GUERRA CIBERNETICA

MÁS ALLA DE UN BOMBARDEO

Ucrania ha estado en conflicto militar con Rusia desde la revolución de Mandian / Euromadian de 2013, en donde a través de los años se han observado ciberataques a infraestructura de Ucrania, resaltando casos como afectaciones al sector de energía entre los años 2015 y 2016, donde, de acuerdo con investigadores de seguridad estos eventos fueron el primer ataque cibernético que causó un corte de energía eléctrica mayor. Otro evento significativo ocurrió en 2017, mediante compromiso ligado al ransomware NotPetya el cual buscó interrumpir el sistema financiero ucraniano, eliminar datos de equipos de cómputo de este sector, afectaciones a empresas de energía, aeropuertos y compromisos de altos funcionarios de gobierno.

Desde el mes de noviembre del año pasado, las tensiones entre Rusia y Ucrania comenzaron a aumentar, tras el despliegue de soldados rusos en la frontera de Rusia, Crimea y Bielorrusia, a raíz de lo anterior, el jueves pasado 24 de febrero de 2022, Rusia anunció el comienzo de una "operación militar" en la región ucraniana, lo que representó un ascenso en el prolongado conflicto, provocando un dilema por parte de Estados Unidos y países miembros de la OTAN (Organización del Tratado del Atlántico Norte). Si bien el conflicto armado ha comenzado, también esto ha desencadenado incidentes cibernéticos, tanto en ataques dirigidos a Ucrania, compromisos a sitios Web de Rusia y una tensión respecto a temas de ciberseguridad a nivel mundial.

En las últimas semanas se han visto diferentes campañas cibernéticas y programas maliciosos empleados por parte de Rusia para comprometer a organizaciones ucranianas. El seguimiento de dicha actividad realizado por Mnemo contempla lo siguiente:

15 de enero, 2022
- El grupo de amenaza "DEV-0586" dirige ataques a Ucrania contra organizaciones relacionadas con el sector gubernamental, instituciones sin fines de lucro y de TI con el propósito de implementar el programa malicioso WhisperGate, que aparenta ser un ransomware, pero en realidad tiene como objetivo dejar inoperables a los dispositivos afectados mediante técnicas de borrado.

31 de enero, 2022
- Campaña atribuida al grupo de amenaza ruso "Shuckworm" donde se envían correos electrónicos con archivos maliciosos adjuntos que instalan el backdoor Pterodo/Pteranodon.

03 de febrero, 2022
- Campañas de ciber espionaje contra organizaciones gubernamentales de Ucrania relacionadas con el grupo APT Gamaredon vinculado a Rusia que utiliza archivos maliciosos para realizar ciber espionaje a las instituciones.

10 de febrero, 2022
- Campaña maliciosa de correo electrónico denominada +380 GlowSpark dirigida a organizaciones de Ucrania.

12 de febrero, 2022
- Campañas de Denegación de Servicio Distribuido (DDoS) contra sitios Web de Ucrania, principalmente realizados por las botnets Mirai, Bashlite, moobot.

20 de febrero, 2022
- Campañas de Denegación de Servicio Distribuido (DDoS) dirigidas a sitios Web ucranianos, como bancos, páginas del gobierno y militar. De acuerdo con las investigaciones se cree que el origen de estos ataques fue la botnet Mirai.

23 de febrero, 2022
- Nuevo programa malicioso denominado "HermeticWiper" utilizado en ataques contra Ucrania, que tiene como objetivo corromper los dispositivos de las víctimas dejando al sistema inoperable.

24 de febrero, 2022
- Agencias de seguridad de Ucrania advierten sobre campañas de spear phishing dirigidas al personal de las fuerzas armadas del país, realizadas por el grupo de amenaza UNC1151.

24 de febrero, 2022
- Programa malicioso denominado "Trojan.Killdisk", de tipo "wiper", empleado para comprometer a organizaciones en Ucrania poco antes de la invasión de Rusia, cuyo objetivo es corromper la información del dispositivo que infecta y hacerla irrecuperable, ha afectado a organizaciones financieras, de defensa, aviación y de TI.

25 de febrero, 2022
- Grupo del ransomware Conti asegura que tomará represalias si se comienza a atacar a la infraestructura crítica de Rusia.

26 de febrero, 2022
- Investigador ucraniano filtra mensajes del servidor de chat XMPP internos pertenecientes a la operación del ransomware Conti.

