Secutec
Cyber security intelligence

Geert Baudewijns

CEO – Founder

Negotiater Cybercrime

Facts and Figures

14M

14 Mil. €

+500k

ENDPOINTS SECURED

650

CUSTOMERS

65E

65 Employees

22Y

EXPERIENCE IN CYBER SECURITY

Secutec
Cyber security intelligence

Focal Services

Services

Audits

E-mail & File Analyse

Secure DNS

Integrated Advanced Malware (SIAM)

Anti-phishing

Darknet Research

Home-use

Support

Managed services

Security Operations Center (SOC)

Secutec
Cyber security intelligence

Our Partners

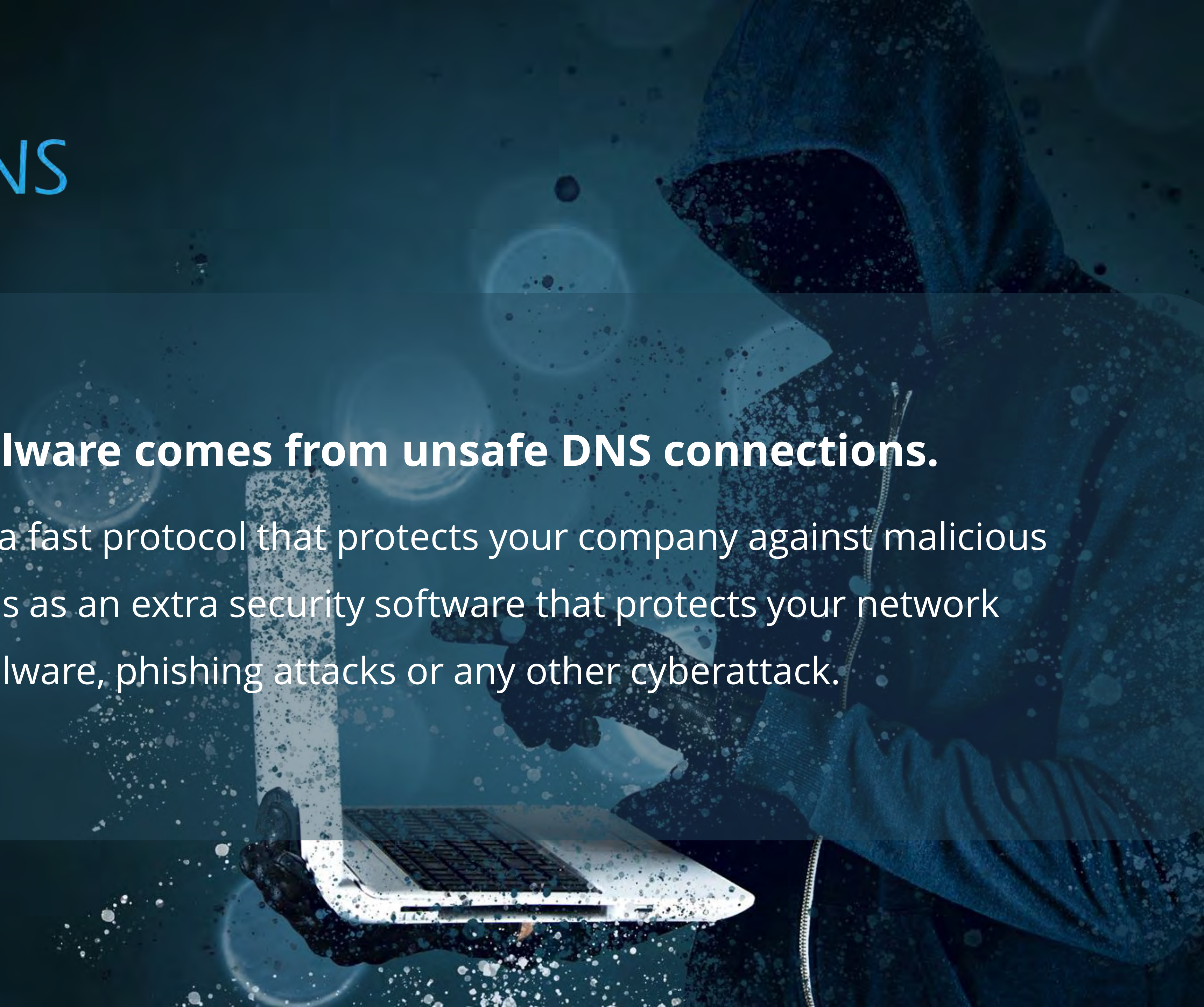
SpyCloud DOMAINTOOLS Recorded Future INTEL471

BITSIGHT McAfee SOPHOS kaspersky FARSIGHT SECURITY

TREND MICRO Check Point SOFTWARE TECHNOLOGIES Symantec FORTINET

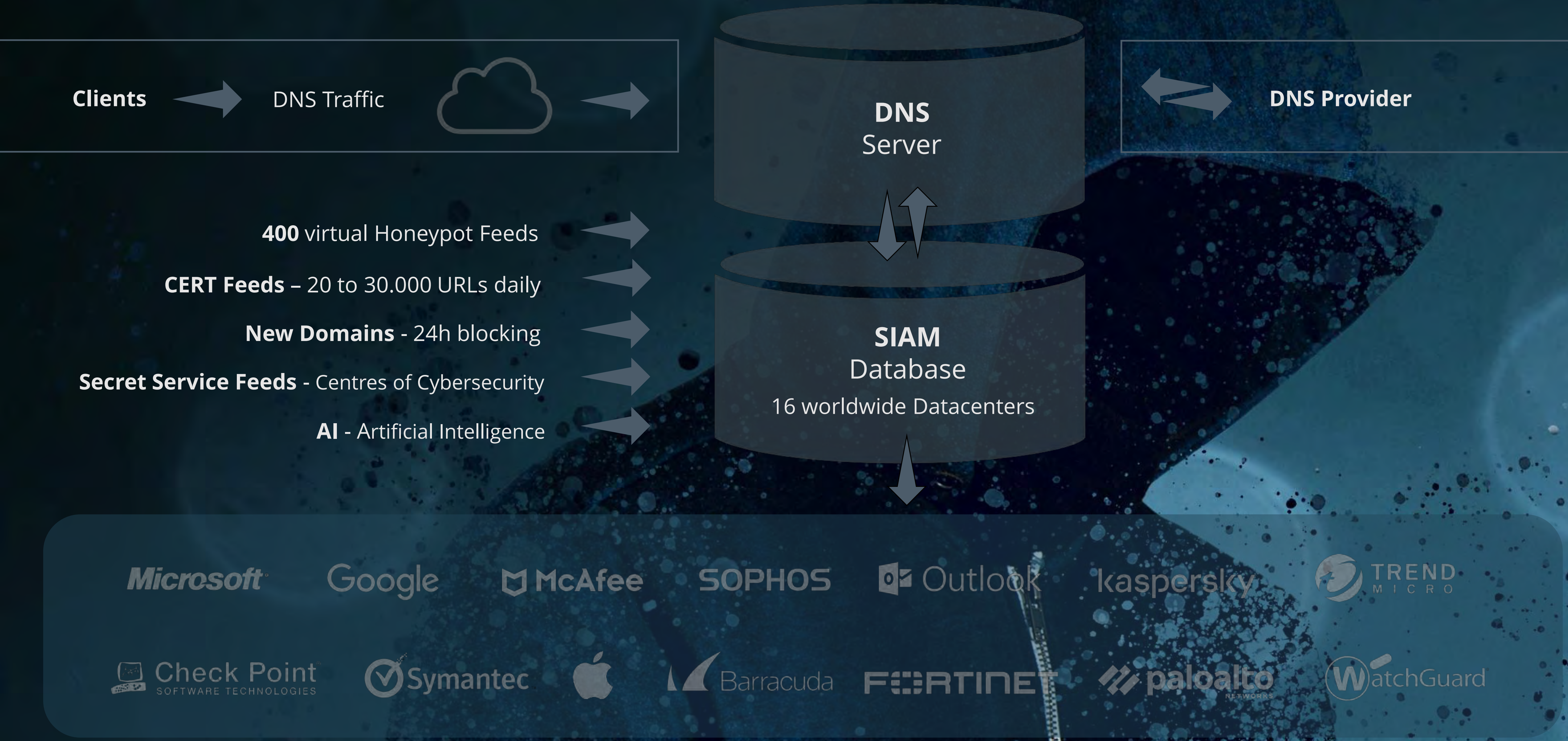
Barracuda paloalto NETWORKS WatchGuard CROWDSTRIKE secureDNS

secureDNS



91% of all malware comes from unsafe DNS connections.

Secutec Secure DNS is a fast protocol that protects your company against malicious host names. It serves as an extra security software that protects your network against malware, phishing attacks or any other cyberattack.



Clients → DNS Traffic →

DNS Server

DNS Provider

400 virtual Honeypot Feeds

CERT Feeds – 20 to 30.000 URLs daily

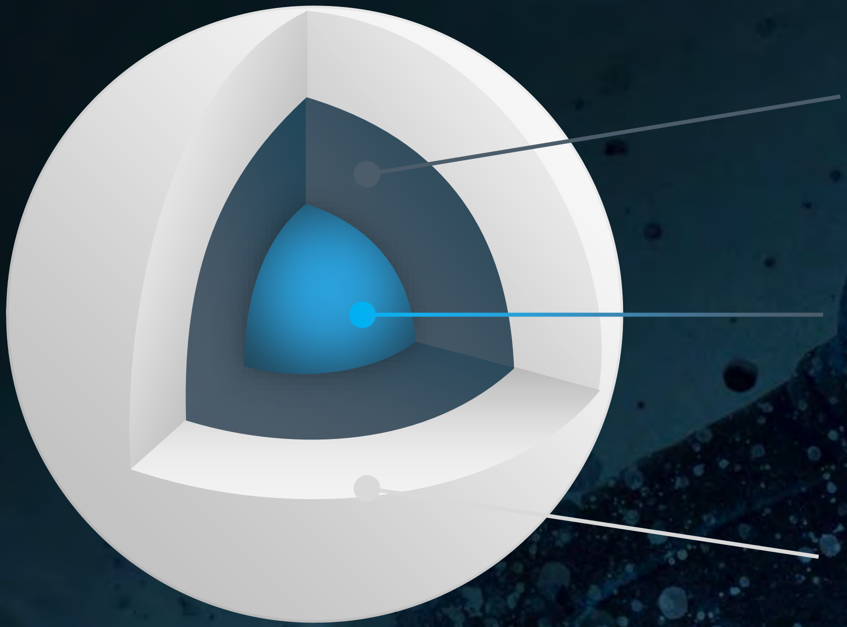
New Domains - 24h blocking

Secret Service Feeds - Centres of Cybersecurity

AI - Artificial Intelligence

SIAM Database

16 worldwide Datacenters



40% Technology

30% Database and Intelligence

30% Experts / Data Analyses

Benefits secureDNS

Block faster – detect more – prevent proactively

- Reporting dashboard
- High-performant security service
- Complete network security
- SOC alerts – malicious detections immediately reported

Peace of mind

- Support within 24 hours
- Implementation in less than 60 minutes

Benefits secureDNS

Easy to implement

-System independent
-Seamless infrastructure integration
-No additional hardware or software required

A safe team, wherever they work

-Safe web browsing guaranteed
-Fast connections assured
-Remote and mobile cybersafety
-We keep all your devices safe

Database

SIAM Database with
35 worldwide vendors.

