



The bridge to possible

Dark networks, worlds...

...and communication

Łukasz Bromirski

Cisco Security Business Group

CONFidence 2021.09



This session agenda from 10k feet

- Defending internet transport
- Defending applications by inspecting traffic without decryption



Matthew Green  @matthew_d_gr... · 16h ...

But the field is called computer security; not computer optimism. We think about worst case outcomes because if we don't do that, our opponents absolutely will. 8/



I'm doing stuff with networks...

- ...since ~1993 (Zyxel, US Robotics and Motorola Codex!)
- CCIE #15929 (R&S/SP) & CCDE #2012::17
- Translated packet filtering HOWTOs, books, created Cisco FAQ PL, then BGP Blackholing PL and co-created PLNOG
- Doing L3, L4, and currently also firewalls, IPSes and all that «fluffy» stuff with malware using encryption and 5G
- Jump here and take a look (you can try breaking stuff, any feedback provided in friendly way is always welcomed):

<https://lukasz.bromirski.net/prezos/>



I was here in 2005, 2006, 2007, 2008 and 2010

**PROJEKT
BGP BLACKHOLING PL**




Łukasz Bromirski
lukasz@bromirski.net
bgp@networkers.pl

(secure)
**ROUTING WITH OSPF AND BGP
FOR FUN, FUN & FUN**



**HOW TO ATTACK, DEFEND AND
OWN NETWORK FOR FUN, FUN &
FUN**









Welcome to the new IP reality
Best practices that failed for YouTube


Łukasz Bromirski
Channel Systems Engineer, CCIE #15929
lbromirski@cisco.com



Łukasz Bromirski
lukasz@bromirski.net



Łukasz Bromirski
lbromirski@cisco.com



Confidence 5.1, Warsaw, XI.2009

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Confidential



**Wirtualizacja sieci –
izolacja ruchu w LAN
oraz sieciach MPLS**



Łukasz Bromirski
lbromirski@cisco.com



CONFidence, maj 2007
Kraków

© 2008 Cisco Systems, Inc. All rights reserved.



**The IPv6
(in)security**



Łukasz Bromirski
lbromirski@cisco.com



Confidence 2010.11, Prague, XI.2010

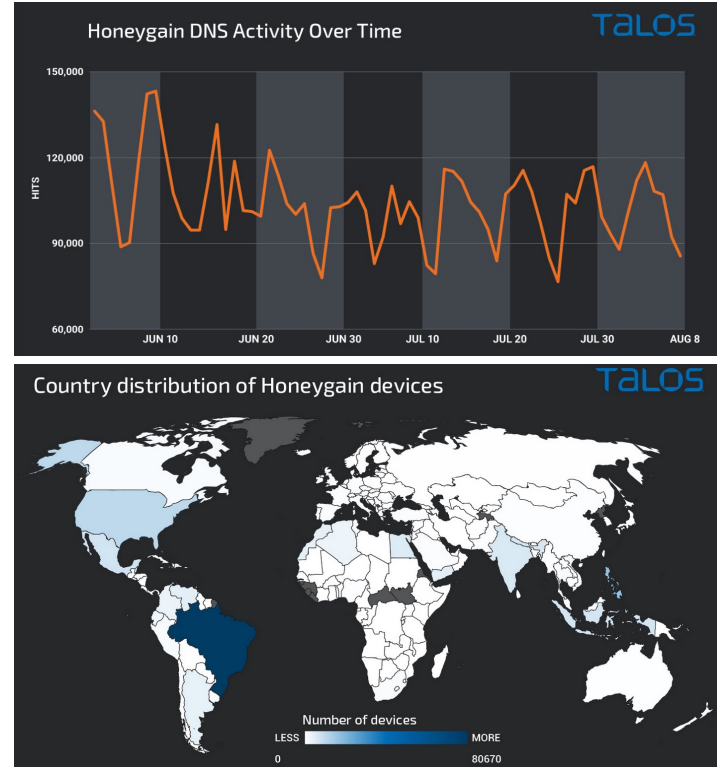
© 2010 Cisco and/or its affiliates. All rights reserved.

Security by obscurity works* until it doesn't

- World-wide honeypot averaged stats:
 - First SSH access to new VM on “used” IP address space – within 2-3 minutes
 - First SSH access on different port (998) on “used” IP address space – within 8-9 minutes
 - First SSH access to new VM on “unused” IP address space – within 5 minutes
 - First SSH access on different port (998) on “unused” IP address space – within 10 minutes
- Now, if your service has security vulnerability, and you play stupid games with ports... where is your god now?
 - Answer: 10 minutes away – maximum
- “Advanced” hint – masscan takes ~15 minutes to scan entire Polish IP assigned space at 50kpps for 2 TCP ports

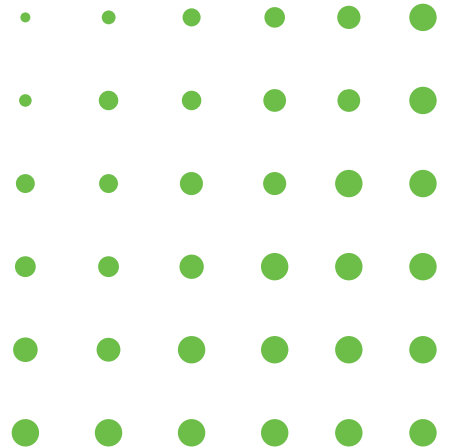
Everything is worth stealing or abusing...

- Ransomware is old news, but likely still best profitable revenue avenue for young and ambitious
- Stealing bandwidth is the next great thing
- So called “proxyware” is new trend, and new attack vector
 - just like with IPv6, now it's another thing to look for in your network telemetry: “do we have it?”
 - “allow list” model vs “block list” model

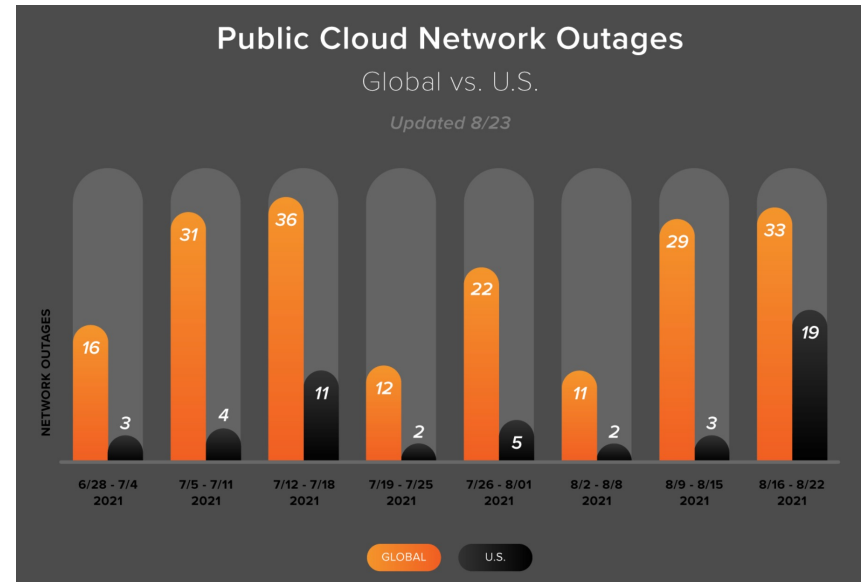
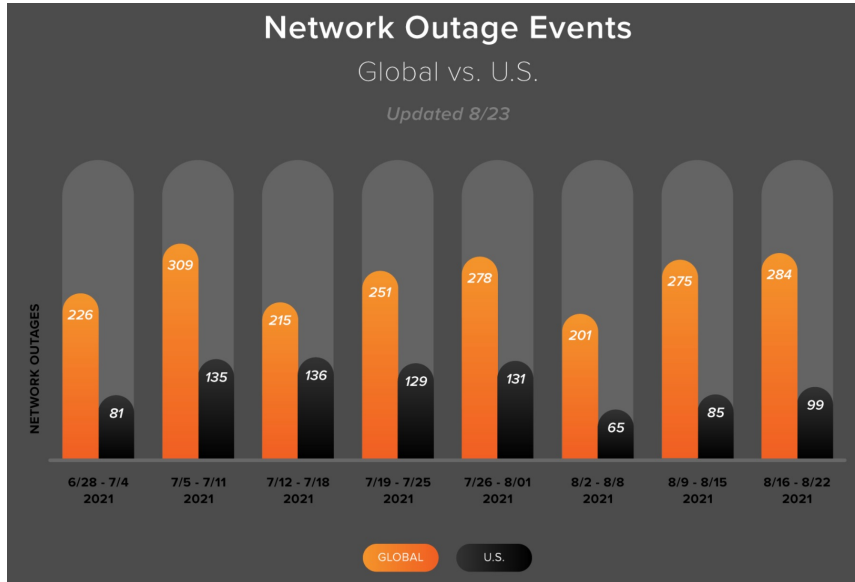


Source: <https://blog.talosintelligence.com/2021/08/proxyware-abuse.html>

Is it an outage or
attack?