26 de febrero, 2022
- Rusia restringe al acceso a Twitter en su país, esto como una medida para impedir que los ciudadanos visualicen videos e imágenes de los ataques llevados a cabo por el ejército ruso en Ucrania.

27 de febrero, 2022
- El grupo de ransomware LockBit 2.0 emite una publicación informando que no tiene intención de realizar ataques cibernéticos contra la infraestructura crítica de ningún país ni participar en un conflicto internacional.

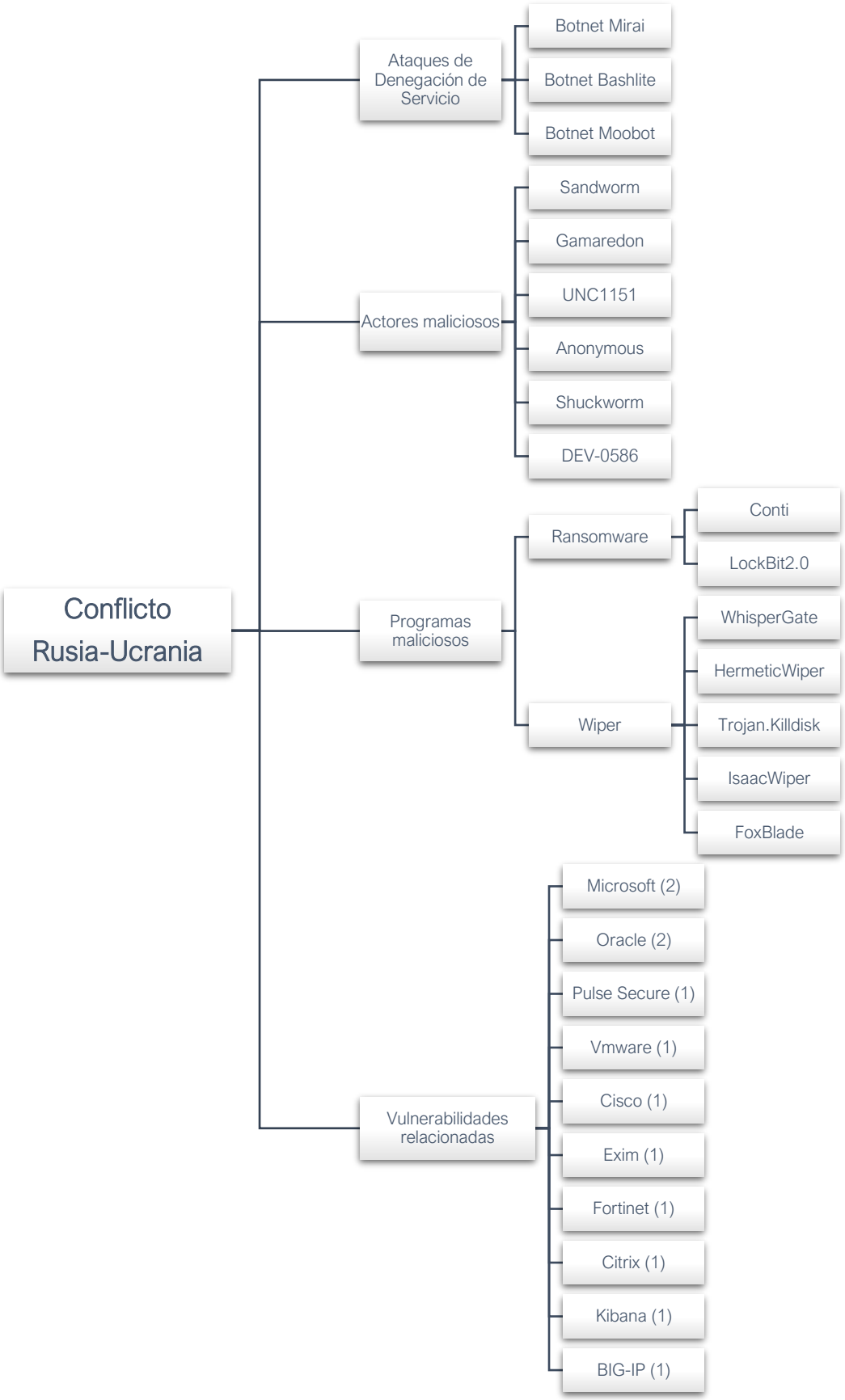
28 de febrero, 2022
- Identifican nuevo programa malicioso utilizado para comprometer las redes de Ucrania llamado IsaacWiper.

