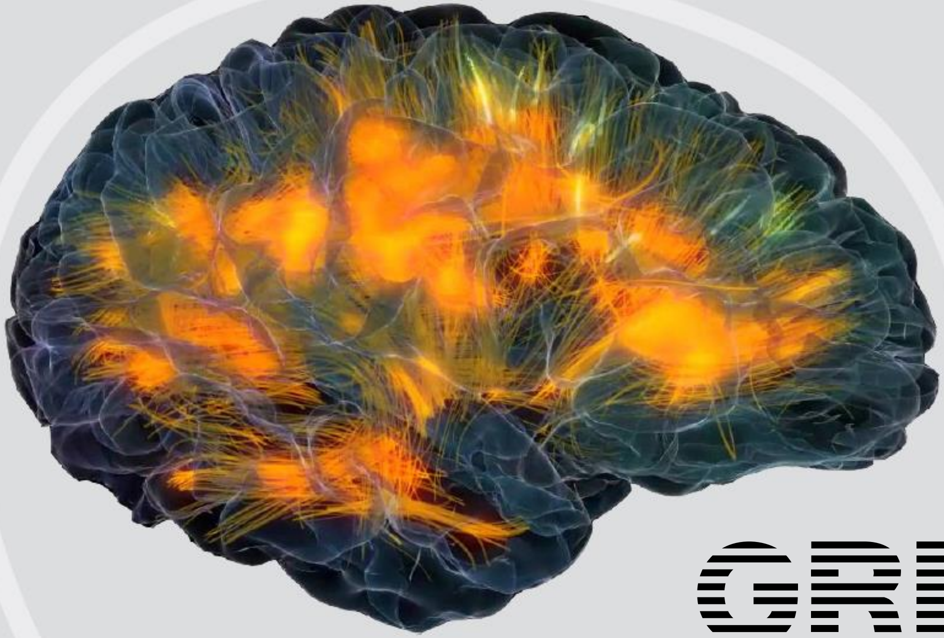


GREYCORTEX

GREYCORTEX MENDEL

NETWORK TRAFFIC ANALYSIS SOLUTION FOR IOT

MY SOLUTION IS PERFECTLY SECURE!

?

IOT IS A NETWORK LIKE ANY OTHER

The category is called "Internet of Things"

- Designed to be inter-**connected**
  - Network goes far beyond the local area
- To enable more
  - Industry 4.0, smart cities, smart homes, wearable health, augmented humans, …

Facts to consider about connected endpoints

- Life cycle beyond "project"
  - Long into the future… or "Do you expect me to replace a light switch every two to five years?"
- Power consumption
  - We want to operate 10+ years on an original battery
- Computing power
  - Strong limits for price and power consumption imposed
  - Cryptosecurity is built on power differences!

IOT IS A NETWORK LIKE ANY OTHER

Facts to consider about connected endpoints (cont‘d)

- Storage capacity
  - Strong limits for price and power consumption imposed
  - Who pays for unused amounts of memory?
- Field upgradability of SW
  - Limits for protocol reliability may prohibit big blobs
  - ROM is cheaper
  - Power is limited
- Production volumes
  - Imagine 100K+ devices produced but a serious vulnerability found at the same time
- M2M
  - Who would ever notice the “feeling“ that something “strange“ is going on?
- The battle is completely automated!
  - There is no human attacker behind remote attacking host

GREYCORTEX

IOT IS A NETWORK LIKE ANY OTHER

Honestly, is there reliable, effective security built within IoT?

GREYCORTEX

ALL NETWORKS ARE VULNERABLE!

- Tearing down natural security frontiers
  - Where there is a connection, there is a strong possibility
- The OSI model is actually the vulnerability stack standard
  - Flaw in lower layer opens a hole to upper layers
- The protocol (media conversion) gateway is no security solution
  - Repacking data does not eliminate the information and the connectivity path
- Security gateway (or protocol) is not security (without upgrades)
  - Still leaving your endpoints untouched?
- Secure computing fundaments decay faster than imagination!
  - Where is RSA56? MD5? TLS1.1?
- Is closed source software more secure than open source?
  - They are equally insecure, but OSS can be investigated and patched more easily.

PROVE IT PLEASE!

Recent Exploitable Flaw in IEEE 802.11: **KRACK (CVE-2017-13082)**

Existing since 2008, introduced into 802.11r by support for fast BSS Transition (envisioning SIP IP roaming)

From Wikipedia, the free encyclopedia [2017-11-05, https://en.wikipedia.org/wiki/KRACK]:

“KRACK (Key Reinstallation AttaCK) is a severe replay attack (a type of exploitable flaw) on the Wi-Fi Protected Access protocol that secures Wi-Fi connections. … discovered in 2016 by the Belgian researchers … published details of the attack in October 2017. By repeatedly resetting the ***nonce*** *transmitted in the* ***third step of the WPA2*** *handshake, an attacker can gradually match encrypted packets seen before and learn the full keychain used to encrypt the traffic.”*

The **weakness is in** the Wi-Fi **standard itself**, … any **correct implementation** of WPA2 is likely **to be vulnerable** … **all major software platforms** …

The widely used **open-source** … wpa_supplicant, … Linux and Android, is especially susceptible as it can be manipulated to install an all-zeros encryption key, effectively nullifying WPA2 protection in a man-in-the-middle attack.

BREACH CONSEQUENCES

Possible benefits for the attacker:

- Fun
- Knowledge
- Power
- Money
- Glory

Possible consequences for the victim:

- Loss in property, reputation, life
- Disruption in suply of goods, services, and commodities
- Possibly even riot and war … or?

SCADA THREATS IN POWER GRIDS

UKRAINE 2015 ….
BLACKENERGY

Exploit in .ppsx

This ICS tailored malware contained exploits for specific types of HMI applications including Siemens SIMATIC, GE CIMPLICITY, and Advantech WebAccess.

