I. DATOS GENERALES:

Clase de alerta: Malware

Tipo de incidente: Campaña maliciosa

Nivel de riesgo: Alto

II. ALERTA

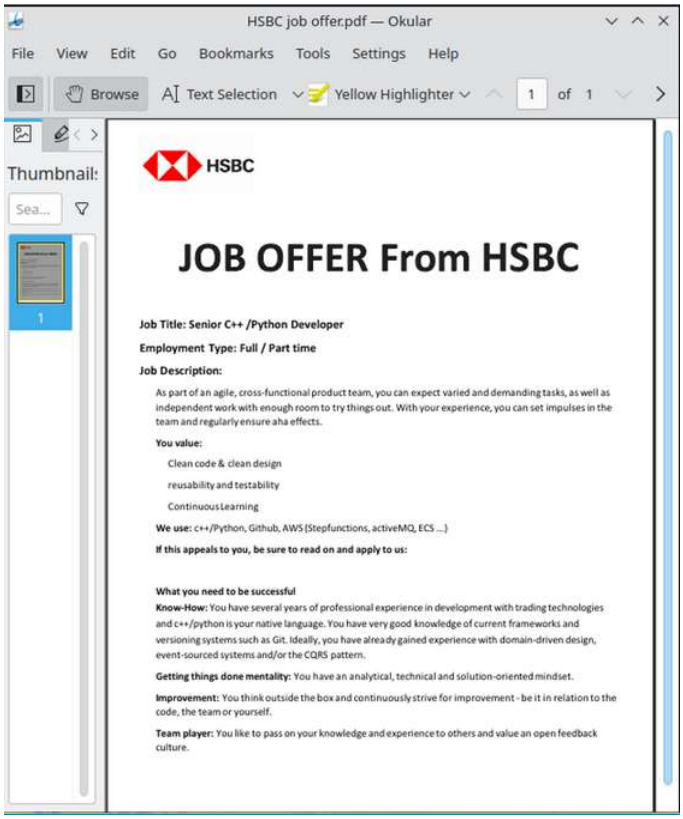

Figura 1.- Un señuelo temático de HSBC en la campaña Linux DreamJob
Fuente: https://www.welivesecurity.com/2023/04/20/linux-malware-strengthens-links-lazarus-3cx-supply-chain-attack/

La Operación DreamJob del grupo Lazarus consiste en acercarse a los objetivos a través de LinkedIn y tentarlos con ofertas de trabajo de los líderes de la industria. El nombre fue acuñado por ClearSky en un artículo publicado en agosto de 2020. Ese artículo describe una campaña de ciberespionaje de Lazarus dirigida a empresas aeroespaciales y de defensa. La actividad se superpone con lo que llamamos Operation In(ter)ception, una serie de ataques de ciberespionaje que han estado en curso desde al menos septiembre de 2019. Se dirige a empresas aeroespaciales, militares y de defensa y utiliza herramientas maliciosas específicas, inicialmente solo para Windows. Durante julio y agosto de 2022, encontramos dos instancias de Operation In(ter)ception dirigidas a macOS. Se envió una muestra de malware a VirusTotal desde Brasil y otro ataque tuvo como objetivo a un usuario de ESET en Argentina. Hace unas semanas, se encontró una carga útil nativa de Linux en VirusTotal con un señuelo de PDF con el tema de HSBC. Esto completa la capacidad de Lazarus para apuntar a todos los principales sistemas operativos de escritorio.

El 20 de marzo, un usuario del país de Georgia envió a VirusTotal un archivo ZIP llamado oferta de trabajo de HSBC.pdf.zip. Dadas otras campañas de DreamJob de Lazarus, esta carga probablemente se distribuyó a través de spearphishing o mensajes directos en LinkedIn. El archivo contiene un solo archivo: un binario Intel Linux nativo de 64 bits escrito en Go y llamado oferta de trabajo de HSBC. pdf.

Curiosamente, la extensión del archivo no es .pdf. Esto se debe a que el caracter de punto aparente en el nombre de archivo es un punto de guía representado por el carácter Unicode U+2024. El uso del punto en el nombre del archivo probablemente fue un intento de engañar al administrador de archivos para que tratara el archivo como un ejecutable en lugar de un PDF. Esto podría hacer que el archivo se ejecute al hacer doble clic en lugar de abrirlo con un visor de PDF. En la ejecución, se muestra un PDF de señuelo al usuario usando xdg-open, que abrirá el documento usando el visor de PDF preferido del usuario (ver Figura 3). Decidimos llamar a este descargador de ELF OdicLoader, ya que tiene una función similar a la de IconicLoaders en otras plataformas y la carga útil se obtiene de OpenDrive.

