricata.yaml --napatec
78026 root 18 -2 8714M 5160M 13356 S 29.6 4.0 13h37:35 /usr/bin/suricata -v -c /etc/suricata/suricata.yaml --napatec
78013 root 18 -2 8714M 5160M 13356 R 27.6 4.0 13h14:45 /usr/bin/suricata -v -c /etc/suricata/suricata.yaml --napatec
78028 root 18 -2 8714M 5160M 13356 S 26.9 4.0 13h26:59 /usr/bin/suricata -v -c /etc/suricata/suricata.yaml --napatec
78019 root 18 -2 8714M 5160M 13356 S 24.9 4.0 13h14:41 /usr/bin/suricata -v -c /etc/suricata/suricata.yaml --napatec
78042 root 18 -2 8714M 5160M 13356 S 24.2 4.0 13h42:26 /usr/bin/suricata -v -c /etc/suricata/suricata.yaml --napatec
78041 root 18 -2 8714M 5160M 13356 R 22.2 4.0 13h02:39 /usr/bin/suricata -v -c /etc/suricata/suricata.yaml --napatec
78039 root 18 -2 8714M 5160M 13356 S 21.5 4.0 15h10:56 /usr/bin/suricata -v -c /etc/suricata/suricata.yaml --napatec
78027 root 18 -2 8714M 5160M 13356 S 20.2 4.0 13h08:16 /usr/bin/suricata -v -c /etc/suricata/suricata.yaml --napatec
78031 root 18 -2 8714M 5160M 13356 S 20.2 4.0 13h13:24 /usr/bin/suricata -v -c /etc/suricata/suricata.yaml --napatec
78024 root 18 -2 8714M 5160M 13356 R 18.8 4.0 13h26:18 /usr/bin/suricata -v -c /etc/suricata/suricata.yaml --napatec
78029 root 18 -2 8714M 5160M 13356 S 18.2 4.0 14h24:33 /usr/bin/suricata -v -c /etc/suricata/suricata.yaml --napatec
78017 root 18 -2 8714M 5160M 13356 S 17.5 4.0 14h24:00 /usr/bin/suricata -v -c /etc/suricata/suricata.yaml --napatec
78049 root 18 -2 8714M 5160M 13356 S 17.5 4.0 13h30:38 /usr/bin/suricata -v -c /etc/suricata/suricata.yaml --napatec

```

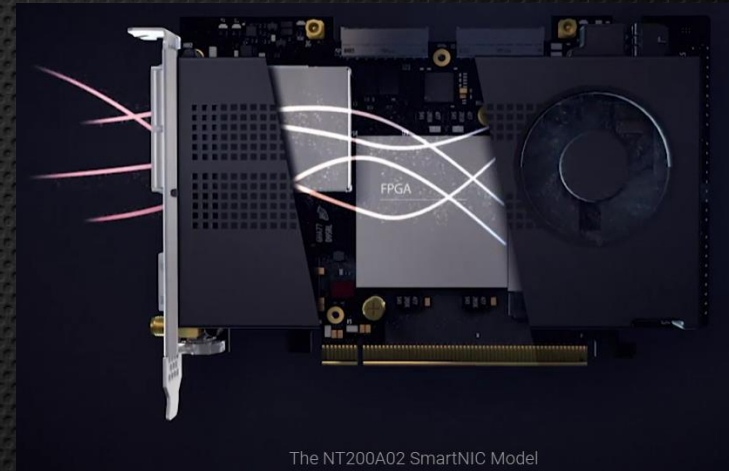

The Open Information Security Foundation

- The Open Information Security Foundation is a 501(c)3 nonprofit organization created to build community and to support open source security technologies like Suricata, the world-class IDS/IPS network monitoring engine.



Suricata is deployed in the backbone network

- Hardware: HP DL380 Gen10 44Core + 96G RAM + NT200A02 FPGA-based SmartNICs
- FPGA (Field Programmable Gate Array)
- Reduces host CPU utilization and solution latency by offloading complex flow classification and packet processing to the SmartNIC.
- Performance Tuning and Optimization
- Supports full-duplex $2 \times 100\text{G}$ packet transfer between network ports



Wireshark



Suricata



n2disk



Snort



Zeek



TReX

Ruleset Signature and trigger alert

suricata[77792]: [**wDrop**] [1:2832617:3] ETPRO MALWARE W32.Bloat-A Checkin
[Classification: **Malware Command and Control Activity Detected**] [**Priority: 1**] {TCP}
163.22.70.254:2026 -> 69.42.215.252:80

suricata[70864]: [1:2017548:7] ET MALWARE Backdoor family PC RAT/Gh0st CnC
traffic (OUTBOUND) 3 [Classification: **Malware Command and Control Activity**
Detected] [**Priority: 1**] {TCP} **192.168.12.1:64946 -> 54.251.88.72:12100**

Proofpoint ET Open and PRO ruleset

The difference between ETPro and ETOpen is based upon the source of the rules. If a rule is contributed from the community it goes into ETOpen. If it is written by Proofpoint based on public research, it will go into ETOpen. If it is based on Proofpoint intellectual property and processes and written by Proofpoint it will go into ETPro. Each day there is a ratio of between 5-10:1 ETPro to ETOpen signatures.

- All major malware families covered by command and control channels and protocols.
- Detection across all network-based threat vectors—from SCADA protocols and web servers to the latest client-side attacks served up by exploit kits.
- The most accurate signatures in the industry for malware callback, dropper, command and control, obfuscation, exploit-kit related threats and exfiltration.
- A comprehensive rule set that also includes regularly prescribed CVE updates, including Microsoft Active Protection Program(MAPP) and Patch Tuesday updates.