Hacking Tools, Remote Access, Kill Disk

Blackout …

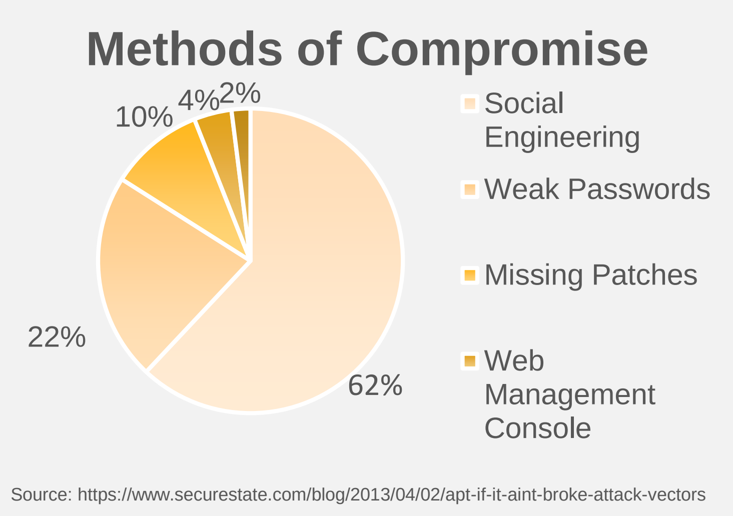
GREYCORTEX

ADVANCED PERSISTENT THREATS

Advanced - Sophisticated evasion techniques using malware and known vulnerabilities to exploit internal systems

Persistent - External command and control system continuously monitors and extracts data from a specific target

Threat - Organized behavior to steal sensitive data from the organization



Source: https://www.securestate.com/blog/2013/04/02/apt-if-it-aint-broke-attack-vectors

8 – 16 hours
Time an adversary needs to break into a network

49 days
Average time to detect an APT attack

8 months
Average time an advanced threat goes unnoticed on a victim's network

71%
Percentage of compromised organizations who did not detect a breach themselves

Your figures may vary, but the amount of threat attempts will only increase

GREYCORTEX

WHAT CAN I DO?

- Design carefully and for the long term
- Hunt for flaws
- Account for failure
- Act on newly disclosed issues
- Monitor deeply and continuously

GREYCORTEX

“Do. Or do not. There is no try.”

Master Yoda – image in [2017-09-18 19:47] http://www.starwars.com/news/15-star-wars-quotes-to-use-in-everyday-life

GREYCORTEX

INTRODUCING

What GREYCORTEX MENDEL can do for IoT?

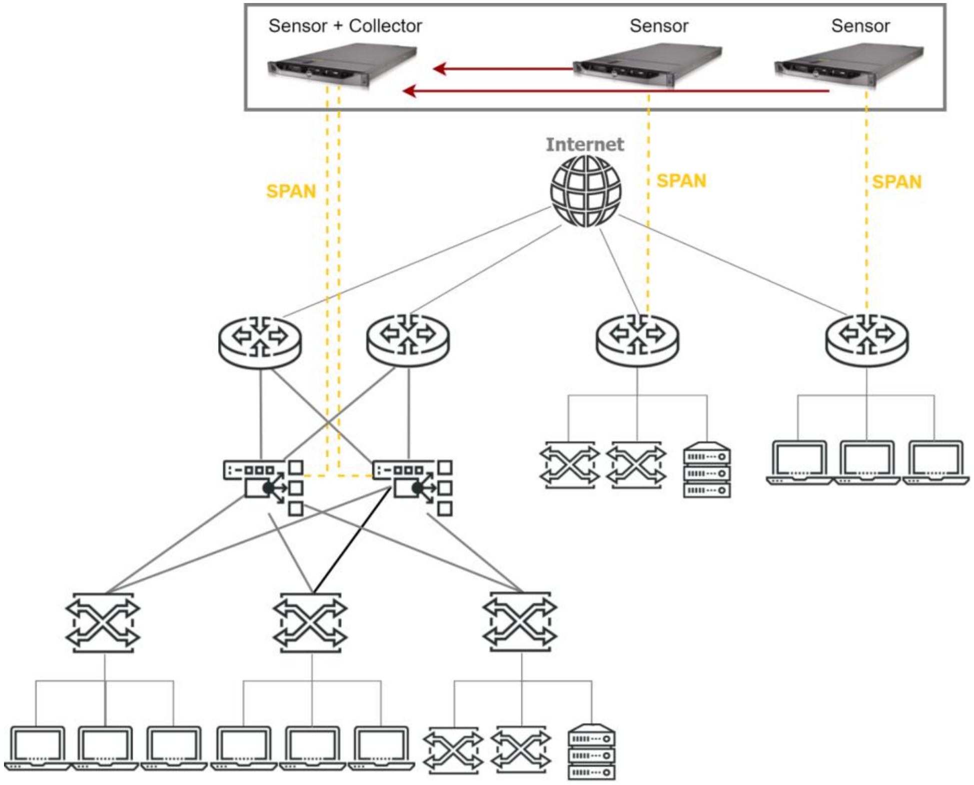
- No, we won’t fix your design or code flaws
- No, we won’t pentest your devices
- No, we won’t go out to upgrade installed devices

MENDEL monitors, detects, and informs you that something malicious is happening (or has happened) in your (IoT) network! *)

*) Depending on the threat, solution architecture, and situation.

Ask for a PoC!

