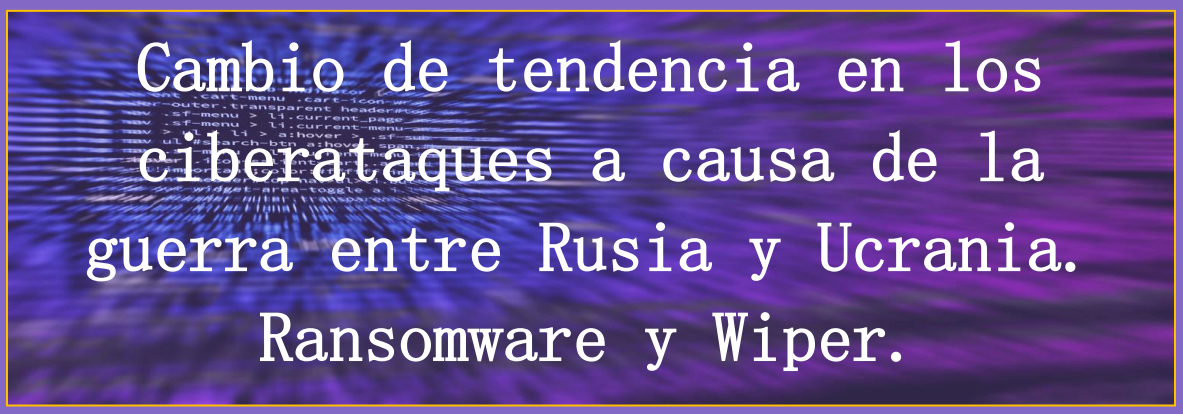
isoph
CyberIntelligence

Cambio de tendencia en los ciberataques a causa de la guerra entre Rusia y Ucrania. Ransomware y Wiper.



Daniel Pérez Cáceres - Técnico en Ciberinteligencia

Resumen

En el presente informe se detalla la tendencia de ciberataques llevada a cabo durante el 2021, en la que el uso de Ransomware destaca notoriamente. Este punto se ha introducido para comprender el cambio de tendencia en el ámbito de los ciberataques a causa de la iniciación del conflicto bélico entre Rusia y Ucrania.
En la actualidad, se destaca el uso de malware tipo *Wiper*, cuya única finalidad es la destrucción y borrado masivo de datos de los sistemas comprometidos.
Además,se lleva a cabo un análisis de los TTP seguidos por actores rusos y se proporcionan distintas guías para evitar, detectar o hacer frente a un incidente de esta índole.

Introducción

En este apartado se dará la información básica sobre Ransomware y Wipper´s para que el lector tenga un conocimiento completo sobre los ataques llevados a cabo, su funcionamiento, en qué consisten.

¿Qué es el Ransomware?

Ransomware, cuya traducción al castellano hace referencia a "malware de rescate", es un tipo de malware que una vez habiendo infectado un dispositivo, encripta toda la información del mismo haciendo que estos datos sean inaccesibles, exigiendo un pago de rescate para poder llegar a recuperarlos, al igual que en un secuestro.
En la actualidad estos pagos de rescate suelen exigirse mediante criptomonedas (Bitcoin o Monero entre muchas otras), dificultando de esta manera la rastreabilidad del actor que ha llevado a cabo esta actividad fraudulenta.
Además, para meter presión al ataque, los actores de amenazas advierten a las víctimas de que si no reciben el pago en un tiempo determinado, venderán sus datos a terceros, ya que han sido obtenidos mediante *"infostealers"*.
Su principal motivación es la económica.

Vía de infección de Ransomware

La infección en una gran mayoría de los casos suele ser llevada a cabo mediante *"Malspam"* (malware spam). Esta etiología de infección consiste en la recepción de mensajes no deseados que utilizan malware embebido en archivos corruptos, que pueden estar en formato .pdf o .doc. Además de contener archivos maliciosos, también se puede infectar a un usuario mediante el acceso a enlaces web cargados con malware.

Este modo de propagación utiliza distintas técnicas de ingeniería social para manipular a los usuarios con el principal fin de que se lleve a cabo la infección con éxito.

¿Qué son los Wiper?

Los *Wiper*, o también conocidos como "limpiaparabrisas", es uno de los tipos de amenazas que pueden llegar a comprometer en mayor medida a una organización actualmente. Esto se debe a que afecta a toda la información que se encuentre en el dispositivo infectado, siendo su principal objetivo realizar un borrado efectivo de la memoria o disco comprometido.

La única manera de hacer frente a esta amenaza consiste en realizar backups periódicamente, para que de esta manera poder restaurar la mayor cantidad de datos posibles, en el caso de que la organización se haya visto afectada mediante esta etiología de ciberataque.

Vía de infección de malware Wiper

Al igual que con el Ransomware, la principal vía de entrada de una amenaza Wiper es el malspam. En estos correos electrónicos se adjuntan archivos o enlaces corruptos que, al abrirlos o acceder a ellos, infecta el dispositivo desencadenando de esta manera un borrado masivo de datos.

Tendencia de ataques durante el 2021

En la alerta (AA22-040A) de CISA, se destaca que distintas autoridades cibernéticas de países como EE.UU, Australia o Reino Unido, observaron cómo a lo largo del 2021 se ha visto un aumento exponencial de los denominados ataques de ransomware de alto impacto contra infraestructuras críticas en todo el mundo.

- FBI, CSI Y NSA reportaron que 14 de los 16 sectores de infraestructuras críticas de EE.UU., reportaron a lo largo del 2021 al menos un ataque relacionado con ransomware.
    - Algunas de las organizaciones afectadas fueron la Base Industrial de Defensa, los servicios de emergencia, instalaciones gubernamentales y sectores de tecnología de la información.
- El ACSC[1] notificó que el ransomware sigue atacando a infraestructuras críticas australianas, como lo son los sectores de atención médica, servicios y mercados financieros, organizaciones de educación superior e investigación y energía.
- El NCSC-UK[2] aseguró que el ransomware representa la mayor amenaza cibernética a la que el Reino Unido hace frente.
    - Tanto organizaciones relacionadas con el sector de la educación, como empresas, organizaciones benéficas y servicios públicos de la salud entre otros, se han visto afectados por ataques atribuidos a actores de ransomware, en especial el primer sector mencionado.