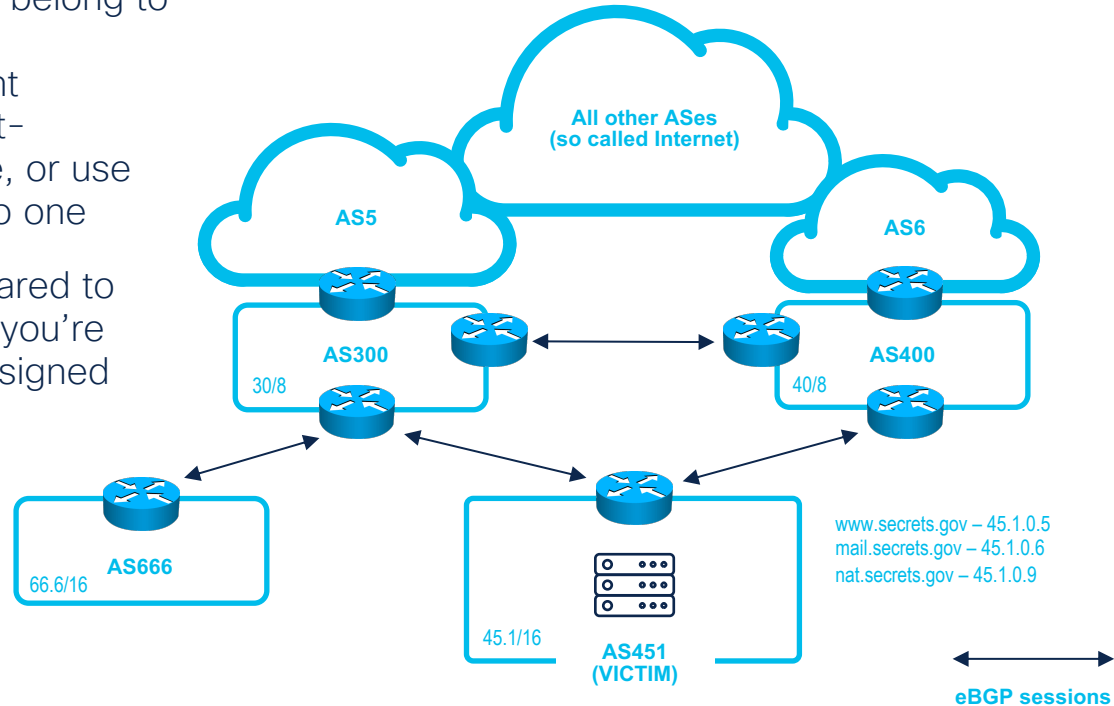
How you spot a problem?



Outages, outages all the way down...

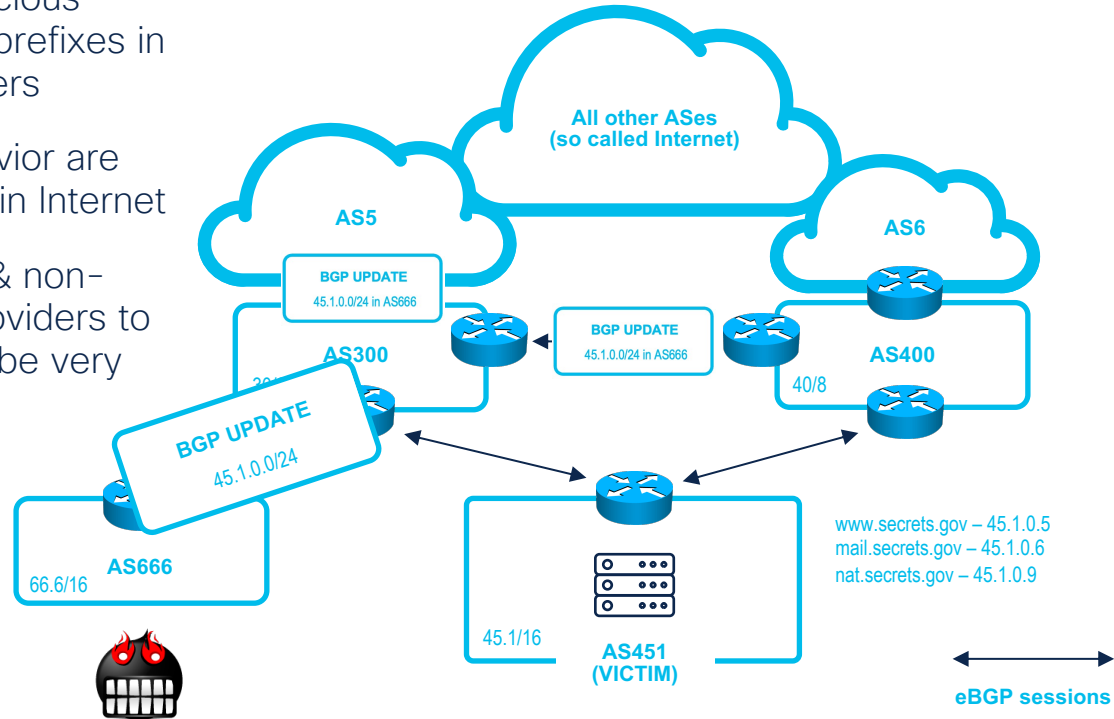
Internet is network of interconnected ASes

- BGP Autonomous Systems belong to companies, government organizations, cloud/content providers – anyone Internet-connected has to have one, or use address space belonging to one
- Up until recently, nobody cared to verify if the address space you're using is the one you got assigned



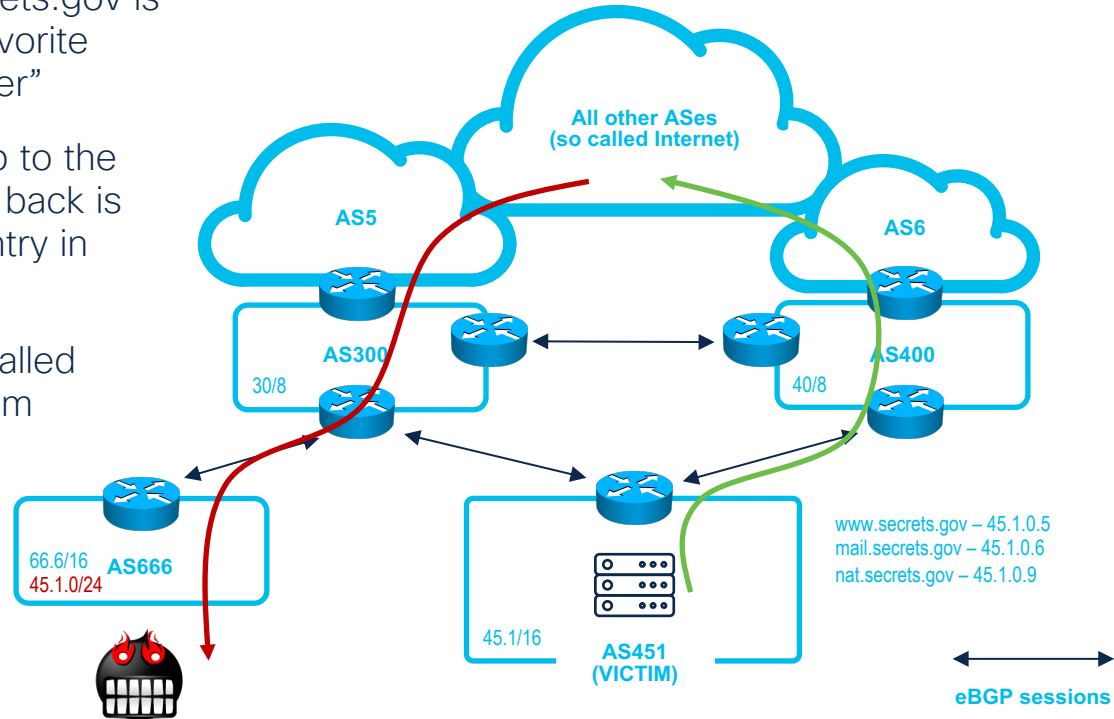
Internet is network of interconnected ASes

