

Mesterséges intelligencia alapú védelemi technológiák



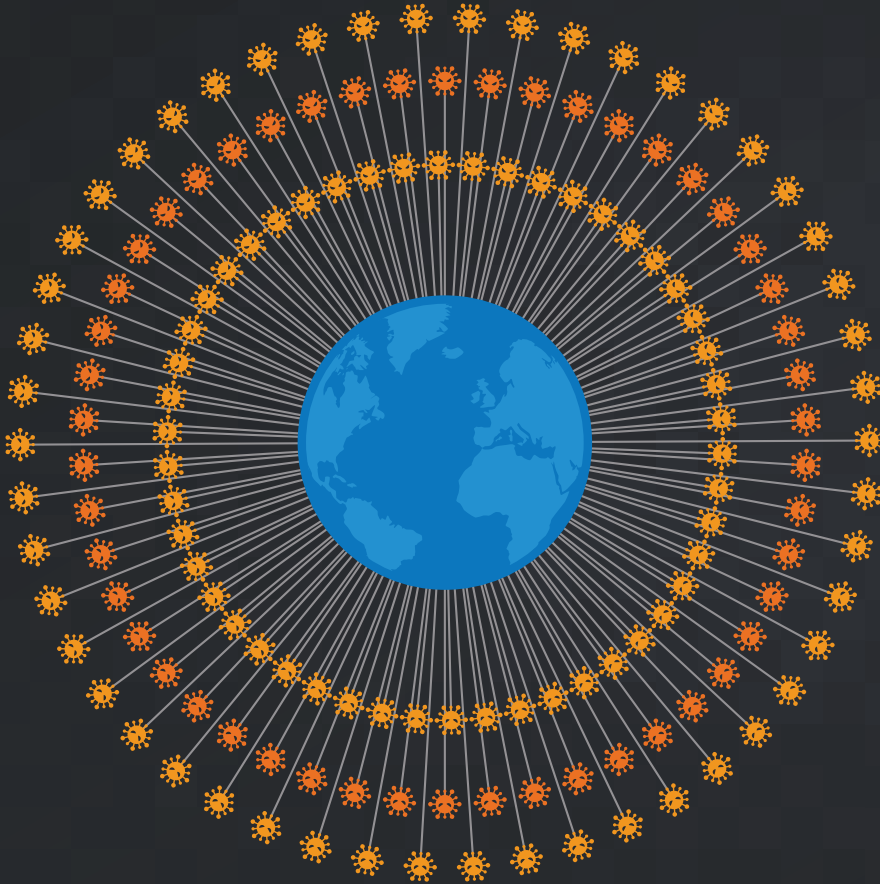
HBONE Workshop 2019.

Ács György

IT biztonsági konzulens

2019. február 14.

Threat Landscape



= 10,000

1.5 Million Unique

Malware samples **DAILY**

“Information Security is Becoming a Big Data Problem”

by Neil MacDonald, VP & Gartner Fellow

Témák

- Néhány szó az elméletről
- MI a rossz oldalon
- MI technológiák a jó oldalon
 - File vizsgálat és osztályozás
 - Ezt a domaint mire fogják használni?
 - Ismerjük fel a malware-t, visszatitkosítás nélkül



Néhány szó az elméletről

*„Amíg van esélyünk megérteni,
hogyan működik az MI, érdemes
lenne megkísérelni megérteni!”*

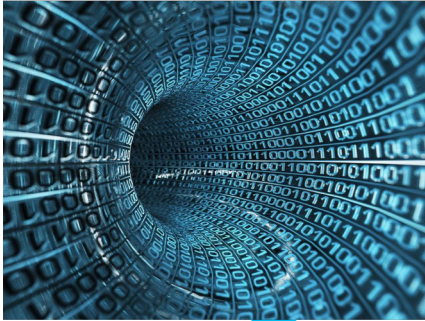
Ács György

Miből áll a mesterséges intelligencia?

- Adat

Algoritmus/Software

Nagy számítási kapacitás (tanítás)



```
from twython import Twython, TwythonStream
import time

APP_KEY = 'YOUR KEY'
APP_SECRET = 'YOUR SECRET'
OAUTH_TOKEN = 'YOUR TOKEN'
OAUTH_TOKEN_SECRET = 'YOUR SECRET'

twitter = Twython(APP_KEY, APP_SECRET, OAUTH_TOKEN, OAUTH_TOKEN_SECRET)
```



Prediction, classification, pattern discovery



“Feature” – “lényegkiemelt paraméterek”, Az adat kritikus : “DATA IS KING”
Rossz adat -> rossz végeredmény, “sok” adat kell jó végeredményhez,
adattisztítás szükséges

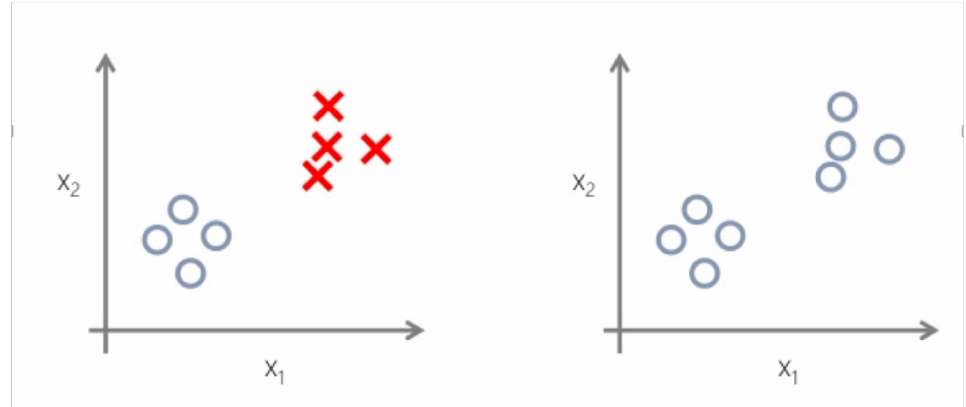
Gépi tanulás

- **Típusok:**

- Supervised L. (felügyelt t.)
- Unsupervised Learning
- Reinforcement L. (megerősítéses t.)
- Deep Learning

- **Lépések:**

- „Feature” kiválasztás
- Tanítás (címkézett adat)
- Becslés – Prediction

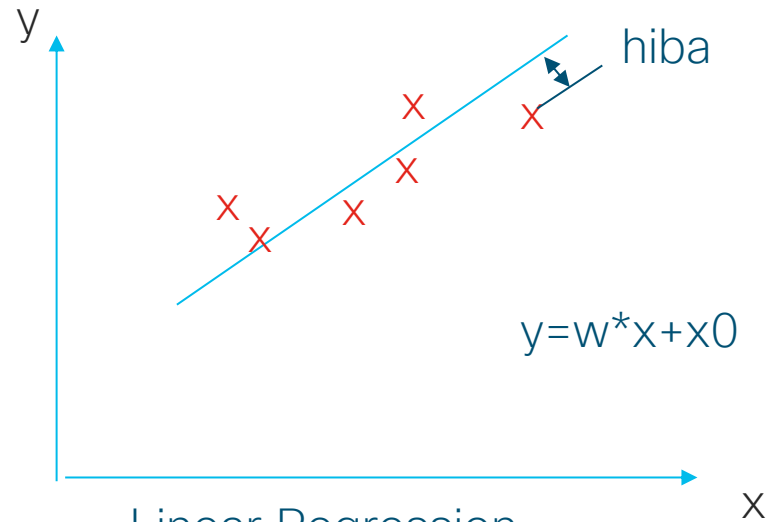


Supervised

Unsupervised

Supervised Learning – Felügyelt tanulás

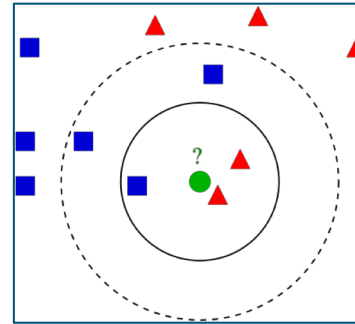
- **Osztályozás (classification):**
csoportok hozzárendelése az új adathoz az előző adatok alapján
- **Regresszió:** a bementi adatból "előrejelzi" az "y" értékeket a korábbi adatok alapján
- Minden adatnak **feature**-ei vannak (x_1, x_2, \dots, x_n) és **címkéje** (y , kimenet)
- A training adat: az adat címkéje ismert



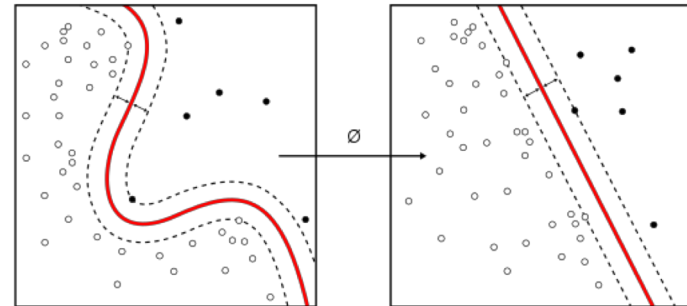
Supervised Learning - Felügyelt tanulás

- **Típusai:**

- Linear Regression
- Logistic Regression (2 kimenet lehet (malware/nem malware), pl.:joy)
- K-Nearest Neighbor (KNN)
- Support Vector Machine (SVM)
- Decision trees and random forests (döntési fát épít a változókból)
- És még sok



Ha $k=3$, akkor piros,
ha $k=5$, akkor kék



Unsupervised Learning – Felügyelet nélküli tanulás

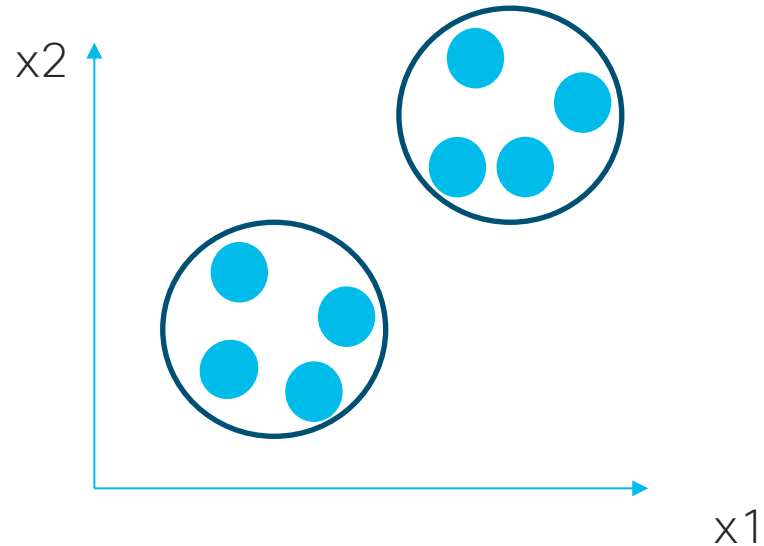
Címkézetlen adatok vannak csak!