MENDEL INTEGRATION



Sensors

- ASNM output (= 0,5% - 1% of traffic)
- 100Mbps – 10Gbps

Collectors

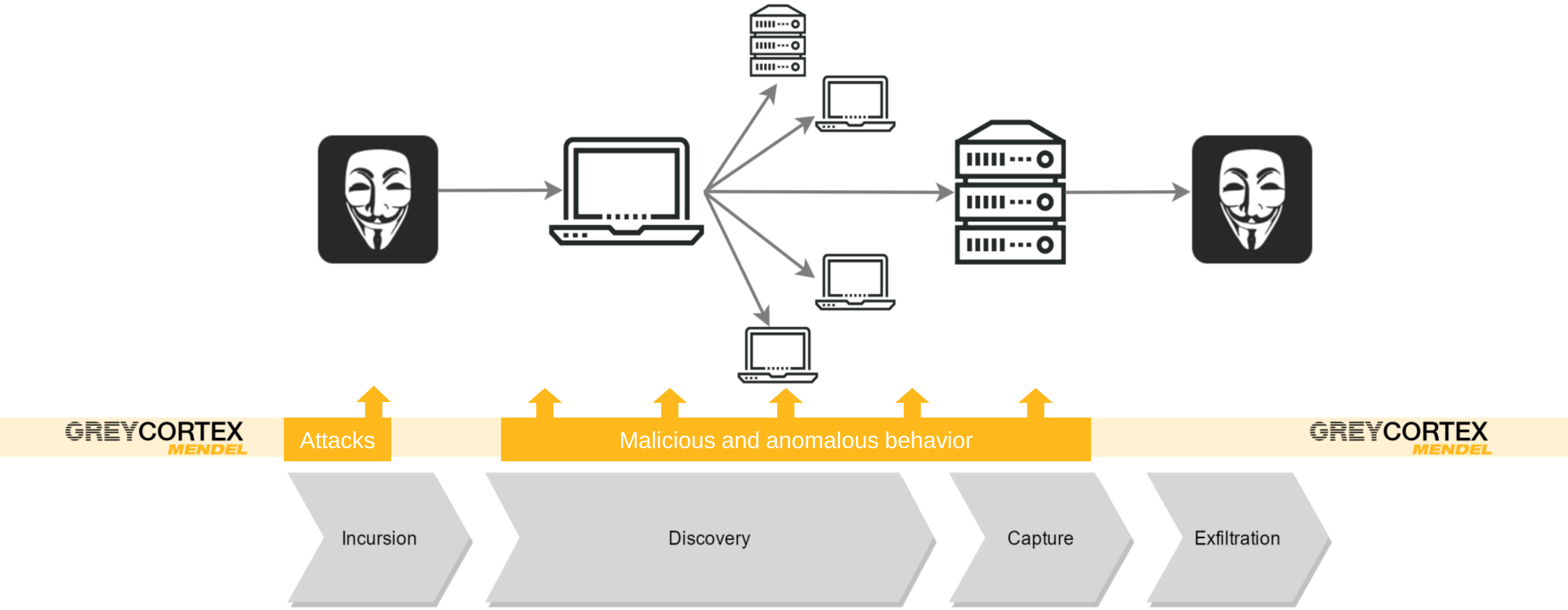
- 1 collector = 10+ sensors
- ASNM as input
- Aggregated input 40Gbps+

Appliances

- Passive
- On premise
- HW or virtual deployment

GREYCORTEX

EFFECTIVE THREAT DETECTION



Attacks

Malicious and anomalous behavior

Incursion

Discovery

Capture

Exfiltration

NETWORK VISIBILITY

Transport decryption *)

HTTPS, FTPS, … ***S

Full data inspection

Conditional data recording

PCAP files

Data decapsulation

IP-IP, IPv4-IPv6, IPv6-IPv4, MPLS, Teredo, GRE

L7 application protocol parsers

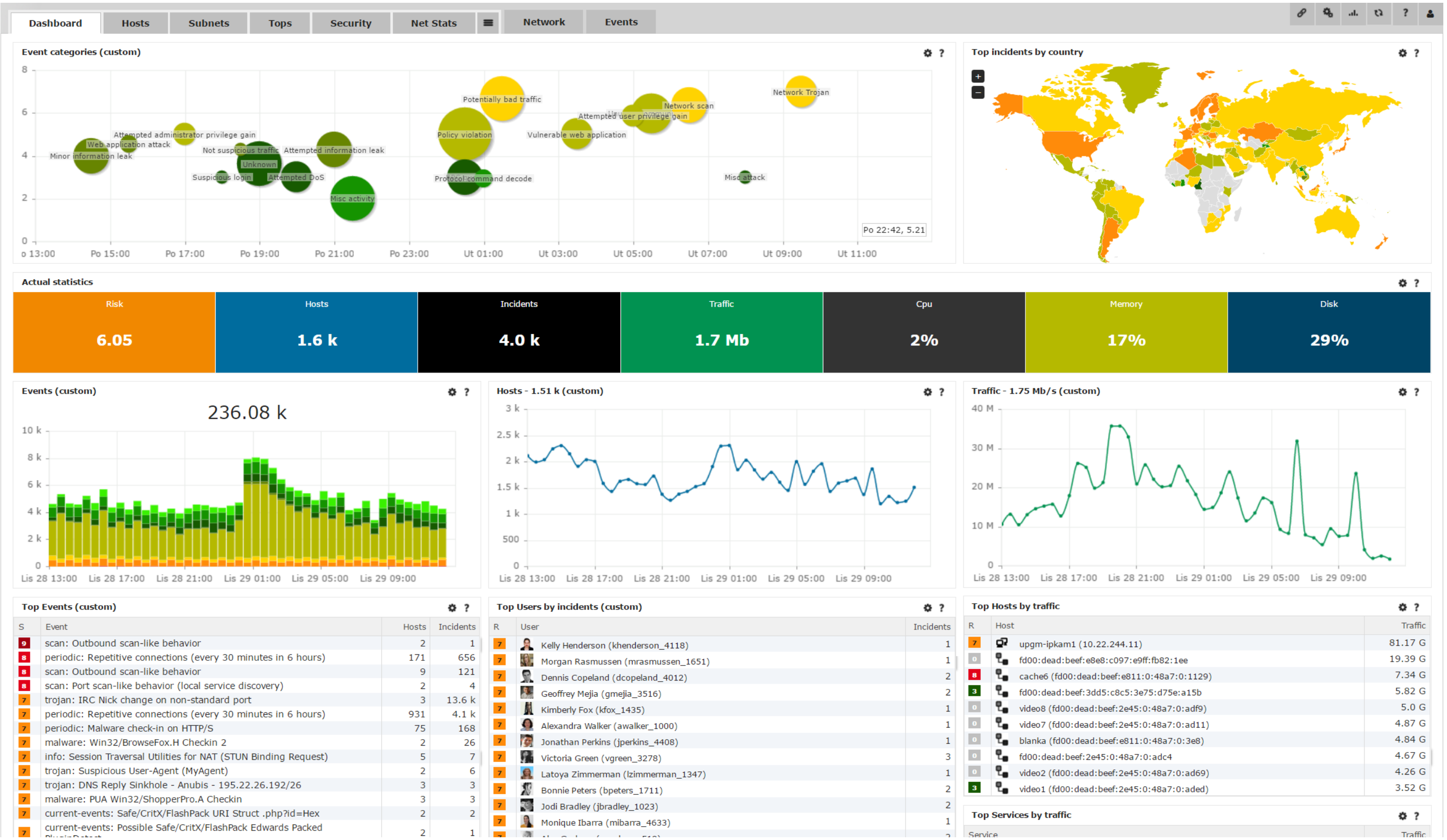
DNS, HTTP, HTTPS, TLS, MODBUS, SMB, SSH, SSL, SMTP,

FTP, DCERPC, IRC, VNC, POP3, Oscar, SIP, MS-SQL, DHCP, …

*) Where feasible or supported

QUICK OVERVIEW

Quick access through user-configured dashboards.



