Trojan Explosion

Austin McBride
Data Scientist
Cisco Umbrella
@armcbride1

Artsiom Holub
Senior Research Analyst
Cisco Umbrella
@Mesiagh

Agenda

1. Attack Trends
2. The Biggest Threats
3. Designing the Defense

$ WHOIS Artsiom

- Senior Security Analyst at Cisco Umbrella
- A.S. in Computer Networking and Information Technology, CCSF
- Tracking bad guys since 2015
- Trying make Internet a safer place

$ WHOIS Austin

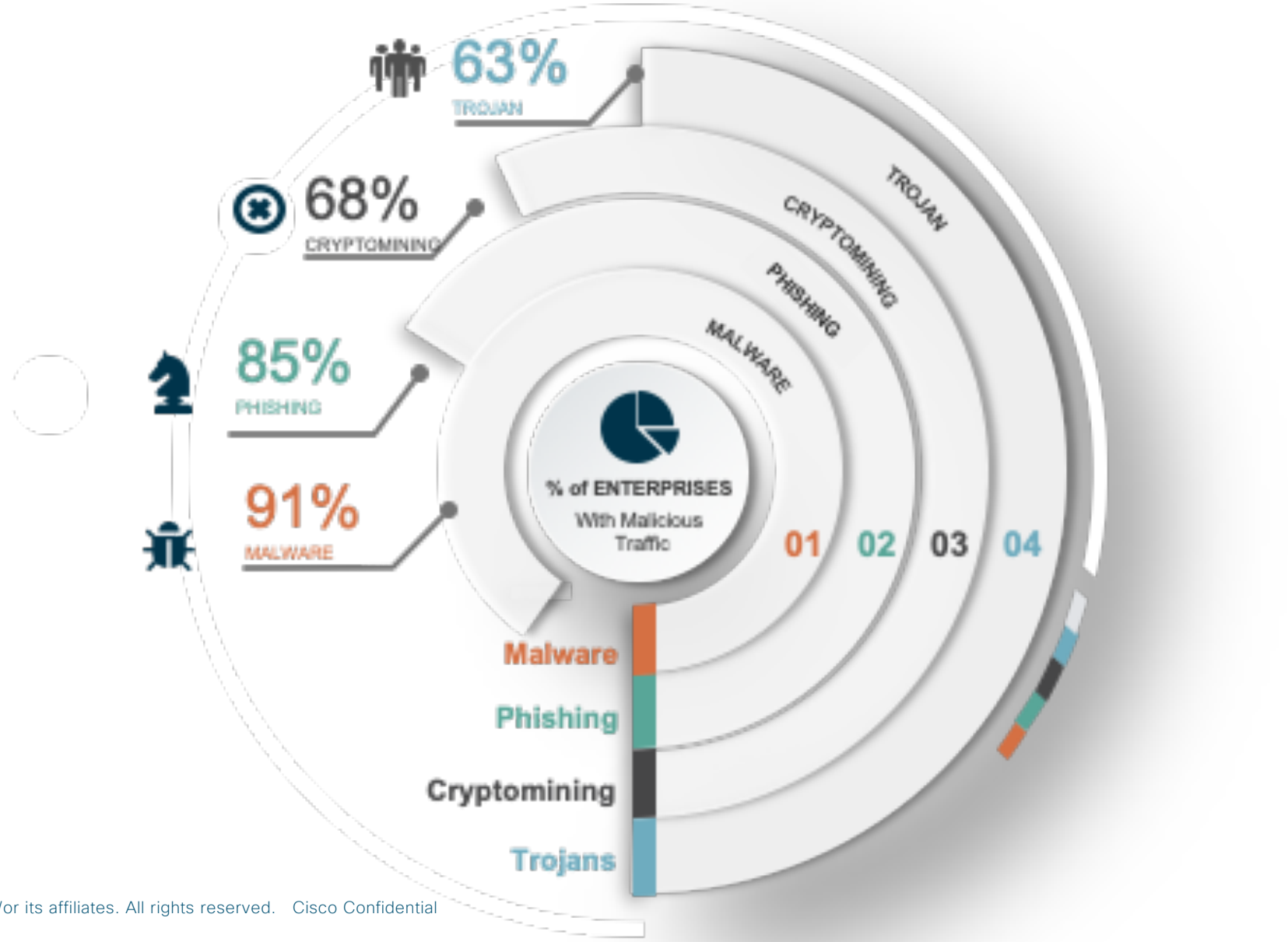
- Data Scientist at Cisco Umbrella
- B.S. in Data Mining and Economics
- Crypto enthusiast
- Hobbies: work, algorithmic crypto trading, and work

Our Research Team

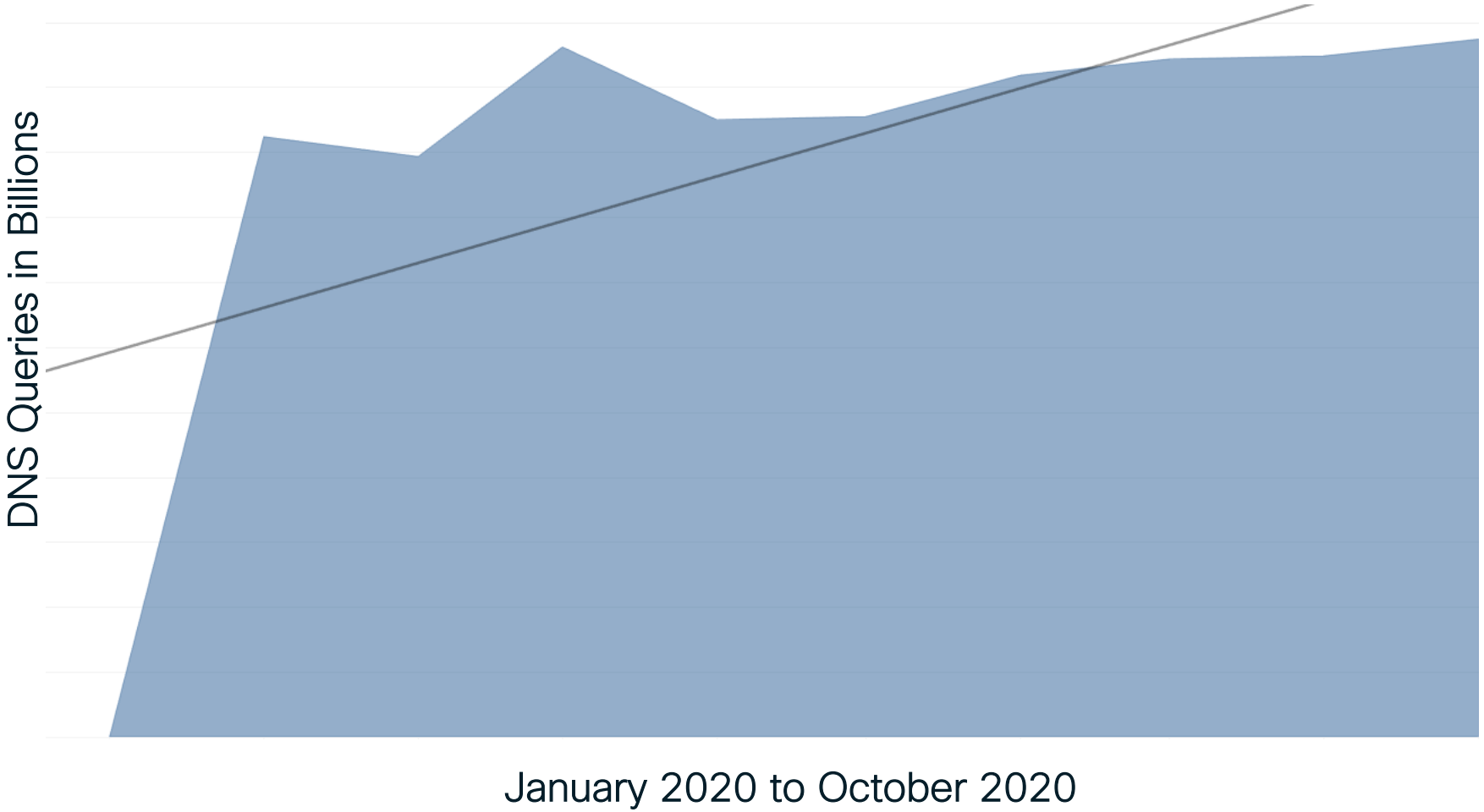
- Data Science & Network Security
- Big Security Data
- DNS Traffic:
  - ~250B DNS requests per day
  - NEWLY SEEN DOMAINS!!
  - …and now all of Cisco data!
- Daily Tasks:
  - Security Data Analysis
  - Customer Data Analysis
  - Big Data Engineering
  - Detection Algorithms

