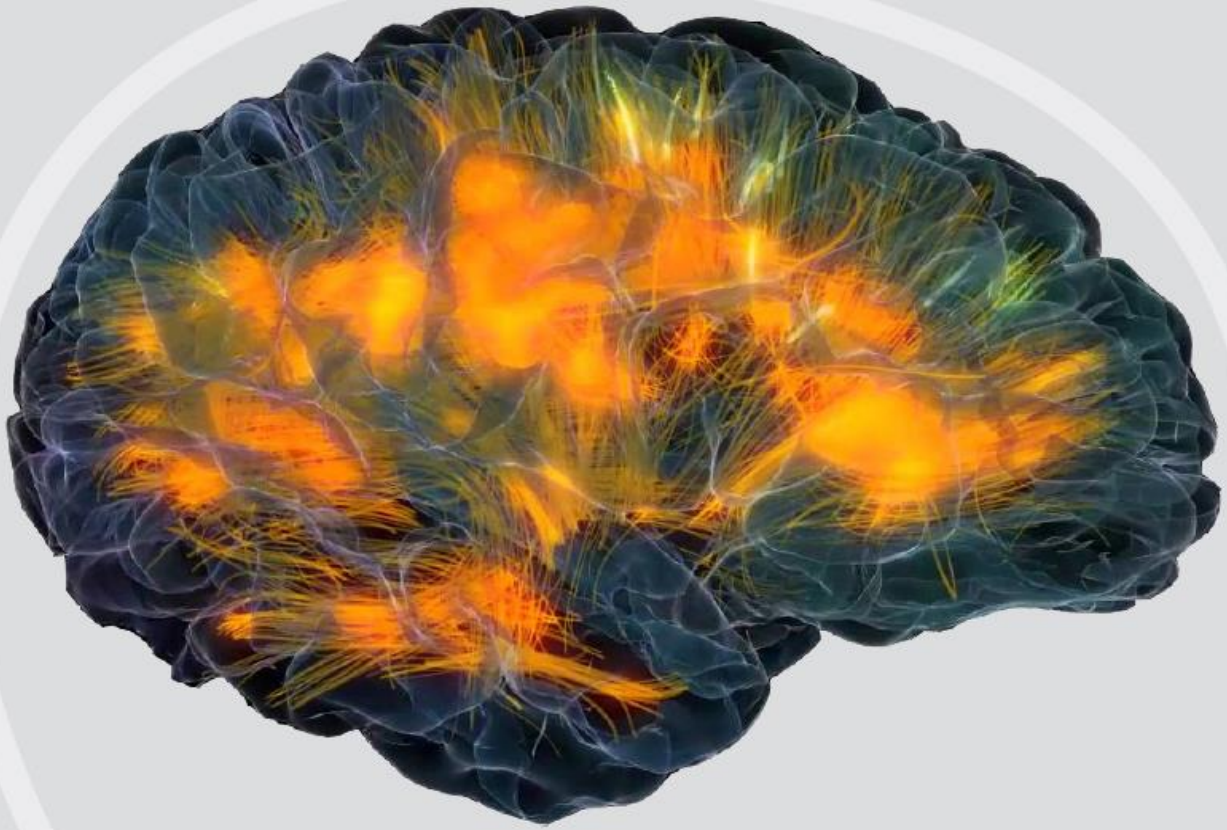


INTELLIGENT NETWORK TRAFFIC ANALYSIS

Michal Drozd
Bratislava 24.4.2018

Beset

GREYCORTEX

Beset

25 years on the market

Core business: software development, system integration, information security, ERP systems for small and medium sized enterprises

GREYCORTEX partner for Slovak Republic

GREYCORTEX

4 years on the market

Network traffic analysis solution for Medium businesses, Enterprise, Government

Seeing threats others miss

Based on university research of machine learning and malware and ethical hacking experience

THE SECURITY GAP…

widespread
ADVANCED THREATS

BAD NETWORK VISIBILIITY

Beset GREYCORTEX

GREYCORTEX NETWORK TRAFFIC ANALYSIS

= statistical analysis, **machine learning**, **artificial intelligence**, metadata and content inspection to detect suspicious activities on the network

≠ NetFlow analysis, full-packet capture

Undetected malware
Insider threats
Forensic investigation
Network visibility
Performance Monitoring
IoT and Standard devices

Rapid Detection & Response

for SOC Capability

Effective

Because Threats Create Detectable Traffic

Beset GREYCORTEX

WHY NTA FROM GREYCORTEX

Gartner : Security monitoring = key value

NEW DETECTION TECHNIQUES

Most advanced behavioural detection (machine learning, discovery, …)

Unique detection algorithms (machine-behaviour)

Powerful signature-based detection with DPI (over 45.000 signatures)