- This means, that if I'm malicious actor, I can advertise your prefixes in my BGP updates to my peers
- Filters for that kind of behavior are easy when you're end site in Internet
- They become challenging & non-trivial for transit Service Providers to the point where they can't be very tight



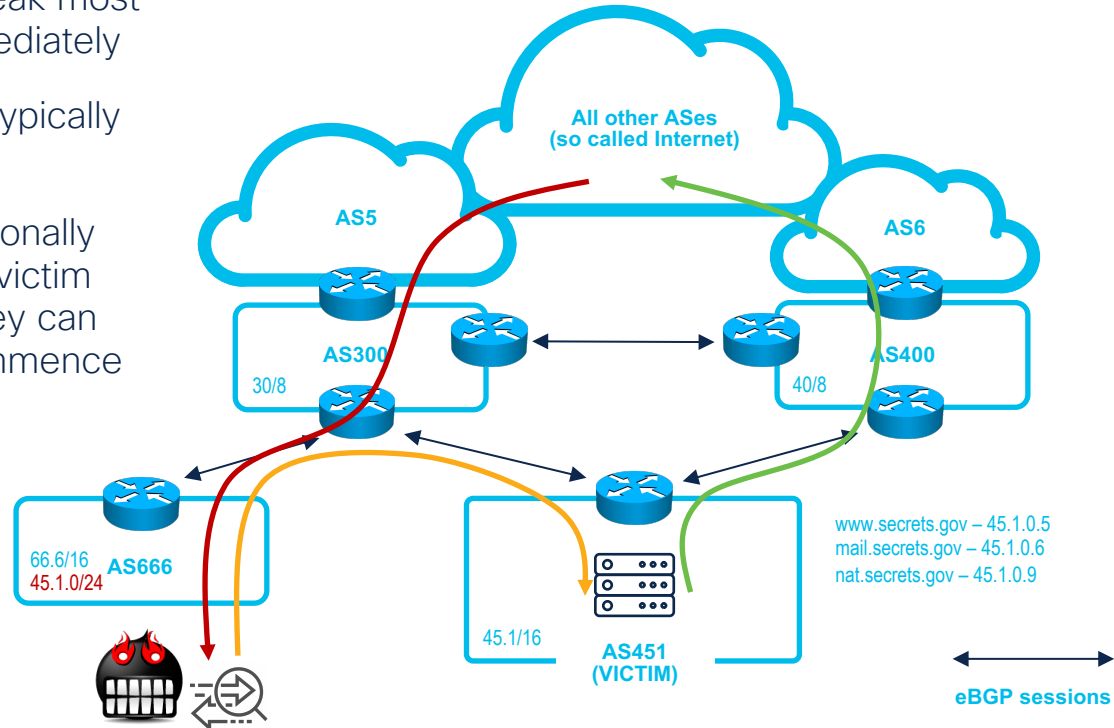
Internet is network of interconnected ASes

- Somebody behind nat.secrets.gov is initiating connection – to favorite social site or "secure partner"
- Traffic is routed hop by hop to the destination, but the routing back is based on most accurate entry in routing tables
- Malicious actor already installed better routing entry for victim network:
 - 45.1/16 -> VICTIM
 - 45.1.0/24 -> BAD ACTOR



Internet is network of interconnected ASes

- Typically, that setup will break most of the communication immediately
- Internet communication is typically two-way
- Careful bad actor will additionally redirect returning traffic to victim network – to make sure they can establish sessions and commence transmission
- Sniffing will be done in the background



BGP hijacking was and is happening

- Remember “Pakistan Telecom wants all your YouTube traffic” from 2008?
- BGP hijacking is common technique in use today, people no longer care that’s very visible in public
- A lot of “BGP monitoring” sites are living off just from informing about such events

Statement regarding BGP hijacking on September 29

Posted on [October 1, 2020](#) by [Proton Team](#)

THROWING DOWN THE GAUNTLET —

Citing BGP hijacks and hack attacks, feds want China Telecom out of the US

With a history of cyber attacks, Chinese-owned telecom is a threat, officials say.

DAN GOODIN - 4/10/2020, 2:42 PM

Russian telco hijacks internet traffic for Google, AWS, Cloudflare, and others

Rostelecom involved in BGP hijacking incident this week impacting more than 200 CDNs and cloud providers.



By [Catalin Cimpanu](#) for [Zero Day](#) | April 5, 2020 — 21:53 GMT (14:53 PDT) | Topic: [Security](#)

Sources:

<https://arstechnica.com/information-technology/2019/06/bgp-mishap-sends-european-mobile-traffic-through-china-telecom-for-2-hours>

<https://www.zdnet.com/article/russian-telco-hijacks-internet-traffic-for-google-aws-cloudflare-and-others/>

https://portal.bgprmon.net/data/12389_apr2020.txt

BGP hijacking got hot in 2018

- China Unicom entered US carrier ecosystem in multiple cities (to have good coverage)
 - It makes sense for any carrier, and as number of migrants from China grew in US, was also “valid” reason
- They started to actively “help” China Communist Party to obtain traffic from major US Enterprises and US DoD, FBI, CIA, NSA and other three-letter agencies in 2018 by BGP hijacking
- USA FCC decided to remove China Unicom from country in 2018 banning them to operate
- China uses proxy countries now – in South America and in Africa to get similar results

2018 Attack Ranking by Country

Country	Attack Distribution
China	85.63%
Barbados	5.04%
Antigua	4.18%
Guyana	0.81%
Switzerland	0.75%

2018 Ranking by Source Operator

Network Operator	Attack Distribution
China Unicom	81.15%
Flow Barbados	5.64%
Cable & Wireless Antigua	4.68%
China Mobile	1.93%
Orange Caraibe Guyana	0.91%

2019 Attack Ranking by Country

Country	Attack Distribution
Barbados	28.10%
Antigua	18.70%
Mexico	12.92%
Switzerland	6.01%
British Virgin Islands	4.22%

2019 Ranking by Source Operator

Network Operator	Attack Distribution
Flow Barbados	29.04%
Cable & Wireless Antigua	19.33%
Telcel Mexico	8.56%
Swisscom Switzerland	6.21%
Telefonica Movistar	4.80%

4. China reduced its attack volumes, favoring more targeted espionage, likely using proxy networks in the Caribbean and Africa to conduct its attacks, having close ties in both trade and technology investment.