Attack Trends

Threats are pervasive across all enterprises



Malicious Traffic Growth



- Malicious threat traffic has increased 38X from Jaunary 2020 to October of 2020

Top Threats Per Region

North America

Malware

Cryptomining

Phishing

Trojan

Ransomware

Dropper

EMEA

Malware

Cryptomining

Phishing

Trojan

Ransomware

RAT

LATAM

Malware

Cryptomining

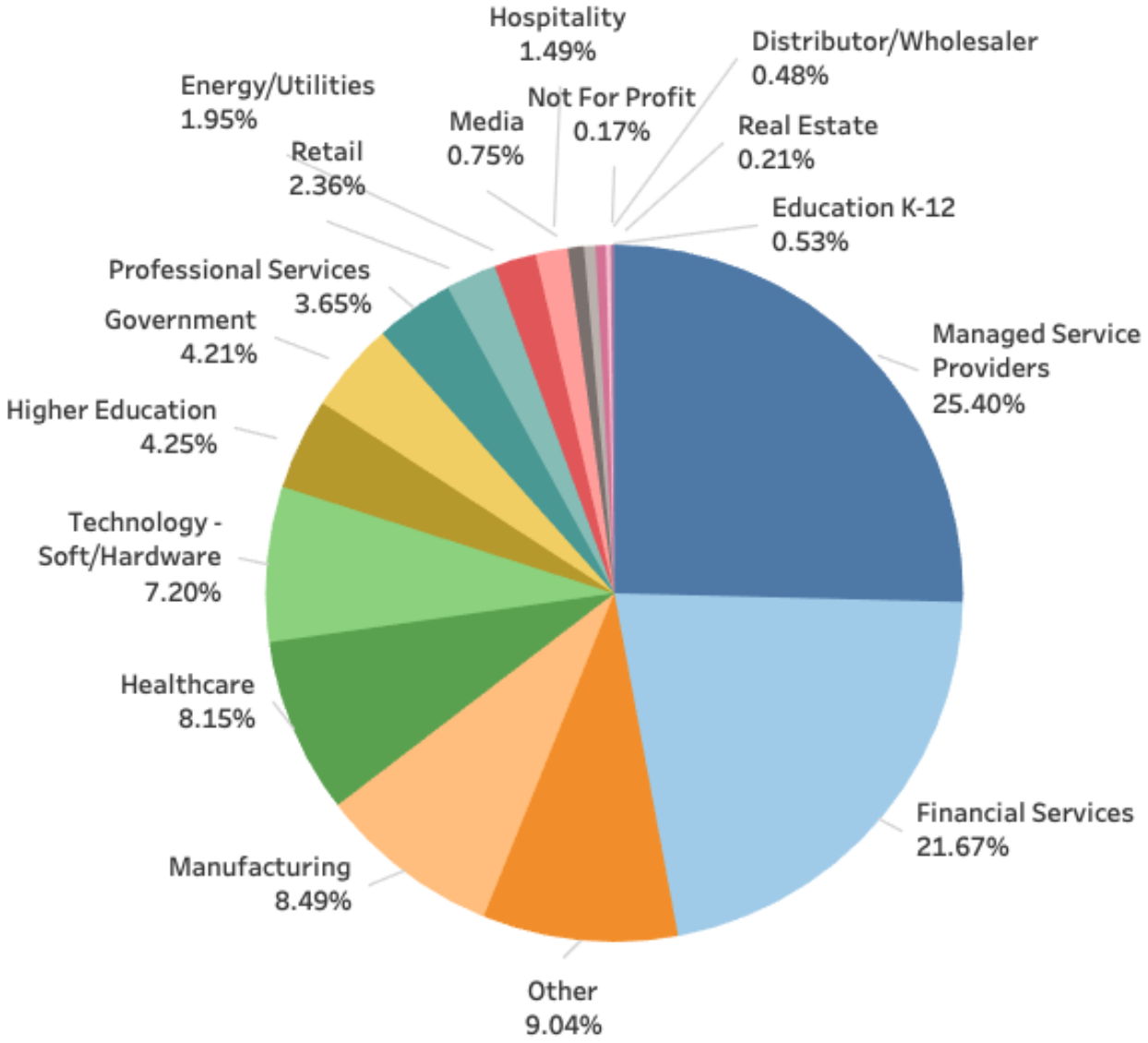
Botnet

Trojan

Phishing

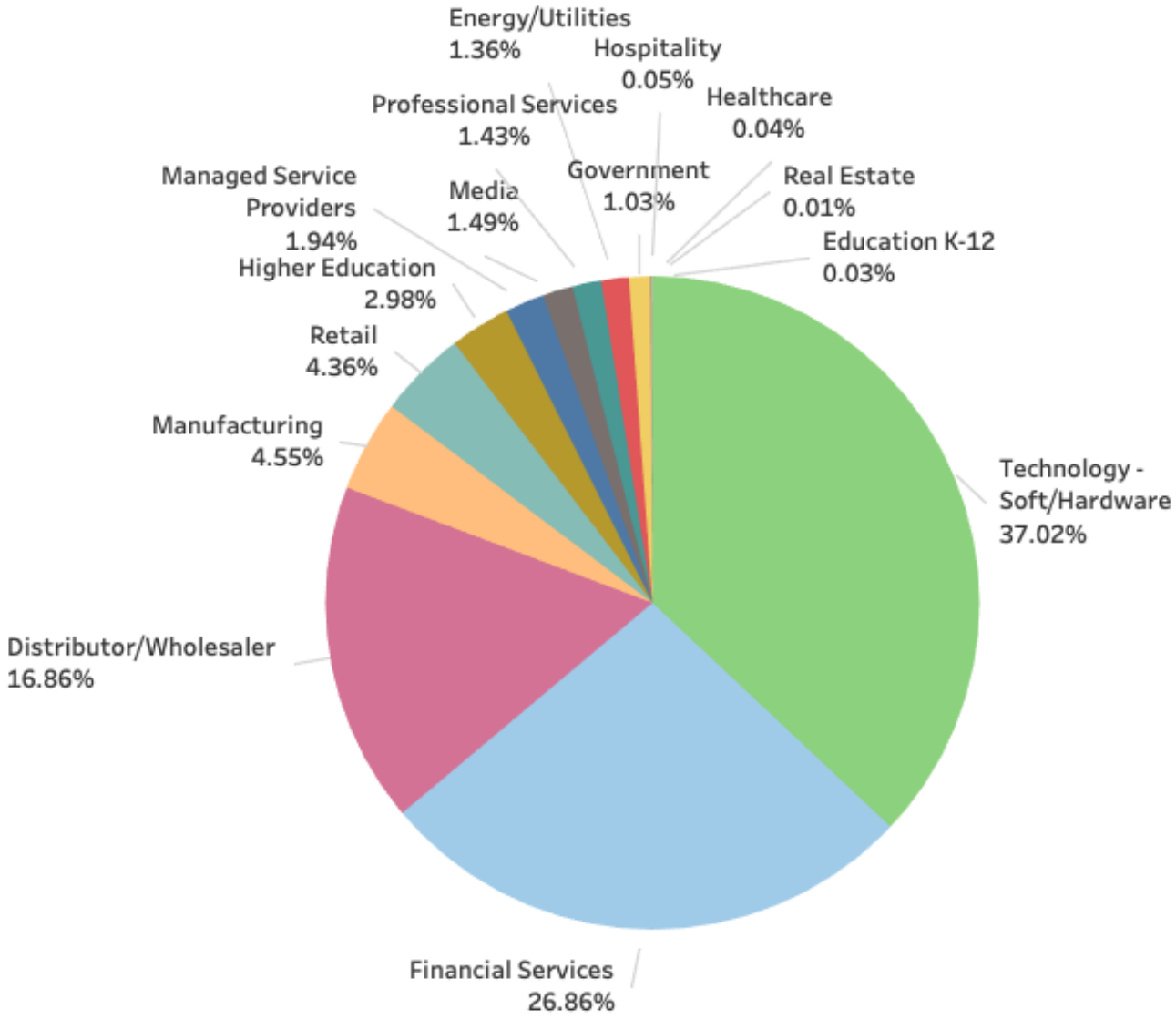
Ransomware

Global Malicious Traffic Industry Distribution



- Malicious traffic is widely distributed
- Top industry fluctuates every 2-3 months, but Finacial Services is always in the top 2