- **Klaszterezés:**

- az adatok csoportosítása hasonlóság vagy különbség alapján

- **Kapcsolatok:**

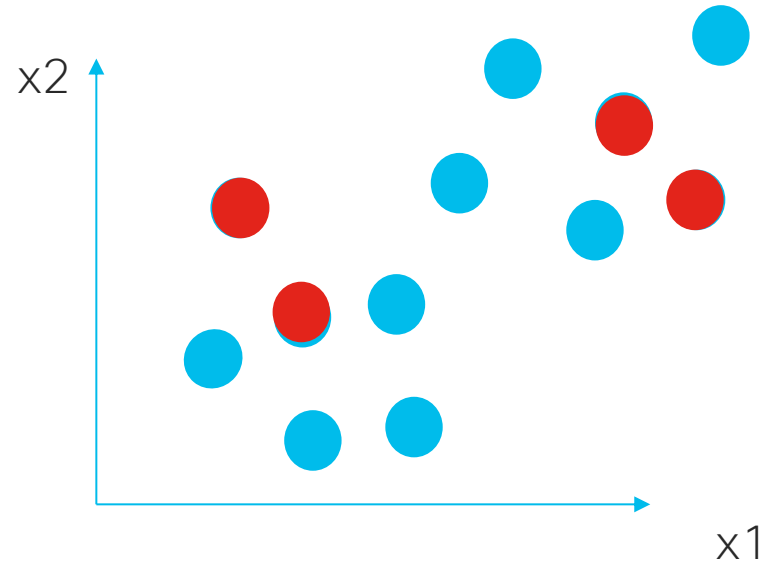
- keressünk szabályokat, amik leírják az adatokat.
- “Aki PC-t vesz, vesz memóriát is.”



Unsupervised Learning – Felügyelet nélküli tanulás

Címkézetlen adatok vannak csak!

- Pl.: **K-means** (k-közép) :
- Próbáljuk meg "k" csoportra osztani az adatokat
- **Algoritmus:**
 - Válasszunk ki "k" random pontot középpontként
 - Adjuk meg az összes pontra a közelség alapján melyik középponthez tartozik
 - Központok frissítése csoporton belül
 - Ismételve addig, amíg a centrumok nem változnak





Axe

Witch Doctor

Dragon Knight

Drow Ranger

JUGGERNAUT



50
3
300
20
26
14



600 / 600 +25.7

229 / 229 +23.7

Drag items to add to quick buy

625





Elon Musk ✓

@elonmusk

Follow



OpenAI first ever to defeat world's best players in competitive eSports. Vastly more complex than traditional board games like chess & Go.

5:15 PM - 11 Aug 2017

4,444 Retweets 15,026 Likes



487



4.4K

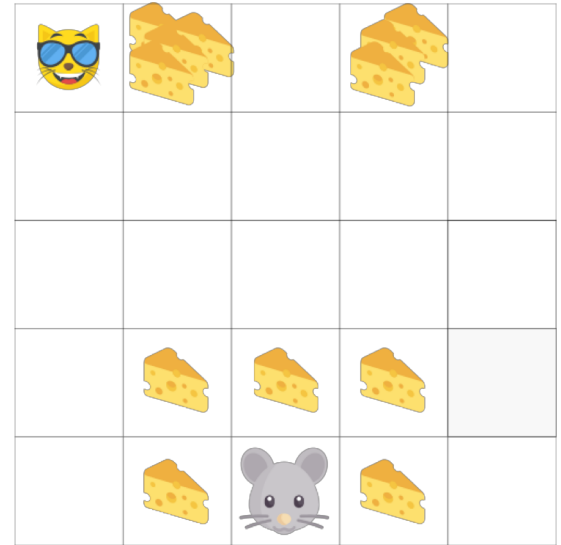


15K



Reinforcement Learning – Megerősítéses tanulás

- A világ “felfedezése”, a cselekvések “jutalmazása” adott
- Véletlenszerű lépésekkel kezdődik, minden lépésnél a jutalom eltárolása (lehet +/-, a “karakter” meghalt)
- Hozzunk létre egy stratégiát, amely magasabb jutalmat eredményez
- Folytassuk a stratégia javítását ”sok” tapasztalattal
- Példák: AlphaGo, OpenAI; magukkal több ezer játékot játszottak, amíg meg nem tanultak egy olyan stratégiát, amely közel “tökéletes” a komplex játékokban





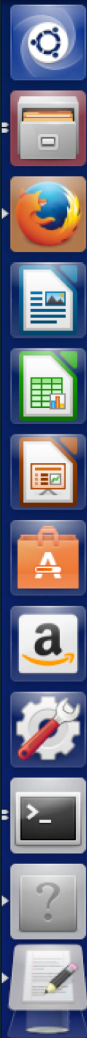
<https://repl.it/@GyorgyAcs/CartPole>

Deep Learning

- A legmodernebb a gépi tanulás
- Leginkább felügyelt tanuláshoz hasonlít
- Neurális hálózatokat használ (az első alkalmazás: agyi neuronok modellezésére)
- Bonyolultabb
- Több adatra van szükség
- Több időt igényel a tanítás
- Kép-, beszéd felismerés
- Natural Language Processing
- Machine translation (DeepL)
- Önvezető autók
- Stb.

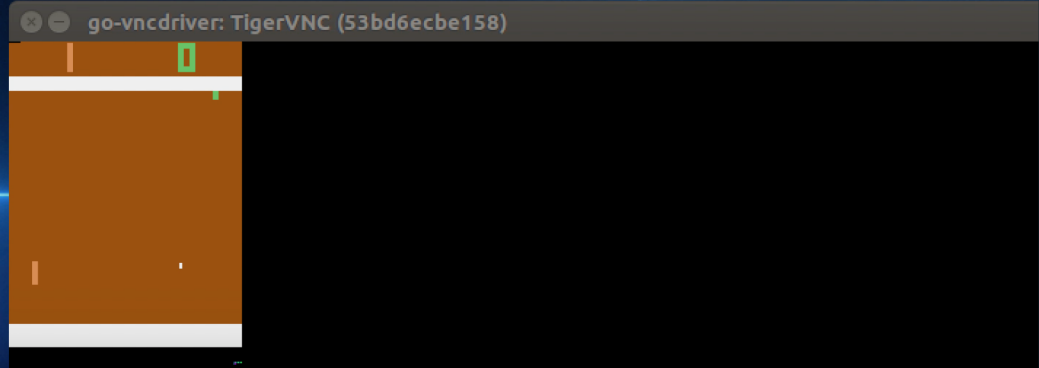


MI a rossz oldalon



vmware-tools-distrib

OpenAI - Universe Installation Guide
Ubuntu 16.04 - Justin's Blog_files



```

Terminal File Edit View Search Terminal Help
tep': 50422}
universe-xIOM9D-0 | [2018-03-25 08:23:00,964] [EnvPlayer] Over past 1.02s, sent 61 reward messages
to agent: reward=-1.0 reward_min=-1.0 reward_max=0.0 done=False info={'ale.lives': 0, 'gym-core.s
tep': 50483}
universe-xIOM9D-0 | [2018-03-25 08:23:01,965] [EnvPlayer] Over past 1.00s, sent 60 reward messages
to agent: reward=-1.0 reward_min=-1.0 reward_max=0.0 done=False info={'ale.lives': 0, 'gym-core.s
tep': 50543}
universe-xIOM9D-0 | [2018-03-25 08:23:02,447] RESET CAUSE: Resetting since done=True
universe-xIOM9D-0 | [2018-03-25 08:23:02,447] [EnvStatus] Changing env_state: running (env_id=gym-
core.PongDeterministic-v0) -> resetting (env_id=gym-core.PongDeterministic-v0) (episode_id: 54->55
, fps=60)
universe-xIOM9D-0 | [2018-03-25 08:23:02,450] [env] Running automatic env.reset()
universe-xIOM9D-0 | [2018-03-25 08:23:02,450] [EnvPlayer] Over past 0.49s, sent 29 reward messages
to agent: reward=-1.0 reward_min=-1.0 reward_max=0.0 done=True info={'ale.lives': 0, 'gym-core.st
ep': 50572}
universe-xIOM9D-0 | [2018-03-25 08:23:02,451] [EnvPlayer] Ending previous episode: episode_reward=
-19.0 episode_count=1058 episode_duration=17.64
universe-xIOM9D-0 | [2018-03-25 08:23:02,477] [EnvStatus] Changing env_state: resetting (env_id=gy
m-core.PongDeterministic-v0) -> running (env_id=gym-core.PongDeterministic-v0) (episode_id: 55->55
, fps=60)
universe-xIOM9D-0 | [2018-03-25 08:23:03,457] [EnvPlayer] Over past 1.01s, sent 54 reward messages
to agent: reward=0.0 reward_min=0.0 reward_max=0.0 done=False info={'ale.lives': 0, 'gym-core.ste
p': 50626}


```

Malware gyártás MI-val

Security

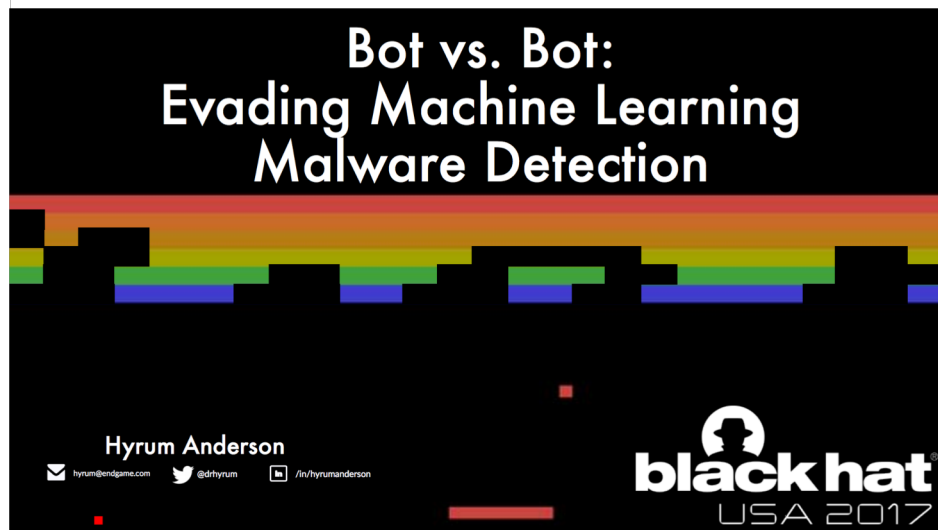
AI quickly cooks malware that AV software can't spot

