

# 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

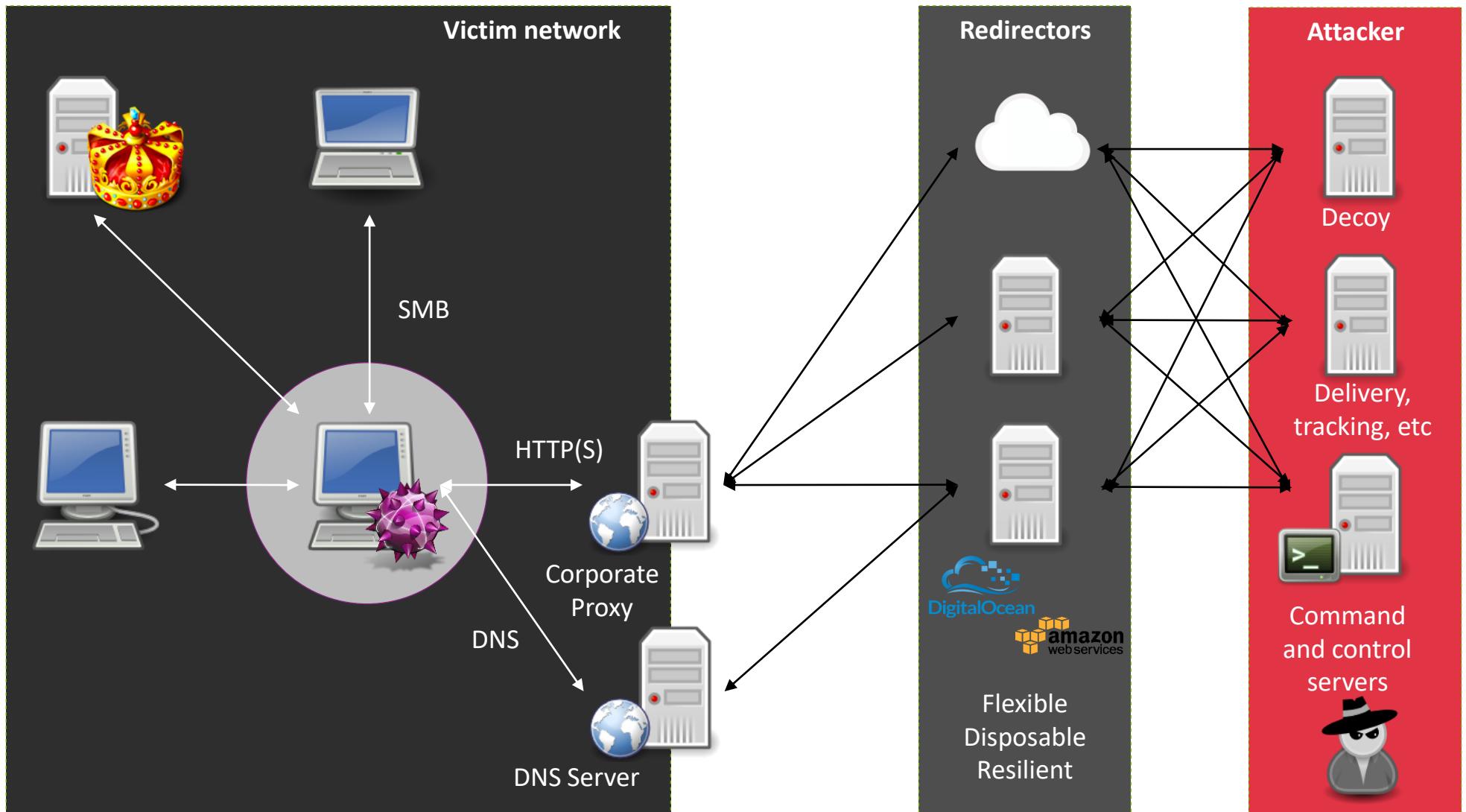
- Red Team operator, tool builder, trainer
- In offensive security since 2006
- Backgrounds: system and network engineering, and security consulting
- Blue Team Threat Hunting experience