Sources:

<https://docs.fcc.gov/public/attachments/FCC-21-37A1.pdf>

https://img1.wsimg.com/blobby/go/cda61771-2b5c-4a41-aac5-0bd319d1fe07/downloads/Far-From-Home_Intel-RP_2018-2019_B.pdf

Smaller players do it as well – all the time

- 8th of August, 2021: Pakistani Telecom (again!) AS17557 hijacks T-Mobile 172.32/11 prefix (172.50.49/24)
- Russia targets Ukraine:
 - NETGROUP, RU AS35004 hijacks 31.148.149/24 & 95.47.59.0/24 belonging to AS212463 NGROUP, UA
- We're being targeted by proxy networks – in Brazil and Ukraine as well:
 - ENTEL CHILE AS27651 hijacks 193.107.216/24 belonging to SKYTECH AS201814
 - BIGNET AS43668 hijacks 185.242/22 belonging to IP Services AS34907



Cisco BGPStream
@bgpstream

...

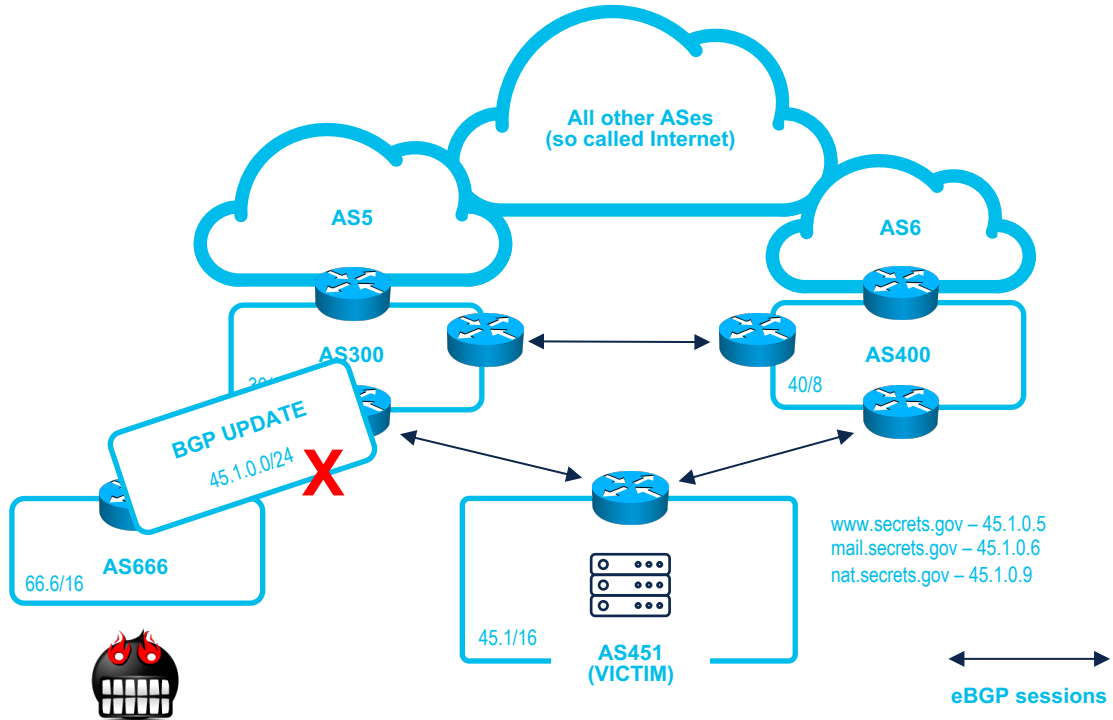
BGP,HJ,hijacked prefix AS8003 11.1.1.0/24, GRS-DOD, US,-,By AS139426 RINJANI-AS-ID PT Rinjani Citra Solusi, ID, bgpstream.com/event/279561

[Translate Tweet](#)

9:47 PM · Sep 3, 2021 · BGPStream

Partial solution is already here – BGP SIDR

- RIRs certify prefix & it's origin ASN and keep this database
- You can have one locally (it's actually recommended) – using tools like Nlnet Labs Routinator 3000*
- You can enable validation of BGP received prefixes against cache of signing information (RPKI)
- After 2018, both service providers and content providers jumped on RPKI ship – nobody likes being constantly hijacked



Configuration and it's effect on traffic

Enable RPKI connection from BGP process

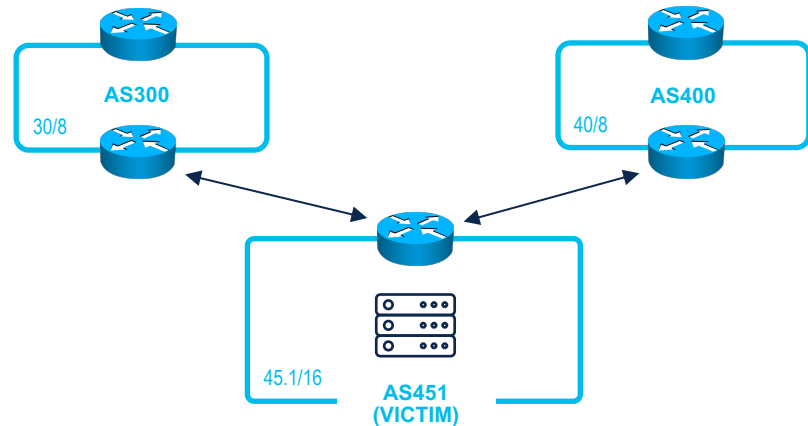
```
router bgp 65055  
  bgp rpki server tcp 192.168.1.1 port 3323 refresh 3600
```

Configure BGP policies to account for RPKI validation status

```
route-map BGP-TE-INGRESS deny 10  
  match invalid  
route-map BGP-TE-INGRESS permit 20  
  match valid  
  set local-preference 150  
route-map BGP-TE-INGRESS permit 30  
  match not-found  
  set local-preference 50
```

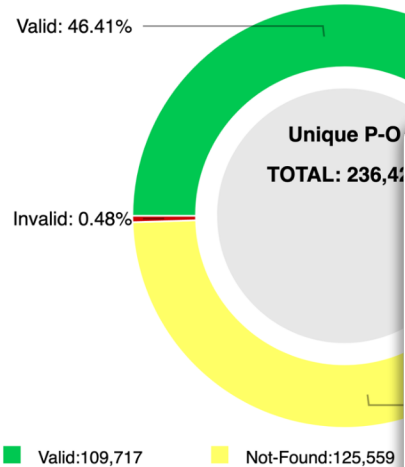
Observe the effect on routing table

```
N*> 1.0.248.0/21      192.168.3.6      6939 4651 23969 i  
V*> 1.1.1.0/24       192.168.3.6      13335 i  
V*> 2.58.228.0/24    192.168.4.6      5617 5511 6762 9481 i
```



BGP SIDR RPKI statistics

RPKI-ROV Analysis of Unique Prefix-Origin Pairs in RIPE (IPv4)

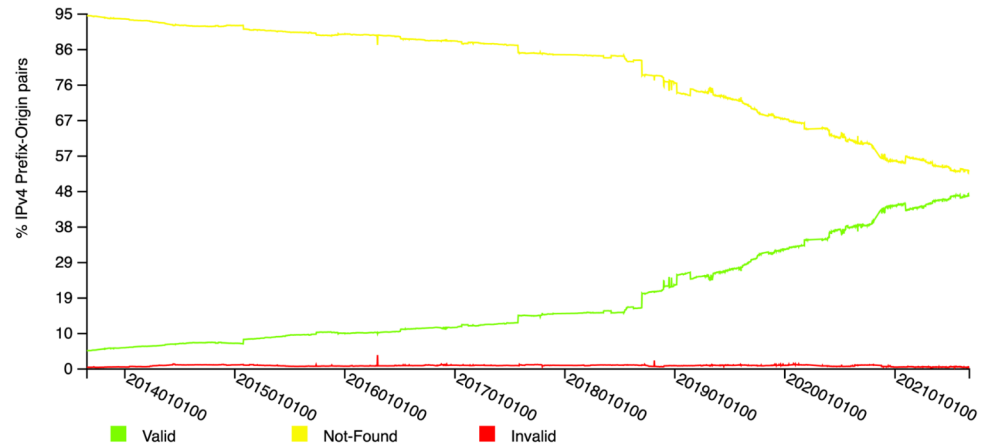


NIST RPKI Monitor: RPKI-ROV Analysis

Protocol: IPv4

RIR: RI

RPKI-ROV History of Unique Prefix-Origin Pairs in RIPE (IPv4)