OdicLoader suelta un documento PDF de señuelo, lo muestra usando el visor de PDF predeterminado del sistema (consulte la Figura 2) y luego descarga una puerta trasera de segunda etapa del servicio en la nube OpenDrive. El archivo descargado se almacena en ~/.config/guiconfigd (SHA-1: 0CA1723AFE261CD85B05C9EF424FC50290DCE7DF). Llamamos a esta puerta trasera de segunda etapa SimplexTea.

Como último paso de su ejecución, OdicLoader modifica ~/.bash_profile, por lo que SimplexTea se inicia con Bash y su salida se silencia (~/.config/guiconfigd >/dev/null 2>&1).

SimplexTea es una puerta trasera de Linux escrita en C++, sus nombres de clase son muy similares a los nombres de funciones que se encuentran en una muestra, con el nombre de archivo sysnetd, enviada a VirusTotal desde Rumania (SHA-1: F6760FB1F8B019AF2304EA6410001B63A1809F1D). Debido a las similitudes en los nombres de clases y nombres de funciones entre SimplexTea y sysnetd, creemos que SimplexTea es una versión actualizada, reescrita de C a C++.

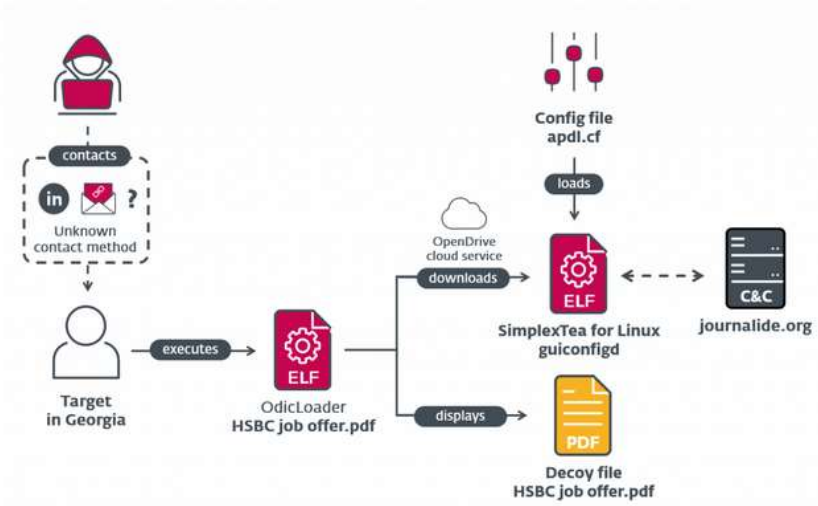

Figura 2.- Ilustración de la probable cadena de compromiso
Fuente: https://www.welivesecurity.com/2023/04/20/linux-malware-strengthens-links-lazarus-3cx-supply-chain-attack/

III. INTRODUCCIÓN

Investigadores de ESET han descubierto una nueva campaña Lazarus Operation DreamJob dirigida a usuarios de Linux. Operation DreamJob es el nombre de una serie de campañas en las que el grupo utiliza técnicas de ingeniería social para comprometer a sus objetivos, con ofertas de trabajo falsas como señuelo. En este caso, reconstruyeron la cadena completa, desde el archivo ZIP que entrega una oferta de trabajo falsa de HSBC

como señuelo, hasta la carga útil final: la puerta trasera SimplexTea Linux distribuida a través de una cuenta de almacenamiento en la nube de OpenDrive. Hasta donde saben, esta es la primera mención pública de este importante actor de amenazas alineado con Corea del Norte que usa malware de Linux como parte de esta operación.

Además, este descubrimiento ayudó a confirmar con un alto nivel de confianza que el reciente ataque a la cadena de suministro de 3CX fue de hecho realizado por Lazarus, un vínculo que se sospechó desde el principio y que varios investigadores de seguridad demostraron desde entonces.

