CIBERBOLETÍN

OCTUBRE 2022

TEMA DEL MES

Guacamaya dirige ataques contra organizaciones de habla hispana

VULNERABILIDADES

Las 10 vulnerabilidades más representativas de 692 que fueron identificadas en el mes de octubre 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

Troyano bancario Alien, una amenaza que afecta a dispositivos móviles

MNEMO

El

TEMA DEL MES

Guacamaya dirige ataques contra organizaciones de habla hispana

Filtraciones de información en distintas instituciones gubernamentales en América Latina

A finales del mes de septiembre un grupo de actores de amenaza llamado **Guacamaya** afirmó haber **filtrado 10 Terabytes de correos electrónicos de organizaciones militares y policiales en varios países de América Latina**. De acuerdo con una serie de investigaciones, Guacamaya es un grupo que dirige sus ataques a **empresas del sector de la minería y el petróleo**, aunque su actividad también se habría enfocado hacia **instituciones gubernamentales latinoamericanas desde marzo de 2022**.

Durante el mes de septiembre **se identificó la filtración de información de diferentes instituciones de Gobierno**, entre las que se encuentran:

- La Secretaría de la Defensa Nacional de México (6TB)
- La Policía Nacional Civil de El Salvador (6.8 TB)
- Fuerza Armada de El Salvador (73 GB)
- El Comando General de las Fuerzas Militares de Colombia (420 GB)
- El Comando Conjunto de las Fuerzas Armadas de Perú (35 GB)
- El Ejército de Perú (70 GB)

El grupo menciona que **la información no está a la venta** y únicamente se encuentra **disponible para periodistas e investigadores** acreditados. Estos deben exponer los motivos por los que desean acceder a los datos filtrados mediante uno de los dos correos electrónicos facilitados por el grupo.

Guacamaya indica que, para comprometer a las organizaciones y obtener acceso inicial a los sistemas, **aprovecha vulnerabilidades de seguridad en los dispositivos**. Para la mayoría de los compromisos **utilizan una serie de fallas en servidores Microsoft Exchange denominadas ProxyShell**. En el caso de México se utilizó una vulnerabilidad en el software Zimbra, usado para la gestión de correos electrónicos.

Las vulnerabilidades aprovechadas por los atacantes tienen asignados los siguientes **identificadores**:

1. CVE-2022-37042 (CVSS v3.1: 9.8 [Crítico]) - Zimbra Collaboration Suite
2. CVE-2021-34473 (CVSS v3.1: 9.8 [Crítico]) - Microsoft Exchange Server
3. CVE-2021-34523 (CVSS v3.1: 9.8 [Crítico]) - Microsoft Exchange Server
4. CVE-2021-31207 (CVSS v3.1: 7.2 [Alto]) - Microsoft Exchange Server
5. CVE-2022-27925 (CVSS v3.1: 7.2 [Alto]) - Zimbra Collaboration Suite

El

El aprovechamiento de las vulnerabilidades en Microsoft Exchange permite que un actor malicioso no autenticado **ejecute código de forma remota y obtenga privilegios de SYSTEM en la instancia afectada**.

En el caso de las **vulnerabilidades en Zimbra**, la falla con identificador CVE-2022-27925 permite a un usuario no autenticado **cargar archivos arbitrarios al sistema con privilegios de administrador**, lo que puede derivar en un **ataque del tipo "directorio transversal"**, **permitiendo el acceso a directorios** a los que no debería poder ingresar. Por su parte, la vulnerabilidad CVE-2022-37042 **surge de una actualización incompleta** de la anterior mencionada con las mismas características de aprovechamiento.

De acuerdo con un **seguimiento realizado por parte de Mnemo-CERT**, **hasta el día 25 de octubre del año en curso, se identificó la siguiente cantidad de servidores Zimbra y Exchange expuestos a Internet** y posiblemente vulnerables a estas fallas de seguridad:

País	Dispositivos Exchange expuestos	Dispositivos Zimbra expuestos
Colombia	31,034	790
España	171,717	913
Estados Unidos	8,180,143	7,291
México	66,151	795

A la fecha **no hay IoCs relacionados con Guacamaya** y el aprovechamiento de estas vulnerabilidades.

Referente al grupo Guacamaya, los miembros afirman tener **motivaciones antimperialistas y ecologistas**, estableciendo el siguiente estatuto:

"***No somos defensoras de la naturaleza, somos la naturaleza***"

También mencionan "somos todos, todos los afectados por la invasión y despojo de Abya Yala[1]". Además, culpa al "Norte Global" y su "proyecto civilizatorio desde 1492" de convertir al territorio en una "despensa de los mal llamados recursos naturales".

En un **vídeo realizado por el grupo**, disponible a través de uno de sus canales de contacto, se muestran parte de las **ejecuciones realizadas en el compromiso de los sistemas de las organizaciones**, donde **se visualiza el aprovechamiento de las vulnerabilidades ProxyShell en servidores de Microsoft Exchange**.

[1] *Abya Yala es el nombre más antiguo conocido que se refiere a un territorio americano.*

El

Finalmente se presenta una **línea del tiempo de las actividades realizadas** por el actor de amenazas Guacamaya:

El

Julio Rafael Gutiérrez Aburto

CTI Mnemo México

Guacamaya se presenta como un **grupo motivado por intereses sociales y políticos**, además de tener convicciones claramente definidas. En una entrevista reciente, afirmaban no temer a las represalias, puesto que no aceptan las fronteras y leyes impuestas por un "sistema injusto", lo que supone un **alto peligro para cualquiera que este grupo considere como enemigo**.

Por otra parte, las recientes brechas a los organismos militares y gubernamentales demuestran la **necesidad de constantes mejoras y el robustecimiento de los sistemas, estrategias y políticas de seguridad de las organizaciones**, resaltando aquellas en Latinoamérica, de las cuales se ha evidenciado una carencia en materia de ciberseguridad.

Adicionalmente, vale la pena resaltar que, de acuerdo con información dada a conocer tras los incidentes recientes, varias organizaciones gubernamentales no toman en cuenta la importancia que implica **actualizar sus sistemas informáticos**, lo que deja al descubierto un gran número de vulnerabilidades fácilmente aprovechables por los grupos de amenaza.