NIST RPKI Monitor: RPKI-ROV Analysis

Protocol: IPv4

RIR: RIPE

Sources:

<https://rpki-monitor.antd.nist.gov/ROV/20210905.00/R/All/4>

Traffic hijacking... in space

- You were able to listen to radio transmissions from satellites for free with decent equipment for decades already
 - Some hacking was done already to access classified feeds (including video) during Falklands, Iraq and Afghanistan conflicts
- As we see more satellites in low orbit and even smartphones capable to send traffic
 - ...we'll have more and more opportunities to start playing with traffic here
 - SDWAN will become “WAN over space”



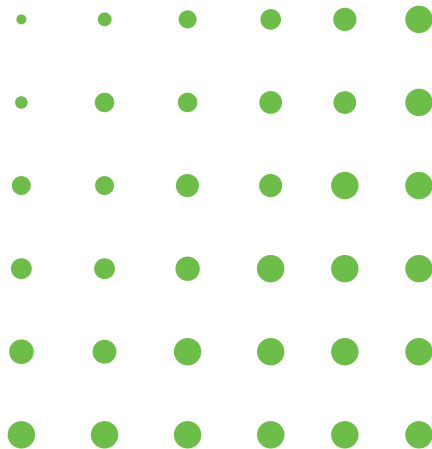
VIDEO STAFF BUSINESS 04.20.2009 12:00 PM

The Great Brazilian Sat-Hack Crackdown

Sources:

<https://www.wired.com/2009/04/fleetcom/>
<https://i.blackhat.com/USA-20/Wednesday/us-20-Pavur-Whispers-Among-The-Stars-Perpetrating-And-Preventing-Satellite-Eavesdropping-Attacks.pdf>
https://www.theregister.com/2021/09/02/in_space_no_security/

Signals, signals
everywhere...



Everything is using “telemetry” today...

- You can't really disable telemetry in Apple and Microsoft products anymore
- All or most of all apps on your smartphones are sending telemetry as well
 - ...even if developer doesn't know anything about it – hundreds of libraries compiled to the app, or even such small things like ads being served in the app windows...
- Protecting your external posture becomes more and more challenging
 - remember IPv6 autoconfiguration surprises?
- AS 112 project is one of those “good things good people do” for internet users

AS 112? Like calling 112 in Poland? Nope...

- Many networks generate DNS reverse lookup queries for RFC 1918 addresses, some also dynamic updates
 - 10/8, 172.16/12, 169.254/16, 192.168/16
- Those queries end up travelling up to the root servers, and can't be typically responded in any way – so they're dropped
- This puts load on root servers but also may be interesting from the attacker point of view
 - Mapping your internal addressing and possibly – resources
- Volunteers setup anycasted instance of AS 112 "sinkhole" to lessen load on the root servers and international links

AS 112 DNS servers – in Poland ;)

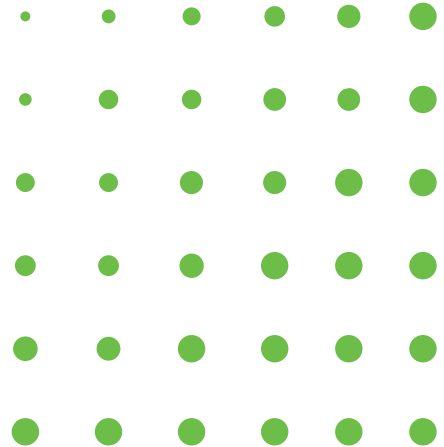
- Free service in Poland, next to the one offered by [Aplitt](#)* (shout out!)
- 4 different VMs, each receiving about 70–80 qps on normal day (200–250 qps in spikes)
- Kudos to ATMAN, EPIX for free hosting!
- I'll start reaching out to companies on the “top” list to help improve their security posture

```
Queries: 78 new, 194134727 total
```

Query Name	Count	%	cum%
16.172.in-addr.arpa	28788201	14.8	14.8
168.192.in-addr.arpa	19127135	9.9	24.7
dropthishost-760cc2c0-bb02-4dcb-ba9e-c6154a929208.empty	15026629	7.7	32.4
dropthishost-7f26f86d-ec9c-4efb-bc8c-5fee20b7aa81.empty	14971068	7.7	40.1
wpad.home.arpa	7477296	3.9	44.0
10.in-addr.arpa	5105963	2.6	46.6
ubuntu.com.home.arpa	4825208	2.5	49.1
openthread.thread.home.arpa	4373740	2.3	51.4
[redacted].ome.arpa	3272806	1.7	53.0
[redacted].home.arpa	3060138	1.6	54.6
brn3c2af4f9b72e.home.arpa	2599282	1.3	56.0
[redacted].home.arpa.home.arpa	2448575	1.3	57.2
[redacted].ome.arpa	2160668	1.1	58.3
[redacted].addr.arpa	2157461	1.1	59.4
[redacted].ome.arpa	1735508	0.9	60.3
drop-64a41445-aa58-446a-b357-5ace532d22c3.empty.as112.a	1606689	0.8	61.2
drop-e058fe90-bc2a-4cb7-b85c-f027e9a154a1.empty.as112.a	1604388	0.8	62.0
wlan-controller.home.arpa	1494135	0.8	62.8

```
[as112] (0x$ sh) [08/15/21 5:47 PM]
```

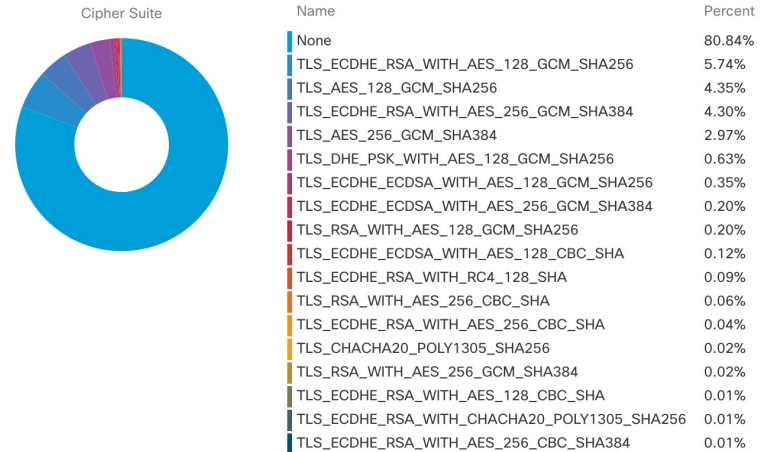
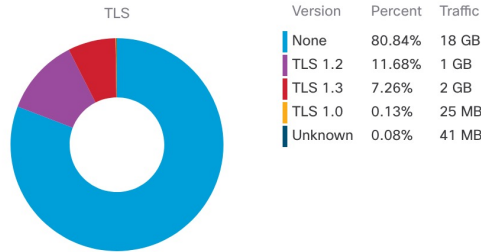
Can you decrypt
everything?