Experiment used Elon Musk's OpenAI framework - no wonder he's so down on AI

By [Iain Thomson](#) in [San Francisco](#) 31 Jul 2017 at 07:02 38  [SHARE](#) ▼

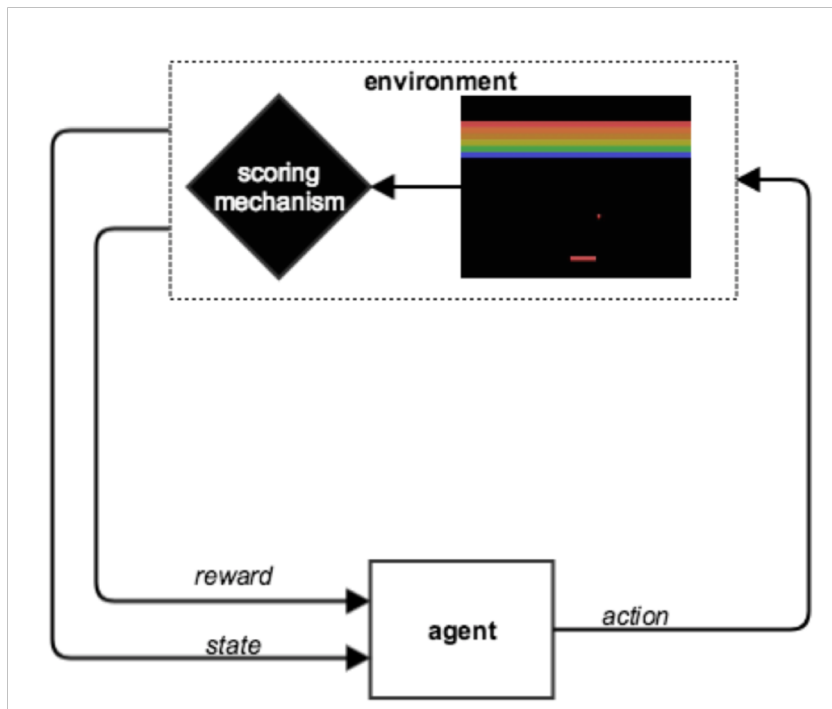
DEF CON Machine-learning tools can create custom malware that defeats antivirus software.

In a keynote demonstration at the [DEF CON hacking convention](#) Hyrum Anderson, technical director of data science at security shop Endgame, showed off research that his company had done in adapting Elon Musk's OpenAI framework to the task of creating malware that security engines can't spot.



https://www.theregister.co.uk/2017/07/31/ai_defeats_antivirus_software/

Atari játékok helyett malware



Környezet:

- Fallabda játék több téglasorral
- Vezérlés: jobbra, balra vagy marad
- Téglá lebontása a cél

“Agent”:

- Bemenet : képpont pixelek
- Kimenet: akció (balra, jobbra)

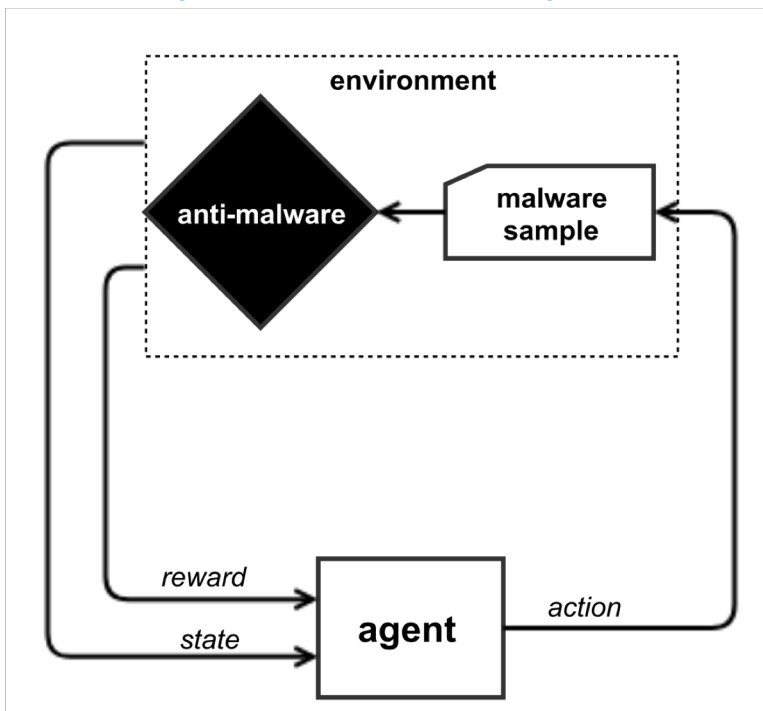
Tanulás: több 1000 játék

Hová kellene lépni?

<https://gym.openai.com/envs/Breakout-v0>

<https://www.blackhat.com/docs/us-17/thursday/us-17-Anderson-Bot-Vs-Bot-Evading-Machine-Learning-Malware-Detection.pdf>

Atari játékok helyett malware



Környezet:

- Malware minta, Windows PE header
- Mutáció: új belépési pont, új section, véletlen importok, byte-ok, stb.

“Agent”:

- Bemenet : malware byte-ok
- Kimenet: akció (sztochasztikus)

Jutalom: az AV riport szerint tiszta a file

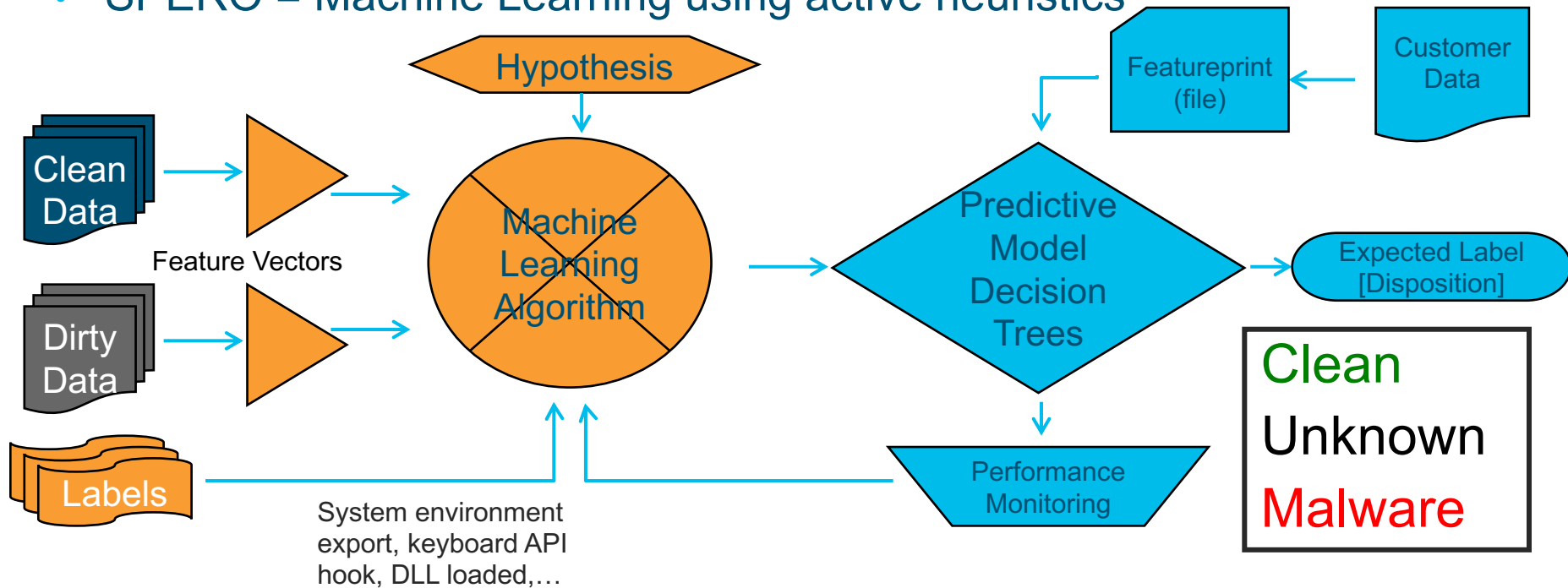
<https://www.blackhat.com/docs/us-17/thursday/us-17-Anderson-Bot-Vs-Bot-Evading-Machine-Learning-Malware-Detection.pdf>

A blue-tinted photograph of a city street at night. The scene is dominated by the silhouettes of street lamps and a church spire in the background. The street is lined with trees and buildings, and the overall atmosphere is quiet and urban.

File vizsgálat és osztályozás

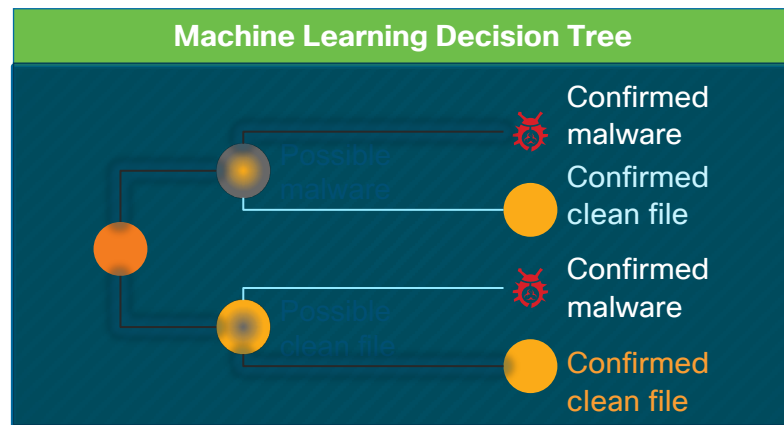
AMP, Advanced Malware Protection Védelmi rendszer : Spero motor

- SPERO = Machine Learning using active heuristics



Védelmi rendszer : Spero vizsgálati motor

- AMP címkék = a végrehajtás során kapott jellemzők
 - Hálózati kapcsolatok?
 - Nem szabványos protokoll –alkalmazás
 - Hooking? Milyen API-kat használ?
 - Filerendszer változtatás?
 - Másolja magát
 - File-ok mozgatása
 - Más processzek indítása?
- Több, mint 400 jellemzőt elemez – azonosítja a malware-t



Jósoljuk meg, hogy Domi fog-e focizni!

