Supercharge your Red Team with RedELK

Marc Smeets

SANS HackFest – June 2020

OUTFLANK

clear advice with a hacker mindset

ABOUT YOUR SPEAKER

Marc Smeets - @MarcOverIP

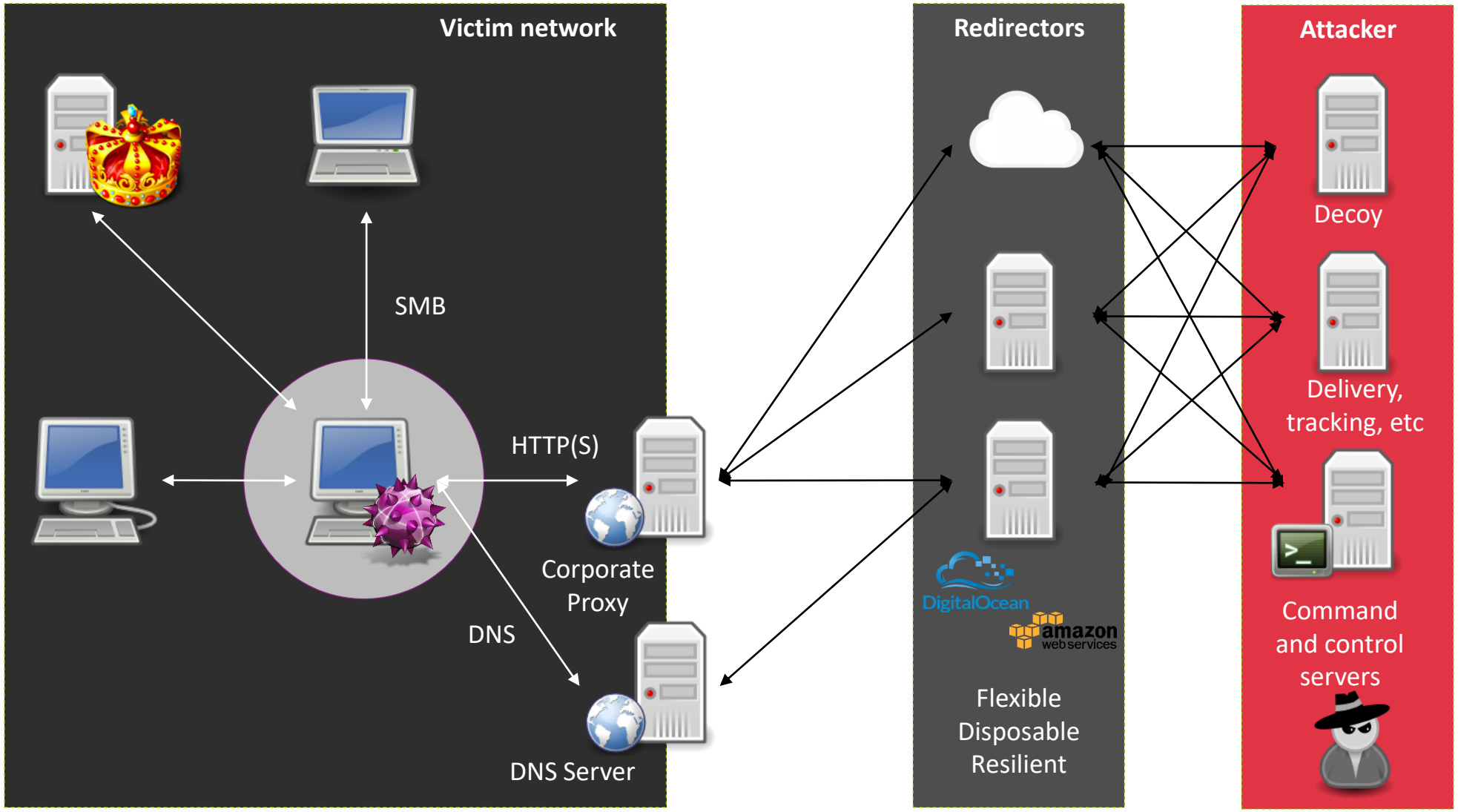
- Red Team operator, tool builder, trainer
- In offensive security since 2006
- Backgrounds: system and network engineering, and security consulting
- Blue Team Threat Hunting experience

Outflank

- Boutique Red Teaming firm in The Netherlands, founded in 2016
- Strong advocates of the TIBER framework
- Sharing knowledge via:
  - IT security trainings
  - https://outflank.nl/blog
  - https://github.com/OutflankNL


PAFFEN
SPORT

OFFENSIVE INFRA – GENERIC OVERVIEW



OFFENSIVE INFRA – TYPICAL SETUP FOR 1 OPERATION

Command and Control

- C2-servers (5+)
- Redirectors / reverse proxies (5+)
- Domain fronting CDN (2+)

Fake identities

- Social media profiles (2+)
- Websites (1+)

Tracking

- Tracking pixels (10+)

Delivery

- Web servers (2+)
- Email (2+)
- File sharing service (0+)
- Messaging platforms (0+)
- …

Generic backend components

- Communication channels (2+)
- Test environments (1+)
- Log aggregation (1+)