Vendor Database 60-90MB
Secutec Database 410 GB

Speed

Integration
20.000-30.000 daily
CERT Feeds

several hours
of time savings

Analysts

40 Data Analysts
monitore 7/24
all data

Active information
in the event of a threat

Darknet

A Kombination with
Darknet Monitoring
is possible

Secutec monitors 99%
of bad traffic connections
worldwide

New Domain

New Domain
blocking for the
first 24 hours

More than 22% of all
newly registered domains
are used for cyber crime

False Positive

108 Mio. daily
DNS-requests
monitored

Only 1 x
false positive
per month

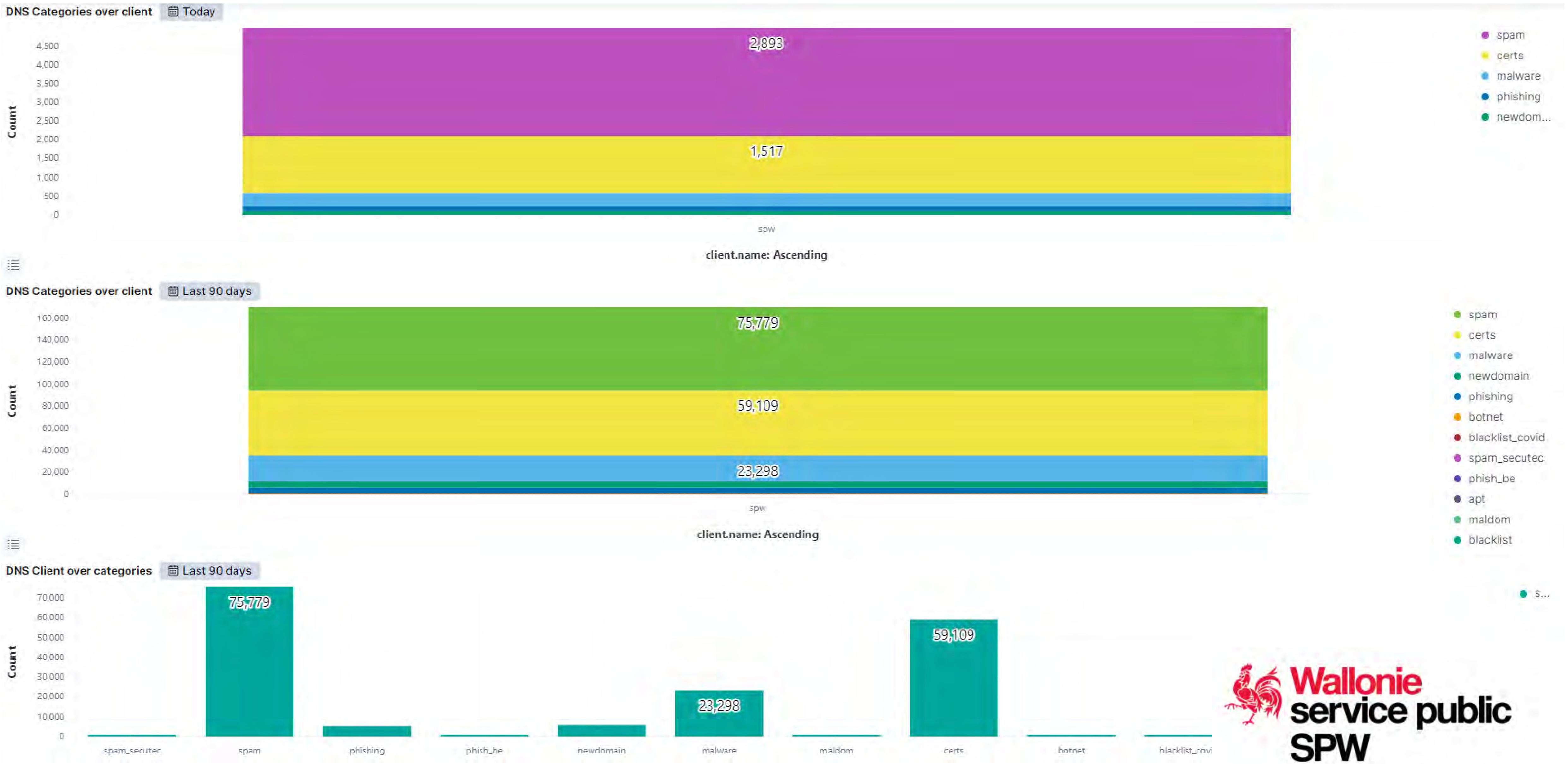
secureDNS

added value

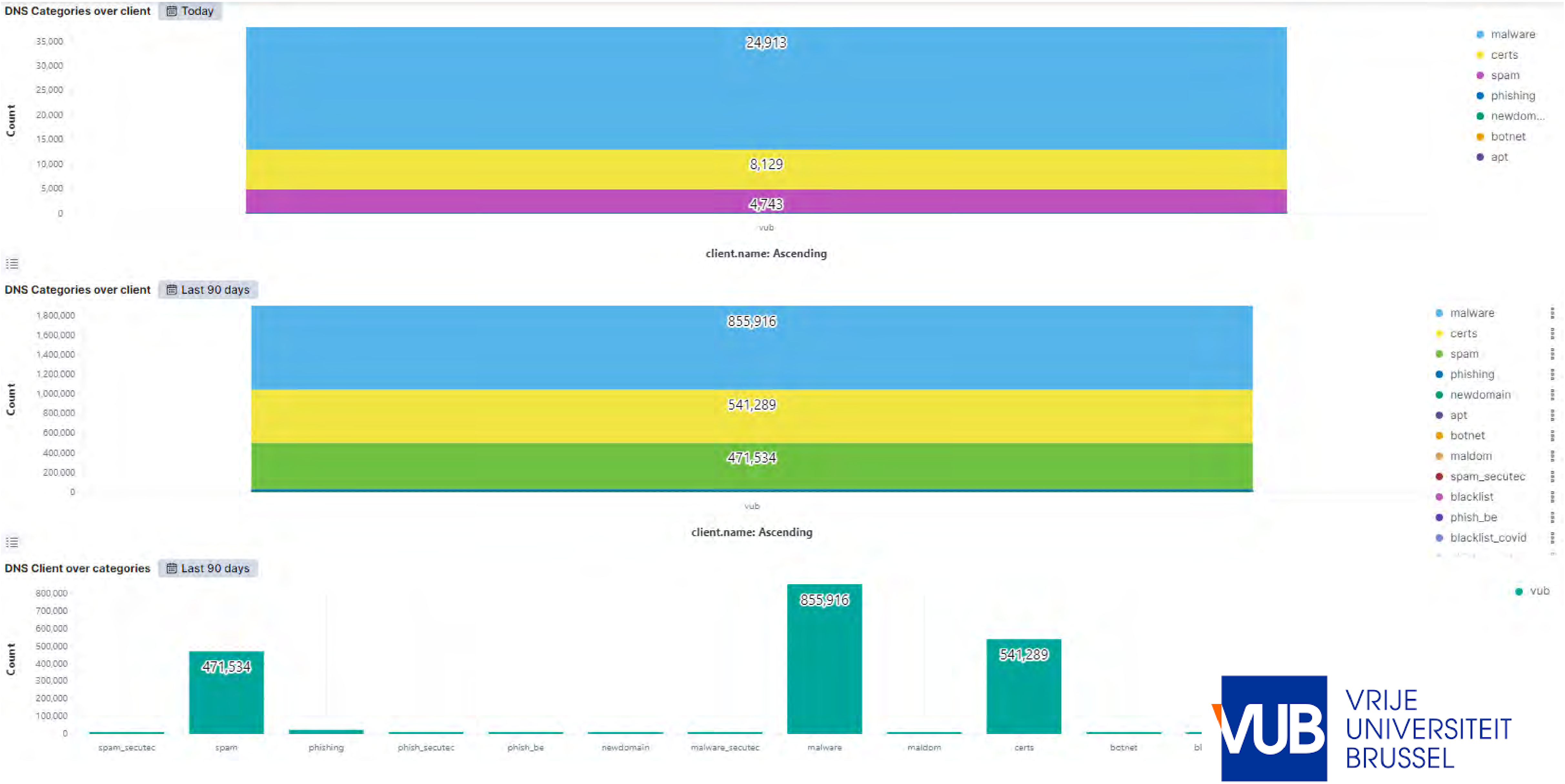
Holistic

secureDNS
= outbound traffic

secureSIGHT
= inbound traffic
+ Clear-Web
+Deep-Web
+Darknet



Wallonie
service public
SPW

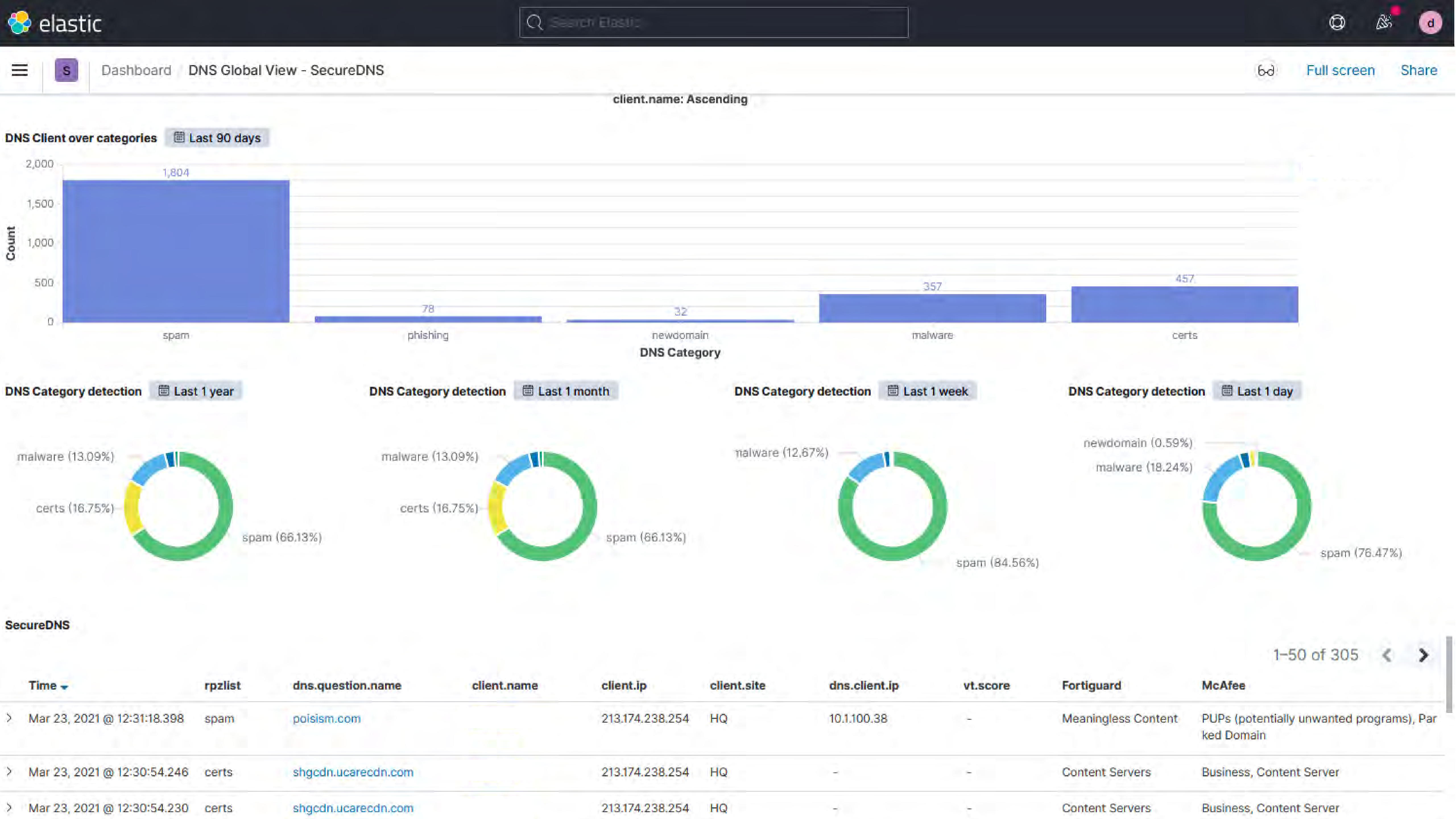


DNS Categories over client — Today

DNS Categories over client — Last 90 days

DNS Client over categories — Last 90 days

VRIJE
UNIVERSITEIT
BRUSSEL



client.name: Ascending

DNS Client over categories — Last 90 days

DNS Category detection — Last 1 year

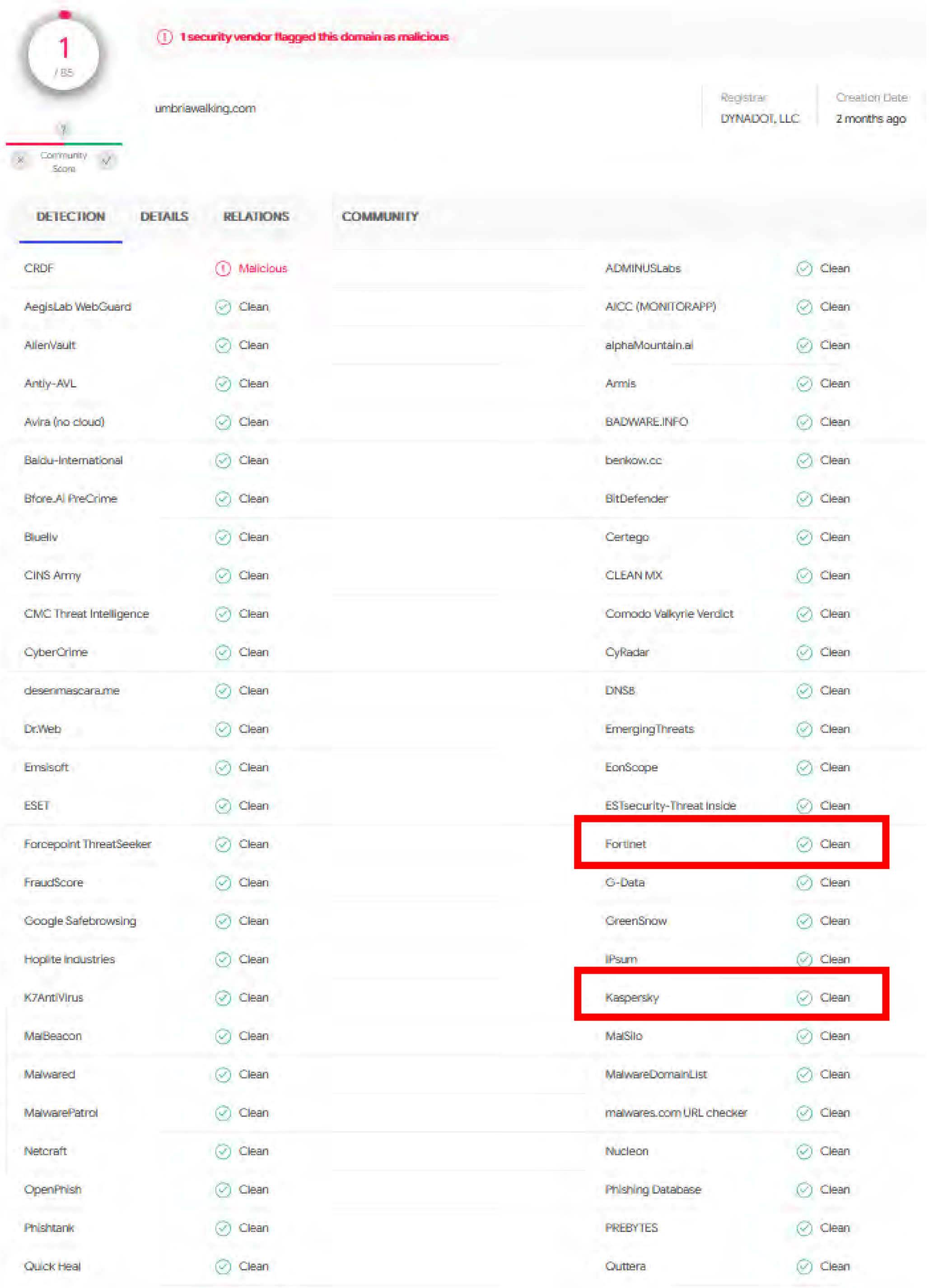
DNS Category detection — Last 1 month

DNS Category detection — Last 1 week

DNS Category detection — Last 1 day

SecureDNS

Time	rpzlist	dns.question.name	client.name	client.ip	client.site	dns.client.ip	vt.score	Fortiguard	McAfee
Mar 23, 2021 @ 12:31:18.398	spam	poisism.com		213.174.238.254	HQ	10.1.100.38	-	Meaningless Content	PUPs (potentially unwanted programs), Parked Domain
Mar 23, 2021 @ 12:30:54.246	certs	shgcdn.ucarecdn.com		213.174.238.254	HQ	-	-	Content Servers	Business, Content Server
Mar 23, 2021 @ 12:30:54.230	certs	shgcdn.ucarecdn.com		213.174.238.254	HQ	-	-	Content Servers	Business, Content Server



1
/ 85

? Community Score

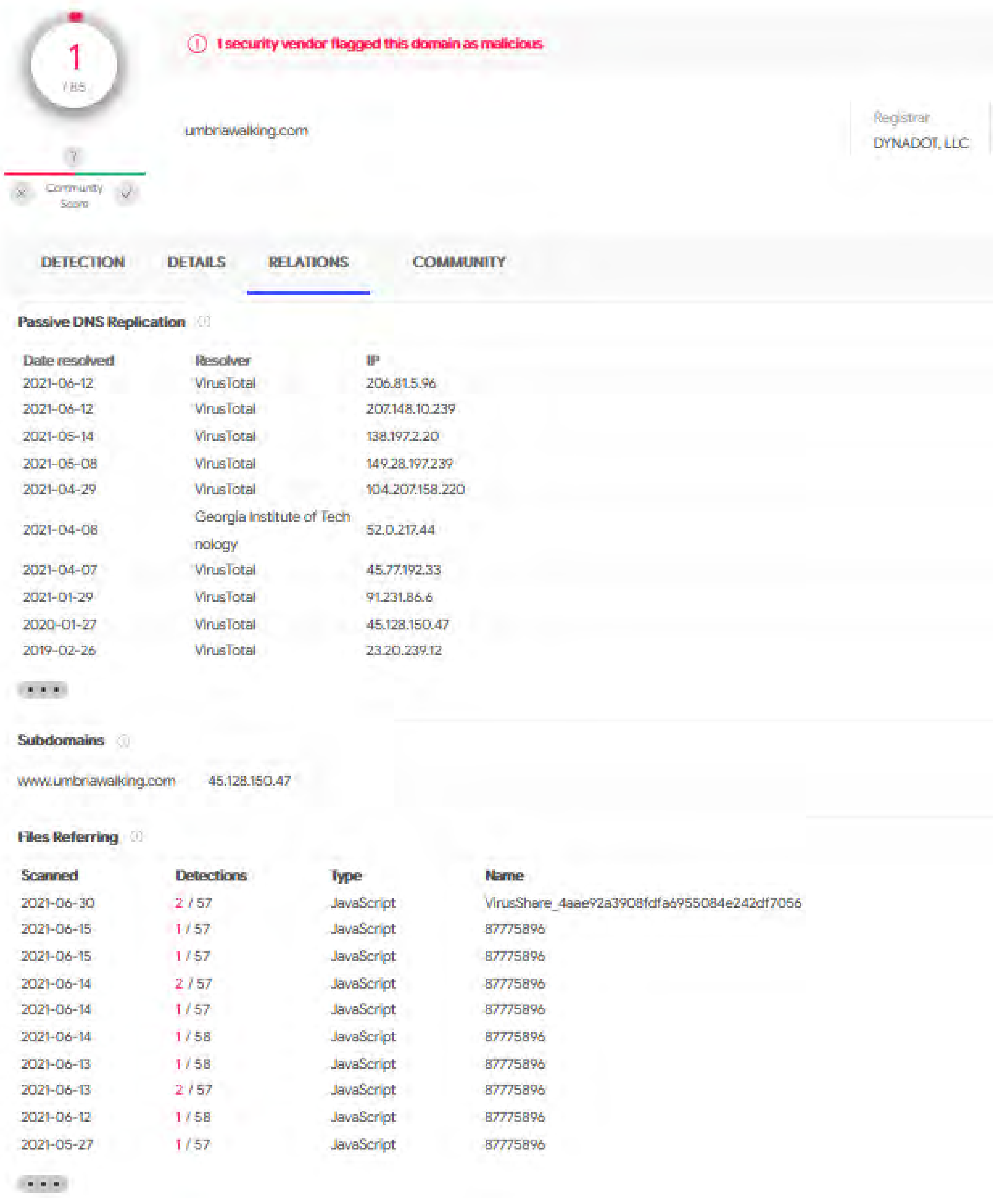
1 security vendor flagged this domain as malicious

umbriawalking.com

Registrar
DYNADOT, LLC

Creation Date
2 months ago

CRDF	Malicious	ADMINUSLabs	Clean
AegisLab WebGuard	Clean	AICC (MONITORAPP)	Clean
