I. DATOS GENERALES:

Clase de alerta: Malware

Tipo de incidente: Nueva variante de Python, Malware CHAES se dirige a la banca e industrias logísticas.

Nivel de riesgo: Alto

II. ALERTA

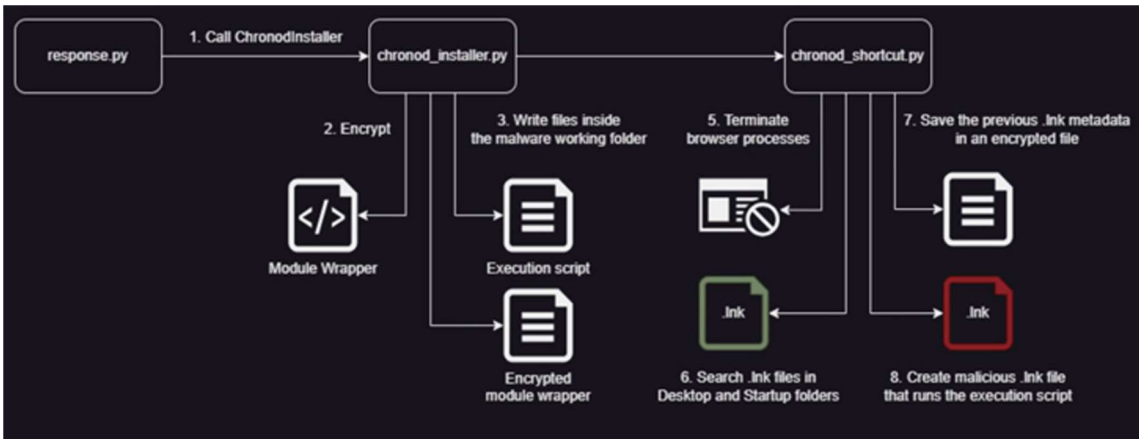

Figura 1.- Versión actualizada de malware conocida como CHAES está atacando los sectores bancarios y logísticos.
Fuente: https://thehackernews.com/2023/09/new-python-variant-of-chaes-malware.html

En enero de 2023, Morphisec identificó una tendencia alarmante en la que numerosos clientes, principalmente dentro de los sectores de logística y financiero, estaban bajo el ataque de una nueva y avanzada variante de malware Chaes. Se observó que la sofisticación de la amenaza aumenta durante múltiples iteraciones de abril a junio de 2023.

Gracias a la tecnología AMTD de vanguardia de Morphisec (defensa de objetivos de movimiento automático), muchos de estos ataques fueron frustrados antes de causar daños significativos.

Esta no es una variante Chaes ordinaria. Se ha sometido a grandes revisiones: desde ser reescritos por completo en Python, lo que resultó en tasas de detección más bajas por los sistemas de defensa tradicionales, hasta un rediseño integral y un protocolo de comunicación mejorado. Además, ahora cuenta con un conjunto de nuevos módulos que promueven sus capacidades maliciosas.

Los objetivos de este malware no son aleatorios. Tiene un enfoque específico en clientes de plataformas y bancos prominentes como Mercado Libre, Mercado Pago, Whatsapp Web, Itau Bank, Caixa Bank e incluso Metamask. Además, docenas de servicios de CMS (gestión de contenido) tampoco se han salvado, incluidos WordPress, Joomla, Drupal y Magento. Es importante tener en cuenta que el malware Chaes no es del todo nuevo en el panorama de ciberseguridad. Su primera aparición se remonta a noviembre de 2020, cuando los investigadores de Cybereason destacaron sus operaciones principalmente dirigidas a clientes de comercio electrónico en América Latina.

La nueva variante Chaes ha sido llamada "Chae $ 4" (Chae $ 4) por Morphisec, ya que es la cuarta variante mayor, y debido a una impresión de depuración en un módulo central que dice "Chae $ 4".

Fuente:https://blog.morphisec.com/chaes4-new-chaes-malware-variant-targeting-financial-and-logistics-customers

III. INTRODUCCIÓN

CHAES, que surgió por primera vez en 2020, se sabe que se dirige a clientes de comercio electrónico en América Latina, particularmente Brasil, a robar información financiera confidencial.