Actual statistics

Risk	Hosts	Incidents	Traffic	Cpu	Memory	Disk
6.05	1.6 k	4.0 k	1.7 Mb	2%	17%	29%

Top Events (custom)

S	Event	Hosts	Incidents
9	scan: Outbound scan-like behavior	2	1
8	periodic: Repetitive connections (every 30 minutes in 6 hours)	171	656
8	scan: Outbound scan-like behavior	9	121
8	scan: Port scan-like behavior (local service discovery)	2	4
7	trojan: IRC Nick change on non-standard port	3	13.6 k
7	periodic: Repetitive connections (every 30 minutes in 6 hours)	931	4.1 k
7	periodic: Malware check-in on HTTP/S	75	168
7	malware: Win32/BrowseFox.H Checkin 2	2	26
7	info: Session Traversal Utilities for NAT (STUN Binding Request)	5	7
7	trojan: Suspicious User-Agent (MyAgent)	2	6
7	trojan: DNS Reply Sinkhole - Anubis - 195.22.26.192/26	3	3
7	malware: PUA Win32/ShopperPro.A Checkin	3	3
7	current-events: Safe/CritX/FlashPack URI Struct .php?id=Hex	2	2
7	current-events: Possible Safe/CritX/FlashPack Edwards Packed	2	1

Top Users by incidents (custom)

R	User	Incidents
7	Kelly Henderson (khenderson_4118)	1
7	Morgan Rasmussen (mrasmussen_1651)	1
7	Dennis Copeland (dcopeland_4012)	2
7	Geoffrey Mejia (gmejia_3516)	2
7	Kimberly Fox (kfox_1435)	1
7	Alexandra Walker (awalker_1000)	1
7	Jonathan Perkins (jperkins_4408)	1
7	Victoria Green (vgreen_3278)	3
7	Latoya Zimmerman (lzimmerman_1347)	1
7	Bonnie Peters (bpeters_1711)	2
7	Jodi Bradley (jbradley_1023)	2
7	Monique Ibarra (mibarra_4633)	1

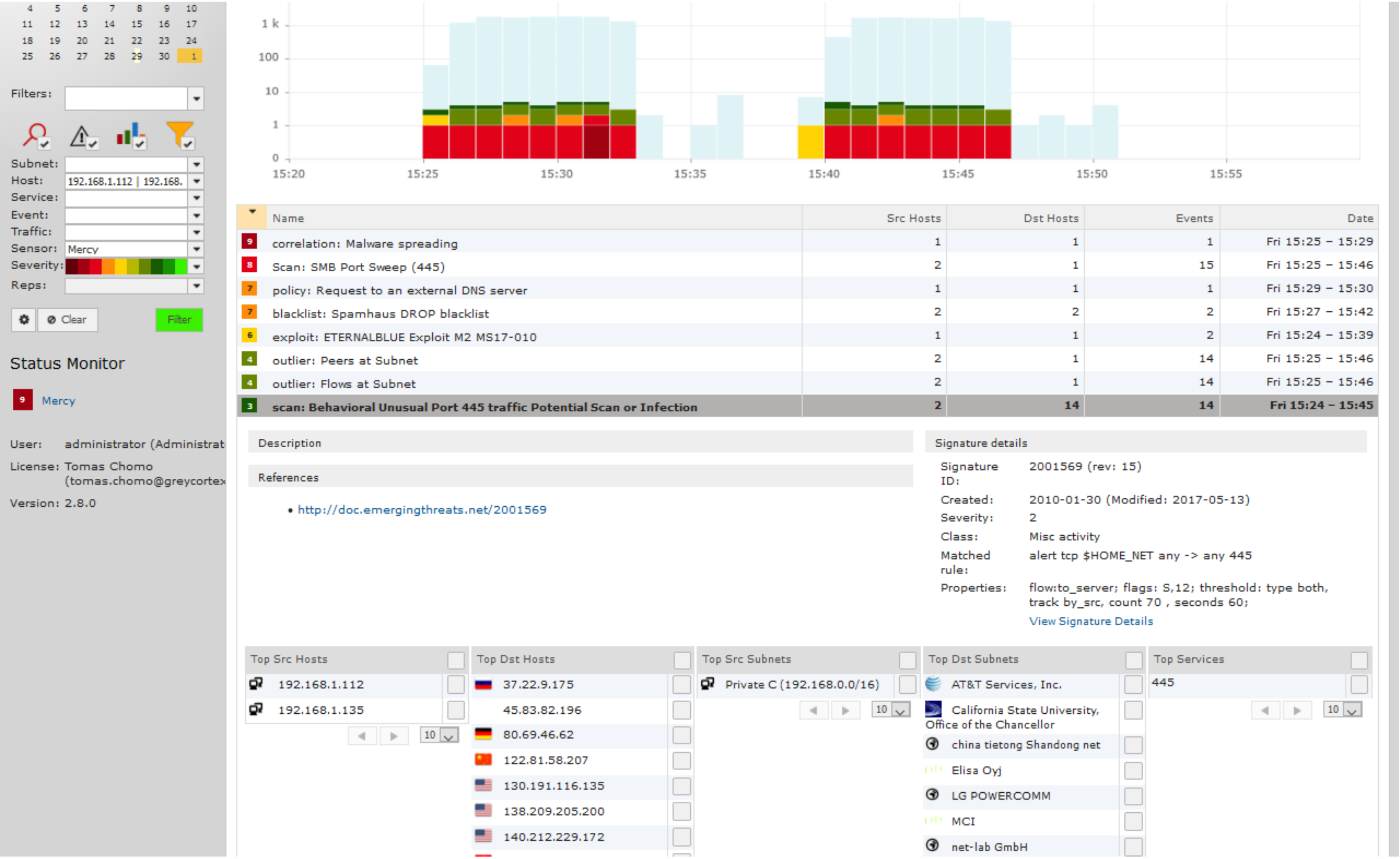
Top Hosts by traffic

R	Host	Traffic
7	upgm-ipkam1 (10.22.244.11)	81.17 G
0	fd00:dead:beef:e8e8:c097:e9ff:fb82:1ee	19.39 G
8	cache6 (fd00:dead:beef:e811:0:48a7:0:1129)	7.34 G
3	fd00:dead:beef:3dd5:c8c5:3e75:d75e:a15b	5.82 G
0	video8 (fd00:dead:beef:2e45:0:48a7:0:adf9)	5.0 G
0	video7 (fd00:dead:beef:2e45:0:48a7:0:ad11)	4.87 G
0	blanka (fd00:dead:beef:e811:0:48a7:0:3e8)	4.84 G
0	fd00:dead:beef:2e45:0:48a7:0:adc4	4.67 G
0	video2 (fd00:dead:beef:2e45:0:48a7:0:ad69)	4.26 G
3	video1 (fd00:dead:beef:2e45:0:48a7:0:aded)	3.52 G

