CIBERBOLETÍN

NOVIEMBRE 2022

TEMA DEL MES

Emotec, una amenaza persistente que fortalece sus capacidades en 2022

VULNERABILIDADES

Las 10 vulnerabilidades más representativas de 612 que fueron identificadas como relevantes en el mes de noviembre de 2022, tomando en cuenta el tipo de componente que afectan, si se encuentra ligado con alguna campaña de compromiso y el nivel de criticidad con base a CVSS V 3.1.

THREAT INTELLIGENCE

Grupo hacktivista KillNet en apoyo al sistema político ruso. Perfilación y análisis del ransomware KillNet

MNEMO

El

TEMA DEL MES

Emotec, una amenaza persistente

El malware Emotec fortalece sus capacidades en 2022

Según **CyberSecuritynews**, medio de comunicación online especializado en información para profesionales del sector de la ciberseguridad, el **malware Emotet** aún **sigue siendo una amenaza persistente** a pesar de todos los intentos por acabar con él desde el año 2014, cuando apareció como un troyano.

Infoblox Inc., líder en servicios de red seguros y gestionados desde la nube, ha publicado un **informe** de inteligencia de amenazas y brechas de seguridad que recopila trimestralmente las **principales amenazas de la actualidad**. En este análisis se encuentra **Emotet como uno de los malware más peligrosos**, cuya **finalidad es robar datos financieros**. Este malware ha infectado a varios objetivos, entre los que se encuentran particulares, empresas y entidades gubernamentales en Estados Unidos, Europa. También se le han asignado robos de datos bancarios e incluso carteras de bitcoin.

Dicho malware **se distribuye vía email**, utilizando una de las técnicas más conocidas: el ***phishing***, el cual **disfraza archivos maliciosos como archivos *Word* y *Excel*** que hace que la víctima sea más propensa a descargarlos.

El malware **comenzó como un simple troyano bancario en 2014**, pero desde entonces ha ido tomando o adquiriendo nuevas funciones. En 2014, las características principales fueron los módulos de transferencia de dinero, spam de correo, DDoS y robo de librerías. En 2015, se le añade la funcionalidad de evasión. En 2016, correo no deseado y entrega de otros troyanos. En 2017, se añade un módulo esparcidor y robo de libretas de direcciones. En 2021, plantillas maliciosas XLS, utiliza MSHTA, eliminadas por Cobalt Strike y en 2022, algunas características se mantuvieron igual, pero este año también trajo varias actualizaciones. Después de casi medio año de espera, **Emotet ha vuelto más fuerte con nuevas características**, como la eliminación de IcedID, un troyano bancario modular, el malware carga XMRig, un minero que roba datos de billetera. El troyano tiene cambios binarios.

Aprendiendo el funcionamiento de Emotet, damos el primer paso para contrarrestar a este malware. Asimismo, se recomienda llevar a cabo las siguientes **recomendaciones**:

- Mantener los **equipos/terminales actualizados** con los últimos parches de *Microsoft* para sistemas *Windows*.
- **No descargar archivos adjuntos sospechosos**, ni hacer clic en enlaces sospechosos.
- Tomar acciones frente al personal realizando **capacitaciones sobre temas relacionados a correos sospechosos** y creación de **contraseñas seguras**.
- Si se **sospecha** que algún **equipo** se encuentra **infectado** con Emotet, lo que se debe hacer es **aislarlo de la red**, con el fin de que el malware no se propague, y

El

realizar una **limpieza profunda** a cada uno de los equipos conectados a la red para evitar que vuelva a infectarse.

Walter Oswaldo Toledo Salamanca

Analista de Seguridad L-1 Master Operaciones

Tomar acciones preventivas con **servicios de monitoreo de eventos de ciberseguridad y análisis de actividad sospechosa** puede ayudar significativamente a las organizaciones para estar **un paso adelante de cibercriminales**. Es importante mantener la continuidad de sus servicios y no solo **garantizar la confidencialidad de la información**, sino también su **integridad y disponibilidad** de esta, todo ello para **evitar filtraciones de datos** y tener mayor **claridad y control sobre cómo actuar** frente a las ciberamenazas.