- Nehéz így átlátni
- „oszd meg és uralkodj”
 - Vágjuk részhalmozokra
 - „Tiszta” halmaz? (Csak igen vagy nem)
 - Ha igen : állj
 - Ha nem : ismételd
- Nézzük, hogy az új adat melyik részhalmozba esik

Tanító minták:

9 Igen / 5 Nem

Új adat:

attributes				
nap	időj.	pára.	szél	játék
D1	napos	magas	gyen.	Nem
D2	napos	magas	erős	Nem
D3	borult	magas	gyen.	Igen
D4	eső	magas	gyen.	Igen
D5	eső	normál	gyen.	Igen
D6	eső	normál	erős	Nem
D7	borult	normál	erős	Igen
D8	napos	magas	gyen.	Nem
D9	napos	normál	gyen.	Igen
D10	eső	normál	gyen.	Igen
D11	napos	normál	erős	Igen
D12	borult	magas	erős	Igen
D13	borult	normál	gyen.	Igen
D14	eső	magas	erős	Nem
D15	eső	magas	gyen.	???

9 Igen / 5 Nem

időj.

napos

borult

eső

nap	időj.	pára.	szél	játék
D1	napos	magas	gyen.	Nem
D2	napos	magas	erős	Nem
D8	napos	magas	gyen.	Nem
D9	napos	normál	gyen.	Igen
D11	napos	normál	erős	Igen

2 Igen / 3 Nem
Osszuk tovább

nap	időj.	pára.	szél	játék
D3	borult	magas	gyen.	Igen
D7	borult	normál	erős	Igen
D12	borult	magas	erős	Igen
D13	borult	normál	gyen.	Igen

4 Igen / 0 Nem
Tiszta részhalmaz

nap	időj.	pára.	szél	játék
D4	eső	magas	gyen.	Igen
D5	eső	normál	gyen.	Igen
D6	eső	normál	erős	Nem
D10	eső	normál	gyen.	Igen
D14	eső	magas	erős	Nem

3 Igen / 2 Nem
Osszuk tovább

9 Igen / 5 Nem

időj.

borult

napos

pára.

magas

normál

nap	időj.	pára.	szél	játék
D3	borult	magas	gyen.	Igen
D7	borult	normál	erős	Igen
D12	borult	magas	erős	Igen
D13	borult	normál	gyen.	Igen

4 Igen / 0 Nem
Tiszta részhalmaz

eső

nap	időj.	pára.	szél	játék
D4	eső	magas	gyen.	Igen
D5	eső	normál	gyen.	Igen
D6	eső	normál	erős	Nem
D10	eső	normál	gyen.	Igen
D14	eső	magas	erős	Nem

3 Igen / 2 Nem
Osszuk tovább

nap	pára.	szél	játék
D1	magas	gyen.	Nem
D2	magas	erős	Nem
D8	magas	gyen.	Nem

nap	pára.	szél	játék
D9	normál	gyen.	Igen
D11	normál	erős	Igen

9 Igen / 5 Nem

időj.

borult

napos

pára.

magas

normál

nap	időj.	pára.	szél	játék
D3	borult	magas	gyen.	Igen
D7	borult	normál	erős	Igen
D12	borult	magas	erős	Igen
D13	borult	normál	gyen.	Igen

4 Igen / 0 Nem
tiszta részhalmaz

eső

szél

gyen.

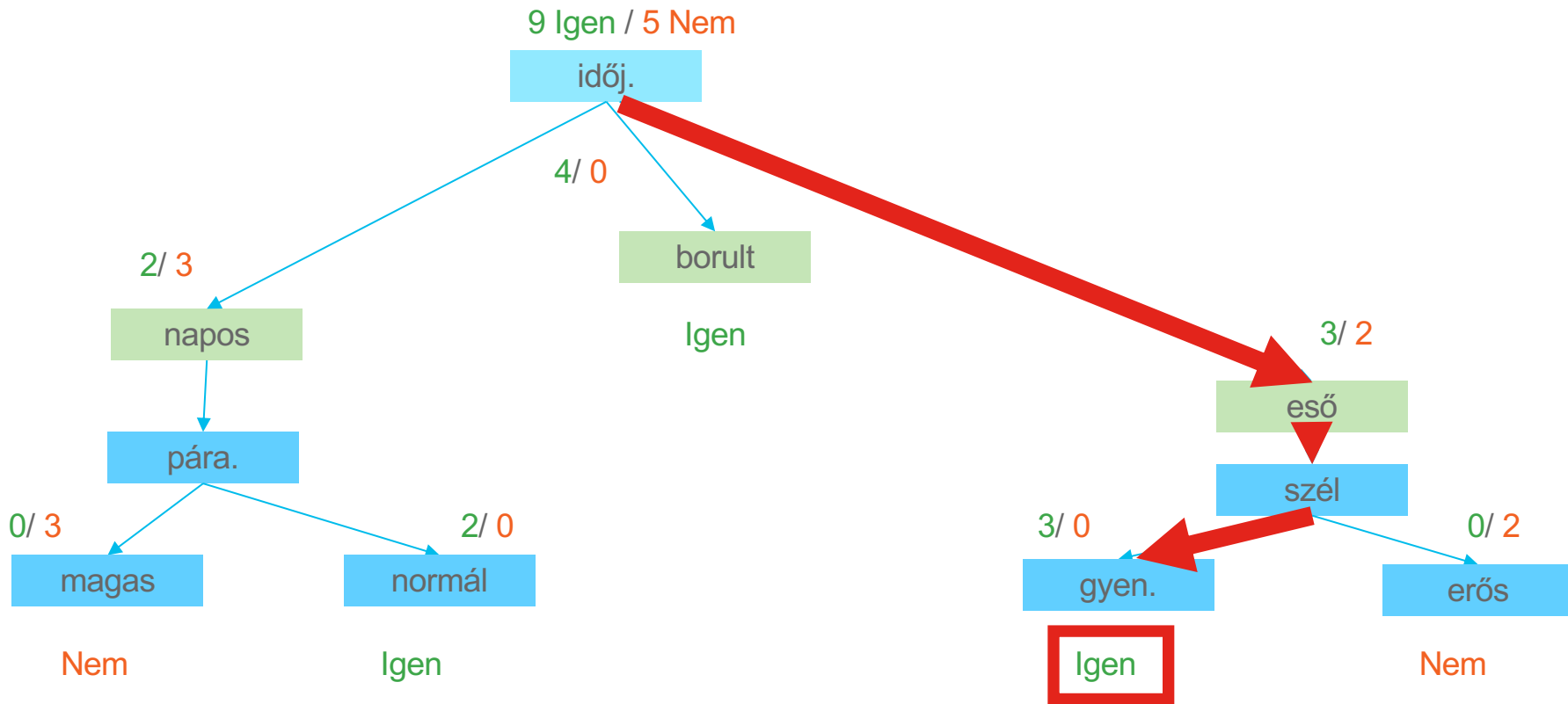
erős

nap	pára.	szél	játék
D1	magas	gyen.	Nem
D2	magas	erős	Nem
D8	magas	gyen.	Nem

nap	pára.	szél	játék
D9	normál	gyen.	Igen
D11	normál	erős	Igen

nap	időj.	pára.	játék
D4	eső	magas	Igen
D5	eső	normál	Igen
D10	eső	normál	Igen

nap	időj.	pára.	játék
D6	eső	normál	Nem
D14	eső	magas	Nem



Új adat:

D15	eső	magas	gyen.	Igen
-----	-----	-------	-------	-------------

Random Forests
menjünk a véletlen erdőbe!

https://colab.research.google.com/drive/1h811s2qow3a857uHnB30jofcWE-bhjC_



Ezt a domaint mire fogják használni?

A kibertámadások elemzése

- Felderítés és infrastruktúra kiépítés
- Domain regisztráció, IP, ASN intelligencia
- Az eredmények alapján monitorozás

○ Az első áldozat megjelenik

- A támadás kiterjed
- Nagy mennyiségű áldozat
- Szignatúrát fejlesztenek

DNS alapú vizsgálat és szűrés



Umbrella

100-140 milliárd napi kérés

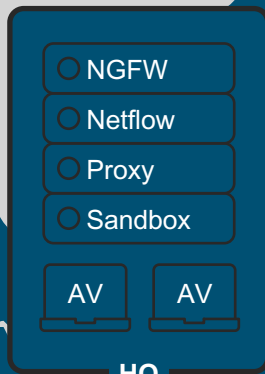
First line

Minden kommunikáció
a DNS-sel kezdődik

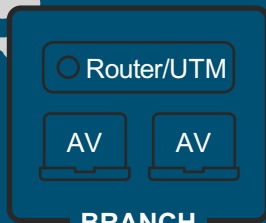
file vizsgálat proxy-val

Minden eszköz (IoT)
használja

Port független



HQ

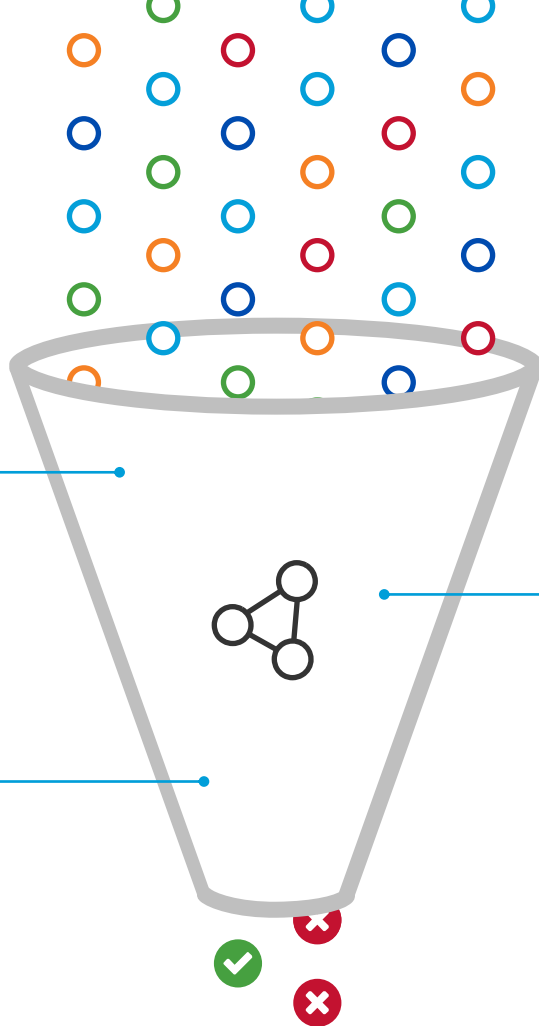


BRANCH



ROAMING

Statisztikai modellek



2M+ live events per second

11B+ historical events

100-140B queries per day

3 million new domains every day

Környezet miatt bűnös

- *Co-occurrence model*
- *IP Geo-Location model*
- *Secure rank model*
- *Sender rank model*