AlienVault	Clean	alphaMountain.ai	Clean
Antiy-AVL	Clean	Armis	Clean
Avira (no cloud)	Clean	BADWARE.INFO	Clean
Baidu-International	Clean	benkow.cc	Clean
Bfore.Ai PreCrime	Clean	BitDefender	Clean
Blueliv	Clean	Certego	Clean
CINS Army	Clean	CLEAN MX	Clean
CMC Threat Intelligence	Clean	Comodo Valkyrie Verdict	Clean
CyberCrime	Clean	CyRadar	Clean
desenmascara.me	Clean	DNS8	Clean
Dr.Web	Clean	EmergingThreats	Clean
Emsisoft	Clean	EonScope	Clean
ESET	Clean	ESTsecurity-Threat Inside	Clean
Forcepoint ThreatSeeker	Clean	Fortinet	Clean
FraudScore	Clean	G-Data	Clean
Google Safebrowsing	Clean	GreenSnow	Clean
Hoplite Industries	Clean	IPsum	Clean
K7AntiVirus	Clean	Kaspersky	Clean
MalBeacon	Clean	MalSilo	Clean
Malwared	Clean	MalwareDomainList	Clean
MalwarePatrol	Clean	malwares.com URL checker	Clean
Netcraft	Clean	Nucleon	Clean
OpenPhish	Clean	Phishing Database	Clean
Phishtank	Clean	PREBYTES	Clean
Quick Heal	Clean	Quttera	Clean



1
/ 85

? Community Score

1 security vendor flagged this domain as malicious

umbriawalking.com

Registrar
DYNADOT, LLC

Passive DNS Replication

Date resolved	Resolver	IP
2021-06-12	VirusTotal	206.81.5.96
2021-06-12	VirusTotal	207.148.10.239
2021-05-14	VirusTotal	138.197.2.20
2021-05-08	VirusTotal	149.28.197.239
2021-04-29	VirusTotal	104.207.158.220
2021-04-08	Georgia Institute of Technology	52.0.217.44
2021-04-07	VirusTotal	45.77.192.33
2021-01-29	VirusTotal	91.231.86.6
2020-01-27	VirusTotal	45.128.150.47
2019-02-26	VirusTotal	23.20.239.12

• • •

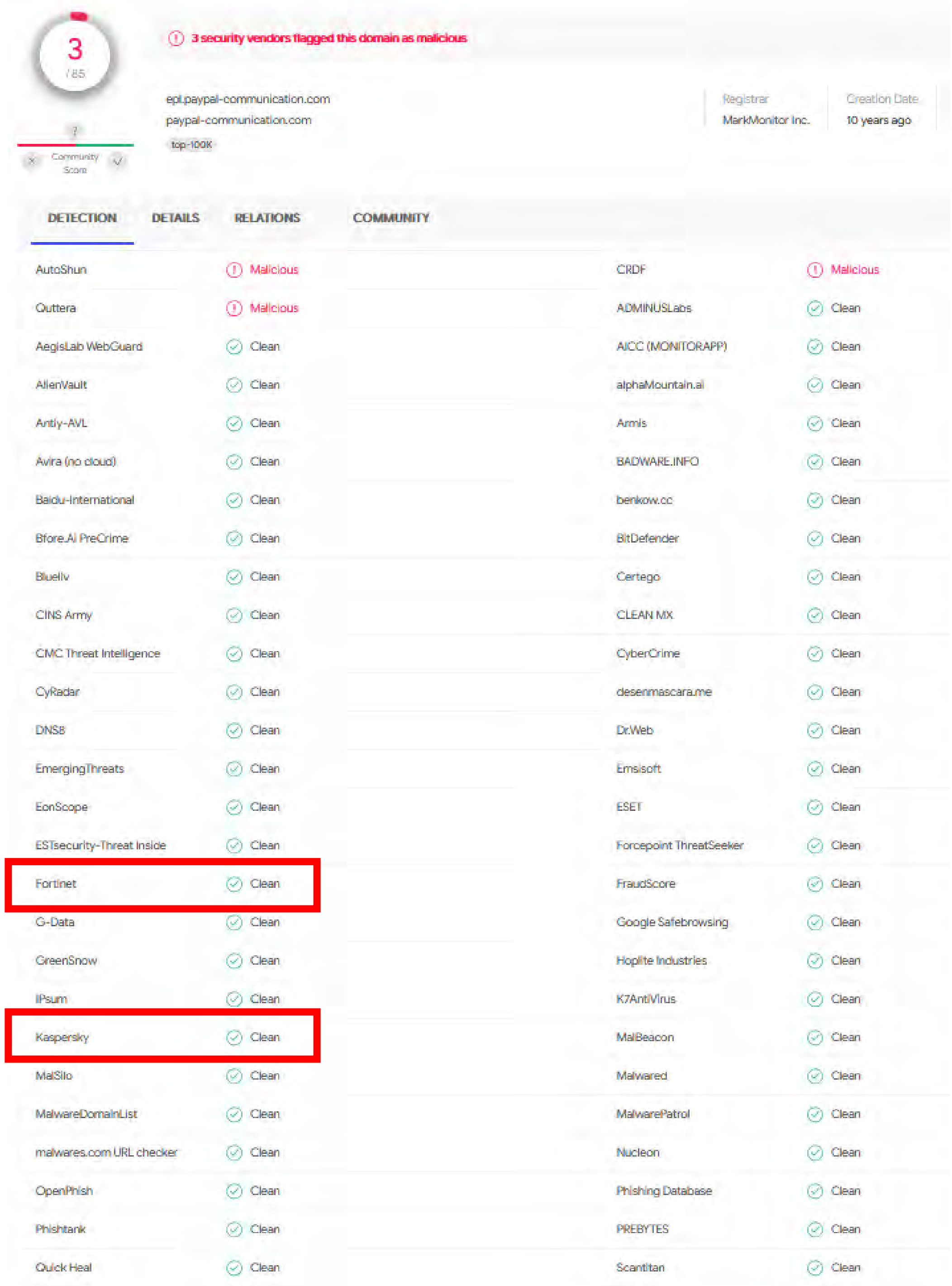
Subdomains

www.umbriawalking.com	45.128.150.47

Files Referring

Scanned	Detections	Type	Name
2021-06-30	2 / 57	JavaScript	VirusShare_4aae92a3908fdfa6955084e242df7056
2021-06-15	1 / 57	JavaScript	87775896
2021-06-15	1 / 57	JavaScript	87775896
2021-06-14	2 / 57	JavaScript	87775896
2021-06-14	1 / 57	JavaScript	87775896
2021-06-14	1 / 58	JavaScript	87775896
2021-06-13	1 / 58	JavaScript	87775896
2021-06-13	2 / 57	JavaScript	87775896
2021-06-12	1 / 58	JavaScript	87775896
2021-05-27	1 / 57	JavaScript	87775896