El

VULNERABILIDADES

Principales vulnerabilidades de noviembre 2022

Google, VMware, SAP, Zoho, Citrix, Tenda

Titulo	Identificador	CVSS	Descripción
Falla de seguridad presente en **Google**	CVE-2022-4135	CVSS v3.1: 9.6 [Crítico]	Vulnerabilidad presente en el navegador de **Chrome** versiones anteriores a **107**. Es de tipo buffer overflow y podría permitir que un actor malicioso escape de una sandbox, a través de una página HTML especialmente diseñada.
Falla de seguridad presente en **VMWare**	CVE-2022-38650	CVSS v3.1: 10.0 [Crítico]	Falla ubicada en **VMware Hyperic Server** versión **5.8.6** causada por una deserialización insegura no autenticada. Un actor de amenaza podría aprovechar con éxito esta falla y ejecutar código arbitrario en la instancia afectada con privilegios del proceso del servidor Hyperic.
Falla de seguridad presente en **SAP**	CVE-2022-41203	CVSS v3.1: 9.9 [Crítico]	Está presente en **SAP BusinessObjects Business Intelligence Platform** versiones **4.2** y **4.3** debido a una deserialización insegura. Podría permitir a un usuario malicioso autenticado y con bajos privilegios interceptar un objeto serializado en los parámetros y sustituirlo por otro objeto malicioso.
Falla de seguridad presente en **VMware**	CVE-2022-31685	CVSS v3.1: 9.8 [Crítico]	Vulnerabilidad presente en **VMware Workspace ONE Assist** versiones **21.x** y **22.x**. Un actor de amenaza podría eludir la autenticación y obtener acceso administrativo en la instancia afectada.
Falla de seguridad presente en **VMware**	CVE-2022-31686	CVSS v3.1: 9.8 [Crítico]	Falla presente en **VMware Workspace ONE Assist** versiones **21.x** y **22.x**. Un atacante podría eludir la autenticación y obtener acceso administrativo en la instancia afectada.
Falla de seguridad presente en **VMware**	CVE-2022-31687	CVSS v3.1: 9.8 [Crítico]	Error presente en **VMware Workspace ONE Assist** versiones **21.x** y **22.x**. Un actor de amenaza podría eludir la autenticación y obtener acceso administrativo en la instancia afectada.
Falla de seguridad presente en **Zoho**	CVE-2022-43671	CVSS v3.1: 9.8 [Crítico]	Es una vulnerabilidad ubicada en **Zoho ManageEngine Password Manager Pro** versiones anteriores a **12122**, **PAM360** anteriores a **5711** y **Access Manager Plus** anteriores a **4306**. Esta falla podría permitir que un actor malicioso envíe una consulta SQL especialmente diseñada y ejecutarla.
Falla de seguridad presente en **Zoho**	CVE-2022-43672	CVSS v3.1: 9.8 [Crítico]	Error presente en **Zoho ManageEngine Password Manager Pro** anteriores a 12122, PAM360 anteriores a 5711 y Access Manager Plus anteriores a 4306. Esta falla podría permitir que un atacante realice una inyección de SQL en un componente diferente a la falla anterior.
Falla de seguridad presente en **Citrix**	CVE-2022-27510	CVSS v3.1: 9.8 [Crítico]	Es un problema presente en algunas versiones de **Citrix ADC** y **Citrix Gateway**, la cual podría permitir que un actor de amenaza obtenga acceso no autorizado a las capacidades del usuario de Gateway.
Falla de seguridad presente en **Tenda**	CVE-2022-42058	CVSS v3.1: 9.8 [Crítico]	Vulnerabilidad ubicada en **routers Tenda AC1200 W15Ev2** versiones **15.11.0.10** y de tipo stack overflow en la función "setRemoteWebManage". Esta falla podría permitir a los actores de amenaza provocar una condición de Denegación de Servicio (DoS).

El

MNEMO-CERT presenta las **10 vulnerabilidades más representativas de 612** que fueron identificadas como relevantes en el mes de **noviembre de 2022**, tomando en cuenta el tipo de componente que afectan, si se encuentra ligado con alguna campaña de compromiso y el nivel de criticidad con base a CVSS V 3.1.

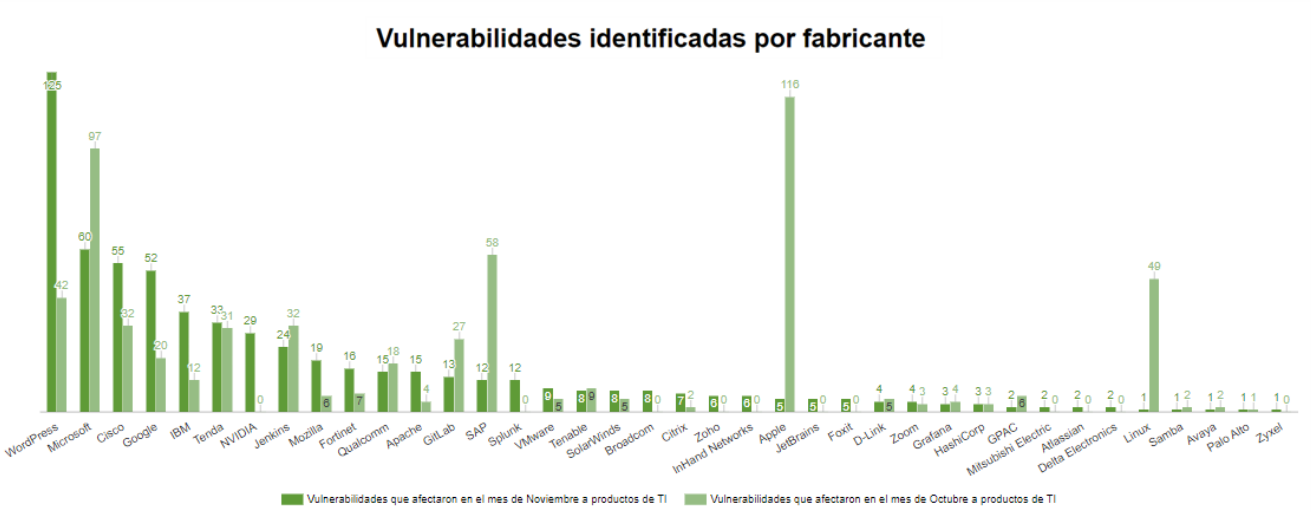
En la primera posición **destaca una vulnerabilidad presente en el navegador de Google Chrome causada por un desbordamiento de búfer**. La empresa, además advirtió sobre una Prueba de Concepto (PoC) que está siendo aprovechada por los actores de amenaza. **MNEMO-CERT publicó dos avisos referentes a esta vulnerabilidad que pueden ser consultadas en las siguientes URLs**:

- https://mailchi.mp/mnemo.com/aviso-de-vulnerabilidad-google-corrige-vulnerabilidad-presente-en-chrome
- https://mailchi.mp/mnemo.com/aviso-de-vulnerabilidadorganizacin-gubernamental-de-estados-unidos-advierte-sobre-vulnerabilidades-aprovechadas-por-actores-maliciosos-gtdllsccef

En la segunda posición, destaca una **falla en VMware Hyperic Server 5.8.6** que podría permitir la ejecución de código, sin embargo, esta versión se encuentra al final de su soporte por lo que VMware no informó acerca de esta, solo fue mencionada por NVD. En la tercera posición se encuentra una **vulnerabilidad en SAP** causada por una deserialización insegura. MNEMO-CERT emitió un aviso relacionado con la tercera falla. Este aviso puede ser consultado en la siguiente URL:

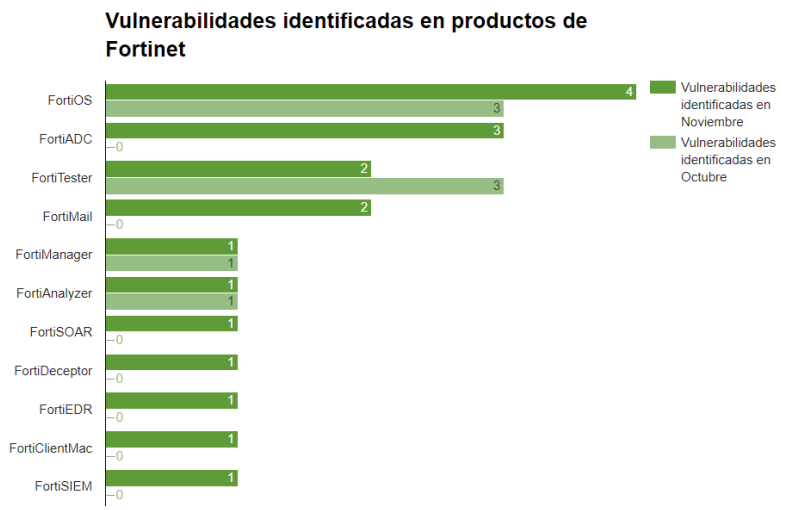
- https://mailchi.mp/mnemo.com/aviso-de-vulnerabilidad-sap-emite-actualizaciones-de-seguridad-de-noviembre-para-varios-productos

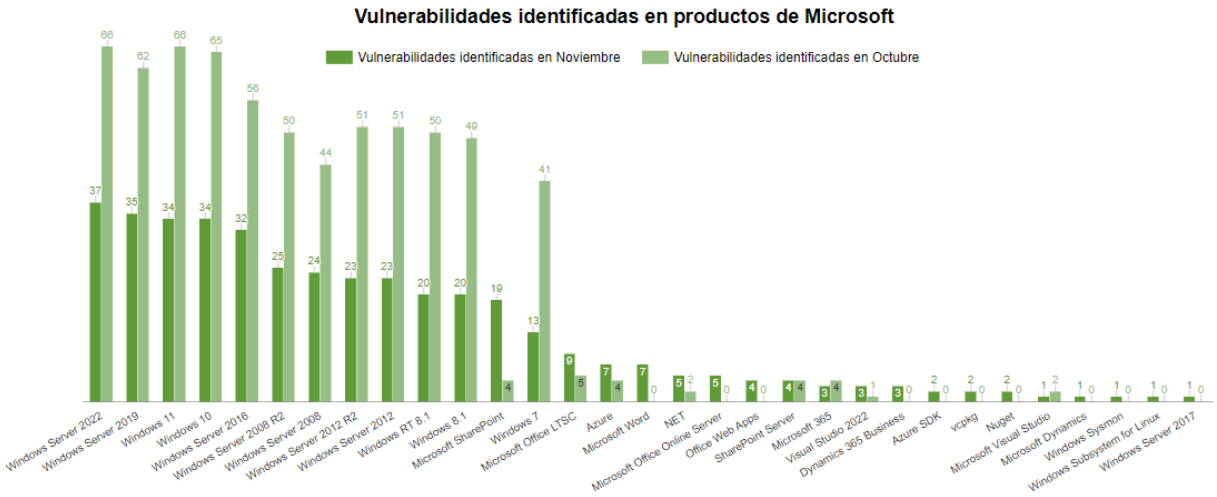
Asimismo, cabe señalar que durante este mes varios **fabricantes corrigieron diversos fallos** en sus diferentes productos, siendo los más destacados "**WordPress**", "**Microsoft**" y "**Cisco**", "**Google**" a comparación del mes pasado, en donde las más sobresalientes fueron "Oracle", "Apple", "Microsoft".