Event correlation

L7 analysis

SSL traffic analysis

BETTER ANALYTICS TECHNIQUES

Unique database approach

Network Search & Visualization

Filter individual subnets, hosts, devices, and applications on the network

Unique behaviour analysis

Unique data set of network metrics

Bi-directional flows

60 – 900 parameters (e.g. spectral analysis of SSL)

Beset GREYCORTEX

NTA FOR
GDPR COMPLIANCE

GREYCORTEX

GDPR

- Článek 24 - Odpovědnost správce

  ...Vhodná technická a organizační opatření

- Článek 32 - Zabezpečení zpracování

- Článek 33+34 - Ohlašování případů porušení zabezpečení

ČLÁNEK 24 - ODPOVĚDNOST SPRÁVCE

1. S přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob zavede správce **vhodná technická a organizační opatření, aby zajistil a byl schopen doložit, že zpracování je prováděno v souladu** s tímto nařízením. Tato opatření musí být podle potřeby revidována a aktualizována.

2. Pokud je to s ohledem na činnosti zpracování přiměřené, zahrnují opatření uvedená v odstavci 1 uplatňování vhodných koncepcí v oblasti ochrany údajů správcem.

3. Jedním z prvků, jimiž lze doložit, že správce plní příslušné povinnosti, je dodržování schválených kodexů chování uvedených v článku 40 nebo schválených mechanismů pro vydávání osvědčení uvedených v článku 42.

ČLÁNEK 32 - ZABEZPEČENÍ ZPRACOVÁNÍ

1. S přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, provedou správce a zpracovatel vhodná technická a organizační opatření, aby zajistili úroveň zabezpečení odpovídající danému riziku, případně včetně:

a) pseudonymizace a šifrování osobních údajů;

b) schopnosti zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování;

c) schopnosti obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů;

d) procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.

2. Při posuzování vhodné úrovně bezpečnosti se zohlední zejména rizika, která představuje zpracování, zejména náhodné nebo protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim.

3. Jedním z prvků, jimiž lze doložit soulad s požadavky stanovenými v odstavci 1 tohoto článku, je dodržování schváleného kodexu chování uvedeného v článku 40 nebo uplatňování schváleného mechanismu pro vydávání osvědčení uvedeného v článku 42.

4. Správce a zpracovatel přijmou opatření pro zajištění toho, aby jakákoliv fyzická osoba, která jedná z pověření správce nebo zpracovatele a má přístup k osobním údajům, zpracovávala tyto osobní údaje pouze na pokyn správce, pokud jí jejich zpracování již neukládá právo Unie nebo členského státu.

ČLÁNEK 33+34 - OHLAŠOVÁNÍ PŘÍPADŮ PORUŠENÍ ZABEZPEČENÍ

…

WHAT'S HIDING IN THE NETWORKS?

CASE 1 – UNKNOWN (YET) BOTNET

A Device on an Internal Network:

Periodically attempts to communicate at port 30303

CASE 1 – UNKNOWN (YET) BOTNET

Unsupervised Learning	***Machine Behavior***	*Flow-based Detection*	*Discovery Analysis*	***Other***
	Periodic repetitive communication at port 30303			Communication with low reputation IP

Beset GREYCORTEX

GREYCORTEX MENDEL

Dashboard | Network | Events | Incidents

Září 2017

P	Ú	S	Č	P	S	N
28	29	30	31	1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	1

Filters:

Subnet:
Host:
Service: 30303
Event:
Traffic: Outbound
MAC: c4:e9:84:02:e2:69
Incident:
Severity:
Reps:

Clear | Filter

Status Monitor

1 No Issues

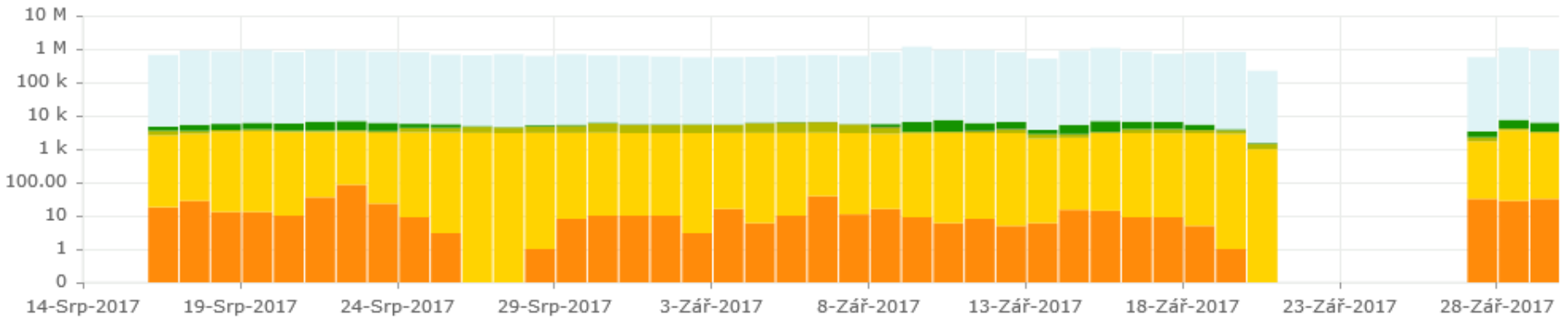
User: support (GreyCortex support)