• • •



3
/ 85

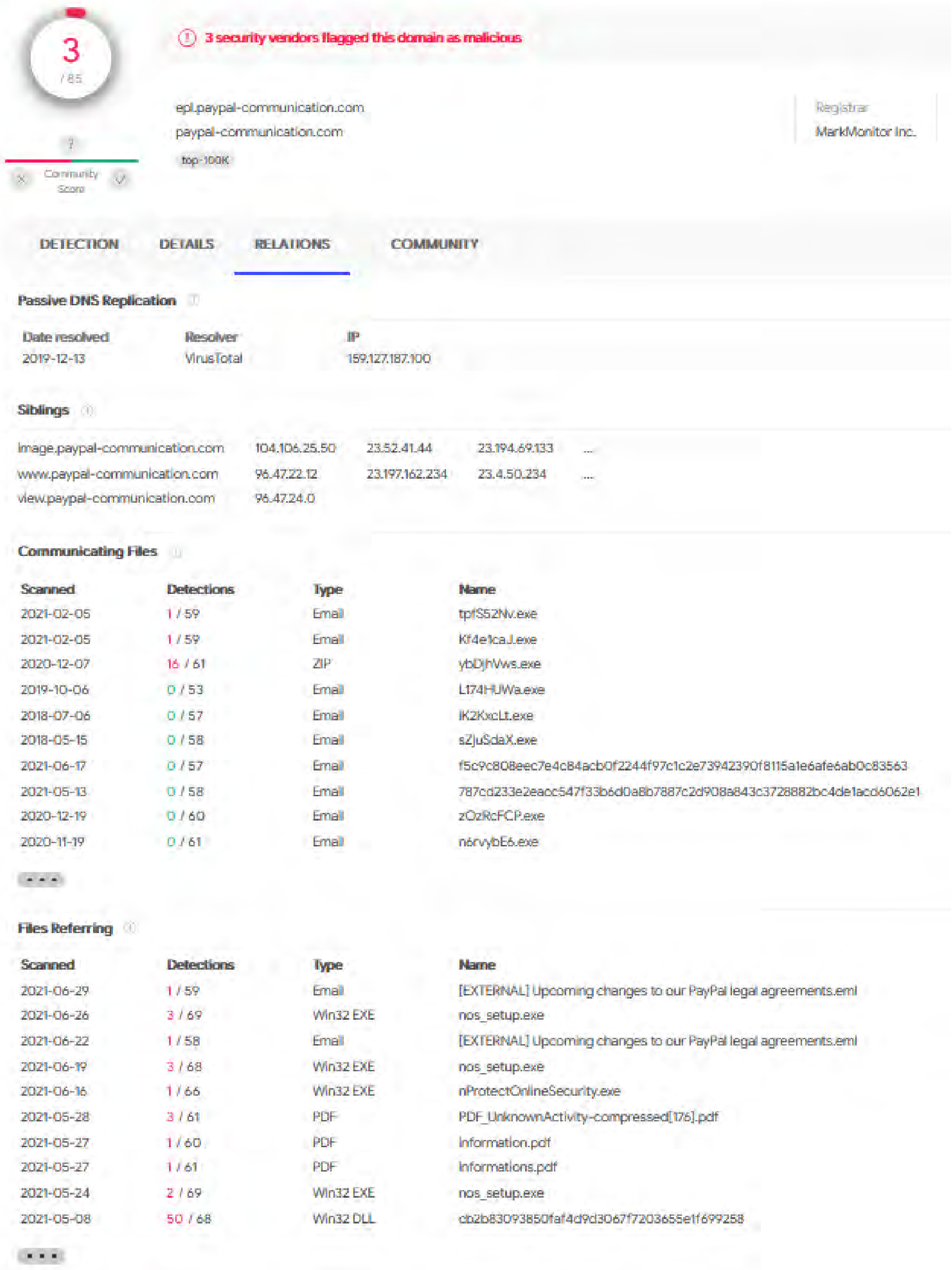
! 3 security vendors flagged this domain as malicious

epl.paypal-communication.com
paypal-communication.com
top-100K

Registrar
MarkMonitor Inc.

Creation Date
10 years ago

AutoShun	Malicious	CRDF	Malicious
Quttera	Malicious	ADMINUSLabs	Clean
AegisLab WebGuard	Clean	AICC (MONITORAPP)	Clean
AlienVault	Clean	alphaMountain.ai	Clean
Antiy-AVL	Clean	Armis	Clean
Avira (no cloud)	Clean	BADWARE.INFO	Clean
Baidu-International	Clean	benkow.cc	Clean
Bfore.Ai PreCrime	Clean	BitDefender	Clean
Bluellv	Clean	Certego	Clean
CINS Army	Clean	CLEAN MX	Clean
CMC Threat Intelligence	Clean	CyberCrime	Clean
CyRadar	Clean	desenmascara.me	Clean
DNS8	Clean	Dr.Web	Clean
EmergingThreats	Clean	Emsisoft	Clean
EonScope	Clean	ESET	Clean
ESTsecurity-Threat Inside	Clean	Forcepoint ThreatSeeker	Clean
Fortinet	Clean	FraudScore	Clean
G-Data	Clean	Google Safebrowsing	Clean
GreenSnow	Clean	Hoplite Industries	Clean
IPsum	Clean	K7AntiVirus	Clean
Kaspersky	Clean	MalBeacon	Clean
MalSilo	Clean	Malwared	Clean
MalwareDomainList	Clean	MalwarePatrol	Clean
malwares.com URL checker	Clean	Nucleon	Clean
OpenPhish	Clean	Phishing Database	Clean
Phishtank	Clean	PREBYTES	Clean
Quick Heal	Clean	Scantitan	Clean



3
/ 85

! 3 security vendors flagged this domain as malicious

epl.paypal-communication.com
paypal-communication.com
top-100K

Registrar
MarkMonitor Inc.

Passive DNS Replication

Date resolved	Resolver	IP
2019-12-13	VirusTotal	159.127.187.100

Siblings

image.paypal-communication.com	104.106.25.50	23.52.41.44	23.194.69.133	...
www.paypal-communication.com	96.47.22.12	23.197.162.234	23.4.50.234	...
view.paypal-communication.com	96.47.24.0			

Communicating Files

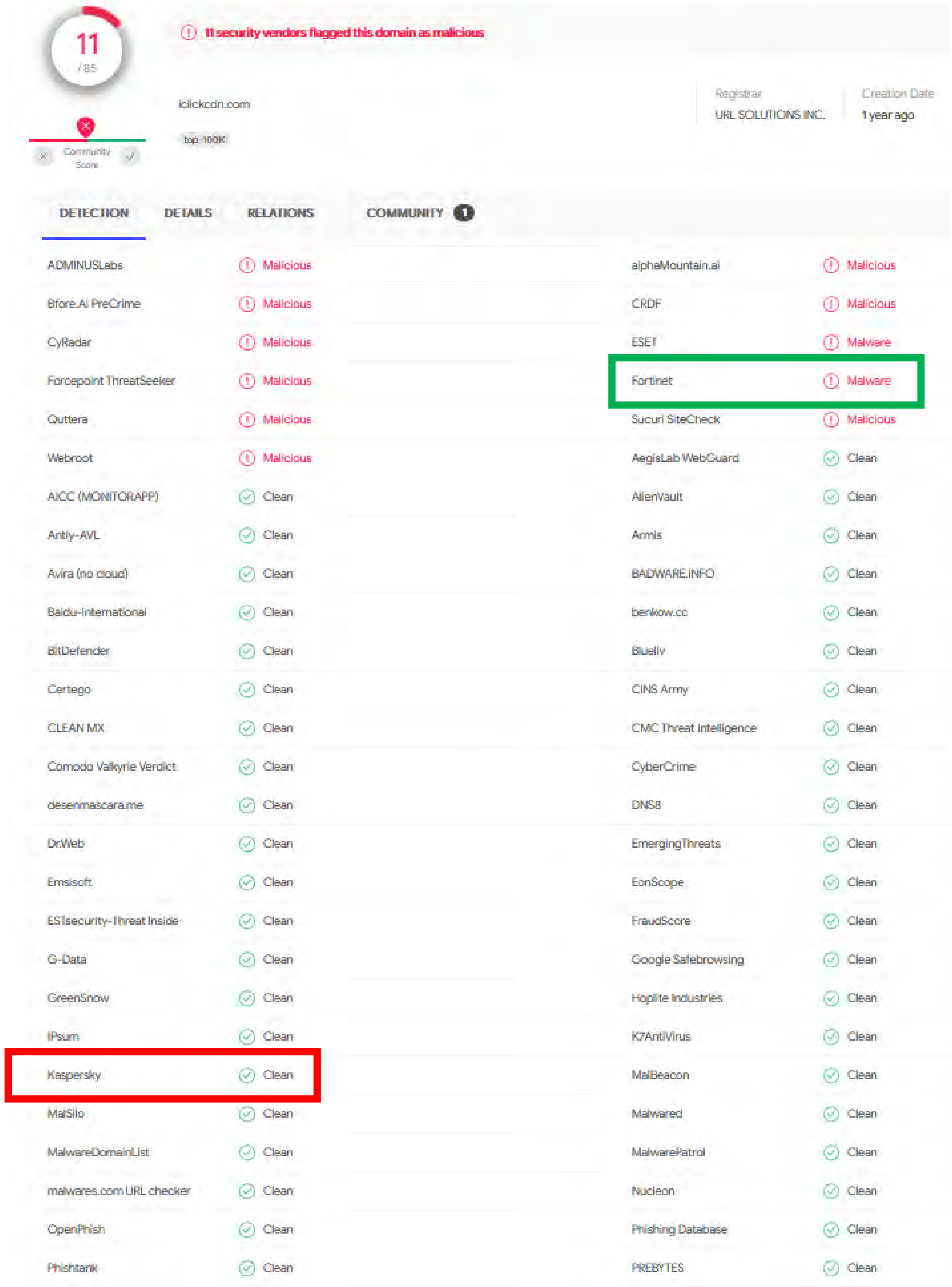
Scanned	Detections	Type	Name
2021-02-05	1 / 59	Email	tpfS52Nv.exe
2021-02-05	1 / 59	Email	Kf4e1caJ.exe
2020-12-07	16 / 61	ZIP	ybDjhVws.exe
2019-10-06	0 / 53	Email	L174HUWa.exe
2018-07-06	0 / 57	Email	lK2KxcLt.exe
2018-05-15	0 / 58	Email	sZjuSdaX.exe
2021-06-17	0 / 57	Email	f5c9c808eec7e4c84acb0f2244f97c1c2e73942390f8115a1e6afe6ab0c83563
2021-05-13	0 / 58	Email	787cd233e2eacc547f33b6d0a8b7887c2d908a843c3728882bc4de1acd6062e1
2020-12-19	0 / 60	Email	zOzRcFCP.exe
2020-11-19	0 / 61	Email	n6rvybE6.exe

• • •

Files Referring

Scanned	Detections	Type	Name
2021-06-29	1 / 59	Email	[EXTERNAL] Upcoming changes to our PayPal legal agreements.eml
2021-06-26	3 / 69	Win32 EXE	nos_setup.exe
2021-06-22	1 / 58	Email	[EXTERNAL] Upcoming changes to our PayPal legal agreements.eml
2021-06-19	3 / 68	Win32 EXE	nos_setup.exe
2021-06-16	1 / 66	Win32 EXE	nProtectOnlineSecurity.exe
2021-05-28	3 / 61	PDF	PDF_UnknownActivity-compressed[176].pdf
2021-05-27	1 / 60	PDF	information.pdf
2021-05-27	1 / 61	PDF	informations.pdf
2021-05-24	2 / 69	Win32 EXE	nos_setup.exe
2021-05-08	50 / 68	Win32 DLL	cb2b83093850faf4d9d3067f7203655e1f699258