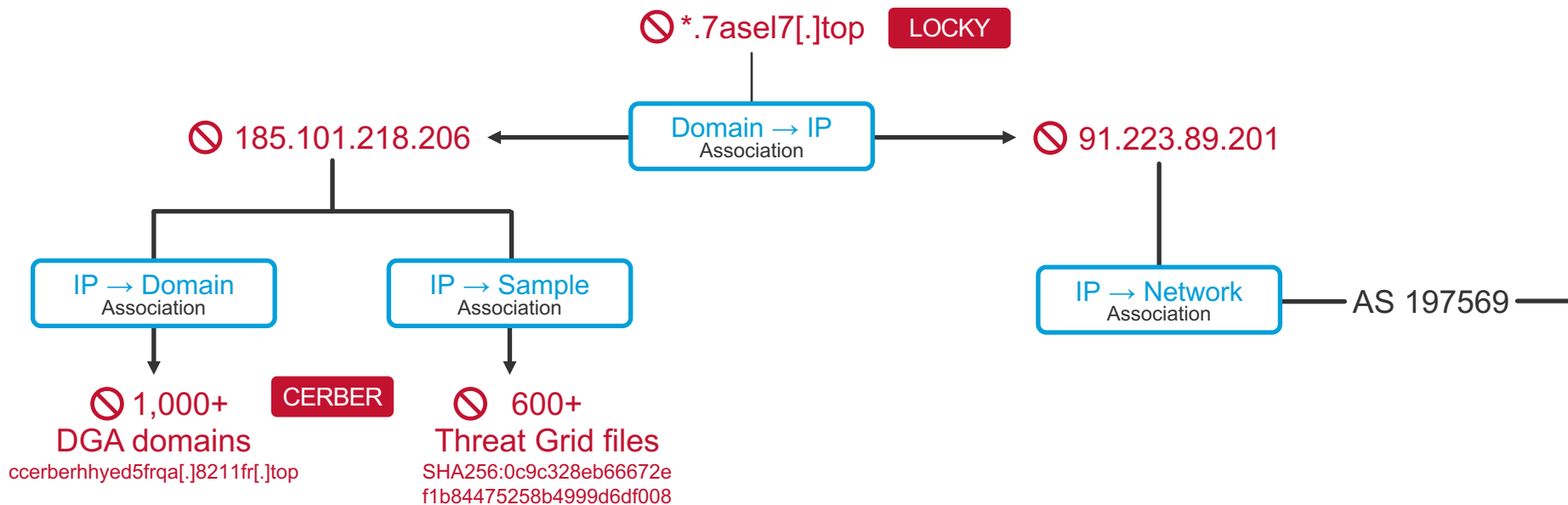
Kapcsolatok miatt bűnös

- *Predictive IP Space Modeling*

A bűnös mintákat mutat

- *Spike rank model*
- *Natural Language Processing rank model*
- *Live DGA Prediction*

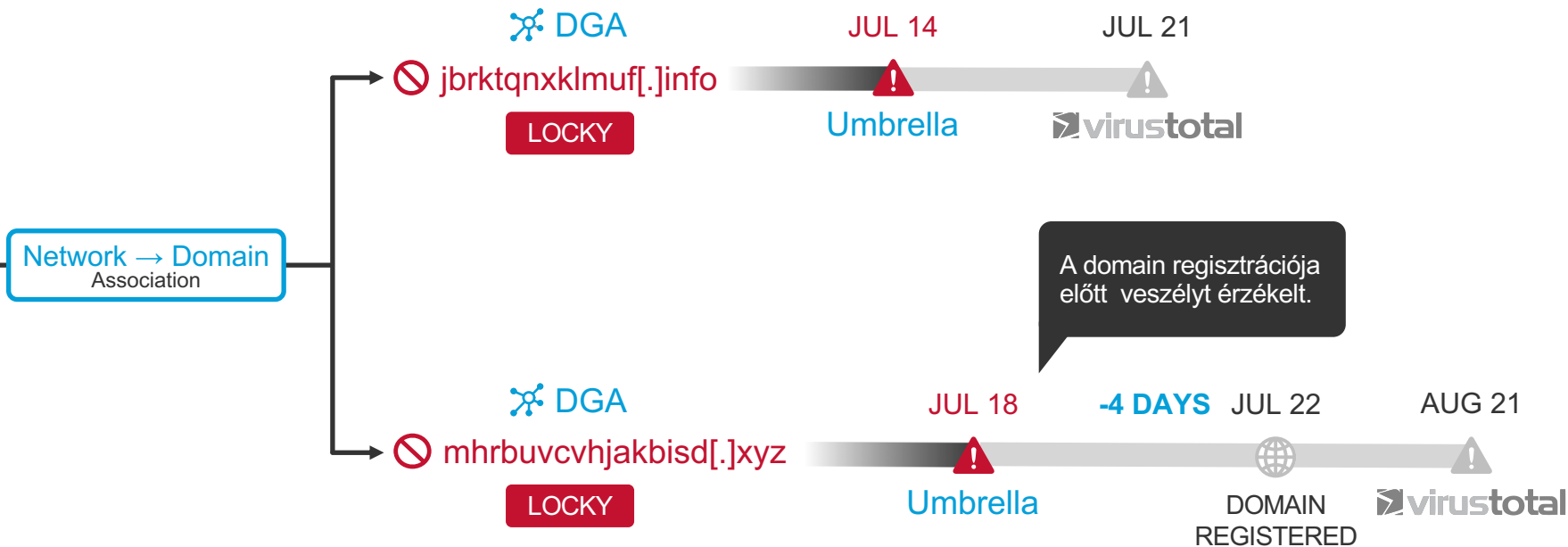
Zsarolóprogram esettanulmány



A Locky és Cerber ugyanazt az infrastruktúrát használja

Zsarolóprogram esettanulmány

Amint a domain-t regisztrálták a veszélyes kategóriába került, DGA detektor algoritmus segítségével



A statisztikus modellek azonosítottak és blokkoltak a DGA algoritmus által generált 2 domain-t, jó néhány nappal azelőtt, hogy regisztrálták.

A blue-tinted photograph of a European city street. The scene shows a cobblestone road with several cars parked and driving. In the background, there are historic buildings, including a prominent church tower with Gothic architecture. The overall atmosphere is quiet and urban.

Ismerjük fel a malware-t, visszatitkosítás nélkül

Titkosítás mindenhol



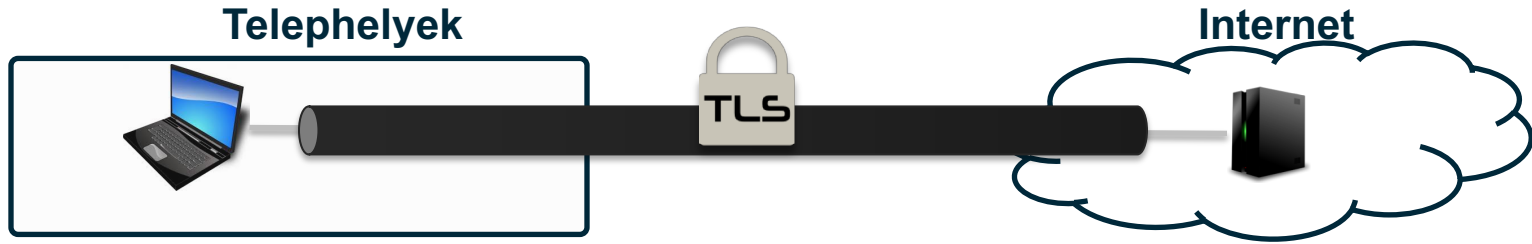
Chrome will start marking
all HTTP sites as not
secure in July

A screenshot of a network traffic analysis tool interface. The main window is titled "Traffic by Application" and displays a table of network traffic data. The table has two columns: "Application" and "Total Connections". The data is as follows:

Application	Total Connections
<input type="checkbox"/> HTTPS	12,549,748
<input type="checkbox"/> HTTP	1,723,660
<input type="checkbox"/> DNS	996,348
<input type="checkbox"/> Apple sites	986,011
+1 ↑ <input type="checkbox"/> Google	744,535
-1 ↓ <input type="checkbox"/> Web browser	740,617
<input type="checkbox"/> STUN	686,813
<input type="checkbox"/> STUN client	686,813
<input type="checkbox"/> iCloud	488,673
<input type="checkbox"/> Exchange Online	422,403

At the bottom of the table, it says "Last updated 1 minute ago".

A probléma: titkosított malware forgalom

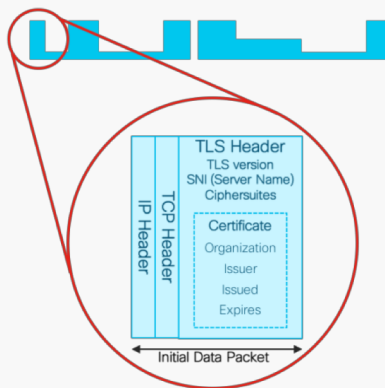


- A TLS használata többségben van már (nem baj!)
- A mintaillesztéses eljárások NEM hatékonyak
- MITM problémák
 - "Privacy", jogi, megvalósítási, „drága”, nem együttműködő kliensek, cert pinning, ...

A “jellemzők” : Enhanced NetFlow és intelligencia

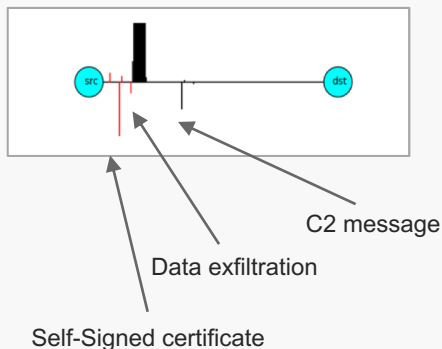
Initial Data Packet

Make the most of the unencrypted fields



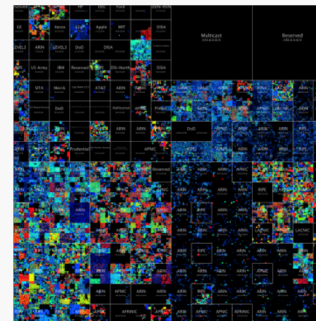
Sequence of Packet Lengths and Times

Identify the content type through the size and timing of packets



Threat Intelligence Map

Who's who of the Internet's dark side



Broad behavioral information about the servers on the Internet.

