Nro. Alerta:	EC-2022-02	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	05-enero-2022	**Nuevo modo de operación de Malware Zloader**	Versión 1.0

I. DATOS GENERALES:

Clase de alerta: Malware
Tipo de incidente: Escalamiento de Privilegios
Nivel de riesgo: Medio

II. ALERTA

Esta amenaza aborda el nuevo modo de operación del Malware Zloader, el mismo que se aprovecha de la verificación de la firma digital de Microsoft para robar información sensible de las víctimas.

Figura 1.- Ilustraciones relacionadas a Zloader
Fuente: Binary Reverse Engineering Blog

III. INTRODUCCIÓN

Zloader es un malware diseñado para grabar toda acción que se realiza en la computadora del infectado, permitiendo robar credenciales de usuario e información privada; cabe señalar que, este malware ha evolucionado en su accionar, por ejemplo:

- Año 2020: Se distribuía a partir de documentos maliciosos, sitios para adultos y anuncios de Google para infectar sistemas.
- Año 2021: Se determinó que el malware incluye nuevas técnicas de infección; incluyendo el uso de software legítimo de administración remota (RMM) para obtener acceso inicial a la máquina de destino; posteriormente, el malware explota el método de verificación de firma digital de Microsoft para inyectar su carga útil en una DLL - Dynamic-

Link Library- del sistema firmada para evadir aún más las defensas del sistema.

IV. VECTOR DE ATAQUE:

A continuación, se describe la cadena de infección:

1. La infección comienza con la entrega de un archivo "Java.msi"; siendo este un instalador modificado del Software Atera[1];este archivo imita una instalación de Java.
2. Posteriormente se instala un agente utilizando un archivo .msi
3. Después de la instalación del agente, el atacante carga y ejecuta el **script load.bat** que descarga y ejecuta **new.bat,** que comprueba los privilegios de administrador y los solicita mediante el **script BatchGotAdmin.**
4. Posteriormente descarga otro archivo bat [**new1.bat**], este script agrega más exclusiones a Windows Defender para diferentes carpetas y deshabilita diferentes herramientas en la máquina que podrían usarse para la detección; también descarga otros archivos en la **carpeta% appdata%**, entre los archivos se pueden mencionar:

    a. **9092.dll:** Carga útil principal, Zloader.
    b. **adminpriv.exe:** Nsudo.exe, que permite ejecutar programas con privilegios elevados.
    c. **appContast.dll:** Se utiliza para ejecutar 9092.dll y new2.bat; es decir ejecuta la carga útil de Zloader y el script de edición del registro, respectivamente. Esta DLL maliciosa lleva una firma de código válida, por lo que el sistema operativo esencialmente confía en él.
    d. **reboot.dll:** También se utiliza para ejecutar 9092.dll.
    e. **new2.bat:** Edita el registro para establecer los privilegios de todas las aplicaciones al nivel de administrador. Para que este cambio surta efecto, es necesario reiniciar, por lo que el malware obliga al sistema infectado a reiniciarse en este punto.
    f. **auto.bat:** ubicado en la carpeta Inicio para la persistencia del inicio.

5. Una vez que el agente está instalado, el atacante tiene acceso al sistema y puede cargar / descargar archivos, ejecutar scripts.
6. El instalador asociado es: **b9d403d17c1919ee5ac6f1475b645677a4c03fe9.**

En la siguiente figura, se observa la cadena de infección de Zloader.

[1] Software de gestión y supervisión remota.

