



**XIII
JORNADAS
STIC
CCN-CERT**



Orangeworm
How I met your master...

COMUNIDAD Y CONFIANZA,
BASES DE NUESTRA CIBERSEGURIDAD

#XIIIJORNADASCCNCERT



Pablo Rincón Crespo



pablo.rincon@cylera.com



Introducción

- Cylera, 2017
- Fabricante de soluciones
- Orangeworm
- “Visto en dispositivos médicos”
- Investigación/desarrollo (<1 año)
- Objetivos → IOCs, TTPs, asociación
- Ponencia

Índice

1. Orangeworm
2. Markel y Yara
3. Paul y el CTF de Suricon
4. Cheating en otro CTF
5. Needle\$ in a haystack
6. Es elfin?



1. Orangeworm

2. Markel y Yara

3. Paul y el CTF de Suricon

4. Cheating en otro CTF

5. Needle\$ in a haystack

6. Es elfin?

1. Orangeworm

Qué es?

- Grupo APT → Sector sanitario → Hospitales



Security Response
Attack Investigation
Team

POSTED: 23 APR, 2018 | 4 MIN READ | THREAT INTELLIGENCE

SUBSCRIBE

New Orangeworm attack group targets the healthcare sector in the U.S., Europe, and Asia

Symantec has identified a new attack group dubbed Orangeworm deploying the Kwampirs backdoor in a targeted attack campaign against the healthcare sector and related industries.

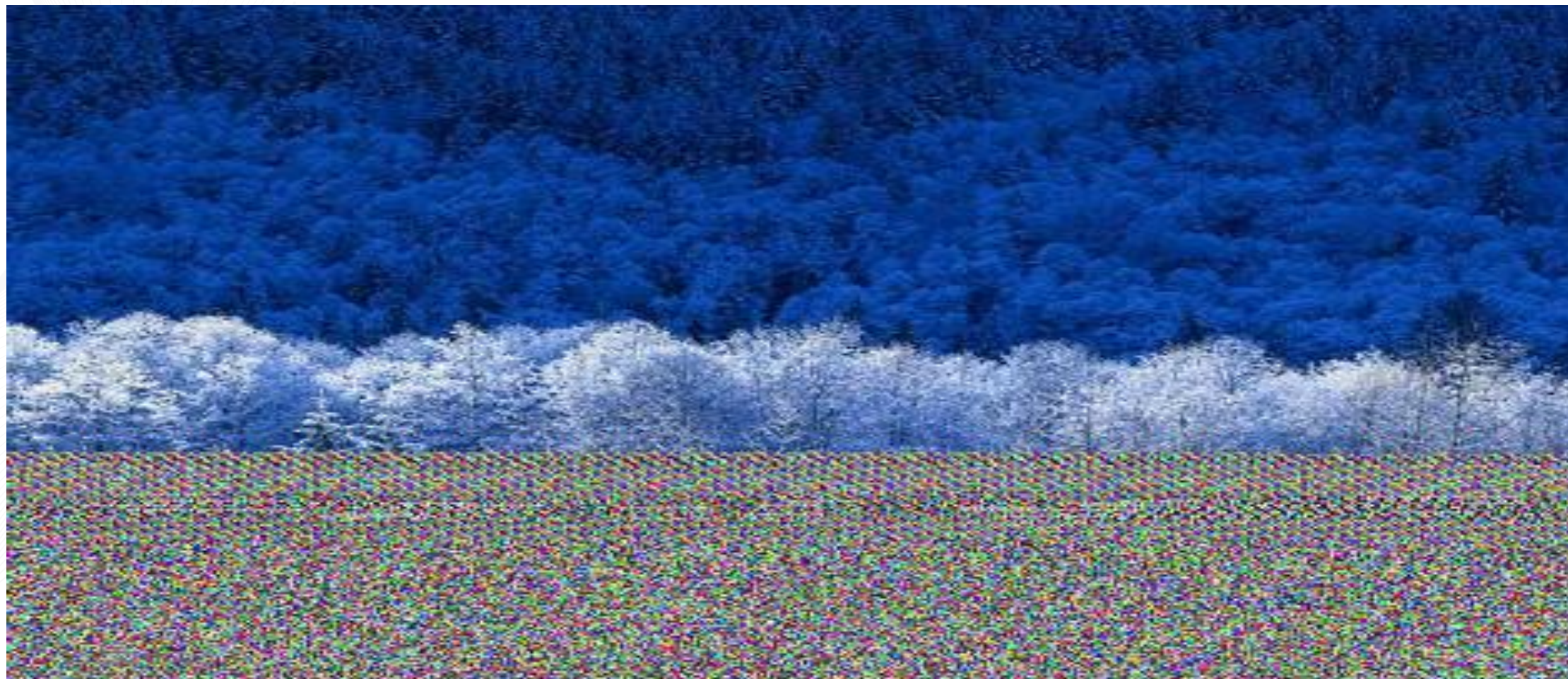
No hallmarks of a nation-state actor

While Orangeworm is known to have been active for at least several years, we do not believe that the group bears any hallmarks of a state-sponsored actor—it is likely the work of an individual or a small group of individuals. There are currently no technical or operational indicators to ascertain the origin of the group.

- Selección de víctimas
- Cadena de suministro...
- Espionaje corporativo

- **kwampirs**
- Nivel de sofisticación medio-alto
- Strings cifrados en estático
- Esteganografía y firma cripto
- Señalización por “pipes”, fechas, otros
- Recursos administrativos windows
- Visto en +27 países
- MRI & X-Ray