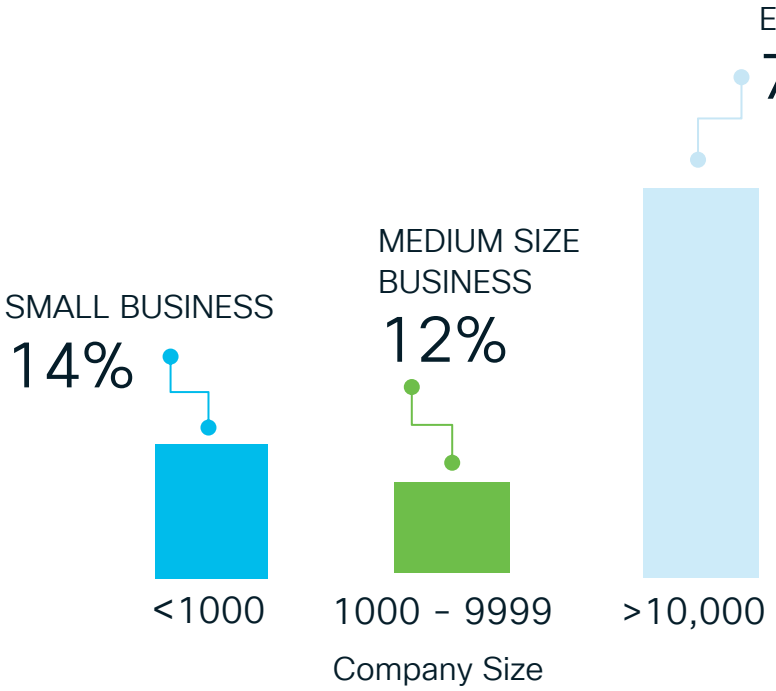
LATAM Malicious Traffic Industry Distribution



- Malicious traffic is more focused on Tech and Financial companies in LATAM

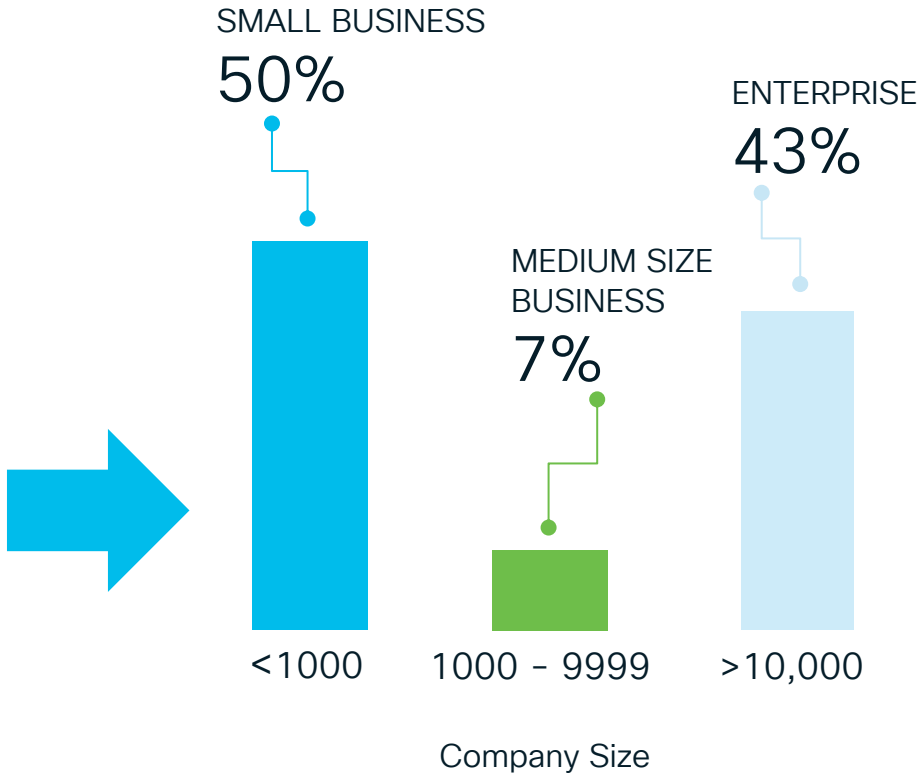
LATAM's Two Most Impacted Verticals

Ursnif and Emotet Target Companies Differently Based on Geography

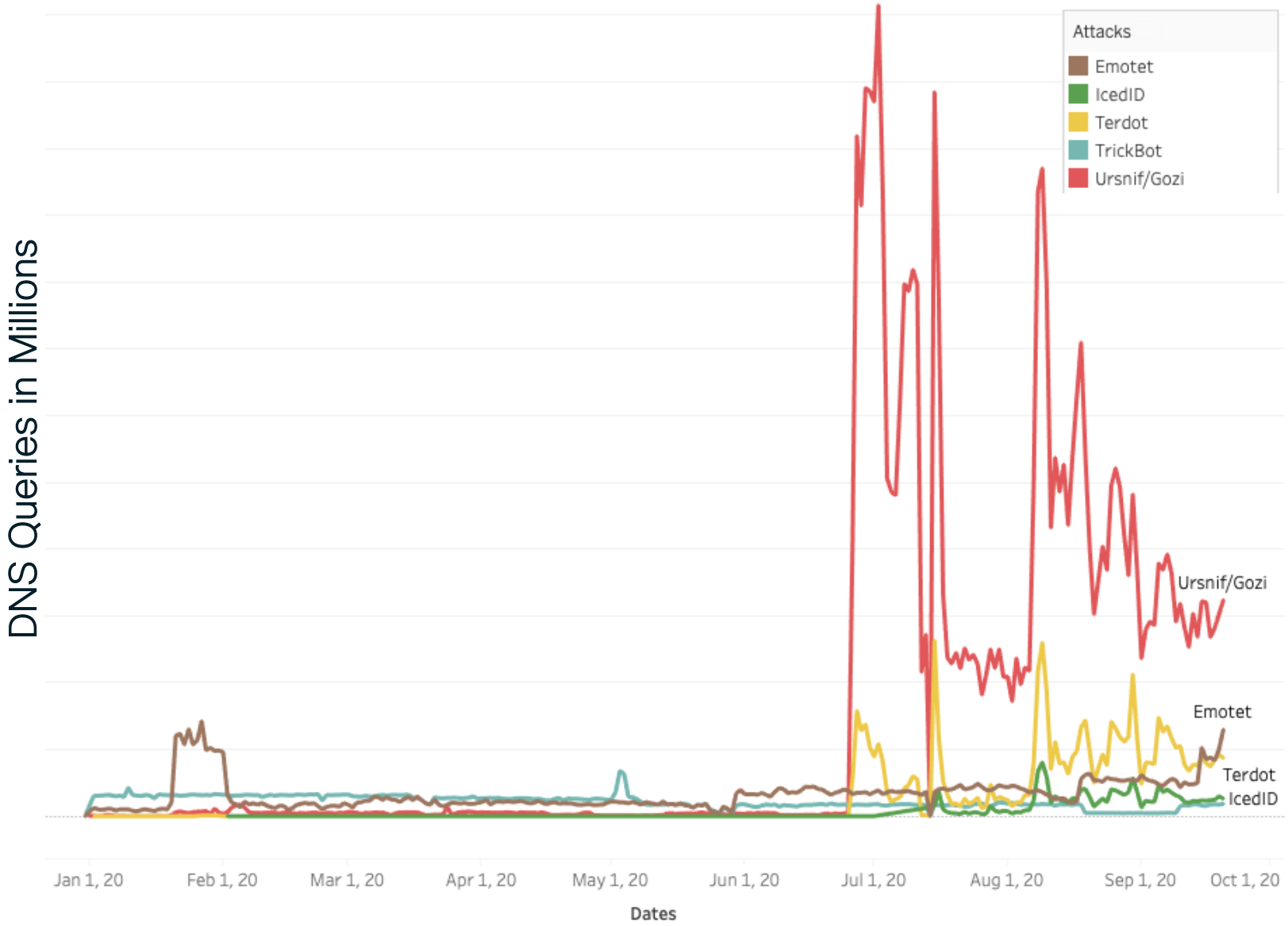


In LATAM we have seen 74% of all Ursnif/Emotet traffic happening in large sized business

Globally, Ursnif/Emotet traffic is split evenly between small and large sized businesses



