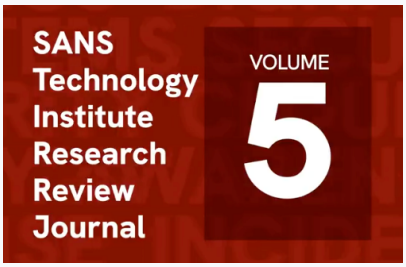


previous next

Click HERE to learn more about classes Johannes is teaching for SANS

Homepage
Diaries
Podcasts
Jobs
Data
Tools
Contact Us
About Us

Slack Channel
Mastodon
Bluesky
X

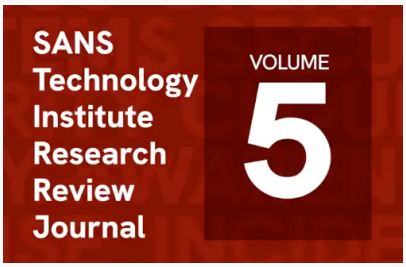
Linksys Worm "TheMoon" Summary: What we know so far

Published: 2014-02-13. **Last Updated**: 2014-02-13 18:37:18 UTC
by Johannes Ullrich (Version: 1)

20 comment(s)

I am writing this summary as the prior diaries about this topic became a bit difficult to parse.

At this point, we are aware of a worm that is spreading among various models of Linksys routers. We do not have a definite list of routers that are vulnerable, but the following routers may be vulnerable depending on firmware
version: E4200, E3200, E3000, E2500, E2100L, E2000, E1550, E1500, E1200, E1000,E900



Homepage
Diaries
Podcasts
Jobs
Data
Tools
Contact Us
About Us

Slack Channel
Mastodon
Bluesky
X

URL. This will return an XML formatted list of router features and firmware versions. The worm appears to extract the router hardware version and the firmware revision. The relevant lines are:

```
<ModelName>E2500</ModelName>
<FirmwareVersion>1.0.07 build 1</FirmwareVersion>
```

(this is a sample from an E2500 router running firmware version 1.0.07 build 1)

Next, the worm will send an exploit to a vulnerable CGI script running on these routers. The request does not require authentication. The worm sends random "admin" credentials but they are not checked by the script. Linksys (Belkin) is aware of this vulnerability.

This second request will launch a simple shell script, that will request the actual worm. The worm is about 2MB in size, samples that we captured so far appear pretty much identical but for a random trailer at the end of the binary. The file is an ELF MIPS binary.

Once this code runs, the infected router appears to scan for other victims. The worm includes a list of about 670 different networks (some /21, some /24). All appear to be linked to cable or DSL modem ISPs in various countries.

An infected router will also serve the binary at a random low port for new victims to download. This http server is only opened for a short period of time, and for each target, a new server with a different port is opened.

We do not know for sure if there is a command and control channel yet. But the worm appears

SANS Technology Institute Research Review Journal VOLUME 5

Homepage
Diaries
Podcasts
Jobs
Data
Tools
Contact Us
About Us

Slack Channel
Mastodon
Bluesky
X

HTML pages with images that look benign and more like a calling card. They include images based on the movie "The Moon" which we used as a name for the worm.

We call this a "worm" at this point, as all it appears to do is spread. This may be a "bot" if there is a functional command and control channel present.

Indicators of compromisse:

- heavy outbound scanning on port 80 and 8080.
- inbound connection attempts to misc ports < 1024.

Detecting potentially vulnerable system:

```
echo "GET /HNAP1/ HTTP/1.1\r\nHost: test\r\n\r\n" | nc
```

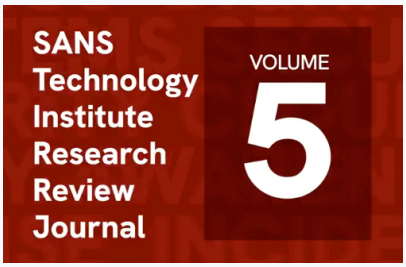
if you get the XML HNAP output back, then you MAY be vulnerable.