Top Services by traffic

Service	Traffic

APT AT A GLANCE



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	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**

Description

References

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

Signature details

Signature ID:	2001569 (rev: 15)
Created:	2010-01-30 (Modified: 2017-05-13)
Severity:	2
Class:	Misc activity
Matched rule:	alert tcp $HOME_NET any -> any 445
Properties:	flow:to_server; flags: S,12; threshold: type both, track by_src, count 70 , seconds 60;

View Signature Details

Top Src Hosts
192.168.1.112
192.168.1.135

Top Dst Hosts
37.22.9.175
45.83.82.196
80.69.46.62
122.81.58.207
130.191.116.135
138.209.205.200
140.212.229.172

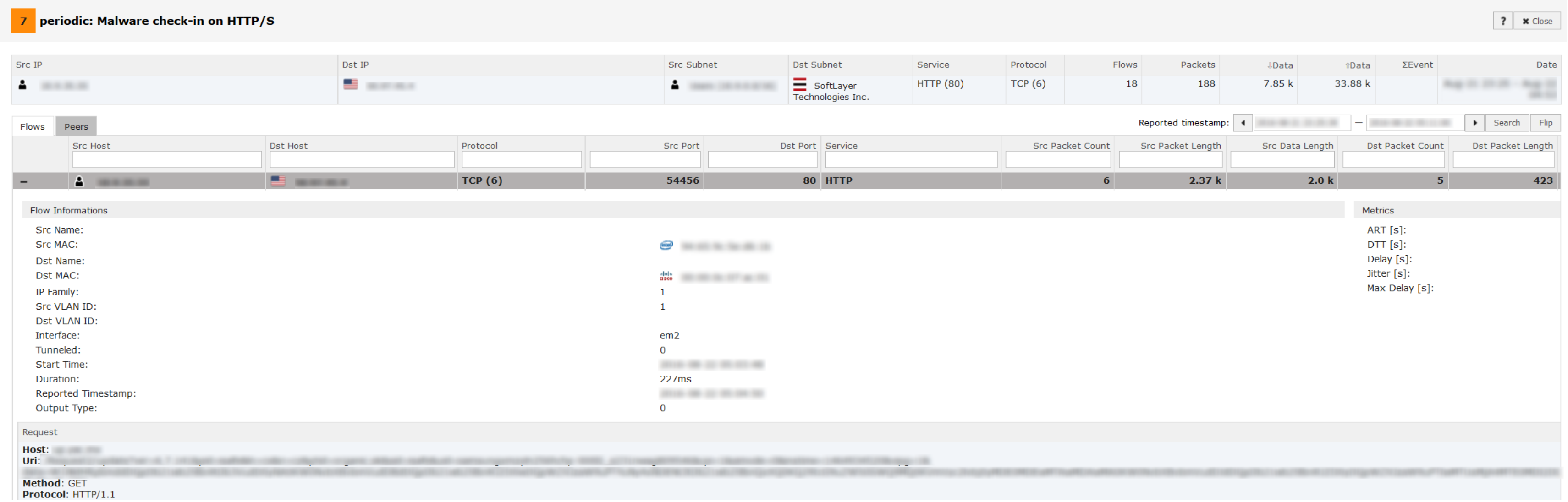
Top Src Subnets
Private C (192.168.0.0/16)

Top Dst Subnets
AT&T Services, Inc.
California State University, Office of the Chancellor
china tietong Shandong net
Elisa Oyj
LG POWERCOMM
MCI
net-lab GmbH

Top Services
445

DETECTED THREAT: PERIODIC COMMUNICATION

MENDEL detected periodic communication with a supposedly legitimate IP-address. The network metadata is classified as anomalous. Most likely, the user installed software with unknown malware.



7 **periodic: Malware check-in on HTTP/S**

Src IP	Dst IP	Src Subnet	Dst Subnet	Service	Protocol	Flows	Packets	⇩Data	⇧Data	ΣEvent	Date
[redacted]	[redacted]	[redacted]	SoftLayer Technologies Inc.	HTTP (80)	TCP (6)	18	188	7.85 k	33.88 k		[redacted]

Reported timestamp: [redacted] — [redacted]

	Src Host	Dst Host	Protocol	Src Port	Dst Port	Service	Src Packet Count	Src Packet Length	Src Data Length	Dst Packet Count	Dst Packet Length
–	[redacted]	[redacted]	TCP (6)	54456	80	HTTP	6	2.37 k	2.0 k	5	423

Flow Informations

Src Name:	
Src MAC:	[redacted]
Dst Name:	
Dst MAC:	[redacted]
IP Family:	1
Src VLAN ID:	1
Dst VLAN ID:	
Interface:	em2
Tunneled:	0
Start Time:	[redacted]
Duration:	227ms
Reported Timestamp:	[redacted]
Output Type:	0