El ataque a la cadena de suministro de 3CX

3CX es un desarrollador y distribuidor internacional de software VoIP que brinda servicios de sistemas telefónicos a muchas organizaciones. Según su sitio web, 3CX tiene más de 600 000 clientes y 12 000 000 de usuarios en varios sectores, incluidos el aeroespacial, el cuidado de la salud y la hospitalidad. Proporciona software de cliente para usar sus sistemas a través de un navegador web, una aplicación móvil o una aplicación de escritorio. A fines de marzo de 2023, se descubrió que la aplicación de escritorio tanto para Windows como para macOS contenía un código malicioso que permitía a un grupo de atacantes descargar y ejecutar código arbitrario en todas las máquinas donde estaba instalada la aplicación. Rápidamente, se determinó que este código malicioso no era algo que 3CX agregó, sino que 3CX estaba comprometida y que su software se usó en un ataque a la cadena de suministro impulsado por actores de amenazas externos para distribuir malware adicional a clientes específicos de 3CX.

Este ciberdelincuente ha sido noticia en los últimos días. Informado inicialmente el 29 de marzo de 2023 en un hilo de Reddit por un ingeniero de CrowdStrike, seguido de un informe oficial de CrowdStrike, afirmando con gran confianza que LABIRINTH CHOLLIMA, el nombre en clave de la compañía para Lazarus, estaba detrás del ataque (pero omitiendo cualquier evidencia que respalde el afirmar). Debido a la gravedad del incidente, varias empresas de seguridad comenzaron a contribuir con sus resúmenes de los eventos, a saber, Sophos, Check Point, Broadcom, Trend Micro y más.

Además, la parte del ataque que afecta a los sistemas que ejecutan macOS se cubrió en detalle en un hilo de Twitter y una publicación de blog de Patrick Wardle.

Cronología de eventos

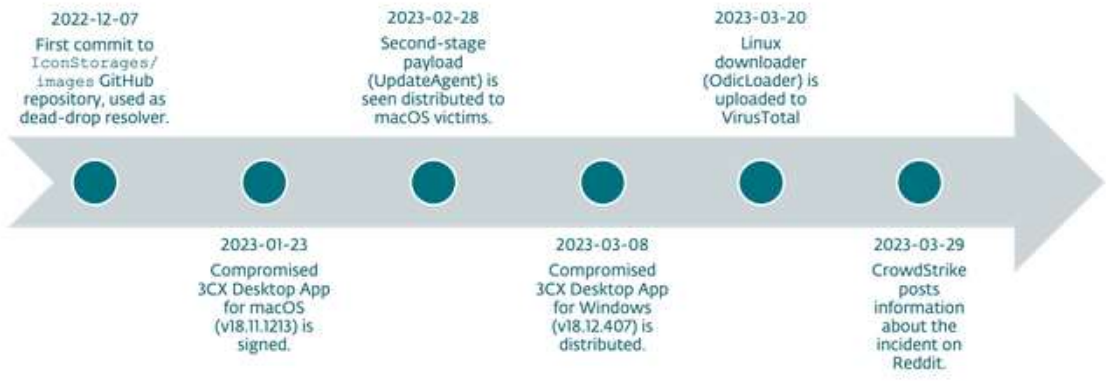

Figura 3. Cronología de eventos relacionados con la preparación y distribución de aplicaciones troyanizadas 3CX
Fuente: https://www.welivesecurity.com/2023/04/20/linux-malware-strengthens-links-lazarus-3cx-supply-chain-attack/

La línea de tiempo muestra que los perpetradores habían planeado los ataques mucho antes de la ejecución; desde diciembre de 2022. Esto sugiere que ya tenían un punto de apoyo dentro de la red de 3CX a fines del año pasado.

Si bien la aplicación 3CX macOS troyanizada muestra que se firmó a fines de enero, no vimos la aplicación incorrecta en nuestra telemetría hasta el 14 de febrero de 2023. No está claro si la actualización maliciosa para macOS se distribuyó antes de esa fecha.

Aunque la telemetría de ESET muestra la existencia de la carga útil de la segunda etapa de macOS ya en febrero, no teníamos la muestra en sí, ni los metadatos para advertirnos sobre su malignidad. Incluimos esta información para ayudar a los defensores a determinar qué tan atrás podrían haberse comprometido los sistemas.

Varios días antes de que se revelara públicamente el ataque, se envió un misterioso descargador de Linux a VirusTotal. Descarga un nuevo payload malicioso de Lazarus para Linux y explicamos su relación con el ataque más adelante en el texto.

