The state of cybersecurity in 2019

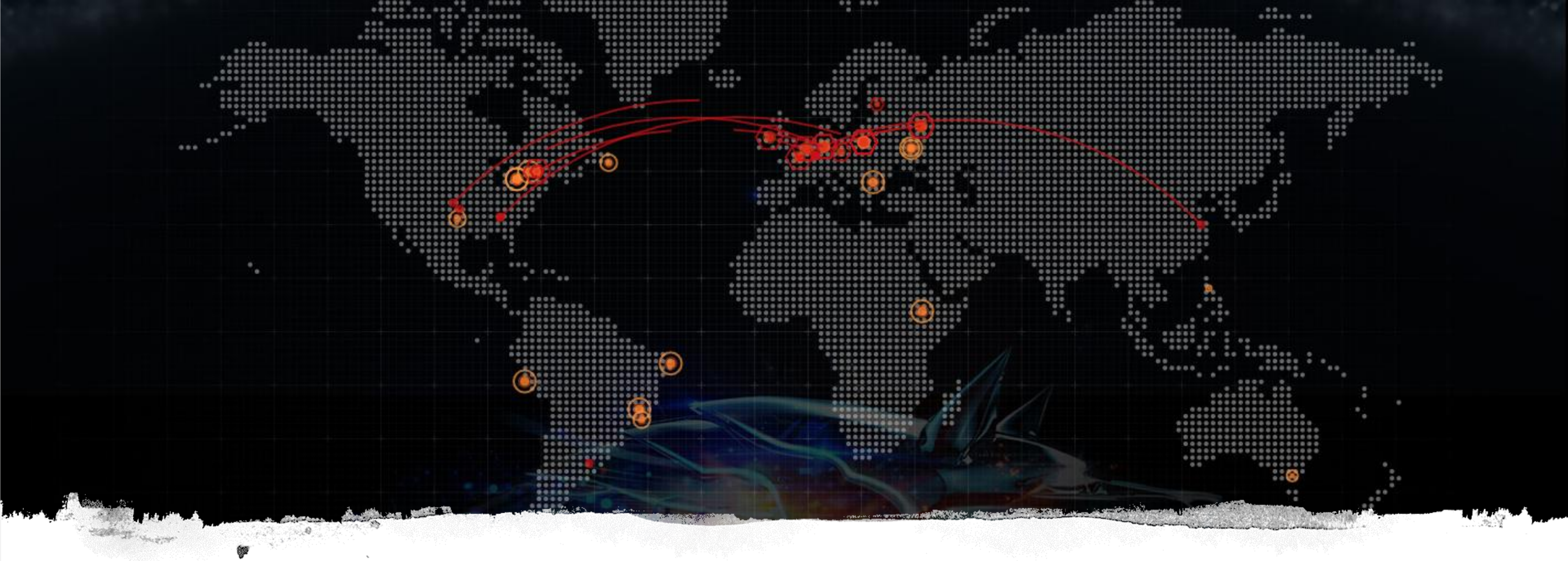
Bitdefender

The state of cybersecurity in 2019

Your Host

Alex “Jay” Bălan
Chief Security Researcher - Bitdefender

Presentation Time:
This presentation should take around 25 - 30min.



Bitdefender at a glance

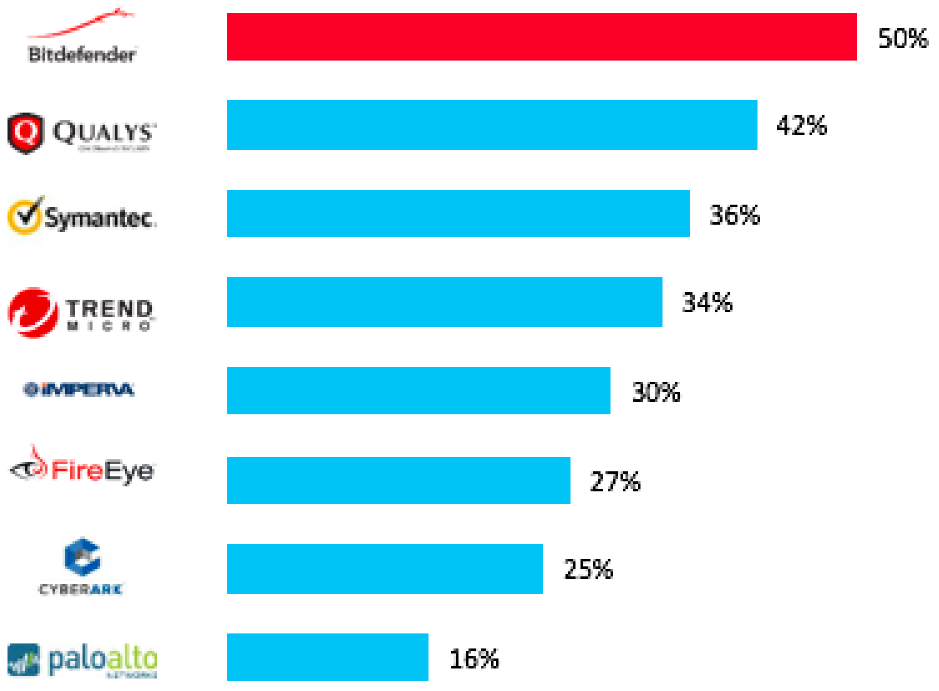
- Founded in 2001
- Privately held, **HQ** in Romania
- **Enterprise HQ** in Santa Clara, USA
- **Consumer HQ** in Bucharest, RO
- **1300+** staff globally
- **650+** developers and engineers, emphasis on machine learning and artificial intelligence
- Offices in 9 Countries. 24 country partners & over 5,000 VARs & 2,000 MSP's
- Protecting over **500 Million** users