Metrics

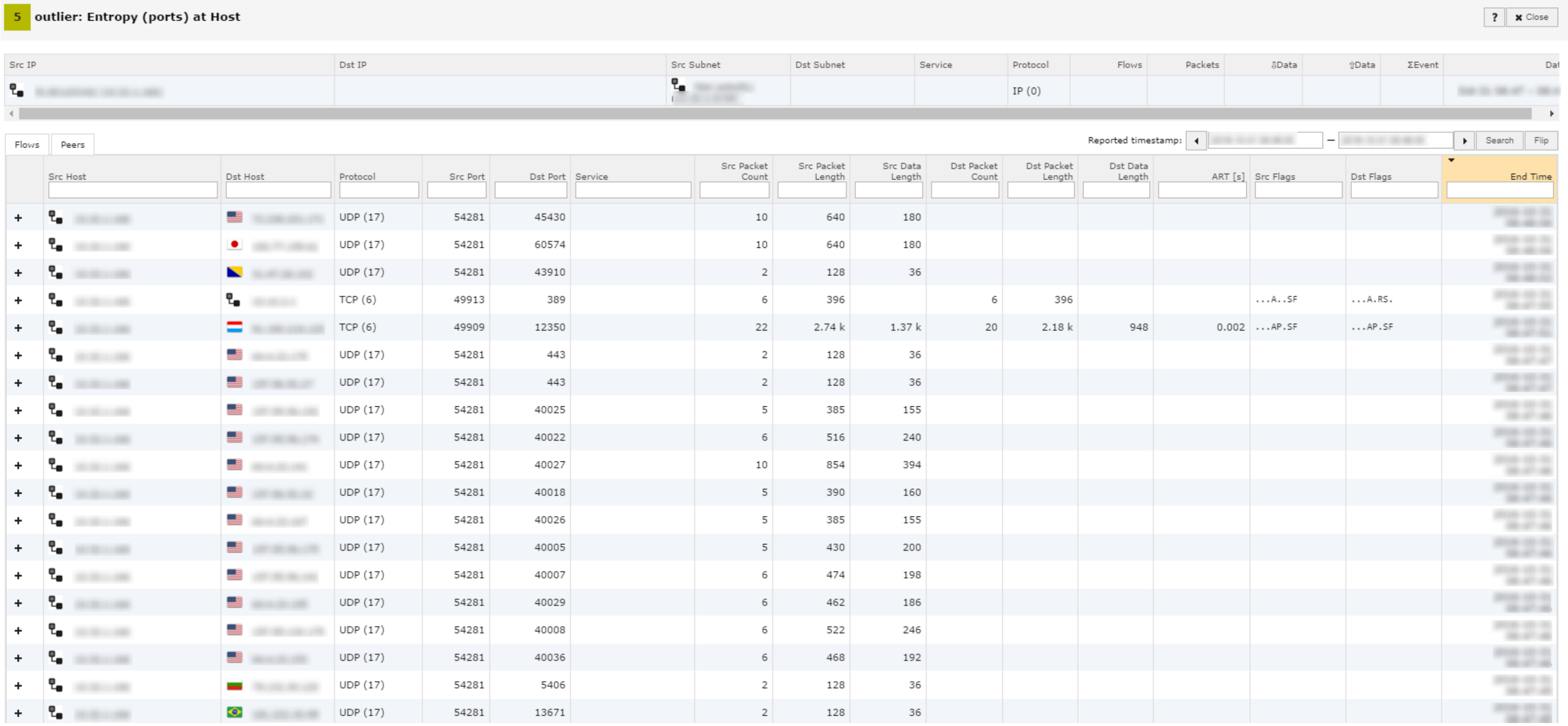
ART [s]:
DTT [s]:
Delay [s]:
Jitter [s]:
Max Delay [s]:

Request

Host: [redacted]
Uri: [redacted]
Method: GET
Protocol: HTTP/1.1

DETECTED THREAT: EXCESSIVE COMMUNICATION

This user normally communicates through 1 to 8 network services. But, the user's device tried to communicate through 39 services, and to 120 devices around the world including Brazil, Serbia, Bosnia and Herzegovina, the United States, Singapore, and Japan. No similar communication had occurred previously in the network.



5 **outlier: Entropy (ports) at Host**

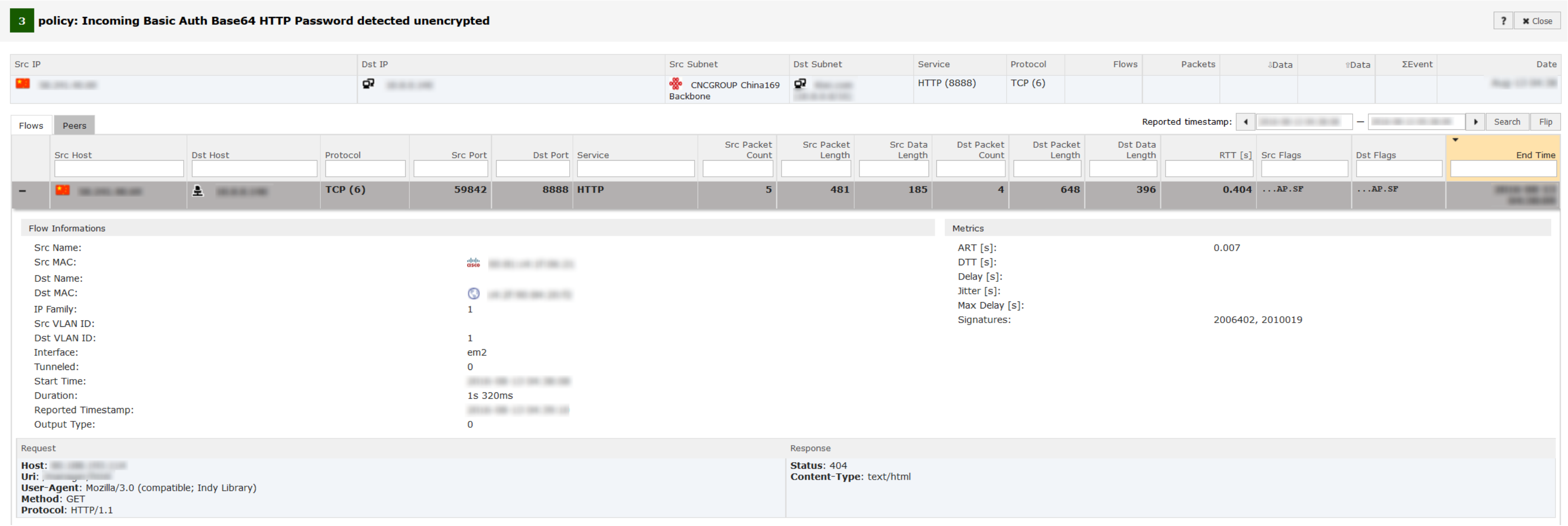
Src IP	Dst IP	Src Subnet	Dst Subnet	Service	Protocol	Flows	Packets	⇩Data	⇧Data	ΣEvent	Dat
[redacted]		[redacted]			IP (0)						[redacted]