IV. VECTOR DE ATAQUE:

Ingeniería social

V. IMPACTO:

Peter Kálnai y Marc-Etienne M. Léveillé, en su publicación del 20 de abril de 2023 a través de https://www.welivesecurity.com/2023/04/20/linux-malware-strengthens-links-lazarus-3cx-supply-chain-attack/, con el título **"Linux malware strengthens links between Lazarus and the 3CX supply-chain attack"** señalan lo siguiente**:**

"(…)

- *El compromiso de 3CX ha llamado mucho la atención de la comunidad de seguridad desde su divulgación el 29 de marzo. Este software comprometido, implementado en varias infraestructuras de TI, que permite la descarga y ejecución de cualquier tipo de carga útil, puede tener efectos devastadores. Desafortunadamente, ningún editor de software es inmune a verse comprometido y distribuir inadvertidamente versiones troyanizadas de sus aplicaciones.*

- *El sigilo de un ataque a la cadena de suministro hace que este método de distribución de malware sea muy atractivo desde la perspectiva de un atacante. Lazarus ya ha utilizado esta técnica en el pasado, apuntando a los usuarios surcoreanos del software WIZVERA VeraPort en 2020. Las similitudes con el malware existente del conjunto de herramientas de Lazarus y con las técnicas típicas del grupo sugieren fuertemente que el reciente compromiso de 3CX también es obra de Lazarus.*

- *También es interesante notar que Lazarus puede producir y usar malware para todos los principales sistemas operativos de escritorio: Windows, macOS y Linux. Tanto los sistemas Windows como macOS fueron atacados durante el incidente de 3CX, y el software VoIP de 3CX para ambos sistemas operativos fue troyanizado para incluir*

código malicioso para obtener cargas útiles arbitrarias. En el caso de 3CX, existen versiones de malware de segunda etapa para Windows y macOS. Este artículo demuestra la existencia de una puerta trasera de Linux que probablemente corresponde al malware SIMPLESEA macOS visto en el incidente de 3CX. Llamamos a este componente de Linux SimplexTea y demostramos que es parte de Operation DreamJob, la campaña insignia de Lazarus que utiliza ofertas de trabajo para atraer y comprometer a víctimas desprevenidas. (…)".

VI. INDICADORES DE COMPROMISO

- **Archivos:**

SHA-1	Nombre del archivo	Nombre de detección de ESET	Descripción
0CA1723AFE261CD85B05C9EF424FC50290DCE7DF	guiconfigd	Linux/NukeSped.E	SimplexTea for Linux.
3A63477A078CE10E53DFB5639E35D74F93CEFA81	HSBC_job_offer. pdf	Linux/NukeSped.E	OdicLoader, a 64-bit downloader for Linux, written in Go.
9D8BADE2030C93D0A010AA57B90915EB7D99EC82	HSBC_job_offer.pdf.zip	Linux/NukeSped.E	A ZIP archive with a Linux payload, from VirusTotal.
F6760FB1F8B019AF2304EA6410001B63A1809F1D	sysnetd	Linux/NukeSped.G	BADCALL for Linux.

- **Red:**

Dirección IP	Dominio	Proveedor de alojamiento	Visto por primera vez	Detalles
23.254.211[.]230	N/A	Hostwinds LLC.	N/A	C&C server for BADCALL for Linux

38.108.185[.]79 38.108.185[.]115	od[.]lk	Cogent Communications	2023-03-16	emote OpenDrive storage containing SimplexTea (/d/NTJfMzg4MDE1NzJf/vxmedia)
172.93.201[.]88	journalide[.]org	Nexeon Technologies, Inc.	2023-03-29	C&C server for SimplexTea (/djour.php)

- **CVE:**

  CVE-2023-29059
  Fuente: https://www.cvedetails.com/cve/CVE-2023-29059/

- **Virus Total señala:**

  SHA-256:
  492a643bd1efdaca4ca125ade1b606e7bbf00e995ac9115ac84d1c4c59cb66dd
  Archivo: Lazarusbgicddcjjh2Elf.elf
  Tamaño: 6.93 MB
  Propiedades:

MD5	3cf7232e5185109321921046d039cf10
SHA-1	3a63477a078ce10e53dfb5639e35d74f93cefa81
SHA-256	492a643bd1efdaca4ca125ade1b606e7bbf00e995ac9115ac84d1c4c59cb66dd
Vhash	ce6b4f2a94f0f0f93850f3a2723d1627
SSDEEP	98304:/m2nawVJcVEKKNJzQ17yZUeXZGGE6kJ6EUGzbrFCgYE7D:BTVMAZUhzIFGEgY6
TLSH	T113766C43FC9161A9C1EAD230C6769252BB717C891B3023D32B50B7B82F76BD86E79354