TLS 1.3 is the way

- Given SSL and TLS 1.0 & 1.1 were already deprecated^{*}, you'd expect to see almost exclusively TLS 1.2 and TLS 1.3 protected traffic in today's Enterprise networks

Summary View



Source: Friendly Enterprise & Cisco StealthWatch Enterprise

^{*} <https://www.rfc-editor.org/rfc/rfc8996.html>

<https://datatracker.ietf.org/doc/html/rfc8404>

TLS 1.3 is the way

- TLS 1.0 use is worrying
 - TLS 1.0 is used to talk to Microsoft servers from Windows 10 workstations – phasing out by Microsoft was delayed due to COVID-19*
 - TLS 1.0 also used by home & appliances (Bosch!), Philips beamers and for example some Samsung TVs to talk to AWS-hosted “media centers”; Onkyo amplifier also uses that, so, likely millions of not upgraded/not upgradeable home devices

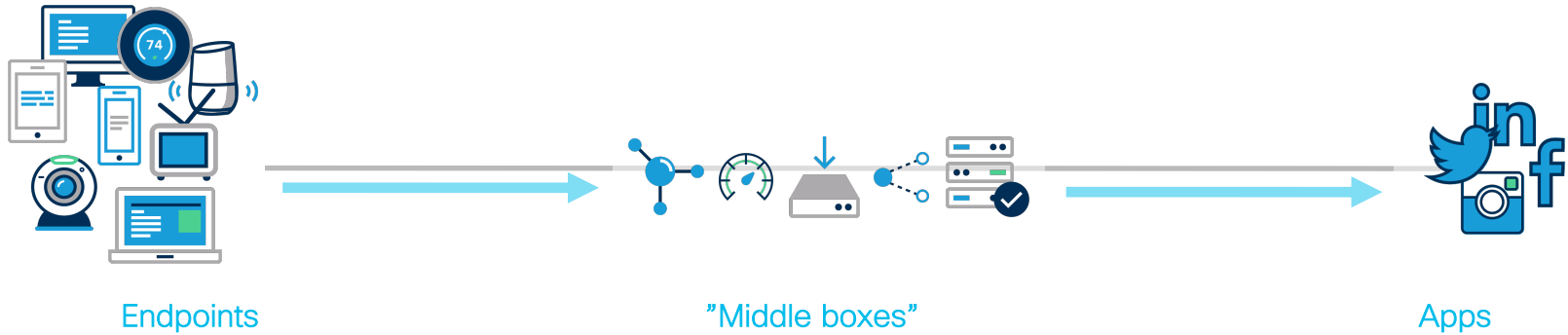
Detailed View

TLS Version ↓	Cipher Suites
TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS 1.0	TLS_ECDHE_RSA_WITH_RC4_128_SHA

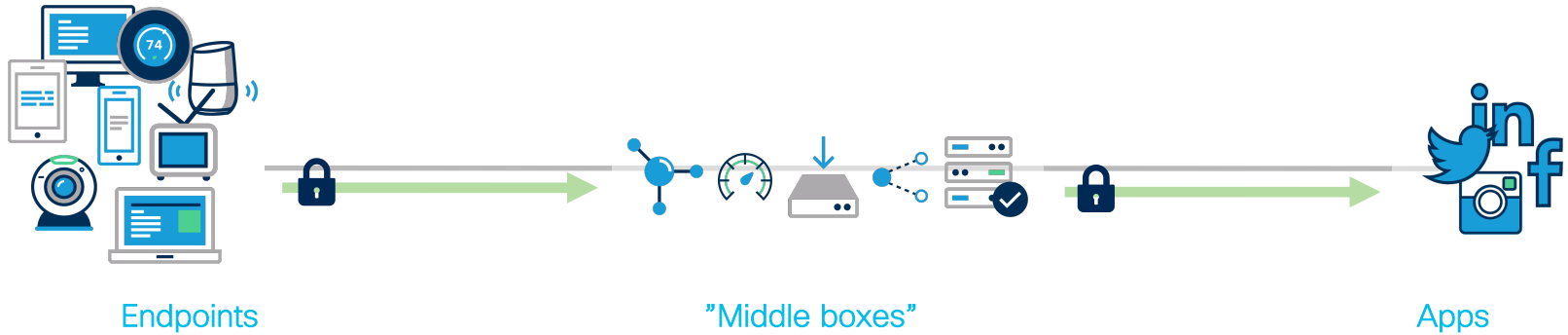
Source: Friendly Enterprise & Cisco StealthWatch Enterprise

* <https://docs.microsoft.com/pl-pl/lifecycle/announcements/transport-layer-security-1x-disablement>

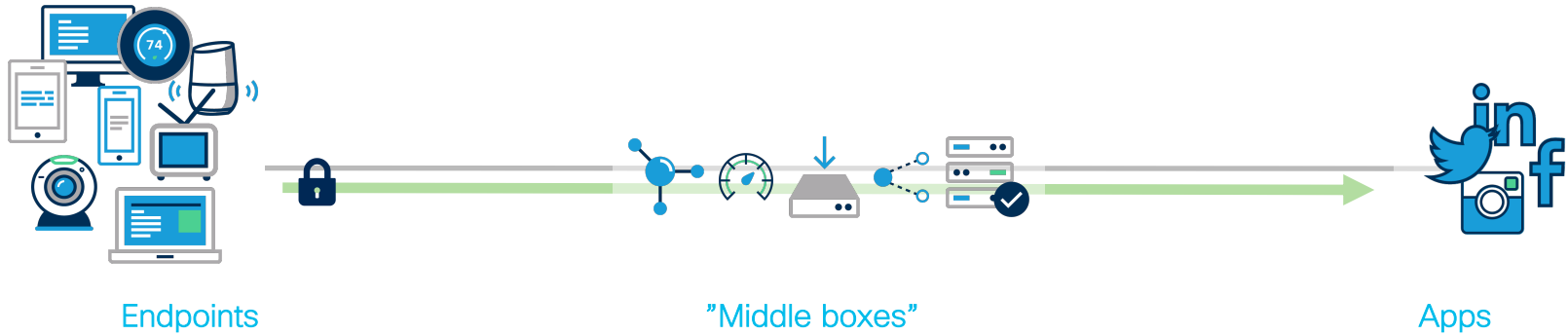
Endpoint vs network – never ending journey



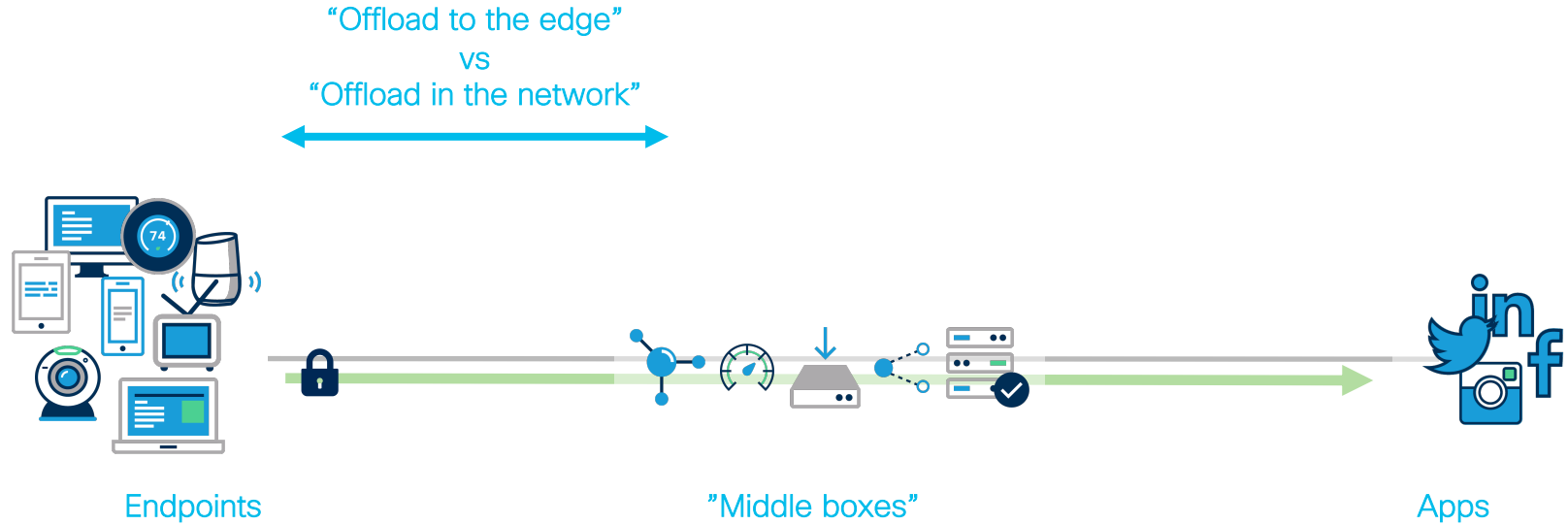
Endpoint vs network – never ending journey