1. Orangeworm



** DLL Cifrada, oculta en una imagen, dentro de los recursos de los droppers de Orangeworm*

1. Orangeworm





1. Orangeworm

2. Markel y Yara

3. Paul y el CTF de Suricon

4. Cheating en otro CTF

5. Needle\$ in a haystack

6. Es elfin?

2. Markel y Yara

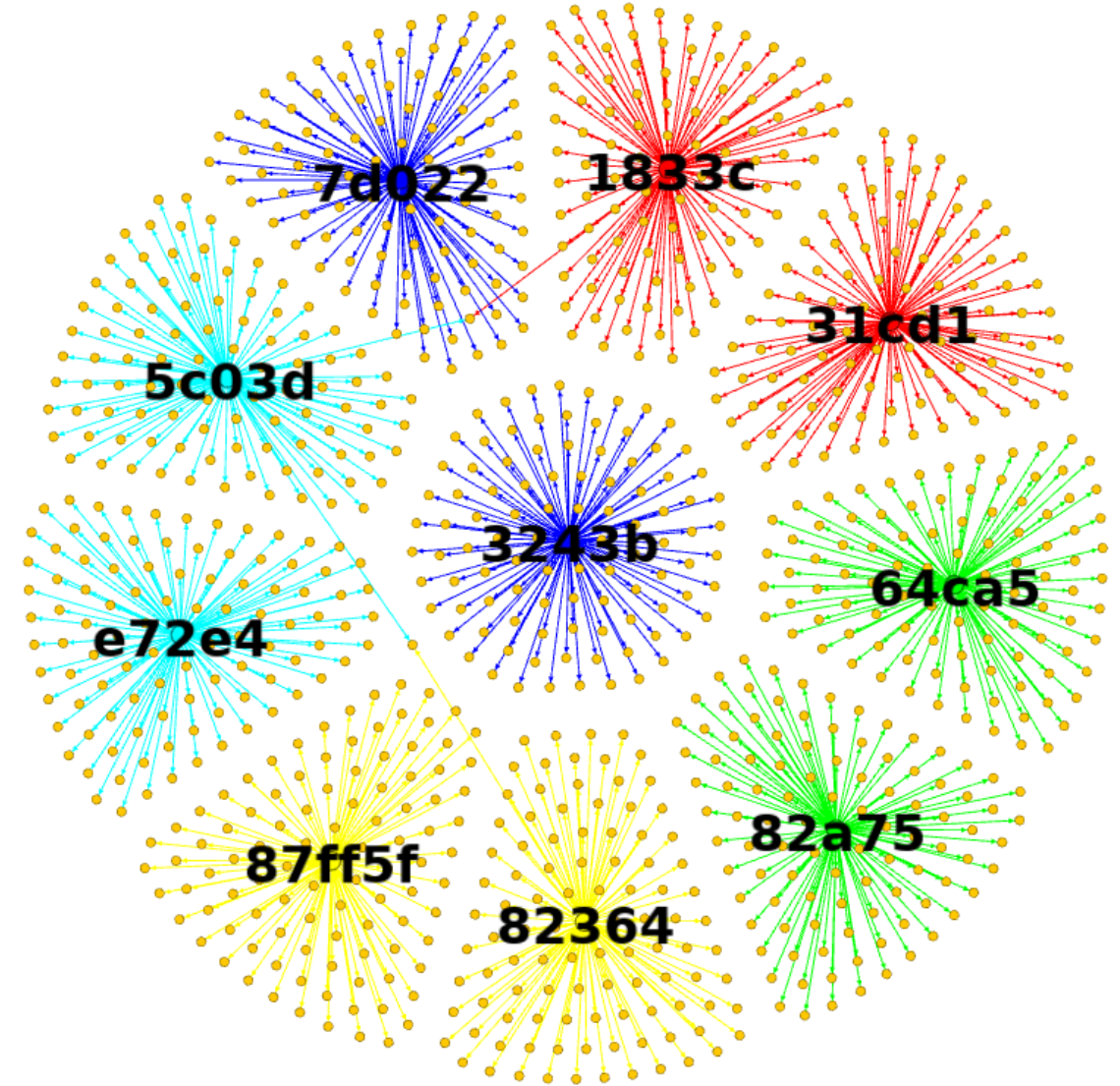
Septiembre de 2018, Madrid

Análisis, scripts y yaras (Markel Picado):

- Extractor configuraciones (2 listas por binario)
- Extractor Dlls (stego)
- Para cifrar/descifrar mensajes con el C&C

2. Markel y Yara

- Bot para descargar módulos
- Información de campañas →
- Regla yara VT para:
 - Algoritmo cifrado C2
 - Key utilizada





1. Orangeworm
2. Markel y Yara
- 3. Paul y el CTF de Suricon**
4. Cheating en otro CTF
5. Needle\$ in a haystack
6. Es elfin?

3. Paul y el CTF de Suricon

Noviembre 2018, Vancouver, SuriCon 2018

- SuriCon CTF
- Directory listing (Paul Bakoyiannis):
 - Mirror completo
 - PuK → Clave pública → Para validar firmas? Para ransomware?
 - Logs cifrados
- Descifrador logs Markel
- Afectación

3. Paul y el CTF de Suricon



ikjpbm.in/users/users/files/log/index.html

Index of /users/users/files/log

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 cl	2018-11-20 14:54	535K	
 cl_20180826210652.7z	2018-08-26 21:06	47K	
 cl_20180827190645.7z	2018-08-27 19:06	51K	
 cl_20180828144105.7z	2018-08-28 14:41	52K	
 cl_20180829102635.7z	2018-08-29 10:26	50K	
 cl_20180830064552.7z	2018-08-30 06:45	50K	
 cl_20180831024332.7z	2018-08-31 02:43	50K	
 cl_20180901033920.7z	2018-09-01 03:39	48K	
 cl_20180902062700.7z	2018-09-02 06:27	54K	

3. Paul y el CTF de Suricon

- MACs, OS versions, plataforma, build, arquitectura, petición de HASH

```
TYPE: 4 MAC: -D9-F8-96 OSMAJOR: 5 OSMINOR: 1 PLATFORMID: 2 BUILD: 0xa28 ARCH: (x86) VAR: '71035'
TYPE: 3 MAC: -D9-F8-96 VAR: 'tu)</center>\r\n</body>\r\n</html>\r\n'
TYPE: 4 MAC: -7E-69-95 OSMAJOR: 6 OSMINOR: 3 PLATFORMID: 2 BUILD: 0x2580 ARCH: (x64) VAR: '713451'
TYPE: 3 MAC: -7E-69-95 VAR: 'tu)</center>\r\n</body>\r\n</html>\r\n'
TYPE: 4 MAC: -B0-63-02 OSMAJOR: 6 OSMINOR: 1 PLATFORMID: 2 BUILD: 0x1db1 ARCH: (x86) VAR: '76713'
TYPE: 3 MAC: -B0-63-02 VAR: 'tu)</center>\r\n</body>\r\n</html>\r\n'
TYPE: 4 MAC: -0E-B0-C5 OSMAJOR: 6 OSMINOR: 1 PLATFORMID: 2 BUILD: 0x1db0 ARCH: (x86) VAR: '728629'
TYPE: 3 MAC: -0E-B0-C5 VAR: 'tu)</center>\r\n</body>\r\n</html>\r\n'
TYPE: 4 MAC: -AB-CE-74 OSMAJOR: 6 OSMINOR: 2 PLATFORMID: 2 BUILD: 0x23f0 ARCH: (x86) VAR: '728705'
TYPE: 3 MAC: -AB-CE-74 VAR: 'tu)</center>\r\n</body>\r\n</html>\r\n'
TYPE: 4 MAC: -BB-61-80 OSMAJOR: 6 OSMINOR: 1 PLATFORMID: 2 BUILD: 0x1db0 ARCH: (x86) VAR: '72767'
TYPE: 3 MAC: -BB-61-80 VAR: 'tu)</center>\r\n</body>\r\n</html>\r\n'
TYPE: 4 MAC: -C2-12-DF OSMAJOR: 6 OSMINOR: 1 PLATFORMID: 2 BUILD: 0x1db1 ARCH: (x86) VAR: '717280'
TYPE: 3 MAC: -C2-12-DF VAR: 'tu)</center>\r\n</body>\r\n</html>\r\n'
TYPE: 4 MAC: -91-BA-ED OSMAJOR: 10 OSMINOR: 0 PLATFORMID: 2 BUILD: 0x42ee ARCH: (x64) VAR: '722209'
```