Innovation-led culture instilled by Tech-focused management team

Unrivalled track record of developing industry firsts

2001	Intelligent Update & Firewall
2002	Spam Image filter
2005	Rescue Mode
2009	Security for Virtualized Environments (SVE)
2011	GravityZone Architecture
2013	Memory introspection
2014	HVI inject
2015	Box v.1
2017	Hypervisor introspection

Bitdefender has highest percentage of R&D staff[1]



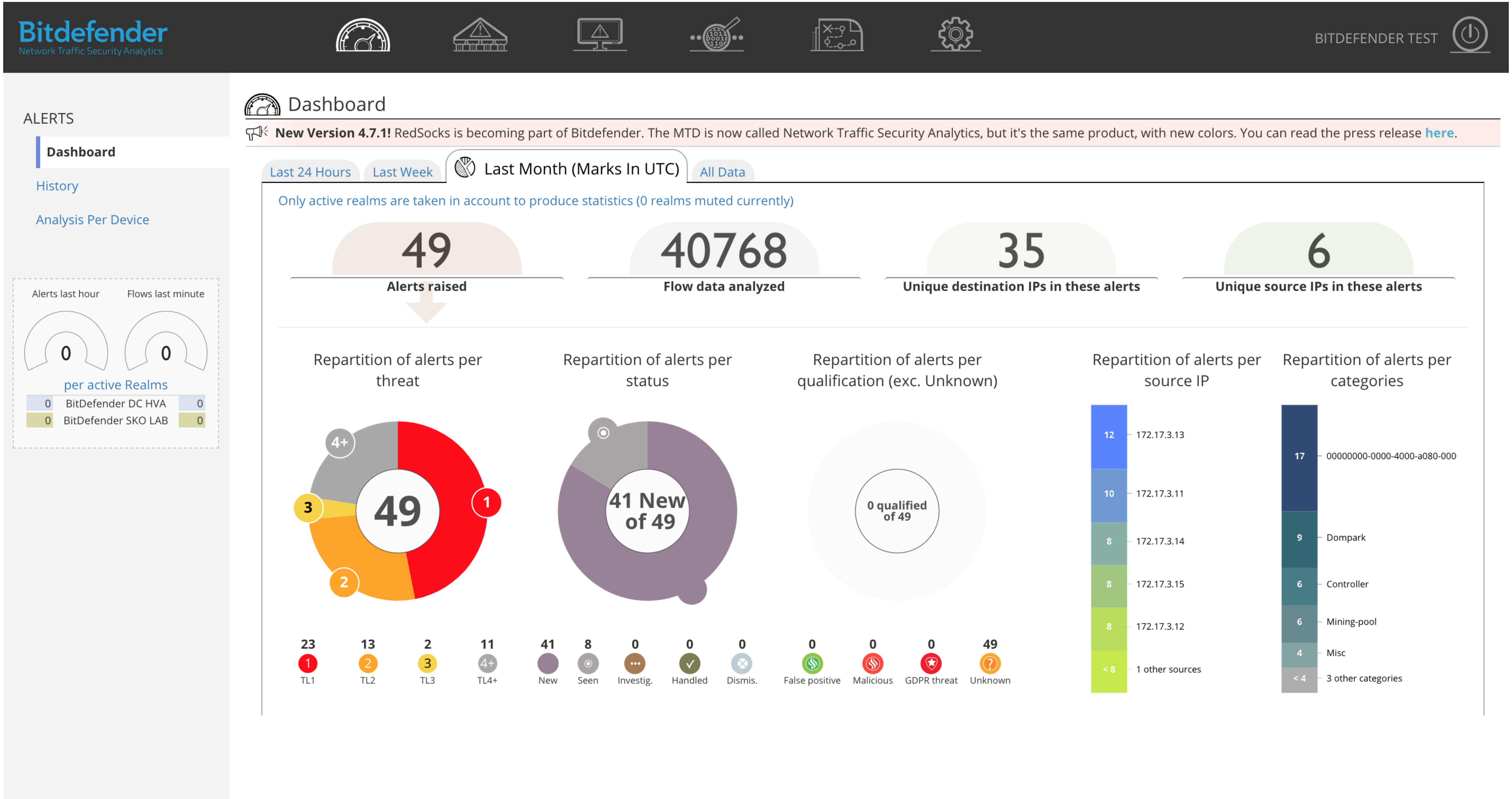
15+ Years of innovation

€89m R&D spent 2014-17E

48 patents and **28** pending

Heaven for R&D talent

Latest addition to Bitdefender’s product portfolio: NTSA



Bitdefender
Network Traffic Security Analytics

BITDEFENDER TEST

ALERTS

Dashboard

History

Analysis Per Device

Alerts last hour 0

Flows last minute 0

per active Realms

0	BitDefender DC HVA	0
0	BitDefender SKO LAB	0

Dashboard

New Version 4.7.1! RedSocks is becoming part of Bitdefender. The MTD is now called Network Traffic Security Analytics, but it's the same product, with new colors. You can read the press release here.