01 de marzo, 2022
- Campañas maliciosas de correo electrónico relacionadas con supuestas donaciones de "Ayuda a Ucrania".

01 de marzo, 2022
- Identifican programa malicioso FoxBlade utilizado en ataques de redes de Ucrania empleado horas antes de la invasión militar por parte de Rusia.

01 de marzo, 2022
- Campaña maliciosa dirigida al personal del gobierno europeo relacionado con la administración de refugiados que huyen de Ucrania.

01 de marzo, 2022
- Investigador ucraniano publica el código fuente relacionado con el ransomware Conti.


Conflicto Rusia-Ucrania
Ataques de Denegación de Servicio
Botnet Mirai
Botnet Bashlite
Botnet Moobot
Actores maliciosos
Sandworm
Gamaredon
UNC1151
Anonymous
Shuckworm
DEV-0586
Programas maliciosos
Ransomware
Conti
LockBit2.0
Wiper
WhisperGate
HermeticWiper
Trojan.Killdisk
IsaacWiper
FoxBlade
Vulnerabilidades relacionadas
Microsoft (2)
Oracle (2)
Pulse Secure (1)
Vmware (1)
Cisco (1)
Exim (1)
Fortinet (1)
Citrix (1)
Kibana (1)
BIG-IP (1)

Entre los principales vectores de compromiso que se emplean en estos ataques es el correo electrónico y el aprovechamiento de vulnerabilidades. Hasta el momento, se han identificado que los actores de amenaza están aprovechando principalmente las siguientes fallas:

1. CVE-2019-11510 (CVSS v3.1: 10.0 [Crítico]) - Pulse Secure Pulse Connect Secure
2. CVE-2019-7609 (CVSS v3.1: 10.0 [Crítico]) - Kibana
3. CVE-2020-5902 (CVSS v3.1: 9.8 [Crítico]) - BIG-IP
4. CVE-2019-19781 (CVSS v3.1: 9.8 [Crítico]) - Citrix Application Delivery Controller
5. CVE-2019-10149 (CVSS v3.1: 9.8 [Crítico]) - Exim
6. CVE-2018-13379 (CVSS v3.1: 9.8 [Crítico]) - Fortinet FortiOS
7. CVE-2021-26855 (CVSS v3.1: 9.8 [Crítico]) - Microsoft Exchange Server
8. CVE-2019-2725 (CVSS v3.1: 9.8 [Crítico]) - Oracle WebLogic Server
9. CVE-2020-14882 (CVSS v3.1: 9.8 [Crítico]) - Oracle WebLogic Server
10. CVE-2019-9670 (CVSS v3.1: 9.8 [Crítico]) - Zimbra
11. CVE-2020-4006 (CVSS v3.1: 9.1 [Crítico]) - VMware Workspace One Access
12. CVE-2020-0688 (CVSS v3.1: 8.8 [Alto]) - Microsoft Exchange Server
13. CVE-2019-1653 (CVSS v3.1: 7.5 [Alto]) - Cisco Small Business
14. CVE-2021-32648 (CVSS v3.1: 6.4 [Medio]) - OctoberCMS -TA DEV-0586

En adición, en el mes de enero, la Agencia de Seguridad Cibernética e Infraestructura (CISA), el Buró Federal de Investigaciones (FBI) y la Agencia de Seguridad Nacional de Estados Unidos (NSA) publicaron un comunicado informando a las organizaciones acerca de las Tácticas, Técnicas y Procedimientos (TTPs) observados por actores de amenaza (APTs) patrocinados por el gobierno de Rusia, entre los que se incluyen APT29, APT28 y Sandworm Team. En este mismo informe se detallan 13 vulnerabilidades aprovechadas por estos grupos, entre las se incluyen 11 consideradas críticas y que afectan a productos de fabricantes como Puse Secure, Oracle, Citrix, VMware, Microsoft, entre otros. *[1]*

Este conflicto también ha provocado que el grupo hacktivista “Anonymous”, conocido por realizar actividades con motivaciones políticas e ideológicas, haya comenzado a realizar campañas contra organizaciones de Rusia y de los países que apoyan al gobierno ruso, incluyendo a Bielorrusia, esto como una manera de demostrar su apoyo a Ucrania.
A la fecha, los afectados por los ataques atribuidos a Anonymous son:

- Sitio Web del Kremlin – DDoS
- Cámara baja del parlamento de la Duma Estatal de Rusia – DDoS
- Ministerio de Defensa ruso – Filtración de datos
- Red interna de los ferrocarriles bielorrusos – DoS
- Instituto nuclear ruso – Filtración de datos