## 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>



# 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

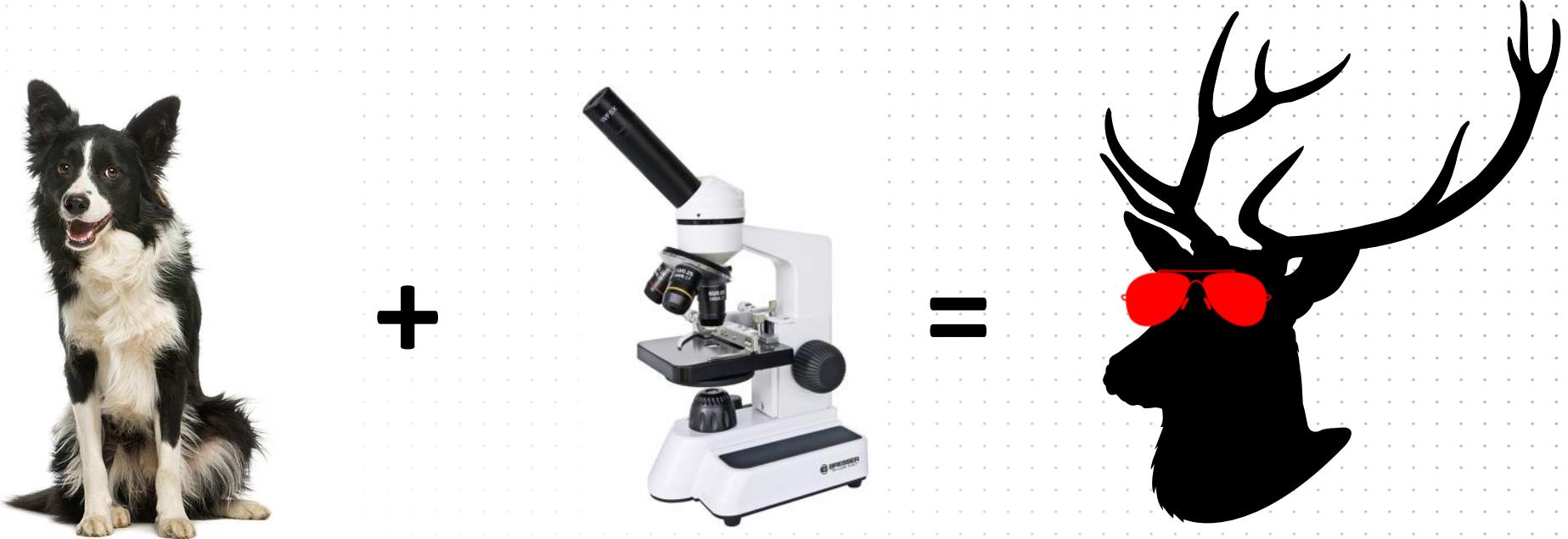


Insight



“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/>

## Redirectors / 1<sup>st</sup> 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

Data feeds



“SIEM”



Dashboard



Index



Enrich



Search

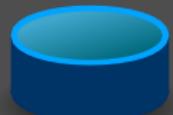
## Target SOC



Analyst submits samples and IOCs

Query for indicators of our attack

## Security service providers



Spamhaus  
Virustotal  
IBM X-Force  
Domain classifiers  
...