3. Paul y el CTF de Suricon

- OSINT de dominios
- Sinkhole:
 - + campañas
 - 2 listas por campaña → 2 dominios
 - Distinta periodicidad
 - Guardamos petición y luego 404 (not found)
- Nada muy distinto a los logs del Directory Listing

3. Paul y el CTF de Suricon

Cabeceras “Via” o “X-Forwarded-For”:

```
Via: 1.1 [REDACTED]-TMG
Via: 1.1 ::ffff:[REDACTED].20 (Mikrotik HttpProxy), 1.1 J5K-NOURNET (jaguar/3.0-11)
Via: 1.1 [REDACTED]DIRSVR-2
Via: 1.1 [REDACTED]-DR-TMG01
Via: 1.1 [REDACTED]TMGSERVER
Via: 1.1 TMG2020
Via: 1.1 TMG-SRV-[REDACTED]
Via: 1.1 [REDACTED]medica.org:80 (Cisco-WSA/11.5.1-115)
Via: 1.1 WIN-TMG
Via: 1.1 WIN-VPQ65PJCVCDC
Via: HTTP/1.1 forward.http.proxy:3128
X-Forwarded-For: [REDACTED]194.175
X-Forwarded-For: [REDACTED]2000:1b:400::18
X-Forwarded-For: [REDACTED]2000:38:400::1f
X-Forwarded-For: [REDACTED]36.210
X-Forwarded-For: [REDACTED].110
```

3. Paul y el CTF de Suricon

- Proxies/Firewalls → DLL
- Geolocalización → alguna “ciudad médica”
- Sinkhole → Directorio payloads → vacío
- Queríamos saber más :(
- Campaña muerta, “Server tostado”



1. Orangeworm
2. Markel y Yara
3. Paul y el CTF de Suricon
- 4. Cheating en otro CTF**
5. Needle\$ in a haystack
6. Elfin... a la luz de la luna

4. Cheating en otro CTF

Diciembre 2018, Madrid

- Llega una alerta extraña de yara, de VT
- Solo la **CLAVE..** No es kwampirs?

¿...?

4. Cheating en otro CTF

#XIIIJORNADASCCNCERT

Qué es...?

[VTMIS][95baf6b8225785b2846c0491e16a4565cf9e588f287c2933265134b881b16639] orange_xor_key
noreply@vt-community.com

Link :
<https://www.virustotal.com/gui/file/95baf6b8225785b2846c0491e16a4565cf9e588f287c2933265134b881b16639>

MD5 : 71b50f2c476e552f9c26545ad7f3aa7b
SHA1 : 32149c402c43b57d64e545c93017712a76e7e668
SHA256 :
95baf6b8225785b2846c0491e16a4565cf9e588f287c2933265134b881b16639
Type : Win32 EXE

First seen : 2018-12-22 07:45:56 UTC

Last seen : 2018-12-22 07:45:56 UTC

First name : dttcodexgigas.32149c402c43b57d64e545c93017712a76e7e668

First source : 29858849 (api)

First country: AR

Key: 28 30 A4 3F 6D 28 04 23 36 2A 32 DC AD 0B A0 4B E8 ...

4. Cheating en otro CTF

Otro CTF

[PDF] Solution du challenge SSTIC 2016

static.sstic.org > solutions > solution_pierre_bienaime ▼ Traducir esta página

24 abr. 2016 - la société Airlhes : suite à un incident de sécurité, il faut prouver ... gramme : la clé de registre Software/Airlhes/Screensaver/config/trajectories.

[PDF] Challenge SSTIC 2016

static.sstic.org > solutions > solution_david_berard ▼ Traducir esta página

installée : Software/Airlhes/Screensaver/config/trajectories avec une chaîne hexadécimale débutant par l'entête. Zlib. La vidéo est un film du mur opposé à un ...

Solution Challenge SSTIC PDF - DocPlayer.fr

<https://docplayer.fr> > 132592941-Solution-challenge-s... - Traducir esta página

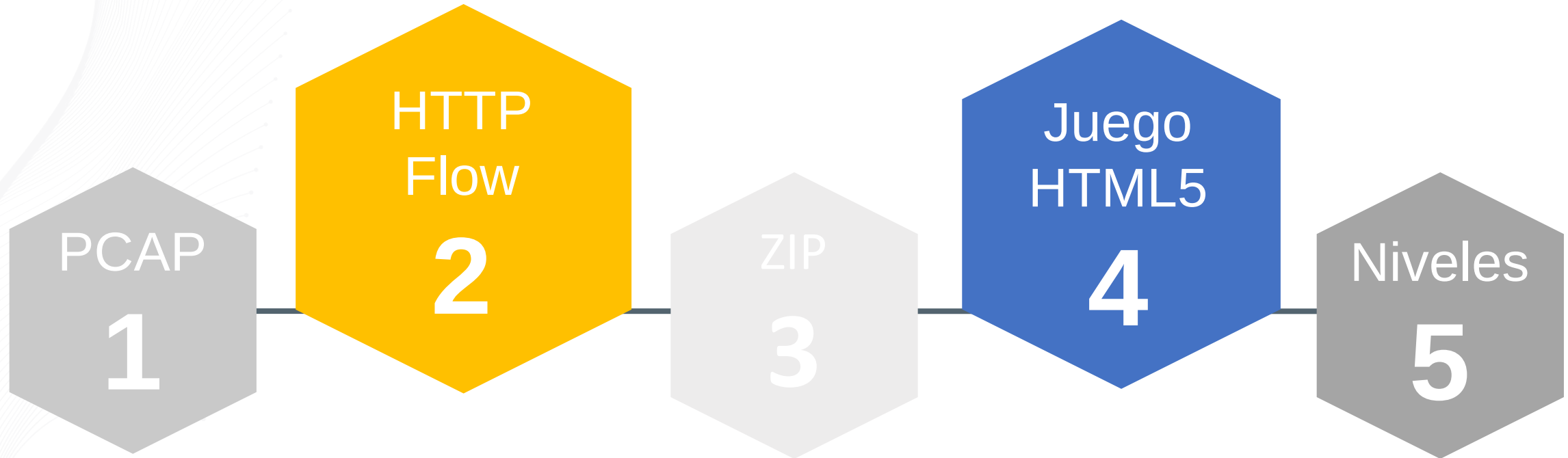
On constate que le programme va lire dans la registry la clef «Software\Airlhes\Screensaver\config\trajectories». Avec regedit, on trouve la séquence suivante ...