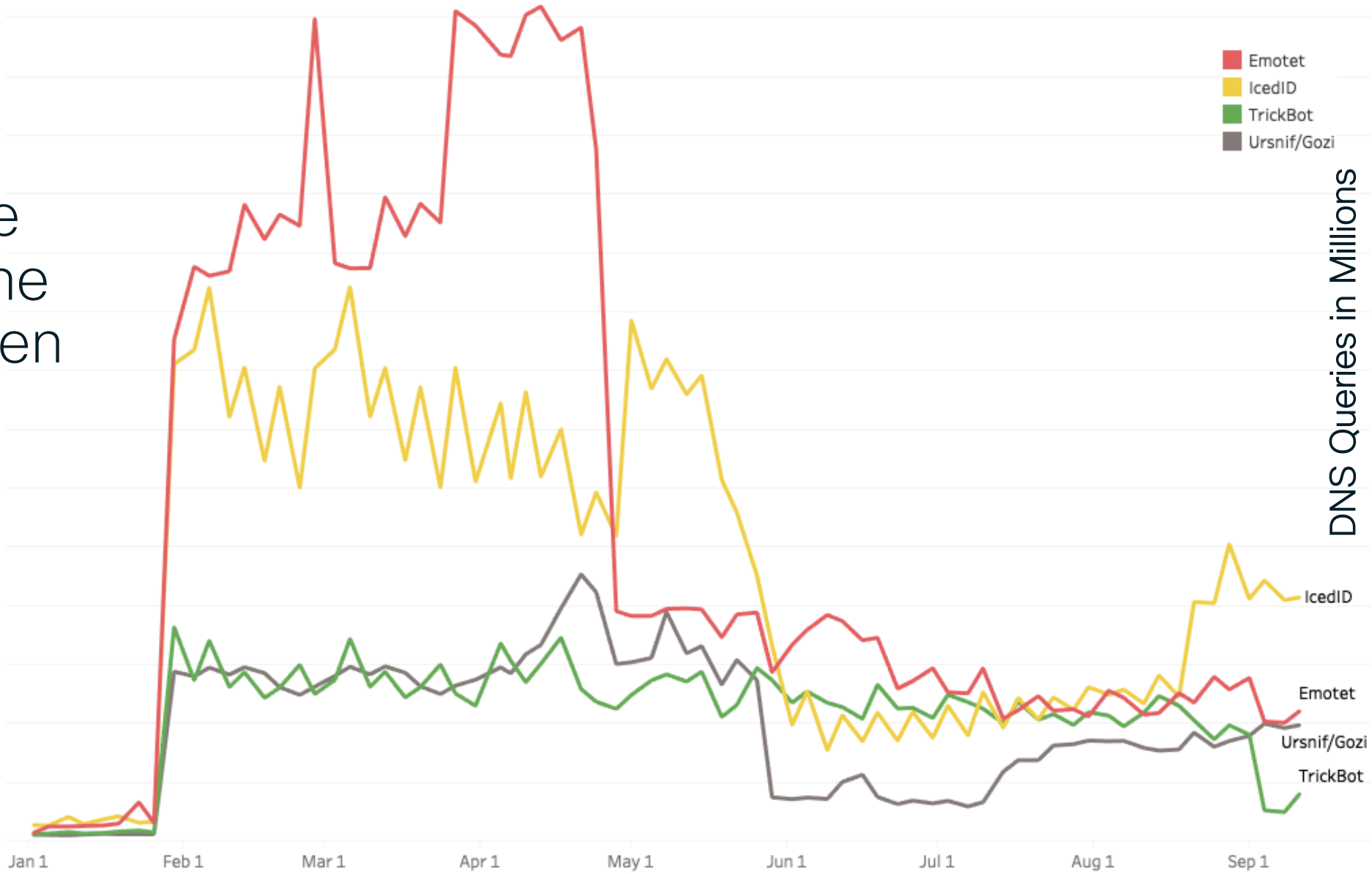
Trojan Threat Traffic in LATAM



- Ursnif has replaced Emotet as the top trojan targeting LATAM business
- At Ursnif's peak in July we saw a 12X spike in traffic

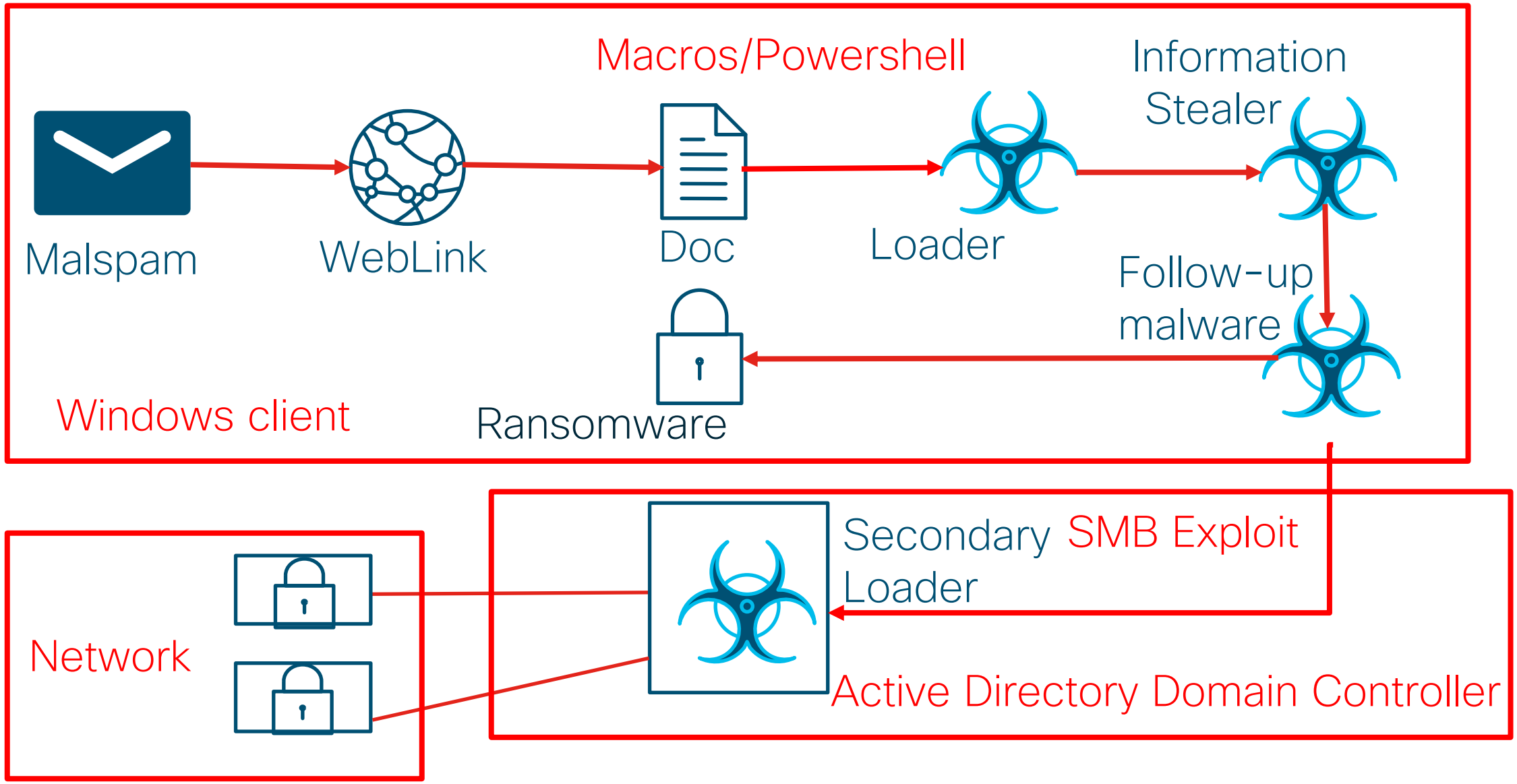
Multi-staged Compromise – Global View

- Looking at the query volumes we can start to see the correlation between the attacks



