



UNCOVERING THE WORLD'S MOST SOPHISTICATED CYBER THREATS

CYBERTINEL. SIGNATURE-LESS ENDPOINT SECURITY PLATFORM

www.CYBERTINEL.com

CYBERTINEL - Technology and Company

- APT's and Zero day attack solution
- Company founded in 2012 after 4 years of research
- First commercial version launched in Q4 2012
- The solution is actively defending hundreds of thousands endpoints worldwide



Business Partners



Clients



Telefonica



JR / DUTY FREE
SHOPPING WORTH TRAVELING FOR



BrightSource

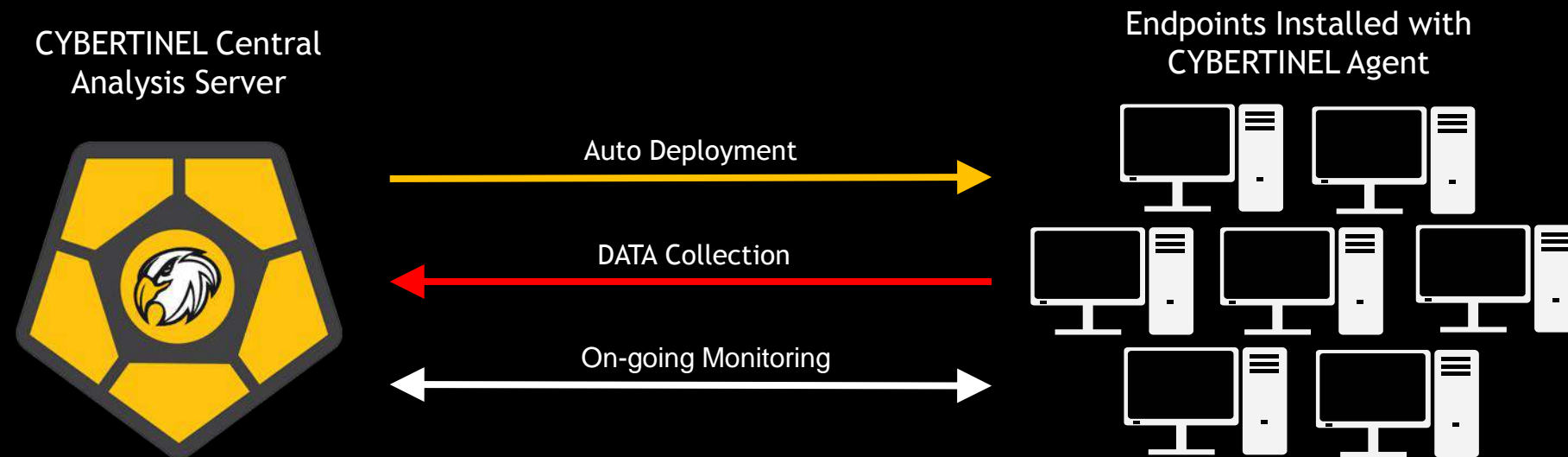


aeris
CAPITAL



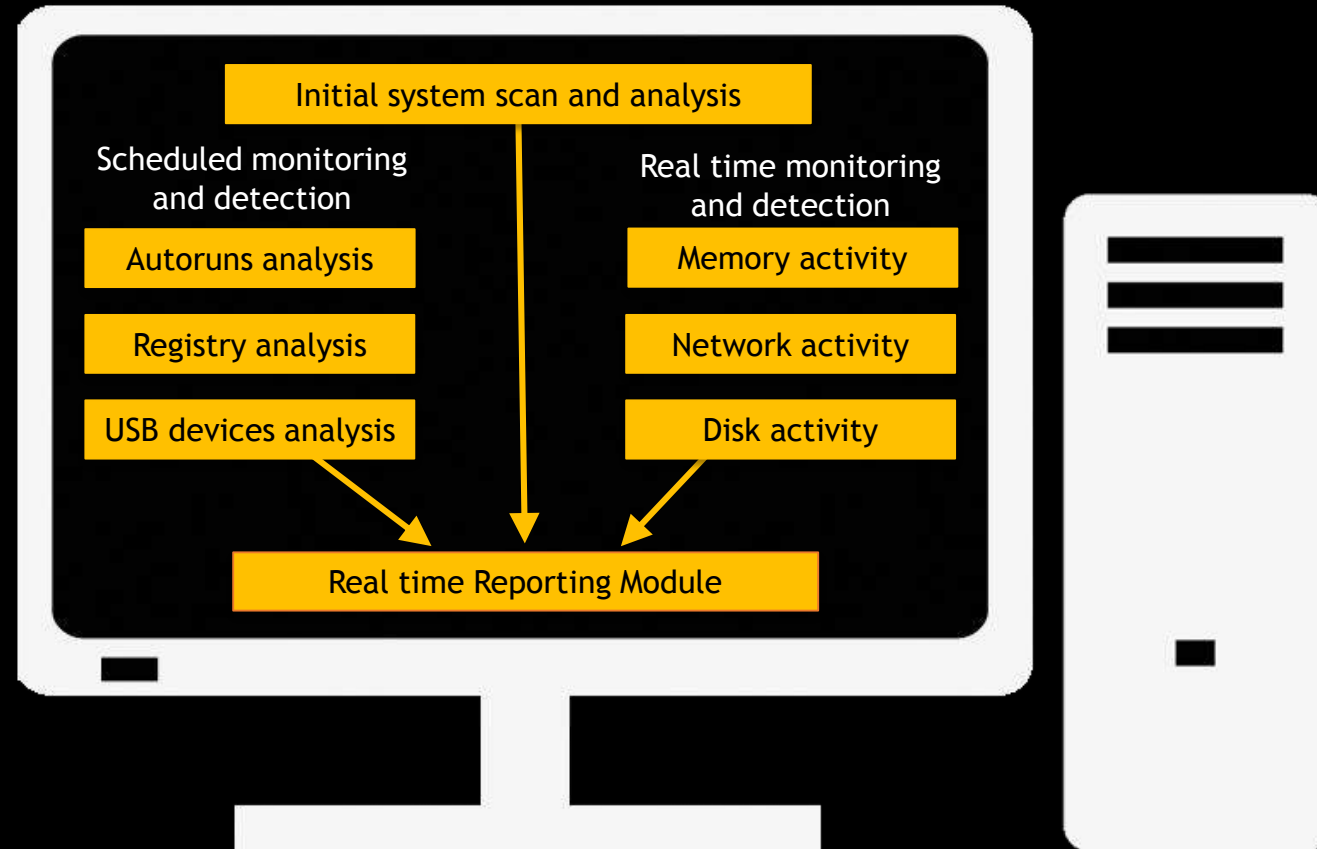
CYBERTINEL - Anti Cyber Threat Infrastructure