Last 24 Hours | Last Week | Last Month (Marks In UTC) | All Data

Only active realms are taken in account to produce statistics (0 realms muted currently)

49 Alerts raised

40768 Flow data analyzed

35 Unique destination IPs in these alerts

6 Unique source IPs in these alerts

Repartition of alerts per threat

49

23	13	2	11
TL1	TL2	TL3	TL4+

Repartition of alerts per status

41 New of 49

41	8	0	0	0
New	Seen	Investig.	Handled	Dismis.

Repartition of alerts per qualification (exc. Unknown)

0 qualified of 49

0	0	0	49
False positive	Malicious	GDPR threat	Unknown

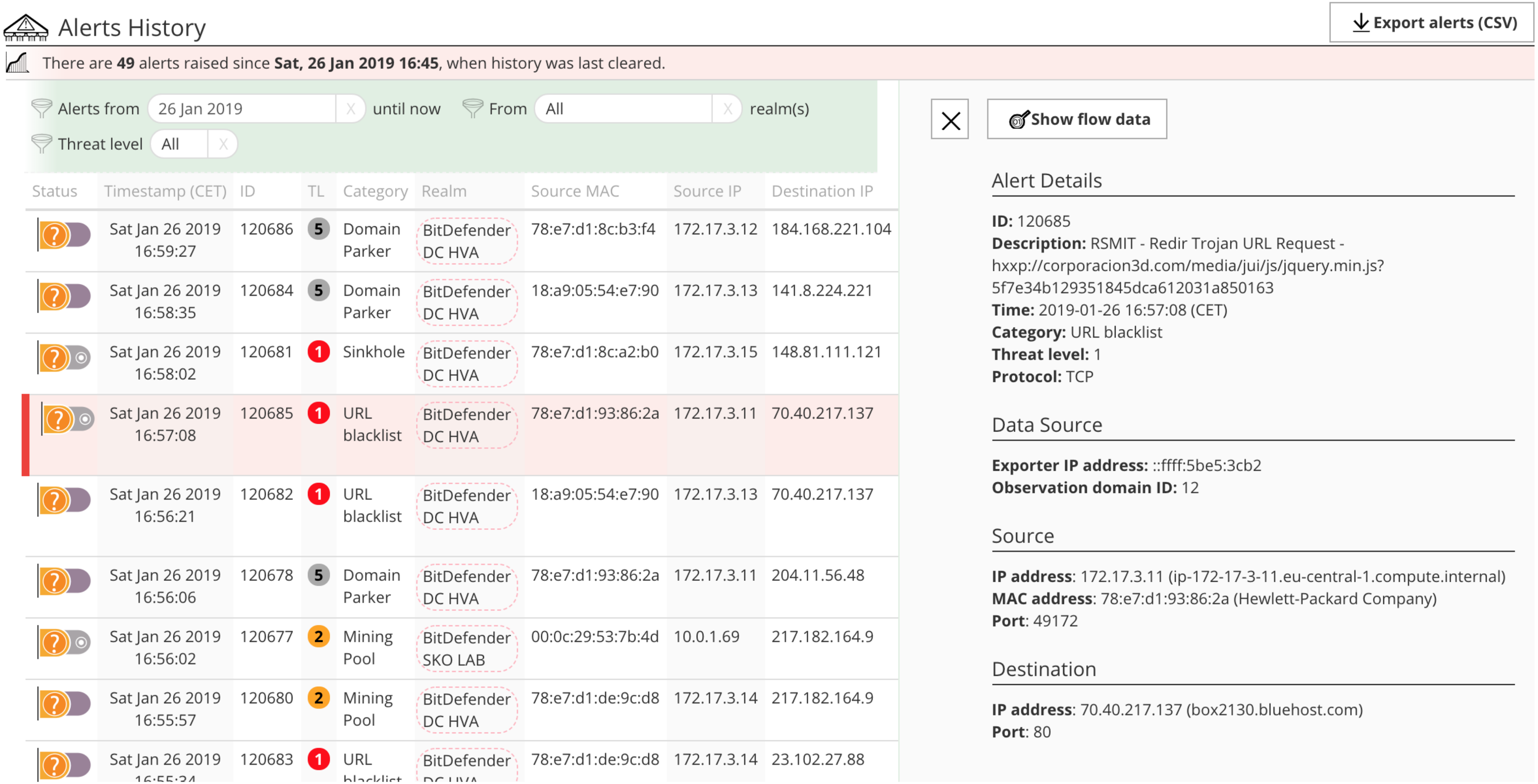
Repartition of alerts per source IP

12	172.17.3.13
10	172.17.3.11
8	172.17.3.14
8	172.17.3.15
8	172.17.3.12
< 8	1 other sources

Repartition of alerts per categories

17	00000000-0000-4000-a080-000
9	Dompark
6	Controller
6	Mining-pool
4	Misc
< 4	3 other categories

Latest addition to Bitdefender's product portfolio: NTSA



Alerts History

There are **49** alerts raised since **Sat, 26 Jan 2019 16:45**, when history was last cleared.