Nro. Alerta:	EC-2022-02	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	05-enero-2022	**Nuevo modo de operación de Malware Zloader**	Versión 1.0

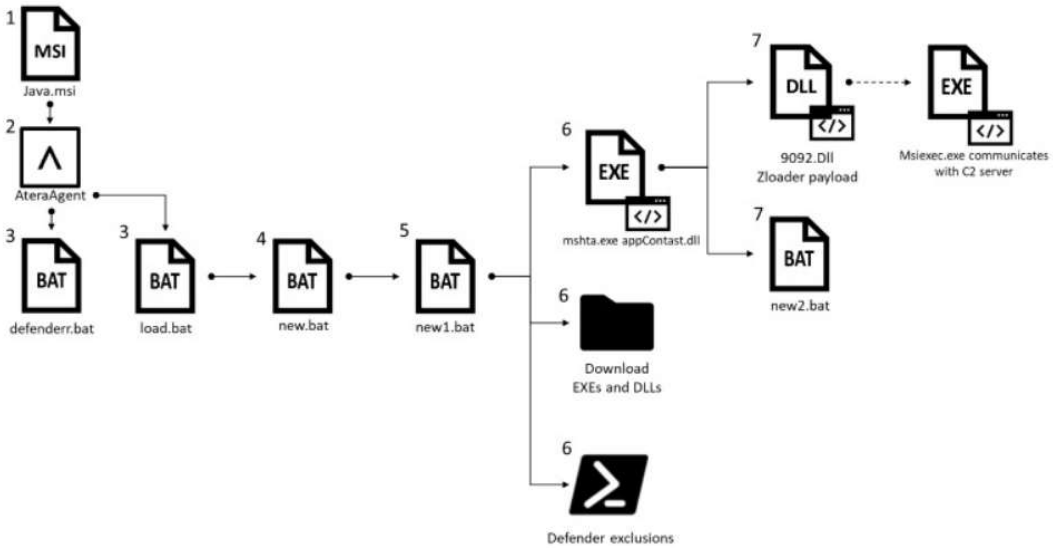
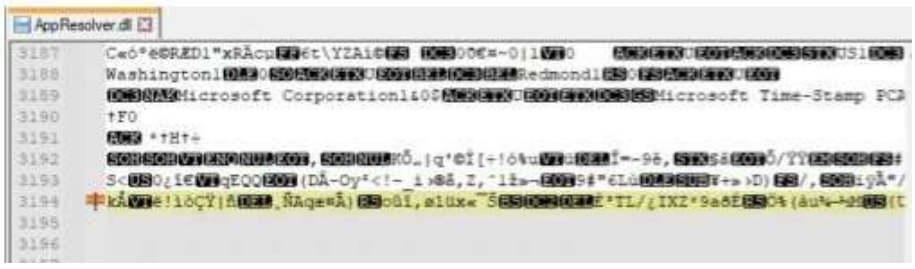


Figura 2.- Cadena de Infección
Fuente: Check Point

V. IMPACTO

El análisis realizado por el grupo de investigación de Check Point Research, encontró ligeras modificaciones entre la **DLL Original [AppResolver.dll]** y la **DLL maliciosa [AppContast.dll];** por ejemplo en la DLL maliciosa, el autor agregó un script al archivo. Estos cambios sutiles no son suficientes para revocar la validez de la firma electrónica, pero al mismo tiempo, permiten que alguien agregue datos en la sección de firma de un archivo.



Nro. Alerta:	EC-2022-02	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	05-enero-2022	**Nuevo modo de operación de Malware Zloader**	Versión 1.0