The Biggest Threats

Sample Loader Attack Chain



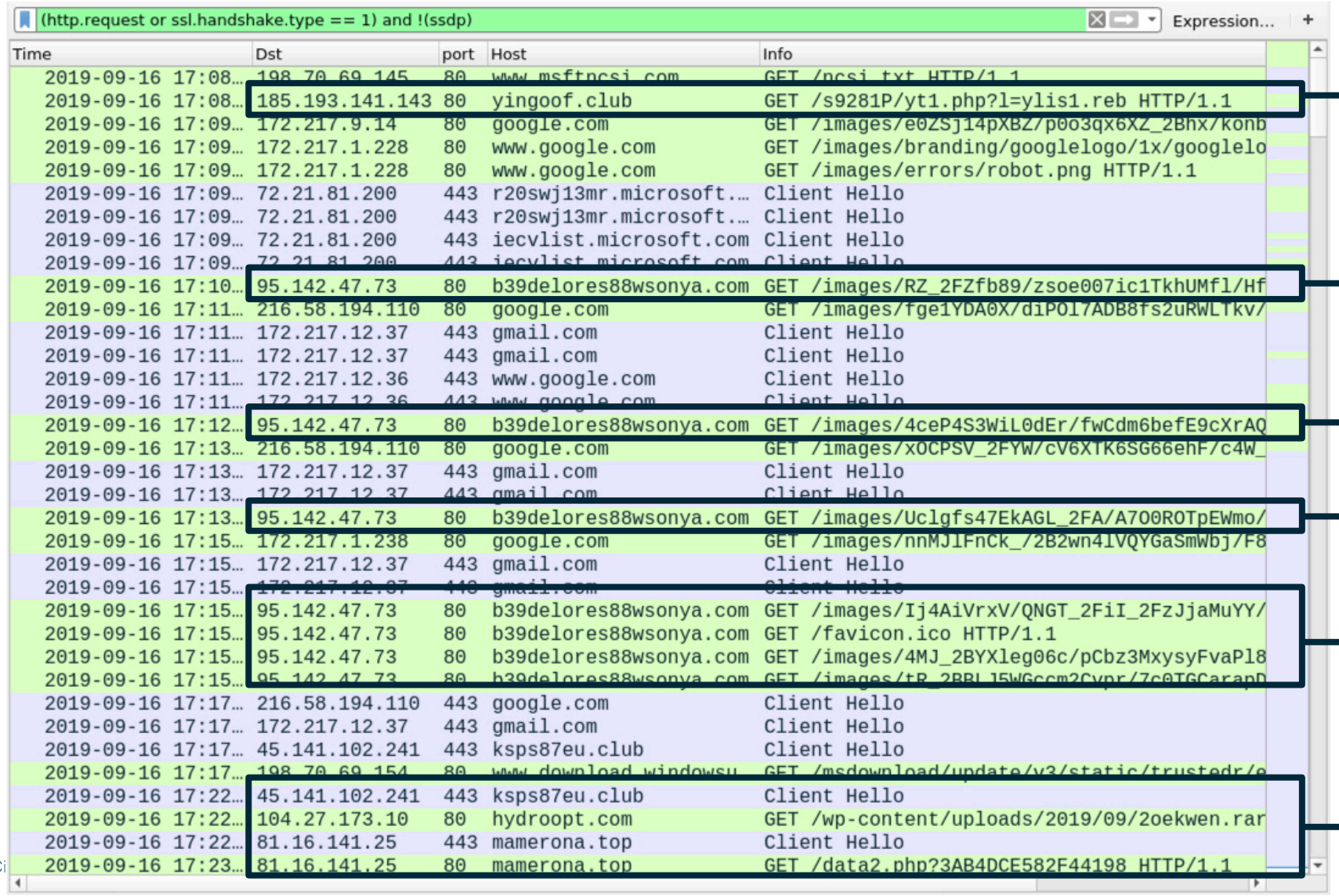
Ursnif (also known as DreamBot, ISFB, Gozi)

- Rapidly evolving loader with trojan capabilities
- Being spread as a standalone version and as a dropper for other malware
- Has a targeted approach to the choice of delivery method depending on potential victims
- Utilizes email thread hijacking
- Leverages abuse of trusted services such as Google Drive, DropBox

Ursnif follow up malware

Malware	Capabilities
IcedID / BokBot	Information Theft, Download Routine
Azorult	Information Theft, Backdoor commands, Exploits, Download Routine
PredatorTheThief	Information Theft, Backdoor commands, Exploits, Download Routine
Vidar	Information Theft, Download Routine
Dridex	Information Theft, Download Routine
rEvil/Sodinokibi	Information Theft, Data Encryption, Ransom Extortion
Ruyk	Information Theft, Data Encryption, Ransom Extortion

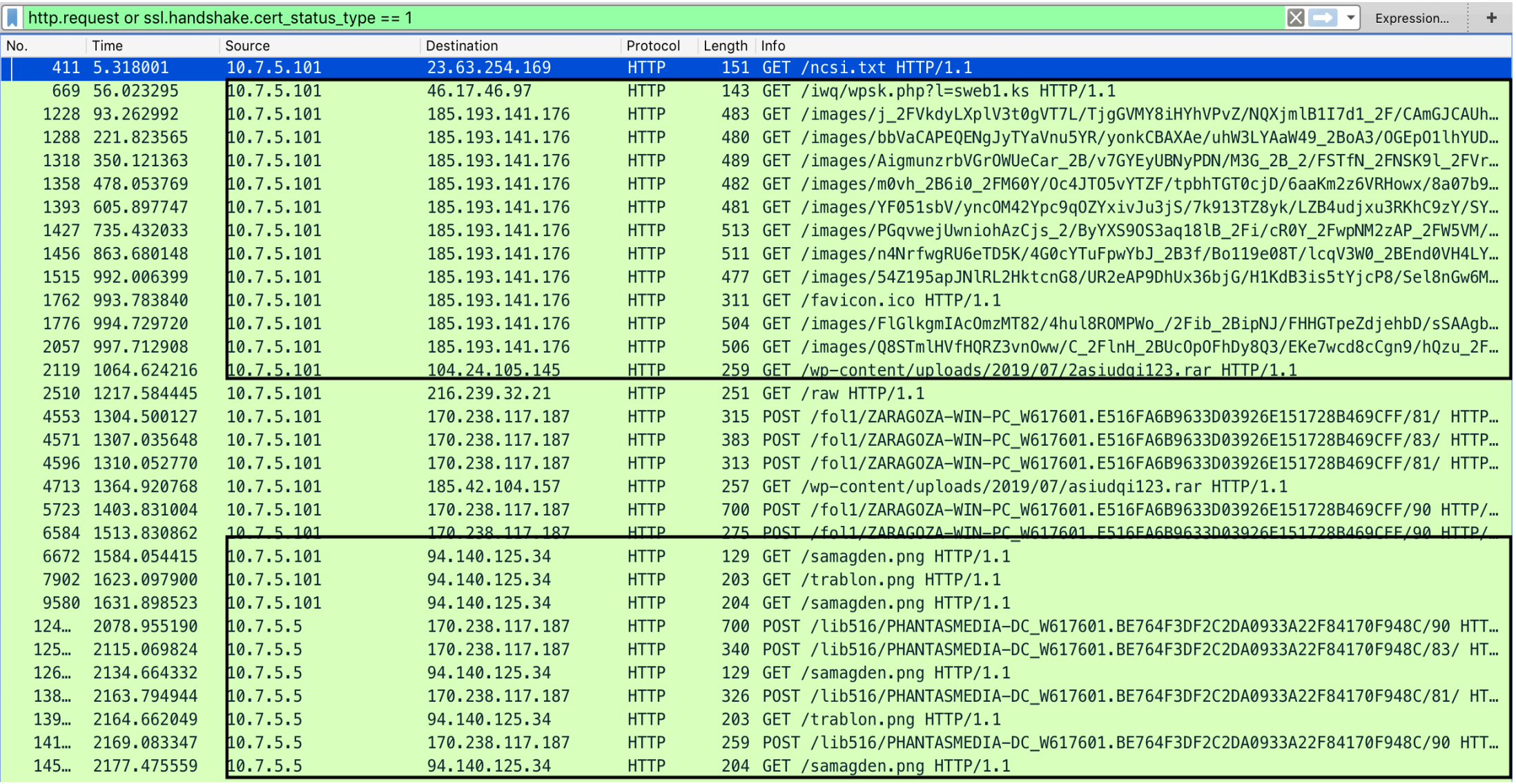
Ursnif with IcedID/BokBot



Ursnif traffic

IcedID/BokBot

Ursnif Infection with TrickBot



http.request or ssl.handshake.cert_status_type == 1

Expression...