• • •



11 security vendors flagged this domain as malicious

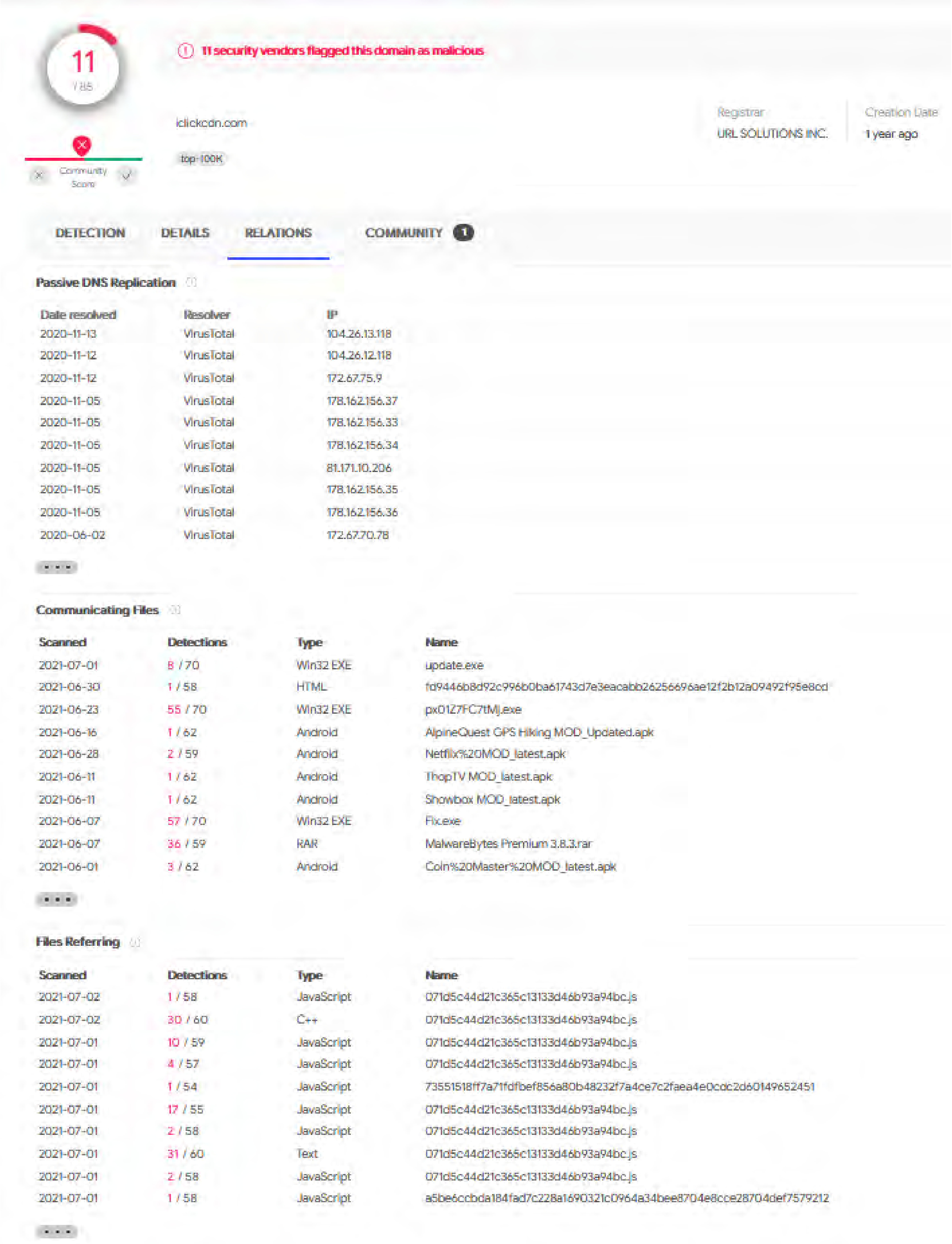
iclickcdn.com

top-100K

Registrar
URL SOLUTIONS INC.

Creation Date
1 year ago

ADMINUSLabs	Malicious	alphaMountain.ai	Malicious
Bfore.Ai PreCrime	Malicious	CRDF	Malicious
CyRadar	Malicious	ESET	Malware
Forcepoint ThreatSeeker	Malicious	Fortinet	Malware
Quttera	Malicious	Sucuri SiteCheck	Malicious
Webroot	Malicious	AegisLab WebGuard	Clean
AICC (MONITORAPP)	Clean	AlienVault	Clean
Antiy-AVL	Clean	Armis	Clean
Avira (no cloud)	Clean	BADWARE.INFO	Clean
Baidu-International	Clean	benkow.cc	Clean
BitDefender	Clean	Bluelìv	Clean
Certego	Clean	CINS Army	Clean
CLEAN MX	Clean	CMC Threat Intelligence	Clean
Comodo Valkyrie Verdict	Clean	CyberCrime	Clean
desenmascara.me	Clean	DNS8	Clean
Dr.Web	Clean	EmergingThreats	Clean
Emsisoft	Clean	EonScope	Clean
ESTsecurity-Threat Inside	Clean	FraudScore	Clean
G-Data	Clean	Google Safebrowsing	Clean
GreenSnow	Clean	Hoplite Industries	Clean
IPsum	Clean	K7AntiVirus	Clean
Kaspersky	Clean	MalBeacon	Clean
MalSilo	Clean	Malwared	Clean
MalwareDomainList	Clean	MalwarePatrol	Clean
malwares.com URL checker	Clean	Nucleon	Clean
OpenPhish	Clean	Phishing Database	Clean
Phishtank	Clean	PREBYTES	Clean



11 security vendors flagged this domain as malicious

iclickcdn.com

top-100K

Registrar
URL SOLUTIONS INC.

Creation Date
1 year ago

Passive DNS Replication

Date resolved	Resolver	IP
2020-11-13	VirusTotal	104.26.13.118
2020-11-12	VirusTotal	104.26.12.118
2020-11-12	VirusTotal	172.67.75.9
2020-11-05	VirusTotal	178.162.156.37
2020-11-05	VirusTotal	178.162.156.33
2020-11-05	VirusTotal	178.162.156.34
2020-11-05	VirusTotal	81.171.10.206
2020-11-05	VirusTotal	178.162.156.35
2020-11-05	VirusTotal	178.162.156.36
2020-06-02	VirusTotal	172.67.70.78

• • •

Communicating Files

Scanned	Detections	Type	Name
2021-07-01	8 / 70	Win32 EXE	update.exe
2021-06-30	1 / 58	HTML	fd9446b8d92c996b0ba61743d7e3eacabb26256696ae12f2b12a09492f95e8cd
2021-06-23	55 / 70	Win32 EXE	px01Z7FC7tMj.exe
2021-06-16	1 / 62	Android	AlpineQuest GPS Hiking MOD_Updated.apk
2021-06-28	2 / 59	Android	Netflix%20MOD_latest.apk
2021-06-11	1 / 62	Android	ThopTV MOD_latest.apk
2021-06-11	1 / 62	Android	Showbox MOD_latest.apk
2021-06-07	57 / 70	Win32 EXE	Fix.exe
2021-06-07	36 / 59	RAR	MalwareBytes Premium 3.8.3.rar
2021-06-01	3 / 62	Android	Coin%20Master%20MOD_latest.apk

• • •

Files Referring

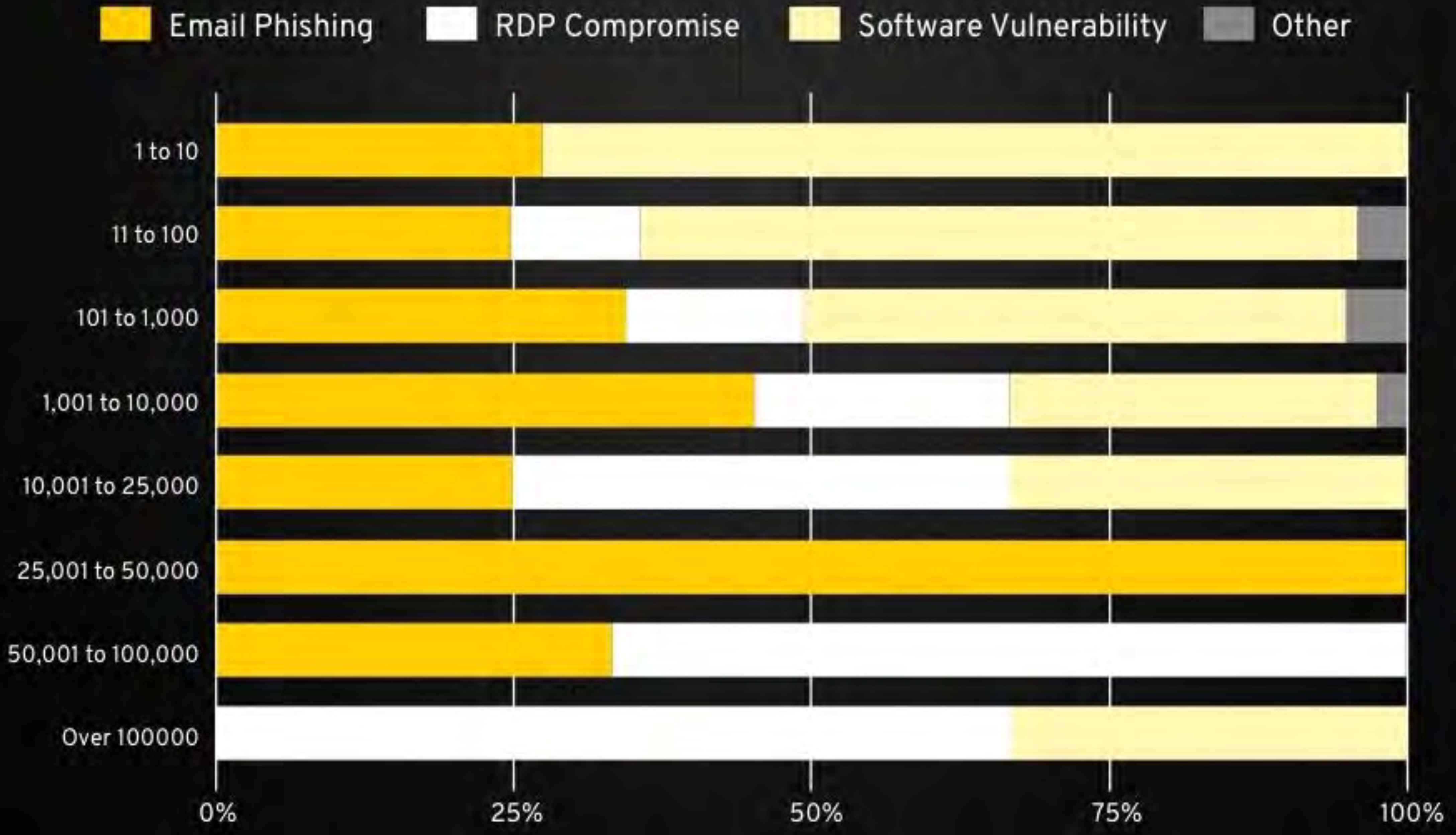
Scanned	Detections	Type	Name
2021-07-02	1 / 58	JavaScript	071d5c44d21c365c13133d46b93a94bc.js
2021-07-02	30 / 60	C++	071d5c44d21c365c13133d46b93a94bc.js
2021-07-01	10 / 59	JavaScript	071d5c44d21c365c13133d46b93a94bc.js
2021-07-01	4 / 57	JavaScript	071d5c44d21c365c13133d46b93a94bc.js
2021-07-01	1 / 54	JavaScript	73551518ff7a71fdfbef856a80b48232f7a4ce7c2faea4e0cdc2d60149652451
2021-07-01	17 / 55	JavaScript	071d5c44d21c365c13133d46b93a94bc.js
2021-07-01	2 / 58	JavaScript	071d5c44d21c365c13133d46b93a94bc.js
2021-07-01	31 / 60	Text	071d5c44d21c365c13133d46b93a94bc.js
2021-07-01	2 / 58	JavaScript	071d5c44d21c365c13133d46b93a94bc.js
2021-07-01	1 / 58	JavaScript	a5be6ccbda184fad7c228a1690321c0964a34bee8704e8cce28704def7579212