License: GreyCortex s.r.o. (tomas.ladr@greycortex.com)

Version: 2.8.0

Chart | Map

Traffic



	Name	Src Hosts	Dst Hosts	Events	Date
7	Periodic: Repetitive Connections (every 30 minutes in 6 hours)	1	1	13	Aug-21 23:00 – Sep-07 00:37
7	blacklist: Spamhaus DROP blacklist	1	5	512	Aug-16 11:15 – Fri 01:37
6	Periodic: Repetitive Connections (every 30 minutes in 6 hours)	1	12	317	Aug-18 18:09 – Thu 16:25
6	Scan: Port Sweep-like Behavior (horizontal port scan)	1	1	102.6 k	Aug-14 13:33 – Fri 02:00
6	blacklist: Blocklist.de blacklist	1	5	243	Aug-17 07:22 – Sep-20 00:02
6	blacklist: Tor blacklist	1	41	6.4 k	Aug-16 02:35 – Fri 01:53
6	blacklist: Compromised or Hostile Host Traffic	1	1	4	Aug-16 10:21 – Sep-08 14:59
6	blacklist: BotCC blacklist	1	3	315	Aug-19 08:53 – Thu 23:06
6	blacklist: General blacklist	1	6	142	Aug-16 19:21 – Sep-20 00:26
5	Periodic: Repetitive Connections (every 30 minutes in 6 hours)	1	5103	46.2 k	Aug-14 23:55 – Fri 00:57
5	p2p: Edonkey Search Request (search by name)	1	1	1	Aug-30 20:04 – 20:05
3	Discovery: External Remote Service No Reply (latency problem)	1	398	1.8 k	Aug-18 12:51 – Wed 17:42
3		1			Aug-15 22:34 – Fri

CASE 2 – ETERNAL BLUE

A Device on the Observed Network:

Suddenly used a DNS tunnel and TOR network together, exchanging one message

After 4 hours of waiting, it started opening port 445/tcp connections on multiple external hosts

Tried to use CVE-2017-0143 (exploit MS17-010) on the connected host

CASE 2 – ETERNAL BLUE

Unsupervised Learning	*Machine Behavior*	***Flow-based Detection***	*Discovery Analysis*	***Other***
Outlier: high number of communication peers & flows		Network scan 445/tcp to internet		Correlation rule matched: malware spreading to internet IDS rules matched: DNS tunnel, TOR IDS rule matched: Eternal Blue (based on CVE-2017-0143, exploit MS17-010)

Beset GREYCORTEX

GREYCORTEX MENDEL

Dashboard | Network | Events

Září 2017

P	Ú	S	Č	P	S	N
28	29	30	31	1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	1

Filters:

Subnet:
Host: 192.168.1.192
Service:
Event:
Traffic:
Sensor: Mercy
Severity:
Reps:

Clear | Filter

Status Monitor

9 Mercy

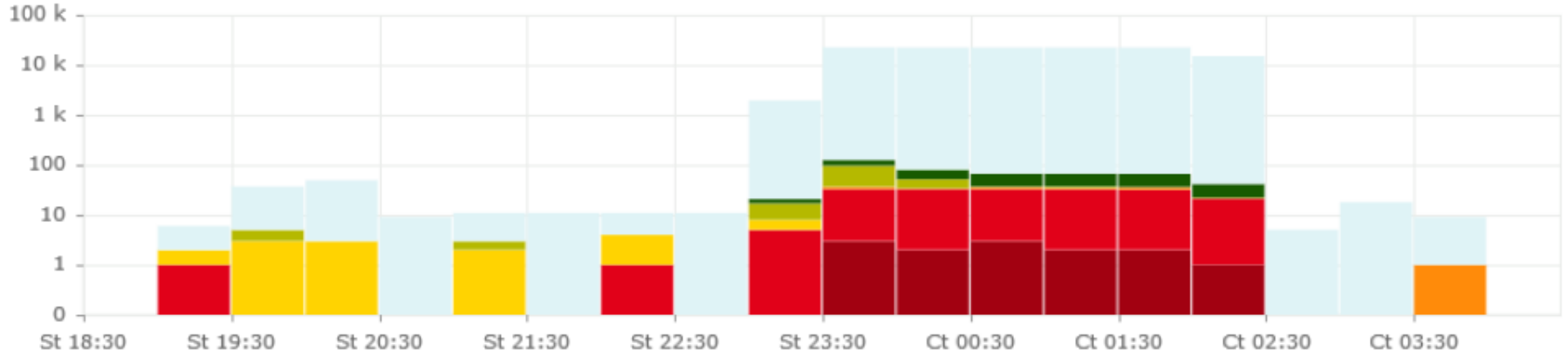
User: administrator (Administrator)