File type	ELF
Magic	ELF 64-bit LSB executable, x86-64, version 1 (SYSV), dynamically linked (uses shared libs), not stripped
Telfhash	t1e450000000000c303030330000000003030ccc303000000030003000000000030f00000
TrID	ELF Executable and Linkable format (Linux) (50.1%) ELF Executable and Linkable format (generic) (49.8%)
DetectItEasy	ELF64 Library: GLIBC (2.34) [EXEC AMD64-64] Compiler: Go (1.10.x-1.17.x) [EXEC AMD64-64]
File size	6.93 MB (7265295 bytes)

Fuente:
https://www.virustotal.com/gui/file/492a643bd1efdaca4ca125ade1b606e7bbf00e995ac9115ac84d1c4c59cb66dd/details

SHA-256:
f638e5a20114019ad066dd0e856f97fd865798d8fbed1766662d970beff652ca
Archivo: HSBC job offer.pdf.zip
Tamaño: 4.05 MB
Propiedades:

MD5	fc41cb8425b6432af8403959bb59430d
SHA-1	9d8bade2030c93d0a010aa57b90915eb7d99ec82
SHA-256	f638e5a20114019ad066dd0e856f97fd865798d8fbed1766662d970beff652ca
Vhash	988ec0c1a4e6a056b92da307c6f68b17
SSDEEP	98304:li7cgArWhfOyV1shPigXEmB5FnlQ8COAKgJQvPDbS18Wo4HUC7gmSH3Yz:McnrlfXV1yIYa8jvXSB0C7gVHu
TLSH	T1451633B6E0CB924EE458304AD77D63D41FB265232C6C759AFCCDCAF8A2621011FF6658

File type	ZIP
Magic	Zip archive data, at least v2.0 to extract
TrID	ZIP compressed archive (80%) PrintFox/Pagefox bitmap (640x800) (20%)
File size	4.05 MB (4250882 bytes)

Fuente:
https://www.virustotal.com/gui/file/f638e5a20114019ad066dd0e856f97fd865798d8fbed1766662d970beff652ca/details

SHA-256:
cc307cfb401d1ae616445e78b610ab72e1c7fb49b298ea003dd26ea80372089a
Archivo: sysnetd
Tamaño: 33.91 KB
Propiedades:

MD5	aac5a52b939f3fe792726a13ff7a1747
SHA-1	f6760fb1f8b019af2304ea6410001b63a1809f1d
SHA-256	cc307cfb401d1ae616445e78b610ab72e1c7fb49b298ea003dd26ea80372089a
Vhash	ab530f284a04fcfc070e237fd2a52e04
SSDEEP	768:hRrPk0kKk52IopET/khkkY7fB+EJTgzja0ER8:PrU5xopEloEJTgqtR8
TLSH	T1E2F2D813F94AC97DD8D982344847823455B3BC70D7299B376604ABB92C937883F2FB65
File type	ELF
Magic	ELF 64-bit LSB executable, x86-64, version 1 (SYSV), dynamically linked (uses shared libs), for GNU/Linux 2.6.18, not stripped
Telfhash	t165d0eb00f23a2e80cff210308c148ea02286f313ecbc2f040fd8c4e0992910f81809ef
TrID	ELF Executable and Linkable format (Linux) (50.1%) ELF Executable and Linkable format (generic) (49.8%)

DetectItEasy	ELF64 Library: GLIBC (2.2.5) [EXEC AMD64-64] Compiler: gcc ((GNU) 4.4.7 20120313 (Red Hat 4.4.7-17)) [EXEC AMD64-64]
File size	33.91 KB (34726 bytes)

Fuente:
https://www.virustotal.com/gui/file/cc307cfb401d1ae616445e78b610ab72e1c7fb49b298ea003dd26ea80372089a/details

VII. RECOMENDACIONES:

El EcuCERT recomienda a su comunidad objetivo tomar en consideración lo siguiente:

- Este software comprometido, implementado en varias infraestructuras de TI, que permite la descarga y ejecución de cualquier tipo de carga útil, puede tener efectos devastadores. Desafortunadamente, ningún editor de software es inmune a verse comprometido y distribuir inadvertidamente versiones troyanas de sus aplicaciones. Se recomienda actualizar los clientes de Mac Update 6 y Windows Update 7. 3CX DesktopApp hasta la 18.12.416 tiene un código malicioso incrustado, como se explotó en marzo de 2023. Esto afecta las versiones 18.12.407 y 18.12.416 de la aplicación 3CX DesktopApp Electron para Windows enviada en la Actualización 7 y las versiones 18.11.1213, 18.12. 402, 18.12.407 y 18.12.416 de la aplicación 3CX DesktopApp Electron para macOS.