Johannes B. Ullrich, Ph.D.
SANS Technology Institute
Twitter

Keywords:

20 comment(s)

previous next



Homepage
Diaries
Podcasts
Jobs
Data
Tools
Contact Us
About Us

Slack Channel
Mastodon
Bluesky
X

Just to be clear, this is all happening on the outside interface of those routers?
With remote administration turned on or off?

That hadn't crossed my mind until reading this latest summary. (worm/spreading)

Anonymous
Feb 13th 2014
1 decade ago

This is happening on the outside interface with remote admin turned on.

Anonymous
Feb 13th 2014
1 decade ago

I am guessing this worm only attacks Linksys routers with original firmware and not open source firmware ie: DD-WRT?

Anonymous
Feb 13th 2014
1 decade ago

Correct: Only routers running stock firmware are vulnerable. OpenWRT is not vulnerable to this issue.

Anonymous
Feb 13th 2014
1 decade ago

Thanks for the clarification Dr J.

Also I assume if the remote admin port is changed that would also thwart the attack? (Unless they scanned you, figured out your new port, and then changed their code to check that port)

Anonymous
Feb 13th 2014
1 decade ago

The worm only scans port 80 and 8080 (http and https). Changing the port will prevent this attack. Restricting access to the admin interface by IP address will help as well.

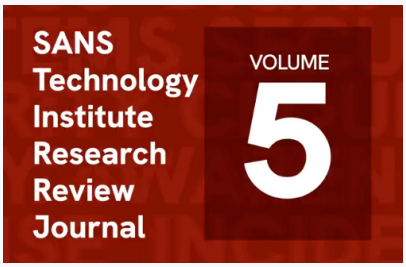
Anonymous
Feb 13th 2014
1 decade ago

Is there a list of the ~670 networks mentioned available? Or a copy of the binary for those of us who have not yet to encounter this in the wild?

Anonymous
Feb 13th 2014
1 decade ago

Can anyone share the 670 IP ranges or even the list of countries being targeted.
Also does anyone know if DNS values inside router are being modified.

Anonymous
Feb 14th 2014
1 decade ago



Homepage
Diaries
Podcasts
Jobs
Data
Tools
Contact Us
About Us

Slack Channel
Mastodon
Bluesky
X

https://isc.sans.edu/diaryimages/moonnets

It isn't clear if DNS values are being modified, but it is likely. Brett saw routers that used Google's DNS servers (8.8.8.8, 8.8.4.4.) instead of the once he pushed. But of course, the Google DNS servers wouldn't cause any problems (maybe better for the attacker then OpenDNS?)

There are some strings in the binary that may indicate that the DNS settings are changed:

@/etc/resolv.conf
nameserver
domain
search
options
timeout
attempts
/etc/hosts

Anonymous
Feb 14th 2014
1 decade ago

GOOD GRIEF!

I've been seeing an tidal wave of HNAP1 probes in the Apache logs since MAY of LAST YEAR!

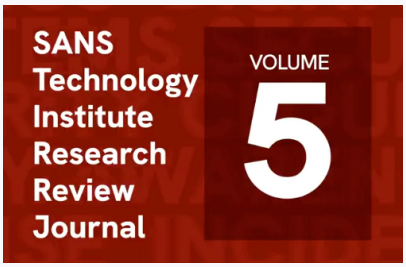
Was so bad that I wrote an ASA firewall rule to unceremoniously drop and discard the plague of annoying connection entries.

It took you guys a YEAR to figure out this was a worm? I guessed as much

I'm not impressed.

Anonymous
Feb 14th 2014
1 decade ago

Login here to join the discussion.



Homepage
Diaries
Podcasts

Top of page

Diary Archives

Tools
Contact Us
About Us

Slack Channel
Mastodon
Bluesky
X