## White team

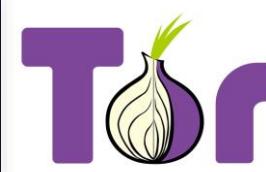


## Red team



Searching and alerting

# DATA ENRICHMENT



reverse DNS



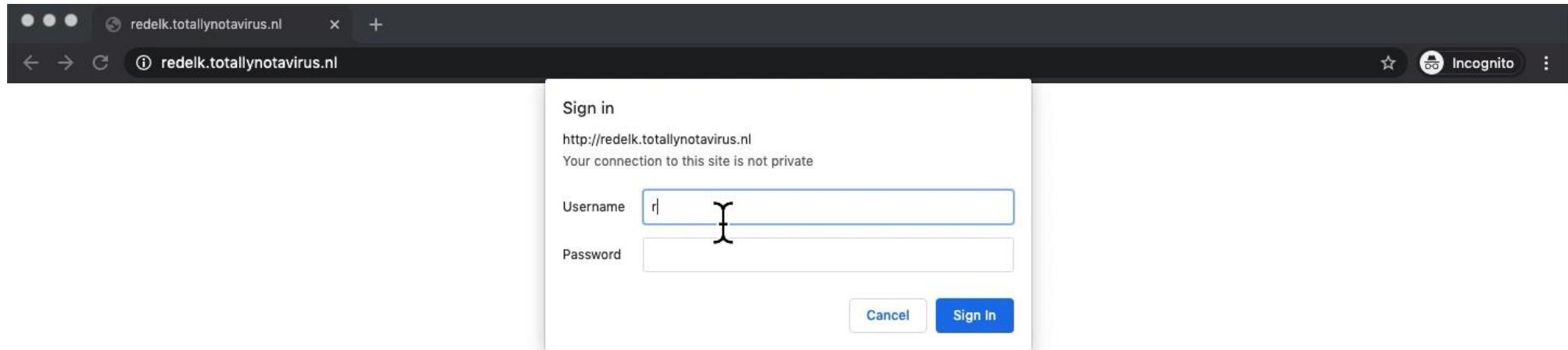
GREY NOISE



# SEE EVERYTHING

Central overview of the operation

# PRE-MADE VIEWS



# REDIRECTOR TRAFFIC

Discover: Redirector Traffic - K × +

Not Secure | redek.totallynotavirus.nl/app/kibana#/discover/0f7dc70-b982-11e8-94dd-171ae5c1fd1a?\_g=(refreshInterval:(pause:1t,value:0),time:(from:now-7d,mode:qui... Q ☆ Incognito :)

Redirector Traffic 10,005 hits

New Save Open Share Inspect C Auto-refresh < ⏪ Last 7 days >

> Search... (e.g. status:200 AND extension:PHP) Options Refresh

Add a filter +

March 23rd 2020, 17:01:38.497 - March 30th 2020, 17:01:38.497 — Auto

Count

2020-03-24 01:00 2020-03-25 01:00 2020-03-26 01:00 2020-03-27 01:00 2020-03-28 01:00 2020-03-29 01:00 2020-03-30 02:00

@timestamp per 3 hours

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

Discover: Red Team Operations

Not Secure | redek.totallynotavirus.nl/app/kibana#/discover/1c580960-b6a9-11e8-bc1a-cf8fa3255855?\_g=(refreshInterval:(pause:1t,value:0),time:(from:now-72h,mode:relative,to:n...)

Incognito

The histogram displays the frequency of events over time. The x-axis represents the timestamp per hour, and the y-axis represents the count of events. There are two main clusters of activity: one around 14:00 on March 29 with counts between 20 and 40, and a larger cluster on March 30 between 02:00 and 14:00 with counts ranging from 20 to over 200.

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/downloadsforDomainadministration.txt C:\users\w.trommel\de...
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

Discover: CS Screenshots - Kit x +

Not Secure | redelk.totallynotavirus.nl/app/kibana#/discover/e8de79f0-b6aa-11e8-bc1a-cf8fa3255855?\_g=(refreshInterval:(pause:1t,value:0),time:(from:now-72h,mode:relative,to:now))&\_sourceType=cloud

Incognito

CS Screenshots 6 hits

New Save Open Share Inspect Auto-refresh Last 72h Options Refresh

Search... (e.g. status:200 AND extension:PHP)

beacon\_output: ""received screenshot"" Add a filter

Actions ▾

March 28th 2020, 21:23:43.867 - March 31st 2020, 22:23:43.867 — Auto

Count

@timestamp per hour

Time	attackscenario	target_hostname	target_user	screenshotfull	screenshotthumb
Mar 30 2020, 10:03:35	shorthaul	L-WIN223	w.tax	/cslogs/c2server1/logs/200330/10.1.310/screenshots/screen_080335_936715360.jpg	
Mar 30 2020, 09:58:30	shorthaul	L-WIN223	w.tax	/cslogs/c2server1/logs/200330/10.1.310/screenshots/screen_075830_936715360.jpg	
Mar 30 2020, 09:57:07	shorthaul	L-WIN223	w.tax	/cslogs/c2server1/logs/200330/10.1.310/screenshots/screen_075707_936715360.jpg	

# ALL IOCS

Discover: CS IOCs - Kibana × redek.totallynotavirus.nl/cslog × + Not Secure | redek.totallynotavirus.nl/app/kibana#discover/4c003e20-b6aa-11e8-bc1a-cf8fa3255855?\_g=(refreshInterval:(pause:it,value:0),time:(from:now-72h,mode:relative,to:n...)| Incognito :| CS IOCs 6 hits New Save Open Share Inspect Auto-refresh Last 72h Options Refresh

> \_ Search... (e.g. status:200 AND extension:PHP)

cslogtype: "ioc" Add a filter + Actions ▾

March 28th 2020, 20:52:17.863 - March 31st 2020, 21:52:17.863 — Auto

Count

2020-03-29 01:00 2020-03-29 14:00 2020-03-30 02:00 2020-03-30 14:00 2020-03-31 02:00 2020-03-31 14:00

