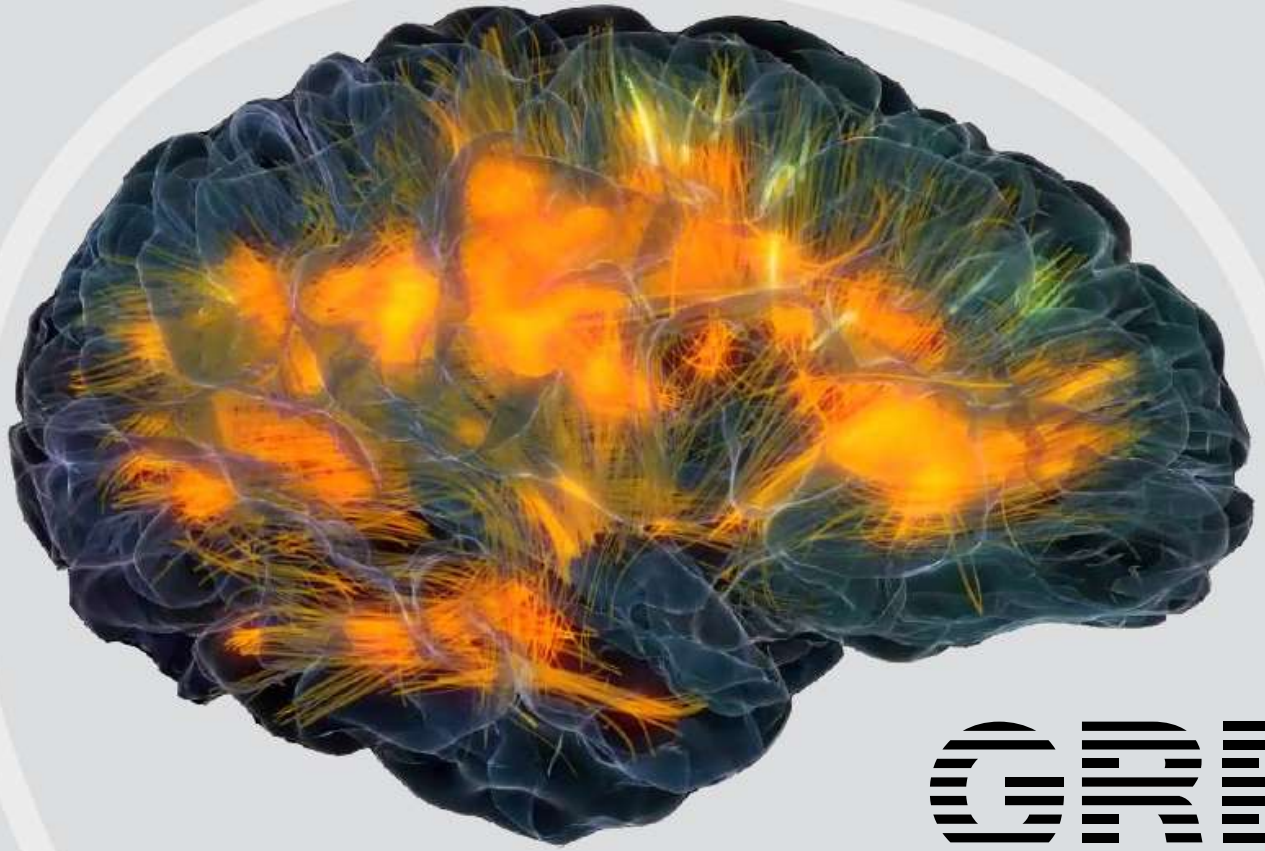


GREYCORTEX

ADVANCED, UNKNOWN MALWARE IN THE HEART OF EUROPE

AGENDA

Network Traffic Analysis: What, Why, Results

Malware in the Heart of Europe

Bonus Round

GREYCORTEX

WHAT: NETWORK TRAFFIC ANALYSIS

Gartner

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

= Mirrored network traffic via TAP/SPAN

≠ NetFlow analysis, full-packet capture

GREYCORTEX

WHY NTA

Unknown malware
Insider threats
Forensic investigation
Network visibility
IoT and BYOD devices