El

VULNERABILIDADES

Principales vulnerabilidades de octubre 2022

Apache, Fortinet, VMware, Adobe, Microsoft, GitLab, SAP, Juniper y Tenda

Titulo	Identificador	CVSS	Descripción
Falla de seguridad presente en **Apache**	CVE-2022-42889	CVSS v3.1: 9.8 [Crítico]	Es una vulnerabilidad presente en la biblioteca **Commons Text** versiones **1.5** a la **1.9**, debido a que una función realiza evaluaciones de secuencias de comandos inseguras. Un atacante podría aprovechar la falla y ejecutar código arbitrario.
Falla de seguridad presente en **Fortinet**	CVE-2022-40684	CVSS v3.1: 9.6 [Crítico]	Es un error ubicado en algunas versiones de **FortiOS**, **FortiProxy** y **FortiSwitchManager** causada por una omisión en la autenticación. Un usuario malicioso podría obtener acceso completo al dispositivo al enviar solicitudes HTTP o HTTPS especialmente diseñadas.
Falla de seguridad presente en **VMware**	CVE-2021-39144	CVSS v3.1: 9.8 [Crítico]	Es una falla presente en **VMware Cloud Foundation** versión **3.11** debido a una validación de entrada incorrecta. Un actor malicioso podría ejecutar código arbitrario de manera remota a través de la biblioteca XStream.
Falla de seguridad presente en **Adobe**	CVE-2022-35698	CVSS v3.1: 10.0 [Crítico]	Es una vulnerabilidad de tipo "Cross-site-Scripting" presente en versiones de **Adobe Commerce** y **Magento Open Source** ocasionada por una neutralización incorrecta. Un actor de amenaza con acceso a la red podría aprovechar la falla y ejecutar código arbitrario en la instancia afectada.
Falla de seguridad presente en **Microsoft**	CVE-2022-37968	CVSS v3.1: 10.0 [Crítico]	En una falla presente en **Kubernetes**, que podría permitir a un atacante elevar privilegios y obtener control del clúster de Kubernetes.
Falla de seguridad presente en **GitLab**	CVE-2022-2884	CVSS v3.1: 9.9 [Crítico]	Es un error ubicado en **GitLab CE/EE** versiones anteriores a **15.3.1**, **15.2.3** y **15.2.3**. Un actor malicioso podría elevar privilegios y ejecutar código arbitrario.
Falla de seguridad presente en **SAP**	CVE-2022-39802	CVSS v3.1: 9.9 [Crítico]	Es una falla localizada en **Manufacturing Execution** versiones **15.1**, **15.2** y **15.3** de tipo "path traversal". Un actor de amenaza podría aprovechar esta falla y acceder a directorios restringidos y leer información confidencial.
Falla de seguridad presente en **Adobe**	CVE-2022-35712	CVSS v3.1: 9.8 [Crítico]	Es una falla de tipo "Heap-based Buffer Overflow" presente en **ColdFusion** anteriores a la versión **14.0** y **4.0**. Un usuario malicioso podría sobrescribir el búfer y ejecutar código arbitrario sin privilegios en el equipo afectado.
Falla de seguridad presente en **Juniper**	CVE-2022-22241	CVSS v3.1: 9.8 [Crítico]	Es un error de validación de entrada incorrecta en el componente **J-Web** de Juniper **Networks Junos OS** en variedad de versiones. Un atacante no autenticado podría enviar una solicitud POST especialmente diseñada y acceder a archivos locales sin autorización o ejecutar comandos.
Falla de seguridad presente en **Tenda**	CVE-2022-43260	CVSS v3.1: 9.8 [Crítico]	Es una vulnerabilidad presente en **Tenda AC18** versión **15.03.05.19** de tipo "stack overflow" en el parámetro de tiempo de la función fromSetSysTime. Un actor de amenaza podría aprovechar el error y ejecutar código.

El

MNEMO-CERT presenta las **10 vulnerabilidades más representativas de 692** que fueron identificadas en el mes de **octubre 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 Apache Commons Text** también conocido como **Text4Shell** debido a su similitud de aprovechamiento con la vulnerabilidad presente en Log4j denominada "Log4Shell". **MNEMO-CERT publicó un aviso referente a esta falla**:

- https://mailchi.mp/mnemo.com/aviso-de-vulnerabilidadexpertos-instan-a-las-organizaciones-a-actualizar-la-biblioteca-de-apache-commons-text

En la segunda posición, se ubica una **falla en Fortinet**, la cual **permite que un actor malicioso omita la autenticación del sistema afectado**. **MNEMO-CERT publicó un aviso** referente a esta falla:

- https://mailchi.mp/mnemo.com/aviso-de-vulnerabilidadfortinet-publica-actualizaciones-para-corregir-vulnerabilidades-en-varios-de-sus-productos

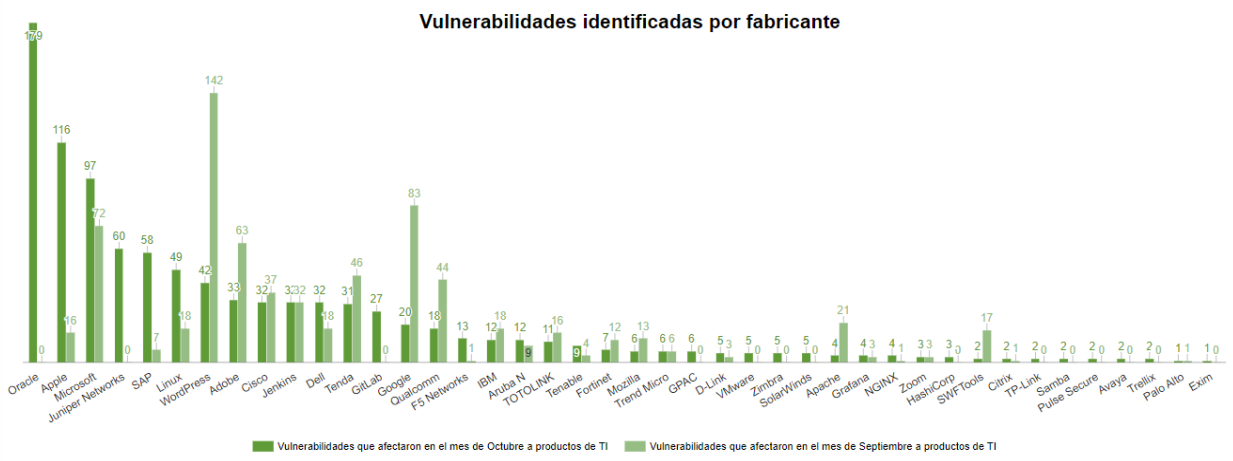
En ambos casos, **se identificaron Pruebas de Concepto** (PoC) **disponibles** en Internet relacionados con estas fallas, las cuales pueden ser consultadas en las siguientes **URLs**:

- https://github.com/ClickCyber/cve-2022-42889
- https://github.com/horizon3ai/CVE-2022-40684

En la tercera posición se encuentra una **vulnerabilidad en VMware**, que podría **permitir a un atacante ejecutar código en la instancia afectada**. **MNEMO-CERT emitió un aviso** relacionado con esta falla que puede ser consultado en la siguiente URL:

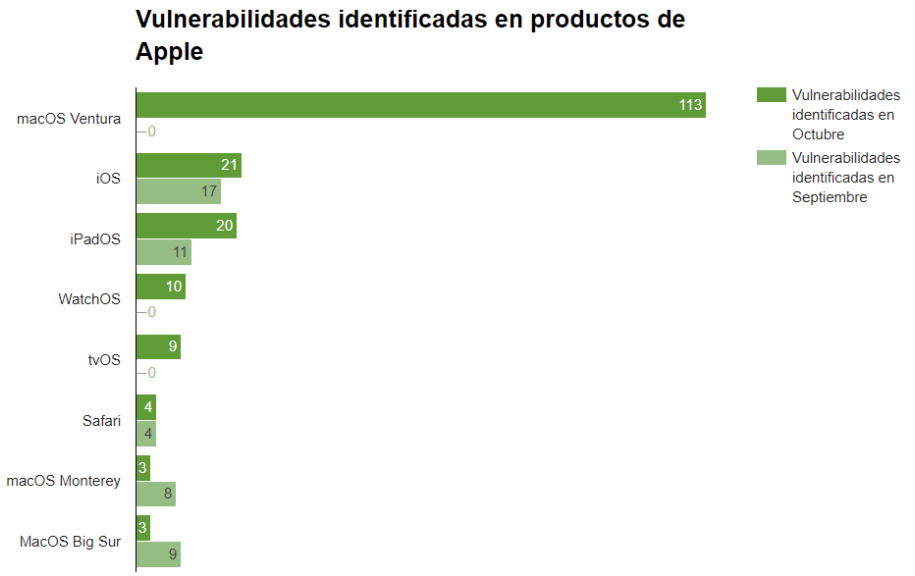
- https://mailchi.mp/mnemo.com/aviso-de-vulnerabilidadvmware-publica-actualizaciones-para-corregir-vulnerabilidades-en-cloud-foundation

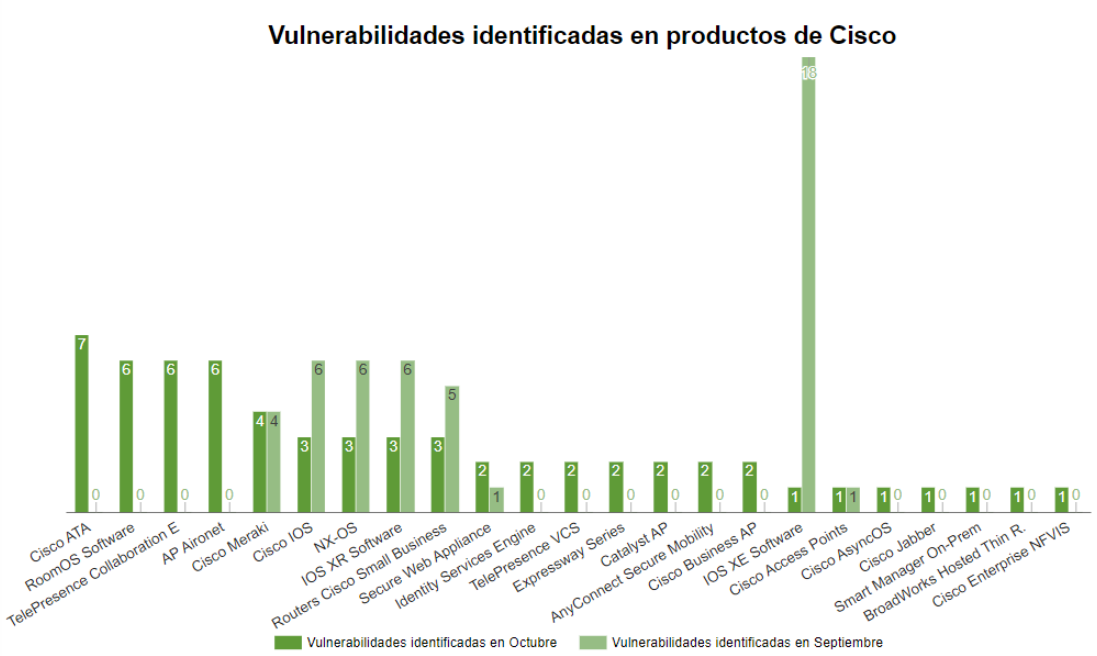
Asimismo, cabe señalar que durante este mes varios **fabricantes corrigieron diversos fallos** en sus diferentes productos, siendo los más destacados "**Oracle**", "**Apple**", "**Microsoft**" y "**Juniper Networks**", a comparación del mes pasado, en donde las más sobresalientes fueron "**WordPress**",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