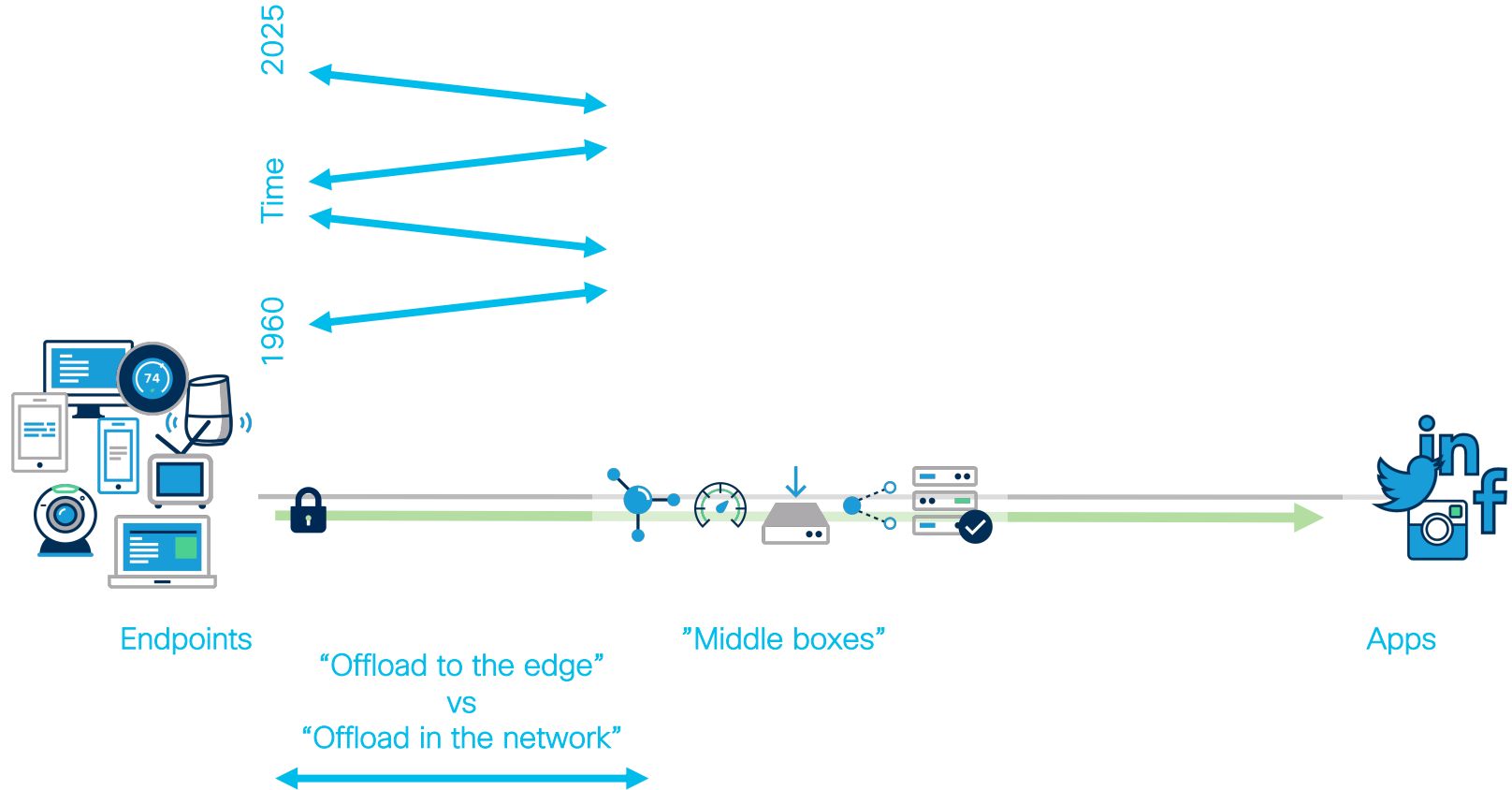
Endpoint vs network – never ending journey



Endpoint vs network – never ending journey



Endpoint vs network – never ending journey



Middleboxes can be weaponized as well

- DPI, IPS, load balancers and web proxy boxes can be used as amplifiers when properly attacked
- Serious issue for “privacy loving countries” and some enterprises as well

Weaponizing Middleboxes for TCP Reflected Amplification

Kevin Bock* Abdulrahman Alaraj† Yair Fax* Kyle Hurley* Eric Wustrow† Dave Levin*
*University of Maryland †University of Colorado Boulder

Abstract

Reflective amplification attacks are a powerful tool in the arsenal of a DDoS attacker, but to date have almost exclusively targeted UDP-based protocols. In this paper, we demonstrate that non-trivial TCP-based amplification is possible and can be orders of magnitude more effective than well-known UDP-based amplification. By taking advantage of TCP-non-compliance in network middleboxes, we show that attackers can induce middleboxes to respond and amplify network traffic. With the novel application of a recent genetic algorithm, we discover and maximize the efficacy of new TCP-based reflective amplification attacks, and present several packet sequences that cause network middleboxes to respond with substantially more packets than we send.

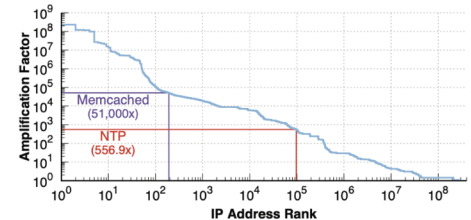


Figure 1: The maximum amplification factor we obtained per IPv4 address, based on several Internet-wide scans. (Note: the axes are log-scale.)

So let's fingerprint TLS sessions and identify agent

- [JA3](#)/JA3S from... Salesforce engineering team (yeah)!
- Open database of fingerprints along with online viewer:
 - <https://ja3er.com/>
- Limitations of single vector identification are pretty obvious when you try to fingerprint your workstation

JA3 SSL Fingerprint

User-Agents seen with the hash

bd50e49d418ed1777b9a410d614440c4

771,4865-4867-4866-49195-49199-52393-52392-49196-49200-49162-49161-49171-49172-156-157-

- Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0 (count: 27, last seen: 2021-08-31 16:36:17)
- Mozilla/5.0 (X11; Fedora; Linux x86_64; rv:88.0) Gecko/20100101 Firefox/88.0 (count: 24, last seen: 2021-07-21 07:57:08)
- Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:78.0) Gecko/20100101 Firefox/78.0 (count: 22, last seen: 2021-03-10 19:00:52)

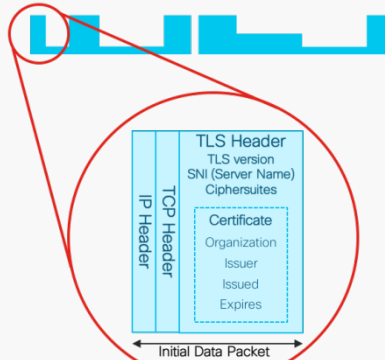
Sources:

<https://github.com/salesforce/ja3> & <https://www.youtube.com/watch?v=oprPu7UIEuk>
<https://www.akamai.com/blog/security/bots-tampering-with-tls-to-avoid-detection>

Inspecting encrypted traffic for malware Cisco way

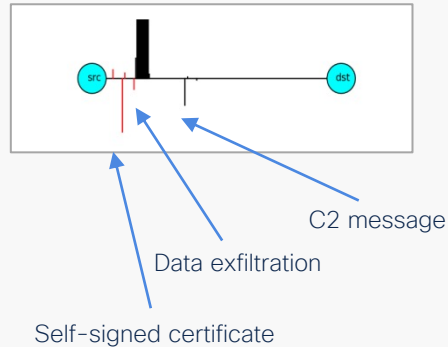
Initial data packet

Make the most of the unencrypted fields



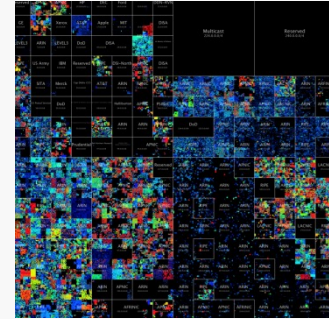
Sequence of packet lengths and times

Identify the content type through the size and timing of packets



Real-time correlation with other data

Who's who of the Internet's dark side



Broad behavioral information about the traffic in the internet.