Rapid Detection & Response

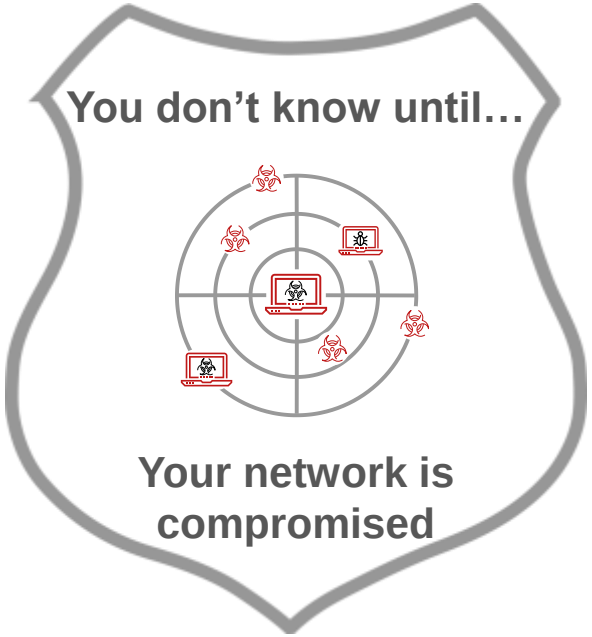
Effective

Because Threats Create Detectable Traffic

GREYCORTEX

NTA RESULTS

Detect Threats



Visualize the Full Network

GREYCORTEX

GREYCORTEX MENDEL

Uses

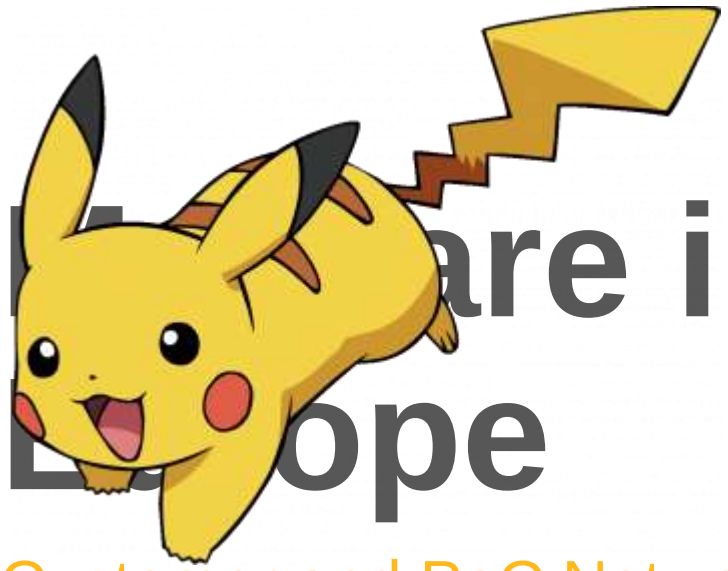
ARTIFICAL INTELLIGENCE MACHINE LEARNING
BIG DATA ANALYSIS

To Help

GOVERNMENTS + CRITICAL INFRASTRUCTURE+ ENTERPRISE

MAKE IT OPERATIONS SECURE AND RELIABLE

GREYCORTEX



[illegible]are in the Heart of [illegible]ope

Customer and PoC Network Examples

GREYCORTEX

CASE 1 – 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

GREYCORTEX

CASE 1 – 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)

GREYCORTEX

	Src Host	Src MACs	Dst Host	Dst Port	Service	Count	Length	Length	Count	
+	10.9.168.38	1	109.236.82.99	1123		149	81.6 k	73.3 k	133	
−	**10.9.168.38**	**1**	**217.23.13.94**	**1123**		**10**	**618**	**35**	**13**	

Source

R (10.9.168.38)

Wifi (10.8.0.0/15)

c4:85:08:4b:ab:9a

1 Ports TCP 1123

Show source ports

Destination

up21.gyasoun.ru (217.23.13.94)

WorldStream B.V.

00:00:5e:00:01:32

Flow | Link layer | Network layer | Transport layer | Application Layer

Protocol: TCP

	Source	Destination
Flags:	ACK(30) PSH(23) SYN(1)	ACK(46) PSH(22) SYN(1)
Port:	49330	1123

	Average	Minimum	Maximum
UET (User experience time):	2.28 s ±2.83 s	0.045 s	7.60 s
RTT (Round trip time):	0.164 s ±0.098 s	0.026 s	0.276 s
ART (Server application response time):	115.66 s ±11.28 s	74.00 s	119.88 s

+	10.9.168.38	1	217.23.14.93	1123		285	267.1 k	251.5 k	202	
+	10.9.168.38	1	217.23.10.118	1123		6	366	25	9	
+	10.9.168.38	1	93.190.140.73	1123		7	432	25	10	