Las tácticas y técnicas utilizadas en 2021 han evolucionado con respecto al pasado, demostrando el mayor conocimiento y sofisticación de los actores de amenaza de ransomware, siendo *"Conti"* y *"LockBit"* las operaciones de ransomware más prolíficas. Se ha observado una tendencia sobre todo a finales de 2021 de una rápida explotación de vulnerabilidades críticas, como lo es el fallo de seguridad de *"Log4shell"*.

[1] Centro de Seguridad Cibernética Australiana.

[2] Centro Nacional de Seguridad Cibernética del Reino Unido.

Han aparecido nuevos actores ransomware debido al gran beneficio económico que aporta este tipo de ataques a los grupos de amenazas, usando el modelo de "doble extorsión"[3] para proporcionar presión adicional a las organizaciones a la hora de realizar el pago. Además de esto, ha existido un cambio en las tácticas y técnicas de ataque pasando a ser los sistemas Linux un nuevo objetivo, lo que aumenta exponencialmente el riesgo a aquellas organizaciones que usan este sistema operativo para dar servicio o alojar sus datos calificados como críticos.

Este cambio de tácticas también implica el reclutamiento de insiders[4], obteniendo de esta manera información privilegiada y violando las redes corporativas de un objetivo.

- Se ponen en contacto con clientes de las víctimas para exigir el pago del rescate.
- Amenaza con ataque de denegación de servicios (DDoS).
- Atacar a cadenas de suministro o proveedores para amplificar los efectos nocivos del ataque.

Los actores de amenazas han utilizado ransomware como "*Avaddon*", "*REvil*", "*DarkSide*" y "*BlackMatter*". Tras cerrar estas operaciones se ha detectado una asociación de una gran parte de los grupos con Conti y LockBit, contribuyendo de esta manera a que se conviertan en los RaaS[5] más activos de 2021.

Detalles técnicos

A continuación, se enumeran las siguientes tendencias seguidas por los ciberdelincuentes y que han sido notificadas por los organismos oficiales mencionados anteriormente:

- **Obtención de acceso mediante Phishing, robo o ataques de fuerza bruta contra credenciales de protocolos de escritorio remoto (RDP) y explotación de vulnerabilidades.**
- **Contratación de ciberdelincuentes para llevar a cabo un servicio (RaaS).**
- **Compartir la información obtenida de la víctima.**
- **Uso de extorsión mediante distintos enfoques:**

[3] Hacer inaccesibles los datos comprometidos y amenazar con la publicación o la venta de los mismos en la Dark Web.

[4] Persona que trabaja dentro de una empresa u organización y que vende información crítica de la misma para obtener un beneficio económico.

[5] Ransomware as a Service.

- Amenaza con divulgar la información sensible.
- Interrumpir acceso a Internet y la actividad de la víctima.
- Informar a los socios, accionistas y proveedores de la víctima sobre el incidente, consiguiendo así una pérdida de confianza sobre el mismo.

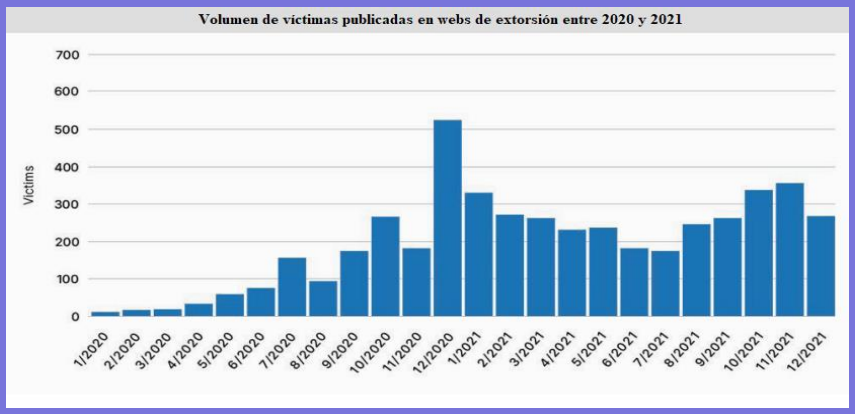
Además de estos puntos, los grupos ransomware han aumentado su impacto de la siguiente manera:

- **Explotación de vulnerabilidades conocidas de aplicaciones y cuentas en la nube.**
  - Obtienen acceso a la nube al comprometer dispositivos locales y dan la posibilidad de moverse lateralmente en dichos sistemas, pudiendo acceder a datos sensibles.
- **Ataque a proveedores de servicios**: Pudiendo tener acceso a múltiples víctimas mediante un solo ataque.
- **Ataque a procesos industriales.**
- **Ataque a la cadena de suministro del software.**
  - Para comprometer y extorsionar a sus clientes.
- **Atacar a organizaciones durante días festivos y fines de semana.**

Estadística

Para observar la tendencia de aumento exponencial de ataques de Ransomware en 2021, se adjunta una tabla representativa del volumen de víctimas publicadas en páginas de extorsión entre 2020 y 2021. A pesar de los distintos picos existentes, es clara la tendencia alcista desde el año 2020 en esta etiología de ataque.

Figura 1:



(Fuente: The Record)

En la siguiente gráfica se representa el número de víctimas publicadas en webs de extorsión de cada operador de Ransomware a lo largo de 2021, identificando de esta manera los más activos.