System Schematic



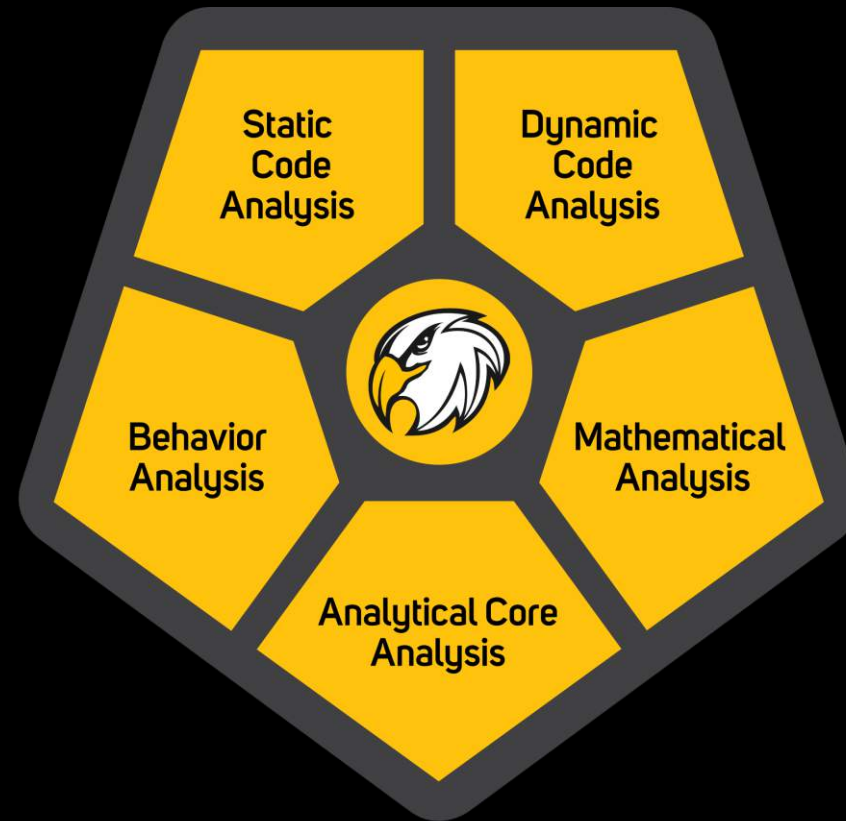
CYBERTINEL - Anti Cyber Threat Infrastructure