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

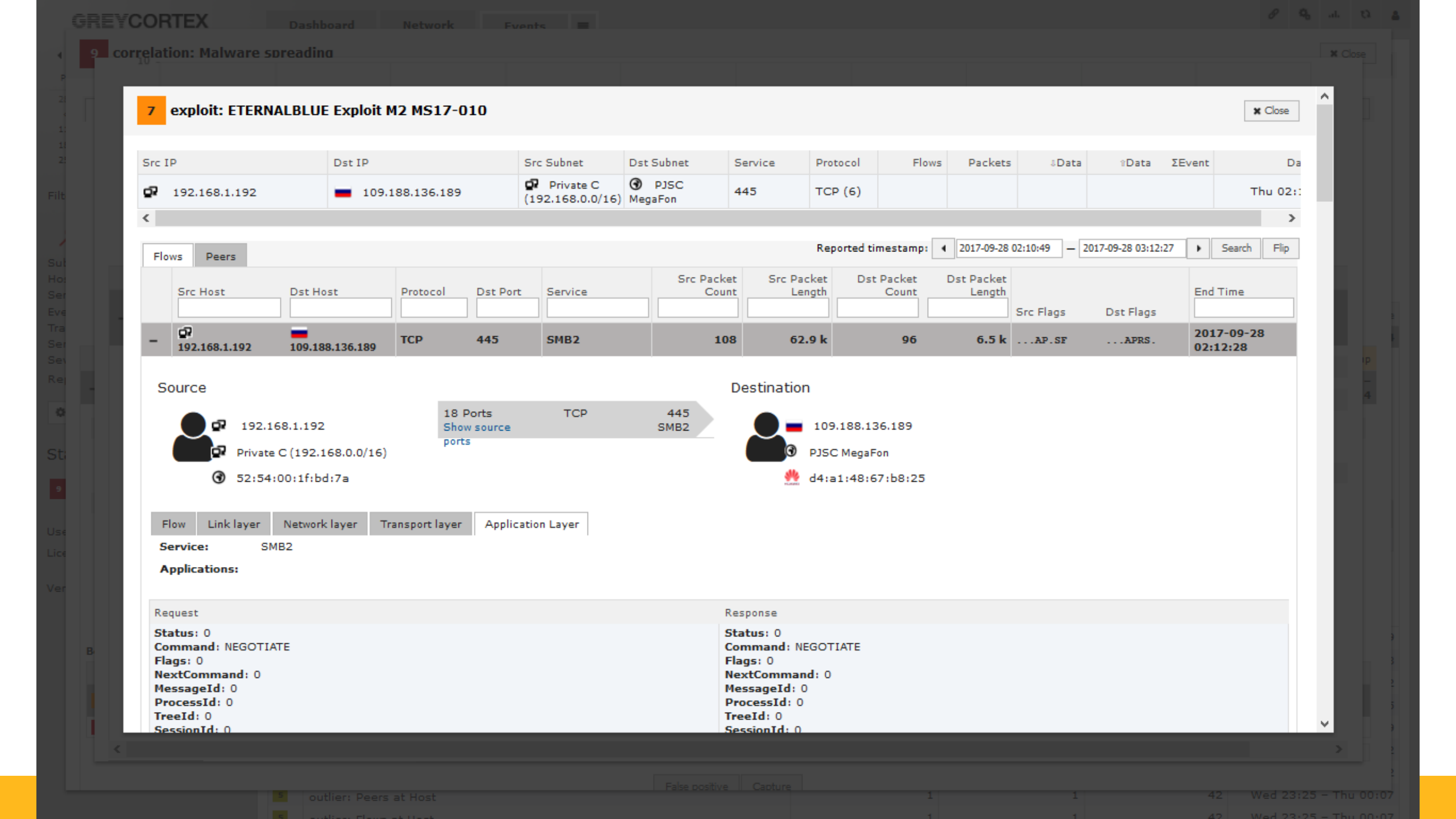
Tried to use CVE-2017-0143 (exploit MS17-010) on the connected host

GREYCORTEX

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 **A day after** updated IDS rule matched: Eternal Blue (based on CVE-2017-0143, exploit MS17-010)

GREYCORTEX


GREYCORTEX
Dashboard
Network
Events
correlation: Malware spreading
Close
7 exploit: ETERNALBLUE Exploit M2 MS17-010
Close
Src IP
Dst IP
Src Subnet
Dst Subnet
Service
Protocol
Flows
Packets
Data
Data
Event
192.168.1.192
109.188.136.189
Private C (192.168.0.0/16)
PJSC MegaFon
445
TCP (6)
Thu 02:
Flows
Peers
Reported timestamp:
2017-09-28 02:10:49
2017-09-28 03:12:27
Search
Flip
Src Host
Dst Host
Protocol
Dst Port
Service
Src Packet Count
Src Packet Length
Dst Packet Count
Dst Packet Length
Src Flags
Dst Flags
End Time
192.168.1.192
109.188.136.189
TCP
445
SMB2
108
62.9 k
96
6.5 k
...AP.SF
...APRS.
2017-09-28 02:12:28
Source
192.168.1.192
Private C (192.168.0.0/16)
52:54:00:1f:bd:7a
18 Ports
Show source ports
TCP
445
SMB2
Destination
109.188.136.189
PJSC MegaFon
d4:a1:48:67:b8:25
Flow
Link layer
Network layer
Transport layer
Application Layer
Service: SMB2
Applications:
Request
Status: 0
Command: NEGOTIATE
Flags: 0
NextCommand: 0
MessageId: 0
ProcessId: 0
TreeId: 0
SessionId: 0
Response
Status: 0
Command: NEGOTIATE
Flags: 0
NextCommand: 0
MessageId: 0
ProcessId: 0
TreeId: 0
SessionId: 0
False positive
Capture
outlier: Peers at Host
Wed 23:25 – Thu 00:07

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

GREYCORTEX

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)

GREYCORTEX

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:

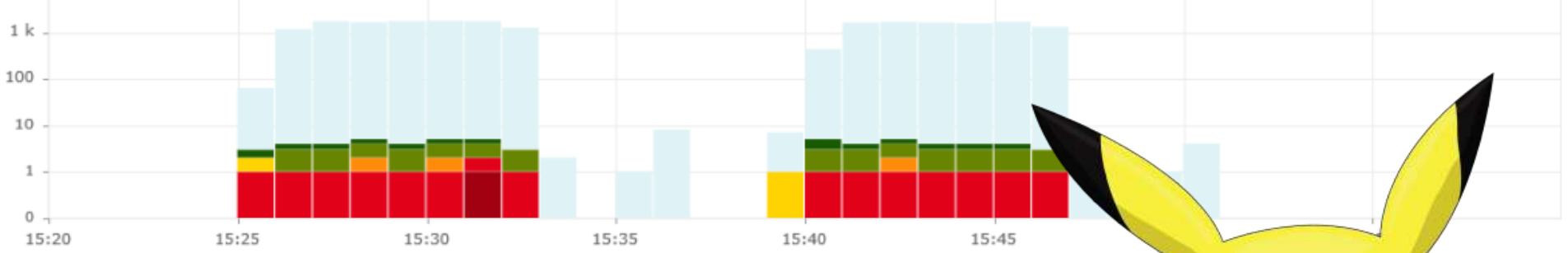
Subnet:
Host: 192.168.1.112 | 192.168.
Service:
Event:
Traffic:
Sensor: Mercy
Severity:
Reps:

Clear Filter

Status Monitor

9 Mercy

User: administrator (Administrat
License: Tomas Chomo (tomas.chomo@greycortex
Version: 2.8.0



	Name	Src Hosts	Dst Hosts	Date
9	correlation: Malware spreading	1	1	Fri 15:25 – 15:29
8	Scan: SMB Port Sweep (445)	2	1	ri 15:25 – 15:46
7	policy: Request to an external DNS server	1	1	ri 15:29 – 15:30
7	blacklist: Spamhaus DROP blacklist	2	2	Fri 15:27 – 15:42
6	exploit: ETERNALBLUE Exploit M2 MS17-010	1	1	Fri 15:24 – 15:39
4	outlier: Peers at Subnet	2	1	15:25 – 15:46
4	outlier: Flows at Subnet	2	1	5:25 – 15:46
3	**scan: Behavioral Unusual Port 445 traffic Potential Scan or Infection**	**2**	**14**	**:24 – 15:45**

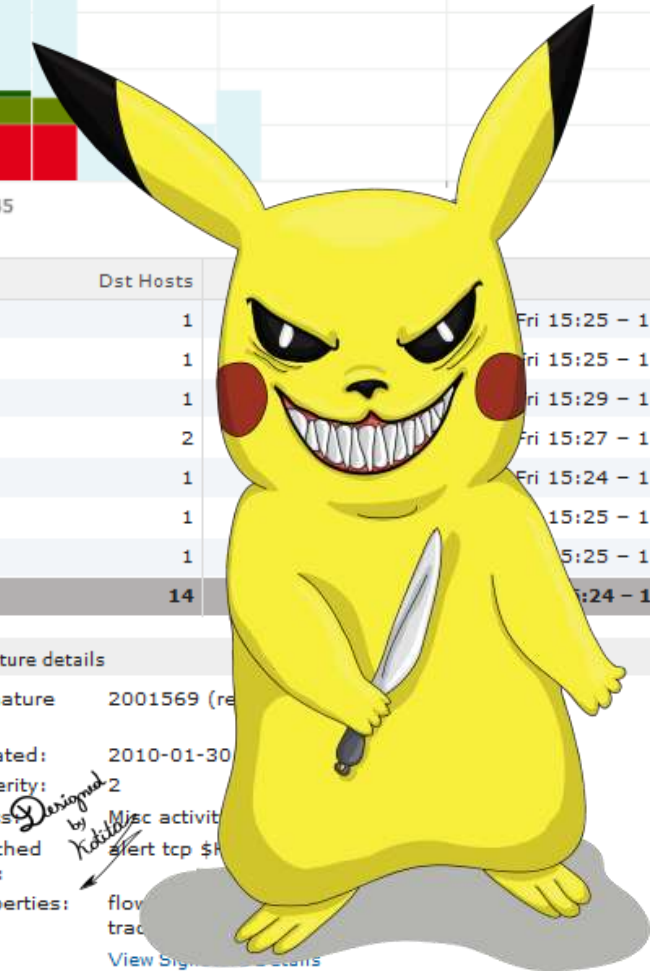
Description

References

- http://doc.emergingthreats.net/2001569

Signature details

Signature ID: 2001569 (re
Created: 2010-01-30
Severity: 2
Class: Misc activit
Matched rule: alert tcp $h
Properties: flow
trac
View Sig Details



Top Src Hosts	Top Dst Hosts	Top Src Subnets	Top Dst Subnets	Top Services
192.168.1.112	37.22.9.175	Private C (192.168.0.0/16)	AT&T Services, Inc.	445
192.168.1.135	45.83.82.196		California State University, Office of the Chancellor	
	80.69.46.62		china tietong Shandong net	
	122.81.58.207		Elisa Oyj	
	130.191.116.135		LG POWERCOMM	
	138.209.205.200		MCI	
	140.212.229.172		net-lab GmbH	

10

CASE 4 – SSH ATTACK

Identified at a Perimeter Router:

Consecutive IP addresses in the public range were tried in an effort to open a session on port 22/tcp; by a host in Canada