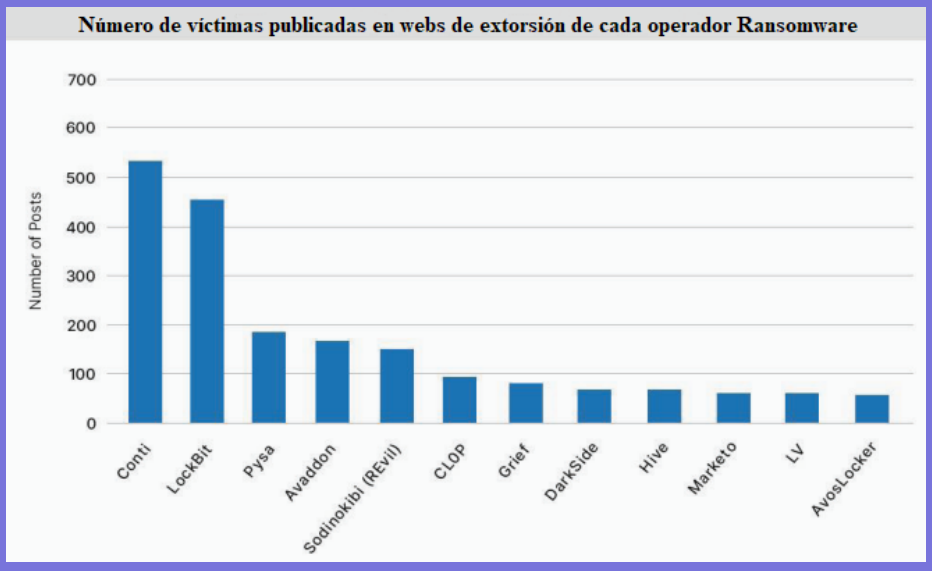


Figura 2: (Fuente The Record)

TTP´s de MITRE ATT&CK usados

TTP	Detalles
T1486 (Encriptación de datos para impacto)	Es la técnica más usada en 2021 debido al gran volumen de ataques ransomware a lo largo del año.
T1082 (Descubrimiento de información del sistema)	Se produce la detección de información del sistema cuando un actor de amenazas intenta obtener información detallada sobre el funcionamiento del sistema y hardware. El descubrimiento es comúnmente realizado por varios malware para recopilar información sobre un dispositivo infectado. Grupo Insikt lo ha observado en uso por bajo nivel y actores sofisticados por igual en todo 2021.
T1055 (Inyección de proceso)	La inyección de procesos implica ejecutar código personalizado dentro del espacio de direcciones de otro proceso. La inyección de proceso ha sido una técnica popular por sus beneficios de evasión (disfraz de comportamiento malicioso como procesos legítimos). A lo largo de 2021, observamos esto técnica utilizada junto con varias cargadores y goteros shellcode.
T1027 (Información o documentos ofuscados)	Ofuscación de archivos o documentos para dificultar el descubrimiento de un ejecutable mediante encriptación. Sirve para evadir sistemas de defensa.
T1005 (Datos del sistema local)	Los actores de amenazas a menudo buscarán exfiltrar estos datos antes del cifrado, en el caso de obtenerlos. Además la usan para extorsionar.

Tendencia actual de ciberataques debido a la guerra entre Rusia y Ucrania

A continuación, se adjunta una imagen en la que se ha sintetizado la cronología de las ciberoperaciones llevadas a cabo por actores a favor de Rusia contra Ucrania, desde el inicio del conflicto.

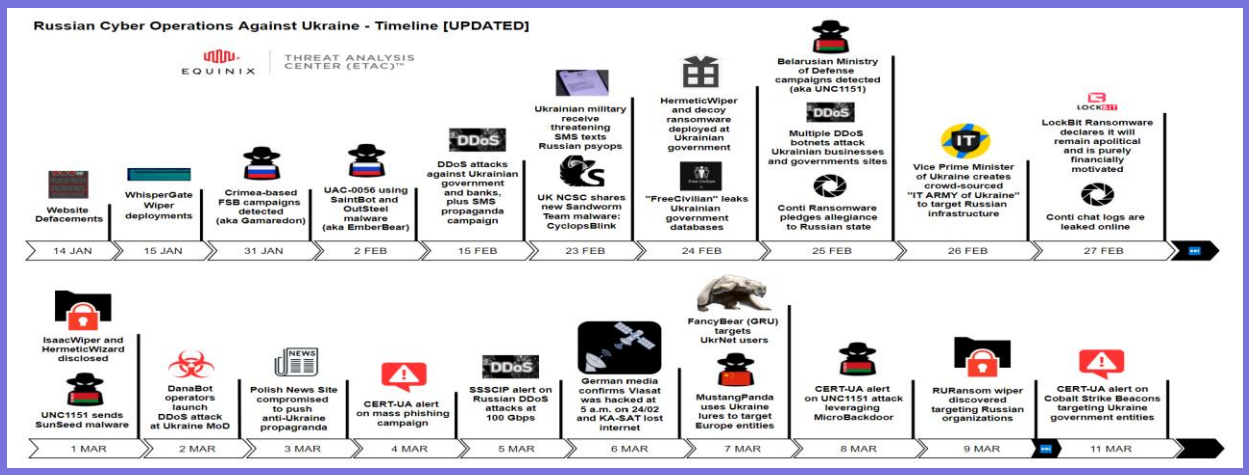


Figura 3: (Fuente: Equinix)

Ataques Pro-Rusia

Campaña DDoS

A principios de febrero, una serie de ataques DDoS se distribuyeron contra sitios web ucranianos. Estos tenían un carácter bancario y de defensa dentro del país; y los ataques se han atribuido al GRU, la agencia de inteligencia militar rusa.

A lo largo de marzo, esta etiología de ataques se ha estado produciendo de forma intermitente, descubriendo que los actores de amenaza prorrusos han utilizado *"DanaBot"*, una plataforma de *"MaaS"*[6] para lanzar ataques de denegación de servicios contra la web del Ministerio de Defensa ucraniano.