OFFENSIVE INFRA – TYPICAL CHALLENGES

Oversight

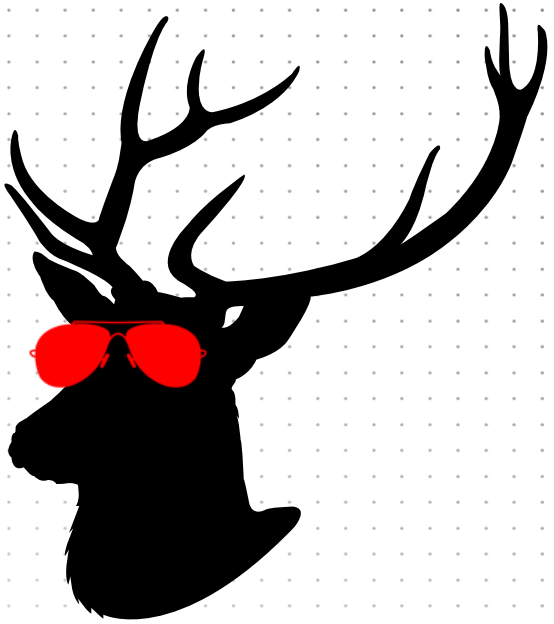
Insight

"Every contact leaves a trace" - Locard's exchange principle

TOOLING -> REDELK

+

=

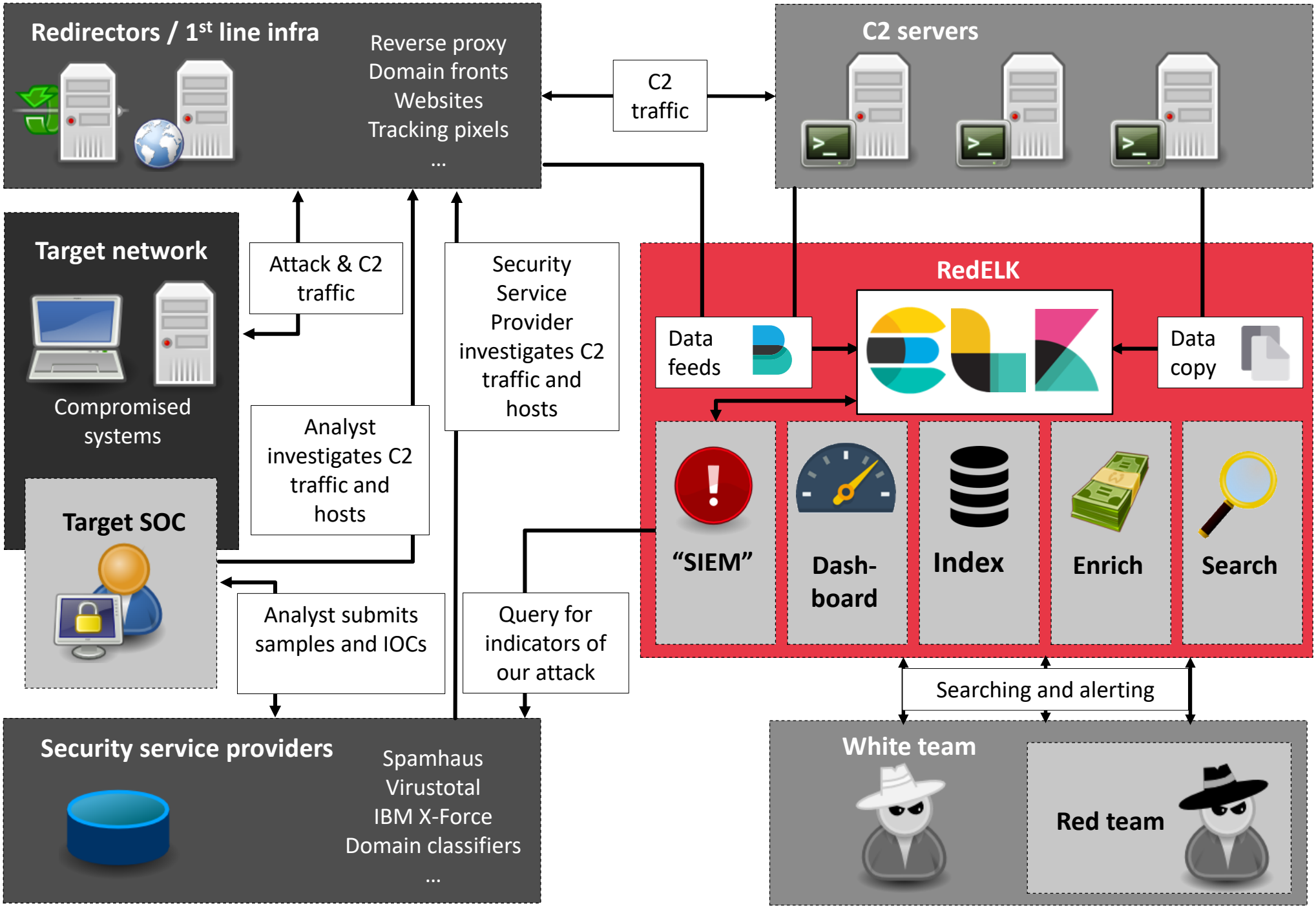


https://github.com/outflanknl/RedELK/

https://outflank.nl/blog/2019/02/14/introducing-redelk-part-1-why-we-need-it/

https://outflank.nl/blog/2020/02/28/redelk-part-2-getting-you-up-and-running/

https://outflank.nl/blog/2020/04/07/redelk-part-3-achieving-operational-oversight/


Redirectors / 1st line infra
Reverse proxy
Domain fronts
Websites
Tracking pixels
...
C2 traffic
C2 servers
Target network
Compromised systems
Attack & C2 traffic
Security Service Provider investigates C2 traffic and hosts
RedELK
Data feeds
Data copy
Analyst investigates C2 traffic and hosts
Target SOC
"SIEM"
Dash-board
Index
Enrich
Search
Analyst submits samples and IOCs
Query for indicators of our attack
Searching and alerting
Security service providers
Spamhaus
Virustotal
IBM X-Force
Domain classifiers
...
White team
Red team

DATA ENRICHMENT

Tor

iana
Internet Assigned Numbers Authority

reverse DNS

GREY NOISE

OUTFLANK

COBALT STRIKE
ADVANCED THREAT TACTICS FOR PENETRATION TESTERS

PoshC2

HYBRID ANALYSIS

COVENANT

VirusTotal

FACTION

APfell
it's not a bug, it's a feature.