License: Tomas Chomo (tomas.chomo@greycortex.cc

Version: 2.8.0

Chart | Map

Traffic



	Name	Src Hosts	Dst Hosts	Events	Date
9	correlation: Malware spreading	1	1	13	Wed 23:26 – Thu 02:14
8	Scan: SMB Port Sweep (445)	1	1	174	Wed 23:26 – Thu 02:19
8	policy: Request to an external DNS server	1	1	1	Wed 19:27 – 19:28
8	correlation: TOR communication	1	1	4	Wed 22:21 – Thu 01:22
7	exploit: ETERNALBLUE Exploit M2 MS17-010	1	12	12	Wed 23:37 – Thu 03:55
7	blacklist: Spamhaus DROP blacklist	1	3	3	Thu 01:25 – 01:59
6	policy: TLS possible TOR SSL traffic	1	3	6	Wed 19:30 – Thu 01:22
6	blacklist: Tor blacklist	1	6	12	Wed 19:28 – Thu 01:22
5	outlier: Peers at Host	1	1	42	Wed 23:25 – Thu 00:07
5	outlier: Flows at Host	1	1	42	Wed 23:25 – Thu 00:07
5	scan: Behavioral Unusual Port 445 traffic Potential Scan or Infection	1	1	1	Thu 00:10 – 00:11

CASE 3 – WANNACRY

A Device on the Observed Network:

Started opening port 445/tcp connections on multiple hosts, external and internal

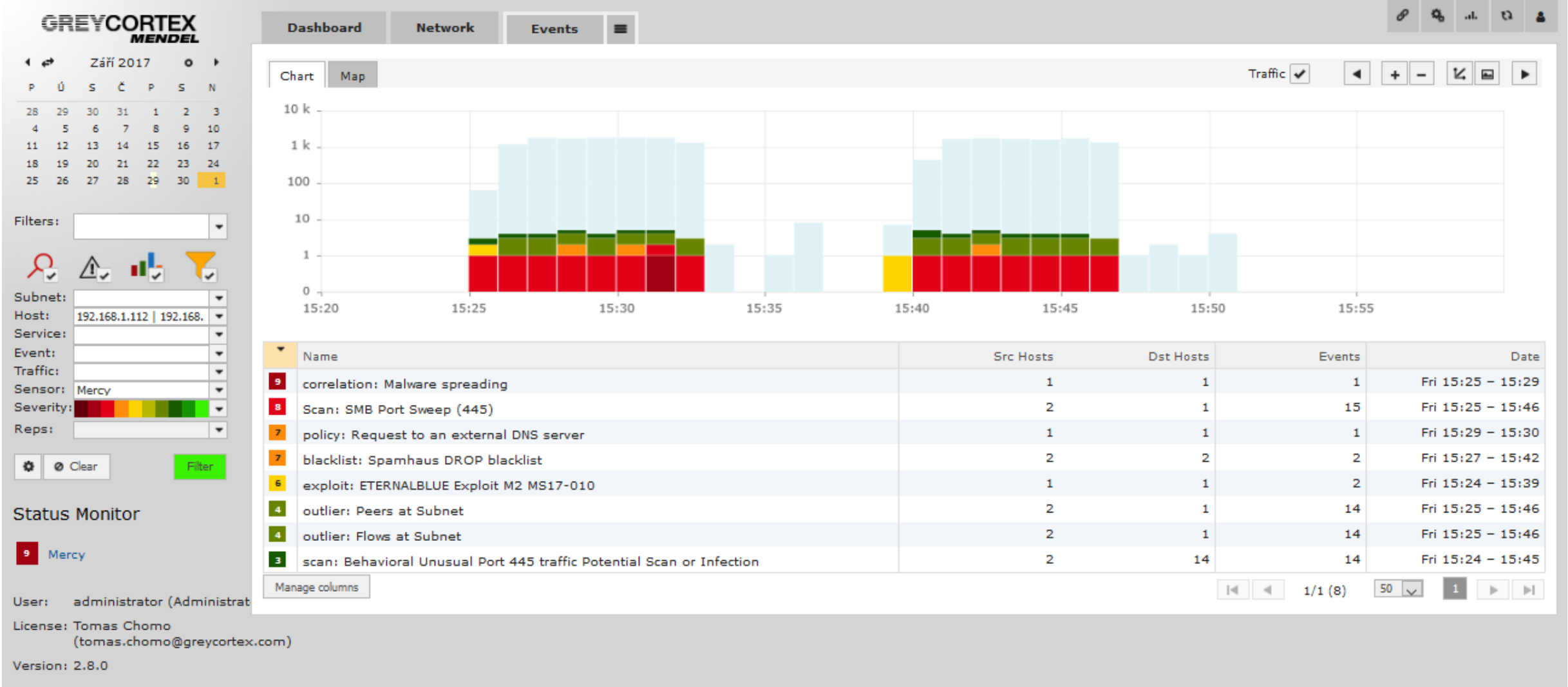
Successfully used CVE-2017-0143 (exploit MS17-010) on another internal host immediately