[6] Malware as a service: Plataforma que provee a sus clientes de malware, la infraestructura y los recursos necesarios para realizar un ciberataque.

Whispergate

Es un malware de tipo Wiper que se introdujo en los sistemas ucranianos el pasado 13 de enero, con anterioridad al inicio del conflicto bélico. Este malware se disfraza como un Ransomware, ofreciendo a las víctimas la posibilidad de descifrar sus datos a través de un pago, pero realmente se borraban todos los datos del sistema.

El Wiper ha sido hallado en sistemas repartidos por toda Ucrania, entre las que se encuentran el Ministerio de Relaciones Exteriores y distintas redes utilizadas por el gabinete ucraniano.

- Este Wiper comparte similitudes con *"NotPetya"*, otro Wiper que afectó a Ucrania en 2017.

HermeticWiper

El 23 de febrero de 2022 se detectó una nueva campaña de ataques usando malware tipo Wiper, denominándose HermeticWiper.

Con este Wiper se implementaron otras piezas de malware, como el ransomware de señuelo *"PartyTicket"* o, un gusano utilizado principalmente para propagar el HermeticWiper.

Este malware se distribuyó más allá de las fronteras ucranianas, pudiendo haber afectado a los sistemas de algunos países bálticos.

- Este Wiper tiene similitudes con campañas lanzadas en el pasado por el APT ruso *"Sandworm"*.

IsaacWiper

Este malware tipo Wiper fue lanzado por actores rusos el 24 de febrero de 2022, el mismo día que se inició la guerra entre Rusia y Ucrania.

Esta campaña se inició justo después de los ataques realizados con HermeticWiper.

- Se sospecha que los atacantes consiguieron infiltrarse en las redes objetivo con anterioridad, moviéndose lateralmente en ellas e infectando los sistemas.
- Se lanzó una segunda versión el 25 de febrero, por lo que es probable que no alcanzaron sus objetivos con la primera versión.

Phishing dirigidos a militares ucranianos

El 25 de febrero de 2022, CERT-UA[7] acusó al grupo UNC1151 patrocinado por el estado Bielorruso por intentar obtener las credenciales de cuentas de correo electrónico relacionadas con el personal militar Ucraniano mediante una campaña de Phishing.

En los casos exitosos, aprovecharon esas cuentas para propagar correos maliciosos a las listas de contactos de las direcciones violadas.

También se relaciona a UNC1151 con otra campaña de phishing denominada *"Asylum Ambuscade"*, que también usó correos militares ucranianos comprometidos para atacar a personas relacionadas con el sector del transporte, la asignación financiera, la administración y el movimiento de refugiados ucranianos dentro de Europa, en un intento de obtener información sobre el movimiento de fondos, suministros y personas dentro de los países miembros de la OTAN. Este ataque contenía malware *"SunSeed"*, comprometiendo de esta manera a los objetivos.

- SunSeed es un script malicioso de Lua.
- Usa ingeniería social para la entrega del malware.

CaddyWiper

El 14 de marzo de 2022 se detectó una nueva campaña en la que se usa un malware tipo Wiper, que no comparte ninguna característica con HermeticWiper o IsaacWiper.

CaddyWiper tiene un potencial más destructivo que los anteriores, en los que además de realizar un borrado masivo de datos, evita borrar información de los controladores de dominio. Esto puede deberse a que es una forma en la que los actores de amenazas mantengan el acceso a la organización mientras siguen realizando distintas acciones.

- Se conoce que CaddyWiper se ha propagado a través de GPO[8], en el que en uno de los casos se abusó del GPO de una red para propagar dicho malware. Esto sugiere que los atacantes tenían acceso a los servicios de *"Active Directory"* previa implementación del malware.

[7] Equipo de Respuesta a Emergencias Informáticas de Ucrania.

[8] *Microsoft Group Policy Objects.*

Interrupción Viasat

El proveedor de Internet vía satélite, Viasat, fue atacado el 24 de febrero de 2022, provocando cortes de comunicaciones que se extendieron no sólo a Ucrania, sino también a distintos países europeos como Alemania.

Los atacantes explotaron un dispositivo VPN mal configurado, obteniendo de esta manera acceso al segmento de administración de la red KA-SAT, moviéndose lateralmente en ella.

El siguiente paso consistió en ejecutar comandos de administración legítimos y específicos en una gran cantidad de módems residenciales simultáneamente.

- Estos comandos sobrescribieron datos clave en la memoria flash de los modem, haciendo que estos no pudieran acceder a la red.

DoubleZero

CERT-UA lanzó una alerta sobre un nuevo Wiper cuya campaña comenzó el 17 de marzo de 2022.

En este caso los actores de amenazas se han servido de ataques phishing para entregar el malware a los objetivos, en los que sobrescribirá el contenido del sistema y eliminará distintos registros de Windows previamente a ser apagado.

- Primeramente, sobrescribe todos los archivos que no pertenecen al sistema en todos los discos.
- Después se realiza la reescritura de la lista de ficheros del sistema.
- Se destruyen distintas ramas de registro de Windows: HKCU, HKU, HKLM, HKLM \ BCD.
- Finalmente se apaga el sistema.

AcidRain Wiper

Este malware tipo Wiper ha sido detectado el día 15 de marzo de 2022. Para el acceso realiza un intento de fuerza bruta, infiriendo que los desarrolladores del mismo no tengan conocimientos sobre el firmware destino.

Acto seguido, realiza un borrado en profundidad del sistema de archivos y de archivos pertenecientes a dispositivos de almacenamiento conocidos.