Doing ETA the right way... your (and open) way

- Open source **Joy** package, massively extended in newer **Mercury** project (also open source)
- Once you have raw data, you can start to build models, use fingerprints, etc:

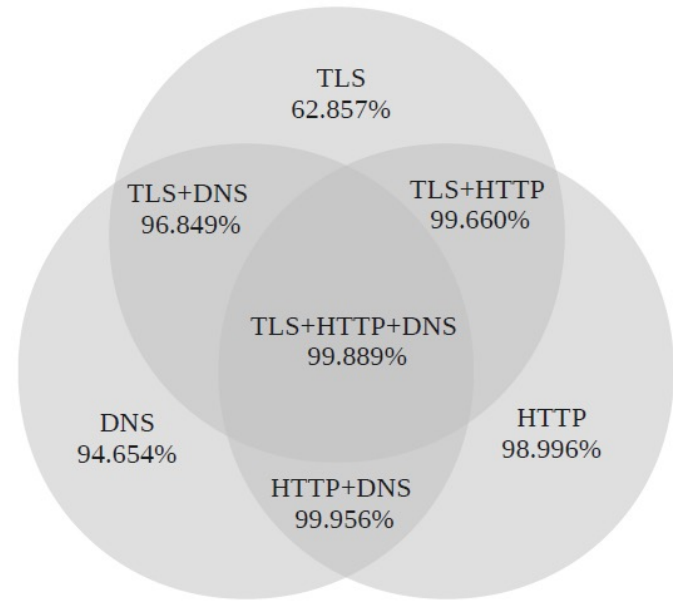
```
{ "fingerprints":  
  { "tcp": "(faf0)(020405b4)(04)(08)(01)(030307)(22)(01)(01)", "src_ip": "172.16.238.5", "dst_ip": "172.16.238.1", "protocol": 6,  
    "src_port": 55144, "dst_port": 53, "event_start": 1630858583.941264 }  
  { "fingerprints":  
    { "tcp": "(fd20)(020405a0)(04)(08)(01)(030307)(22)(01)(01)", "src_ip": "fe80:0000:0000:0000:ebfc:b64e:5d82:b604",  
      "dst_ip": "fe80:0000:0000:0000:00a7:c47d:89db:c4f3", "protocol": 6, "src_port": 55952, "dst_port": 53,  
      "event_start": 1630858583.942548 }  
    { "dns": { "base64": "Q1cBAAABAAZZZAHAAB" }, "src_ip": "172.16.238.5", "dst_ip": "172.16.238.1", "protocol": 17,  
      "src_port": 55942, "dst_port": 53, "event_start": 1630858584.119078 }  
  }  
  { "fingerprints":  
    { "tcp": "(fd20)(020405a0)(04)(08)(01)(030307)(22)(01)(01)", "src_ip": "fe80:0000:0000:0000:ebfc:b64e:5d82:b604",  
      "dst_ip": "fe80:0000:0000:0000:00a7:c47d:89db:c4f3", "protocol": 6, "src_port": 55954, "dst_port": 53,  
      "event_start": 1630858584.120109 }  
  }  
  { "fingerprints":  
    { "tcp": "(faf0)(020405b4)(04)(08)(01)(030307)", "src_ip": "172.16.238.5", "dst_ip": "80.252.0.132", "protocol": 6,  
      "src_port": 45052, "dst_port": 443, "event_start": 1630858584.122538 }  
  }  
  { "fingerprints":  
    { "tls": "(0303)(130113031302c02bc02fcc9cca8c02cc030c00ac009c013c014009c009d002f0035000a)((0000)(0017) [...]
```

Sources:

<https://github.com/cisco/joy>
<https://github.com/cisco/mercury>

It will take some time and skilful ML to see patterns

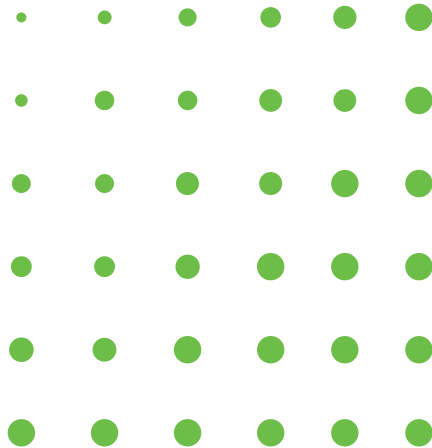
- The more you see (and can correlate) the more accurate you are
 - Fingerprints for TLS and applications, both encrypted and not
 - DNS data to provide weighting data for initial fingerprint analysis/matching; Cisco Umbrella is used for Cisco ETA
- Data obtained in real-world testing using internet exchange point as traffic source (~100G line rate on Catalyst 9k switch) and 4 days worth of traffic for observations



Start reading here, dig deeper for more

- “Machine Learning for Encrypted Malware Traffic Classification: Accounting for Noisy Labels and Non-Stationarity”, Blake Anderson & David McGrew
- “Detecting Malware in TLS Traffic”, Olivier Roques
- “Malware Detection by Analysing Encrypted Network Traffic with Neural Networks”, Paul Prasse, Luka Machlica, Toma Pevny, Jiri Havelka, Tobias Scheffer
- “ME-Box: A reliable method to detect malicious encrypted traffic”, Bingfeng Xu, Gaofeng He, Haiting Zhu
- “Network Traffic Anomaly Detection Using Recurrent Neural Networks”, Benjamin Radford, Leonardo Apolonio, Antonio Trias, Jim Simpson
- “DeepMAL – Deep Learning Models for Malware Traffic Detection and Classification”, Gonzalo Marin, Pedro Casas, German Capdehourat

What's out there for
us?



Big battle for endpoints & privacy began

- In future, badly chosen hash will decide if you'll be asked by Police or not
 - Transparency is key to free society
- We built the internet, if what we're doing today is not enough, we have to try harder
 - There's massive trove of best practices and security right now starts with hundreds of hours invested into training people and configuring your infra and apps right
 - Don't look for unicorns to come and save you, start from the basics and implement them NOW
- „Zero Trust Architecture” while marketing name, conveys the approach:
 - Segment everyone from everyone else – no connectivity by default
 - Layer your defenses
 - Use multifactor authentication with each app you're interacting with

Best practice reference sources for networking security

FOR REFERENCE

- Barry Raveendran Greene security reference site:
<https://www.senki.org/>
- Best practices for configuring crypto across different servers, devices and apps:
<https://bettercrypto.org/>
- NIST monitor & RIPE RPKI validator:
<https://rpki-monitor.antd.nist.gov/Cov> | <https://rpki-validator.ripe.net/trust-anchors>
- NLNOG IRR explorer & NLNOG prefix list recommendation reference guide (multivendor)
<https://irrexplorer.nlnog.net/prefix/> | https://bgpfilterguide.nlnog.net/guides/bogon_prefixes/
- FIRST best practices guide:
<https://www.first.org/resources/guides/>

Polish (!) security landscape reports

FOR REFERENCE



<https://cert.pl/publikacje/>
<https://www.cert.pl/raporty-roczne/>



<https://cert.orange.pl/raporty-cert>



[https://csirt.gov.pl/cer/publikacje/
raporty-o-stanie-bezpi](https://csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi)