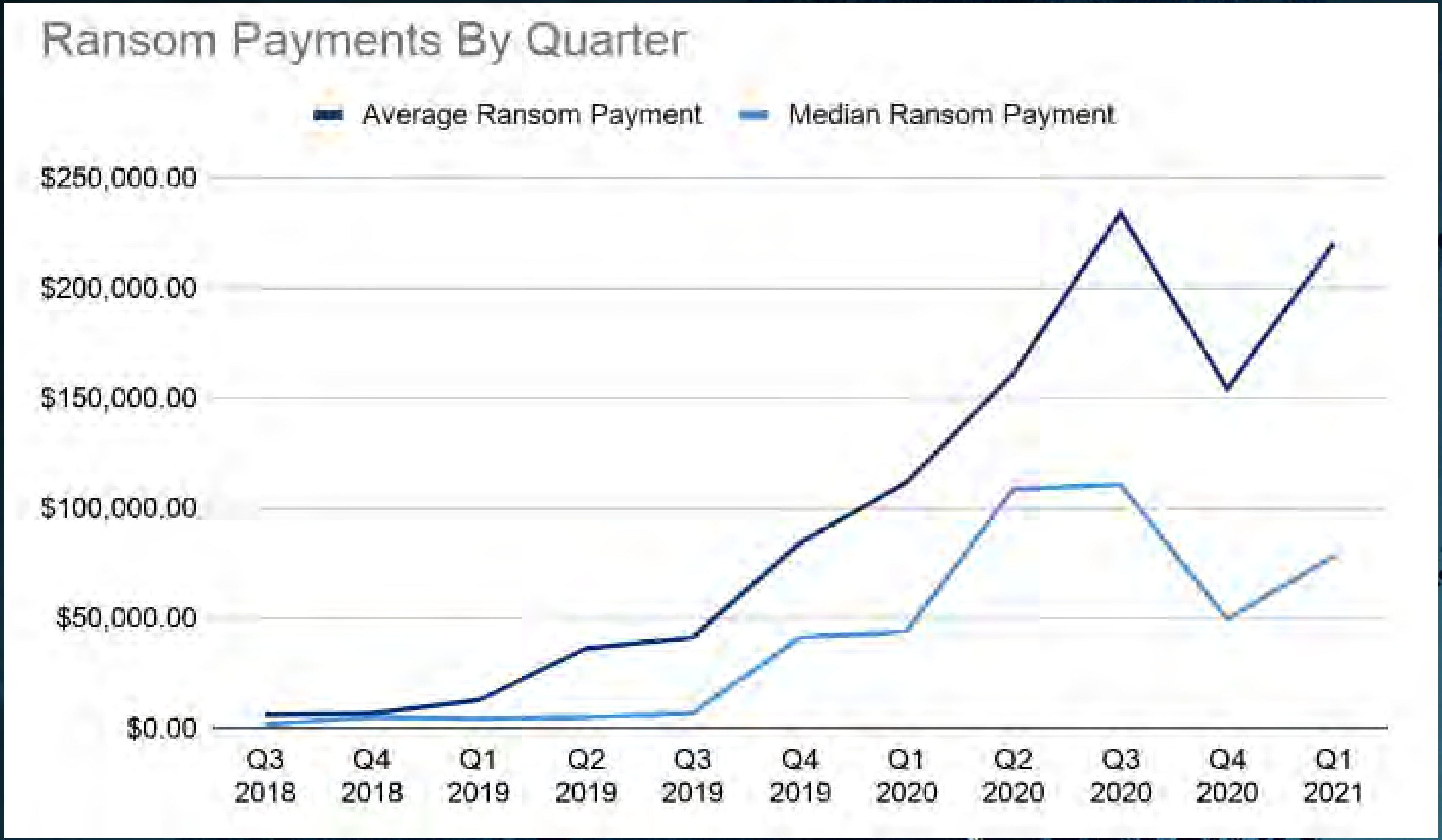
• • •

Secutec negotiation services

Secutec
Cyber security intelligence

ATTACK VECTOR BY COMPANY SIZE




Ransom Payments By Quarter
Average Ransom Payment
Median Ransom Payment
$250,000.00
$200,000.00
$150,000.00
$100,000.00
$50,000.00
$0.00
Q3 2018
Q4 2018
Q1 2019
Q2 2019
Q3 2019
Q4 2019
Q1 2020
Q2 2020
Q3 2020
Q4 2020
Q1 2021

Press releases:

„Antwerp IT company Itxx pays 252.000 euros ransom after Conti ransomware attack“

„Ransomware attack is over, at cost of $300,000“

„Antwerp ICT service provider Itxx victim of cyber attack“

When a ransomware hit your company:

✓First 48 hours

✓Forensic investigation onsite

✓Info on the Darknet

✓Start negotiation

✓Prioritise stakeholders in your company

✓Prioritise data in your company

✓Methodology of the recovery

✓Clear strategy

In all cases:

✓You need in best case 1 month to rebuild the network

✓Never forget the human part

✓Best teambuilding ever!

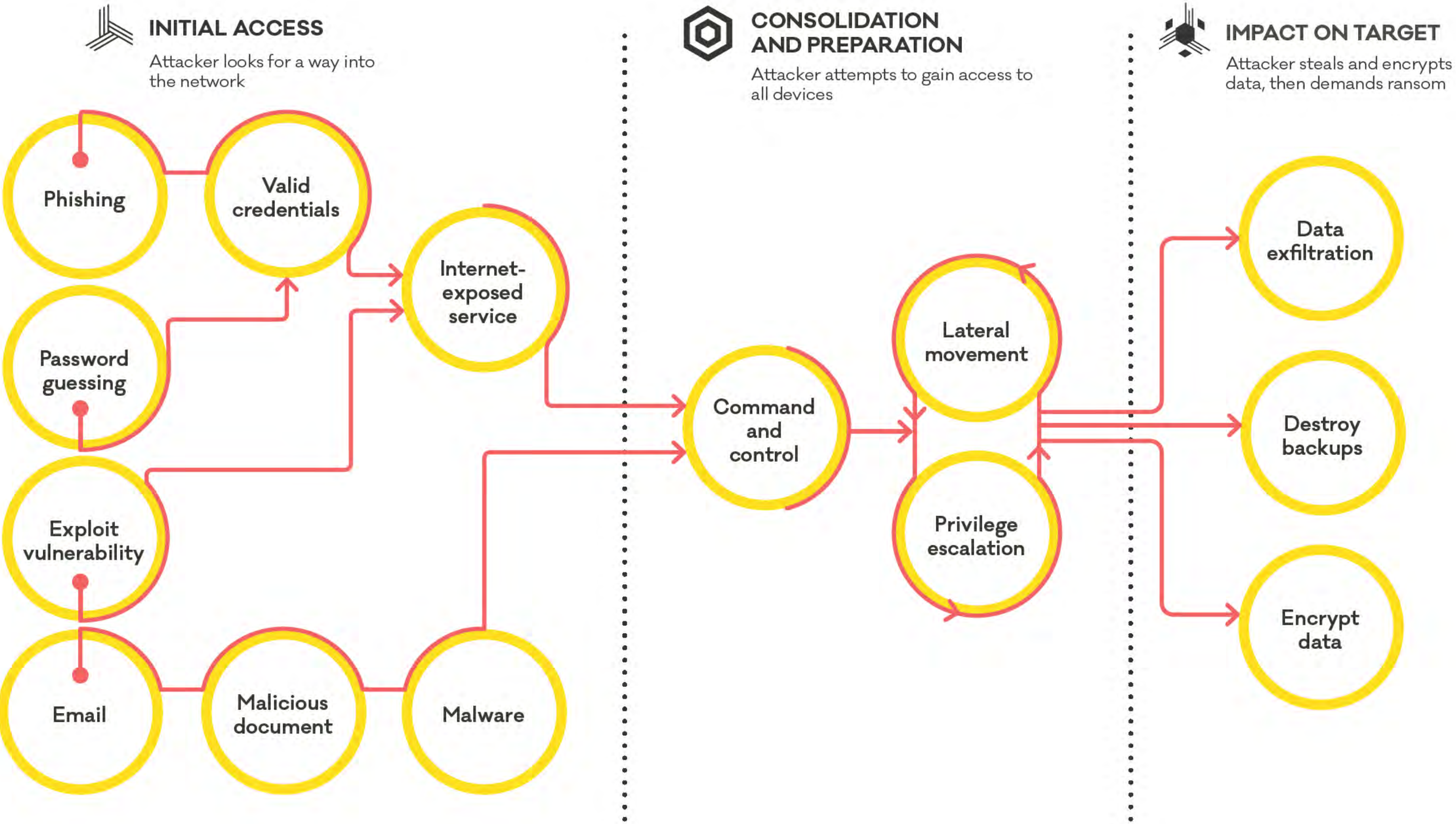
secureSIGHT

The digital footprint of your company is constantly growing, and with it the digital risk. SecureSIGHT is a managed service that shows and evaluates the attack surfaces for cybercrime in your company.

certnz

Lifecycle of a Ransomware Insident

Secutec
Cyber security intelligence

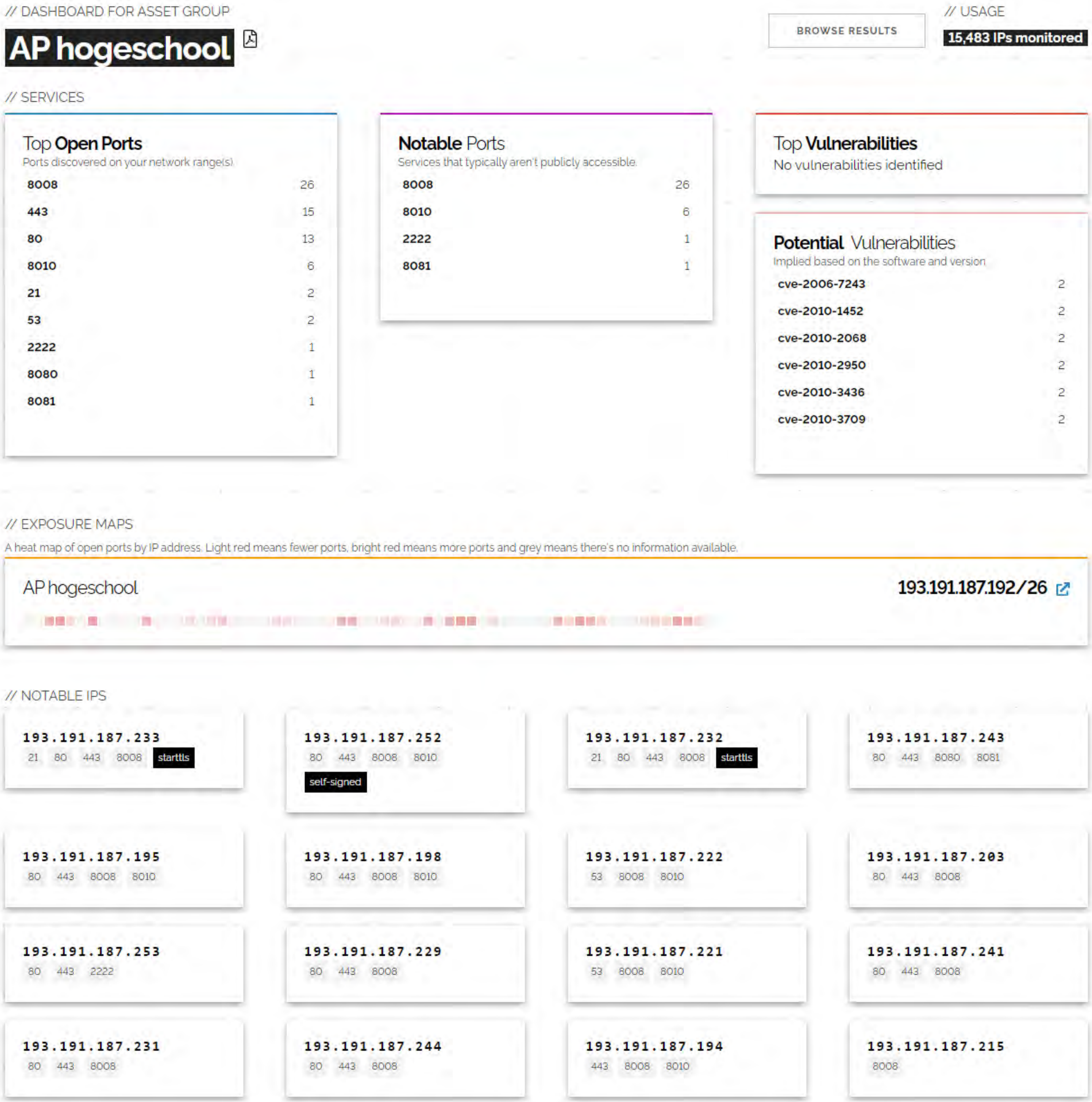


Weekly Vulnerability Scanning

- High-level look at possible vulnerabilities

- coverage for more than 65K vulnerabilities

- SOC alerts – detections immediately reported



// DASHBOARD FOR ASSET GROUP

AP hogeschool

// USAGE

15,483 IPs monitored

// SERVICES

Top **Open Ports**

Ports discovered on your network range(s).