Después de esto, busca destruir archivos de los siguientes dispositivos de almacenamiento:

- /dev/sd*
- /dev/mtdblock*
- /dev/block/mtdblock*
- /dev/mtd*

- /dev/mmcblk*
- /dev/block/mmcblk*
- /dev/loop*

Grupos prorrusos más significativos

- **UNC1151 / Ghostwriter**

A este actor bielorruso se le relaciona con el ciberataque llevado a cabo contra 70 páginas web del gobierno ucraniano, perpetrado el 14 de enero de 2022. En este ciberataque se desfiguraron dichas páginas objetivo. Debido al resultado conseguido y teniendo en cuenta los ataques posteriores, se sospecha que esta acción fue realizada para distraer a las autoridades a la hora de llevar a cabo acciones más destructivas.
El 7 de marzo UNC1151 instaló una puerta trasera denominada *"MicroBackdoor"* en los sistemas del gobierno ucraniano. Dicha puerta trasera se caracteriza por estar disponible de manera pública, recibir comandos de un servidor de Comando y Control (C2) y dar la posibilidad de realizar varias actividades.
Por último, son los responsables de la campaña de phishing anteriormente mencionada.

- **APT28**

Este conocido actor de amenazas ruso, APT28 está relacionado con una campaña de phishing dirigida a usuarios de la empresa UKRNet[9]; aunque esta fue interrumpida en el momento en el que el Grupo de Análisis de Amenazas de Google (TAG), detectó dicha campaña.
Este grupo de amenazas se ha atribuido a la unidad militar 26165 del Centro Principal de Servicios Especiales (GTsSS), de la Dirección Principal de Inteligencia (GRU) del Estado Mayor General de Rusia.

- **Gamaredon**

Se detectó que se difundió la puerta trasera *"LoadEdge"* entre organizaciones ucranianas el 20 de marzo de 2022.

[9] Medios de audio y vídeo en línea.

Esta puerta trasera da la posibilidad al actor de amenazas de instalar distintos softwares de vigilancia de actividad y malwares en los sistemas comprometidos.

- **Scarab/ UAC-0026**

Scarab es un actor de amenazas procedente de China, representando de esta manera el primer grupo chino que se conoce que ha entrado en este conflicto.
En la alerta #4244 del 22 de marzo de 2022. CER-UA compartió un breve resumen e IOC´s relacionados con un intento de intrusión por parte de este grupo.

1. Entrega de un archivo comprimido .rar.
2. El archivo contiene un ejecutable, que abre un documento señuelo y suelta un archivo DLL y otro archivo por lotes denominado "officecleaner".
3. La DLL maliciosa se ha denominado "*HeaderTip*".

La propagación de esta campaña se realiza mediante phishing.

- **Sandworm Team**

Sandworm Team es un APT ruso al que se le puede relacionar con la campaña de HermeticWiper.
Además, con fecha de 16 de marzo de 2022, el Centro Nacional de Seguridad Cibernética (NCSC) del Reino Unido, la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA), la Agencia de Seguridad Nacional (NSA) y la Oficina Federal de Investigaciones (FBI) han descubierto que el actor de Sandworm está empleando un nuevo malware conocido como Cyclops Blink. Cyclops Blink parece ser un marco de reemplazo para el virus VPNFilter, que se descubrió por primera vez en 2018 y se dirigió a equipos de red como enrutadores SOHO y dispositivos de almacenamiento conectado a la red (NAS).

TTP de ataques Pro-Rusia

Táctica	Técnica	Procedimiento
Reconocimiento [TA0043]	Escaneo activo: Escaneo de vulnerabilidades [T1595.002]	
		Los actores APT (Advanced Persistent Threat) patrocinados por el estado ruso han realizado escaneos a gran escala para encontrar servidores vulnerables.
	Suplantación de identidad para obtener información [T1598]	Los actores APT patrocinados por el estado ruso han llevado a cabo campañas de phishing para obtener las credenciales de las redes objetivo.
Desarrollo de recursos [TA0042]	Desarrollar Capacidades: Malware [T1587.001]	Los actores APT patrocinados por el estado ruso han desarrollado e implementado malware, incluido el malware destructivo centrado en ICS.
Acceso Inicial [TA0001]	Explotar aplicaciones orientadas al público [T1190]	Los actores de APT patrocinados por el estado ruso se enfocan en las vulnerabilidades conocidas públicamente, así como en los 0day, en los sistemas orientados a Internet para obtener acceso a las redes.
	Compromiso de la cadena de suministro: Compromiso de la cadena de suministro de software [T1195.002]	Los actores de APT patrocinados por el estado ruso han obtenido acceso inicial a las organizaciones de víctimas al comprometer el software confiable de terceros. Los incidentes notables incluyen el software de contabilidad MEDoc y SolarWinds Orion.
Ejecución [TA0002]	Intérprete de comandos y secuencias de comandos: PowerShell [T1059.003] y Windows Command Shell [T1059.003]	Los actores APT patrocinados por el estado ruso han utilizado cmd.exe para ejecutar comandos en máquinas remotas. También han usado PowerShell para crear nuevas tareas en máquinas remotas, identificar ajustes de configuración, filtrar datos y ejecutar otros comandos.