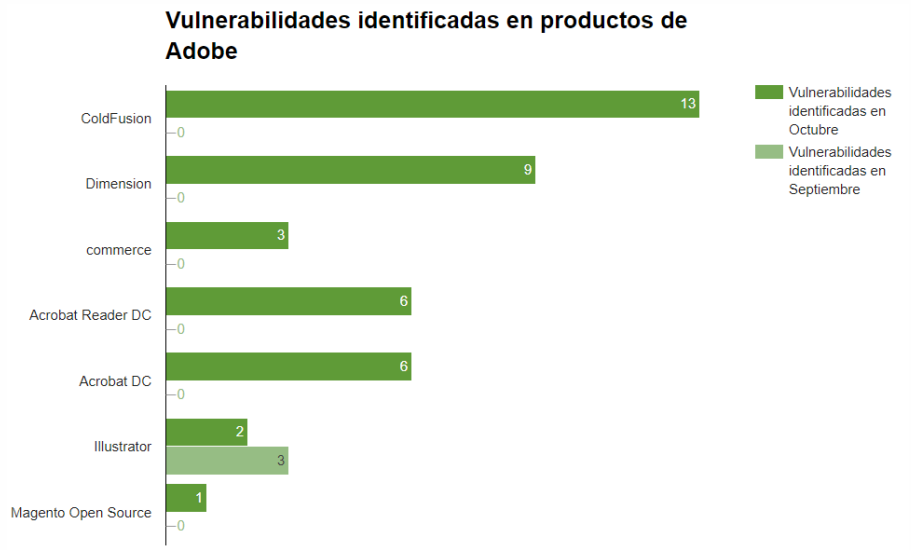
El

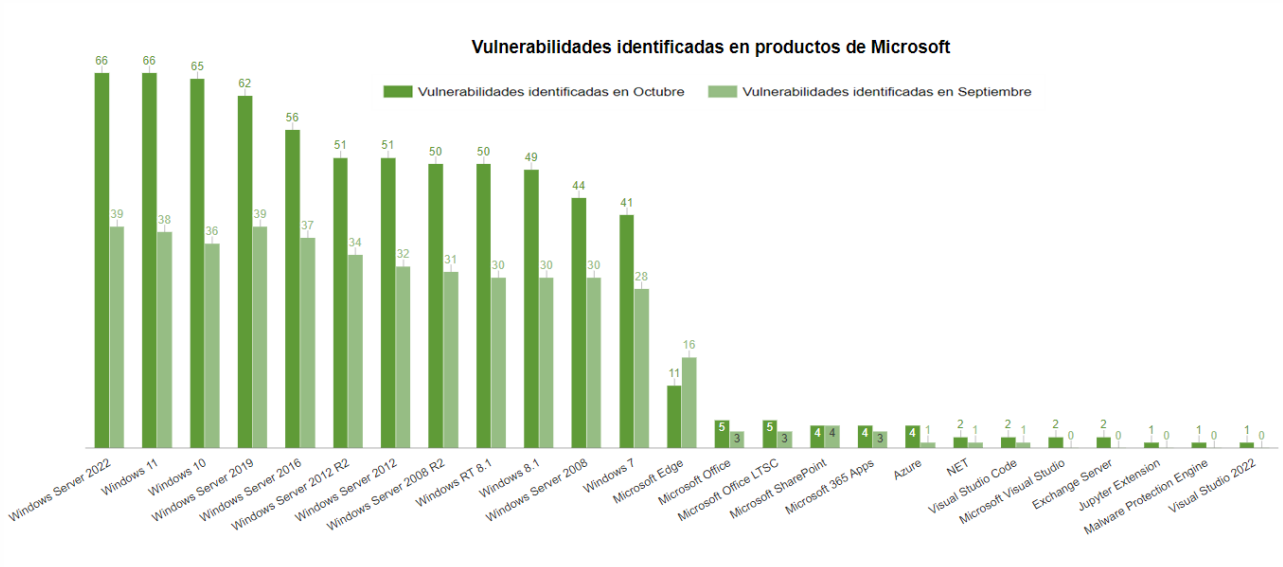
Del mismo modo, en las siguientes gráficas se muestra el **número de vulnerabilidades por producto** para los fabricantes con mayor cantidad de fallas identificadas en el mes de octubre de 2022 y un comparativo con el mes de septiembre.





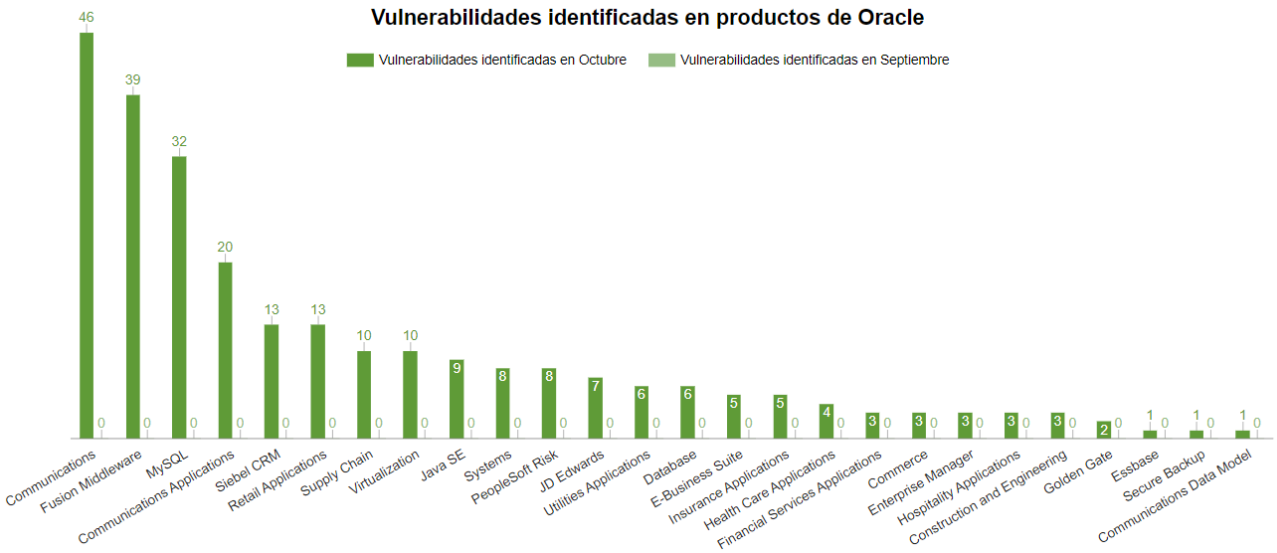
El

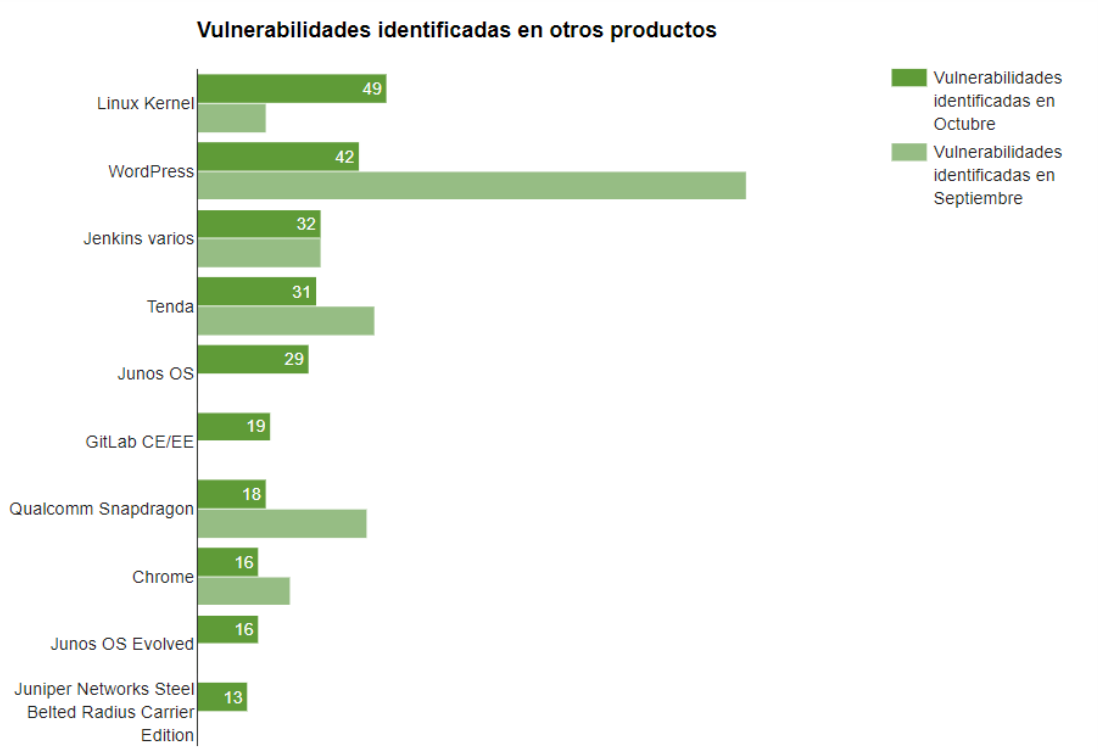

Vulnerabilidades identificadas en productos de Adobe
ColdFusion
Dimension
commerce
Acrobat Reader DC
Acrobat DC
Illustrator
Magento Open Source
13
0
9
0
3
0
6
0
6
0
2
3
1
0
Vulnerabilidades identificadas en Octubre
Vulnerabilidades identificadas en Septiembre