Alerts from 26 Jan 2019 until now From All realm(s)

Threat level All

Status	Timestamp (CET)	ID	TL	Category	Realm	Source MAC	Source IP	Destination IP
?	Sat Jan 26 2019 16:59:27	120686	5	Domain Parker	BitDefender DC HVA	78:e7:d1:8c:b3:f4	172.17.3.12	184.168.221.104
?	Sat Jan 26 2019 16:58:35	120684	5	Domain Parker	BitDefender DC HVA	18:a9:05:54:e7:90	172.17.3.13	141.8.224.221
?	Sat Jan 26 2019 16:58:02	120681	1	Sinkhole	BitDefender DC HVA	78:e7:d1:8c:a2:b0	172.17.3.15	148.81.111.121
?	Sat Jan 26 2019 16:57:08	120685	1	URL blacklist	BitDefender DC HVA	78:e7:d1:93:86:2a	172.17.3.11	70.40.217.137
?	Sat Jan 26 2019 16:56:21	120682	1	URL blacklist	BitDefender DC HVA	18:a9:05:54:e7:90	172.17.3.13	70.40.217.137
?	Sat Jan 26 2019 16:56:06	120678	5	Domain Parker	BitDefender DC HVA	78:e7:d1:93:86:2a	172.17.3.11	204.11.56.48
?	Sat Jan 26 2019 16:56:02	120677	2	Mining Pool	BitDefender SKO LAB	00:0c:29:53:7b:4d	10.0.1.69	217.182.164.9
?	Sat Jan 26 2019 16:55:57	120680	2	Mining Pool	BitDefender DC HVA	78:e7:d1:de:9c:d8	172.17.3.14	217.182.164.9
?	Sat Jan 26 2019 16:55:34	120683	1	URL blacklist	BitDefender DC HVA	78:e7:d1:de:9c:d8	172.17.3.14	23.102.27.88

Alert Details

ID: 120685
Description: RSMIT - Redir Trojan URL Request - hxxp://corporacion3d.com/media/jui/js/jquery.min.js?5f7e34b129351845dca612031a850163
Time: 2019-01-26 16:57:08 (CET)
Category: URL blacklist
Threat level: 1
Protocol: TCP

Data Source

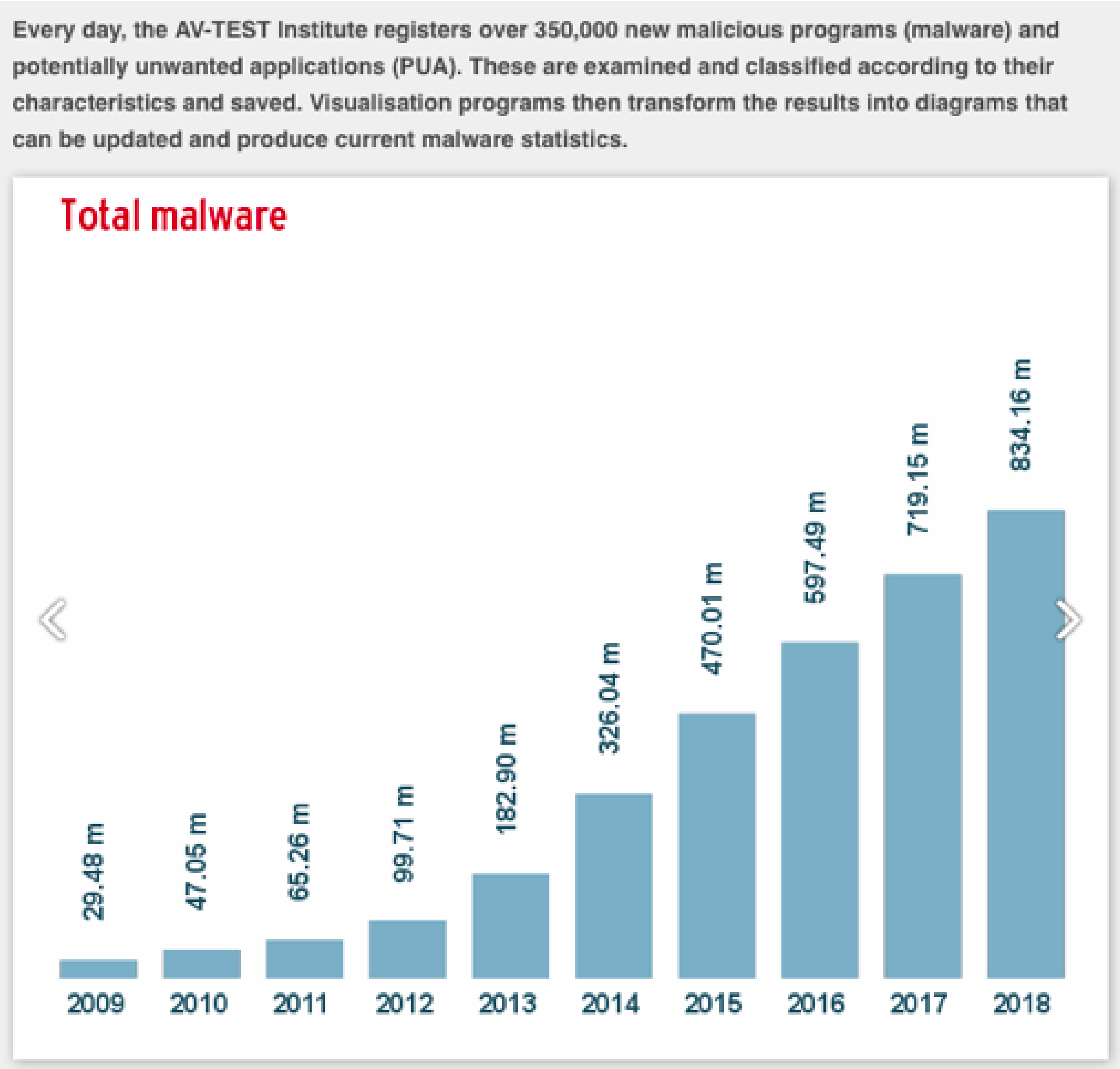
Exporter IP address: ::ffff:5be5:3cb2
Observation domain ID: 12