Persistencia [TA0003]	Cuentas válidas [T1078]	Los actores APT patrocinados por el estado ruso han utilizado las credenciales de las cuentas existentes para mantener un acceso persistente a largo plazo a las redes comprometidas.
Credencial de Acceso [TA0006]	Fuerza bruta: Búsqueda del acceso de forma secuencial [T1110.001] y accesos tabulados [T1110.003]	Los actores de APT patrocinados por el estado ruso han llevado a cabo campañas de fuerza bruta y por medio de diccionarios.
	Volcado de credenciales del sistema operativo: NTDS [T1003.003]	Los actores APT patrocinados por el estado ruso han extraído credenciales y exportado copias de la base de datos de Active Directory ntds.dit.
	Robar o falsificar tickets de Kerberos: Kerberoasting [T1558.003]	Los actores de APT patrocinados por el estado ruso han realizado "Kerberoasting", mediante el cual obtuvieron los boletos del Servicio de concesión de boletos (TGS) para los nombres principales del servicio de directorio activo (SPN) para el descifrado fuera de línea.
	Credenciales de almacenes de contraseñas [T1555]	Los actores de APT patrocinados por el estado ruso han utilizado credenciales de cuenta previamente comprometidas para intentar acceder a las contraseñas de la cuenta de servicio administrado de grupo (gMSA).
	Explotación para acceso de credenciales [T1212]	Los actores de APT patrocinados por el estado ruso han explotado la vulnerabilidad de Windows Netlogon CVE-2020-1472 para obtener acceso a los servidores de Windows Active Directory.
	Credenciales no seguras: claves privadas [T1552.004]	Los actores APT patrocinados por el estado ruso han obtenido claves de cifrado privadas del contenedor de Servicios de federación de Active Directory (ADFS) para descifrar los certificados de firma SAML (Security Assertion Markup Language) correspondientes.

Comando y Control [TA0011]	Proxy: Proxy multisalto [T1090.003]	Los actores APT patrocinados por el estado ruso han utilizado servidores privados virtuales (VPS) para enrutar el tráfico a los objetivos. Los actores a menudo usan VPS con direcciones IP en el país de origen de la víctima para ocultar la actividad entre el tráfico de usuarios legítimos.

Tabla 1: (Fuente: CISA)

CVE´s explotados por APT´s rusos

CVE	Detalle
CVE-2018-13379	FortiGate VPNs
CVE-2019-1653	Cisco router
CVE-2019-2725	Oracle WebLogic Server
CVE-2019-7609	Kibana
CVE-2019-9670	Zimbra software
CVE-2019-10149	Exim Simple Mail Transfer Protocol
CVE-2019-11510	Pulse Secure
CVE-2019-19781	Citrix
CVE-2020-0688	Microsoft Exchange
CVE-2020-4006	VMWare
CVE-2020-5902	F5 Big-IP
CVE-2020-14882	Oracle WebLogic
CVE-2021-26855	Microsoft Exchange

Tabla 2: (Fuente: CISA)

Ataques Pro-Ucrania

RuRansom Wiper

Representa el primer malware Wiper usado por hacktivistas proucranianos. A pesar de que el nombre infiere que podría ser un ransomware, este funciona como un Wiper ya que destruye archivos cifrados del sistema infectado.

Este malware analiza la IP del sistema comprometido, en el que solo actuará si llega a geolocalizarse en Rusia.

Este malware se propaga como un gusano y se cifra en el momento de haber infectado exitosamente un sistema objetivo, haciendo que el cifrado sea irreversible y no pueda realizarse una recuperación de datos sin un backup.

Existen varias versiones de este Wiper, por lo que es muy probable que se esté desarrollando para actuar de nuevo de una manera más sofisticada.

Ataques DDoS

A lo largo de estas semanas el ejército TI ucraniano ha realizado ataques a los servidores de sitios web rusos, inundando el tráfico hasta el punto de dejarlos inutilizados durante un tiempo determinado.

De este tipo de ataques se han visto afectados distintos bancos rusos y páginas web oficiales gubernamentales rusas, como la oficina de Putin; pudiendo llegar a afectar en un futuro cercano a infraestructuras críticas rusas.

Grupos proucranianos más significativos

- Anonymous

El 1 de marzo de 2022, este grupo de hacktivistas declaró la ciberguerra al estado ruso como consecuencia de la iniciación del conflicto bélico en Ucrania.

Anonymous se ha centrado primeramente en medios de comunicación prorrusos, dejando mensajes y videos sobre los actos llevados a cabo en Ucrania, intentado combatir de esta manera una posible desinformación sobre la población civil rusa.

Se ha afirmado que este grupo ha comprometido emisoras de radios rusas, además de canales de televisión como *Russia 24*, *Channel 1*, *Moscow 24* y servicios de transmisión como *Wink* e *Ivi*.

- En ellos se empezaron a mostrar clips sobre hechos ocurridos recientemente en Ucrania.

El 10 de marzo Anonymous anunció el compromiso de los sistemas pertenecientes a *"Roskomnadzor"*, una agencia rusa que es responsable de monitorear y censurar los medios de comunicación estatales.

- **Ejército TI ucraniano**

Este "ejército" se compone de voluntarios repartidos alrededor del mundo, que se coordinan a través de distintas redes sociales y canales como Telegram, aprovechándose de las ventajas de privacidad y difusión que proporciona esta plataforma.

En estos canales de comunicación se publican numerosos objetivos que buscan ser atacados por este grupo de voluntarios, utilizando detalles proporcionados para lanzar ataques. Este actor es responsable de numerosos ataques DDoS realizados contra páginas web que representan intereses rusos.

- **Cyber Partisans**

Es un grupo centrado en Bielorrusia, atacó primeramente en enero, sucediéndose durante el mes de febrero, los sistemas ferroviarios de Bielorrusia, como protesta por el despliegue de tropas rusas en el país.

Principalmente se centraron en atacar las webs que venden los tickets de acceso al metro.