Endpoint Agent



CYBERTINEL - Anti Cyber Threat Infrastructure

CYBERTINEL Central Analysis Server - 5 powerful engines working in parallel



CYBERTINEL - Anti Cyber Threat Infrastructure

Static Code Analysis Engine

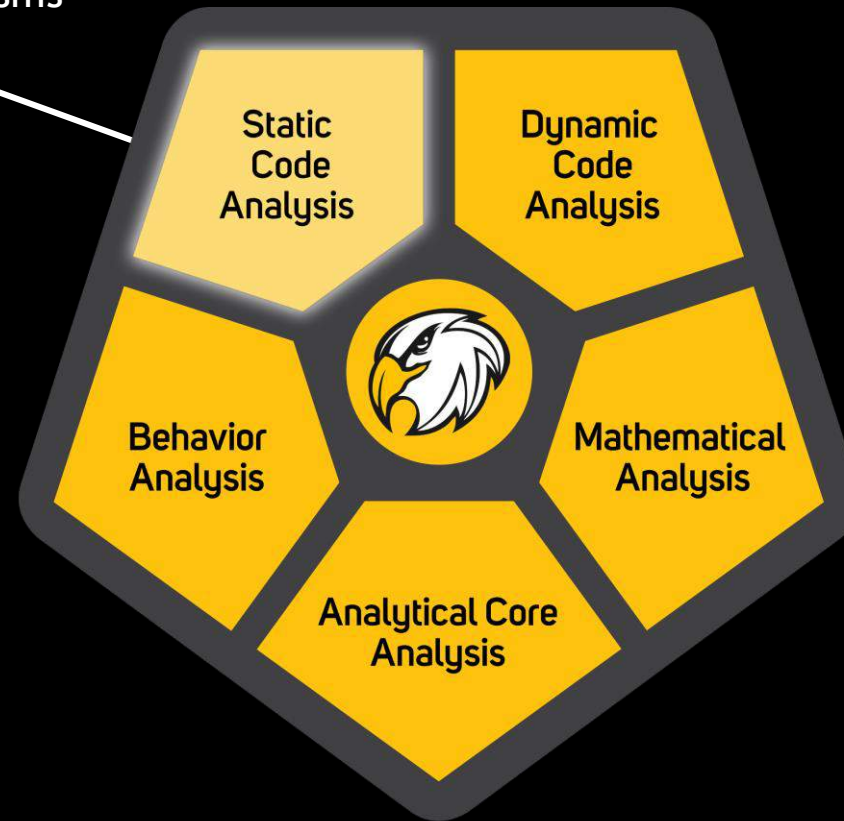
Removes attack protection mechanisms

Extracts embedded object

Extracts sensitive information

Inspects and scores file structure

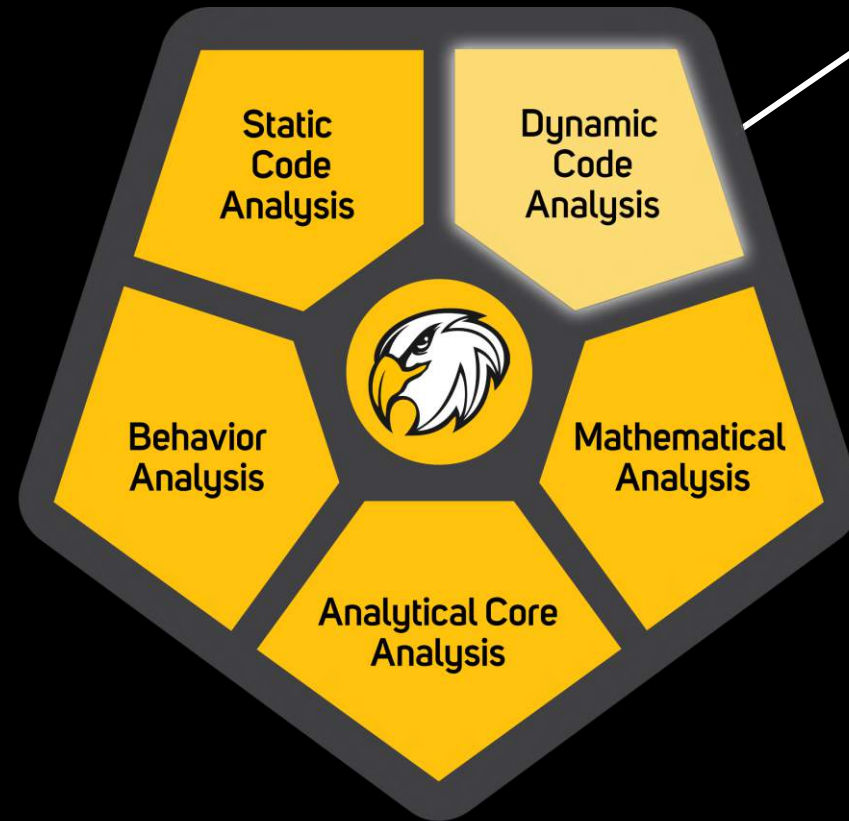
Anti Virus



CYBERTINEL - Anti Cyber Threat Infrastructure

Dynamic Code Analysis Engine

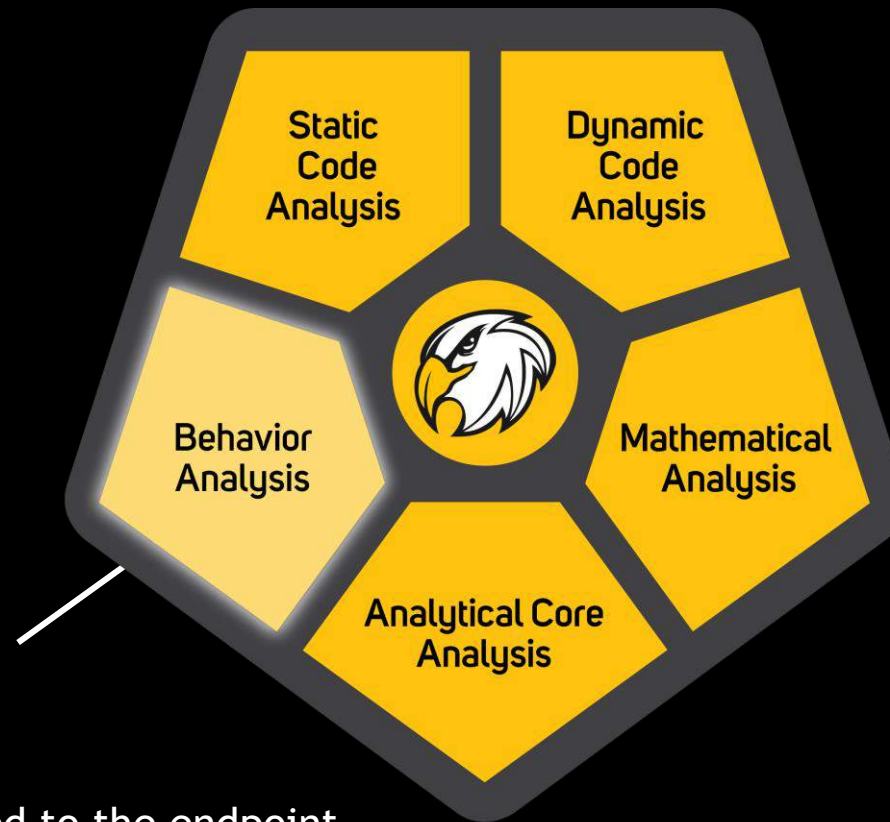
- Debugs in a controlled environment
- Overcomes anti-vm and anti-sandbox techniques
- Generates profile based on the capabilities



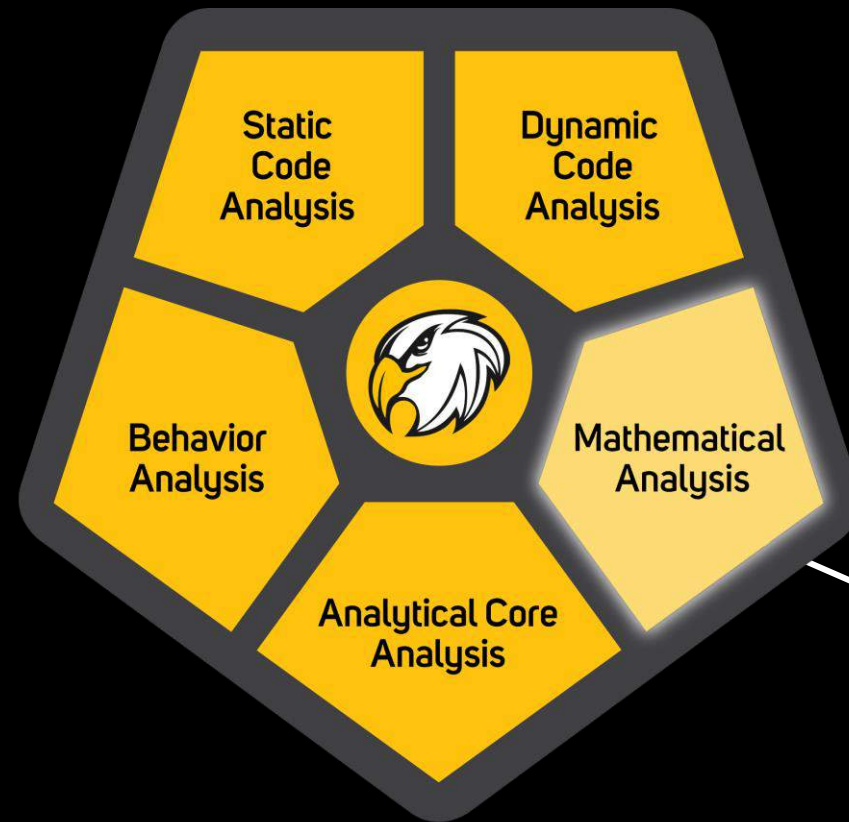
CYBERTINEL - Anti Cyber Threat Infrastructure

Behavioral Analysis Engine

- Monitor Any Process / command
- Track down network activity
- Detect suspicious disk activities
- Monitor any device ever connected to the endpoint