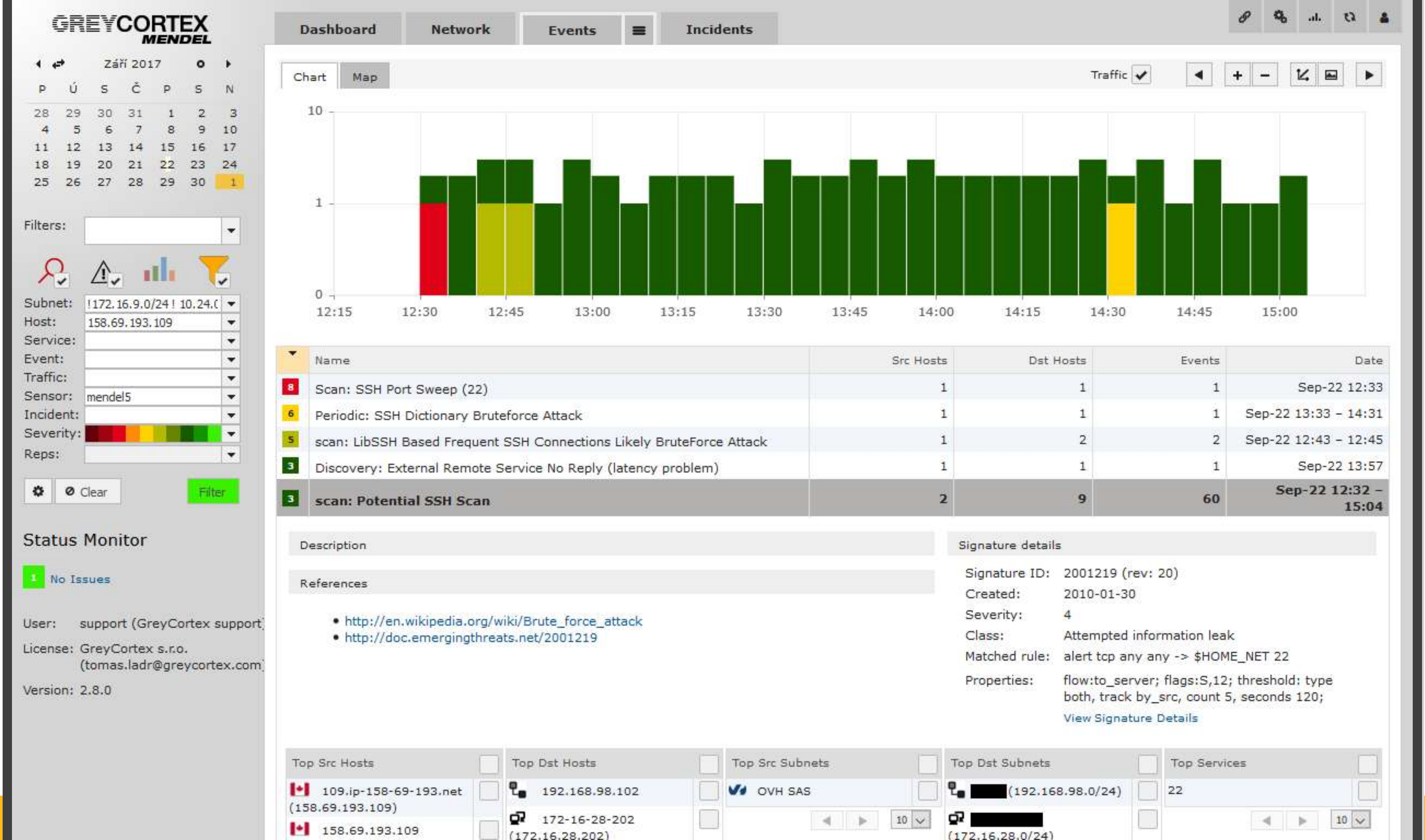
Subsequently, a high number of connections via port 22/tcp to some hosts in the range were detected

GREYCORTEX

CASE 4 – SSH ATTACK

Unsupervised Learning	*Machine Behavior*	***Flow-based Detection***	*Discovery Analysis*	*Other*
		SSH port sweep (22/tcp) Brute force SSH attack (22/tcp)		

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: !172.16.9.0/24 ! 10.24.(
Host: 158.69.193.109
Service:
Event:
Traffic:
Sensor: mendel5
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
10
1
0
12:15 12:30 12:45 13:00 13:15 13:30 13:45 14:00 14:15 14:30 14:45 15:00
Name | Src Hosts | Dst Hosts | Events | Date
8 Scan: SSH Port Sweep (22) | 1 | 1 | 1 | Sep-22 12:33
6 Periodic: SSH Dictionary Bruteforce Attack | 1 | 1 | 1 | Sep-22 13:33 – 14:31
5 scan: LibSSH Based Frequent SSH Connections Likely BruteForce Attack | 1 | 2 | 2 | Sep-22 12:43 – 12:45
3 Discovery: External Remote Service No Reply (latency problem) | 1 | 1 | 1 | Sep-22 13:57
3 scan: Potential SSH Scan | 2 | 9 | 60 | Sep-22 12:32 – 15:04
Description
References
• http://en.wikipedia.org/wiki/Brute_force_attack
• http://doc.emergingthreats.net/2001219
Signature details
Signature ID: 2001219 (rev: 20)
Created: 2010-01-30
Severity: 4
Class: Attempted information leak
Matched rule: alert tcp any any -> $HOME_NET 22
Properties: flow:to_server; flags:S,12; threshold: type both, track by_src, count 5, seconds 120;
View Signature Details
Top Src Hosts
109.ip-158-69-193.net (158.69.193.109)
158.69.193.109
Top Dst Hosts
192.168.98.102
172-16-28-202 (172.16.28.202)
Top Src Subnets
OVH SAS
Top Dst Subnets
[redacted](192.168.98.0/24)
[redacted]
(172.16.28.0/24)
Top Services
22

CASE 5 – UNKNOWN (YET) BOTNET

A Device on an Internal Network:

Periodically attempts to communicate with blacklisted IP addresses at port 30303

GREYCORTEX

CASE 5 – UNKNOWN (YET) BOTNET

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

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

	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**

Description

A horizontal network scan was detected. The source host scanned multiple other hosts for services, which you can find in the event. This could be a manifestation of malware or an attempt to attack the system. This anomaly has been detected on the basis of communication coming from the listed host addresses to multiple addresses on the same service.