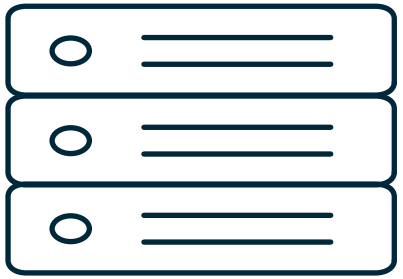
No.	Time	Source	Destination	Protocol	Length	Info
411	5.318001	10.7.5.101	23.63.254.169	HTTP	151	GET /ncsi.txt HTTP/1.1
669	56.023295	10.7.5.101	46.17.46.97	HTTP	143	GET /iwq/wpsk.php?l=sweb1.ks HTTP/1.1
1228	93.262992	10.7.5.101	185.193.141.176	HTTP	483	GET /images/j_2FVkdyLXplV3t0gVT7L/TjgGVMY8iHYhVPvZ/NQXjmlB1I7d1_2F/CAmGJCAUh…
1288	221.823565	10.7.5.101	185.193.141.176	HTTP	480	GET /images/bbVaCAPEQENgJyTYaVnu5YR/yonkCBAXAe/uhW3LYAaW49_2BoA3/OGEpO1lhYUD…
1318	350.121363	10.7.5.101	185.193.141.176	HTTP	489	GET /images/AigmunzrbVGrOWUeCar_2B/v7GYEyUBNyPDN/M3G_2B_2/FSTfN_2FNSK9l_2FVr…
1358	478.053769	10.7.5.101	185.193.141.176	HTTP	482	GET /images/m0vh_2B6i0_2FM60Y/Oc4JTO5vYTZF/tpbhTGT0cjD/6aaKm2z6VRHowx/8a07b9…
1393	605.897747	10.7.5.101	185.193.141.176	HTTP	481	GET /images/YF051sbV/yncOM42Ypc9qOZYxivJu3jS/7k913TZ8yk/LZB4udjxu3RKhC9zY/SY…
1427	735.432033	10.7.5.101	185.193.141.176	HTTP	513	GET /images/PGqvwejUwniohAzCjs_2/ByYXS9OS3aq18lB_2Fi/cR0Y_2FwpNM2zAP_2FW5VM/…
1456	863.680148	10.7.5.101	185.193.141.176	HTTP	511	GET /images/n4NrfwgRU6eTD5K/4G0cYTuFpwYbJ_2B3f/Bo119e08T/lcqV3W0_2BEnd0VH4LY…
1515	992.006399	10.7.5.101	185.193.141.176	HTTP	477	GET /images/54Z195apJNlRL2HktcnG8/UR2eAP9DhUx36bjG/H1KdB3is5tYjcP8/Sel8nGw6M…
1762	993.783840	10.7.5.101	185.193.141.176	HTTP	311	GET /favicon.ico HTTP/1.1
1776	994.729720	10.7.5.101	185.193.141.176	HTTP	504	GET /images/FlGlkgmIAcOmzMT82/4hul8ROMPWo_/2Fib_2BipNJ/FHHGTpeZdjehbD/sSAAgb…
2057	997.712908	10.7.5.101	185.193.141.176	HTTP	506	GET /images/Q8STmlHVfHQRZ3vnOww/C_2FlnH_2BUcOpOFhDy8Q3/EKe7wcd8cCgn9/hQzu_2F…
2119	1064.624216	10.7.5.101	104.24.105.145	HTTP	259	GET /wp-content/uploads/2019/07/2asiudqi123.rar HTTP/1.1
2510	1217.584445	10.7.5.101	216.239.32.21	HTTP	251	GET /raw HTTP/1.1
4553	1304.500127	10.7.5.101	170.238.117.187	HTTP	315	POST /fol1/ZARAGOZA-WIN-PC_W617601.E516FA6B9633D03926E151728B469CFF/81/ HTTP…
4571	1307.035648	10.7.5.101	170.238.117.187	HTTP	383	POST /fol1/ZARAGOZA-WIN-PC_W617601.E516FA6B9633D03926E151728B469CFF/83/ HTTP…
4596	1310.052770	10.7.5.101	170.238.117.187	HTTP	313	POST /fol1/ZARAGOZA-WIN-PC_W617601.E516FA6B9633D03926E151728B469CFF/81/ HTTP…
4713	1364.920768	10.7.5.101	185.42.104.157	HTTP	257	GET /wp-content/uploads/2019/07/asiudqi123.rar HTTP/1.1
5723	1403.831004	10.7.5.101	170.238.117.187	HTTP	700	POST /fol1/ZARAGOZA-WIN-PC_W617601.E516FA6B9633D03926E151728B469CFF/90 HTTP/…
6584	1513.830862	10.7.5.101	170.238.117.187	HTTP	275	POST /fol1/ZARAGOZA-WIN-PC_W617601.E516FA6B9633D03926E151728B469CFF/90 HTTP/…
6672	1584.054415	10.7.5.101	94.140.125.34	HTTP	129	GET /samagden.png HTTP/1.1
7902	1623.097900	10.7.5.101	94.140.125.34	HTTP	203	GET /trablon.png HTTP/1.1
9580	1631.898523	10.7.5.101	94.140.125.34	HTTP	204	GET /samagden.png HTTP/1.1
124…	2078.955190	10.7.5.5	170.238.117.187	HTTP	700	POST /lib516/PHANTASMEDIA-DC_W617601.BE764F3DF2C2DA0933A22F84170F948C/90 HTT…
125…	2115.069824	10.7.5.5	170.238.117.187	HTTP	340	POST /lib516/PHANTASMEDIA-DC_W617601.BE764F3DF2C2DA0933A22F84170F948C/83/ HT…
126…	2134.664332	10.7.5.5	94.140.125.34	HTTP	129	GET /samagden.png HTTP/1.1
138…	2163.794944	10.7.5.5	170.238.117.187	HTTP	326	POST /lib516/PHANTASMEDIA-DC_W617601.BE764F3DF2C2DA0933A22F84170F948C/81/ HT…
139…	2164.662049	10.7.5.5	94.140.125.34	HTTP	203	GET /trablon.png HTTP/1.1
141…	2169.083347	10.7.5.5	170.238.117.187	HTTP	259	POST /lib516/PHANTASMEDIA-DC_W617601.BE764F3DF2C2DA0933A22F84170F948C/90 HTT…
145…	2177.475559	10.7.5.5	94.140.125.34	HTTP	204	GET /samagden.png HTTP/1.1

Ursnif traffic

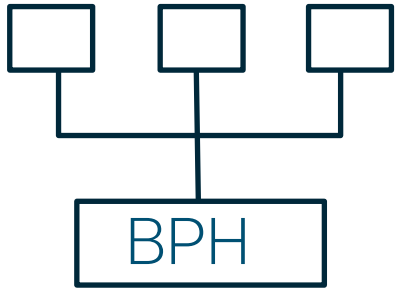
TrickBot traffic

Ursnif C2 infrastructure

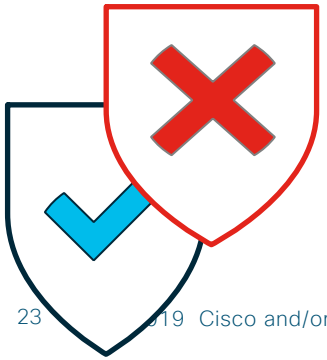
Protection Mechanisms



Abuse of legitimate third party cloud and hosting providers



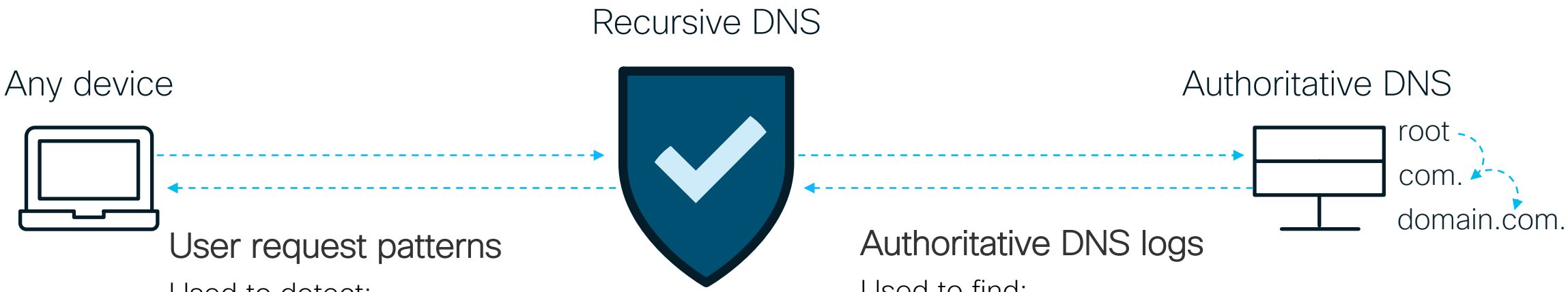
Have only upstream peers, no downstream



Domain shadowing(domain is on legitimate provider, subdomain is on BPH

Designing the Defense

Gathering Intelligence at the DNS Layer



User request patterns

Used to detect:

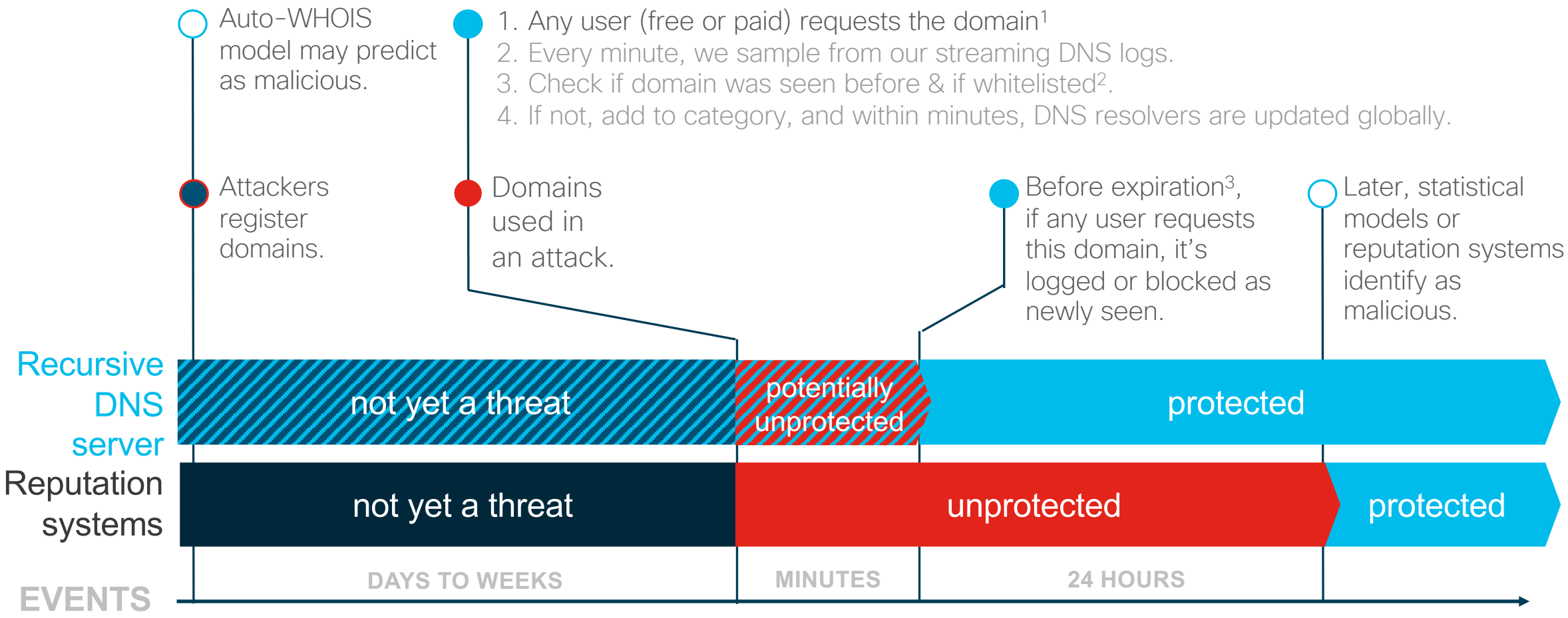
- Compromised systems
- Command and control callbacks
- Algorithm-generated domains
- Domain co-occurrences
- Newly seen domains

Authoritative DNS logs

Used to find:

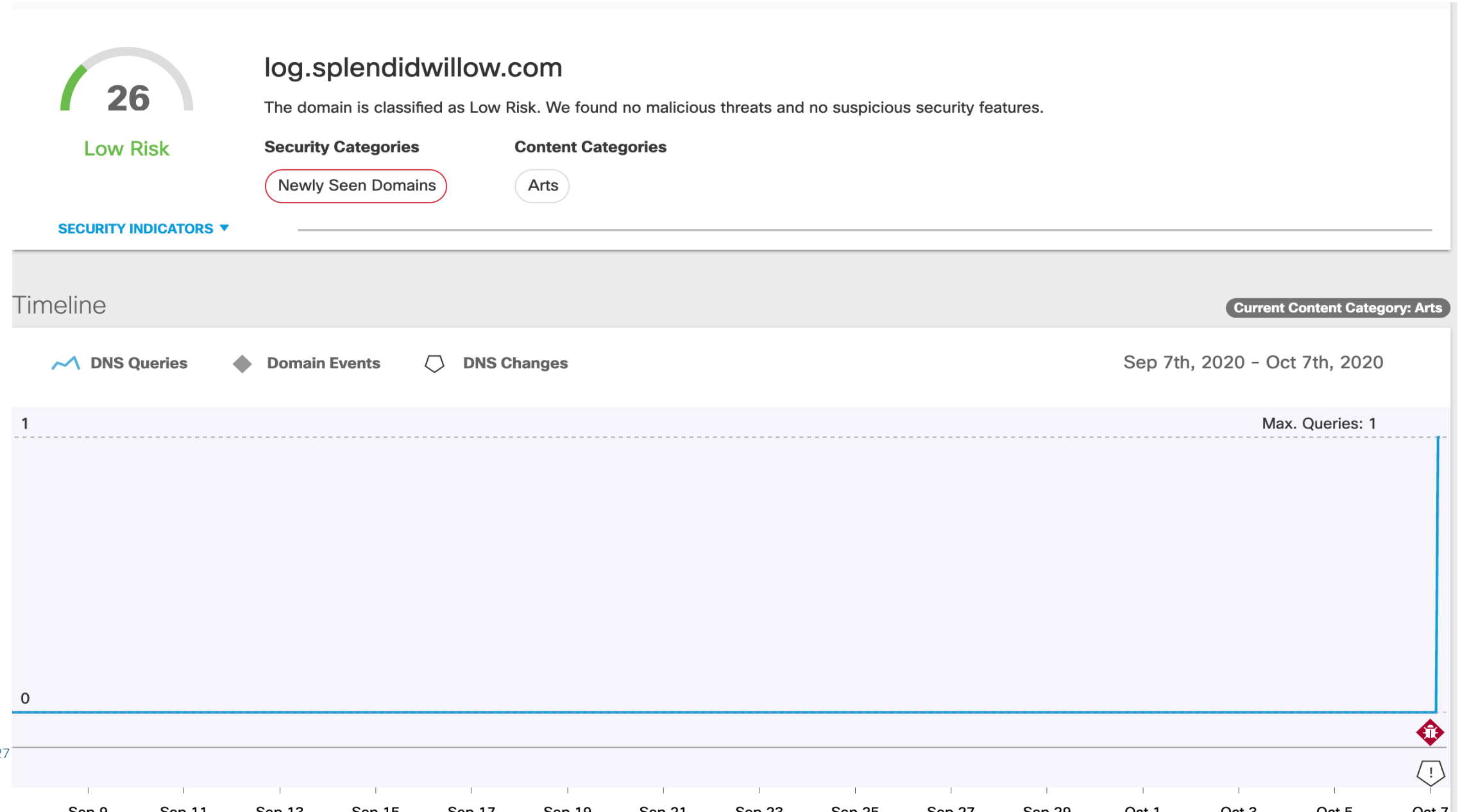
- Newly staged infrastructures
- Malicious domains, IPs, ASNs
- BulletProofHostings

Newly Seen Domains Category Reduces Risk of the Unknown



1. May have predictively blocked it already, and likely the first requestor was a free user.
2. E.g. domain generated for CDN service.
3. Usually 24 hours, but modified for best results, as needed.