Esto también ha provocado que un representante ucraniano de la ICANN, haya solicitado que los dominios relacionados con Rusia sean revocados, entre los que se incluyen [.]ru, [.]su y [.]рф. En adición, el gobierno de Ucrania ha solicitado voluntarios informáticos para ayudar a proteger la infraestructura crítica de su país y realizar misiones de espionaje contra las tropas de Rusia. El gobierno informó que el voluntariado se dividiría en unidades defensivas y ofensivas, la unidad defensiva se empleará para proteger la infraestructura crítica como plantas de energía y sistemas de agua. La unidad ofensiva se estará organizando para ayudar al ejército de Ucrania a realizar operaciones de ciber espionaje contra las fuerzas invasoras rusas. Según los informes, para esta actividad el gobierno de Ucrania ha utilizado un canal de Telegram para planificar los ataques cibernéticos contra las organizaciones rusas.

En complemento, el gobierno de Ucrania, asegura que ha comenzado a realizar ataques contra sitios Web rusos y bielorrusos teniendo como objetivos a organizaciones públicas y privadas, entre los que se incluyen páginas Web como:

- Surgetneftegas
- Tatneft
- Evraz
- Compañía Rusa de Cobre
- Eurosibenergo
- OMK
- Banco Sberbank
- Servicios públicos estatales
- Servicios estatales de Moscú
- Kremlin
- Gobierno de la Federación de Rusia
- Ministerio de Defensa
- Organización relacionada con impuestos
- Aduanas
- Fondo de Pensiones
- Roskomnadzor

[1] https://www.cisa.gov/uscert/ncas/alerts/aa22-011a

Se ha identificado en RaidForums, uno de los foros underground con mayor actividad hoy en día, la inconformidad por las acciones tomadas por el presidente de Rusia, y ha anunciado que no permitirá el acceso a los usuarios con ubicación geográfica de este país, manifestando su oposición ante los acontecimientos.

Además, un usuario de este foro publicó una base de datos con correos electrónicos y contraseñas codificadas asociados al dominio del Servicio Federal de Seguridad de Rusia (FSB). No obstante, el grupo del ransomware Conti también ha emitido un mensaje informando que está dispuesto a tomar represalias si se comienza a afectar a infraestructura crítica de Rusia.

Esto también ocasionó que un usuario filtrara en un foro underground mensajes del servidor de chat XMPP internos pertenecientes a la operación del ransomware Conti. En adición, días después otro ucraniano filtró el código fuente para el cifrador y descifrador del ransomware, además publicó información del panel administrativo y la API relacionados con el programa BazarBackdoor. Si bien, el código fuente está protegido con contraseña, esta fue divulgada por otro investigador.