Lista completa de grupos activos en la ciberguerra

GROUP	SUPPORTS	TYPE	COMMS	LOC
Anonymous Associated				
Anonymous	Ukraine	DDoS/Hack	Twitter	UNK
BlackHawks	Ukraine	DDoS/Hack	Twitter	Georgia
Anon Liberland & PWN-BAR	Ukraine	DDoS/Hack	UNK	UNK
LiteMods	Ukraine	Psyops/DDoS	Twitter	UNK
SHDWSec	Ukraine	Hackivism	Twitter	UNK
RootUser	Ukraine	Radio	Twitter	Ukraine
N3UR0515	Ukraine	DDoS	Twitter	UNK
PuckArks	Ukraine	Pysops	Twitter	UNK
GrenXPaRTa_9haan	Ukraine	Databreach	Twitter	Indonesia
YourAnonNews	Ukraine	Psyops	Twitter	UNK
DeepNetAnon	Ukraine	Radio/hack	Twitter	UNK
Anonymous Younes	Ukraine	DDoS/Hack	Twitter	UNK
0xAnonLeet	Ukraine	DDoS/hack	Twitter	UNK
AnonGh0st	Ukraine	DDoS/Hack	Twitter	UNK
Anonymous Romania	Ukraine	DDoS/Hack	Twitter	Romania
Shadow_Xor	Ukraine	Databreach	Twitter	UNK
PuckArks	Ukraine	Defacement	Twitter	UNK
Vest1geSec	Ukraine	Hack/DDoS	Twitter	UNK
Squad303	Ukraine	DDoS/psyops	Twitter	Poland
AlphaDisiak	Ukraine	Ransomware	Twitter	UNK
GhostSec	Ukraine	Hack	Telegram	UNK
DDoS Secrets	Ukraine	Databreach	Twitter	UNK
Nation-State				
GhostWriter UNC1151	Russia	Hack	UNK	Belarus
SandWorm	Russia	Hack	UNK	Russia
Gamaredon	Russia	Hack	UNK	Russia
DEV-0586 APT NEW	Russia	Hack	UNK	Russia
DEV-0665 APT NEW	Russia	Hack	UNK	Russia
FancyBear APT NEW	Russia	Hack	UNK	Russia
IT Army of Ukraine	Ukraine	DDoS	Twitter	Ukraine
IT Army of Ukraine Pysops	Ukraine	Pysops	Twitter	Ukraine
Internet Forces of Ukraine	Ukraine	Pysops	UNK	Ukraine
MustandPanda APT NEW	UNK	Hack	UNK	China
Pro-Ukraine Groups				
BlueHornet (ATW return)	Ukraine	Hack	Twitter	UNK
KelvinSecurity Hacking Team	Ukraine	Hack	Twitter	UNK
GNG	Ukraine	DDoS	Twitter	Georgia
NB65	Ukraine	Hack	Twitter	UNK
RaidForums2	Ukraine	DDoS	Twitter	UNK
ContiLeaks	Ukraine	Databreach	Twitter	UNK
GhostClan	Ukraine	DDoS/Hack	Telegram	UNK
1LevelCrew	Ukraine	DDoS	Twitter	UNK
Spot (ATW Return)	Ukraine	Hack	Twitter	UNK
Hydra UG	Ukraine	Radio	Twitter	UNK
SecJuice	Ukraine	OSINT/Psyop	Twitter	UNK
v0g3lSec	Ukraine	Hack	Twitter	UNK
Belarusian Cyber-Partisans	Ukraine	Ransomware	Twitter	Belarus
DDoS Secrets	Ukraine	Databreach	Twitter	UNK
Monarch Turkish Hacktivists	Ukraine	Defacement	UNK	Turkey
Shadow_Xor	Ukraine	UNK	Twitter	UNK
The Connections	Ukraine	UNK	Twitter	UNK
TrickLeaks	Ukraine	Databreach	Twitter	UNK
Crystal_MSF	Ukraine	Hack/DDoS	Twitter	UNK
Rabbit Two	Ukraine	Hack/DDoS	Twitter	UNK
M3moryK1tten	Ukraine	Hack/support	Twitter	UNK
SecDet	Ukraine	Hack	Twitter	US
BeeHive Cybersecurity	Ukraine	Phishing/hack	Twitter	UNK
Cyber_legion_hackers	Ukraine	Defacement	Twitter	UNK
Stand for Ukraine NEW	Ukraine	hack/ DDoS	Telegram	Ukraine
Ring3API NEW	Ukraine	Hack	Twitter	Ukraine
Pro-Russia Groups				
RedBanditsRU	Russia	Hack	Twitter	Russia
Free Civilian	Russia	Databreach	Site	UNK
CoomingProject	Russia	Databreach	Site	UNK
Stormous Ransomware	Russia	Ransomware	Telegram	UNK
Hydra (Was Digital Cobra Gang)	Russia	Dox/DDoS	Twitter	Russia
RaHDit	Russia	Hack	UNk	Russia
Devilix-EU	Russia	UNK	Twitter	Russia
Xaknet	Russia	Hack	Site	Russia
Killnet	Russia	Hack/DDoS	Telegram	Russia
DragOn	Russia	Hijack	Twitter	Russia
404 Cyber Defense	Russia	DDoS	Twitter	UNK
ECO	Russia	DDoS/Hack	Twitter	UNK
WeretheGoons	Russia	Hack	Twitter	Russia
FfboyG	Russia	Psyops/DDoS	Twitter	India
Conti ransomware	Russia	Ransomware	Onion	Russia
punisher_346 NEW	Russia	PsyOps	Twitter	UNK
Lorec53 NEW	Russia	hack	UNK	Russia
DDoS Hacktivist Team NEW	Russia	DDoS	Telegram	Russia
cyberwar_world NEW	Russia	hack/ddos	Telegram	Russia
Tips/Changes https://twitter.com/Cyberknow20				

Figura 4: (Fuente: CyberKnow)

Conclusiones

Actualmente observamos como grupos reducidos de actores de amenazas se sirven de la situación de la guerra para usar phishing, malware o ransomware para obtener un beneficio económico. Esto lo hemos observado mediante canales procrania falsos en Telegram, que usan ingeniería social para estafar económicamente a distintos voluntarios mal informados.

Sin embargo, existe un aumento exponencial en el uso de malware tipo Wiper, existiendo 7 campañas de esta etiología contra Ucrania (WhisperKill, WhisperGate, HermeticWiper, IsaacWiper, CaddyWiper, DoubleZero y AcidRain), y 1 contra Rusia (RuRansom). Este tipo de ataques tienen una clara motivación política, ya que el borrado de datos crea desinformación y puede llegar a parar actividades esenciales de cada estado.