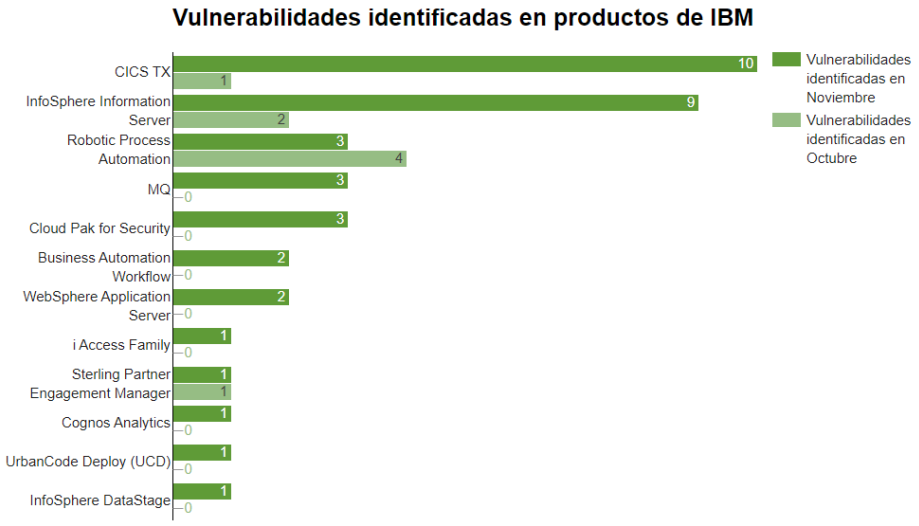


El

Del mismo modo, en las siguientes gráficas se muestra el número de **vulnerabilidades por producto para los fabricantes** con mayor cantidad de fallas identificadas en el mes de **noviembre de 2022** y un **comparativo con el mes de octubre**.