Source

IP address: 172.17.3.11 (ip-172-17-3-11.eu-central-1.compute.internal)
MAC address: 78:e7:d1:93:86:2a (Hewlett-Packard Company)
Port: 49172

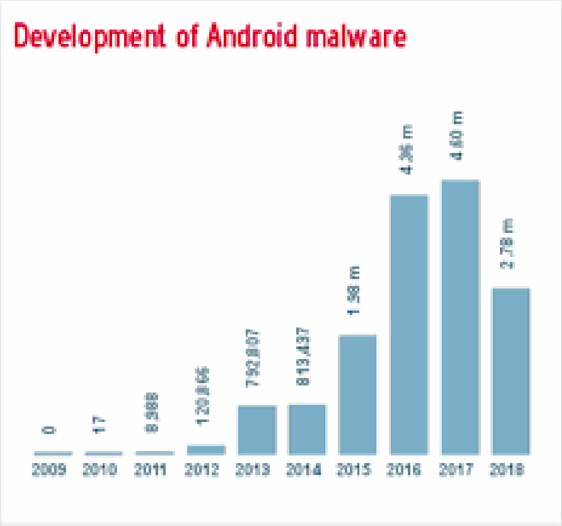
Destination

IP address: 70.40.217.137 (box2130.bluehost.com)
Port: 80

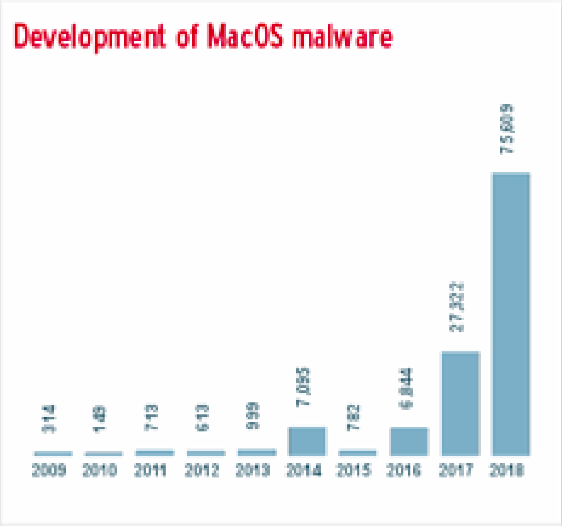


Every day, the AV-TEST Institute registers over 350,000 new malicious programs (malware) and potentially unwanted applications (PUA). These are examined and classified according to their characteristics and saved. Visualisation programs then transform the results into diagrams that can be updated and produce current malware statistics.