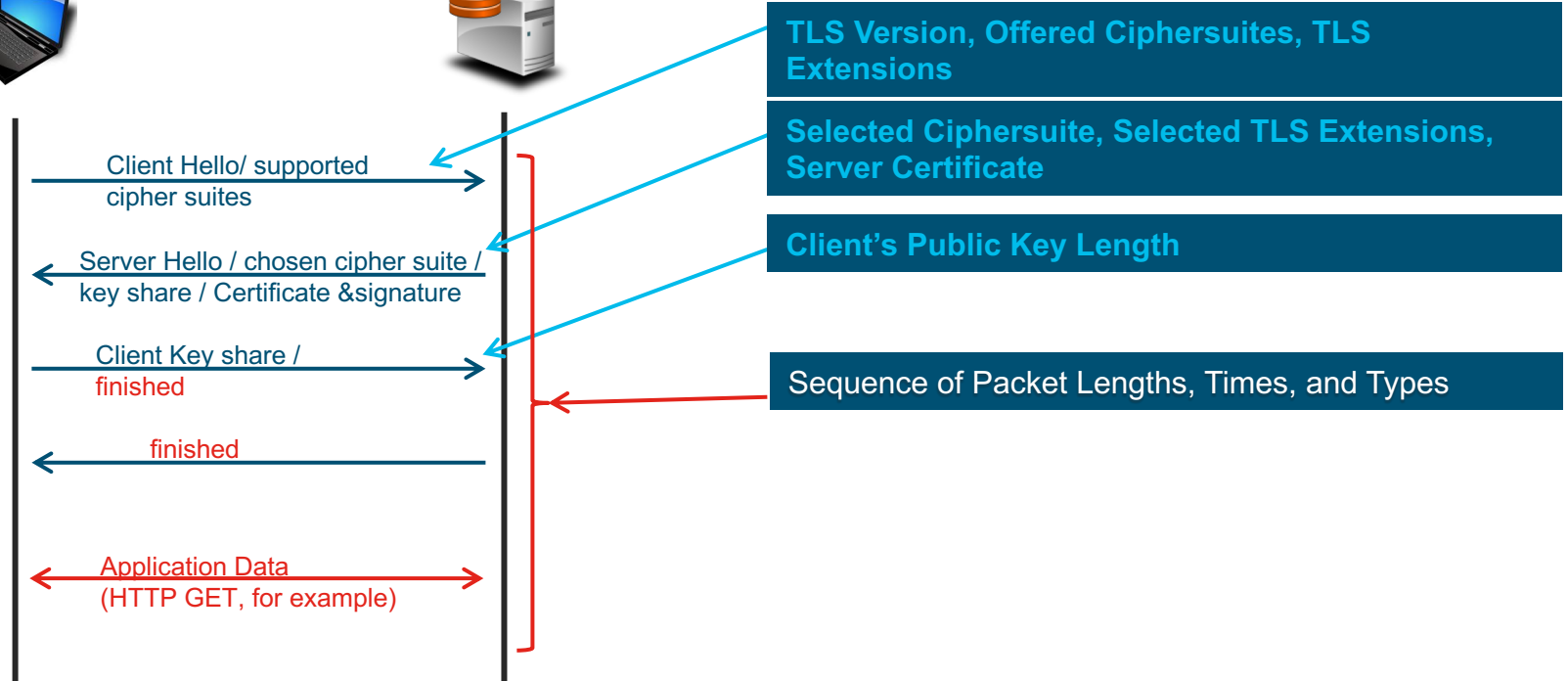


Initial Data Packet, IDP, TLS 1.2

Client

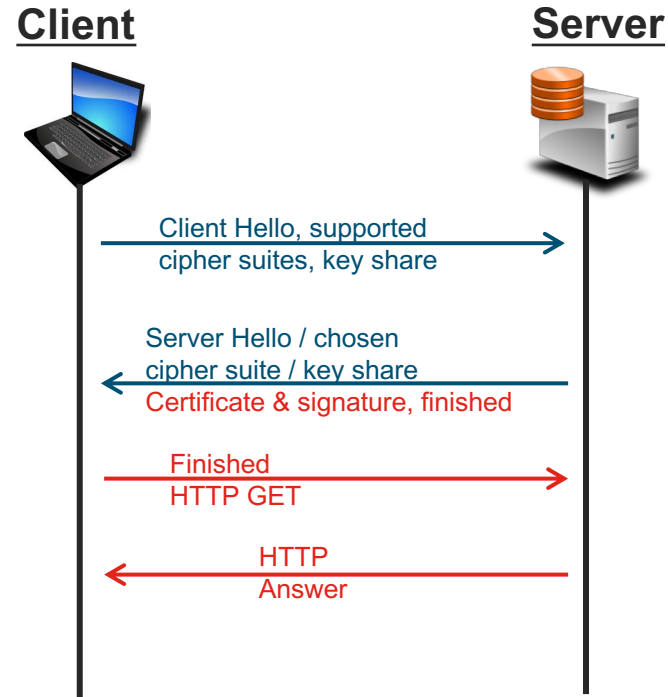


Server



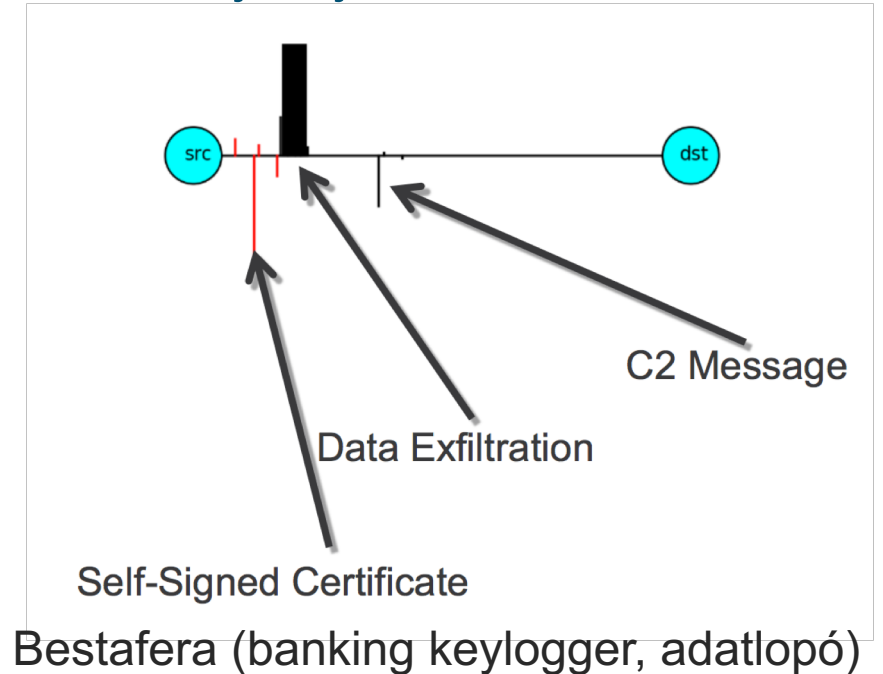
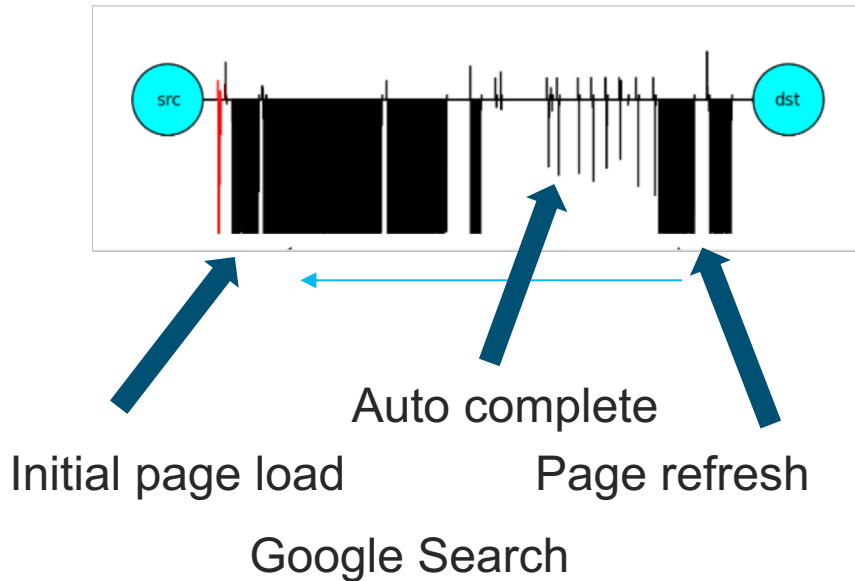
TLS 1.3

- 2018. március 21-én hagyták jóvá
- Számos biztonsági és gyorsítási fejlesztés
 - nem biztonságos régi protokollok, SHA1, DES, MD5, ... elhagyása
 - two-trip helyett one-trip, sőt, zero-trip (emlékszik a kapcsolatra), gyorsabb kapcsolatfelépítés
 - Szerver tanúsítvány is titkosított
- Böngészők elkezdték támogatni (Chrome, Firefox)
- Az ETA (eddig) gond nélkül kezeli
 - A tanúsítvány infó mégis begyűjthető aktív monitorozással és a CTA/GTA adatbázisa tartalmazza, + SPLT



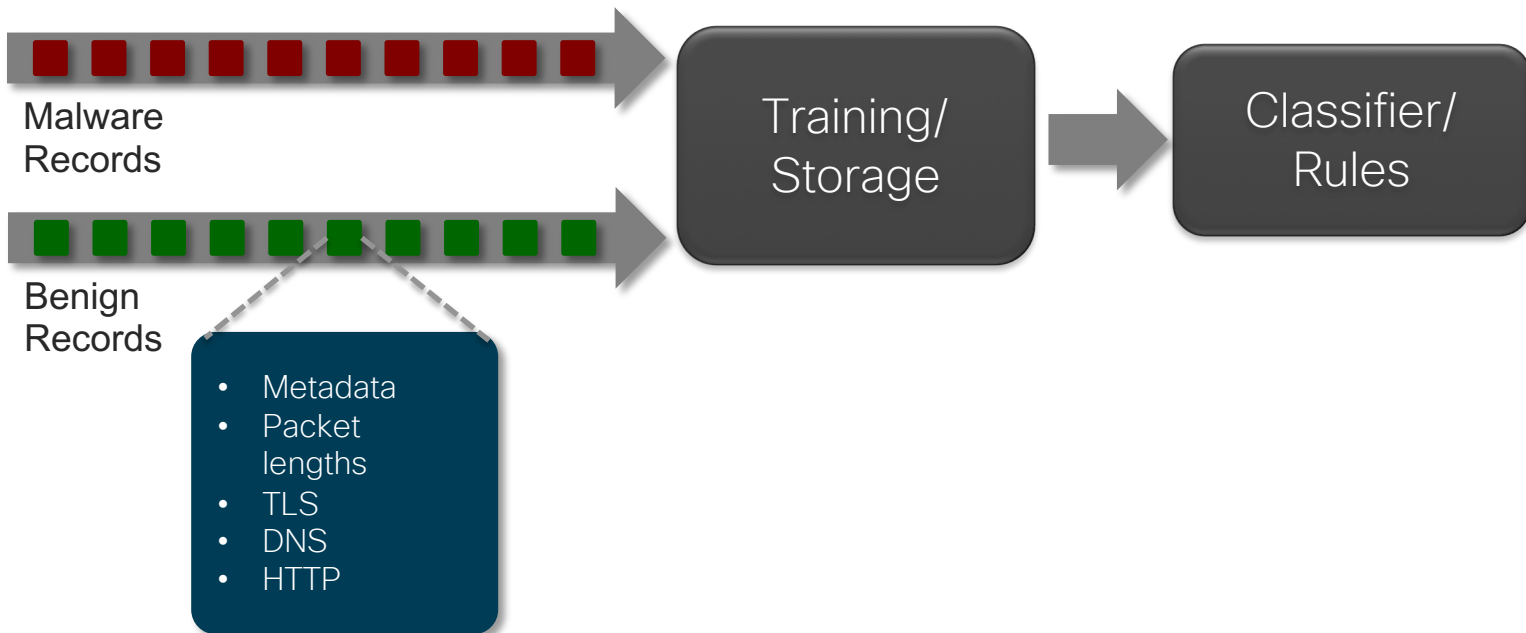
Sequence of Packet Lengths and Times (SPLT)