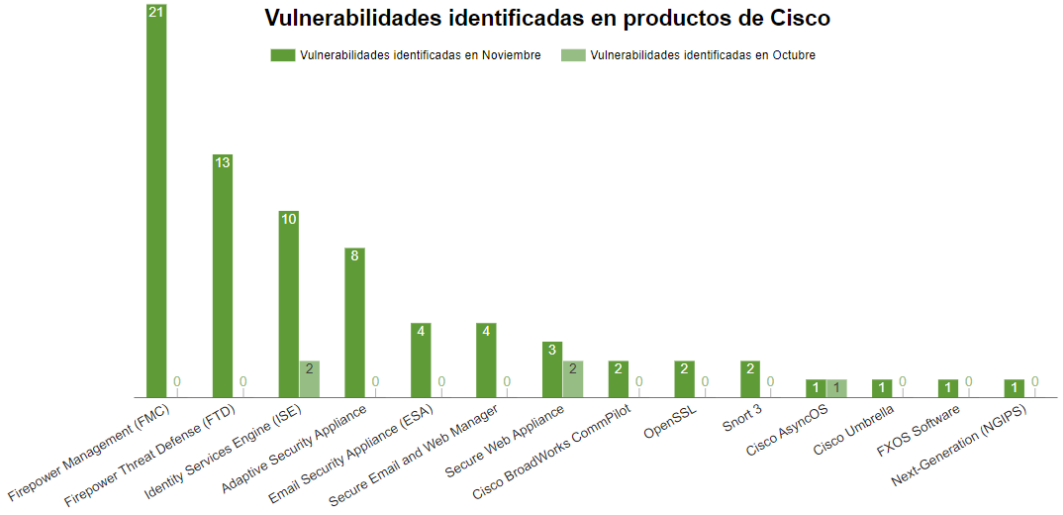


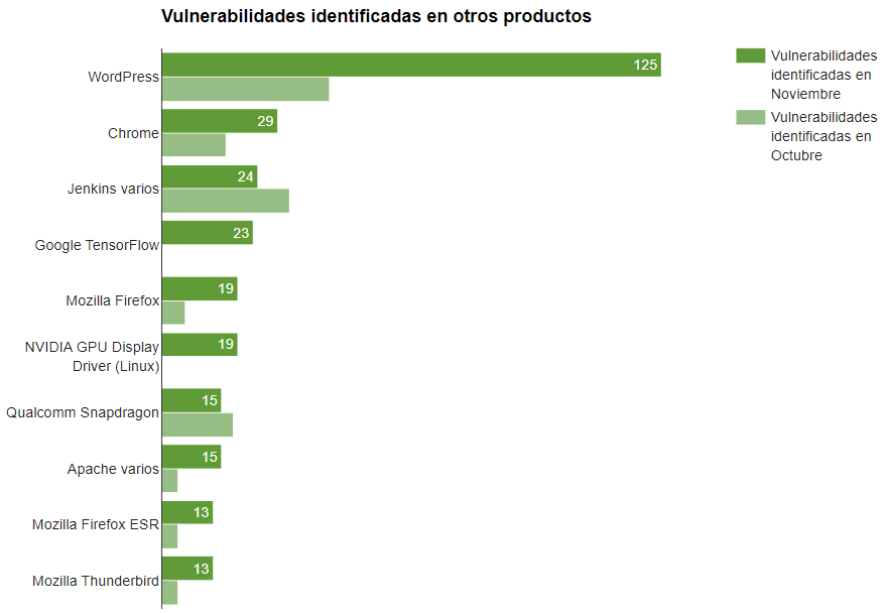




El


Vulnerabilidades identificadas en productos de Apple
Vulnerabilidades identificadas en Noviembre
Vulnerabilidades identificadas en Octubre
Xcode
4
0
macOS Ventura
1
113
iPadOS
1
20
iOS
1
21


Vulnerabilidades identificadas en productos de Cisco
Vulnerabilidades identificadas en Noviembre
Vulnerabilidades identificadas en Octubre
Firepower Management (FMC) 21 0
Firepower Threat Defense (FTD) 13 0
Identity Services Engine (ISE) 10 2
Adaptive Security Appliance 8 0
Email Security Appliance (ESA) 4 0
Secure Email and Web Manager 4 0
Secure Web Appliance 3 2
Cisco BroadWorks CommPilot 2 0
OpenSSL 2 0
Snort 3 2 0
Cisco AsyncOS 1 1
Cisco Umbrella 1 0
FXOS Software 1 0
Next-Generation (NGIPS) 1 0


Vulnerabilidades identificadas en otros productos
Vulnerabilidades identificadas en Noviembre
Vulnerabilidades identificadas en Octubre
WordPress 125
Chrome 29
Jenkins varios 24
Google TensorFlow 23
Mozilla Firefox 19
NVIDIA GPU Display Driver (Linux) 19
Qualcomm Snapdragon 15
Apache varios 15
Mozilla Firefox ESR 13
Mozilla Thunderbird 13

El

Producto	Vulnerabilidades identificadas en Octubre	Vulnerabilidades identificadas en Noviembre
Splunk Enterprise	0	12
Splunk Cloud Platform	0	12
Tenda AC1200 Router	0	10
GitLab CE/EE	19	9
Tenda AC18	1	9
Tenda AC23	0	8
Tenable Nessus	0	8
Zoho ManageEngine	0	6
NVIDIA GPU Display Driver para Windows	0	6
InHand Networks InRouter302	0	6
JetBrains	0	5
Foxit PDF Reader	0	5
VMware Workspace ONE Assist	0	5
Zoom	3	4
Citrix Hypervisor	2	4
D-Link	5	4
Tenda AC15	1	4
Citrix Gateway	0	3
Citrix ADC	0	3
Grafana	4	3
HashiCorp	3	3
SolarWinds Serv-U	0	3
SolarWinds Platform	4	3
SolarWinds Orion Platform	4	3
VMware Hyperic Server	0	3
SAP Financial Consolidation	0	3
GPAC	6	2
Tenda AC21	0	2
Atlassian Confluence	0	2
GitLab	2	2
Mitsubishi Electric	0	2
Delta Electronics	0	2
NVIDIA vGPU software	0	2
Broadcom Symantec VIP	0	2
Broadcom CA Application Test	0	2
NetWeaver Application Server ABAP	0	2
Linux Kernel	49	1
GitLab EE	5	1
Samba	2	1
GitLab EE/CE	1	1
NVIDIA Display Driver para Linux	0	1
Brocade Fabric OS	0	1
Cortex XSOAR engine	0	1
Avaya Scopia Pathfinder	0	1
VMware Tools para Windows	0	1
SAP 3D Visual Enterprise Viewer	43	1
Objects Business Intelligence	6	1
SAP SQL Anywhere	1	1
SAP GUI para Windows	0	1
Biller Direct	0	1
SAPUI5	0	1
3D Visual Enterprise Author	0	1

El

THREAT INTELLIGENCE

Grupo hacktivista KillNet en apoyo al sistema político ruso

Perfilación y análisis del ransomware KillNet

A continuación, se presenta un apartado de la investigación realizada por el equipo de **Cyber Threat Intelligenc**e (CTI) a las actividades del **grupo hacktivista** de nombre **KillNet**, del cual se ha observado una serie de **ciberataques a partir del mes de enero de 2022 en contra de países u organizaciones que apoyan a Ucrania** en el presente conflicto con Rusia. Este grupo se autoproclamó como partido del sistema político ruso.