Total malware

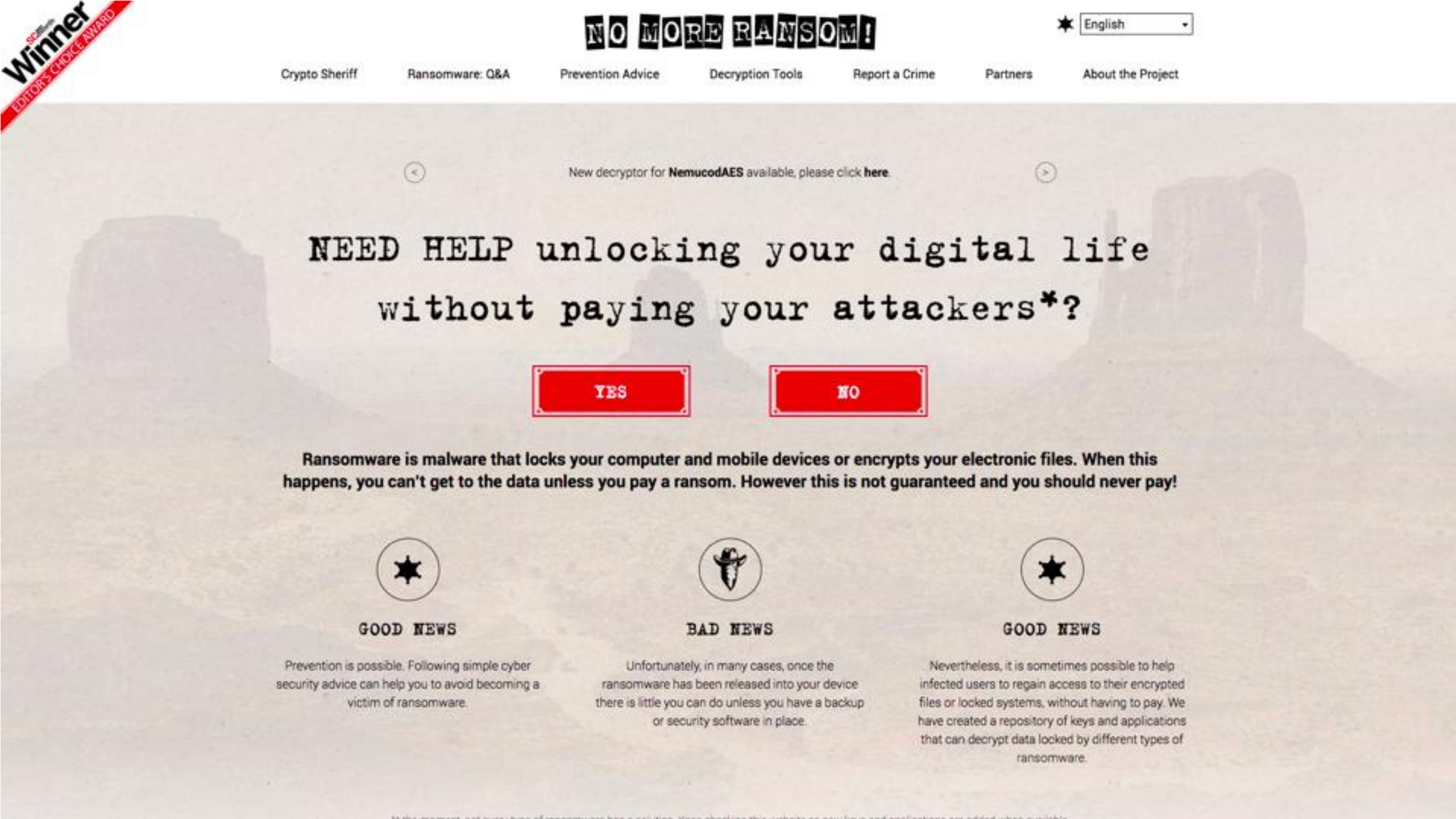


Development of Android malware



Development of MacOS malware

RANSOMWARE
RANSOMWARE
RANSOMWARE



New decryptor for **NemucodAES** available, please click **here**.

NEED HELP unlocking your digital life without paying your attackers*?

Ransomware is malware that locks your computer and mobile devices or encrypts your electronic files. When this happens, you can't get to the data unless you pay a ransom. However this is not guaranteed and you should never pay!

GOOD NEWS

Prevention is possible. Following simple cyber security advice can help you to avoid becoming a victim of ransomware.

BAD NEWS

Unfortunately, in many cases, once the ransomware has been released into your device there is little you can do unless you have a backup or security software in place.

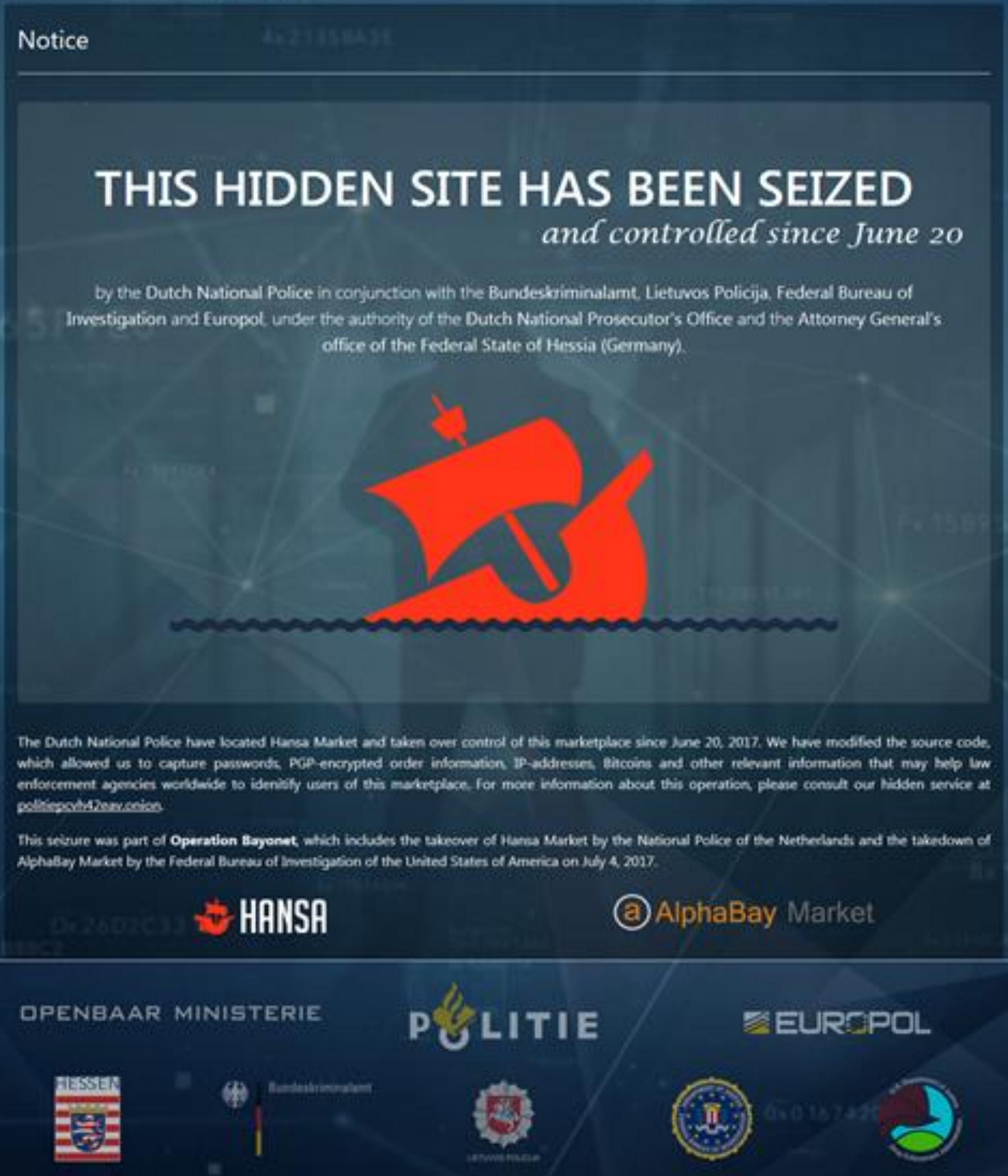
GOOD NEWS

Nevertheless, it is sometimes possible to help infected users to regain access to their encrypted files or locked systems, without having to pay. We have created a repository of keys and applications that can decrypt data locked by different types of ransomware.