CYBERTINEL - Anti Cyber Threat Infrastructure

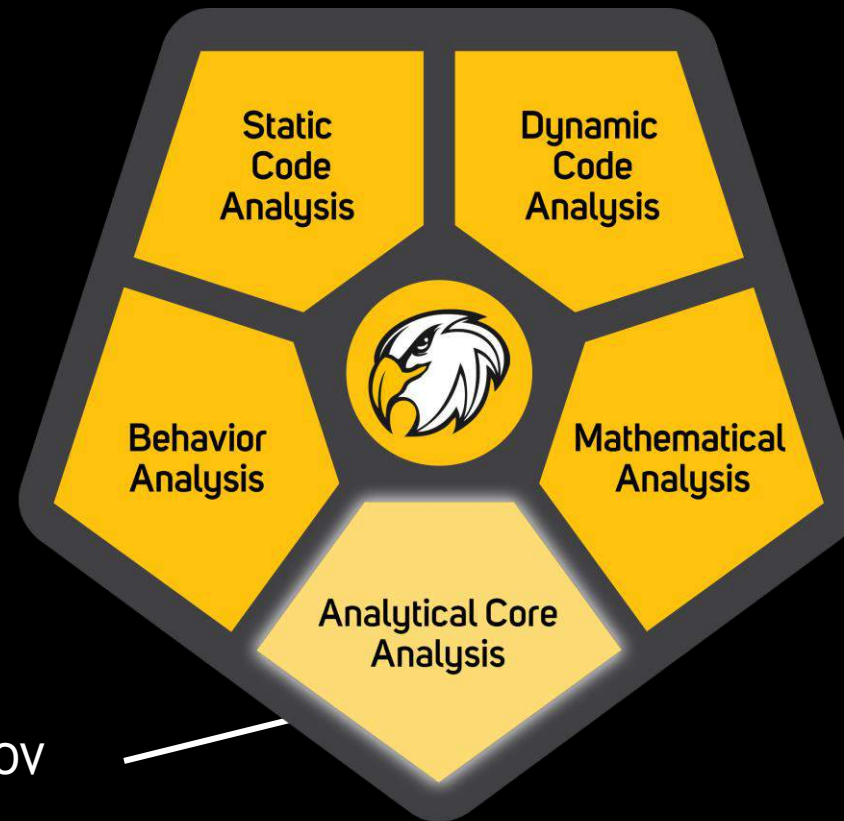


Mathematical Analysis Engine

- Detects anomalies by Statistical analysis
- Detects both internal & external attacks



CYBERTINEL - Anti Cyber Threat Infrastructure



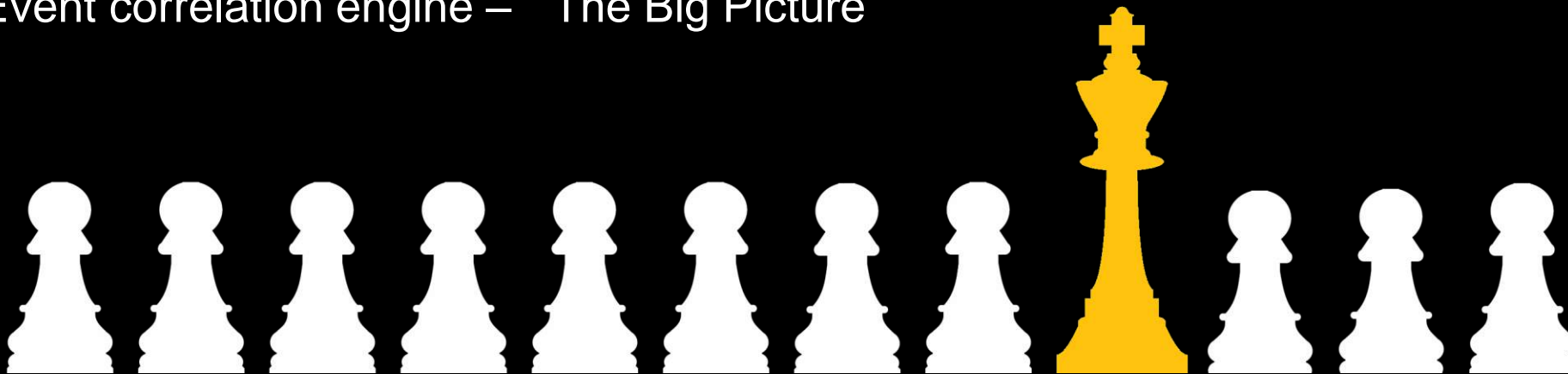
Analytical Core Analysis Engine

- Gets the “big picture” from a single POV
- Correlates collected information to scope the entire attack



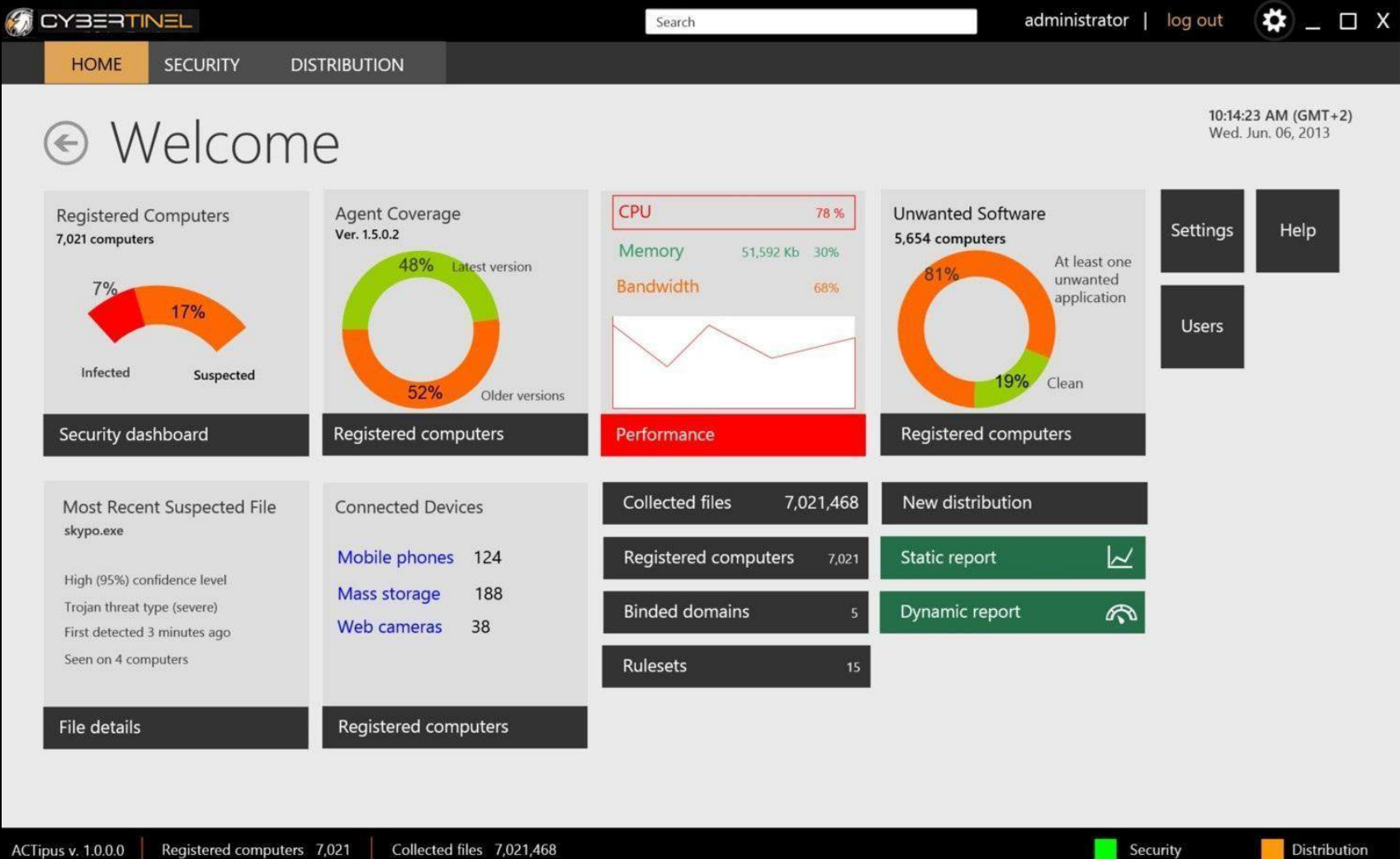
Differentiators - Technology & Architecture