Signature details

Signature ID: 2200
Created: 2014-11-24 (Modified: 2017-04-04)
Class: Network scan

CASE 6 – DOCUMENT LEAKAGE

A Device on an Internal Network:

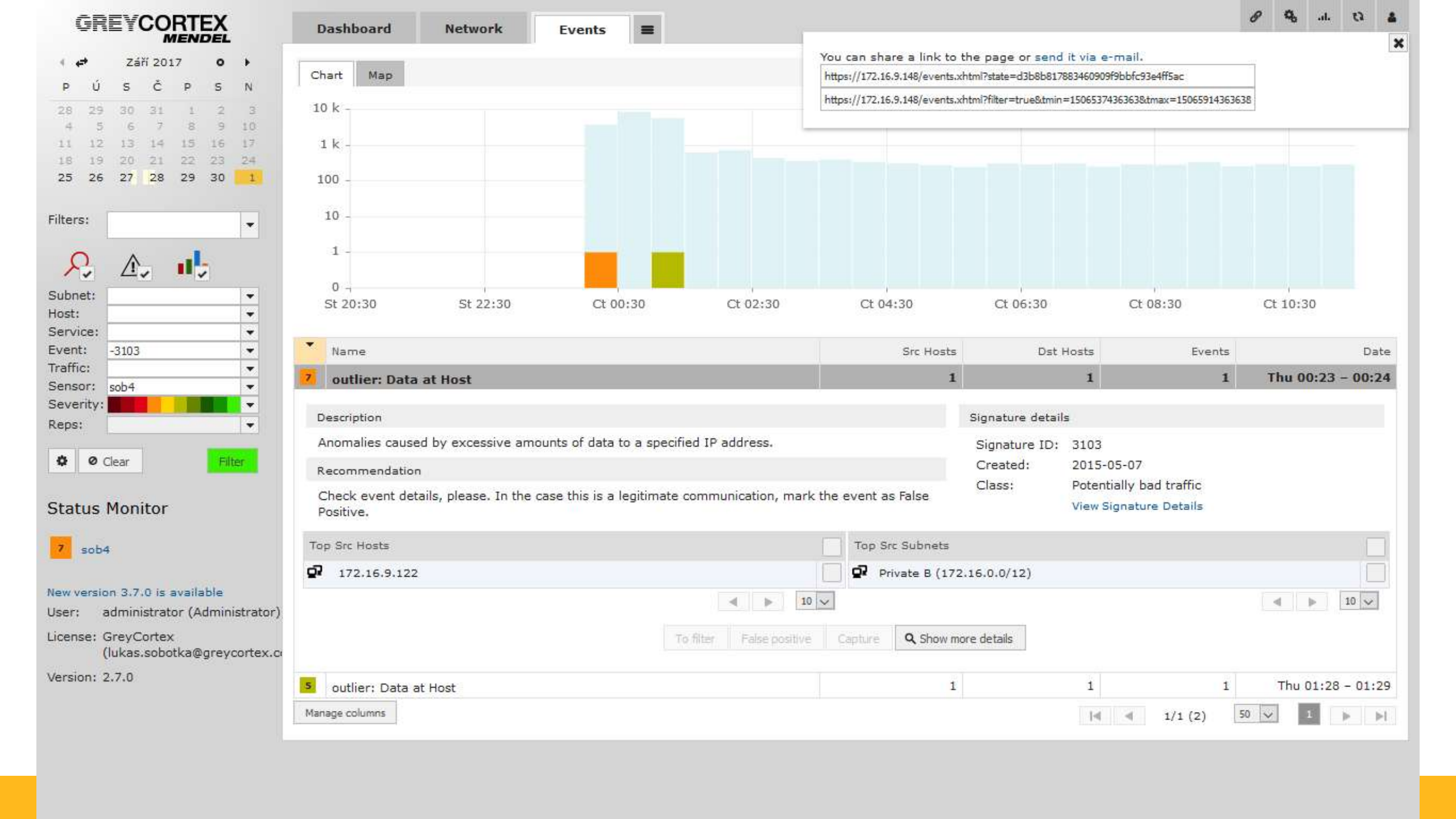
Exhibited an unusually high data transfer volume to an external network