@timestamp per hour

Time	attackscenario	target_user	target_ipint	ioc_type	ioc_hash	ioc_name	ioc_bytessize	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\A DMIN\$\203b554.exe	289,280	[indicator] file: 10ba5a6a5e0316fedf7fd10d257b3f91 289280 bytes \\L-WIN27\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: f06d1ae4cbde0 150,016 bytes

# INDICATORS

## ONLINE SERVICES

# HASH OF MALWARE



Symantec EDR

Symantec EDR is Healthy

Marc Smeets

**Good**  
DISPOSITION**Insight**  
REASON**No**  
TARGETED ATTACK38847dc4c82c0 [REDACTED] cdac7b50ab8602e8fdfad4401954c87  
SHA25673c519f050c20 [REDACTED]  
MD5Microsoft Windows  
CERTIFICATEUnknown  
MIME TYPE

## File Overview

1 RELATED INCIDENTS

0 EMAIL DETECTIONS

0 CRYPT MODIFICATIONS

0 EXTERNAL DOMAINS ACCESSED

## Global Reputation

Months ago  
FIRST SEENMillions of users  
PREVALENCE

## Local Reputation

Months ago  
FIRST SEEN17737 internal endpoints  
PREVALENCE[Process Dump](#) [Add to Blacklist](#) [Add to Whitelist](#) [Submit to Sandbox](#) [Submit to VirusTotal](#) [Copy to File Store](#) [Delete File](#) [Details](#)[File Attributes](#)[Related Events](#)

# HASH OF MALWARE

machine1 > ⚡ Process has injected code into another process. > File

File worldwide



Actions ▾

Sha1: 93e44751e2ac832448c99bab7136e6fe341b74f6

MD5: c667972576a0855899c8c7c9dcf5d7b

Sha256: 4a92955a951220102167b9916d461ea4b9308dbe2fecc42b5413ed5f1af332d1

Size: 4.7 MB

Signer: Microsoft Corporation

Issuer: Microsoft Code Signing PCA

Malware detection

Virus Total detection ratio:

0/57

Virus Total

Windows Defender AV:

No detections found

Prevalence worldwide

2.2k

First seen: 7 months ago

Last seen: 16 hours ago

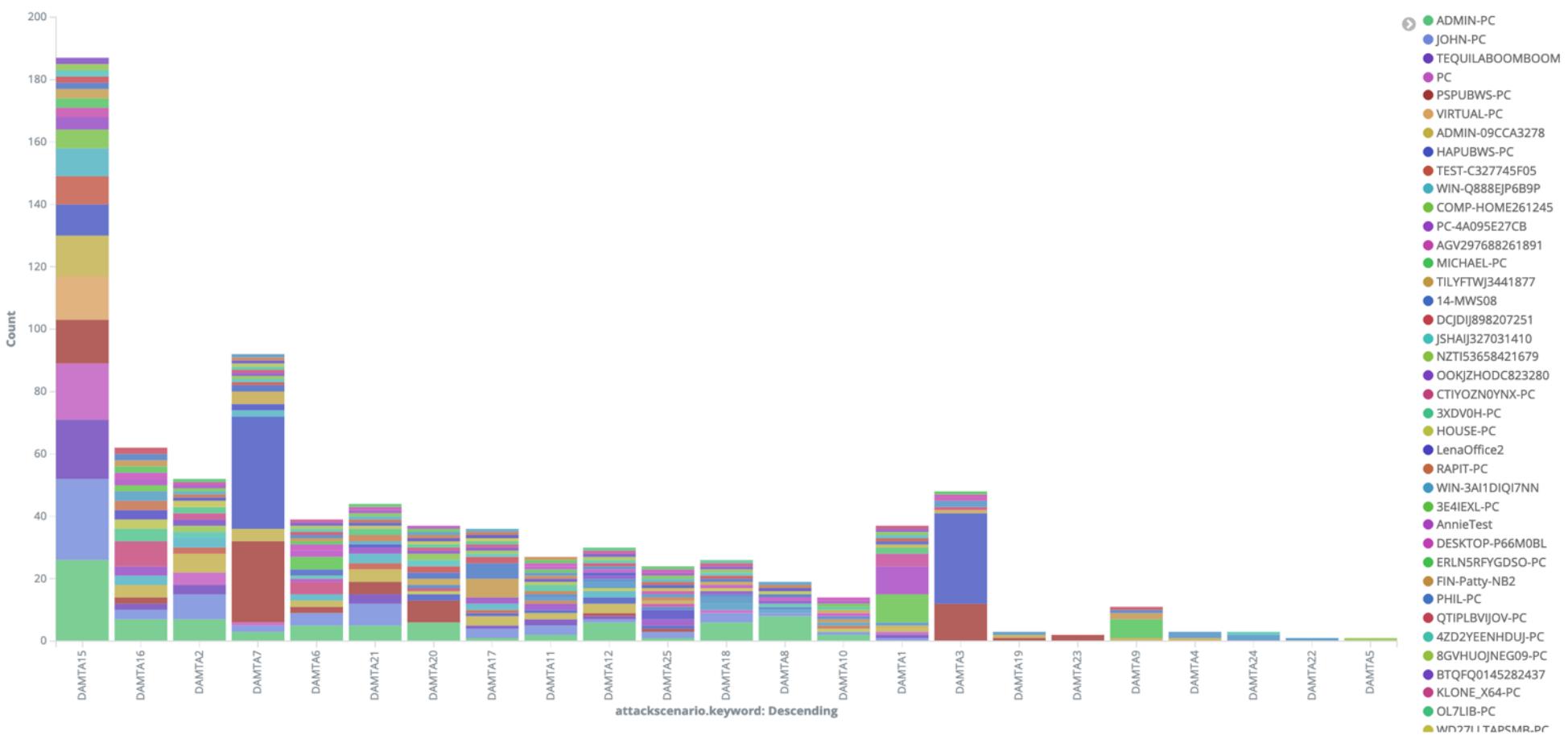
Deep analysis

Deep analysis request ?

Submit

# SANDBOX CONNECTIONS

DAMTA - new AV beacons



# 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	149.154.1 61.16	149.154.161.16	Telegram Messenger LLP	GET /test_TELEGRAM-20190317_2 HTTP/1.1	TelegramBot (like TwitterBot)
www-decoy	149.154.1 61.11	149.154.161.11	Telegram Messenger LLP	GET /test_TELEGRAM-20190317_22	TelegramBot (like TwitterBot)
www-decoy	149.154.1 61.17	149.154.161.17	Telegram Messenger LLP	GET /test_TELEGRAM- 20190317_223 HTTP/1.1	TelegramBot (like TwitterBot)
www-decoy	149.154.1 61.10	149.154.161.10	Telegram Messenger LLP	GET /test_TELEGRAM- 20190317_2234 HTTP/1.1	TelegramBot (like TwitterBot)
www-decoy	149.154.1 61.17	149.154.161.17	Telegram Messenger LLP	GET /test_TELEGRAM-20190317_	TelegramBot (like TwitterBot)
www-decoy	149.154.1 61.3	149.154.161.3	Telegram Messenger LLP	GET /test_TELEGRAM-2019031	TelegramBot (like TwitterBot)
www-decoy	149.154.1 61.19	149.154.161.19	Telegram Messenger LLP	GET /test_TELEGRAM-20190317	TelegramBot (like TwitterBot)
www-decoy	149.154.1 61.12	149.154.161.12	Telegram Messenger LLP	GET /test_TELEGRAM-201903	TelegramBot (like TwitterBot)
www-decoy	149.154.1 61.18	149.154.161.18	Telegram Messenger LLP	GET /test_TELEGRAM-20190	TelegramBot (like TwitterBot)
www-decoy	149.154.1 61.18	149.154.161.18	Telegram Messenger LLP	GET /test_TELEGRAM-2019	TelegramBot (like TwitterBot)
www-decoy	149.154.1 61.8	149.154.161.8	Telegram Messenger LLP	GET /test_TELEGRAM-20 HTTP/1.1	TelegramBot (like TwitterBot)
www-decoy	149.154.1 61.16	149.154.161.16	Telegram Messenger LLP	GET /test_TELEGRAM-201	TelegramBot (like TwitterBot)
www-decoy	149.154.1 61.5	149.154.161.5	Telegram Messenger LLP	GET /test_TELEGRAM-2 HTTP/1.1	TelegramBot (like TwitterBot)

# INDICATORS

## TARGET INTERNAL CHECKS

# KRBTGT RESET

```
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 ← REDACTED
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 ne
```

```
[L-WIN223] w.tax/6340
```

```
beacon>
```

# INDICATORS OF ANALYSES / INVESTIGATION / DETECTION

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

**@curiousJack** : 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](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](http://www.outflank.nl/marc)

@MarcOverIP