Tras analizar su **modus operandi**, se observa que actúan en **defensa del sistema político ruso y en contra de organizaciones que consideran que participan en la defensa de Ucrania**. Las técnicas principalmente usadas se basan en **ataques DoS** (denegación de servicio) y **DDoS** (denegación de servicio distribuida).

Dentro de la inteligencia generada por el equipo CTI se destacan **dos campañas** que se consideran relevantes por el nivel de afectación hacia sus objetivos; estas son:

- **Compromiso dirigido a Lockheed Martin**, compañía multinacional de origen estadounidense dedicada a la industria aeroespacial y militar con enormes recursos en tecnología avanzada y guerra global.
- **Afectación al sitio web Starlink** (proyecto de internet por satélite de Elon Musk) que imposibilitó que sus usuarios pudieran hacer uso del servicio.

En cuanto al modo de operar al momento de realizar los ataques de tipo DDoS se ha encontrado que por lo general se realizan en las **capas 4 y 7 del modelo OSI** (Transporte y Aplicación). Debido a la cantidad de peticiones generadas (alrededor de 40Gbps) y el tiempo que dura el ataque (apróx. 10 horas), **sus ataques tienen una alta probabilidad de éxito**.

De acuerdo con lo que se conoce, **estos ataques se dividen en 3 fases**:

- **Envío de paquetes TCP/SYN, UDP, SYN/ACK y amplificación de DNS**.
- Ataques de **fragmentación de IP**.
- **Incremento en la volumetría de paquetes** enviados.

Un hecho destacado sobre KillNet que indica el uso de una **estructura jerarquizada**, ocurrió en julio del 2022. El **líder del grupo**, apodado **Killmilk**, manifestó en redes sociales que **se separaba para crear nuevos equipos**, dejando en su lugar a otra persona apodada **Blackside**, este **nuevo encargado** cuenta con **otro tipo de perfil** digital **especializado en Ransomware**, **phishing** y **robo de criptomonedas**.

El

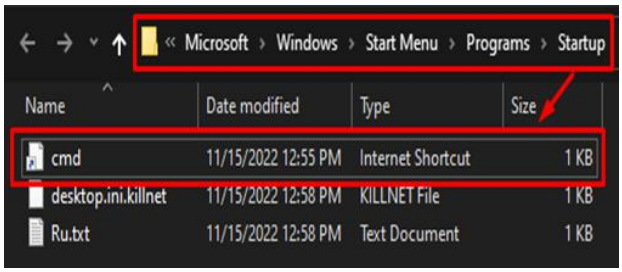
En consideración con lo antes expuesto, se ha identificado que el grupo **está utilizando un ransomware que ha recibido el mismo nombre del grupo**. El ransomware KillNet es un programa malicioso desarrollado con capacidades que le **permiten realizar actividades de cifrado de archivos**, asignándole a cada uno de estos que sea comprometido la extensión .killNet, lo cual inhabilita el acceso a los mismos y, por lo tanto, generando la posibilidad de impactar la disponibilidad de las infraestructuras tecnológicas infectadas; por último, **genera cambio en el fondo de pantalla** y una **nota de texto identificada como Ru.txt** la cual está escrita en idioma ruso que contiene las indicaciones para la recuperación de la data.

El equipo de **CTI de Mnemo** ha realizado el **análisis a una de las muestras** de este ransomware y ha encontrado aspectos importantes como lo son:

Este ransomware genera **persistencia en el sistema comprometido** a través de la **modificación de la llave de registro** SOFTWARE\\Microsoft\\Windows\\CurrentVersion \\Run con el objetivo de ejecutarse cada vez que el equipo se apague o reinicie.

```
private static void registryStartup()
{
    try
    {
        RegistryKey registryKey = Registry.CurrentUser.OpenSubKey("SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run", true);
        registryKey.SetValue("Microsoft Store", Assembly.GetExecutingAssembly().Location);
    }
```

Otro modo que utiliza como persistencia es la **creación de un acceso directo** en la ubicación "C:\Users\Usuario\AppData\Roaming\Microsoft\Windows\StartMenu \Programs\ Startup" que permite ejecutar la muestra del ransomware (copiada previamente en %AppData%) cada vez que el sistema se inicie.