At the moment, not every type of ransomware has a solution. Keep checking this website as new keys and applications are added when available.

Dark Net
Hidden Services
ToR
Malware as a Service
CryptoCurrency
Remote Access Trojan
Online Drugs
Firearms
Grenades
Pornography
Escrow Services

BotNets
Ransomware
Hacking Services
DDoS Services
Anonymity
Encryption
Criminals
Burners
MONEY



Notice

THIS HIDDEN SITE HAS BEEN SEIZED

and controlled since June 20

by the **Dutch National Police** in conjunction with the **Bundeskriminalamt**, **Lietuvos Policija**, **Federal Bureau of Investigation** and **Europol**, under the authority of the **Dutch National Prosecutor's Office** and the **Attorney General's office of the Federal State of Hessia (Germany)**.

The Dutch National Police have located Hansa Market and taken over control of this marketplace since June 20, 2017. We have modified the source code, which allowed us to capture passwords, PGP-encrypted order information, IP-addresses, Bitcoins and other relevant information that may help law enforcement agencies worldwide to idenitify users of this marketplace. For more information about this operation, please consult our hidden service at politiepcvh42eav.onion.

This seizure was part of **Operation Bayonet**, which includes the takeover of Hansa Market by the National Police of the Netherlands and the takedown of AlphaBay Market by the Federal Bureau of Investigation of the United States of America on July 4, 2017.

The Internet of Threats

Breaking into a household 101

…the old way

- Break into WiFi | sniff traffic | break into laptop/phone/table | profit
- Plant malware into laptop/tablet/phone | profit
- Hijack upstream connections (after router) | break into laptop/tablet/phone | profit

A somewhat limited attack surface

Logitech Harmony Elite: Home Controller

Deeper: Smart portable fish finder

Philips Hue Go: Portable connected lighting

Norm: Connected thermostat

Use Norm to tailor your home's temperature exactly to your liking and control your climate from anywhere. It offers intelligence, convenience, and efficiency, so don't just call it a thermostat—Norm is your home's sixth sense.