The second device started exhibiting the same behavior

CASE 3 – WANNACRY

Unsupervised Learning	*Machine Behavior*	***Flow-based Detection***	*Discovery Analysis*	***Other***
Outlier: high number of communication peers & flows		Network scan 445/tcp to internal network and internet		Correlation rule matched: malware spreading to internal network **A day after** updated IDS rule matched: WannaCry variant (CVE-2017-0143, exploit MS17-010)

Beset GREYCORTEX


GREYCORTEX MENDEL
Dashboard
Network
Events
Září 2017
P Ú S Č P S N
28 29 30 31 1 2 3
4 5 6 7 8 9 10
11 12 13 14 15 16 17
18 19 20 21 22 23 24
25 26 27 28 29 30 1
Filters:
Subnet:
Host: 192.168.1.112 | 192.168.
Service:
Event:
Traffic:
Sensor: Mercy
Severity:
Reps:
Clear
Filter
Status Monitor
9 Mercy
User: administrator (Administrat
License: Tomas Chomo
(tomas.chomo@greycortex.com)
Version: 2.8.0
Chart
Map
Traffic
10 k
1 k
100
10
1
0
15:20
15:25
15:30
15:35
15:40
15:45
15:50
15:55
Name
Src Hosts
Dst Hosts
Events
Date
9 correlation: Malware spreading 1 1 1 Fri 15:25 – 15:29
8 Scan: SMB Port Sweep (445) 2 1 15 Fri 15:25 – 15:46
7 policy: Request to an external DNS server 1 1 1 Fri 15:29 – 15:30
7 blacklist: Spamhaus DROP blacklist 2 2 2 Fri 15:27 – 15:42
6 exploit: ETERNALBLUE Exploit M2 MS17-010 1 1 2 Fri 15:24 – 15:39
4 outlier: Peers at Subnet 2 1 14 Fri 15:25 – 15:46
4 outlier: Flows at Subnet 2 1 14 Fri 15:25 – 15:46
3 scan: Behavioral Unusual Port 445 traffic Potential Scan or Infection 2 14 14 Fri 15:24 – 15:45
Manage columns
1/1 (8)
50
1

CASE 4 – CRYPTOCOIN MINING

Active mining:

Cryptocoin mining mostly on compromised servers or endpoint devices

Passive minig:

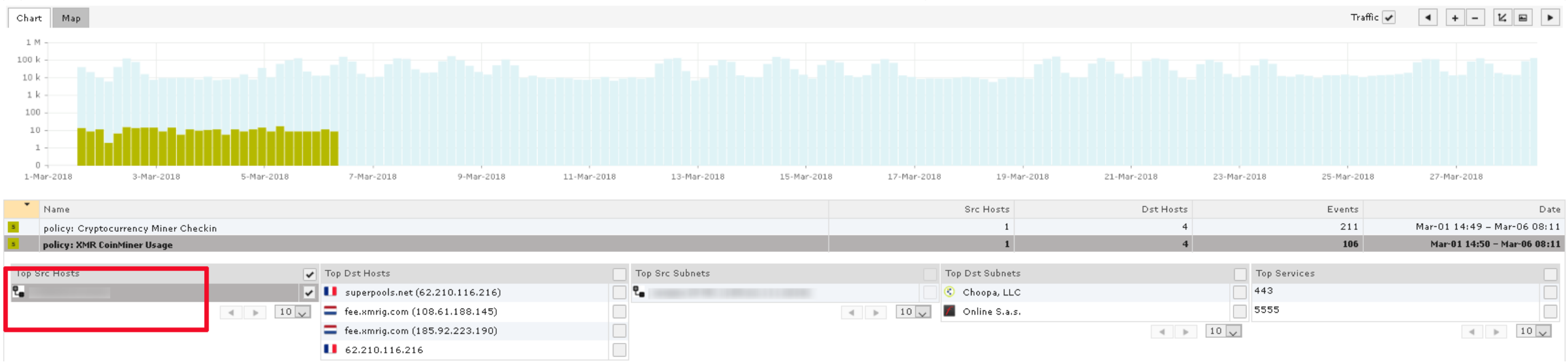
Built-in javascript miner on web application