4. Cheating en otro CTF

#XIIJORNADASCCNCERT

Enero 2019, Madrid

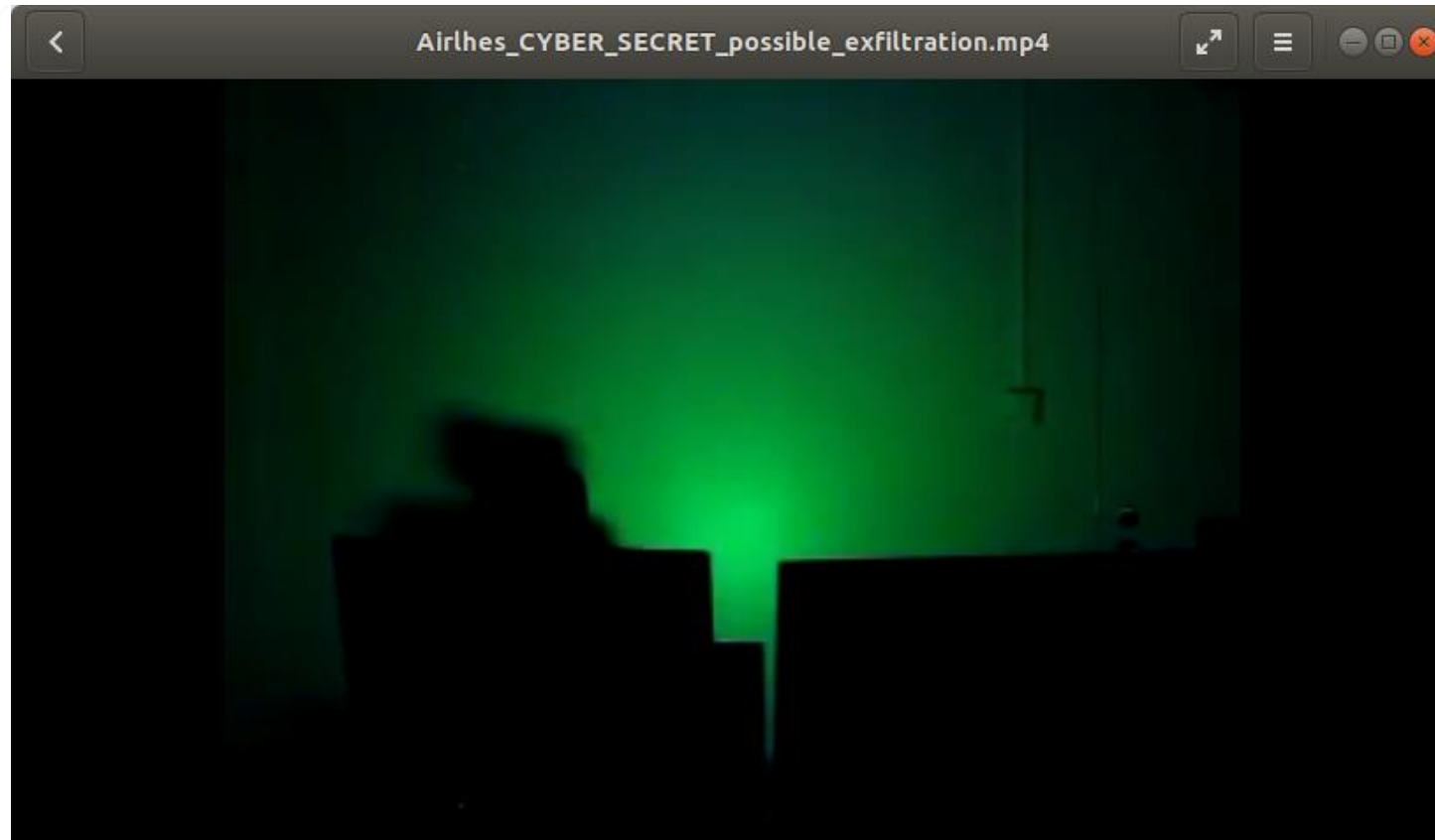


4. Cheating en otro CTF

- Writeups disponibles :D
- Confirmando que está la clave
- Simula aerolínea comprometida
- “Primo de Duqu”
- Leak de la “clave maestra”
- MP4 con Stego → screensaver → colores

SHA256: 0d39c9c1d09741a06ef8e35c0b63e538f60f8d5a7f995c7764e98a3ec595e46f - challenge.pcap

4. Cheating en otro CTF



- Hipótesis → Incidente Aerolínea → misma clave o familia → nivel del CTF basado en el mismo

- PE/DICOM
- Lab52 "Kwampirs Analysis Update"
- **LONG TIME LATER...**



1. Orangeworm
2. Markel y Yara
3. Paul y el CTF de Suricon
4. Cheating en otro CTF
- 5. Needle\$ in a haystack**
6. Es elfin?

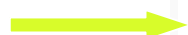
5. Needle\$ in a haystack

Octubre 2019, Madrid

- Alerta de VT (otra de tantas)
- Último intento?
- Infinidad de samples (Rompen hash)
- Busco unicidad
- VT...
- Algo curioso..