Un análisis posterior de Avast a principios de 2022 descubrió que los actores de amenaza detrás de la operación, que se hacen llamar Lucifer, habían violado más de 800 sitios web de WordPress para entregar Chaes a los usuarios de Banco do Brasil, Loja Integrada, Mercado Bitcoin, Mercado Livre y Mercado y Mercado. Pago.

Se detectaron más actualizaciones en diciembre de 2022, cuando la empresa de seguridad cibernética brasileña Tempest Security Intelligence descubrió el uso del malware de Windows Management Instrumentation (WMI) en su cadena de infección para facilitar la recopilación de metadatos del sistema, como BIOS, procesador, tamaño de disco e información de memoria e información de memoria.

La última iteración del malware, denominado Chae$ 4, en referencia a los mensajes de registro de depuración presentes en el código fuente, incluye "transformaciones y mejoras significativas", incluido un catálogo ampliado de servicios dirigidos al robo de credenciales y las funcionalidades de Clipper.

A pesar de los cambios en la arquitectura de malware, el mecanismo de entrega general se ha mantenido igual en los ataques que se identificaron en enero de 2023.

- **Init,** que recopila información extensa sobre el sistema.
- **Online**, que actúa como un faro para transmitir un mensaje al atacante que el malware está ejecutando en la máquina
- **Chronod**, que roba credenciales de inicio de sesión ingresadas en los navegadores web e intercepta transferencias de pago BTC, ETH y PIX
- **APPITA**, un módulo con características similares que la de Chronod pero diseñada específicamente para apuntar a la aplicación de escritorio de Itaú Unibanco ("itauaplicateguo.exe")

- **Chrautos,** una versión actualizada de Chronod y Appita que se centra en recopilar datos de Mercado Libre, Mercado Pago y WhatsApp

- **Stealer**, una variante mejorada de la Chrolog que recoge datos de tarjetas de crédito, cookies, automáticamente y otra información almacenada en navegadores web, y

- **File Uploader,** que carga datos relacionados con la extensión Chrome de Metamask.