- Para mitigar el incidente, considere utilizar las siguientes técnicas de MITRE ATT&CT:

Táctica	ID	Nombre	Descripción
Reconocimiento	T1593.001	Buscar sitios web/dominios abiertos: redes sociales	Los atacantes de Lazarus probablemente se acercaron a un objetivo con una oferta de trabajo falsa con el tema de HSBC que encajaría con el interés del objetivo. Esto se ha hecho principalmente a través de LinkedIn en el pasado.
Desarrollo de recursos	T1584.001	Adquirir Infraestructura: Dominios	A diferencia de muchos casos anteriores de C&C comprometidos utilizados en Operation DreamJob, los

Táctica	ID	Nombre	Descripción
			operadores de Lazarus registraron su propio dominio para el objetivo de Linux.
	T1587.001	Capacidades de desarrollo: Malware	Es muy probable que los atacantes desarrollen herramientas personalizadas del ataque.
	T1585.003	Establecer cuentas: cuentas en la nube	Los atacantes alojaron la etapa final en el servicio en la nube OpenDrive.
	T1608.001	Capacidades de etapa: Subir malware	Los atacantes alojaron la etapa final en el servicio en la nube OpenDrive.
Ejecución	T1204.002	Ejecución de usuario: archivo malicioso	OdicLoader se hace pasar por un archivo PDF para engañar al objetivo.
Acceso inicial	T1566.002	Phishing: enlace Spearphishing	El objetivo probablemente recibió un enlace a un almacenamiento remoto de terceros con un archivo ZIP malicioso, que luego se envió a VirusTotal.
Persistencia	T1546.004	Ejecución desencadenada por evento: cambio de configuración de Unix Shell	OdicLoader modifica el perfil de Bash de la víctima, por lo que SimplexTea se inicia cada vez que se mira Bash y su salida se silencia.
Evasión de defensa	T1134.002	Manejo de tokens de acceso: Crear proceso con token	SimplexTea puede crear un nuevo proceso, si así lo indica su servidor C&C.
	T1140	Desofuscar/Decodificar archivos o información	SimplexTea almacena su configuración en un apdl.cf encriptado.
	T1027.009	Archivos o información ofuscados: cargas útiles integradas	Los cuentagotas de todas las cadenas maliciosas contienen

Táctica	ID	Nombre	Descripción
			una matriz de datos integrada con una etapa adicional.
	T1562.003	Impair Defenses: Impair Command History Logging	OdicLoader modifica el perfil de Bash de la víctima, por lo que la salida y los mensajes de error de SimplexTea se silencian. SimplexTea ejecuta nuevos procesos con la misma técnica.
	T1070.004	Eliminación del indicador: eliminación de archivos	SimplexTea tiene la capacidad de eliminar archivos de forma segura.
	T1497.003	Evasión de virtualización/sandbox: evasión basada en el tiempo	SimplexTea implementa múltiples retrasos de sueño personalizados en su ejecución.
Descubrimiento	T1083	Descubrimiento de archivos y directorios	SimplexTea puede enumerar el contenido del directorio junto con sus nombres, tamaños y marcas de tiempo (imitando el comando ls -la).
Comando y control	T1071.001	Protocolo de capa de aplicación: protocolos web	SimplexTea puede usar HTTP y HTTPS para comunicarse con su servidor C&C, usando una biblioteca Curl enlazada estáticamente.
	T1573.001	Canal cifrado: criptografía simétrica	SimplexTea cifra el tráfico de C&C utilizando el algoritmo AES-GCM.
	T1132.001	Codificación de datos: codificación estándar	SimplexTea codifica el tráfico de C&C usando base64.
	T1090	Apoderado	SimplexTea puede utilizar un proxy para las comunicaciones.

