



State of Security 2018

quick recap of the most interesting events



Bitdefender®



INTERPOL



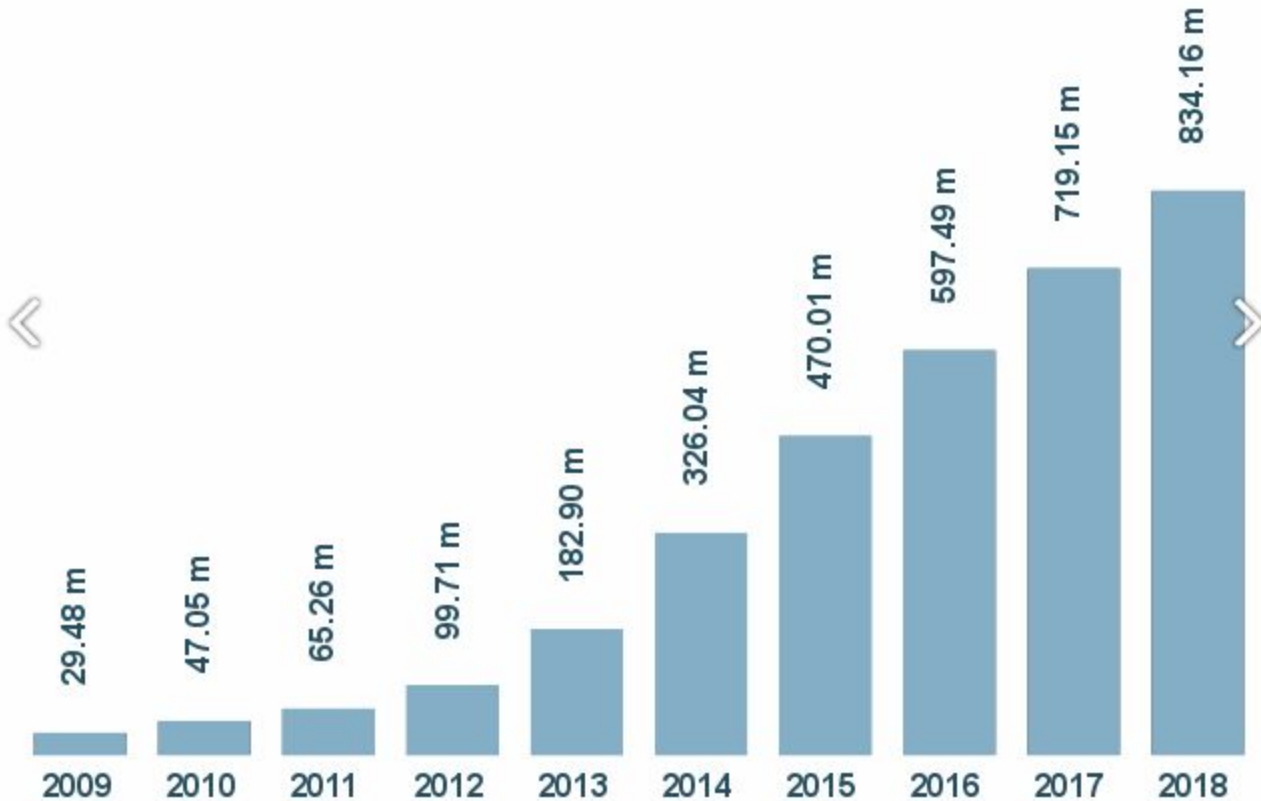
COUNCIL OF EUROPE



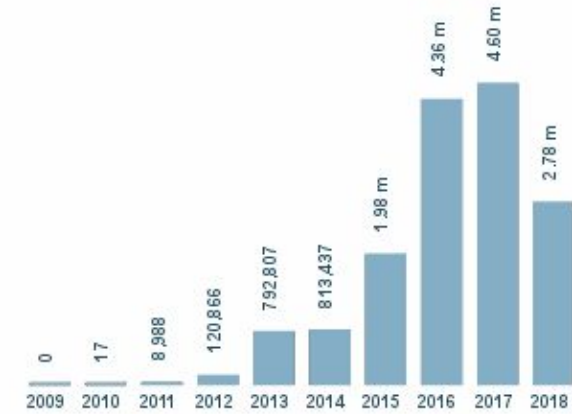
CONSEIL DE L'EUROPE

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.