- Az alkalmazás/felhasználó viselkedési mintáját írja le



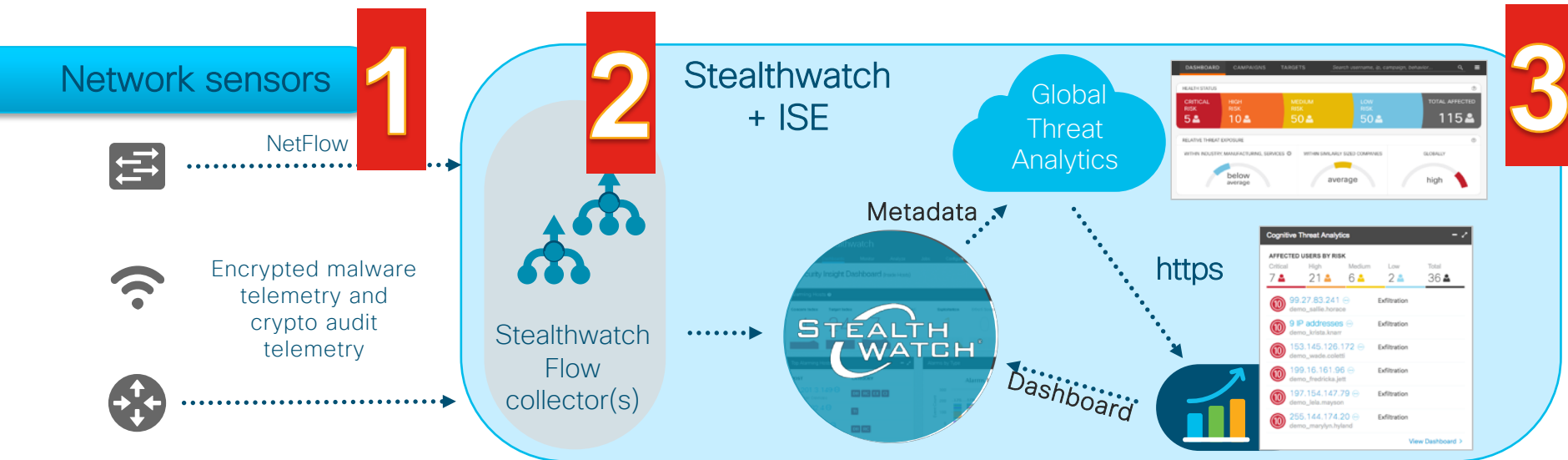
Adatgyűjtés

API, több milliárd flow



<https://github.com/cisco/joy>

Encrypted Traffic Analytics overview



Cisco's unique hardware and software architecture



Enhanced NetFlow with Encrypted Traffic Analytics from Cisco's newest routers and switches



Stealthwatch enhanced analytics and machine learning reduces threat investigation time



Global-to-local knowledge correlation results in higher precision of threat findings

Stealthwatch Enterprise Learning Engines

Stealthwatch “On Box”

- Behavioural Analysis
- Anomaly detection through statistical learning
- **Unsupervised Learning Engine**
- User Defined Behaviour Analysis

Global / Cognitive Analytics

- Cloud Hosted
- **Multi-layer Machine Learning**
- Anomaly detection through statistical learning
- **Supervised Learning Engine**
- Malware classification

HOST	CATEGORY
10.201.3.149 ⓘ	DH RC CI EX
End User Devices	
10.201.3.18 ⓘ	DH RC
End User Devices	
10.201.0.23 ⓘ	DH EX
Terminal Servers	
10.150.1.200 ⓘ	RC DH EX CI
WebHostedApp	
10.10.101.24 ⓘ	EP
End User Devices	

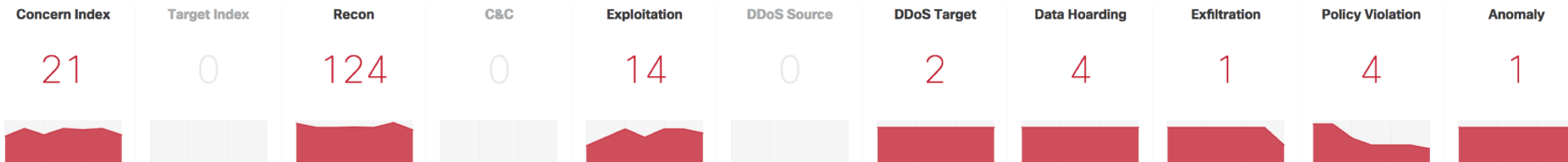
AFFECTED USERS BY RISK			
Critical	High	Medium	Low
1	13	1	1

10	dusti.hilton ⓘ	ENCRYPTED
	Ransomware	
9	10.201.3.40 ⓘ	ENCRYPTED
	Banking trojan	
9	tana.rusin ⓘ	
	Information stealer, Ad injector	
8	10.10.30.16 ⓘ	

Stealthwatch Enterprise

Security Insight Dashboard | Inside Hosts

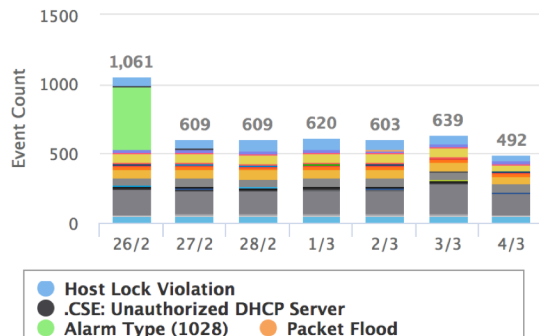
Alarming Hosts ⓘ



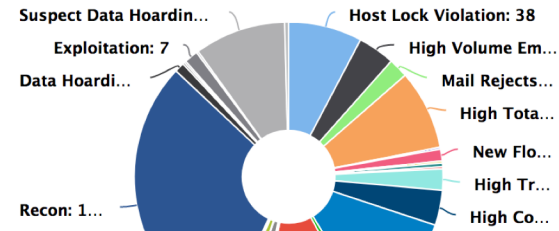
Top Alarming Hosts

HOST	CATEGORY
10.201.3.149	DH RC CI
10.10.30.11	AN
10.201.3.18	DH RC
10.201.0.23	DH
209.182.184.2	RC
10.201.0.15	RC
10.150.1.200	RC DH EX CI

Alarms by Type



Today's Alarms



Titkosítási adatok az összes hálózati kapcsolatban

Stealthwatch

Dashboards Monitor Analyze Jobs Configure Deploy

Flow Search Results (8,196)

Edit Search Time Range: Last 2 Days

Subject: Orientation: Either

100% Complete Delete Search

Save Search Save Results Start New Search

START	DURATION	CONNECTION APPLICATION	CONNECTION BYTES	ENCRYPTION TLS/SSL VERSION	ENCRYPTION KEY EXCHANGE	ENCRYPTION ALGORITHM AND KEY LENGTH	ENCRYPTION AUTHENTICATION ALGORITHM	ENCRYPTION MAC	PEER IP ADDRESS	PEER PORT/PROTOCOL	PEER HOST GROUPS	PEER BYTES
▶ Apr 20, 2017 12:05:48 PM	2m 11s	HTTPS (unclassified)	132.61K	TLS 1.2	RSA	RSA_128	RSA	AES_128_CBC	10.0.40.10	443/TCP	Catch All	92.54K
▶ Apr 20, 2017 11:58:48 AM	6m 11s	HTTPS (unclassified)	309.67K	TLS 1.2	RSA	RSA_128	RSA	AES_128_CBC	10.0.40.10	443/TCP	Catch All	216.14K
▶ Apr 20, 2017 11:48:48 AM	9m 11s	HTTPS (unclassified)	444.16K	TLS 1.2	RSA	RSA_128	RSA	AES_128_CBC	10.0.40.10	443/TCP	Catch All	309.55K
▶ Apr 20, 2017 11:34:48 AM	13m 11s	HTTPS (unclassified)	626.72K	TLS 1.2	RSA	RSA_128	RSA	AES_128_CBC	10.0.40.10	443/TCP	Catch All	437.98K
▶ Apr 20, 2017 11:14:48 AM	19m 11s	HTTPS (unclassified)	871.41K	TLS 1.2	RSA	RSA_128	RSA	AES_128_CBC	10.0.40.10	443/TCP	Catch All	606.05K
▶ Apr 20, 2017 10:46:48 AM	27m 11s	HTTPS (unclassified)	1.21M	TLS 1.2	RSA	RSA_128	RSA	AES_128_CBC	10.0.40.10	443/TCP	Catch All	861.54K
▶ Apr 20, 2017 10:06:48 AM	39m 11s	HTTPS (unclassified)	1.73M	TLS 1.2	RSA	RSA_128	RSA	AES_128_CBC	10.0.40.10	443/TCP	Catch All	1.21M
▶ Apr 20, 2017 9:10:48 AM	55m 11s	HTTPS (unclassified)	2.39M	TLS 1.2	RSA	RSA_128	RSA	AES_128_CBC	10.0.40.10	443/TCP	Catch All	1.67M
▶ Apr 20, 2017 7:51:48 AM	1h 18m 11s	HTTPS (unclassified)	2.85M	TLS 1.2	RSA	RSA_128	RSA	AES_128_CBC	10.0.40.10	443/TCP	Catch All	1.98M
▶ Apr 20, 2017 7:40:12 AM	10m 47s	HTTPS (unclassified)	503.88K	TLS 1.2	RSA	RSA_128	RSA	AES_128_CBC	10.0.40.10	443/TCP	Catch All	351.75K

Encrypted Traffic Analytics

Stealthwatch Domain 1

Security Insight Dashboard (Inside Hosts)

Alerting Hosts (Last 7 Days)