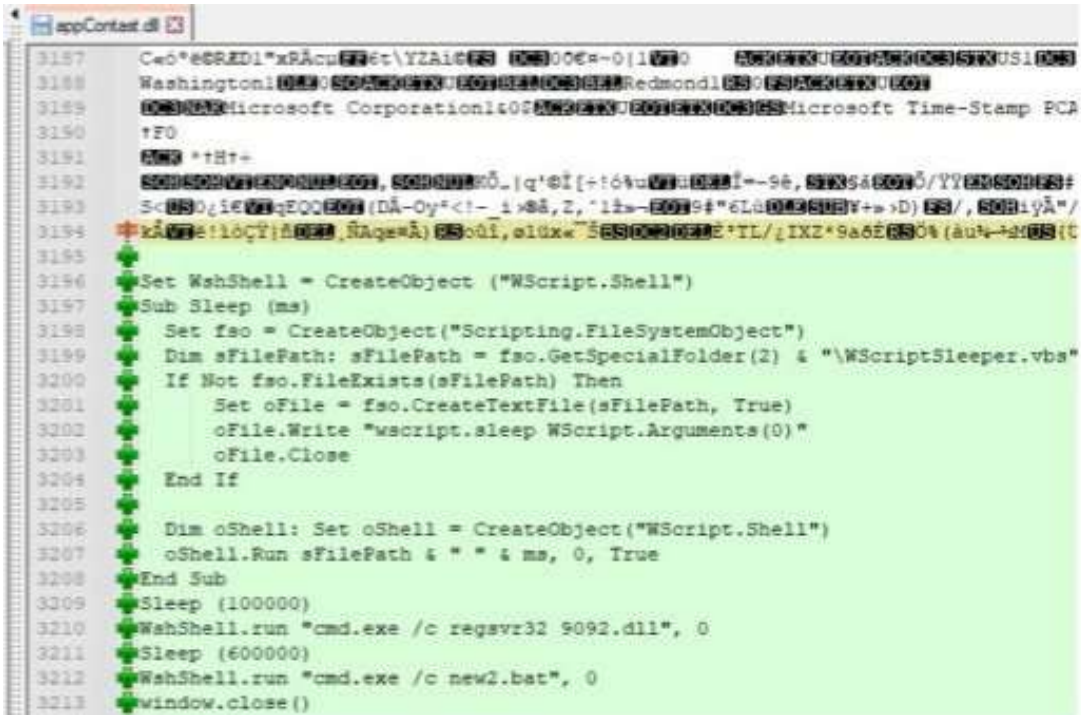


Figura 3.- Comparación de appResolver.dll y appContast.dll
Fuente: Check Point

Finalmente, a partir del 02 de enero del 2022 se ha detectado que alrededor de 2170 direcciones IP han sido afectadas por este Malware; siendo la mayoría de víctimas originarias de Estados Unidos y Canadá.

VI. INDICADORES DE COMPROMISO:

Con base a lo expuesto anteriormente, se tiene que los usuarios afectados por este Malware están expuestos al robo de credenciales de usuario e información privada de las víctimas. En la siguiente figura, se indica los proveedores de seguridad que marcaron como malicioso el presente malware.

Nro. Alerta:	EC-2022-02	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	05-enero-2022	**Nuevo modo de operación de Malware Zloader**	Versión 1.0

Figura 4.- Proveedores de Seguridad que identifican este malware.
Fuente: Virus Total

A continuación, se describen más características de este malware.

Propiedades	Descripción
MD5	a5aae214006bf6eeab3cdf70b087e0ec
SHA-1	b9d403d17c1919ee5ac6f1475b645677a4c03fe9
SHA-256	b5cd3ac0dce6e3b58763ae20ba937c018fa230ce432b6931154103508c109a40
Tipo de archivo	Instalador de ventanas

Tabla 1: Propiedades Básicas Zloader
Fuente: Virus Total

Parámetro	TimeStamp	
Tiempo de creación	2021-10-26	13:42:40
Fecha de firma	2021-11-10	18:46:00
Visto por primera vez	14-11-2021	17:07:41
Primera presentación	2021-11-17	01:01:08
Última presentación	2021-11-17	01:01:08
Último análisis	2022-01-05	18:30:30

Tabla 2: Línea de Tiempo Zloader
Fuente: Virus Total

Finalmente, se describen los Indicadores de Compromiso encontrados:

Nombre del Archivo	Descripción
Defenderr.bat	1CA89010E866FB97047383A7F6C83C00C3F31961
Load.bat	F3D73BE3F4F5393BE1BC1CF81F3041AAD8BE4F8D

Nro. Alerta:	EC-2022-02	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	05-enero-2022	**Nuevo modo de operación de Malware Zloader**	Versión 1.0