8008	26
443	15
80	13
8010	6
21	2
53	2
2222	1
8080	1
8081	1

Notable Ports

Services that typically aren't publicly accessible.

8008	26
8010	6
2222	1
8081	1

Top **Vulnerabilities**

No vulnerabilities identified

Potential Vulnerabilities

Implied based on the software and version

cve-2006-7243	2
cve-2010-1452	2
cve-2010-2068	2
cve-2010-2950	2
cve-2010-3436	2
cve-2010-3709	2

// EXPOSURE MAPS

A heat map of open ports by IP address. Light red means fewer ports, bright red means more ports and grey means there's no information available.

AP hogeschool

193.191.187.192/26

// NOTABLE IPS

193.191.187.233
21 80 443 8008 starttls

193.191.187.252
80 443 8008 8010 self-signed

193.191.187.232
21 80 443 8008 starttls

193.191.187.243
80 443 8080 8081

193.191.187.195
80 443 8008 8010

193.191.187.198
80 443 8008 8010

193.191.187.222
53 8008 8010

193.191.187.203
80 443 8008

193.191.187.253
80 443 2222

193.191.187.229
80 443 8008

193.191.187.221
53 8008 8010

193.191.187.241
80 443 8008

193.191.187.231
80 443 8008

193.191.187.244
80 443 8008

193.191.187.194
443 8008 8010

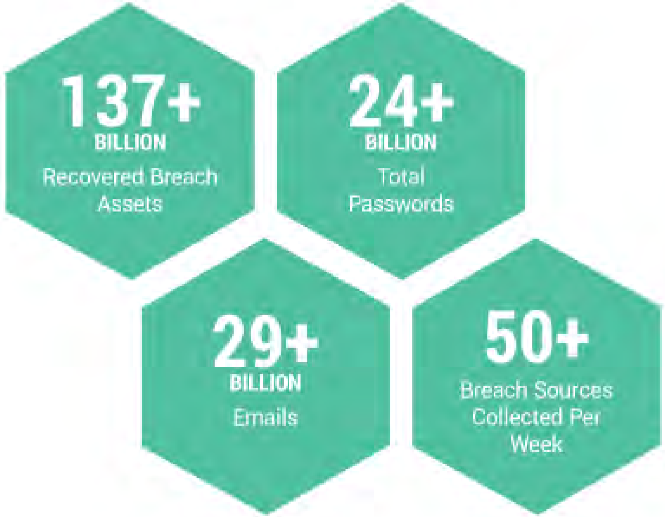
193.191.187.215
8008

Account Takeover Fraud Prevention and Monitoring

- Recover the most current breached data directly from the criminal underground

- User credentials: email/username and password

- Dark Web Monitoring

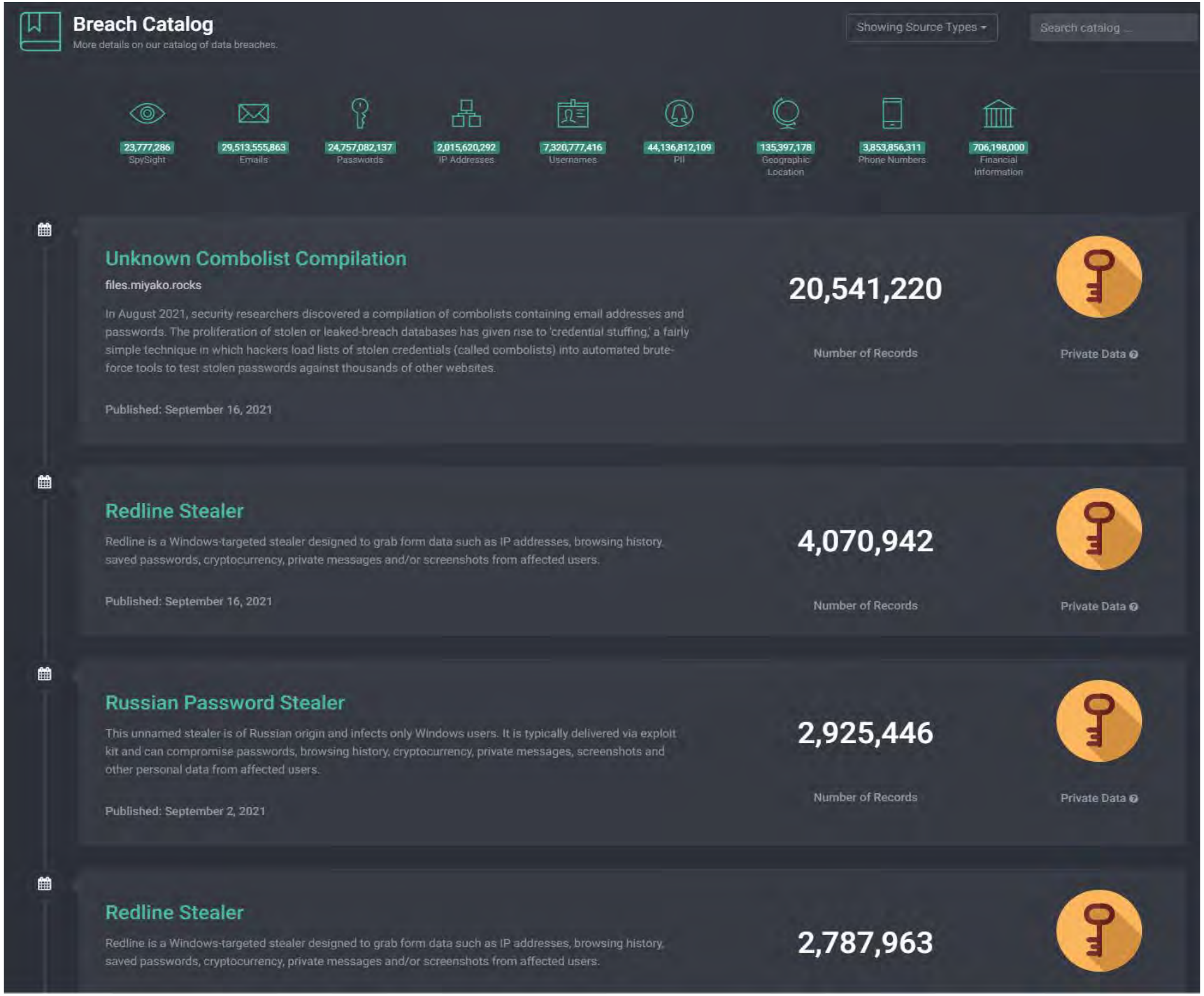


137+ BILLION Recovered Breach Assets

24+ BILLION Total Passwords

29+ BILLION Emails

50+ Breach Sources Collected Per Week



Breach Catalog

More details on our catalog of data breaches.

23,777,286	29,513,555,863	24,757,082,137	2,015,620,292	7,320,777,416	44,136,812,109	135,397,178	3,853,856,311	706,198,000
SpySight	Emails	Passwords	IP Addresses	Usernames	PII	Geographic Location	Phone Numbers	Financial Information

Unknown Combolist Compilation

files.miyako.rocks

In August 2021, security researchers discovered a compilation of combolists containing email addresses and passwords. The proliferation of stolen or leaked-breach databases has given rise to 'credential stuffing,' a fairly simple technique in which hackers load lists of stolen credentials (called combolists) into automated brute-force tools to test stolen passwords against thousands of other websites.

Published: September 16, 2021

20,541,220 Number of Records

Private Data

Redline Stealer

Redline is a Windows-targeted stealer designed to grab form data such as IP addresses, browsing history, saved passwords, cryptocurrency, private messages and/or screenshots from affected users.

Published: September 16, 2021

4,070,942 Number of Records

Private Data

Russian Password Stealer

This unnamed stealer is of Russian origin and infects only Windows users. It is typically delivered via exploit kit and can compromise passwords, browsing history, cryptocurrency, private messages, screenshots and other personal data from affected users.

Published: September 2, 2021

2,925,446 Number of Records

Private Data

Redline Stealer

Redline is a Windows-targeted stealer designed to grab form data such as IP addresses, browsing history, saved passwords, cryptocurrency, private messages and/or screenshots from affected users.

2,787,963

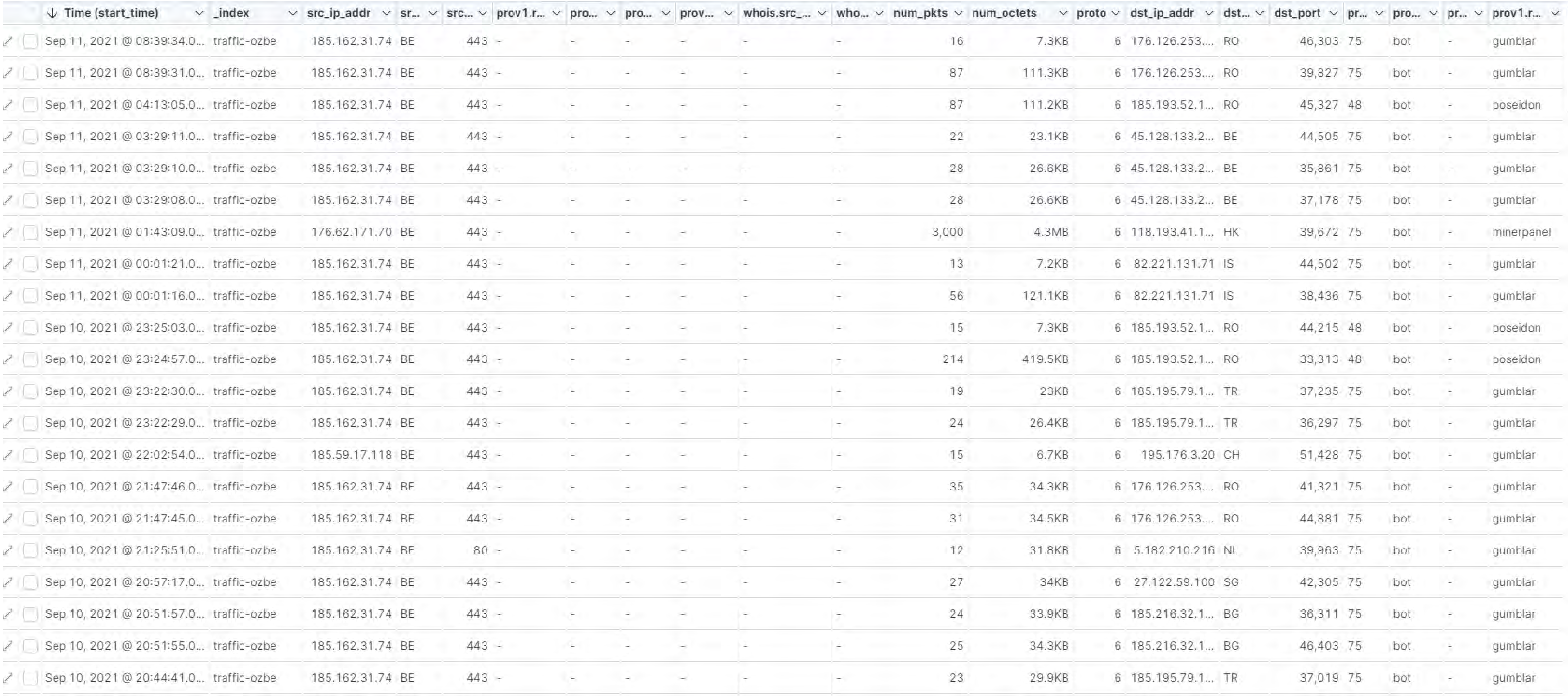
secureSIGHT

Active Manged Threat hunting

- Weekly parsing of all connections to find suspicious connections

- 70% of all continental internet traffic; 99% visibility on all malicious connections