5. Needle\$ in a haystack

```
Monday
Sunday
WUSER32.DLL
CONOUT$
%s "%s" MyDllMain
%s /c start /b "" %s
%s%s%s
ADMIN$
C$\WINDOWS
D$\WINDOWS
E$\WINDOWS
\system32\csrss.exe
\system32\
%s%s%s.%s
SeDebugPrivilege
```



5. Needle\$ in a haystack

content:{450024005c00570049004e0044004f0057005300}

☐ FILES 2+

241a6fda84870a73800a2fa818e5dc880c55fd8feaa86964cf5ee5e2721157ed



trksvr

peexe

corrupt

overlay



7a26d5492a46d53e028f7ab9d4c8fa4307e9614e8cb54539a5bb82ce3c0bbdf5



_carved_027808.exe

peexe

assembly



5. Needle\$ in a haystack

W32.Disttrack | Symantec

<https://www.symantec.com> > security-center > writeup ▼ Traducir esta página

22 ago. 2012 - 64-bit Dropper: %System%\trksrv.exe (contained in the "X509" resource) ...

Distributed Link Tracking Server; ImagePath: %System%\trksvr.exe.

Shamoon (Troj/Mdrop-ELD) – Targeted destructive malware ...

<https://nakedsecurity.sophos.com> > 2012/08/17 > targe... ▼ Traducir esta página

17 ago. 2012 - \System32\cmd.exe /c "ping -n 30 127.0.0.1 >nul && sc config TrkSvr binpath=system32\trksrv.exe && ping -n 10 127.0.0.1 >nul && sc start ...

5. Needle\$ in a haystack

Agosto 2012, Arabia Saudi

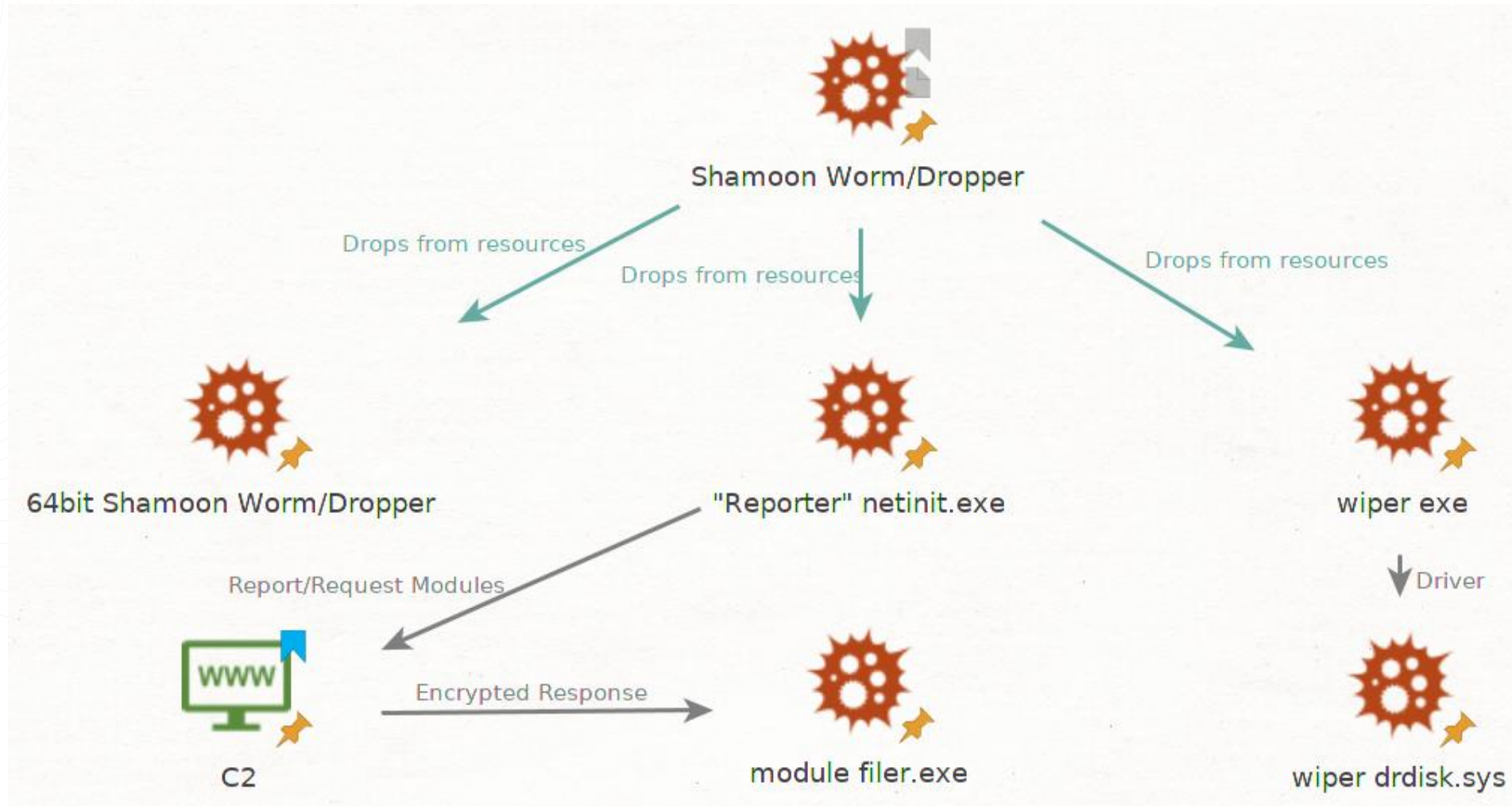


- Se infiltran en Saudi Aramco
- Infectan +30000 equipos con SHAMOON
- 15 de Agosto, Saudi Aramco deja de operar
- Al mes, casi sin stock de HD a nivel mundial
- + variantes → no solo Oriente Medio