- ❖ Uncovers APTs and zero-day attacks
- ❖ Real time detection
- ❖ Multi-layer data collection
- ❖ Automatic analysis and remediation
- ❖ Fully detailed forensics reporting
- ❖ Event correlation engine – “The Big Picture”

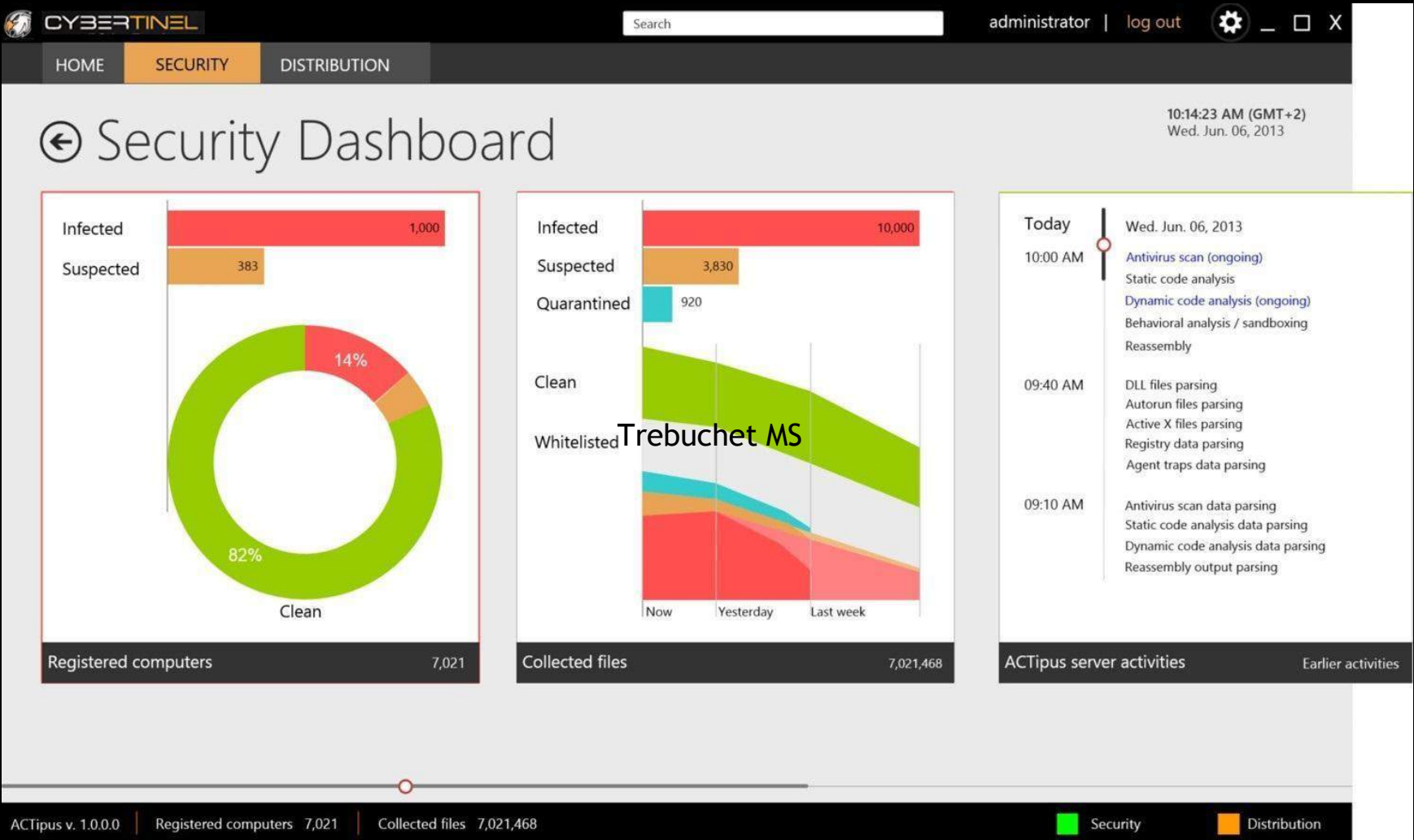


Dashboards

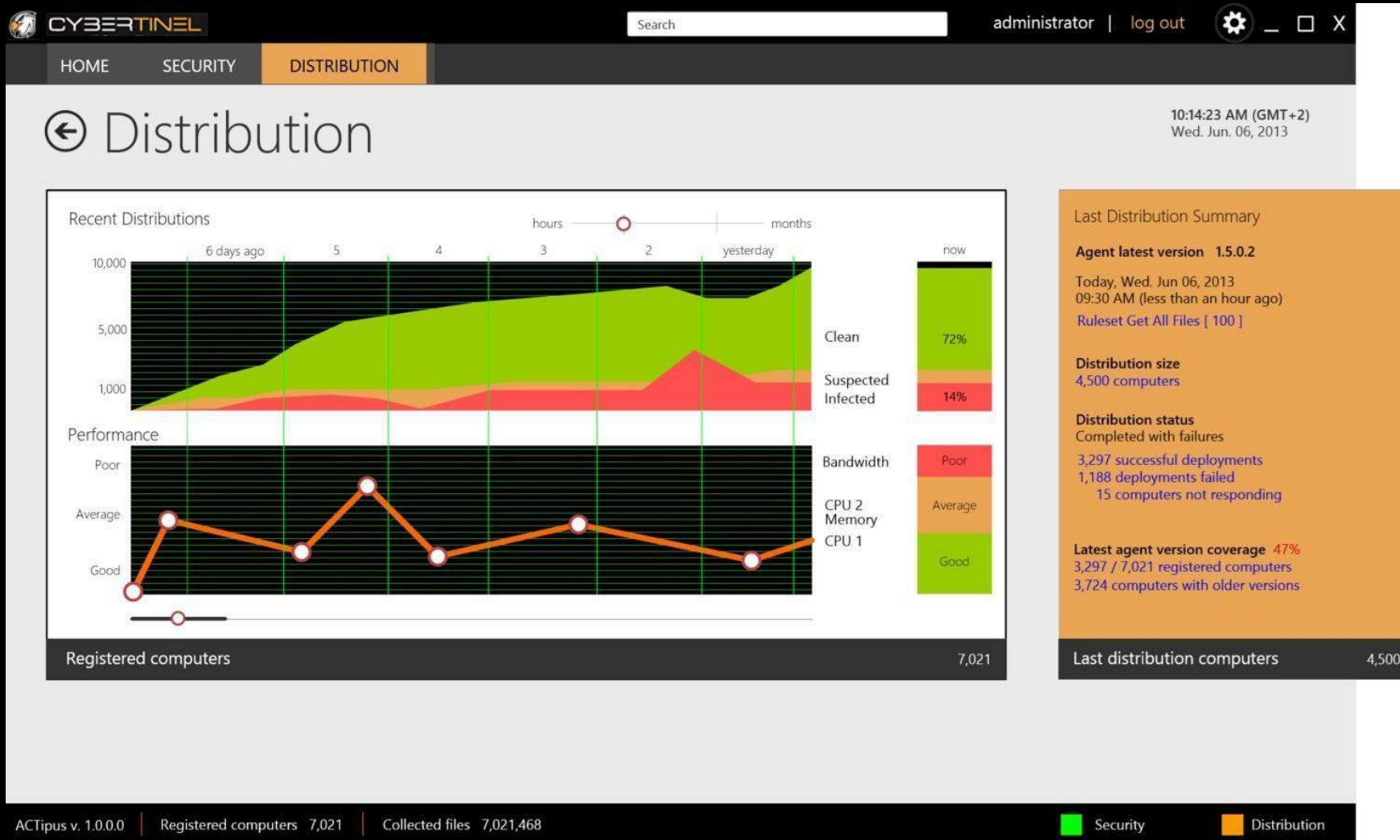
CYBERTINEL Dashboards



CYBERTINEL Dashboards



CYBERTINEL Dashboards



CYBERTINEL Dashboards

CYBERTINEL Search administrator | log out 10:14:23 AM (GMT+2) Wed. Jun. 06, 2013

HOME SECURITY DISTRIBUTION

7,021,468 Collected Files

Filter Select Recently analyzed first Full details view Page 1 of 15,456 Reload

File Skyp0.exe

[SHA-1 939bd888607dee57c12b33a194c92a87a1163e92]

Analyzed: Today, Wed. Jun. 06, 2013 at 09:15 AM

Collected: Wed. Jun. 06, 2013 at 09:14 AM

Details	
Size	473,584 Kb
Type	Win32 EXE
Security status	Suspected
Threat	Trojan (XtremeRAT)
Severity	High
Confidence	80% (high)
Spread	3 computers
AV Detection	0/16

First appearance

4 Minutes ago

Wed. Jun. 06, 2013 at 09:13 AM

Open full report

Insights

Code	5%
Strings	249 (0.05%)
PE sections	8
Dll imports	2 (0.8%)
IP addresses	1 China
URL addresses	2/4 Dynamic
Email addresses	0
External PE objects	0
External text objects	1 Keylogger
External drivers	0
String packer signatures	0
Binary packer signatures	0 Unknown Packer