- 35 Security Vendor Feeds

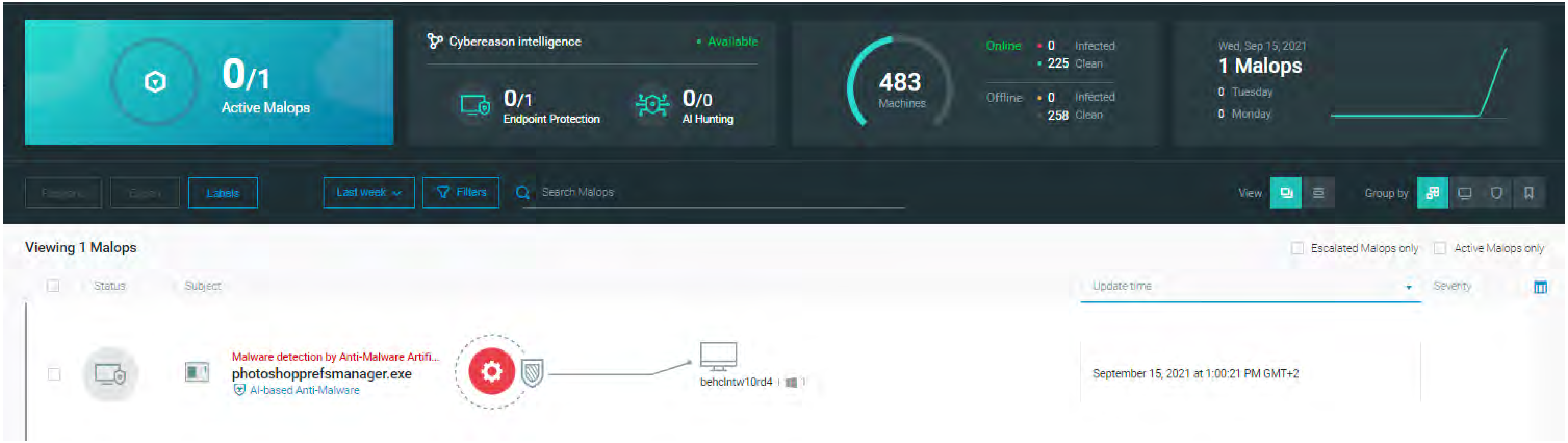


Time (start_time)	_index	src_ip_addr	sr...	src...	prov1.r...	pro...	pro...	prov...	whois.src_...	who...	num_pkts	num_octets	proto	dst_ip_addr	dst...	dst_port	pr...	pro...	pr...	prov1.r...
Sep 11, 2021 @ 08:39:34.0...	traffic-ozbe	185.162.31.74	BE	443	-	-	-	-	-	-	16	7.3KB	6	176.126.253....	RO	46,303	75	bot	-	gumblar
Sep 11, 2021 @ 08:39:31.0...	traffic-ozbe	185.162.31.74	BE	443	-	-	-	-	-	-	87	111.3KB	6	176.126.253....	RO	39,827	75	bot	-	gumblar
Sep 11, 2021 @ 04:13:05.0...	traffic-ozbe	185.162.31.74	BE	443	-	-	-	-	-	-	87	111.2KB	6	185.193.52.1...	RO	45,327	48	bot	-	poseidon
Sep 11, 2021 @ 03:29:11.0...	traffic-ozbe	185.162.31.74	BE	443	-	-	-	-	-	-	22	23.1KB	6	45.128.133.2...	BE	44,505	75	bot	-	gumblar
Sep 11, 2021 @ 03:29:10.0...	traffic-ozbe	185.162.31.74	BE	443	-	-	-	-	-	-	28	26.6KB	6	45.128.133.2...	BE	35,861	75	bot	-	gumblar
Sep 11, 2021 @ 03:29:08.0...	traffic-ozbe	185.162.31.74	BE	443	-	-	-	-	-	-	28	26.6KB	6	45.128.133.2...	BE	37,178	75	bot	-	gumblar
Sep 11, 2021 @ 01:43:09.0...	traffic-ozbe	176.62.171.70	BE	443	-	-	-	-	-	-	3,000	4.3MB	6	118.193.41.1...	HK	39,672	75	bot	-	minerpanel
Sep 11, 2021 @ 00:01:21.0...	traffic-ozbe	185.162.31.74	BE	443	-	-	-	-	-	-	13	7.2KB	6	82.221.131.71	IS	44,502	75	bot	-	gumblar
Sep 11, 2021 @ 00:01:16.0...	traffic-ozbe	185.162.31.74	BE	443	-	-	-	-	-	-	56	121.1KB	6	82.221.131.71	IS	38,436	75	bot	-	gumblar
Sep 10, 2021 @ 23:25:03.0...	traffic-ozbe	185.162.31.74	BE	443	-	-	-	-	-	-	15	7.3KB	6	185.193.52.1...	RO	44,215	48	bot	-	poseidon
Sep 10, 2021 @ 23:24:57.0...	traffic-ozbe	185.162.31.74	BE	443	-	-	-	-	-	-	214	419.5KB	6	185.193.52.1...	RO	33,313	48	bot	-	poseidon
Sep 10, 2021 @ 23:22:30.0...	traffic-ozbe	185.162.31.74	BE	443	-	-	-	-	-	-	19	23KB	6	185.195.79.1...	TR	37,235	75	bot	-	gumblar
Sep 10, 2021 @ 23:22:29.0...	traffic-ozbe	185.162.31.74	BE	443	-	-	-	-	-	-	24	26.4KB	6	185.195.79.1...	TR	36,297	75	bot	-	gumblar
Sep 10, 2021 @ 22:02:54.0...	traffic-ozbe	185.59.17.118	BE	443	-	-	-	-	-	-	15	6.7KB	6	195.176.3.20	CH	51,428	75	bot	-	gumblar
Sep 10, 2021 @ 21:47:46.0...	traffic-ozbe	185.162.31.74	BE	443	-	-	-	-	-	-	35	34.3KB	6	176.126.253....	RO	41,321	75	bot	-	gumblar
Sep 10, 2021 @ 21:47:45.0...	traffic-ozbe	185.162.31.74	BE	443	-	-	-	-	-	-	31	34.5KB	6	176.126.253....	RO	44,881	75	bot	-	gumblar
Sep 10, 2021 @ 21:25:51.0...	traffic-ozbe	185.162.31.74	BE	80	-	-	-	-	-	-	12	31.8KB	6	5.182.210.216	NL	39,963	75	bot	-	gumblar
Sep 10, 2021 @ 20:57:17.0...	traffic-ozbe	185.162.31.74	BE	443	-	-	-	-	-	-	27	34KB	6	27.122.59.100	SG	42,305	75	bot	-	gumblar
Sep 10, 2021 @ 20:51:57.0...	traffic-ozbe	185.162.31.74	BE	443	-	-	-	-	-	-	24	33.9KB	6	185.216.32.1...	BG	36,311	75	bot	-	gumblar
Sep 10, 2021 @ 20:51:55.0...	traffic-ozbe	185.162.31.74	BE	443	-	-	-	-	-	-	25	34.3KB	6	185.216.32.1...	BG	46,403	75	bot	-	gumblar
Sep 10, 2021 @ 20:44:41.0...	traffic-ozbe	185.162.31.74	BE	443	-	-	-	-	-	-	23	29.9KB	6	185.195.79.1...	TR	37,019	75	bot	-	gumblar

Managed EDR on Servers

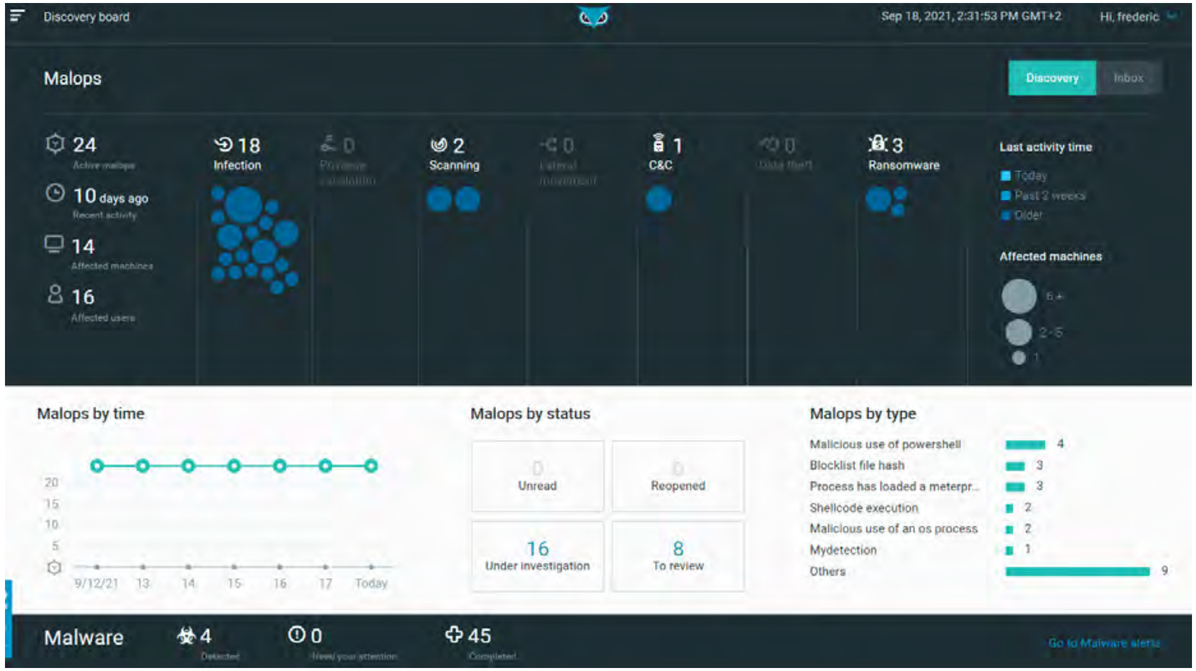
- Detect suspicious activity on your network

- EDR in monitoring mode

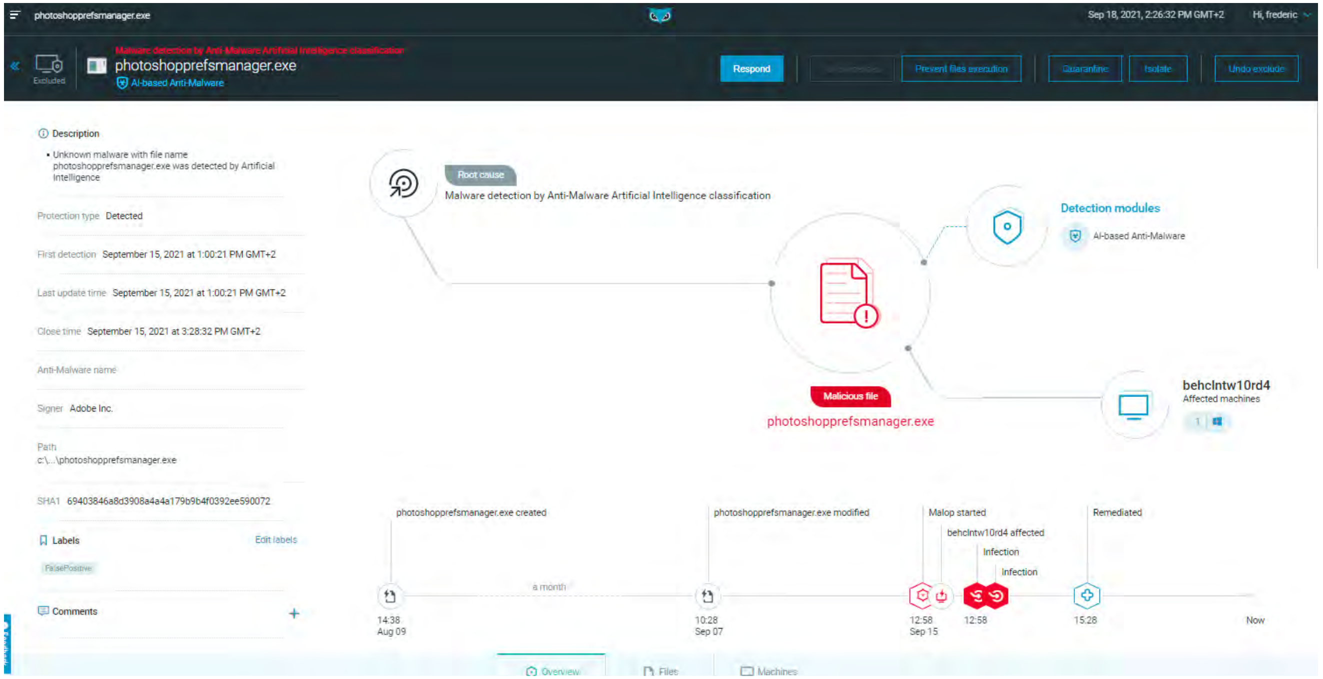


Viewing 1 Malops

	Subject		Update time
□	Malware detection by Anti-Malware Artifi... photoshopprefsmanager.exe AI-based Anti-Malware	behclntw10rd4 | 1	September 15, 2021 at 1:00:21 PM GMT+2



Malops by type	
Malicious use of powershell	4
Blocklist file hash	3
Process has loaded a meterpr...	3
Shellcode execution	2
Malicious use of an os process	2
Mydetection	1
Others	9



Description

- Unknown malware with file name photoshopprefsmanager.exe was detected by Artificial Intelligence

Protection type Detected

First detection September 15, 2021 at 1:00:21 PM GMT+2

Last update time September 15, 2021 at 1:00:21 PM GMT+2

Close time September 15, 2021 at 3:28:32 PM GMT+2

Anti-Malware name

Signer Adobe Inc.

Path
c:\...\photoshopprefsmanager.exe

SHA1 69403846a8d3908a4a4a179b9b4f0392ee590072

Labels Edit labels

FalsePositive

Comments +

Secutec

Cyber security intelligence