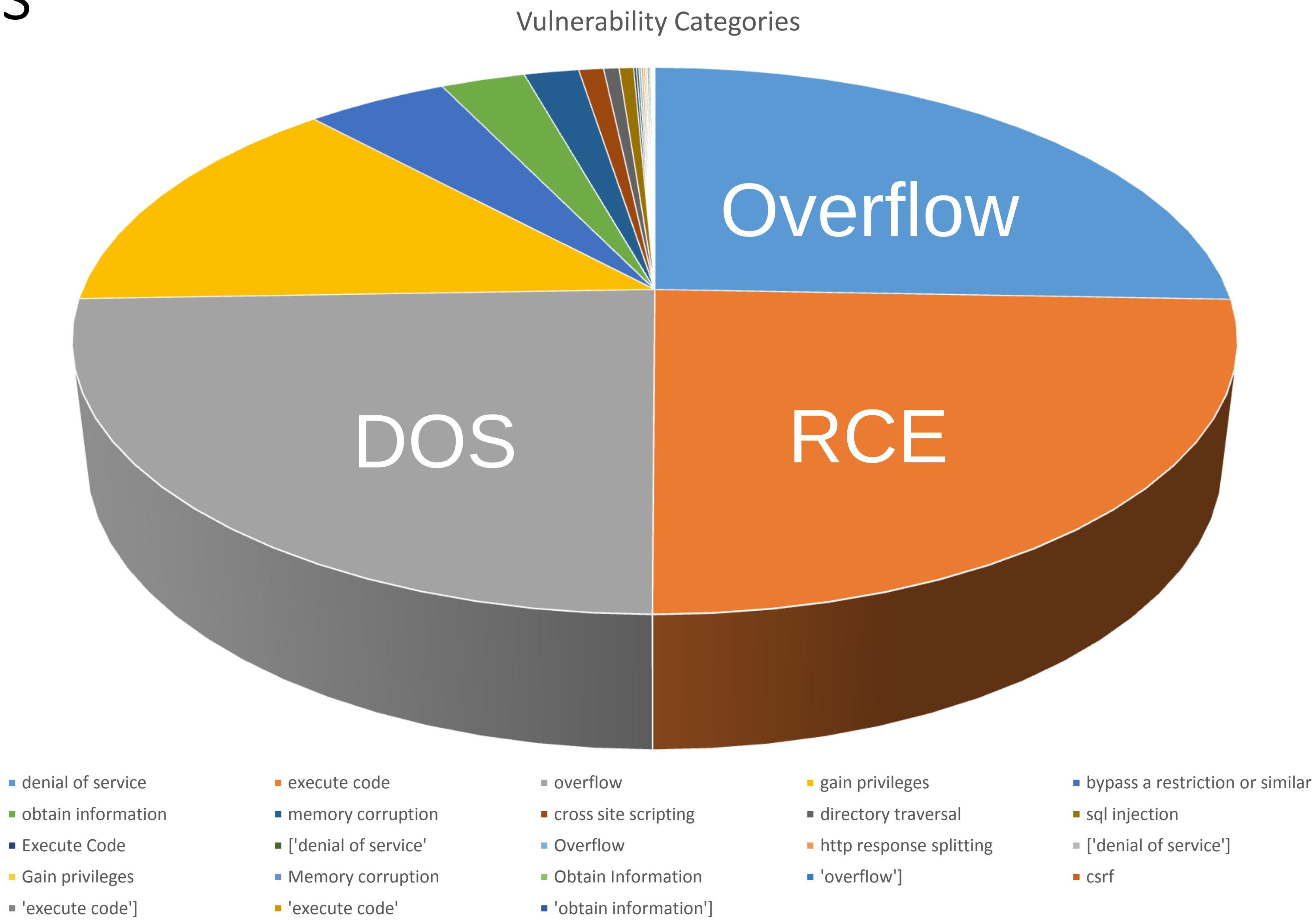
SmartMat: Intelligent yoga mat

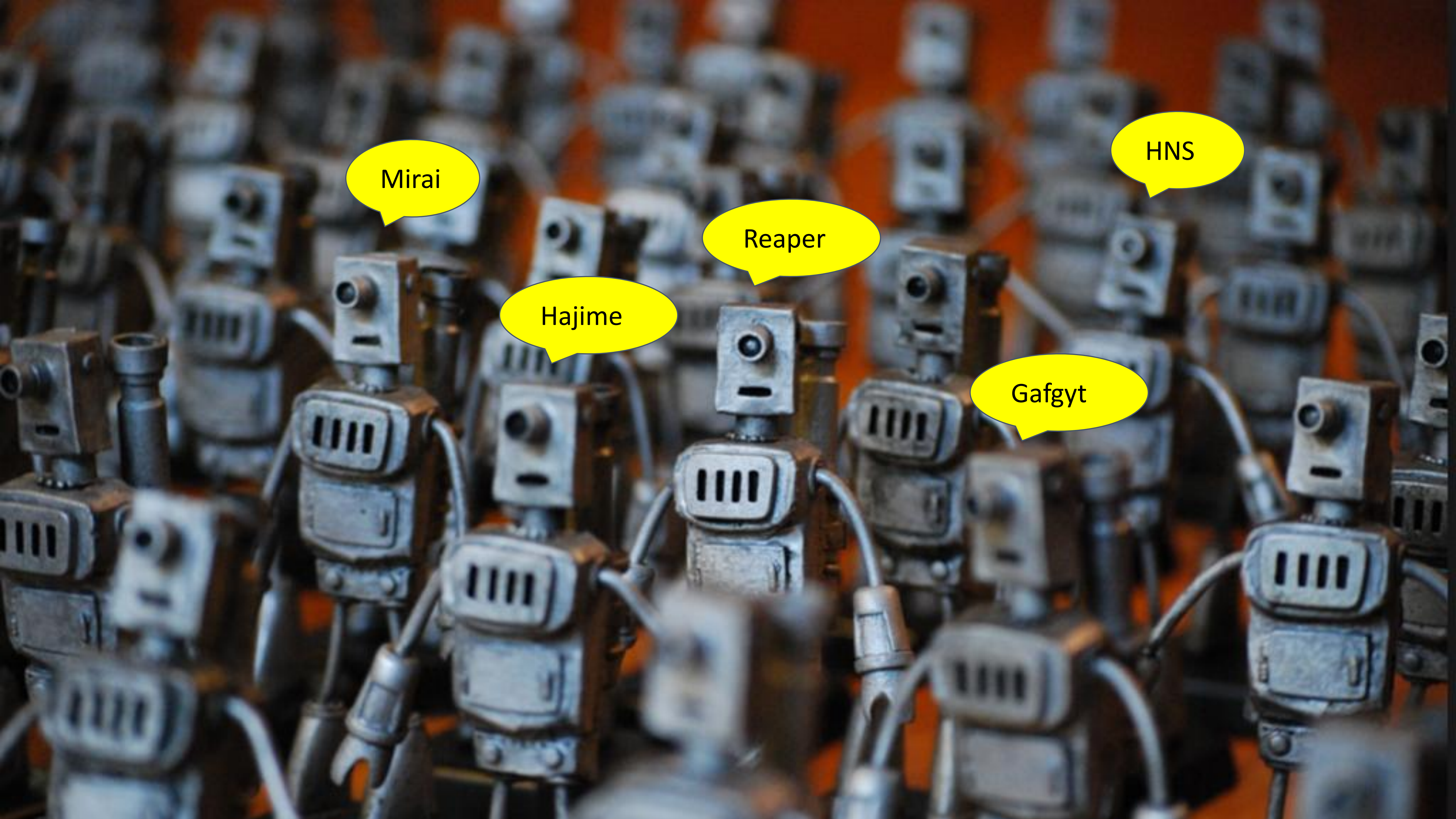
Netatmo Welcome: Smart camera with face recognition

OpenSprinkler: Automate your sprinklers

August: Smart lock

Findings


Vulnerability Categories
Overflow
DOS
RCE
denial of service
execute code
overflow
gain privileges
bypass a restriction or similar
obtain information
memory corruption
cross site scripting
directory traversal
sql injection
Execute Code
['denial of service'
Overflow
http response splitting
['denial of service']
Gain privileges
Memory corruption
Obtain Information
'overflow']
csrf
'execute code']
'execute code'
'obtain information']



Mirai
HNS
Reaper
Hajime
Gafgyt

Ask us anything :)

abalan@bitdefender.com & @jaymzu
acosoi@bitdefender.com & @catalincosoi

PROTECTING **500 MILLION USERS** WORLWIDE