Además, se sigue usando los ataques DDoS contra distintas infraestructuras críticas, con la motivación de paralizar dicha actividad y obtener cierta ventaja en el conflicto. En estos últimos días se están extendiendo estos ciberataques a países relacionados con la OTAN, entrando además APT´s relacionados con China; por lo que es recomendable que todas las organizaciones sigan las siguientes vías para proteger la disponibilidad, confidencialidad e integridad de sus datos y servicios.

Debido a esta guerra, los ciberataques han pasado de tener una motivación económica a una política y estratégica, para obtener cierta ventaja con respecto a otros países en la situación actual.

Guía de detección

1. **Implementar un sistema de recopilación y retención de registros**: Sin este recurso, las organizaciones carecen de capacidad a la hora de investigar incidentes o detectar comportamientos que puedan comprometer el correcto funcionamiento de la misma.
2. **Búsqueda de inicios de sesión sospechosos**: Ya sea por las credenciales del usuario o la geolocalización de la IP.

3. Búsqueda de una IP usada por varias cuentas.
4. Búsqueda de inicios de sesión seguidos desde localizaciones alejadas.
5. Búsqueda de procesos que puedan indicar un volcado de credenciales.
6. Uso sospechoso de cuentas privilegiadas.
7. Actividad inusual de usuarios.

Guía de respuesta ante ataques cibernéticos

1. **Aplicación de parches**: Los APT suelen aprovechar vulnerabilidades de sistemas que están sin parchear. Por lo tanto, la primera pauta de defensa debe ser la correcta gestión y actualización de parches. Las organizaciones deben preocuparse por actualizar debidamente las aplicaciones y servicios de sus sistemas, evitando así una vía de entrada a través de vulnerabilidades incipientes.
    a. En la siguiente página existe un historial de vulnerabilidades, con el fin de que las organizaciones e instituciones mantengan al día la versión de sus sistemas: https://www.cisa.gov/uscert/ncas/alerts/aa22-011a)
2. **Bases de datos de protección**: Con información sobre IOC´s[10] o reglas YARA.
3. **Sistemas críticos de copias de seguridad**: La mejor defensa ante ataques ransomware o wiper, es mantener copias de seguridad actualizadas para poder recomponer los sistemas tras el incidente.
   Estas copias deben mantenerse fuera de línea, ya que si no pueden llegar a ser comprometidas.
4. **Phishing**: Es una de las vías de acceso más populares actualmente, por lo que es recomendable que se lleven a cabo campañas de concientización entre el personal de una organización para evitar en mayor medida ese fenómeno.
5. **Hunt**: Usar TTP conocidos para detectar actividad inusual en los sistemas.
6. **Emular**: Al conocer los TTP de muchos actores de amenazas, estos pueden ser usados por la propia organización para descubrir puntos ciegos de sus sistemas de seguridad, pudiendo mejorar de esta manera su protección.
7. **Respuesta**: Se debe mantener una política de respuesta ante incidentes actualizada, centrándose en estrategias de recuperación de actividad y continuidad de negocio a pesar de posibles incidentes.

[10] Indicadores de compromiso.

8. Monitorización de vulnerabilidades.

Guía de prevención

1. Implementación de autenticación multifactorial.
2. Implementar una política de contraseñas seguras, con renovación periódica.
3. Auditar controladores de dominio, asegurándose que se supervisa correctamente una posible actividad anómala.
4. Habilitar fuertes filtros de spam.
5. Actualizar software y firmware en los activos TI.
6. Usar programas antivirus recomendados.
7. Deshabilitar puertos y protocolos innecesarios.

Fuentes

- https://es.malwarebytes.com/ransomware/#:~:text=El%20malware%20de%20rescate%2C%20o,acceder%20de%20nuevo%20a%20ellos.
- https://www.redeszone.net/tutoriales/seguridad/malware-wiper-consejos-seguridad/
- https://www.cisa.gov/uscert/ncas/alerts/aa22-040a#:~:text=Technical%20Details-,Cybersecurity%20authorities%20in%20the%20United%20States%2C%20Australia%2C%20and%20the%20United,brute%20force%2C%20and%20exploiting%20vulnerabilities.
- https://www.cisa.gov/critical-infrastructure-sectors
- https://attack.mitre.org/software/S0575/
- https://www.trendmicro.com/en_us/research/21/h/lockbit-resurfaces-with-version-2-0-ransomware-detections-in-chi.html
- https://attack.mitre.org/software/S0640/
- https://attack.mitre.org/software/S0496/
- https://www.cisa.gov/uscert/ncas/analysis-reports/ar21-189a
- https://www.cisa.gov/uscert/ncas/alerts/aa21-291a
- https://therecord.media/ransomware-tracker-the-latest-figures/

- https://www.cfr.org/blog/tracking-cyber-operations-and-actors-russia-ukraine-war
- https://www.sentinelone.com/labs/hermetic-wiper-ukraine-under-attack/
- https://www.zdnet.com/article/security-researchers-spot-another-form-of-wiper-malware-that-was-used-against-ukraines-networks/
- https://www.proofpoint.com/us/blog/threat-insight/asylum-ambuscade-state-actor-uses-compromised-private-ukrainian-military-emails
- https://www.zdnet.com/article/caddywiper-more-destructive-wiper-malware-strikes-ukrainian-targets/
- https://cert.gov.ua/article/38088
- https://www.fortiguard.com/threat-signal-report/4447/microbackdoor-used-in-attacks-against-ukraine-organizations
- https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/
- https://www.cisa.gov/uscert/ncas/alerts/aa22-011a

¡Gracias!

www.isophcybersecurity.com

Contact us:

info@isophcybersecurity.com

T: + 34 911 74 35 66