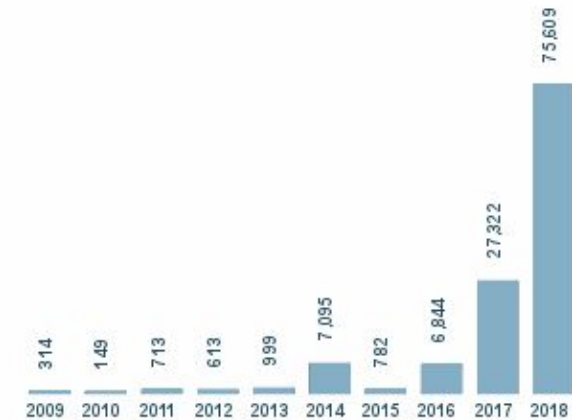
Total malware



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*?

YES

NO

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.

CobaltStrike

The screenshot shows the CobaltStrike interface with a network diagram and a terminal window. The network diagram illustrates a flow from an external IP (172.16.14.1) through a host (whatta.hogg COPPER @ 2680) to a host (whatta.hogg GRANITE @ 4380), which then connects to a SYSTEM * COPPER @ 4284, and finally to a SYSTEM * DC @ 1752.

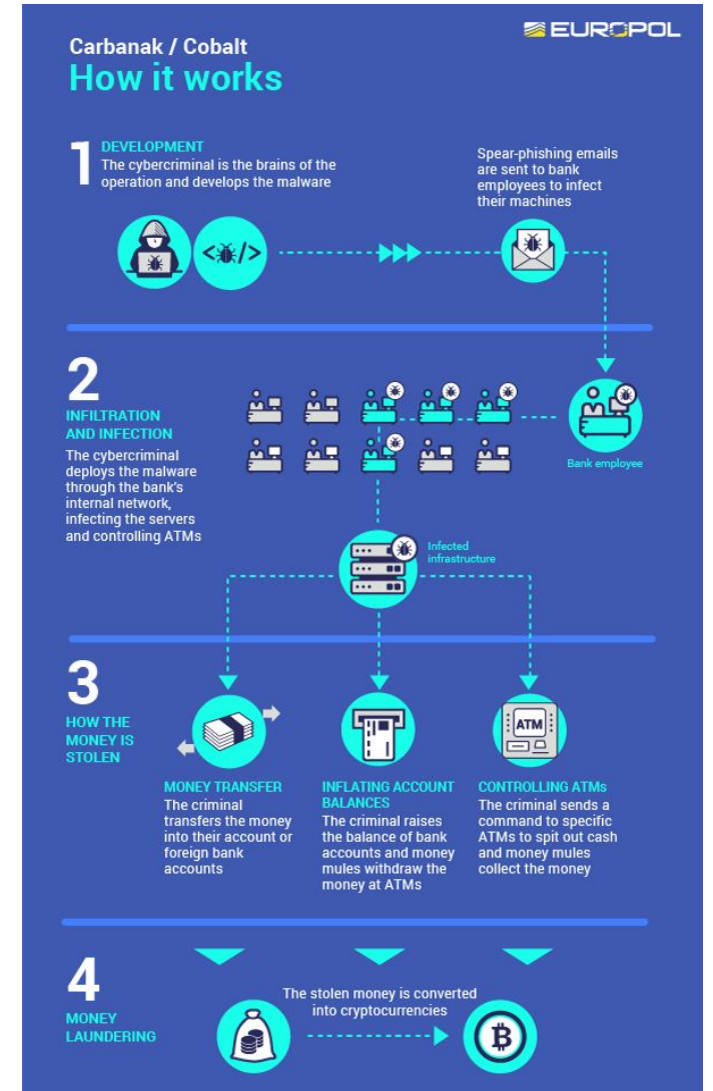
The terminal window displays the following output:


```
[+] received output:
List of hosts:

Server Name      IP Address      Platform  Version  Type      Comment
-----
COPPER           172.16.20.81   500      10.0     -
DC               172.16.20.3    500      6.1      PDC      Domain Controller
GRANITE          172.16.20.80   500      6.1      -

beacon> psexec_psh COPPER local - beacon smb
[*] Tasked beacon to run windows/beacon_smb/bind_pipe (\\COPPER\pipe\status_9977) on COPPER via Service Control Manager (PSH)
[+] host called home, sent: 5765 bytes
[+] received output:
Started service 2b66a4c on COPPER
[+] host called home, sent: 190063 bytes
[+] established link to child beacon: 172.16.20.81

[GRANITE] whatta.hogg */5944                                     last: 11s
beacon>
```





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

THIS HIDDEN SITE HAS BEEN SEIZED

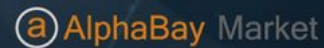
and controlled since June 20

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 Hessa (Germany).