SCYTHE

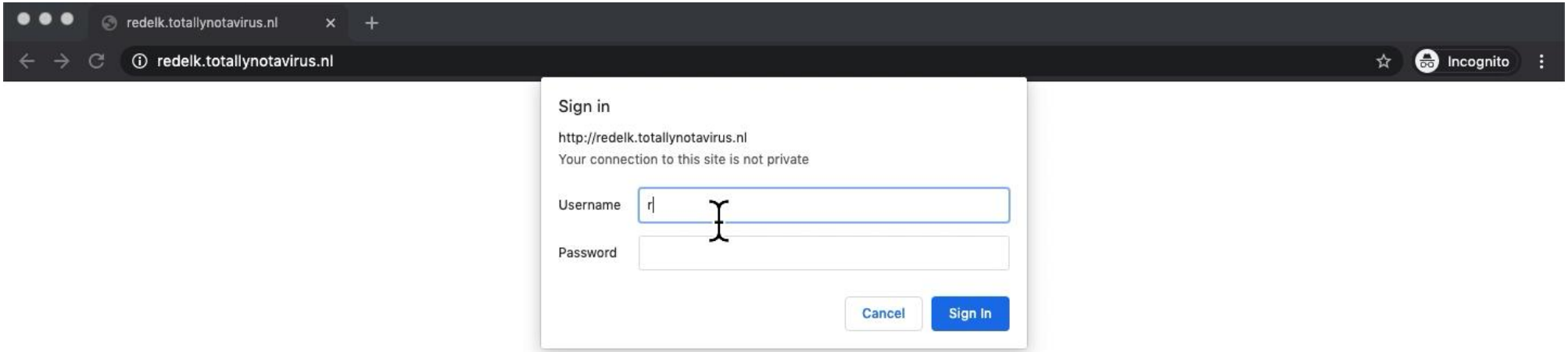
IBM X-Force

ABUSE.ch

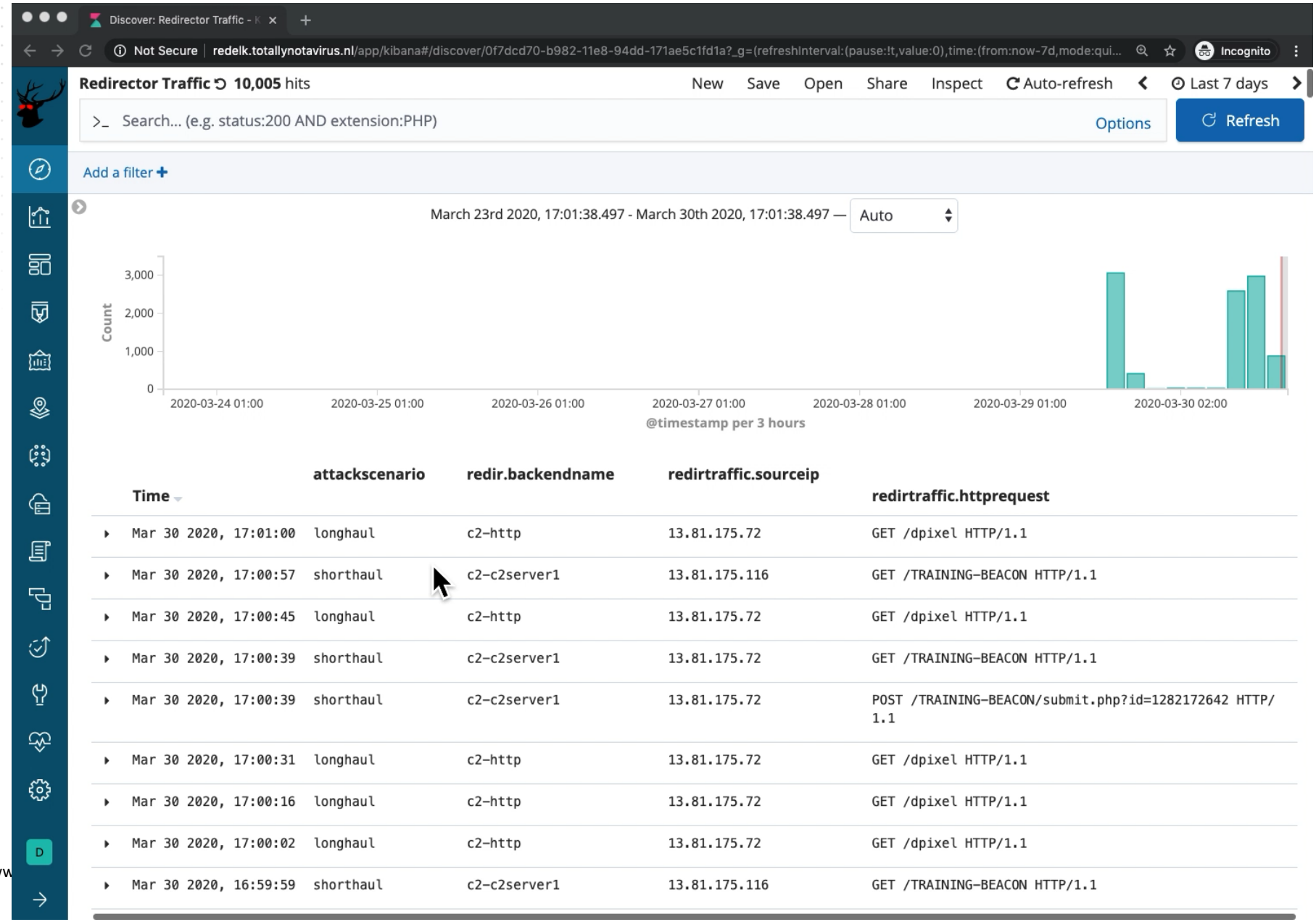
SEE EVERYTHING

Central overview of the operation

PRE-MADE VIEWS

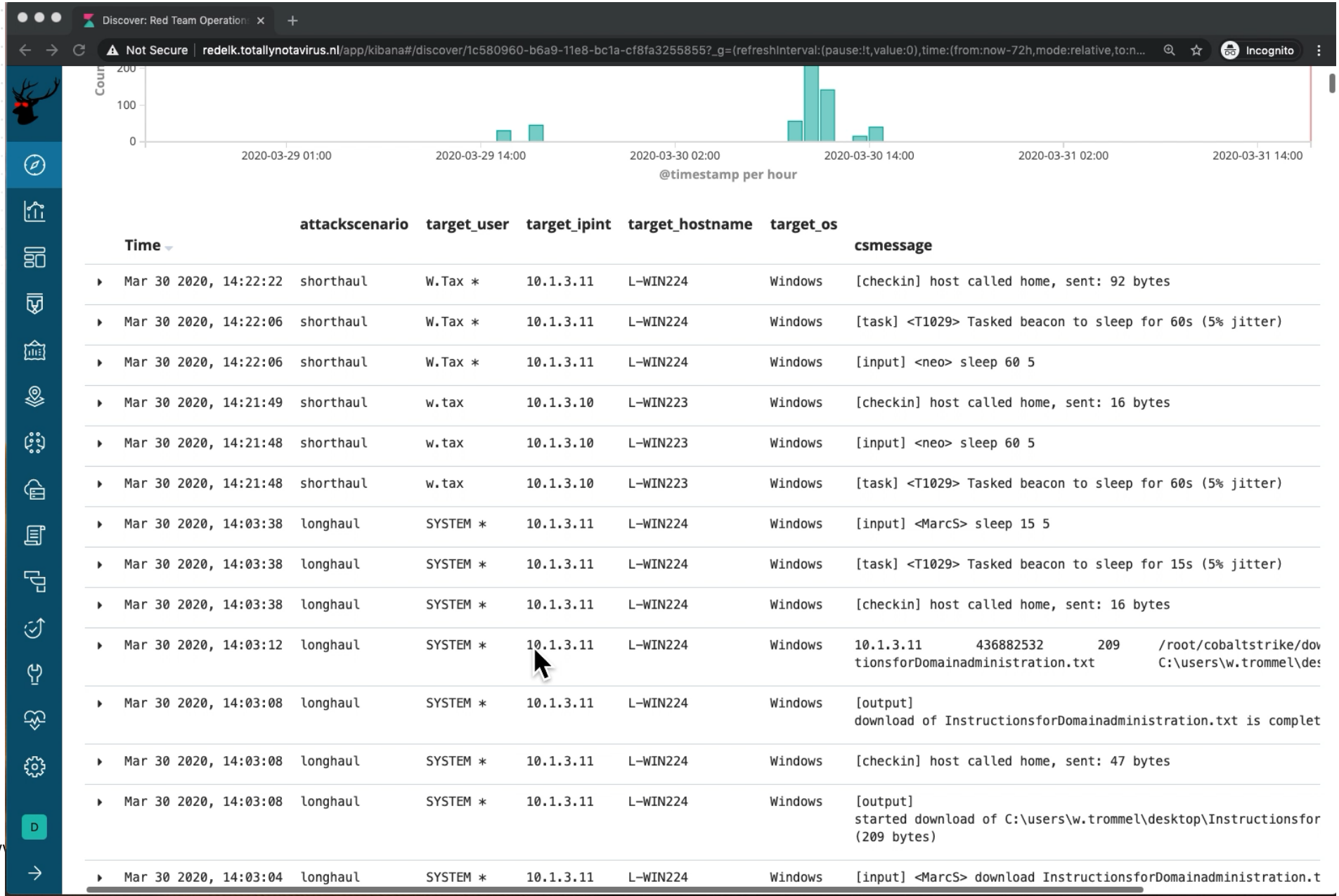


REDIRECTOR TRAFFIC



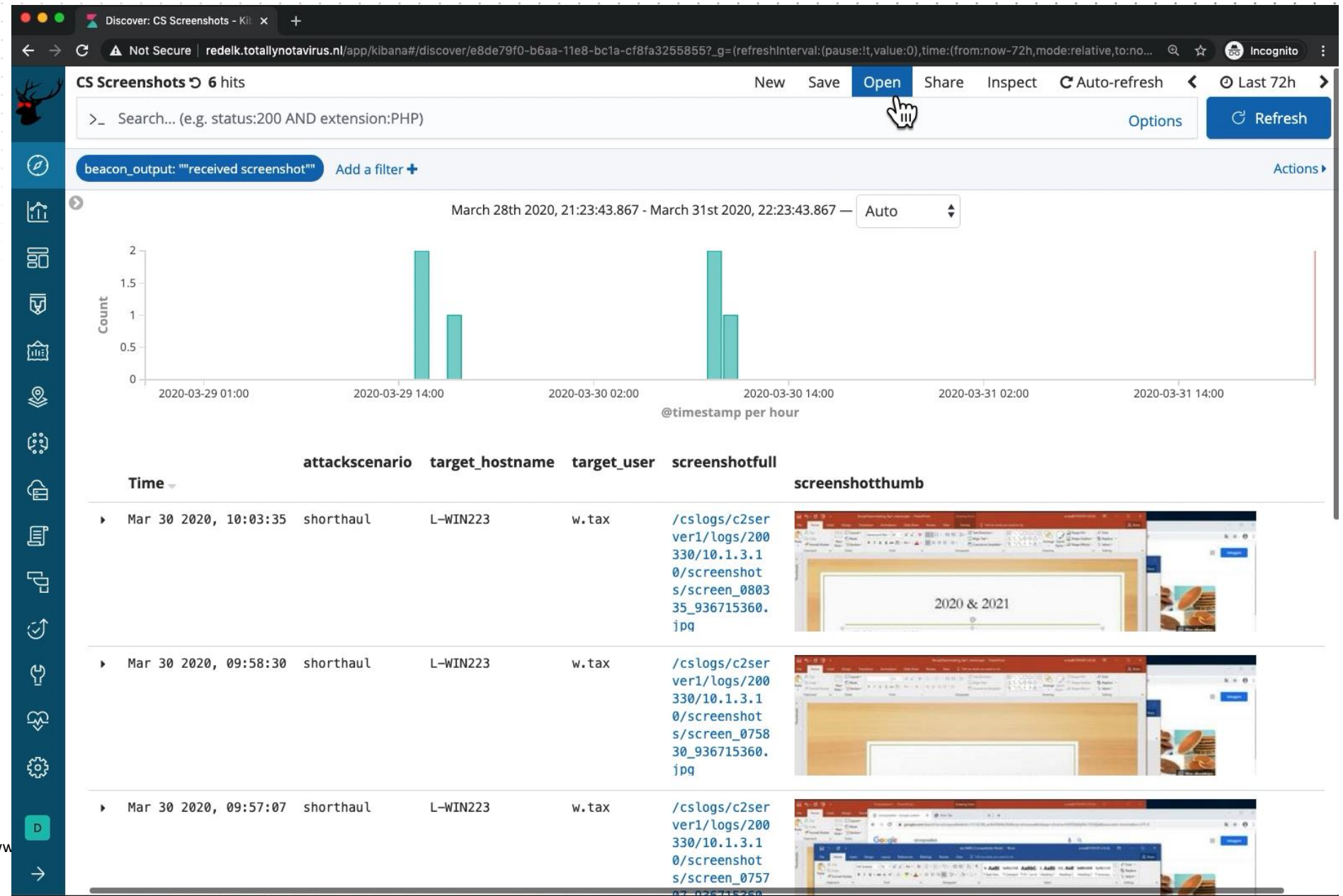
Time	attackscenario	redir.backendname	redirtraffic.sourceip	redirtraffic.httprequest
Mar 30 2020, 17:01:00	longhaul	c2-http	13.81.175.72	GET /dpixel HTTP/1.1
Mar 30 2020, 17:00:57	shorthaul	c2-c2server1	13.81.175.116	GET /TRAINING-BEACON HTTP/1.1
Mar 30 2020, 17:00:45	longhaul	c2-http	13.81.175.72	GET /dpixel HTTP/1.1
Mar 30 2020, 17:00:39	shorthaul	c2-c2server1	13.81.175.72	GET /TRAINING-BEACON HTTP/1.1
Mar 30 2020, 17:00:39	shorthaul	c2-c2server1	13.81.175.72	POST /TRAINING-BEACON/submit.php?id=1282172642 HTTP/1.1
Mar 30 2020, 17:00:31	longhaul	c2-http	13.81.175.72	GET /dpixel HTTP/1.1
Mar 30 2020, 17:00:16	longhaul	c2-http	13.81.175.72	GET /dpixel HTTP/1.1
Mar 30 2020, 17:00:02	longhaul	c2-http	13.81.175.72	GET /dpixel HTTP/1.1
Mar 30 2020, 16:59:59	shorthaul	c2-c2server1	13.81.175.116	GET /TRAINING-BEACON HTTP/1.1