Vulnerabilidades identificadas en productos de Microsoft
Vulnerabilidades identificadas en Octubre
Vulnerabilidades identificadas en Septiembre
Windows Server 2022 66 39
Windows 11 66 38
Windows 10 65 36
Windows Server 2019 62 39
Windows Server 2016 56 37
Windows Server 2012 R2 51 34
Windows Server 2012 51 32
Windows Server 2008 R2 50 31
Windows RT 8.1 50 30
Windows 8.1 49 30
Windows Server 2008 44 30
Windows 7 41 28
Microsoft Edge 11 16
Microsoft Office 5 3
Microsoft Office LTSC 5 3
Microsoft SharePoint 4 4
Microsoft 365 Apps 4 3
Azure 4 1
.NET 2 1
Visual Studio Code 2 1
Microsoft Visual Studio 2 0
Exchange Server 2 0
Jupyter Extension 1 0
Malware Protection Engine 1 0
Visual Studio 2022 1 0


Vulnerabilidades identificadas en productos de SAP
3D Visual Enterprise Viewer
Objects Business Intelligence
Commerce
Customer Data Cloud
Business Objects Platform
Manufacturing Execution
Enable Now
SQL Anywhere
IQ
Data Services Management Console
43
0
6
3
2
0
2
0
1
0
1
0
1
0
1
0
1
0
1
0
Vulnerabilidades identificadas en Octubre
Vulnerabilidades identificadas en Septiembre

El


Vulnerabilidades identificadas en productos de Oracle
Vulnerabilidades identificadas en Octubre
Vulnerabilidades identificadas en Septiembre
46
39
32
20
13
13
10
10
9
8
8
7
6
6
5
5
4
3
3
3
3
3
2
1
1
1
Communications
Fusion Middleware
MySQL
Communications Applications
Siebel CRM
Retail Applications
Supply Chain
Virtualization
Java SE
Systems
PeopleSoft Risk
JD Edwards
Utilities Applications
Database
E-Business Suite
Insurance Applications
Health Care Applications
Financial Services Applications
Commerce
Enterprise Manager
Hospitality Applications
Construction and Engineering
Golden Gate
Essbase
Secure Backup
Communications Data Model


Vulnerabilidades identificadas en otros productos
Linux Kernel
49
WordPress
42
Jenkins varios
32
Tenda
31
Junos OS
29
GitLab CE/EE
19
Qualcomm Snapdragon
18
Chrome
16
Junos OS Evolved
16
Juniper Networks Steel Belted Radius Carrier Edition
13
Vulnerabilidades identificadas en Octubre
Vulnerabilidades identificadas en Septiembre

El

Producto	Vulnerabilidades identificadas en Septiembre	Vulnerabilidades identificadas en Octubre
Aruba InstantOS	0	12
Dell BIOS y Client	11	12
F5 Networks BIG-IP	0	12
TOTOLINK	16	11
Tenable Nessus	4	9
Session Smart Router	0	8
Dell GeoDrive	0	6
GPAC	0	6
Mozilla Firefox	8	6
Trend Micro Apex One	6	6
Dell varios	0	5
D-Link	3	5
GitLab EE	0	5
Zimbra	0	5
Android	0	4
Robotic Process Automation	0	4
Cloud Foundation	0	4
Apache varios	21	4
Dell PowerScale OneFS	3	4
Grafana	3	4
Mozilla Firefox ESR	7	4
Mozilla Thunderbird	12	4
Nginx	1	4
Solarwinds Orion Platform	0	4
Solarwinds Platform	0	4
FortiOS	3	3
FortiTester	0	3
Junos Space	0	3
Dell Hybrid Client	0	3
HashiCorp	0	3
Zoom	3	3
Junos Space	0	3
FortiProxy	0	2
InfoSphere Information Server	1	2
QRadar SIEM	0	2
Vmware ESXi	0	2
VMware vCenter Server	0	2
Avaya	0	2
Citrix Hypervisor	1	2
Dell Container Storage Modules	0	2
GitLab	0	2
Pulse Secure	0	2
Samba	0	2
SWFTools	17	2
TP-Link	0	2
Trellix	0	2
FortiManager	1	1
FortiAnalyzer	1	1
FortiSwitch	0	1
Sterling Partner Engagement Manager	1	1
CICS TX	0	1
Navigator Mobile Android	0	1
WebSphere	2	1
vRealize Operations	0	1
Exim	0	1
F5 Networks F5OS-A	0	1
GitLab EE/CE	0	1
Palo Alto Networks PAN-OS	0	1
Solarwinds SQL Sentry	0	1
Junos OS PTX Series	0	1

El

THREAT INTELLIGENCE

Troyano bancario Alien

Amenaza que afecta a dispositivos móviles

Una de las amenazas que impacta de manera significativa al sector financiero y a sus usuarios son los **troyanos bancarios**, en especial aquellos **dirigidos a los sistemas operativos Android**, en gran parte debido a que el uso de estos dispositivos se ha **incrementado exponencialmente por la variedad de funciones y facilidad en la ejecución** de diferentes actividades como movimientos bancarios, compras en sitios web, ingreso a cuentas de correo electrónico, entre otras.

Aunado a lo anterior, **algunas compañías se han acogido a la política BYOD** (Bring Your Own Device – trae tu propio dispositivo), la cual **promueve el uso de dispositivos personales para acceder a los recursos corporativos**, lo que representa **menores costos** para las empresas; no obstante, **las medidas de seguridad** implementadas **no son tan robustas** como las empleadas en los equipos de cómputo, lo que **los hace vulnerables**, permitiendo que los ciberdelincuentes aprovechen estas debilidades para dirigir sus ataques a estos dispositivos con el fin de obtener información sensible.

Sólo en los primeros cinco meses de este año se observó un **incremento en más del 40%** en las familias de **malware** que afectan a los **sistemas operativos Android**. Sumado a esto, esta tendencia va de la mano con el **descubrimiento constante de aplicaciones maliciosas en Google Play Store** y en otros sitios que buscan engañar a los usuarios para realizar distribución de malware.

De otro lado, **los troyanos bancarios dirigidos a dispositivos Android** como la mayoría de las amenazas identificadas, están **en constante evolución** actualizando sus capacidades y características para causar mayor impacto. Un ejemplo de ello está el **caso de Alien**, una amenaza conocida por primera vez en febrero de 2020 y ofrecida en foros clandestinos como MaaS (Malware as a Service) que, en su última versión, **busca obtener privilegios elevados en el dispositivo comprometido** y realizar **acciones maliciosas a través suplantación de aplicaciones**.