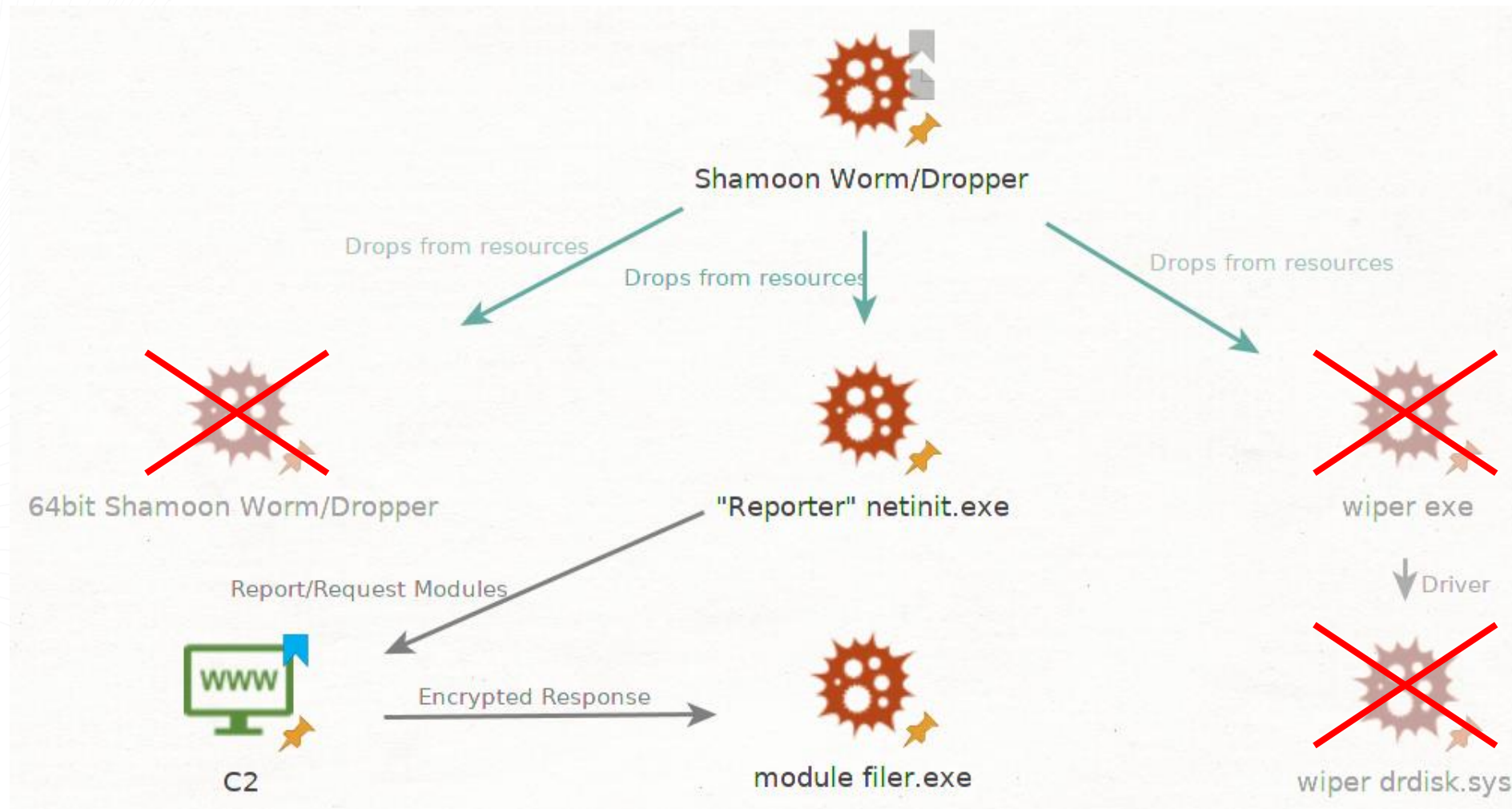
5. Needle\$ in a haystack

- Análisis de las dos familias en paralelo
- Droppers y DLLs
- Fork o reutilización de componentes
- Complica el funcionamiento