Investigate

Comments

No comments

Ignore

- Ignore
- Quarantine
- Clean

File tcpipreg.sys

Analyzed: Today, Wed. Jun. 06, 2013 at 09:15 AM (1 hour)

Details	
Size	473,584 Kb
Type	Win32 EXE
Security status	Clean
Threat	None
Severity	None
Confidence	97% (high)
Spread	178 computers
AV Detection	0/16

First appearance

4 Minutes ago

Wed. Jun. 06, 2013 at 09:13 AM

Open full report

Page 1 of 15,456


Clear filters 15,456 / 7,021,468 Clear selections (1) Ignore (1) Quarantine (1) Clean (1) Export

ACTipus v. 1.0.0.0 Registered computers 7,021 Collected files 7,021,468 Security Distribution




File Name and Hash
(SHA1)




CYBERTINEL Dashboards

 **CYBERTINEL**

Search


administrator | log out   



File Report

File **Skype.exe** 7,021,468 collected files

10:14:23 AM (GMT+2)
Wed. Jun. 06, 2013



Skype.exe [SHA-1 939bd888607dee57c12b33a194c92a87a1163e92] Security score **8.9 / 10** Export

Analysis Today, Wed. Jun 06, 2013 at 09:15 AM | Collection Today, Wed. Jun 06, 2013 at 09:13 AM

Details

Size	473,584 Kb
Type	Win32 EXE
MIME type	application/octet-stream
Security status	Suspected
Threat	Trojan (XtremeRAT)
Severity	High
Confidence	80% (high)
AV Detection	0/16
Spread	3 computers

Checks

Entropy check for packer	Positive
Driver check	Negative
Executable check	Positive
DLL check	Negative