Domain is flagged as Newly Seen



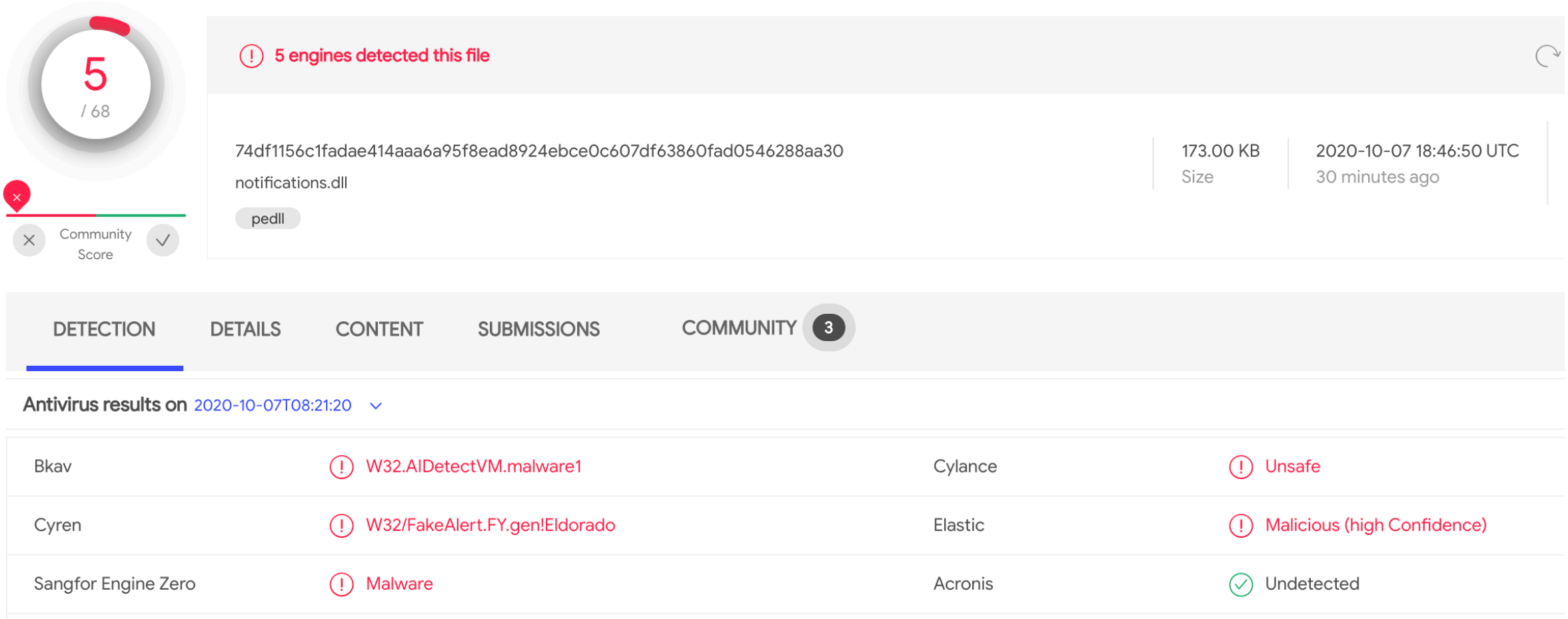
Using OSINT to analyze domain

URLs

Scanned	Detections	URL
2020-10-07	2 / 79	http://log.splendidwillow.com/notifications.dll
2020-10-07	3 / 79	https://log.splendidwillow.com/
2020-10-07	4 / 79	http://log.splendidwillow.com/notifications.dll/

Only few vendors recognize domain as malicious

Early detection of the endpoint is also low



Domain shadowing used for evasion

Malicious IPs

log.splendidwillow.com INVESTIGATE BACK TO TOP

50.31.1.31	14400	October 7, 2020	October 7, 2020

stats.splendidwillow.com INVESTIGATE BACK TO TOP

IP	Security Category	TTL (seconds)	First Seen	Last Seen
109.248.203.40		14400	October 7, 2020	October 7, 2020

Legitimate IPs

splendidwillow.com INVESTIGATE BACK TO TOP

50.87.253.158	3600 - 14400	June 5, 2020	October 7, 2020
193.233.30.117	3600	July 5, 2020	October 6, 2020
69.89.31.229	14400	March 25, 2018	June 4, 2020
108.179.228.213	14400	June 9, 2017	March 24, 2018
74.220.199.6	60	May 19, 2017	March 22, 2018

Same technique used by C&C

Malicious IPs

web.synizstore.com INVESTIGATE BACK TO TOP

IP	Security Category	TTL (seconds)	First Seen	Last Seen
185.98.87.159		14400	October 6, 2020	October 7, 2020
195.24.65.73	Malware	14400	October 6, 2020	October 7, 2020

Legitimate IPs

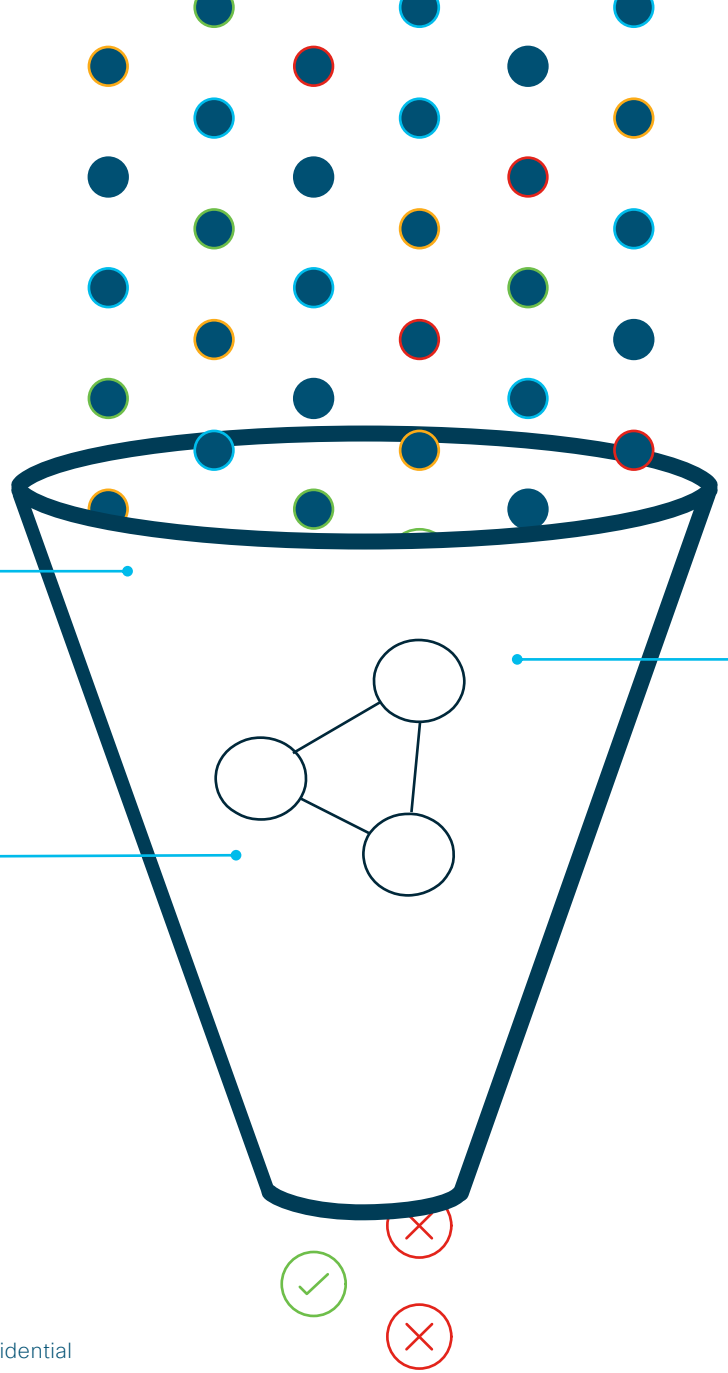
synizstore.com INVESTIGATE BACK TO TOP

IP	Security Category	TTL (seconds)	First Seen	Last Seen
162.241.224.143		11709 - 14400	July 29, 2018	October 7, 2020
18.213.250.117		300	July 1, 2019	July 19, 2020
18.215.128.143		300	July 1, 2019	July 19, 2020
52.4.209.250		300	July 1, 2019	July 19, 2020

Bullet Proof Hosted Infrastructure

188.130.138.0/23	Russian Federation	grandmain.ru zeroportal.ru taxi-elite.ru line.hotelcabosanlorenzo.com link.fixuppropertysolutions.com log.whateverittakesdoc.org service.21stcenturyleadersawards.org stats.21stcentury-leadership.org corona-pay.online stats.softoptions.com line.republicpracticesolutions.com link.republichealthresources.com service.heritageimagingcenter.com
185.244.40.0/22	Russian Federation	web.coryriley.com line.tdrcoastalhomes.com link.hybridcorehomescc.com log.newhybridhome.com
109.248.200.0/22	Russian Federation	theimajing.com zeroauthentaction.org web.fromtheeast.org web.kundertviolas.com
109.248.10.0/23	Russian Federation	uacujgnkrqpmjiwfb.com mwbsgpeaty.com sbqvopddilae.com pvalavol.com mfqiugrume.com hotphonecall.xyz web.brookmeggs.com web.zdesigns-studio.net gstat.rayzacastillo.com gooodburber.agency torrobonitp.today log.angelicabrown.com service.drnjithendran.com stats.charleswbrownonline.com link.panibaba.com line.queensfurnitureoutlet.com link.giantfurnitureoutlet.com log.idealfurnituredirect.com service.idealfurnitureoutlet.com stats.idealfurnituregalleryny.com corona-payments.online covid-payments.online

Using DNS as added layer of protection



Guilt by inference

- Co-occurrence model
- Sender rank model

Guilt by association

- Predictive IP Space Modeling
- Passive DNS and WHOIS Correlation

Patterns of guilt

- Spike rank model
- DGA prediction
- Clustering

Questions?

@armcbride1
aumcbrid@cisco.com

@Mesiagh
artholub@cisco.com

www.umbrella.cisco.com