Alien, que al parecer **es una bifurcación del troyano bancario CerberusV1** por su similitud en la estructura de su código. Cuenta con capacidades que le **permiten al ciberdelincuente ejecutar acciones como eludir las medidas de seguridad de dos factores** (2FA) **para obtener las credenciales** de sus víctimas, logrando capturar contraseñas de al menos 226 aplicaciones móviles, entre las que se encuentran **apps bancarias** como Bank of America Mobile Banking y Capital One Mobile, así como apps de **redes sociales** como Telegram, Snapchat y del **correo** como Microsoft Outlook.

El

De la misma manera, Alien cuenta con **técnicas que le permiten la evasión de detección de malware** por parte de Google, **instalación y navegación desde TeamViewer**[2], **monitoreo de las acciones del usuario**, **cambios en la configuración** del dispositivo, **interacción con otras aplicaciones**, **distribución a través de SMS** a los contactos del dispositivo comprometido, **registro de pulsaciones de teclado** y **superposición de pantalla**.

Teniendo en cuenta estas capacidades y en atención al impacto que ha generado este troyano en diferentes entidades a nivel global, que seguirá ocasionando, el equipo de **Cyber Threat Intelligence de Mnemo ha realizado análisis de una muestra que ha sido utilizada en campañas de Alien**, observando lo siguiente:

Los actores maliciosos detrás de Alien **utilizan como vector de infección la tienda oficial de Google Play Store,** suplantando aplicaciones como Flash Player, Fitness4Everybody, Google Update, FitnessTrainer, InPost, Bildirim, DHL, e-Devlet, MobdroTV, AndroidUpdate11.18, Player Sistem Güncelleme, entre otras, **evadiendo los controles implementados por Google Play Protect**; además de **enviar mensajes SMS tipo smishing** a los contactos de los dispositivos comprometidos, con un texto **que persuade a las víctimas a realizar la descarga de la app maliciosa**.

Por otro lado, también se observó que **este troyano bancario es ofrecido en sitios clandestinos**, en donde relacionan sus características y precio. Este último varía de acuerdo con el tiempo de uso, como se puede observar en la siguiente imagen.

Fuente: CTI Mnemo

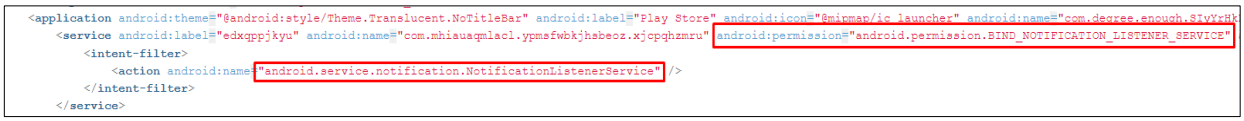
[2] Aplicación que brinda acceso remoto completo al dispositivo infectado.

El

La aplicación maliciosa **requiere acceso a 34 permisos del dispositivo**, de los cuales **16 son considerados peligrosos**, toda vez que permite que los ciberdelincuentes puedan abusar de ellos. En la siguiente tabla se presenta una descripción de algunos de ellos:

Nombre del permiso	Información	Descripción
ACCESS_BACKGROUND_LOCATION	Ubicación de acceso en segundo plano	Permite que la aplicación acceda a la ubicación en segundo plano.
GET_ACCOUNTS	Enumerar cuentas	Permite el acceso a la lista de cuentas en el Servicio de Cuentas.
GET_TASKS	Recuperar aplicaciones en ejecución	Permite que la aplicación recupere información sobre las tareas que se están ejecutando actualmente y de manera reciente. Puede permitir que las aplicaciones maliciosas descubran información privada sobre otras aplicaciones.
READ_CONTACTS	Leer datos de contacto	Permite que una aplicación lea todos los datos de contactos (direcciones) almacenados en su teléfono. Las aplicaciones maliciosas pueden usar esto para enviar sus datos a otras personas.
RECEIVE_SMS	Recibir SMS	Permite que la aplicación reciba y procese mensajes SMS. Las aplicaciones maliciosas pueden monitorear sus mensajes o eliminarlos sin mostrárselos.
RECORD_AUDIO	Grabar audio	Permite que la aplicación acceda a la ruta de grabación de audio.
SEND_SMS	Enviar mensajes SMS	Permite que la aplicación envíe mensajes SMS. Las aplicaciones maliciosas pueden costarle dinero al enviarle mensajes sin su confirmación.
SYSTEM_ALERT_WINDOW	Mostrar alertas a nivel del sistema	Permite que una aplicación muestre ventanas de alerta del sistema. Las aplicaciones maliciosas pueden apoderarse de toda la pantalla del teléfono.
WRITE_EXTERNAL_STORAGE	Leer/modificar/eliminar contenidos de almacenamiento externo	Permite que una aplicación escriba en el almacenamiento externo.

Por otro lado, Alien configu**ra el servicio de notificaciones para leer y modificar las notificaciones recibidas** en el dispositivo; esta actividad permite a los actores de amenaza interceptar todas las notificaciones como OTP (One Time Password, contraseña de único uso utilizada como segundo factor de autenticación), mensajes personales, entre otros.



Fuente: CTI Mnemo

El

Asimismo, **se configura la app fraudulenta como aplicación para el envío de mensajes** en el dispositivo móvil, actuando como aplicación de mensajería predeterminada, por lo que este troyano **podrá enviar, recibir y manejar los mensajes SMS y MMS**.

```
<intent-filter>
    <action android:name="android.intent.action.SEND" />
    <action android:name="android.intent.action.SENDTO" />
    <category android:name="android.intent.category.DEFAULT" />
    <category android:name="android.intent.category.BROWSABLE" />
    <data android:scheme="sms" />
    <data android:scheme="smsto" />
    <data android:scheme="mms" />
    <data android:scheme="mmsto" />
</intent-filter>
```

Fuente: CTI Mnemo

De igual forma, a través de la siguiente configuración el actor de amenaza utiliza una API de administración de dispositivos, que le proporciona al ciberdelincuente **funciones de administración de dispositivos a nivel del sistema**.

```
<service android:name="com.mhiauaqmlacl.ypmsfwbkjhsbeoz.bubnjkaluagi" android:exported="false" />
<service android:name="com.mhiauaqmlacl.ypmsfwbkjhsbeoz.vakurcpyiawjef" android:exported="false" />
<activity android:theme="@android:style/Theme.NoDisplay" android:label="" android:name="com.mhiauaqmlacl.ypmsfwbkjhsbeoz.gwsbwjljwqx" android:excludeFromRecents="true" />
<receiver android:label="" android:name="com.mhiauaqmlacl.ypmsfwbkjhsbeoz.fnz" android:permission="android.permission.BIND_DEVICE_ADMIN">
    <meta-data android:name="android.app.device_admin" android:resource="@xml/ozjbjkrbn" />
    <intent-filter android:priority="136">
        <action android:name="android.app.action.DEVICE_ADMIN_DISABLED" />
        <action android:name="android.app.action.ACTION_DEVICE_ADMIN_DISABLE_REQUESTED" />
        <action android:name="android.app.action.DEVICE_ADMIN_ENABLED" />
    </intent-filter>
</receiver>
```