Táctica	ID	Nombre	Descripción
Exfiltración	T1041	Exfiltración sobre el canal C2	SimplexTea puede filtrar datos como archivos ZIP a su servidor C&C.

Fuente: https://www.welivesecurity.com/2023/04/20/linux-malware-strengthens-links-lazarus-3cx-supply-chain-attack/

En general se debe considerar las siguientes recomendaciones:

- Instalar actualizaciones disponibles en medios oficiales del proveedor, previo análisis del impacto que podría provocar en los servicios críticos para el negocio de la organización.
- Realizar copias de respaldo de seguridad periódicas, de la información crítica para evitar la pérdida de la misma.
- Actualizar el sistema operativo de los equipos a las últimas versiones.
- No abrir, manipular, o interactuar, con correos electrónicos altamente sospechosos que lleguen a las bandejas de correo o mensaje en redes sociales.
- Otorgar privilegios de usuario al mínimo dependiendo del tipo de labor a realizar.
- Implementar técnicas de navegación segura en toda la Institución/Organización, como por ejemplo visita únicamente de sitios con certificados SSL, y, de origen no sospechoso.
- Bloquear el acceso de usuarios, a dispositivos de almacenamiento externo, ajenos a la Institución/Organización, a través de políticas de seguridad adecuadas.
- Implementar y monitorear, plataformas de seguridad perimetral para identificar posible tráfico malicioso tanto a nivel interno como externo a la infraestructura de red de la organización/Institución
- Descargar programas, archivos y actualizaciones, solamente desde fuentes oficiales y verificadas.
- Cerrar todo tipo de conexión/protocolo de acceso remoto a infraestructuras críticas en la Organización/Institución, en el caso de requerir su implementación, realizarlo bajo estrictas normas de seguridad apalancados en plataformas de seguridad perimetral y, uso de una VPN.
- Tener actualizado y utilizar, un software anti-virus
- Mantener actualizados, y, bajo licenciamiento, (ya sea a nivel de software libre o de paga, de ser el caso), todos y cada uno de los sistemas y subsistemas de software y hardware de toda la infraestructura de IT y OT de la Institución, esto es, incluido a nivel de Firmware de todos los componentes.

- Diseñar una política de revisión de logs, que permita detectar comportamientos fuera de lo normal en procesos legítimos del sistema.
- Mantener listas de control de acceso para las unidades mapeadas en red restringiendo los privilegios de escritura. Con esto podrá identificar el impacto generado por el cifrado de archivos, entendiendo que el secuestro de información se producirá en todas las unidades de red mapeadas en el equipo víctima.
- Capacitar a todos los usuarios, mediante la concientización y simulaciones para reconocer e informar sobre intentos de phishing e ingeniería social. Seguir las normativas internacionales tales como ISO 27001:2013 en su control A.7.2.2 "Concienciación con educación y capacitación en seguridad de la información" o NIST PR.AT-1: "Todos los usuarios se encuentran entrenados e informados", a fin de tener bases para divulgar campañas educativas orientadas a nivel de usuarios respecto al correcto uso de las herramientas tecnológicas
- Implementar un plan de respuesta a emergencias de la Organización/Institución.
- En el caso de sufrir un ataque de proporciones mayores, contacte a las Autoridades competentes en base a la Normativa Legal Vigente a nivel Nacional.

VIII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta; se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

IX. REFERENCIAS:

- **Kálnai Peter y M-Léveillé Marc-Etienne (2023)**. Linux malware strengthens links between Lazarus and the 3CX supply-chain attack. Welivesecurity by ESET; recuperado de: https://www.welivesecurity.com/2023/04/20/linux-malware-strengthens-links-lazarus-3cx-supply-chain-attack/

- **Virus Total (2023).** *Lazarusbgicddcjjh2Elf.elf*, recuperado de: https://www.virustotal.com/gui/file/492a643bd1efdaca4ca125ade1b606e7bbf00e995ac9115ac84d1c4c59cb66dd/details

- **Virus Total (2023).** *HSBC job offer.pdf.zip*, recuperado de: https://www.virustotal.com/gui/file/f638e5a20114019ad066dd0e856f97fd865798d8fbed1766662d970beff652ca/details

- **Virus Total (2023).** sysnetd, recuperado de: https://www.virustotal.com/gui/file/cc307cfb401d1ae616445e78b610ab72e1c7fb49b298ea003dd26ea80372089a/details