C2 LOGS– HISTORIC SEARCHING

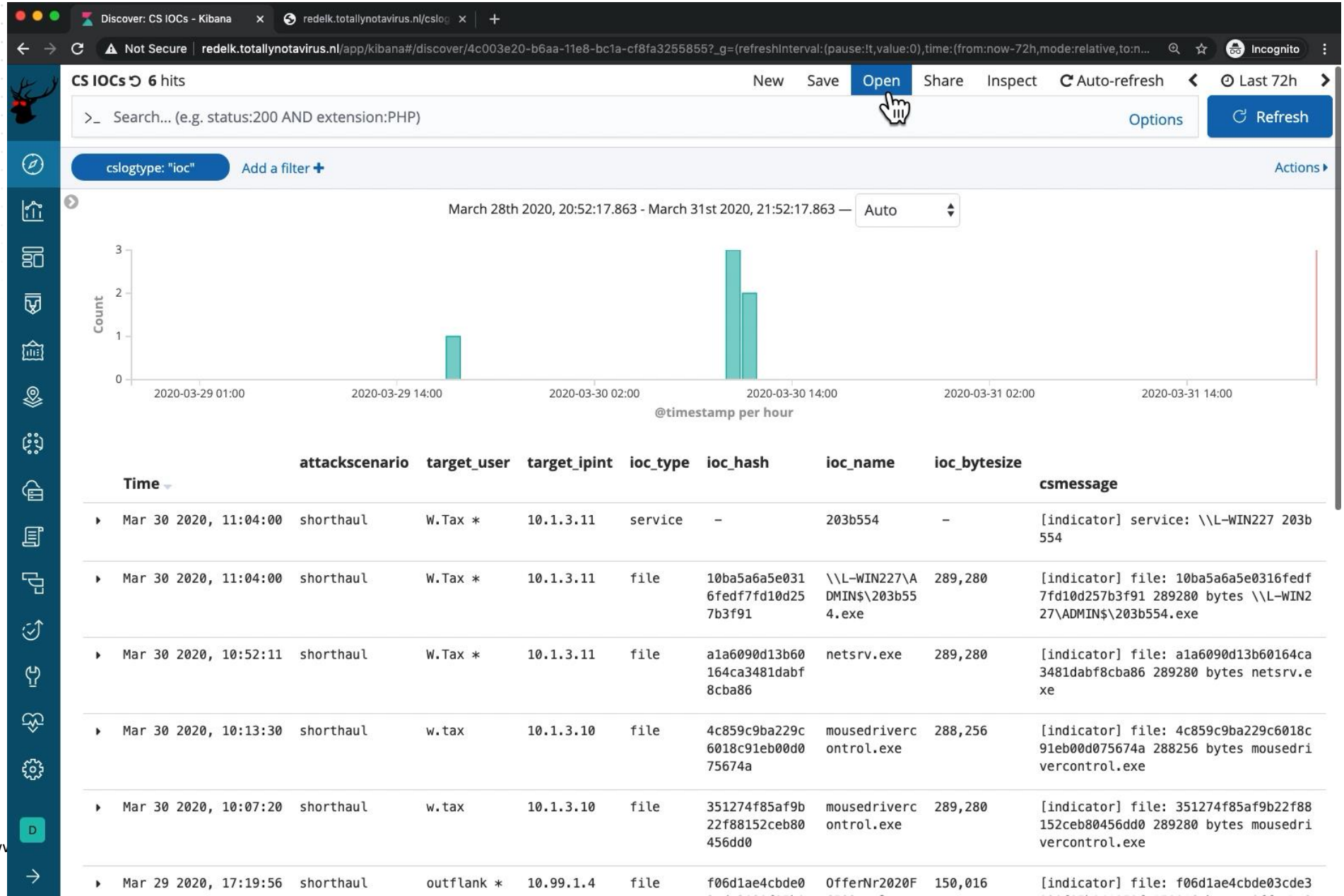


Time	attackscenario	target_user	target_ipint	target_hostname	target_os	csmessage
Mar 30 2020, 14:22:22	shorthaul	W.Tax *	10.1.3.11	L-WIN224	Windows	[checkin] host called home, sent: 92 bytes
Mar 30 2020, 14:22:06	shorthaul	W.Tax *	10.1.3.11	L-WIN224	Windows	[task] <T1029> Tasked beacon to sleep for 60s (5% jitter)
Mar 30 2020, 14:22:06	shorthaul	W.Tax *	10.1.3.11	L-WIN224	Windows	[input] <neo> sleep 60 5
Mar 30 2020, 14:21:49	shorthaul	w.tax	10.1.3.10	L-WIN223	Windows	[checkin] host called home, sent: 16 bytes
Mar 30 2020, 14:21:48	shorthaul	w.tax	10.1.3.10	L-WIN223	Windows	[input] <neo> sleep 60 5
Mar 30 2020, 14:21:48	shorthaul	w.tax	10.1.3.10	L-WIN223	Windows	[task] <T1029> Tasked beacon to sleep for 60s (5% jitter)
Mar 30 2020, 14:03:38	longhaul	SYSTEM *	10.1.3.11	L-WIN224	Windows	[input] <MarcS> sleep 15 5
Mar 30 2020, 14:03:38	longhaul	SYSTEM *	10.1.3.11	L-WIN224	Windows	[task] <T1029> Tasked beacon to sleep for 15s (5% jitter)
Mar 30 2020, 14:03:38	longhaul	SYSTEM *	10.1.3.11	L-WIN224	Windows	[checkin] host called home, sent: 16 bytes
Mar 30 2020, 14:03:12	longhaul	SYSTEM *	10.1.3.11	L-WIN224	Windows	10.1.3.11 436882532 209 /root/cobaltstrike/dov tionsforDomainadministration.txt C:\users\w.trommel\des
Mar 30 2020, 14:03:08	longhaul	SYSTEM *	10.1.3.11	L-WIN224	Windows	[output] download of InstructionsforDomainadministration.txt is complet
Mar 30 2020, 14:03:08	longhaul	SYSTEM *	10.1.3.11	L-WIN224	Windows	[checkin] host called home, sent: 47 bytes
Mar 30 2020, 14:03:08	longhaul	SYSTEM *	10.1.3.11	L-WIN224	Windows	[output] started download of C:\users\w.trommel\desktop\Instructionsfor (209 bytes)
Mar 30 2020, 14:03:04	longhaul	SYSTEM *	10.1.3.11	L-WIN224	Windows	[input] <MarcS> download InstructionsforDomainadministration.t