Fuente: CTI Mnemo

Por otro lado, el cibercriminal puede ejecutar otras **actividades como realizar encendido y apagado de la pantalla, conocer el estado de la batería y reiniciar del equipo**.

```
<receiver android:name="com.mhiauaqmlacl.ypmsfwbkjhsbeoz.lywl" android:permission="android.permission.BROADCAST_SMS">
    <intent-filter android:priority="993">
        <action android:name="android.intent.action.BOOT_COMPLETED" />
        <action android:name="android.intent.action.ACTION_POWER_CONNECTED" />
        <action android:name="android.intent.action.BATTERY_OKAY" />
        <action android:name="android.net.wifi.WIFI_STATE_CHANGED" />
        <action android:name="android.intent.action.SCREEN_OFF" />
        <action android:name="android.intent.action.DREAMING_STOPPED" />
        <category android:name="android.intent.category.HOME" />
        <category android:name="android.intent.action.QUICKBOOT_POWERON" />
        <action android:name="android.net.conn.CONNECTIVITY_CHANGE" />
        <action android:name="android.intent.action.ACTION_POWER_DISCONNECTED" />
        <action android:name="android.intent.action.BATTERY_LOW" />
        <action android:name="android.intent.action.SCREEN_ON" />
        <action android:name="android.intent.action.BATTERY_CHANGED" />
        <action android:name="android.intent.action.REBOOT" />
        <action android:name="android.intent.action.EXTERNAL_APPLICATIONS_AVAILABLE" />
        <action android:name="android.provider.Telephony.SMS_RECEIVED" />
        <action android:name="com.htc.intent.action.QUICKBOOT_POWERON" />
        <action android:name="android.intent.action.USER_PRESENT" />
        <action android:name="android.intent.action.PACKAGE_ADDED" />
        <action android:name="android.intent.action.PACKAGE_REMOVED" />
        <action android:name="android.provider.Telephony.SMS_DELIVER" />
    </intent-filter>
```

Fuente: CTI Mnemo

El

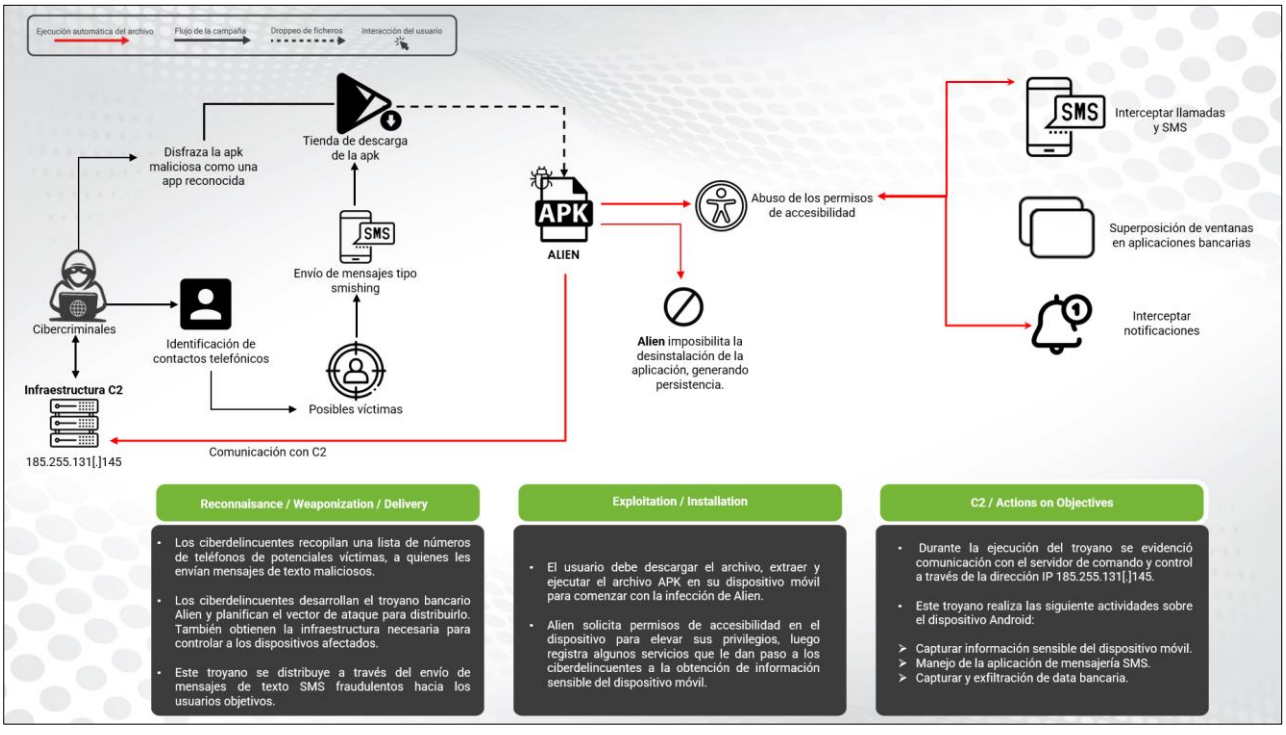
Adicionalmente, Alien habilita el servicio de accesibilidad que es utilizado para ayudar a los usuarios con discapacidades; sin embargo, las aplicaciones maliciosas se aprovechan de este servicio para **interceptar y monitorear todas las actividades que suceden en la pantalla del dispositivo**; un ejemplo de ello es la captura de credenciales que se ingresen en otra aplicación.

```
<service android:label="Play Store" android:name="com.mhiauaqmlacl.ypmsfwbkjhsbeoz.ojfiq" android:permission="android.permission.BIND_ACCESSIBILITY_SERVICE">
    <intent-filter>
        <action android:name="android.accessibilityservice.AccessibilityService" />
    </intent-filter>
    <meta-data android:name="android.accessibilityservice" android:resource="@xml/kxtxfwkalotsegdc" />
</service>
```

Fuente: CTI Mnemo

Aunado a lo anterior, es de indicar que la **aplicación no permite su desinstalación**, imposibilitando el acceso a la información de la app una vez instalada, lo que dificulta que el usuario realice acciones que la puedan dejar sin funcionamiento.