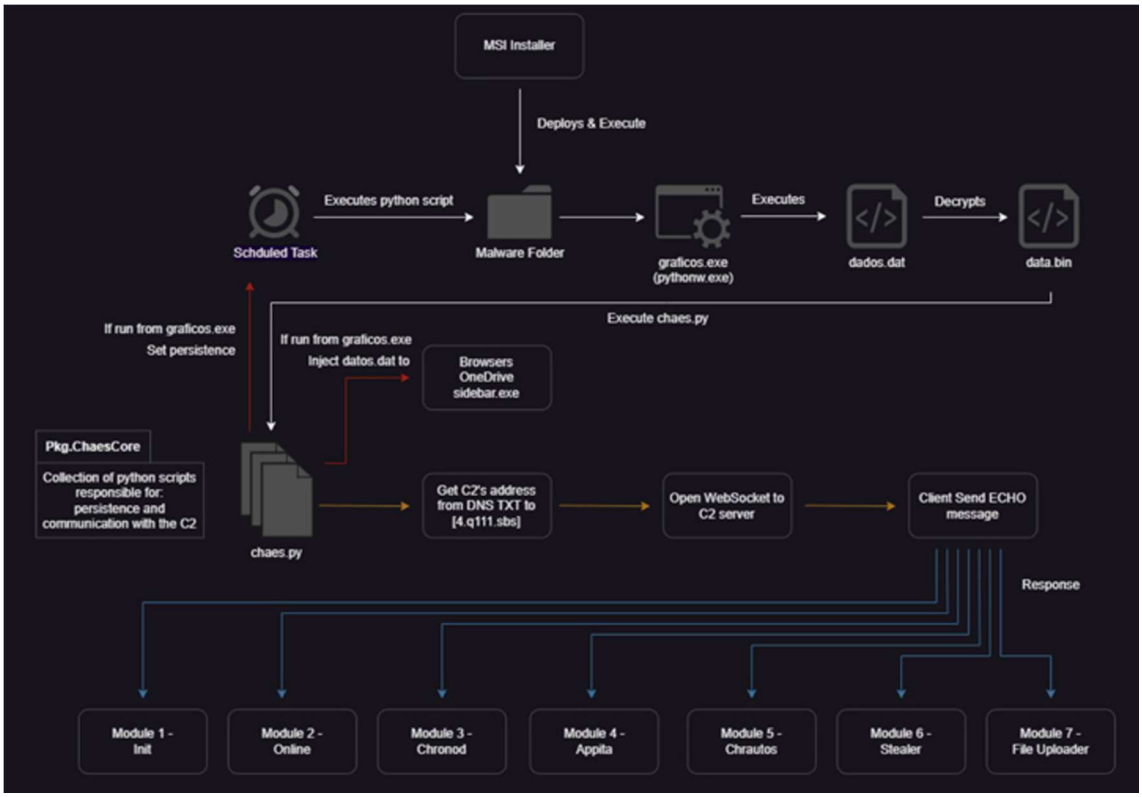

Figura 2.- CHAES - Establecer una ruta de comunicación con el servidor de comando y control (C2) es responsabilidad del componente, desde el cual recupera módulos adicionales que facilitan la actividad posterior a la compromiso y al robo de datos
Fuente: https://thehackernews.com/2023/09/new-python-variant-of-chaes-malware.htmlttps://thehackernews.com/2023/09/new-python-variant-of-chaes-malware.html

IV. VECTOR DE ATAQUE:

Descarga de aplicaciones comprometidas desde sitio Web.

Las víctimas potenciales que aterrizan en uno de los sitios web comprometidos son recibidas por un mensaje emergente que les pide que descarguen un instalador para el tiempo de ejecución de Java o una solución antivirus, lo que provoca la implementación de un archivo MSI malicioso que, a su vez, lanza un módulo de orquestador primario conocido como chaescore.

El componente es responsable de establecer un canal de comunicación con el servidor de comando y control (C2) desde donde obtiene módulos adicionales que admiten actividades posteriores al compromiso y robo de datos.

V. IMPACTO:

- Una variante nueva y avanzada de malware Chaes dirigido principalmente a los sectores de logística y financiero. Esta variante Chaes, llamada "Chae$ 4", es la cuarta iteración principal, que presenta cambios significativos en el cambio de Python, encriptado mejorado y un enfoque en plataformas de pago como Mercado Libre, Mercado Pago, Whatsapp Web, Itaubank, Caixabank y Servicios de CMS como WordPress, Joomla, Drupal y Magento. El malware Chaes ha estado activo desde noviembre de 2020, inicialmente dirigido a clientes de comercio electrónico en Latinoamérica.

- El malware Chaes evoluciona constantemente y Cybereason ha descifrado por primera vez en noviembre de 2020. Avast examinó las variantes posteriores en enero de 2022. Sorprendentemente, los actores de malware de Chaes reconocieron el análisis de Avast y apreciaron sus comentarios como un medio para mejorar y avanzar en las capacidades del malware. El actor de la amenaza fue referido como 'Lucifer'. Más tarde, en diciembre de 2022, CHAES evolucionó y adoptó WMI para la recopilación de datos del sistema.

- Chae$ 4 trae transformaciones significativas, incluida la arquitectura de código refinado, el aumento de las capacidades de sigilo, un cambio a Python, la adopción de sockets web para la comunicación y la resolución dinámica de la dirección del servidor C2. El malware comienza con el instalador de MSI, creando una carpeta dedicada para sus archivos e implementando el módulo principal, CHAES Core, que es responsable de la persistencia y la comunicación con el servidor C2. Se identificaron siete en módulos dependientes, incluido un módulo de iniciación, un módulo en línea, un robador de credenciales y otros, todos con un enfoque en robar información y datos confidenciales.