Reported timestamp: [redacted] – [redacted]

	Src Host	Dst Host	Protocol	Src Port	Dst Port	Service	Src Packet Count	Src Packet Length	Src Data Length	Dst Packet Count	Dst Packet Length	Dst Data Length	ART [s]	Src Flags	Dst Flags	End Time
+	[redacted]	🇺🇸 [redacted]	UDP (17)	54281	45430		10	640	180							[redacted]
+	[redacted]	🇯🇵 [redacted]	UDP (17)	54281	60574		10	640	180							[redacted]
+	[redacted]	🇧🇦 [redacted]	UDP (17)	54281	43910		2	128	36							[redacted]
+	[redacted]	[redacted]	TCP (6)	49913	389		6	396		6	396			...A..SF	...A.RS.	[redacted]
+	[redacted]	🇱🇺 [redacted]	TCP (6)	49909	12350		22	2.74 k	1.37 k	20	2.18 k	948	0.002	...AP.SF	...AP.SF	[redacted]
+	[redacted]	🇺🇸 [redacted]	UDP (17)	54281	443		2	128	36							[redacted]
+	[redacted]	🇺🇸 [redacted]	UDP (17)	54281	443		2	128	36							[redacted]
+	[redacted]	🇺🇸 [redacted]	UDP (17)	54281	40025		5	385	155							[redacted]
+	[redacted]	🇺🇸 [redacted]	UDP (17)	54281	40022		6	516	240							[redacted]
+	[redacted]	🇺🇸 [redacted]	UDP (17)	54281	40027		10	854	394							[redacted]
+	[redacted]	🇺🇸 [redacted]	UDP (17)	54281	40018		5	390	160							[redacted]
+	[redacted]	🇺🇸 [redacted]	UDP (17)	54281	40026		5	385	155							[redacted]
+	[redacted]	🇺🇸 [redacted]	UDP (17)	54281	40005		5	430	200							[redacted]
+	[redacted]	🇺🇸 [redacted]	UDP (17)	54281	40007		6	474	198							[redacted]
+	[redacted]	🇺🇸 [redacted]	UDP (17)	54281	40029		6	462	186							[redacted]
+	[redacted]	🇺🇸 [redacted]	UDP (17)	54281	40008		6	522	246							[redacted]
+	[redacted]	🇺🇸 [redacted]	UDP (17)	54281	40036		6	468	192							[redacted]
+	[redacted]	🇧🇬 [redacted]	UDP (17)	54281	5406		2	128	36							[redacted]
+	[redacted]	🇧🇷 [redacted]	UDP (17)	54281	13671		2	128	36							[redacted]

DETECTED THREAT: SERIOUS POLICY BREACH

An exposed network device administrator with an unencrypted HTTP service resulted in illegitimate access attempt from China. This poses a high risk for penetration and misuse.



3 policy: Incoming Basic Auth Base64 HTTP Password detected unencrypted

Src IP	Dst IP	Src Subnet	Dst Subnet	Service	Protocol	Flows	Packets	⇩Data	⇧Data	ΣEvent	Date
[redacted]	[redacted]	CNCGROUP China169 Backbone	[redacted]	HTTP (8888)	TCP (6)						[redacted]

Reported timestamp: [redacted] — [redacted]

	Src Host	Dst Host	Protocol	Src Port	Dst Port	Service	Src Packet Count	Src Packet Length	Src Data Length	Dst Packet Count	Dst Packet Length	Dst Data Length	RTT [s]	Src Flags	Dst Flags	End Time
–	[redacted]	[redacted]	TCP (6)	59842	8888	HTTP	5	481	185	4	648	396	0.404	...AP.SF	...AP.SF	[redacted]

Flow Informations

Src Name:	
Src MAC:	[redacted]
Dst Name:	
Dst MAC:	[redacted]
IP Family:	1
Src VLAN ID:	
Dst VLAN ID:	1
Interface:	em2
Tunneled:	0
Start Time:	[redacted]
Duration:	1s 320ms
Reported Timestamp:	[redacted]
Output Type:	0

Metrics

ART [s]:	0.007
DTT [s]:	
Delay [s]:	
Jitter [s]:	
Max Delay [s]:	
Signatures:	2006402, 2010019

Request

Host: [redacted]
Uri: [redacted]
User-Agent: Mozilla/3.0 (compatible; Indy Library)
Method: GET
Protocol: HTTP/1.1