El

Entre las **actividades iniciales** se encuentra el **eliminar las copias de seguridad existentes** en el equipo comprometido mediante tres comandos (vssadmin, bcdedit y wbadmin) con el **fin de que no se pueda restaurar las copias de seguridad** una vez se haya cifrado la misma; ocasionando posibles fallos en los servicios prestados a las partes interesadas.

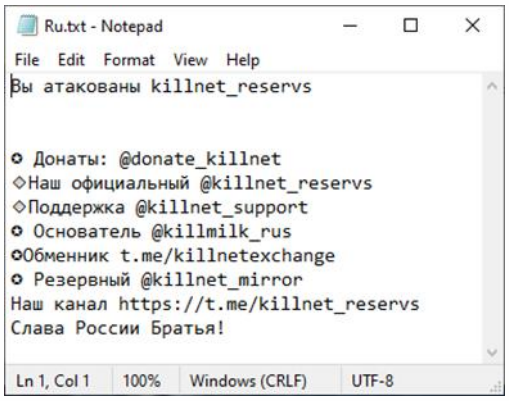
```
// Token: 0x06000019 RID: 25 RVA: 0x00002E4C File Offset: 0x0000104C
private static void deleteShadowCopies()
{
    Program.runCommand("vssadmin delete shadows /all /quiet & wmic shadowcopy delete");
}

// Token: 0x0600001A RID: 26 RVA: 0x00002E58 File Offset: 0x00001058
private static void disableRecoveryMode()
{
    Program.runCommand("bcdedit /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no");
}

// Token: 0x0600001B RID: 27 RVA: 0x00002E64 File Offset: 0x00001064
private static void deleteBackupCatalog()
{
    Program.runCommand("wbadmin delete catalog -quiet");
}
```

También se observaron un par de strings relacionadas con la creación de dos mutex durante su proceso de ejecución (recuadro blanco); así mismo el uso de la extensión killnet que se asignará a cada uno de los archivos cifrados (recuadro rojo) y adicionalmente el nombre del proceso cmd.exe a utilizar en el proceso de ejecución (recuadro amarillo).

```
private static string userName = Environment.UserName;

// Token: 0x04000002 RID: 2
private static string userDir = "C:\\Users\\";

// Token: 0x04000003 RID: 3
public static string appMutexRun = "7z459ajrk722yn8c5j4fg";

// Token: 0x04000004 RID: 4
public static bool encryptionAesRsa = true;

// Token: 0x04000005 RID: 5
public static string encryptedFileExtension = "killnet";

// Token: 0x04000006 RID: 6
private static bool checkSpread = true;

// Token: 0x04000007 RID: 7
private static string spreadName = "surprise.exe";

// Token: 0x04000008 RID: 8
private static bool checkCopyRoaming = true;

// Token: 0x04000009 RID: 9
private static string processName = "cmd.exe";

// Token: 0x0400000A RID: 10
public static string appMutexRun2 = "2X28tfRmWaPyPQgvoHV";
```

El

Una vez se ha **cifrado la información, se deja en cada carpeta la nota de rescate** (Ru.txt) indicando las redes sociales del grupo KillNet.



Las **extensiones de archivos que este ransomware busca cifrar** son:

.txt	.jar	.dat	.contact	.settings	.doc	.docx	.xls	.xlsx	.ppt
.pptx	.odt	.jpg	.mka	.mhtml	.oqy	.png	.csv	.py	.sql
.mdb	.php	.asp	.aspx	.html	.htm	.xml	.psd	.pdf	.xla
.cub	.dae	.indd	.cs	.mp3	.mp4	.dwg	.zip	.rar	.mov
.rtf	.bmp	.mkv	.avi	.apk	.lnk	.dib	.dic	.dif	.divx
.iso	.7zip	.ace	.arj	.bz2	.cab	.gzip	.lzh	.tar	.jpeg
.xz	.mpeg	.torrent	.mpg	.core	.pdb	.ico	.pas	.db	.wmv
.swf	.cer	.bak	.backup	.accdb	.bay	.p7c	.exif	.vss	.raw
.m4a	.wma	.flv	.sie	.sum	.ibank	.wallet	.css	.js	.rb
.crt	.xlsm	.xlsb	.7z	.cpp	.java	.jpe	.ini	.blob	.wps
.docm	.wav	.3gp	.webm	.m4v	.amv	.m4p	.svg	.ods	.bk
.vdi	.vmdk	.onepkg	.accde	.jsp	.json	.gif	.log	.gz	.config
.vb	.m1v	.sln	.pst	.obj	.xlam	.djvu	.inc	.cvs	.dbf
.tbi	.wpd	.dot	.dotx	.xltx	.pptm	.potx	.potm	.pot	.xlw
.xps	.xsd	.xsf	.xsl	.kmz	.accdr	.stm	.accdt	.ppam	.pps
.ppsm	.1cd	.3ds	.3fr	.3g2	.accda	.accdc	.accdw	.adp	.ai
.ai3	.ai4	.ai5	.ai6	.ai7	.ai8	.arw	.ascx	.asm	.asmx
.avs	.bin	.cfm	.dbx	.dcm	.dcr	.pict	.rgbe	.dwt	.f4v
.exr	.kwm	.max	.mda	.mde	.mdf	.mdw	.mht	.mpv	.msg
.myi	.nef	.odc	.geo	.swift	.odm	.odp	.oft	.orf	.pfx
.p12	.pl	.pls	.safe	.tab	.vbs	.xlk	.xlm	.xlt	.xltm
.svgz	.slk	.tar.gz	.dmg	.ps	.psb	.tif	.rss	.key	.vob
.epsp	.dc3	.iff	.onepkg	.onetoc2	.opt	.p7b	.exe	.lnk	