Static Code Analysis

Insights

Code	5%
Strings	249 (0.05%)
PE sections	8
DLL imports	2 (0.8%)
IP addresses	1 China
URL addresses	2/4 Dynamic
Email addresses	0
External PE objects	0
External text objects	1 Keylogger
External drivers	0
String packer signatures	0
Binary packer signatures	0 Unknown Packer !
Compiler signature	NeoLite v2.00
File original name	Skype.exe (changed)
Time Stamp (compiled)	04.06.13 (two days ago)
Linker Version	7.0
File Description	Skype Corp Inc. (fake)

First Appearance

4 Minutes ago
Today, Wed. Jun 06, 2013 at 09:13

First Computer

Computer	borisr-LAP
User	borisr
Domain	lab
Organizational unit	lab\Laptops
Operating system	Windows Vista™ Enterprise
Computer log	

Additional Computers

- Ilannm-LAP**
- Tomis-LAP**

File Locations

- Boris-LAP:** c:\users\borisr\print hood\
- Ilannm-LAP:** c:\temp\
- Tomis-LAP:** c:\users\tomis\documents\

Autorun Locations

- C:\Users\kobi.EXPLOITEAM\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\ **.lnk**

Comments

15 comments

administrator 5 sec
There are more infected files created on the same computer (196.156.123.45) !!!

administrator 16 min
There are more infected files created on the same computer (196.156.123.45) !!!


administrator 2 hrs
There are more infected files created on the same computer (196.156.123.45) !!!


administrator 15 hrs
There are more infected files created on the same computer (196.156.123.45) !!!


administrator 24 hrs
There are more infected files created on the same computer (196.156.123.45) !!!

administrator 2 days
There are more infected files created on the same computer (196.156.123.45) !!!

ACTipus v. 1.0.0.0 | Registered computers 7,021 | Collected files 7,021,468

 Security

 Distribution



ANTI CYBER THREATS

CYBERTINEL Dashboards



administrator | [log out](#)



File Report

File **Skypo.exe**

7,021,468 collected files

10:14:23 AM (GMT+2)
Wed. Jun. 06, 2013



Skypo.exe [SHA-1 939bd888607dee57c12b33a194c92a87a1163e92]

Security score **8.9 / 10**

[Export](#)

Analysis Today, Wed. Jun 06, 2013 at 09:15 AM

Collection Today, Wed. Jun 06, 2013 at 09:13 AM

DLL check

Negative

Name-Similarity check

Positive

File Description

Skype Corp Inc. (fake)

C:\Users\kobi.EXPLOITTEAM\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\ .lnk

Static Code Analysis

PE Sections

Name	Virtual Address	Virtual Size (Kb)	Raw Size (Kb)	Entropy	ID (SHA-1)
.text	4096	139.264	0	0.0	e121a89e5cd409c3886ef47af6b3b17ef79af61
.tls	143360	199,229.440	0	0.0	9c0dc7642b0efd3e067d04b939f30013993bff
.yccup	199372800	311.296	0	0.0	8bf1819659b79d10121294f37f7d9cf7d95559
.idata	199684096	4.096	0	0.0	0123456789012345678901234567890123mjyt
.rsrc	199688192	98.304	98.100	7.8	52e04d5c27622d027c39632c1291f9a4279c07
dwnj76zr	199786496	81.920	0	0.0	ff2dcf53c6f77aeb33ff8e3d4e1671e2875cc225
i6q8y.2y	199868416	372.736	368.874	7.9	ee062d364e159e3fd4caf0051c35ee57ce6950
tricf1tf	200241152	4.096	0.512	7.6	cdc7a4d3fa10b12ad2b8827d17890953739fa1

DLL Imports (2)

► kernel32.dll

▼ user32.dll

MessageBoxA

URL Addresses (2)

Comments

15 comments



administrator

5 sec

There are more infected files created on the same computer (196.156.123.45) !!!

administrator

16 min

There are more infected files created on the same computer (196.156.123.45) !!!

administrator

2 hrs

There are more infected files created on the same computer (196.156.123.45) !!!

administrator

15 hrs

There are more infected files created on the same computer (196.156.123.45) !!!

administrator

24 hrs

There are more infected files created on the same computer (196.156.123.45) !!!

administrator

2 days

There are more infected files created on the same computer (196.156.123.45) !!!



Security







Distribution

NEL




CYBERTINEL Dashboards



administrator | [log out](#)   

File Report

File **Skypo.exe** 7,021,468 collected files

10:14:23 AM (GMT+2)
Wed. Jun. 06, 2013 

Skypo.exe [SHA-1 939bd888607dee57c12b33a194c92a87a1163e92] Security score **8.9 / 10** Export

Analysis Today, Wed. Jun 06, 2013 at 09:15 AM | Collection Today, Wed. Jun 06, 2013 at 09:13 AM

URL Addresses (2)

<http://oscp.thawte.com> (part of fake certification)

<http://crl.thawte.com/ThawteTimestampingCA.crl> (part of fake certification)

Dynamic Code Analysis

Mutex	xcvxc	Collected files	1	Domains	2
Injection	proquota.exe	Modified files	0	URL addresses	0
Autorun value	startup\lnk			IP addresses	1

Deleted Files (5)

C:\Documents and Settings\Alex\Application Data\Microsoft\Templates\~\$Normal.dotm

C:\Documents and Settings\Alex\Local Settings\Temp_tmp_rar_sfx_access_check_78592140 (part of self extracted archive)

C:\Documents and Settings\Alex\Local Settings\Temp\~\$f.doc

C:\Documents and Settings\Alex\Local Settings\Temporary Internet Files\Content.Word\~WRS(1F07D208-B3AE-4892-8C9B-85FB33120363).tmp


C:\Documents and Settings\Alex\Local Settings\Temporary Internet Files\Content.Word\~WRS(1F07D208-4A32-4892-8C9B-85FB33120363).tmp

Domains (2)

toornt.servegame.com

backop.dyndns-web.com

Comments

15 comments 

administrator 5 sec

There are more infected files created on the same computer (196.156.123.45) !!!

administrator 16 min

There are more infected files created on the same computer (196.156.123.45) !!!

administrator 2 hrs

There are more infected files created on the same computer (196.156.123.45) !!!

administrator 15 hrs

There are more infected files created on the same computer (196.156.123.45) !!!

administrator 24 hrs

There are more infected files created on the same computer (196.156.123.45) !!!


administrator 2 days

There are more infected files created on the same computer (196.156.123.45) !!!