CASE 4 – CRYPTOCOIN MINING

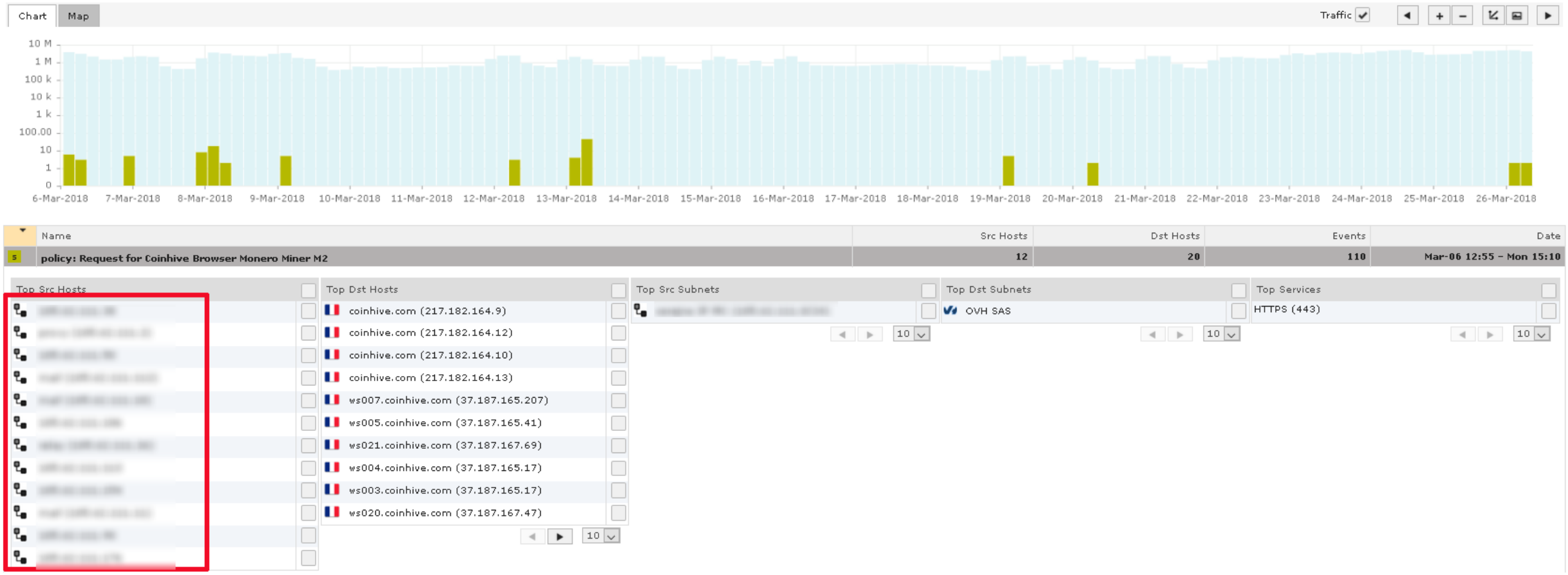
Unsupervised Learning	***Machine Behavior***	*Flow-based Detection*	*Discovery Analysis*	***Other***
	Periodic repetitive communication at port 443 or 5555			Detection signature

Beset GREYCORTEX

CASE 4 – ACTIVE CRYPTOCOIN MINIG



CASE 4 – PASSIVE CRYPTOCOIN MINING



Beset GREYCORTEX

CASE 5 – LETHIC SPAMBOT

A Device in the Observed Network:

Queried external DNS servers (Google) for known-infected server names

Communicated via port 1123 to servers in Norway

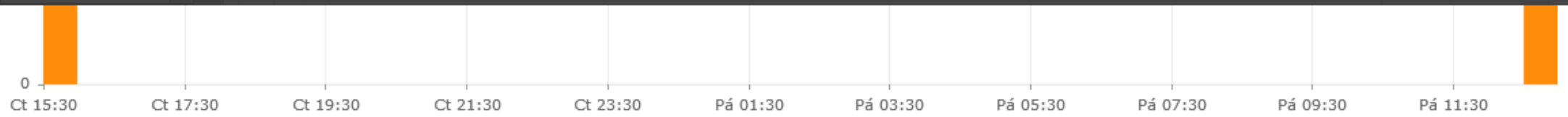
Silenced traffic when the device was running anti-virus scanner and remained silent for the next two hours, later resuming communication on port 1123

Communicated periodically to MS Hotmail service on port 25/tcp

CASE 5 – LETHIC SPAMBOT

Unsupervised Learning	***Machine Behavior***	***Flow-based Detection***	***Discovery Analysis***	***Other***
Outlier: high number of communication peers & flows	SMTP Permanent Communication Anomaly: Communicated periodically to MS Hotmail service on port 25/tcp		A new service on a host discovered	IDS rule matched (Lethic SpamBOT) External DNS server, poor reputation Ips High external DNS traffic (1-2 queries reached170)