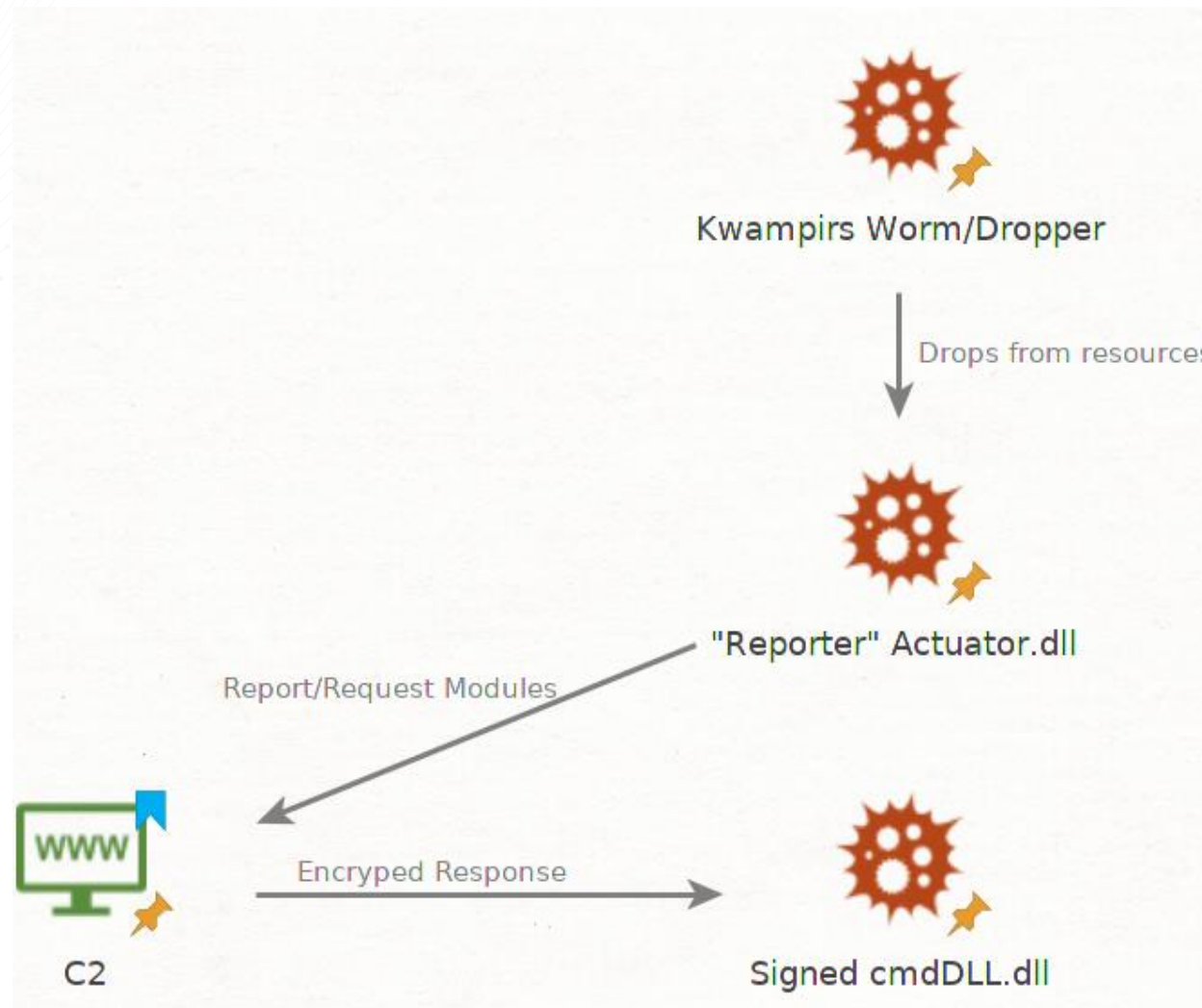
5. Needle\$ in a haystack



5. Needle\$ in a haystack



5. Needle\$ in a haystack



5. Needle\$ in a haystack

- Parece un fork mejorando técnicas
- Mismas APIS
- Metadatos

5. Needle\$ in a haystack

- Rich headers de Droppers **Kwampirs** | **Shamoon**

```
python rich.py wmiapsvre_exe|sort -n
Checksum valid
PROPID  name          build count
    1   Import0         0    133
   147   Implib900      30729    9
   154   Cvtres1000     30319    1
   157   Linker1000     30319    1
   158   Masm1000       30319   16
   170   Utc1600_C      30319  101
   171   Utc1600_CPP    30319   40
   175   Utc1600_LTCG_CPP 30319    5
```

```
python rich.py shamoon_exe|sort -n
Checksum valid
PROPID  name          build count
    1   Import0         0    134
   147   Implib900      30729   13
   154   Cvtres1000     30319    1
   157   Linker1000     30319    1
   158   Masm1000       30319   16
   170   Utc1600_C      30319  117
   171   Utc1600_CPP    30319   50
```

- También coinciden payloads (DLL/Exe)..

5. Needle\$ in a haystack

- Metadatos versiones Droppers Kwampirs | Shamoon

```
1 1 VERSIONINFO
2 FILEVERSION 5,3,3790,3959
3 PRODUCTVERSION 5,3,3790,3959
4 FILEOS 0x40004
5 FILETYPE 0x1
6 {
7 BLOCK "StringFileInfo"
8 {
9     BLOCK "040904b0"
10    {
11        VALUE "CompanyName", "Microsoft Corporation"
12        VALUE "FileDescription", "WMI Performance Adapter Service Extension"
13        VALUE "FileVersion", "5.3.3790.3959 (srv03_sp3_rtm.070216-1710)"
14        VALUE "InternalName", "WmiApSrv.exe"
15        VALUE "LegalCopyright", "© Microsoft Corporation. All rights reserved."
16        VALUE "OriginalFilename", "WmiApSrv.exe"
17        VALUE "ProductName", "Microsoft® Windows® Operating System"
18        VALUE "ProductVersion", "5.3.3790.3959"
19    }
20 }
21 }
22 BLOCK "VarFileInfo"
23 {
24     VALUE "Translation", 0x0409 0x04B0
25 }
26 }
27 }
```

```
1 1 VERSIONINFO
2 FILEVERSION 5,2,3790,0
3 PRODUCTVERSION 5,2,3790,0
4 FILEOS 0x40004
5 FILETYPE 0x1
6 {
7 BLOCK "StringFileInfo"
8 {
9     BLOCK "040904b0"
10    {
11        VALUE "CompanyName", "Microsoft Corporation"
12        VALUE "FileDescription", "Distributed Link Tracking Server"
13        VALUE "FileVersion", "5.2.3790.0 (srv03_rtm.030324-2048)"
14        VALUE "InternalName", "Distributed Link Tracking Server"
15        VALUE "LegalCopyright", "© Microsoft Corporation. All rights reserved."
16        VALUE "OriginalFilename", "trksvr"
17        VALUE "ProductName", "Microsoft® Windows® Operating System"
18        VALUE "ProductVersion", "5.2.3790.0"
19    }
20 }
21 }
22 BLOCK "VarFileInfo"
23 {
24     VALUE "Translation", 0x0409 0x04B0
25 }
26 }
27 }
```

5. Needle\$ in a haystack

- Propagación Shamoon | Kwampirs

```
do
{
next_addr_in_list = (const char *)&hostent_struct->h_addr_list[next_addr_in_list_idx];
if ( !*next_addr_in_list )
break;
copy_to_from_sz((int *)&in, *next_addr_in_list, hostent_struct->h_length, *next_addr_in_list, &in);
last_octet_of_current_host = in.S_un.S_un_b.s_b4;
last_octet_idx = 1;
do
{
if ( last_octet_of_current_host != last_octet_idx )
{
in.S_un.S_un_b.s_b4 = last_octet_idx;
addr_in_ascii = inet_ntoa(in);
len_addr_in_ascii = strlen(addr_in_ascii);
if ( (unsigned int)(len_addr_in_ascii - 1) <= 18 )
{
strncpy(addr_in_ascii_ptr_copy, &target_ip, len_addr_in_ascii);
propagate_to_ip((const WCHAR *)&local_file_path, (const
}
}
}
}
}
while ( last_octet_idx < 255u );
++next_addr_in_list_idx;
}
while ( next_addr_in_list_idx < 10 );
WSACleanup();

// Why limiting

while ( next_addr_in_list_idx < 10 )
{
next_addr_in_list = (int *)&hostent_struct->h_addr_list[next_addr_in_list_idx];
if ( !*next_addr_in_list )
break;
copy_sz_from_to(hostent_struct->h_length, *next_addr_in_list, &in);
last_octet_of_current_host = in.S_un.S_un_b.s_b4;
if ( in != 0x100007F )
{
for ( last_octet_idx = 1; last_octet_idx < 255u; ++last_octet_idx )
{
if ( last_octet_of_current_host != last_octet_idx )
{
in.S_un.S_un_b.s_b4 = last_octet_idx;
addr_in_ascii = inet_ntoa(in);
len_addr_in_ascii = strlen(addr_in_ascii);
if ( (unsigned int)(len_addr_in_ascii - 1) <= 18 )
{
strncpy(&target_ip_optimized_out, len_addr_in_ascii, addr_in_ascii);
propagate_to_ip(*(const WCHAR **)&local_file_path, // target_ip_optimized_out
// propagate_to_ip but the
// decompiler doesn't display
}
}
}
}
}
hostent_struct = hostent_struct;
}
++next_addr_in_list_idx;
}
ms_exc.registration.TryLevel = -2;
WSACleanup();
```