ACTipus v. 1.0.0.0 | Registered computers 7,021 | Collected files 7,021,468

Security




Distribution




CYBERTINEL Dashboards

 **CYBERTINEL**

Search


administrator | log out   



File Report

File **Skype.exe** 7,021,468 collected files

10:14:23 AM (GMT+2)
Wed. Jun. 06, 2013



Skype.exe [SHA-1 939bd888607dee57c12b33a194c92a87a1163e92] Security score **8.9 / 10** Export

Analysis Today, Wed. Jun 06, 2013 at 09:15 AM | Collection Today, Wed. Jun 06, 2013 at 09:13 AM

▼ backup.dyndns-web.com (shows only positive tests)

Name Similarity Backup // Backup

Dynamic IP Dyndns listed as dynamic domain service provider

File 5 Min

Black Lists Listed in above 10 DNSBL databases

IP addresses (1)

▼ 58.218.199.147

Country: China

City: Jiangsu

ISP: China Telecom

▼ Net Segment: 255.255.255.128

► 58.218.199.155 (linked to additional file)

▼ 58.218.199.167 (linked to additional file)

Excel.exe [SHA-1 idnj37dnchc9d898sknsdh928js8ss88jsbdmel1 (first seen one days ago)]

Computer Name: guy-PC | OS: windows XP | OU: workstations |

Reverse Lookup None

▼ IP Black Lists Listed in above 10 IPBL databases

DNS BL None

IP Who Is

Administrative Contact
Chinanet Hostmaster
No.31 jingrong street,beijing 100032
Telephone: 861058501724
Fax: 861058501724
Email: anti-spam@ns.chinanet.cn.net

▼ Key Login

Logging Method Filter Driver

Logging Location C:\windows\system32\config\key.dat

Encryption Method Dynamic Caesar shifting

Encryption Key +16 (+1 for char location in string)

▼ Screen Capture

Capture Method Filter Driver

Capture Location C:\windows\system32\config\[datetime].jpg

▼ C&C Connectivity

Network Protocol Port 80 (None Http)

Encryption Method Symmetric key

Encryption Key Hostname + mac address
Shifted + 16

Insertion Vector

▼ Email

Method Spear Phishing


Sender ldf.un@gmail.com

Recipients boris@exploiteam.com
ilanm@exploiteam.com

Links none

Attachments ▼ Tt_slip.rar
Images.scr

Comments

15 comments 

administrator 5 sec

There are more infected files created on the same computer (196.156.123.45) !!!

administrator 16 min

There are more infected files created on the same computer (196.156.123.45) !!!

administrator 2 hrs

There are more infected files created on the same computer (196.156.123.45) !!!

administrator 15 hrs

There are more infected files created on the same computer (196.156.123.45) !!!

administrator 24 hrs

There are more infected files created on the same computer (196.156.123.45) !!!


administrator 2 days

There are more infected files created on the same computer (196.156.123.45) !!!

ACTipus v. 1.0.0.0 | Registered computers 7,021 | Collected files 7,021,468

Security

Distribution



CYBERTINEL Dashboards



administrator | log out



File Report

File **Skypo.exe**

7,021,468 collected files

10:14:23 AM (GMT+2)
Wed. Jun. 06, 2013



Skypo.exe [SHA-1 939bd888607dee57c12b33a194c92a87a1163e92]

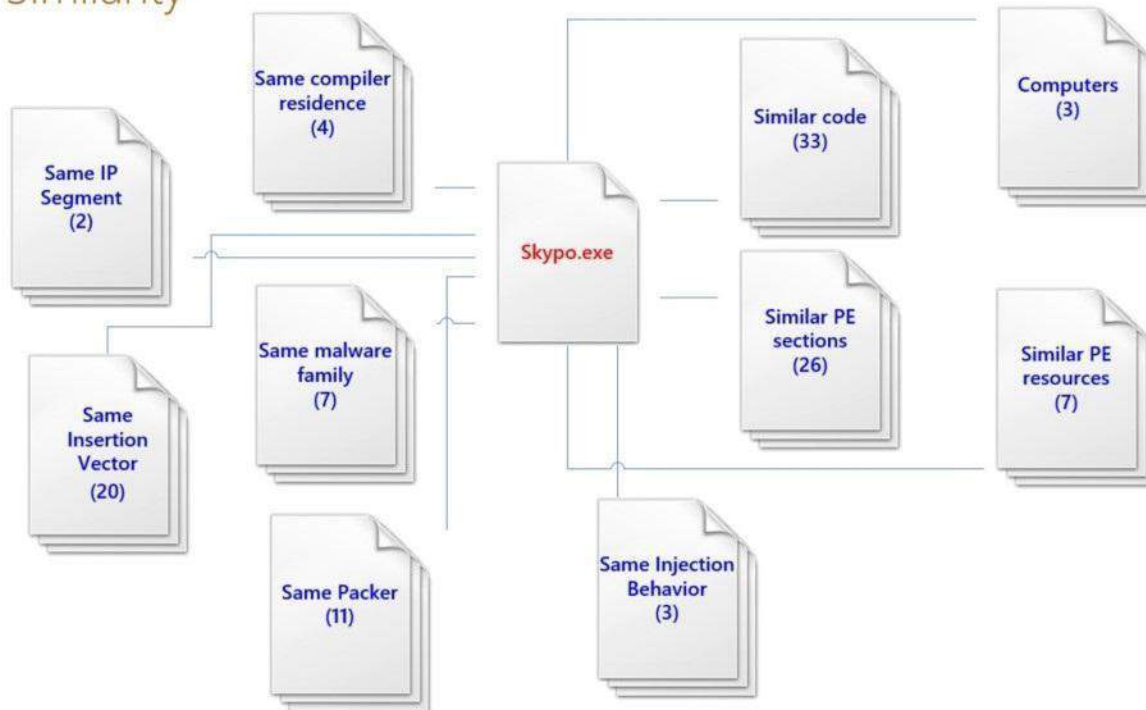
Security score **8.9 / 10**

Export

Analysis Today, Wed. Jun 06, 2013 at 09:15 AM

Collection Today, Wed. Jun 06, 2013 at 09:13 AM

Similarity



Comments

15 comments



- administrator** 5 sec
There are more infected files created on the same computer (196.156.123.45) !!!
- administrator** 16 min
There are more infected files created on the same computer (196.156.123.45) !!!
- administrator** 2 hrs
There are more infected files created on the same computer (196.156.123.45) !!!
- administrator** 15 hrs
There are more infected files created on the same computer (196.156.123.45) !!!
- administrator** 24 hrs
There are more infected files created on the same computer (196.156.123.45) !!!
- administrator** 2 days
There are more infected files created on the same computer (196.156.123.45) !!!



The Operation HARKONNEN Discovery



Thank you
You are now protected