C2 SCREENSHOTS



ALL IOCS

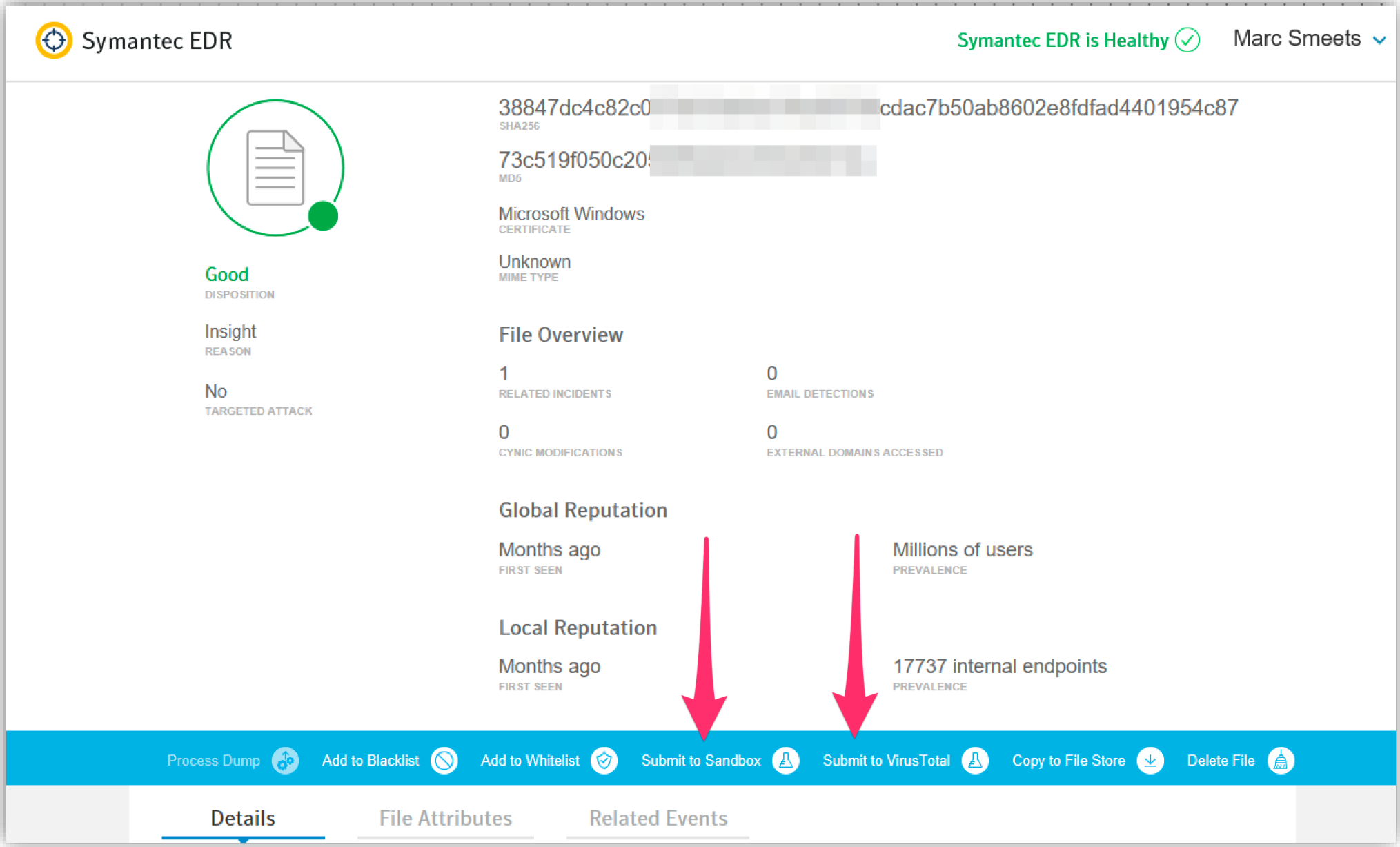


Time	attackscenario	target_user	target_ipint	ioc_type	ioc_hash	ioc_name	ioc_bytesize	csmessage
Mar 30 2020, 11:04:00	shorthaul	W.Tax *	10.1.3.11	service	-	203b554	-	[indicator] service: \\L-WIN227 203b554
Mar 30 2020, 11:04:00	shorthaul	W.Tax *	10.1.3.11	file	10ba5a6a5e0316fedf7fd10d257b3f91	\\L-WIN227\ADMIN$\203b554.exe	289,280	[indicator] file: 10ba5a6a5e0316fedf7fd10d257b3f91 289280 bytes \\L-WIN227\ADMIN$\203b554.exe
Mar 30 2020, 10:52:11	shorthaul	W.Tax *	10.1.3.11	file	a1a6090d13b60164ca3481dabf8cba86	netsrv.exe	289,280	[indicator] file: a1a6090d13b60164ca3481dabf8cba86 289280 bytes netsrv.exe
Mar 30 2020, 10:13:30	shorthaul	w.tax	10.1.3.10	file	4c859c9ba229c6018c91eb00d075674a	mousedrivercontrol.exe	288,256	[indicator] file: 4c859c9ba229c6018c91eb00d075674a 288256 bytes mousedrivercontrol.exe
Mar 30 2020, 10:07:20	shorthaul	w.tax	10.1.3.10	file	351274f85af9b22f88152ceb80456dd0	mousedrivercontrol.exe	289,280	[indicator] file: 351274f85af9b22f88152ceb80456dd0 289280 bytes mousedrivercontrol.exe
Mar 29 2020, 17:19:56	shorthaul	outflank *	10.99.1.4	file	f06d1ae4cbde0	OfferNr2020F	150,016	[indicator] file: f06d1ae4cbde03cde3