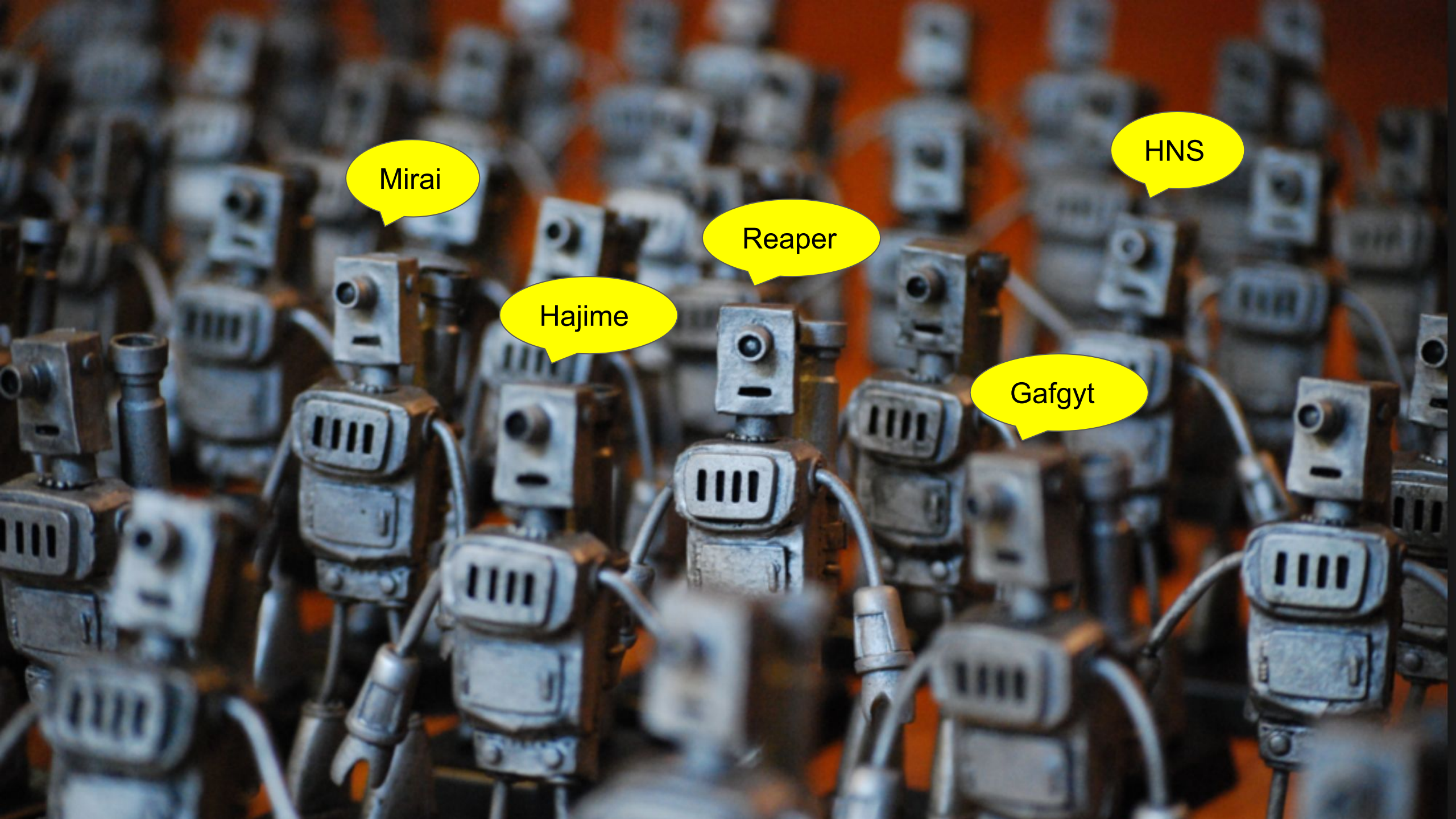
The Dutch National Police have located Hansa Market and taken over control of this marketplace since June 20, 2017. We have modified the source code, which allowed us to capture passwords, PGP-encrypted order information, IP-addresses, Bitcoins and other relevant information that may help law enforcement agencies worldwide to identify 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.



OPENBAAR MINISTERIE





Mirai

HNS

Reaper

Hajime

Gafgyt



B

PROTECTING 500 MILLION USERS WORLDWIDE