GREYCORTEX

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

GREYCORTEX


GREYCORTEX MENDEL
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:
Event: -3103
Traffic:
Sensor: sob4
Severity:
Reps:
Clear
Filter
Status Monitor
7 sob4
New version 3.7.0 is available
User: administrator (Administrator)
License: GreyCortex
(lukas.sobotka@greycortex.c
Version: 2.7.0
Dashboard
Network
Events
You can share a link to the page or send it via e-mail.
https://172.16.9.148/events.xhtml?state=d3b8b817883460909f9bbfc93e4ff5ac
https://172.16.9.148/events.xhtml?filter=true&tmin=1506537436363&tmax=15065914363638
Chart
Map
10 k
1 k
100
10
1
0
St 20:30
St 22:30
Ct 00:30
Ct 02:30
Ct 04:30
Ct 06:30
Ct 08:30
Ct 10:30
Name
Src Hosts
Dst Hosts
Events
Date
7 outlier: Data at Host 1 1 1 Thu 00:23 – 00:24
Description
Anomalies caused by excessive amounts of data to a specified IP address.
Recommendation
Check event details, please. In the case this is a legitimate communication, mark the event as False Positive.
Signature details
Signature ID: 3103
Created: 2015-05-07
Class: Potentially bad traffic
View Signature Details
Top Src Hosts
172.16.9.122
Top Src Subnets
Private B (172.16.0.0/12)
10
10
To filter
False positive
Capture
Show more details
5 outlier: Data at Host 1 1 1 Thu 01:28 – 01:29
Manage columns
1/1 (2)
50
1

CASE 7 – ALL TOGETHER

Cases 1-6 Combined

GREYCORTEX

CASE 7 – ALL TOGETHER

Unsupervised Learning	*Machine Behavior*	*Flow-based Rules*	*Discovery Analysis*	*Other*
Outliers: data, flows, packets, peers, hosts, ports, performance Bayesian Expectation Maximization Gaussian Mixture Models	Repetitive periodic connections or checks	Port scan Port sweep Brute-force Dictionary attacks Data enumeration DoS, DDoS	Detection of new or lost/unreachable: services, devices (IP, MAC, hostname), gateways, VLANs, subnets Detection of changed/duplicated hostname/IP/MAC, changed VLAN, …	Event correlation L7 content analysis (DPI) Tunneled and encrypted data inspection IDS in the internal network, all rules active (45k+)

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:
Service:
Event:
Traffic:
Severity:
Reps:

Clear | Filter

Status Monitor

7 Mercy

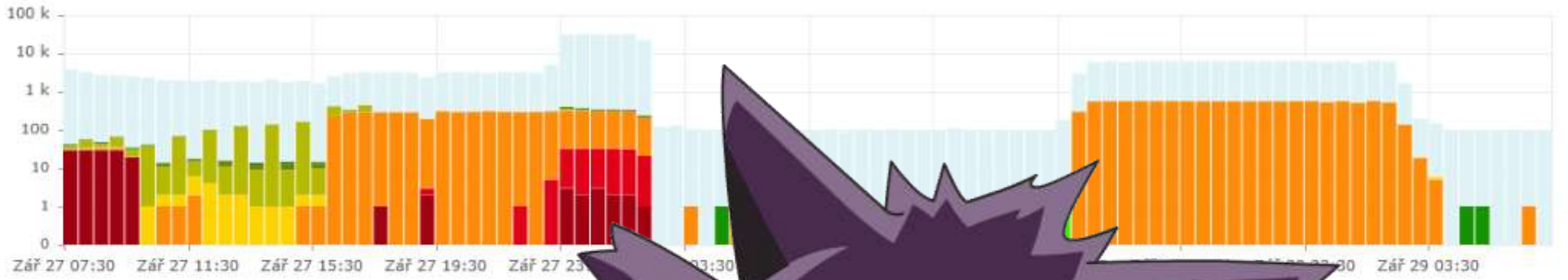
User: administrator (Administrat

License: Tomas Chomo (tomas.chomo@greycortex

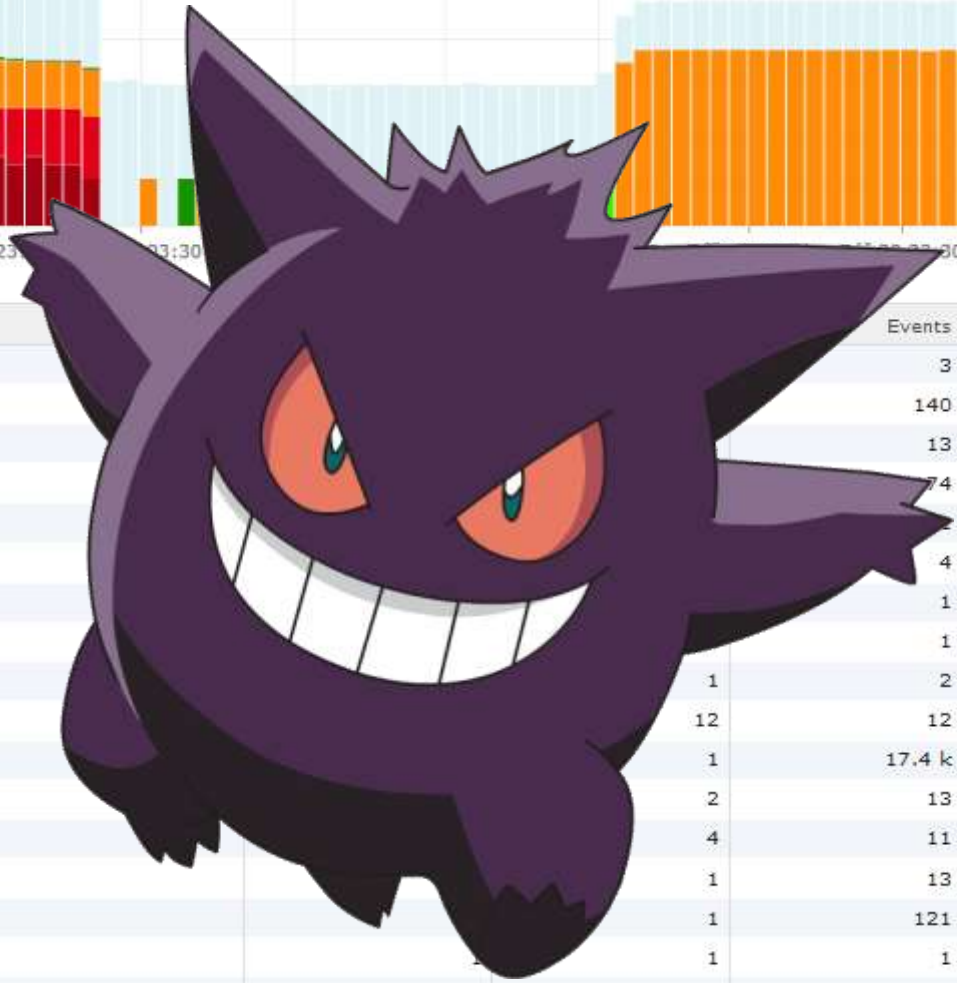
Version: 2.8.0

Chart | Map

Traffic



	Name			Events	Date
9	status monitor: Long time CPU performance issues			3	Wed 17:58 – 19:21
9	status monitor: Span/Tap port outage			140	Wed 07:30 – 09:49
9	correlation: Malware spreading			13	Wed 23:26 – Thu 02:14
8	Scan: SMB Port Sweep (445)			74	Wed 23:26 – Thu 02:19
8	policy: Request to an external DNS server				Wed 19:27 – 19:28
8	correlation: TOR communication			4	Wed 22:21 – Thu 01:22
7	outlier: Application Performance at Service			1	Wed 19:28 – 19:29
7	outlier: Data at Host			1	Wed 16:02 – 16:03
7	Discovery: New Gateway		1	2	Wed 09:14 – 17:59
7	exploit: ETERNALBLUE Exploit M2 MS17-010		12	12	Wed 23:37 – Thu 03:55
7	trojan: Possible Gozi ISFB/Dreambot DGA Domain in SNI		1	17.4 k	Wed 16:06 – Fri 03:18
7	policy: Request to an external DNS server		2	13	Wed 10:55 – Thu 22:12
7	blacklist: Spamhaus DROP blacklist		4	11	Wed 08:13 – Thu 01:59
7	status monitor: Update failed		1	13	Wed 08:53 – Fri 06:47
7	status monitor: Span/Tap port disruption		1	121	Wed 19:21 – Fri 03:36
7	status monitor: System service disruption		1	1	Wed 19:22
7	correlation: Malware installation	2	1	4	Thu 16:12 – 16:59
6	Periodic: Outgoing Web Communication (i.e. remote access trojan)	1	1	1	Fri 00:04 – 02:45
6	Scan: Port Sweep-like Behavior (horizontal port scan)	1	1	1	Wed 12:05 – 12:08
6	Discovery: Forbidden local service (forbidden by policies)	1	3	21	Wed 07:00 – Thu 10:00
6	policy: TLS possible TOR SSL traffic	1	3	6	Wed 19:30 – Thu 01:22
6	blacklist: Tor blacklist	3	17	59	Wed 11:45 – Fri 02:22



“BONUS” – CAUTIONARY TALES

Ministry “Outer System“ E-mail Server Provided Mailbox Access:

- To IP addresses of Tor endpoints and to server hosting PhpBB forum “СуперМамочки Нижнекам
  (static.7.236.46.78.clients.your-server.de, Hetzner Online GmbH)
- 170 accounts/users compromised, unnoticed almost a year
- More than 7100 documents stolen.
- The attacker “basically maintained undisturbed access to any of the email accounts”
- “Strategic advantage” gained?

Vulnerable Network at Political Organization:

- Multiple intrusions by different organizations (2015, 2016)
- Unnoticed almost a year
- Internal strategy documents, emails, and possible donor lists stolen

Spear-Phishing Attack on Campaign Manager:

- Fake security alert/log-in page
- Identified as “legitimate” by security team (or not)
- Secret to creamy risotto

GREYCORTEX

“BONUS” CASE – FINDINGS, VERDICT

Findings

- Weak or leaked account password (“admin5”) using single factor authentication for strong accounts.
- Using private accounts for work, prone to social engineering, etc.
- No proper evaluation of operations data in place, no insight

Verdict

- Always watch what happens in your network, use the right tools!
- Do not trust administrators, they have too much power!
- And …

GOTTA CATCH ‘EM ALL.

GREYCORTEX

PALDIES PAR JŪSU UZMANĪBU!

GreyCortex s.r.o.
Purkyňova 127
612 00 Brno

www.greycortex.com
twitter.com/greycortex
linkedin.com/company/greycortex

Vladimír Sedláček
info@greycortex.com
+420 511 205 388

GREYCORTEX