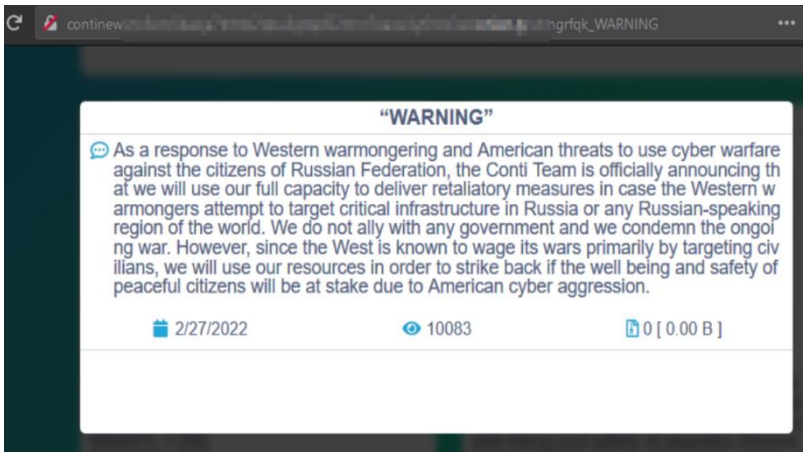


Ilustración 1, comunicado de ransomware Conti

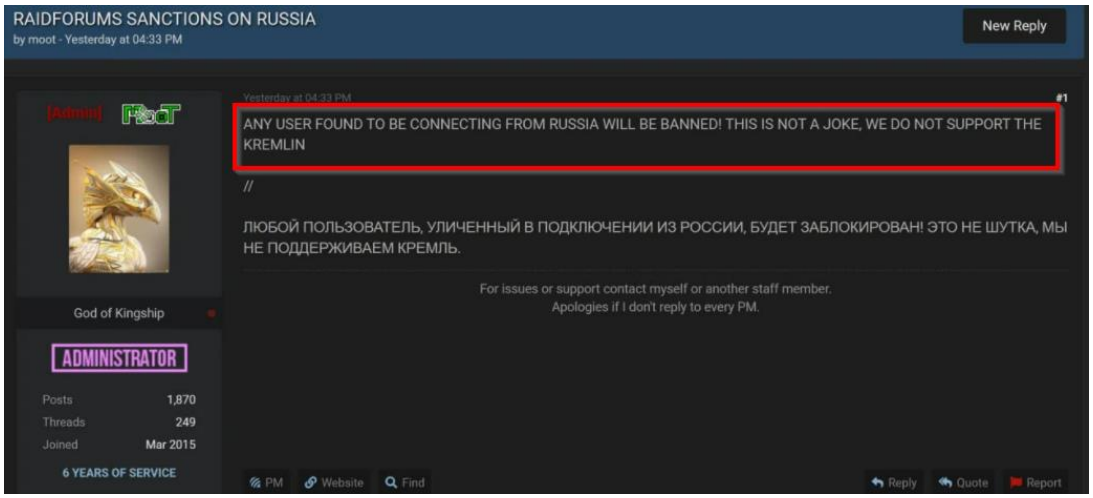


Ilustración 2, publicación del foro RaidForums

Dicho acontecimiento también ha ocasionado que **empresas en apoyo a Ucrania comiencen a cerrar las operaciones** que tienen con usuarios rusos, una de ellas ha sido **Namecheap**, un proveedor que brinda servicios para alojar páginas Web. Esta empresa **ha enviado correos electrónicos a los clientes registrados en Rusia, indicando que no brindará servicios a estos usuarios y solicitando que cambien de hosting**, esto ocasionado por la invasión rusa a Ucrania. Namecheap **fijó el plazo para realizar esto antes del 06 de marzo del año en curso**, de lo contrario se dará de baja los dominios.
Otras empresas que no tienen relación con el área de TI, pero que han tomado estas acciones son organizaciones como: Apple, Nike, Adidas, la FIFA, la UEFA, entre algunas otros.

Durante estos últimos días la actividad cibernética ocasionada por el despliegue militar en Ucrania también ha causado incertidumbre en el mundo de la ciberseguridad. En adición, **se cree que Rusia continuará realizando campañas cibernéticas contra Ucrania**, además, se especula que estos ataques también se dirigirán a regiones más allá de Ucrania, y es probable que se produzcan incidentes cibernéticos indirectos y cualquier actividad de este tipo probablemente se relacionará a campañas disruptivas. Por ello es importante que las organizaciones implementen medidas para protegerse contra este tipo de amenazas, ya que se pueden comenzar a realizar campañas contra otros países, como un efecto colateral.

Conclusiones y Recomendaciones

Con independencia de los eventos previamente descritos, hoy en día obliga a todos los equipos de ciberseguridad a tener acercamiento respecto a los diversos escenarios de compromiso cibernético alrededor de estos eventos, así como contexto de las capacidades de actores de amenaza rusos, tomando en cuenta con mayor urgencia temas como:

- **Gestión de vulnerabilidades**, en particular respecto a las identificadas en las campañas de ataque y las que puedan estar expuesta al perímetro de las organizaciones. *[2]*
- **Mejorar los mecanismos de defensa ligados a los servicios de correo:**
    - Soluciones antispam, filtrado SPF, DKIM, DMARC.
    - Concientización de usuarios finales respecto a compromisos vía correo electrónico.
- **Implementación de controles de seguridad anti malware** en endpoints y servidores.
- **Consumo de información periódica** de Inteligencia de amenazas.
- **Automatizar el consumo de IoC** referentes a campañas de compromiso.
- **Generar casos de uso de detección con tecnología que así lo permita** en la organización ligada a la identificación de actividad maliciosa relacionada a:
    - Ejecución de procesos, hilos de procesos, servicios, instalación de aplicaciones, actividad de cuentas de usuario locales y de dominio, integridad de archivos, nombres de usuario fuera del formato establecido, monitoreo de conexiones de red, actividades de persistencia (llaves de registro, tareas programadas), ejecución de artefactos (Pefetch y simcache), creación de GPO (Group Policy Object).
    - Ejecuciones de Powershell con codificaciones en base64.
    - Bloqueo de ejecución de archivos con extensiones .js, .vbs, .zip, .7z, .sxf.
    - Recolectar scripts y binarios creados en directorios como:
        - /dev/shm/tmp
        - /var/tmp
    - En sistemas Linux revisión de tareas programas mediante el “cron”.
    - Detenciones por soluciones de seguridad EndPoint.
- Incrementar análisis de riesgos en los entornos de procesamiento de información.
- Complementar y mantener actualizada la documentación de red y sistemas:
    - Diagramas de red.
    - Memorias técnicas.
    - Dueños de activos.
    - Tipos de activos.
    - Plan de respuesta a incidentes / Plan de gestión de crisis cibernéticas.
- Ejecutar ciberejercicios que involucren funciones de comunicación y toma de decisión estratégica, en particular bajo escenarios de ransomware y destrucción de datos.
- Prestar atención a las familias de actores maliciosos de origen ruso como:
    - Unit 74455 / GRU
    - Sofacy / APT 28 / Fancy Bear / Sednit / Group 74 / TG-4127 / Pawn Storm / Tsar Team / Strontium / Swallowtail / SIG40 / Snakemackerel / Iron Twilight / ATK 5 / T-APT-12 / ITG05 / TAG-0700 / Grizzly Steppe
        - CVE-2021-42292 CVSS 3.1 7.8, relacionada con vulnerabilidad en Excel
    - APT 29 / Cozy Bear / The Dukes / Group 100 / Yttrium / Iron Hemlock / Minidionis / CloudLook / ATK 7 / ITG11 / Grizzly Steppe / UNC2452 / Dark Halo / SolarStorm / StellarParticle / Nobelium
    - Berserk Bear / Dragonfly 2.0 / Dymalloy
    - Buhtrap / Ratopak Spider
    - Cobalt Group / Cobalt Gang / Cobalt Spider / Gold Kingswood / ATK 67 / TAG-CR3
    - Corkow / Metel
    - Doppel Spider / Gold Heron / Grief Group

[2] https://csrc.nist.gov/publications/detail/sp/800-40/rev-3/final

- Energetic Bear / Dragonfly / Crouching Yeti / Group 24 / Koala Team / Iron Liberty / TG-4192 / Electrum / ATK 6 / ITG15 / Bromine
- FIN7 / Gold Niagara / Calcium / Navigator / ATK 32 / APT-C-11 / ITG14 / TAG-CR1
- Gamaredon Group / Winterflounder / Primitive Bear / BlueAlpha / Blue Otso / Iron Tilden / Armageddon / SectorC08 / Callisto / Shuckworm / Actinium / DEV-0157
- GCMAN
- Hades
- IAmTheKing
- Inception Framework / Cloud Atlas / Oxygen / ATK 116 / The Rocra
- Indrik Spider / Gold Drake / Gold Winter / Evil Corp
- InvisiMole
- Lurk
- MoneyTaker
- OldGremlin
- Operation BugDrop
- Operation Domino / Operation Kremlin
- Pinchy Spider / Gold Southfield / Gold Garden
- Sandworm Team / Iron Viking / CTG-7263 / Voodoo Bear / Quedagh / TEMP.Noble / ATK 14 / BE2
- TA505 / Graceful Spider / Gold Evergreen / Gold Tahoe / TEMP.Warlock / ATK 103 / SectorJ04 / Hive0065 / Chimborazo
- TeamSpy Crew / SIG39 / Iron Lyric
- TeleBots
- Turla / Waterbug / Venomous Bear / Group 88 / SIG2 / SIG15 / SIG23 / Iron Hunter / CTG-8875 / Pacifier APT / ATK 13 / ITG12 / Makersmark / Krypton / Belugasturgeon / Popeye / Wraith / TAG-0530
- Venom Spider / Golden Chickens
- Wizard Spider / Grim Spider / TEMP.MixMaster / Gold Blackburn / Gold Ulrick

Finalmente, es importante mencionar que MNEMO-CERT realiza un seguimiento continuo de los hechos ocurridos entre Rusia y Ucrania, identificando a la fecha diversos eventos y más de 3 mil Indicadores de Compromiso (IoCs) relacionados con este acontecimiento. Además, es importante mencionar que los miembros de FIRST, del cual forma parte MNEMO continúan trabajando para ayudar a prevenir afectaciones cibernéticas y así proteger a las organizaciones y los usuarios finales, con el objetivo de contribuir para hacer del Internet una red más segura. Si estás interesado en recibir la información de nuestras alertas e IoCs envía un correo electrónico a cert@mnemo.com