5. Needle\$ in a haystack

- Infección Kwampirs

```
copy_sz_from_to(4, (int)L"\\", (BYTE *)NewDestFileName); // NewDestFileName = "\\\"
IP_STR_size = strlen_unicode_wcslen(IP_STR);
copy_sz_from_to(2 * IP_STR_size, (int)IP_STR, str_container); // str_container = "A.B.C.D" (an ip addr)
IP_STR_size_2 = strlen_unicode_wcslen(IP_STR);
copy_sz_from_to(2, (int)L"\\", &str_container[2 * IP_STR_size_2]); // str_container = "A.B.C.D\\"
v64[strlen_unicode_wcslen(IP_STR)] = 0;
size_prefix = strlen_unicode_wcslen((BYTE *)NewDestFileName); // vars are contiguous, so in unicode is the length of \\A.B.C.D\
size_prefix_in_bytes = 2 * size_prefix;
memcpy(&slashes_ip_admin_system32_csrss_exe[0], 2 * size_prefix);
for ( hidden_path_index = 0; ; ++hidden_path_index ) // iterates the possible hidden paths
{
    if ( hidden_path_index >= 4 )
    {
        result = 0;
        ms_exc.registration.TryLevel = -2;
        return result;
    }
    len_str_hidden_paths$ = strlen_unicode_wcslen((_BYTE *)hidden_paths[hidden_path_index]);
    memcpy_0(
        (char *)slashes_ip_admin_system32_csrss_exe + size_prefix_in_bytes,
        hidden_paths[hidden_path_index],
        2 * len_str_hidden_paths$);
    len_system32_csrss_exe_in_bytes = 2 * strlen_unicode_wcslen((_BYTE *)L"\\system32\\csrss.exe");
    len_str_admin$ = strlen_unicode_wcslen((_BYTE *)hidden_paths[hidden_path_index]);
    memcpy_0(
        &slashes_ip_admin_system32_csrss_exe[size_prefix + len_str_admin$],
        L"\\system32\\csrss.exe",
        len_system32_csrss_exe_in_bytes);
    strlen_unicode_wcslen((_BYTE *)hidden_paths[hidden_path_index]);
    slashes_ip_admin_system32_csrss_exe[size_prefix_plus_size_str_admin
        + strlen_unicode_wcslen((_BYTE *)L"\\system32\\csrss.exe")] = 0;
    if ( create_file_disable wow64fs_redir(slashes_ip_admin_system32_csrss_exe) // test if writable
```

5. Needle\$ in a haystack

- Infección Shamoon

```
copy_to_from_sz((int)NewDestFileName, (const char *)L"\\\\\\", 4, &unk_416804); // NewDestFileName = "\\\\\\"
IP_STR_size = strlen_unicode_wcslen((int)IP_STR);
copy_to_from_sz((int)str_container, (const char *)IP_STR, 2 * IP_STR_size); // str_container = "A.B.C.D" (an ip addr)
//
IP_STR_size_2 = strlen_unicode_wcslen((int)IP_STR);
copy_to_from_sz((int)&str_container[2 * IP_STR_size_2], (const char *)L"\\", 2); // str_container = "A.B.C.D\\"
v46[strlen_unicode_wcslen((int)IP_STR)] = 0;
nullsub_1();
size_prefix = strlen_unicode_wcslen((int)NewDestFileName); // vars are contiguous, so in unicode is the length of \\A.B.C.D\
size_prefix_ = size_prefix;
size_prefix__ = size_prefix;
memcpy(&slashes_ip_admin_system32_csrss_exe, NewDestFileName, 2 * size_prefix);
hidden_path_index = 0;
hidden_paths_ = hidden_paths;
while ( 1 ) // iterates the possible hidden paths
{
    len_str_hidden_path$ = strlen_unicode_wcslen((int)hidden_paths_);
    memcpy(&slashes_ip_admin_system32_csrss_exe[size_prefix_], hidden_paths_, 2 * len_str_hidden_path$);
    len_system32_csrss_exe_in_bytes = 2 * strlen_unicode_wcslen((int)L"\\system32\\csrss.exe");
    len_str_admin$ = strlen_unicode_wcslen((int)hidden_paths_);
    memcpy(
        &slashes_ip_admin_system32_csrss_exe[size_prefix__ + len_str_admin$],
        L"\\system32\\csrss.exe",
        len_system32_csrss_exe_in_bytes);
    len_str_admin$ = strlen_unicode_wcslen((int)hidden_paths_);
    slashes_ip_admin_system32_csrss_exe[size_prefix__
        + len_str_admin$
        + strlen_unicode_wcslen((int)L"\\system32\\csrss.exe")] = 0;
    if ( create_file_disable_wow64fs_redir(slashes_ip_admin_system32_csrss_exe) ) // tests if writable
```

5. Needle\$ in a haystack

- Instalación servicio remoto
- Recursos y Fechas
- Bugs y singularidades (10 adapt., len. 18, “cout random..”)
- Ojo! **No** es versión de SHAMOON, parece fork o reutilización de componentes

5. Needle\$ in a haystack

- **Atribuir, a nivel técnico, es muy complicado**
- **En ocasiones imposible**



1. Orangeworm
2. Markel y Yara
3. Paul y el CTF de Suricon
4. Cheating en otro CTF
5. Needle\$ in a haystack
6. Es elfin?

6. Es elfin?

Noviembre 2019, Holanda (Suricon 2019)

- Symantec → “**Elfin**” → atribución autoría Shamoon
- FireEye, Mitre/Att&ck → “**APT33**” (**IRÁN**)
- Shamoon → “**The Cutting Sword of Justice**”
- A nivel técnico Kwampirs → sólo relación con SHAMOON

ARABIA SAUDÍ ›

Arabia Saudí interrumpe la mitad de su producción de crudo tras un ataque con drones

Estados Unidos acusa directamente a Irán como responsable



- Diez drones cargados de explosivos
- 2 principales instalaciones → al 50%
- Arabia Saudi → atribuye a Irán

6. Es elfin?

- Contexto geopolítico encajaría; Sin embargo...
- Cargador de DLL → Lazarus, Sofacy y otros
- Imagen en recurso → **Lazarus**, olympic destroyer
- Shamoan 3 → kwampirs
- Atribución incierta

No podemos afirmar origen

Pero podemos afirmar que se basa en SHAMOON

Orangeworm:

How I met your master...

BRANCH

Eso es todo!

Agradecimientos a:

- Markel Picado
- Paul Bakoyiannis

GRACIAS !



@PabloForThePPL





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**