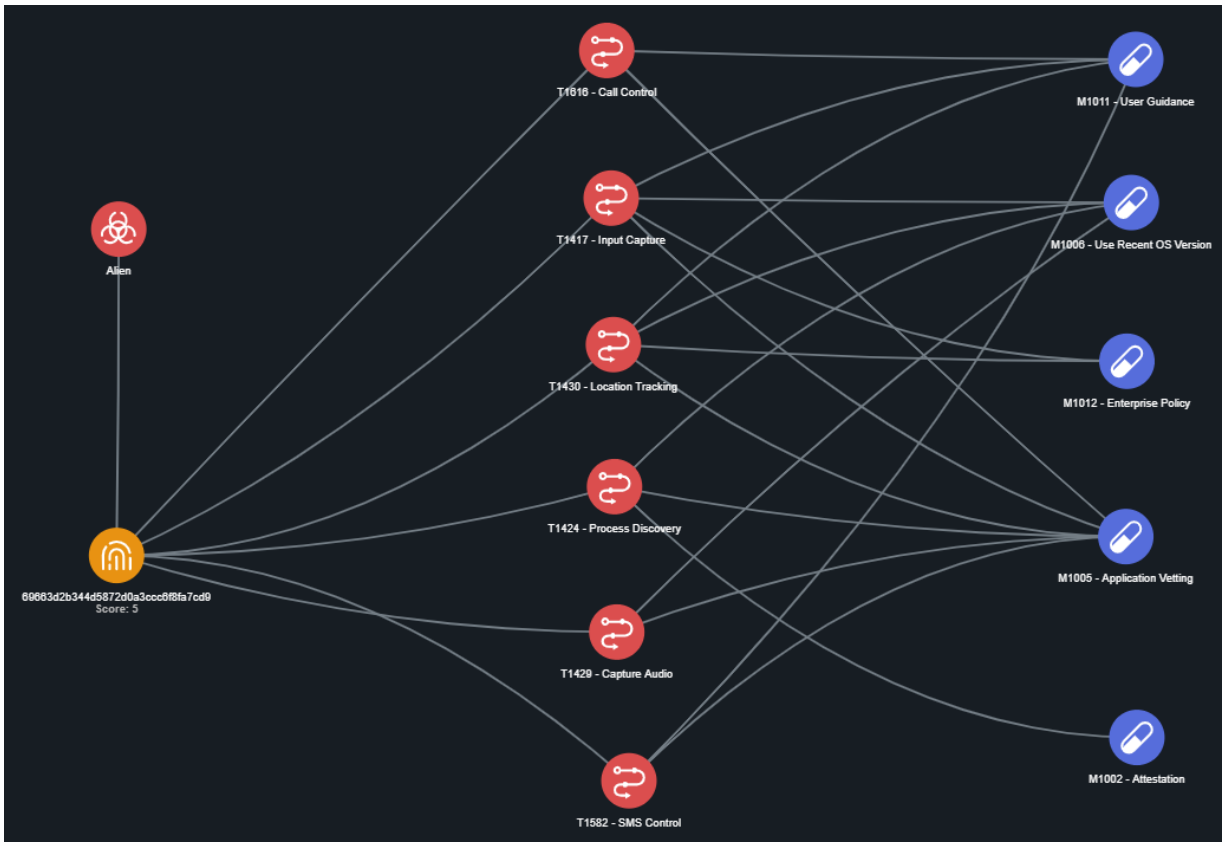
En la siguiente imagen se puede observar el **modelado de la campaña** analizada anteriormente, ejecutada por los actores de amenaza detrás del troyano bancario Alien:



Fuente: CTI Mnemo

El

Continuando con la investigación, el equipo de CTI de Mnemo realizó **correlación de la información asociada al comportamiento de Alien**, identificando que **se relaciona directamente con 11 técnicas de MITRE**, sin embargo, para este artículo **se resaltan 6** de ellas, asociándolas con algunas mitigaciones definidas por Mitre, las cuales se muestran en azul en la siguiente imagen.



Fuente: CTI Mnemo

Además de las mitigaciones que se han identificado para las técnicas, el equipo de CTI ha generado algunas **recomendaciones para tener en cuenta**, con el fin de generar una **defensa robusta** frente a este tipo de amenazas:

- Aunque se ha comprobado que muchas aplicaciones maliciosas logran pasar los filtros establecidos por las tiendas oficiales, la primera recomendación es **instalar el software que requiera desde las tiendas legítimas**, ya que, si se instalan desde tiendas no autorizadas, el riesgo de infección aumenta ya que no hay ningún filtro de seguridad en estas aplicaciones.
- **Revisar los permisos solicitados por las Apps** para identificar anomalías en aquellas aplicaciones que no requieren esas funciones.
- **Mantener actualizados a las versiones más recientes** tanto el sistema operativo como las aplicaciones instaladas en el dispositivo celular.
- **Realizar copia de seguridad** de los datos almacenados en el dispositivo.

El

- **Cerrar la sesión** cuando se finalice el uso de aplicaciones sensibles.
- **Implementar una política y medidas de seguridad** para dispositivos móviles que permitan gestionar los riesgos que se puedan presentar por el uso de estos elementos; conforme lo establece el numeral 6.2.1 del anexo A de la norma ISO-IEC-27001/2013.

Como conclusión es de indicar que **los dispositivos móviles no son ajenos a los ataques** por parte de los ciberdelincuentes, quienes se aprovechan de las vulnerabilidades presentes en estos elementos, así como en el factor humano para lograr la **obtención de información sensible con diferentes propósitos como beneficios económicos a través de fraude** (por medio del control de las cuentas bancarias pueden realizar transferencias y compras), **distribución de crimeware** (software malicioso que se encarga de robar datos financieros), **robo de identidad y daño reputacional**.

Por lo anterior, es de **gran importancia para las organizaciones contar con controles orientados a la protección de los dispositivos móviles** que permitan minimizar los riesgos que se puedan presentar por el uso de estos elementos. Así mismo, **fortalecer la cultura en seguridad de la información en los clientes y usuarios** a través de diferentes actividades enfocadas en crear conciencia y fomentar el uso responsable de estos elementos.

Para finalizar, se anexa una **regla yara la cual permite identificar y clasificar muestras de este troyano bancario**.

```
rule Alien_trojan {
    meta:
        description = "Detect suspicious strings and characters that are related to the Alien trojan"
        reference = "Internal Research"
        date = "2022-10-12"
        author = "Cyber Threat Intelligence"
    strings:
        $s1 = "META-INF/MANIFEST.MF"
        $s2 = "META-INF/TESTKEY.RSA"
        $s3 = "META-INF/TESTKEY.SF"
        $s4 = "res/xml/kxtxfwkalotsegdc.xml"
        $s5 = "/i_message_1.svg"
        $s6 = "omsdk-v1.js"
        $s7 = "mts_sans_bold.otf"
        $s8 = "SegoeWP.ttf"
    condition:
        all of them
}
```

Fuente: CTI Mnemo