Beset GREYCORTEX



Src Host	Src MAC	Src Subnet	Dst Host	Dst MAC	Dst Subnet	Src Port	Service	Service Type	Protocol	Src Flags	Dst Flags
R[redacted] (10.9.168.38)	c4:85:08:4b:ab	[redacted] Wifi (10.8.0.0/15)	8.8.8.8	00:00:5e:00:01	Google Inc.	60909	DNS (53)	REMOTE	UDP (17)		

Description

Signature details

Signature ID:	2018455 (rev: 4)
Created:	2014-01-08
Severity:	6
Class:	Network Trojan
Matched rule:	alert udp any 53 -> $HOME_NET any
Properties:	content:"|00 01 00 01|"; content:"|00 04 c3 16 1a|"; distance:4; within:5; byte_test:1,>,224,0,relative; content:!"|0e|anubisnetworks|03|com|00|"; nocase; content:!"|05|mpsmx|03|net|00|"; nocase; content:!"|09|mailspike|03|com|00|"; nocase; threshold: type limit, track by_src, seconds 60, count 1;

View Signature Details

Packet bytes

```
0. F5 70 81 80 00 01 00 01 00 00 00 00 02 76 31 08   õp...........v1
1. 6A 73 6A 6C 75 6C 77 69 03 63 6F 6D 00 00 01 00   jsjlulwi.com...
2. 01 C0 0C 00 01 00 01 00 00 00 43 00 04 C3 16 1A   .À........C..Ã..
3. F8                                                ø
```

False positive | Capture | Report Incident | Show flows

R[redacted] (10.9.168.38)	c4:85:08:4b:ab:	[redacted] Wifi (10.8.0.0/15)	8.8.8.8	00:00:5e:00:01:	Google Inc.	56338	DNS (53)	REMOTE	UDP (17)		
R[redacted] (10.9.168.38)	c4:85:08:4b:ab:	[redacted] Wifi (10.8.0.0/15)	8.8.8.8	00:00:5e:00:01:	Google Inc.	55209	DNS (53)	REMOTE	UDP (17)		
R[redacted] (10.9.168.38)	c4:85:08:4b:ab:	[redacted] Wifi (10.8.0.0/15)	8.8.8.8	00:00:5e:00:01:	Google Inc.	61582	DNS (53)	REMOTE	UDP (17)		

CASE 6 – DOCUMENT LEAKAGE

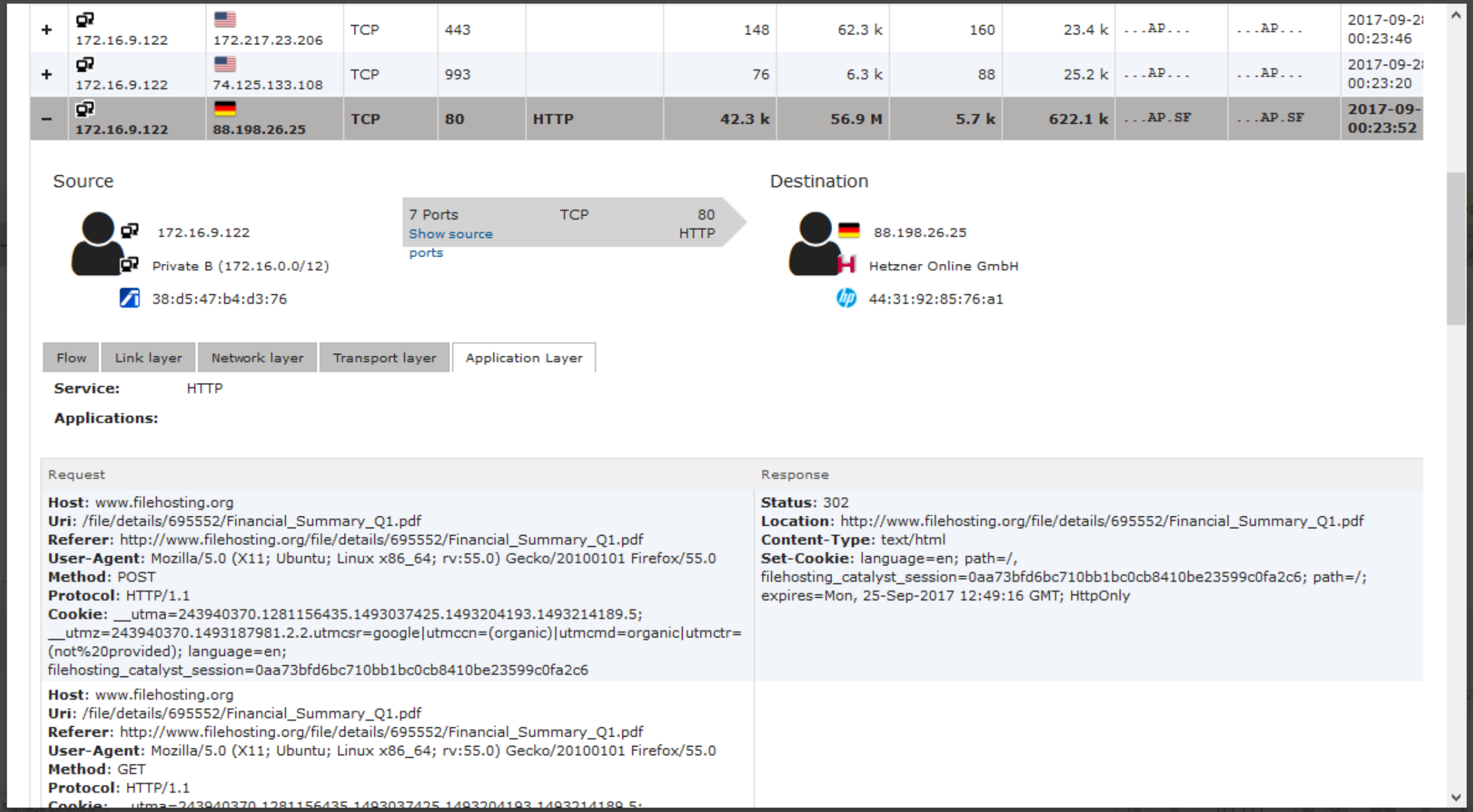
A Device on an Internal Network:

Exhibited an unusually high data transfer volume to an external network

CASE 6 – DOCUMENT LEAKAGE

Unsupervised Learning	*Machine Behavior*	*Flow-based Detection*	*Discovery Analysis*	***Other***
Outlier: high volume of data transfer detected (Severity 7) Outlier: high volume of data transfer detected (Severity 5)				L7 content analysis: file named _Financial_Summary _Q1.pdf_ uploaded to www21.filehosting.org; a domain of Hetzner Online GmbH

Beset GREYCORTEX


GREYCORTEX
Dashboard
Network
Events
+ 172.16.9.122 172.217.23.206 TCP 443 148 62.3 k 160 23.4 k ...AP... ...AP... 2017-09-2 00:23:46
+ 172.16.9.122 74.125.133.108 TCP 993 76 6.3 k 88 25.2 k ...AP... ...AP... 2017-09-2 00:23:20
– 172.16.9.122 88.198.26.25 TCP 80 HTTP 42.3 k 56.9 M 5.7 k 622.1 k ...AP.SF ...AP.SF 2017-09- 00:23:52
Source
172.16.9.122
Private B (172.16.0.0/12)
38:d5:47:b4:d3:76
7 Ports TCP 80
Show source ports
HTTP
Destination
88.198.26.25
Hetzner Online GmbH
44:31:92:85:76:a1
Flow
Link layer
Network layer
Transport layer
Application Layer
Service: HTTP
Applications:
Request
Host: www.filehosting.org
Uri: /file/details/695552/Financial_Summary_Q1.pdf
Referer: http://www.filehosting.org/file/details/695552/Financial_Summary_Q1.pdf
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:55.0) Gecko/20100101 Firefox/55.0
Method: POST
Protocol: HTTP/1.1
Cookie: __utma=243940370.1281156435.1493037425.1493204193.1493214189.5; __utmz=243940370.1493187981.2.2.utmcsr=google|utmccn=(organic)|utmcmd=organic|utmctr=(not%20provided); language=en; filehosting_catalyst_session=0aa73bfd6bc710bb1bc0cb8410be23599c0fa2c6
Response
Status: 302
Location: http://www.filehosting.org/file/details/695552/Financial_Summary_Q1.pdf
Content-Type: text/html
Set-Cookie: language=en; path=/, filehosting_catalyst_session=0aa73bfd6bc710bb1bc0cb8410be23599c0fa2c6; path=/; expires=Mon, 25-Sep-2017 12:49:16 GMT; HttpOnly
Host: www.filehosting.org
Uri: /file/details/695552/Financial_Summary_Q1.pdf
Referer: http://www.filehosting.org/file/details/695552/Financial_Summary_Q1.pdf
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:55.0) Gecko/20100101 Firefox/55.0
Method: GET
Protocol: HTTP/1.1

SUCCESS STORIES

DIEBOLD NIXDORF

T · · Systems ·

KIWI · COM

AST

Česká pošta

mga
MALTA GAMING AUTHORITY

Linde

TSB
TECHNICKÉ SÍTĚ BRNO

Czech Republic
Ministry of Transport

KONICA MINOLTA

BRNO UNIVERSITY OF TECHNOLOGY

UACM
Universidad Autónoma de la Ciudad de México
Nada humano me es ajeno

Beset

GREYCORTEX

INTELLIGENT NETWORK TRAFFIC ANALYSIS

GREYCORTEX

michal.drozd@greycortex.com



Beset GREYCORTEX