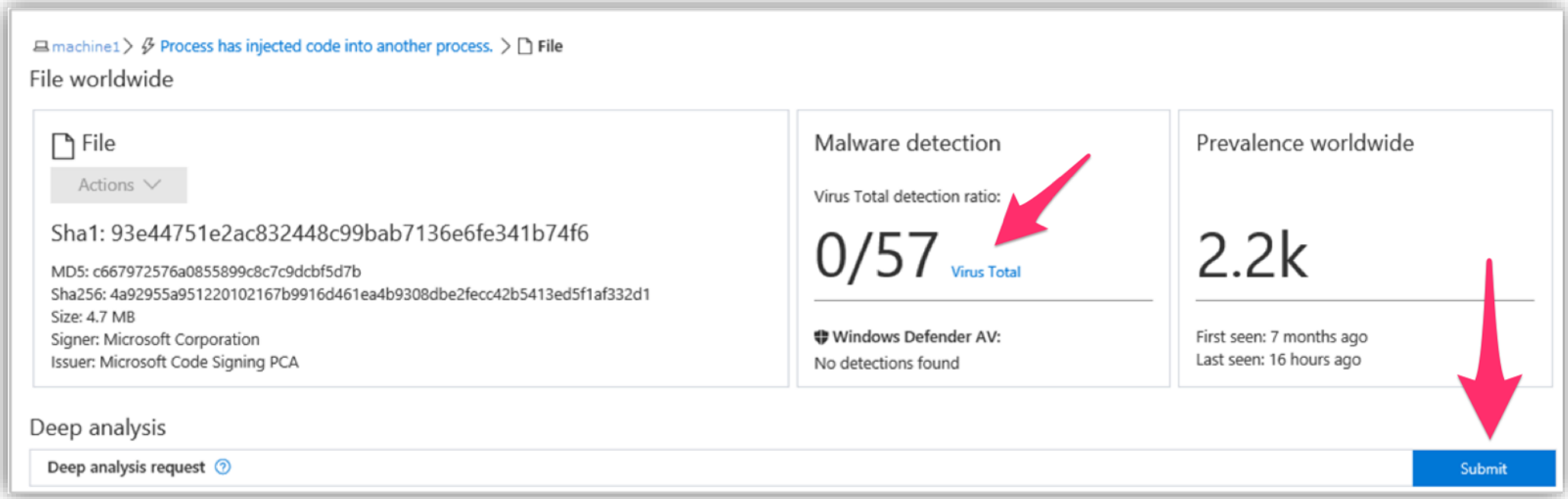
INDICATORS

ONLINE SERVICES

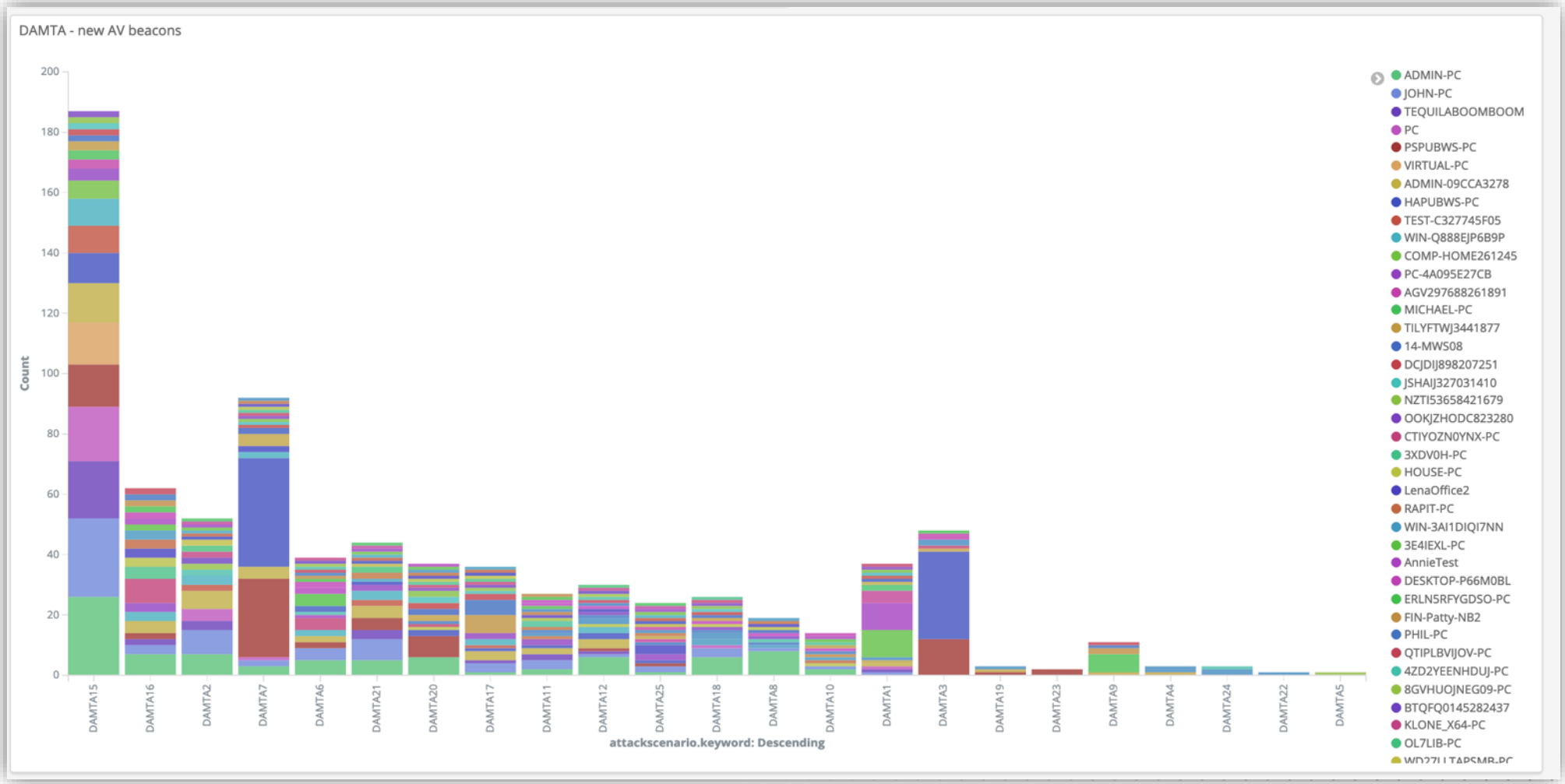
HASH OF MALWARE



HASH OF MALWARE



SANDBOX CONNECTIONS



INDICATORS

TRAFFIC TO OFFENSIVE INFRASTRUCTURE

ANALYST TRAFFIC

haproxy_useragent.keyword: Descending	src_ip.keyword: Descending	src_dns.keyword: Descending
curl/7.35.0	52.58.12.201	ec2-52-58-12-201.eu-central-1.compute.amazonaws.com
python-requests/2.13.0	51.15.62.204	204-62-15-51.rev.cloud.scaleway.com
python-requests/2.13.0	196.52.34.22	ip-22-34-52-196.sg.asianpacifictelephone.com
python-requests/2.13.0	192.40.95.32	192.40.95.32
python-requests/2.20.1	35.161.55.221	ec2-35-161-55-221.us-west-2.compute.amazonaws.com
Python-urllib/2.7	118.219.252.193	118.219.252.193
curl/7.35.0	52.58.51.176	ec2-52-58-51-176.eu-central-1.compute.amazonaws.com
python-requests/2.13.0	196.55.2.2	ip-2-2-55-196.in.asianpacifictelephone.com
python-requests/2.13.0	194.187.249.46	194.187.249.46
curl/7.62.0	94.210.111.193	5ED26FC1.cm-7-3b.dynamic.ziggo.nl
Python-urllib/3.6	91.213.143.247	nat.2-47-prg.avast.com