- Detects distributed denial-of-service attacks (DDoS)



CVE-2024-3400

- PAN-OS: OS Command Injection Vulnerability in GlobalProtect
- CVSS score of 10

Ruleset Update Summary - 2024/04/12 - v10574

Added rules:

Open:

2052024 - ET MALWARE Possible UPSTYLE Command Output Retrieval Attempt (malware.rules)

2052025 - ET MALWARE Possible UPSTYLE Payload Retrieval Attempt (malware.rules)

2052026 - ET MALWARE Possible UPSTYLE Command Attempt (malware.rules)

Ruleset Update Summary - 2024/04/16 - v10576

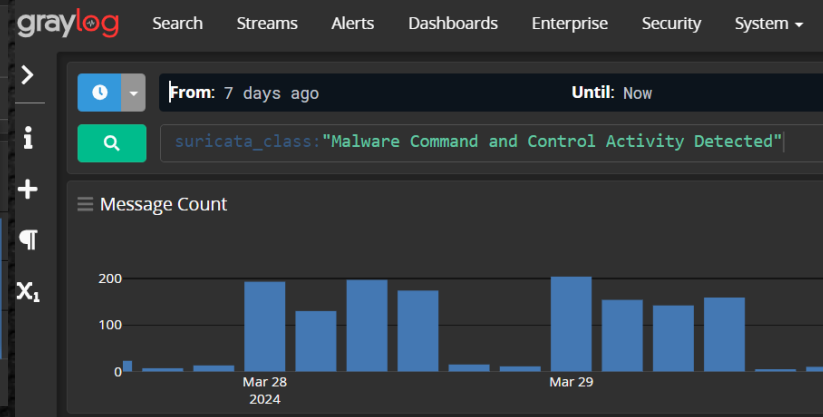
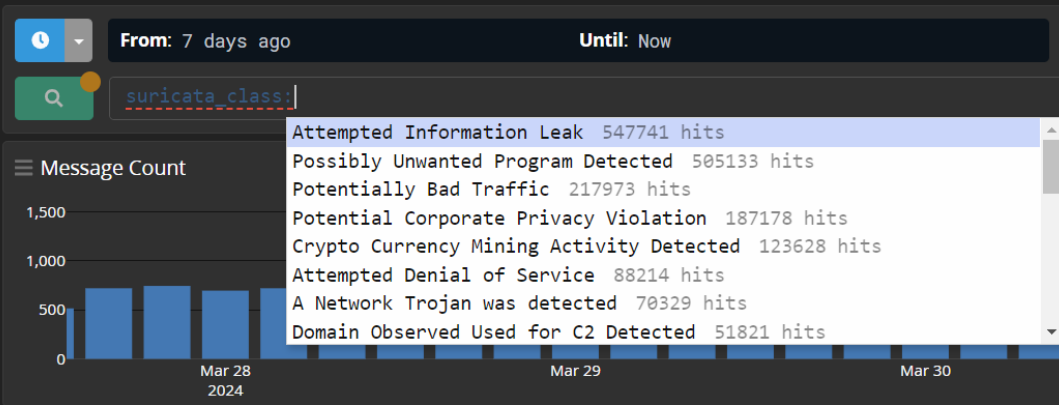
2052122 - ET WEB_SPECIFIC_APPS Palo Alto GlobalProtect Session Cookie Command Injection Attempt (CVE-2024-3400) (web_specific_apps.rules)

Botnet TOP14 Alerts (Schools at NTCT)

1. ETPRO MALWARE W32.Bloat-A Checkin
2. ET MALWARE NuggetPhantom Module Download Request
3. ETPRO MALWARE Linopid HTTP CnC Beacon
4. ET MALWARE Zeus POST Request to CnC - URL agnostic
5. ET MALWARE Possible NanoCore C2 60B
6. ET MALWARE Possible Netwire RAT Client HeartBeat C2
7. ETPRO MALWARE Win32/Bayrob Checkin
8. ET MALWARE Pushdo v3 Checkin
9. ETPRO MALWARE Nanocore Checkin Pattern
10. ETPRO MALWARE PWS.Win32/Zbot.gen!AF CnC traffic
11. ET MALWARE Backdoor family PC RAT/Gh0st CnC traffic (OUTBOUND) 3
12. ET MALWARE APT 41 LOWKEY Backdoor - Ping Command Inbound
13. **ETPRO MOBILE_MALWARE Trojan-Spy.AndroidOS.Agent.rz Checkin**
14. ETPRO MOBILE_MALWARE Trojan.Android.Apptrack.flinok CnC Beacon

Graylog

- SIEM (Security Information and Event Management)
- IDPS syslog to Graylog
- Triggering alerts by ET Open or ET PRO ruleset
- The blocklist IPs are exported as a text file, with one IP address per line.



Conclude

- Open-source solutions
- Cost-effectiveness
- Maximizing security protection with limited cybersecurity budgets.
- High performance
- Adding Your Own Rules
- Multi pattern matching/fast pattern analysis
- Simple yet effective
- Future: Facing Cybersecurity Threats
- AI and ML (Machine Learning)

Reference

- <https://opnsense.org/>
- <https://www.zenarmor.com/>
- <https://oisf.net/>
- <https://suricata.io/>
- <https://docs.suricata.io/en/latest/capture-hardware/napatech.html>
- <https://www.napatech.com/>
- <https://rules.emergingthreats.net/>
- <https://www.proofpoint.com/us/threat-insight/et-pro-ruleset>
- <https://graylog.org/>
- https://twitter.com/ET_Labs
- [https://man.freebsd.org/cgi/man.cgi?netmap\(4\)](https://man.freebsd.org/cgi/man.cgi?netmap(4))