Concerns Index	Target Index	Reason	C & C	Exploitation	DDoS Source	DDoS Target
10	0	1	0	6	2	0

Top Alerting Hosts

HOST	CATEGORY
10.0.12.14 Atlanta Workstations	PF, C, EX, EP
172.18.42.221 Mail Servers	C, RC
192.168.12.185 Mailboxes	EP, DS
172.16.32.2 VoIP Gateways	EP, DS
11.0.12.55 DMZ	EP
10.2.28.20 Atlanta Workstations	EP
10.0.12.14 NAT Gateway	EP

Top Alerting Host Groups

HOST	7 DAY TREND
San Francisco Lorem ipsum dolor sit amet	Credit Data
Workstations Diam quisque erat sed morbi	lorem ipsum
Boston Mauris quis ante at enim cursus mattis	
HR Mauris tempus	
Raleigh	
Servers Suspendisse mattis purus id sapien	

Cognitive Threat Analytics

Critical risk	High risk	Medium risk	Low risk	Total affected
7	20	9	1	37

RISK USER SPECIFIC BEHAVIORS

RISK	USER	SPECIFIC BEHAVIORS
10	haywood.nagel 153.146.126.172	Exfiltration
10	iffny.brent 197.154.147.79	Exfiltration
10	aleen.eisenbarth 199.16.161.98	Exfiltration
10	rackary.beeble 9 IP addresses -	Ransomware, Information stealer, Banking trojan
10	donnie.costats 11 IP addresses -	Malware, Banking trojan

Cognitive Analytics

Cognitive Threat Analytics

AFFECTED USERS BY RISK

Critical	High	Medium	Low
2	7	2	3

- 10 25.186.195.138 Exfiltration
michal.heimann
- 10 107.195.226.254 Exfiltration **ENCRYPTED**
rolanda.torsiello
- 9 192.168.82.25 Banking trojan
- 9 172.29.54.16 Banking trojan
- 9 195.113.166.14 Banking trojan
- 8 192.168.233.32

[View Dashboard >](#)

Expanded CTA Dashboard View

Cognitive Threat Analytics

Health Status

CRITICAL RISK	HIGH RISK	MEDIUM RISK	LOW RISK	TOTAL AFFECTED
5	10	50	50	115

Relative threat exposure

- below average (WITHIN INDUSTRY, MANUFACTURING, SERVICES)
- average (WITHIN SIMILARLY SIZED COMPANIES)
- high (GLOBALLY)

Specific Behaviors

- Exfiltration: 3
- Ransomware: 2
- Banking trojan: 8
- Information stealer: 13
- Trojan: 11
- Spam botnet: 3
- Click fraud: 28
- Exploit kit: 10
- Malware distribution: 3
- Ad injector: 234
- PUA: 643
- Malicious content distribution: 224

Highest Risk

- 10 winnt//usaca1fr5zz 20 IP addresses
Exfiltration today 7 hours
- 8 winnt//usaca1fcd5 192.168.0.12
Banking trojan, Ad injector, PUA, Spam tracking yesterday 17 days
- 7 winnt//usaca1fr5zz 20 IP addresses
Mar 28 3 seconds

Top Risk Escalations

- 10 7 winnt//usaca1f... 20 IP addresses
Ransomware, PUA, Spam tracking v1 Mar 4
- 9 8 192.168.0.64
Exploit kit, Spam tracking v1 today
- 7 6 192.168.0.64
v1 yesterday

Cognitive Threat Analytics

8 hannelore.meuser
201.177.212.19
📅 Dec 9 🕒 28 days

🔴 REOCCURRING

7 malicious http

Oct 28

🟢 REMEDIATED

🔍 INVESTIGATING

Oct 25

8 **7**

4 heavy uploader
📁 dropbox.com

Oct 16

7 **3**

7 anomalous http

Oct 15

8 Information stealer
CDCH01

🖱️ c&c url

Oct 4

3 **5**

3 Spam tracking
CSPM02

Oct 3

5

★ NEW

FTP (uncla...	138B	< 0.01	138B		0B		
ICMP	992B	< 0.01	890B		102B		
Undefined...	549.07KB	< 0.01	548.67KB		408B		
Undefined...	277.39MB	< 0.01	235.45MB		41.94MB		
HTTP (uncl...	620B	< 0.01	144B		476B		
FTP (uncla...	138B	< 0.01	138B		0B		
ICMP	992B	< 0.01	890B		102B		
Undefined...	549.07KB	< 0.01	548.67KB		408B		
Undefined...	277.39MB	< 0.01	235.45MB		41.94MB		
HTTP (uncl...	620B	< 0.01	144B		476B		
FTP (uncla...	138B	< 0.01	138B		0B		
ICMP	992B	< 0.01	890B		102B		



MALWARE

ENCRYPTED

100% confidence, in #CWNC01

★ NEW / TRIAGE ⋮

AFFECTING

dusti.hilton

10.201.3.51 ⋮

OCURRENCE

7 days

Apr 9 - Apr 16

Add notes...

ACTIVITIES AND FLOWS

SEVERITY FILTER: **9** 8 7 6 5 4 3 2 1 Hide related

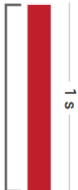
Activities (1 out of 3)

Domains (1 out of 6)

IPs (1 out of 6)

Autonomous systems (1 out of 5)

Time



UPLOAD 1.6 KiB
 DOWNLOAD 1.2 KiB
 REQUESTS 1
 DURATION 1 second
 USER AGENTS 0
 NO REFERRER 100%
 HTTP 0

Client IP, Server IP, URL, SHA

Filter



TYPE	TIMESTAMP	CLIENT	CLIENT F	CLIENT L	SERVER IP	SEF	NETWOI	URL	DUR	PASSIVE DNS HI	CLIEN	CLIEN	SERVI	SERVE
N	Apr 16, 2018 00:06:09 GMT+02:00	10.201.3.51	49476	49481	104.17.41.137	80	TCP		1 s	iuqerfsodp9lfjaposc	1628		712	5

TOR kapcsolatok

4 POSSIBLY UNWANTED APPLICATION TOR **ENCRYPTED** **AFFECTING** **OCCURRENCE**
95% confidence unknown username 2 days
★ NEW / TRIAGE (⋮) 192.168.120.115 (⋮) Dec 4 - today

Add notes...

ACTIVITIES AND FLOWS

SEVERITY FILTER: 9 8 7 6 5 4 3 2 1 **Show related**

showing level 6

Activities (12)

- 6 tor relay
- 6 tor relay
- 6 tor relay
- 6 tor relay
- 6 tor relay

Domains (38)

- 163.172.157.213
- 193.11.114.45
- 193.23.244.244
- *.seul.org (33%)
- 5kqci.com
- bakunin.gtor.org (53%)
- datenspeicher.info2intel.com (100%)
- faravahar.redteam.net (73%)
- gjutcdqsaasawmkn.com
- hiokbyvm.com
- htt4iqh645jsckyfmgl.com
- kd5drxqgx5n3m.com
- longclaw.riseup.net (71%)
- mcfnt36a4yq7gur3sj4t.com
- mvyznz6nxsentd5bsb4wo.com

IPs (20)

- 193.11.114.45
- 128.31.0.34
- 192.187.124.98
- 163.172.157.213
- 178.16.208.57
- 154.35.175.225
- 178.62.197.82
- 193.23.244.244

Autonomous systems (16)

- SUNET SUNET Swedish University Network
- Massachusetts Institute of Technology
- DataShack, LC
- Online S.a.s.
- SITAB Infrastruktur
- Rethem Hosting LLC

Time



Cryptomining!

7

POSSIBLY UNWANTED APPLICATION CRYPTOMINING ENCRYPTED

95% confidence

★ NEW / TRIAGE ⋮

Add notes...

AFFECTING

darrin

3 IP addresses ⋮

OCCURRENCE

6 days

Feb 22 - Feb 27

ACTIVITIES AND FLOWS

SEVERITY FILTER: 9 8 7 6 5 4 3 2 1 Show related

Activities (14 out of 53)

- 7 cryptomining
- 7 persistent cryptomining
- 7 cryptomining
- 7 cryptomining
- 7 cryptomining
- 7 cryptomining
- 7 persistent cryptomining
- 7 persistent cryptomining
- 7 cryptomining
- 7 cryptomining
- 7 cryptomining
- 7 persistent cryptomining
- 7 cryptomining
- 7 cryptomining

Domains (3 out of 59)

- Q AMP *.pool.minergate.com (100%)
- Q AMP xmr.pool.minergate.com (58%)
- Q AMP fcn-xmr.pool.minergate.com (59%)

IPs (10 out of 64)

- Q AMP Q SMC 176.9.47.243
- Q AMP Q SMC 78.46.23.253
- Q AMP Q SMC 94.130.48.154
- Q AMP Q SMC 94.130.64.225
- Q AMP Q SMC 136.243.88.145
- Q AMP Q SMC 136.243.94.27
- Q AMP Q SMC 136.243.102.157
- Q AMP Q SMC 176.9.0.89
- Q AMP Q SMC 138.201.60.198
- Q AMP Q SMC 138.201.124.177

Autonomous systems (1 out of 30)

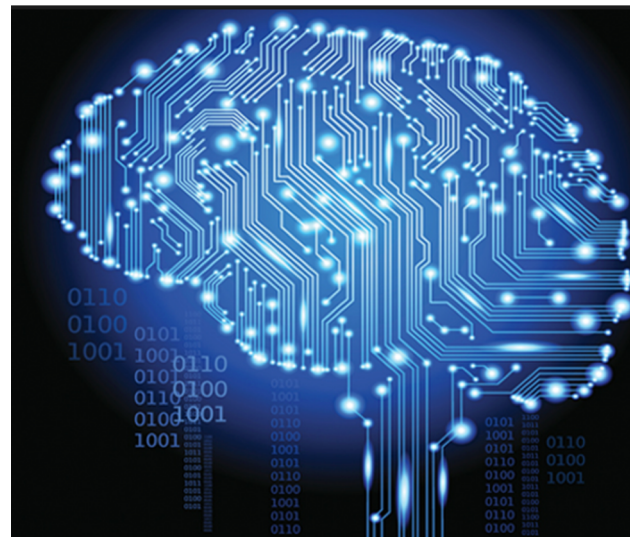
Hetzner Online GmbH

Time



Az MI segíthet

- A kiberbűnözők nem fognak morális kérdést csinálni az MI-ből
- Csak "emberi erőforrással" nem lehet lépést tartani a nagyszámú malware áradattal
- MI-val hatékonyabb felderítés, megelőzés lehetséges
 - malware file felismerés, DNS forgalom,
 - titkosított forgalomban,
 - HTTP logok, NetFlow információk feldolgozása
- Új megközelítéseket is adhat (DeepMind go példa)



Köszönöm