PREVIEWS BY MESSAGING APPS

haproxy_dest	src_ip	src_dns	geoip.as_org	haproxy_request	haproxy_useragent
www-decoy	149.154.161.16	149.154.161.16	Telegram Messenger LLP	GET /test_TELEGRAM-20190317_2 HTTP/1.1	TelegramBot (like TwitterBot)
www-decoy	149.154.161.11	149.154.161.11	Telegram Messenger LLP	GET /test_TELEGRAM-20190317_22 HTTP/1.1	TelegramBot (like TwitterBot)
www-decoy	149.154.161.17	149.154.161.17	Telegram Messenger LLP	GET /test_TELEGRAM-20190317_223 HTTP/1.1	TelegramBot (like TwitterBot)
www-decoy	149.154.161.10	149.154.161.10	Telegram Messenger LLP	GET /test_TELEGRAM-20190317_2234 HTTP/1.1	TelegramBot (like TwitterBot)
www-decoy	149.154.161.17	149.154.161.17	Telegram Messenger LLP	GET /test_TELEGRAM-20190317_ HTTP/1.1	TelegramBot (like TwitterBot)
www-decoy	149.154.161.3	149.154.161.3	Telegram Messenger LLP	GET /test_TELEGRAM-2019031 HTTP/1.1	TelegramBot (like TwitterBot)
www-decoy	149.154.161.19	149.154.161.19	Telegram Messenger LLP	GET /test_TELEGRAM-20190317 HTTP/1.1	TelegramBot (like TwitterBot)
www-decoy	149.154.161.12	149.154.161.12	Telegram Messenger LLP	GET /test_TELEGRAM-201903 HTTP/1.1	TelegramBot (like TwitterBot)
www-decoy	149.154.161.18	149.154.161.18	Telegram Messenger LLP	GET /test_TELEGRAM-20190 HTTP/1.1	TelegramBot (like TwitterBot)
www-decoy	149.154.161.18	149.154.161.18	Telegram Messenger LLP	GET /test_TELEGRAM-2019 HTTP/1.1	TelegramBot (like TwitterBot)
www-decoy	149.154.161.8	149.154.161.8	Telegram Messenger LLP	GET /test_TELEGRAM-20 HTTP/1.1	TelegramBot (like TwitterBot)
www-decoy	149.154.161.16	149.154.161.16	Telegram Messenger LLP	GET /test_TELEGRAM-201 HTTP/1.1	TelegramBot (like TwitterBot)
www-decoy	149.154.161.5	149.154.161.5	Telegram Messenger LLP	GET /test_TELEGRAM-2 HTTP/1.1	TelegramBot (like TwitterBot)

INDICATORS

TARGET INTERNAL CHECKS

KRBTGT RESET

```
[redacted] get-aduser krbtgt -properties passwordlastset


DistinguishedName : CN=krbtgt,CN=Users,DC=[redacted]DC=net
Enabled           : False
GivenName         :
Name              : krbtgt
ObjectClass       : user
ObjectGUID        : d029589c-f6ad-4b4c-96c2-2613d[redacted]
PasswordLastSet   : 23/08/2010 17:20:00
SamAccountName    : krbtgt
SID               : S-1-5-21-1561531455-114652488[redacted]-502
Surname           :
UserPrincipalName : krbtgt@[redacted]net
```

PASSWORD RESET OF SPECIFIC ACCOUNTS

```
beacon> help BlueCheck
Synopsis: BlueCheck

Use Active Directory Service Interfaces (ADSI) to query for user password changes.

beacon> BlueCheck krbtgt
[*] Tasked beacon to spawn BlueCheck
[+] host called home, sent: 103479 bytes
[+] received output:
[+] BLUECHECK: stroop.local\krbtgt password last changed at: 1/27/2020 8:41:40 AM, account disabled.
beacon> BlueCheck admin-w.trommel
[*] Tasked beacon to spawn BlueCheck
[+] host called home, sent: 103488 bytes
[+] received output:
[+] BLUECHECK: stroop.local\admin-w.trommel password last changed at: 1/27/2020 8:53:19 AM, password n
[L-WIN223] w.tax/6340
beacon>
```

INDICATORS OF ANALYSES / INVESTIGATION / DETECTION

TYPE OF CHECK	DETAIL
Online service	**AV hash** : hash of our malware is known at VirusTotal or others
	Infra blacklist : IP, URL of TLS cert blacklist
Traffic to infra	**C2 scanners** : global scans for C2 tool artefacts
	AV sandbox : C2 session from a known malware sandbox
	Analyst traffic : traffic from analyst, e.g. TOR IP, curl, other URIs
	Sec Vendor traffic : security vendor visits our infra – each with own characteristics
	Instant Messaging : ‘previews’ of Instant Messaging clients
Target internal	**KRBTGT / admin reset** : unexpected password changes of critical accounts
	Security tool : unexpected change of AV / EDR tools installed

START SUPERCHARGING YOUR RED TEAM

WHERE TO BEGIN

Planning

- RedELK server is intended per operation. Do not mix clients.
- Stores high confidential data.
- 3 components: RedELK server, c2server, redirector
- Identifiers used for Attack Scenario and Component Name
- Requires modified logging by redirector, e.g. Apache or HAProxy
- Read the docs: wiki on Github and blog post series

Installation

- Get latest release at Github. Or YOLO try `master` or `maindev` branch.
- Modify config file and run `./initial-setup.sh certs/config.cnf`
- Run installers for redirs, c2servers and main RedELK server
- Post installation edits (`/etc/redelk/*` and `/etc/cron.d/redelk`)

SUPPORT AND ROADMAP

Version 1

- Main focus on oversight, help the RT operator with his workflow
- Alarms for basic checks
- Support for Cobalt Strike C2
- Support for HAProxy and Apache redirectors

Version 2 – currently in dev

- Main focus on alarms and more supported tech
- More alarms and making alarms easier to manage
- Support for PoshC2, and possibly more (Scythe, Covenant)
- Support for Nginx and possibly Infra as Code redirectors
- Bring Hunting to Red Teams with integrated Jupyter Notebooks

ACKNOWLEDGEMENTS

@xychix : co-developer, python ninja and automation enthusiast

@curi0usJack : Ansible Playbooks for RedELK:
https://www.trustedsec.com/blog/automating-a-redelk-deployment-using-ansible/

@_xpn_ : wrangling RedELK into docker containers:
https://twitter.com/_xpn_/status/1263401556843659264

@benpturner : PoshC2 support

@fastlorenzo, @justly, etc for pull request

Many people/firms reaching out with support: happy to give back to the community

SUMMARY

Goal of Red Teaming is to make Blue Teams better

Dear red, RedELK is here to help you

Dear blue, think of your OPSEC

https://github.com/OutflankNL/RedELK

https://outflank.nl/blog/

OUTFLANK

clear advice with a hacker mindset

Marc Smeets
+31 6 5136 6680
marc@outflank.nl
www.outflank.nl/marc
@MarcOverIP