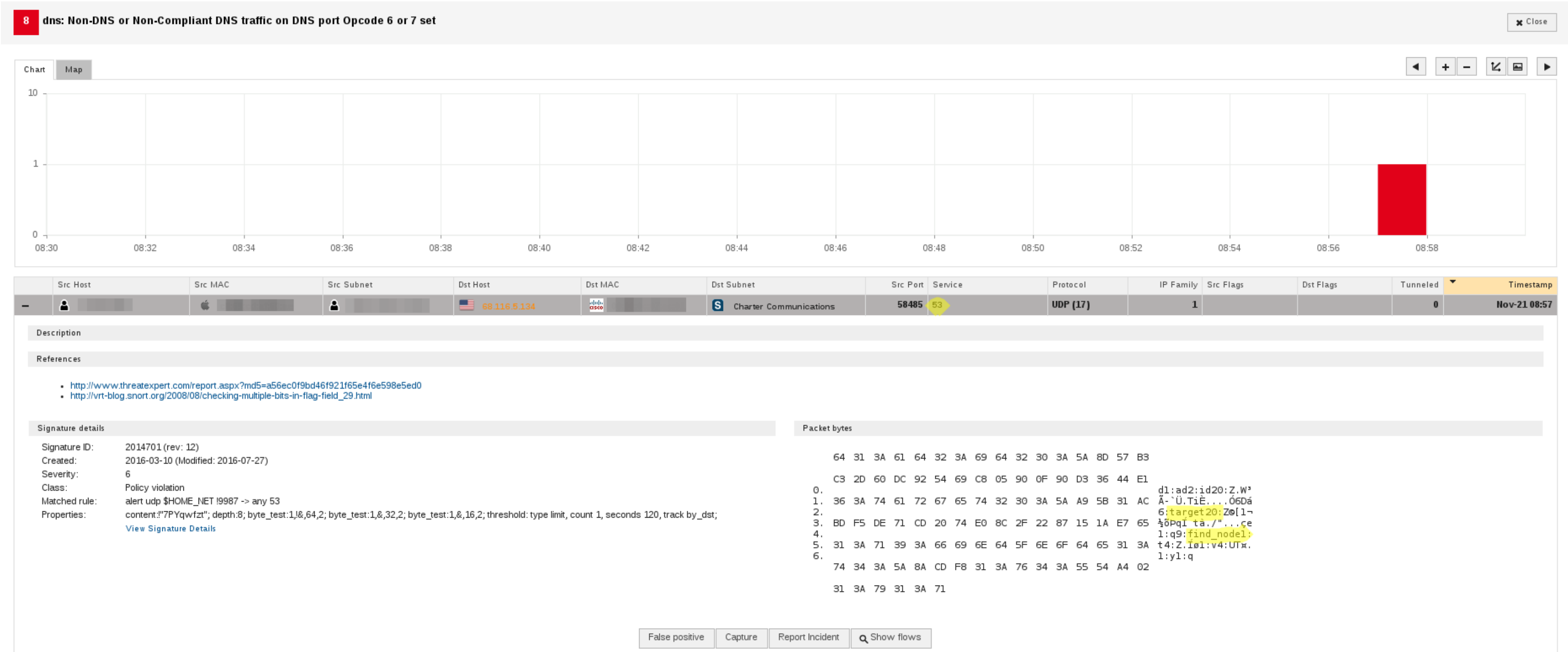
Response

Status: 404
Content-Type: text/html

GREYCORTEX

DETECTED THREAT: DNS TUNNEL

Unusual communication with a blacklisted IP address on Port 53 (DNS). The user has installed an infected torrent client. This poses a high risk of data leakage.



	Src Host	Src MAC	Src Subnet	Dst Host	Dst MAC	Dst Subnet	Src Port	Service	Protocol	IP Family	Src Flags	Dst Flags	Tunneled	Timestamp
–	[redacted]	[redacted]	[redacted]	68.116.5.134	[redacted]	Charter Communications	58485	53	UDP (17)	1			0	Nov-21 08:57

Description

References

- http://www.threatexpert.com/report.aspx?md5=a56ec0f9bd46f921f65e4f6e598e5ed0
- http://vrt-blog.snort.org/2008/08/checking-multiple-bits-in-flag-field_29.html

Signature details

Signature ID:	2014701 (rev: 12)
Created:	2016-03-10 (Modified: 2016-07-27)
Severity:	6
Class:	Policy violation
Matched rule:	alert udp $HOME_NET !9987 -> any 53
Properties:	content:!"7PYqwfzt"; depth:8; byte_test:1,!&,64,2; byte_test:1,&,32,2; byte_test:1,&,16,2; threshold: type limit, count 1, seconds 120, track by_dst;

View Signature Details

Packet bytes

```
    64 31 3A 61 64 32 3A 69 64 32 30 3A 5A 8D 57 B3

    C3 2D 60 DC 92 54 69 C8 05 90 0F 90 D3 36 44 E1
 0.                                                  d1:ad2:id20:Z.W³
 1. 36 3A 74 61 72 67 65 74 32 30 3A 5A A9 5B 31 AC  Ã-`Ü.TiÈ....Ó6Dá
 2.                                                  6:target20:Z©[1¬
 3. BD F5 DE 71 CD 20 74 E0 8C 2F 22 87 15 1A E7 65  ½õÞqÍ tà./"...çe
 4.                                                  1:q9:find_node1:
 5. 31 3A 71 39 3A 66 69 6E 64 5F 6E 6F 64 65 31 3A  t4:Z.Íø1:v4:UT¤.
 6.                                                  1:y1:q
    74 34 3A 5A 8A CD F8 31 3A 76 34 3A 55 54 A4 02

    31 3A 79 31 3A 71
```

GREYCORTEX RESEARCH

Monitoring and Network Traffic Analysis of …

- critical energy infrastructure
- industrial networks
- wireless networks
- IoT

GREYCORTEX MENDEL

BRNO UNIVERSITY OF TECHNOLOGY

SUCCESS STORIES

NBÚ

Linde

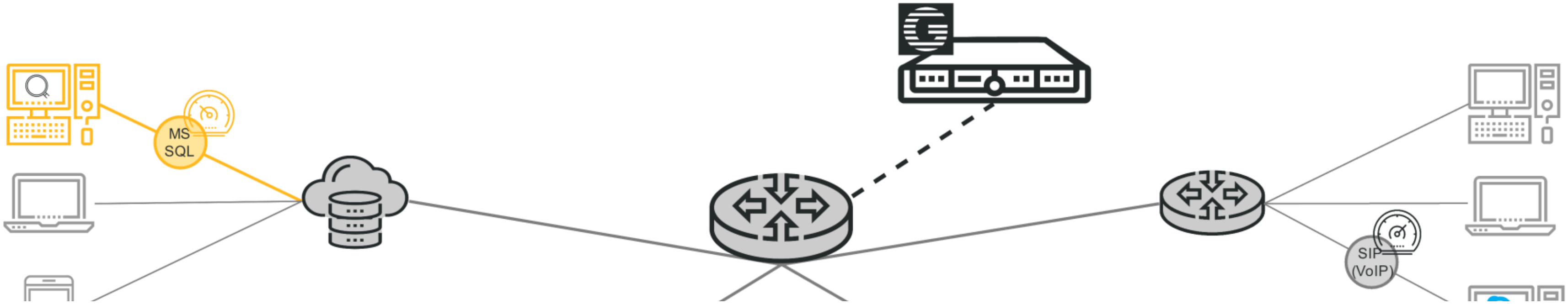
KIWI · COM

Česká pošta

T · · Systems ·

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

TOGETHER, WE CAN SEE IOT IN DETAIL



WE WILL BE HAPPY TO DISCUSS COOPERATION OPPORTUNITIES!

GREYCORTEX

THANK YOU FOR YOUR ATTENTION!

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

www.greycortex.com *)
twitter.com/greycortex
linkedin.com/company/greycortex
youtube.com/greycortex **)

Vladimír Sedláček
info@greycortex.com ***)
+420 511 205 388
linkedin.com/in/vsedlacek/

*) whitepapers, use cases, and more
**) watch more presentations
***) request access to our DEMO!

GREYCORTEX