Es **importante que las organizaciones identifiquen constantemente las amenazas** que están **activas en todo el mundo** y a su vez, **perfilarlas para saber si pueden llegar a afectar** dicha organización o realmente se salen del mapa de objetivos del grupo y/o amenaza. Actualmente **KillNet parece ser un grupo que busca atacar a entidades que de algún modo están apoyando a Ucrania**, por lo que toma un papel importante en la guerra que continúa en curso actualmente.

El

De acuerdo con la información obtenida sobre este actor de amenazas, el equipo de CTI presenta las siguientes **recomendaciones**:

- Mantener **actualizado el software** utilizado en las organizaciones.
- De ser posible **habilitar la autenticación multifactor** en las aplicaciones utilizadas.
- Implementar **segmentación de redes** según el rol y funcionalidad de los servicios y usuarios.
- Establecer un **playbook interno** en el que se plasme qué y quién debería realizar las acciones necesarias para gestionar una incidencia de tipo Denegación de Servicios (DoS).
- **Ubicar los servicios que se deben publicar en una DMZ** para evitar que, si el servidor es vulnerado puedan tener acceso a la red interna.
- Identificar e implementar las medidas necesarias para **garantizar redundancia y balance de carga** a todos los niveles (servidores, canal de internet, dispositivos de seguridad).
- Contar con un **firewall para aplicaciones web** en cada uno de los servicios publicados.
- Establecer **métodos tempranos para identificar la generación de persistencia** en los equipos y servidores.

A partir de la investigación realizada, el **equipo de CTI de Mnemo da a conocer** a sus clientes este tipo de amenazas a tal nivel de detalle, que permite la identificación de la amenaza teniendo en cuenta los comportamientos y herramientas que utiliza para así, generar **medidas de contención basados en indicadores de alto nivel y no solo en indicadores de compromiso.**

A continuación, se comparte una **regla yara** creada por el equipo de CTI; con el fin de que las diferentes entidades puedan utilizar para identificar esta amenaza.

```
rule Ransomware_KillNet {
    meta:
        author = "Cyber Threat Intelligence - Mnemo"
        description = "Detects KillNet ransomware"
    strings:
        $s1 = "<EncyptedKey>" fullword wide
        $s2 = "<EncryptedKey>" fullword wide
        $s3 = "C:\\Users\\" fullword wide
        $s4 = "read_it.txt" fullword wide
        $s5 = "#base64Image" fullword wide
        $s6 = "(?:[13]{1}[a-km-zA-HJ-NP-Z1-9]{26,33}|bc1[a-z0-9]{39,59})" fullword wide
        $s7 = /check(Spread|Sleep|AdminPrivilage|deleteShadowCopies|disableRecoveryMode|deleteBackupCatalog)/ fullword ascii nocase
        $s8 = /(delete|disable)(ShadowCopies|RecoveryMode|BackupCatalog)/ fullword ascii nocase
        $s9 = "spreadName" fullword ascii
        $s10 = "processName" fullword ascii
        $s11 = "sleepOutOfTempFolder" fullword ascii
        $s12 = "AlreadyRunning" fullword ascii
        $s13 = "random_bytes" fullword ascii
        $s14 = "encryptDirectory" fullword ascii nocase
        $s15 = "EncryptFile" fullword ascii nocase
        $s16 = "intpreclp" fullword ascii
        $s17 = "bytesToBeEncrypted" fullword ascii
        $s18 = "textToEncrypt" fullword ascii
        $s19 = "killnet" wide ascii
        $m1 = "Chaos is" wide
        $m2 = "Payment informationAmount:" wide
        $m3 = "Coinmama - hxxps://www.coinmama.com Bitpanda - hxxps://www.bitpanda.com" wide
        $m4 = "where do I get Bitcoin" wide
    condition:
        uint16(0) == 0x5a4d and 6 of ($s*) or all of ($m*) or (2 of ($m*) and 4 of ($s*))
}
```