Nombre del Archivo	Descripción
Servidores C2	https: // asdfghdsajkl [.] com / gate.php https: // iasudjghnasd [.] com / gate.php https: // kdjwhqejqwij [.] com / gate.php https: // kjdhsasghjds [.] com / gate.php https: // dkisuaggdjhna [.] com / gate.php https: // dquggwjhdmq [.] com / gate.php https: // lkjhgfgsdshja [.] com / gate.php https: // daksjuggdhwa [.] com / gate.php https: // eiqwuggejqw [.] com / gate.php https: // djshggadasj [.] com / gate.php
Archivos	**Java.msi** - B9D403D17C1919EE5AC6F1475B645677A4C03FE9 **new.bat** - 0926F8DF5A40B58C6574189FFB5C170528A6A34D **new1.bat** - 9F1C72D2617B13E591A866196A662FEA590D5677 **new2.bat -** DE0FA1529BC652FF3C10FF16871D88F2D39901A0 **9092.dll -** A25D33F3F8C2DA6DC35A64B16229D5F0692FB5C5, 7A57118EE3122C9BDB45CF7A9B2EFD72FE258771, 2C0BC274BC2FD9DAB82330B837711355170FC606 **Adminpriv.exe -** 3A80A49EFAAC5D839400E4FB8F803243FB39A513 **appContast.dll -** 117318262E521A66ABA4605262FA2F8552903217 **reinicio.dll -** F3B3CF03801527C24F9059F475A9D87E5392DAE9 **auto.bat -** 3EA3B79834C2C2DBCE0D24C73B022A2FF706B4C6

Tabla 3: Indicadores de Compromiso
Fuente: Check Point

VII. RECOMENDACIONES:

El EcuCERT recomienda a su comunidad objetivo:

- Aplicar la actualización de Microsoft para una verificación estricta de Authenticode, para aplicar esta actualización es necesario ejecutar las siguientes líneas de código [extensión .reg]:
  Editor del registro de Windows, versión 5.00
  [HKEY_LOCAL_MACHINE \ Software \ Microsoft \ Cryptography \ Wintrust \ Config]
  "EnableCertPaddingCheck" = "1"
  [HKEY_LOCAL_MACHINE \ Software \ Wow6432Node \ Microsoft \ Cryptography \ Wintrust \ Config]
  "EnableCertPaddingCheck" = "1"

Nro. Alerta:	EC-2022-02	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	
TLP:	TLP:BLANCO		
Fecha:	05-enero-2022	**Nuevo modo de operación de Malware Zloader**	Versión 1.0

- No abrir, manipular, o interactuar con correos electrónicos altamente sospechosos recibidos en las respectivas bandejas de correo ya sea personales o Institucionales; asi mismo, establecer las precauciones necesarias en el caso de instalar software de la página Atera.
- Fortalecer las políticas de seguridad para evitar ser víctimas de cualquier técnica de ingeniería social.
- Mantener actualizados y, en funcionamiento, el software antivirus en cada computador personal o Institucional.

VIII. REFERENCIAS:

Alday, J. (06 de 10 de 2021). *Sistemas AS*. Obtenido de https://assistemas.net/que-es-zloader/

Atera. (s.f.). *Atera*. Obtenido de https://www.atera.com/

Blog, B. R. (s.f.). *Binary Reverse Engineering Blog* . Obtenido de https://bin.re/blog/the-dga-of-zloader/

Cohen, G. (05 de 01 de 2022). *Check Point Researcher*. Obtenido de Check Point Researcher: https://research.checkpoint.com/2022/can-you-trust-a-files-digital-signature-new-zloader-campaign-exploits-microsofts-signature-verification-putting-users-at-risk/

Total, V. (05 de 01 de 2022). *Virus Total*. Obtenido de https://www.virustotal.com/gui/file/b5cd3ac0dce6e3b58763ae20ba937c018fa230ce432b6931154103508c109a40/details

Toulas, B. (05 de 01 de 2022). *BleepingComputer*. Obtenido de BleepingComputer: https://www.bleepingcomputer.com/news/security/microsoft-code-sign-check-bypassed-to-drop-zloader-malware/