VI. INDICADORES DE COMPROMISO

- **Archivos:**

Tipo	Valor
SHA256 (MSI Installer)	d1885b4f515cea0d5c262c8d0b19db9c1cb7bc98efe761c4021fc4e40a9584d6 05b10fc19273045a3e70fa0057873643af289db75878949912c925163ad3c9fd

	b58161c867b2bd6ac4e2332b951b7897efd2b19f696901b078a395ddcf7d134a 628b1ba59150a1b66167bec71d16eef23cafc167ffb47c916c69adb2ac372a57 6d4a7488cb559035d5d06d5a94adc76188cd2dfc6a647f8a77da7565e244898c
Domains	4.q111.sbs <day_domain>.mail89.us.to, <day_domain>.ns99.uk.ms
IPV4	18.228.15.16 18.229.122.137 13.248.205.89 13.248.185.41
URLs	hxxp://l-1038939961.sa-east-1.elb.amazonaws.com hxxp://l-1038939961.sa-east-1.elb.amazonaws.com
WebSocket URLs	ws://54.233.147.24 ws://18.231.31.151 ws://18.229.170.213 ws://54.94.248.242 ws://18.231.70.213 ws://18.231.91.245 ws://18.230.36.203 ws://54.232.236.117

- **Virus Total señala:**

SHA-256:
d1885b4f515cea0d5c262c8d0b19db9c1cb7bc98efe761c4021fc4e40a9584d6
Archivo: 5a5fec.msi
Tamaño: 110.98 MB

Propiedades:

MD5	6e7dcfd13260001c8fbfcc96b72e6e75
SHA-1	c044d74485b31e31a9573506b2133d8b54ede250
SHA-256	d1885b4f515cea0d5c262c8d0b19db9c1cb7bc98efe761c4021fc4e40a9584d6

Vhash	6341e08ec6b7dd6583975006796696c0
SSDEEP	24576:PYDBgJu/MjYc9vxkI3tCOfwdU+nm/Cb/yNxK:PYDB+h/9aOCEwdFLav
TLSH	T16648BE3738890C32D387BCBD1A777E2E05933D4543E961955266FC27E0ADFB0A1B52A2
File type	Windows Installer
Magic	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, MSI Installer, Create Time/Date: Mon Jun 21 07:00:00 1999, Name of Creating Application: Windows Installer, Security: 1, Code page: 1252, Template: Intel;1046, Number of Pages: 200, Number of Words: 10, Revision Number: {da2dfbb7-efe9-400e-b319-66ee986e49b1}, Title: Gerenciamento de Dispositivo de Engenharia, Author: Database, Last Printed: Thu May 18 19:50:07 2023, Last Saved Time/Date: Thu May 18 19:50:07 2023
TrID	Microsoft Windows Installer (80%) Windows SDK Setup Transform script (10.7%) Windows Installer Patch (7.8%) Generic OLE2 / Multistream Compound (1.4%)
File size	110.98 MB (116372480 bytes)

Fuente:
https://www.virustotal.com/gui/file/d1885b4f515cea0d5c262c8d0b19db9c1cb7bc98efe761c4021fc4e40a9584d6/details

SHA-256:
05b10fc19273045a3e70fa0057873643af289db75878949912c925163ad3c9fd
Archivo: 55c7c7.msi
Tamaño: 106.95 MB

Propiedades:

MD5	9bcc9f4fafe710a2cef3c3192c1e3a98
SHA-1	cf30d3b861a3648e26c2406c9f78564bb872ed81
SHA-256	05b10fc19273045a3e70fa0057873643af289db75878949912c925163ad3c9fd
Vhash	6341e08ec6b7dd6583975006796696c0
SSDEEP	24576:mLSBXJu/MjYc9vxkI3tCOfwdU+nm/Cw/yKC19M:mLSB5h/9aOCEwdFAaJM

TLSH	T1CD38AF3778491C32D387BCB91A72BE2E05A33D4543ED625652B5FC27E06DFB091B42A2
File type	Windows Installer
Magic	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, MSI Installer, Create Time/Date: Mon Jun 21 07:00:00 1999, Name of Creating Application: Windows Installer, Security: 1, Code page: 1252, Template: Intel;1046, Number of Pages: 200, Number of Words: 10, Revision Number: {95f9d083-1a2c-452e-9e97-665d72299894}, Title: Pesquisador de Medicina, Author: Options.bin, Last Printed: Sat May 27 19:25:06 2023, Last Saved Time/Date: Sat May 27 19:25:06 2023
TrID	Microsoft Windows Installer (89.6%) Windows Installer Patch (8.7%) Generic OLE2 / Multistream Compound (1.5%)
File size	106.95 MB (112144896 bytes)

Fuente:
https://www.virustotal.com/gui/file/05b10fc19273045a3e70fa0057873643af289db75878949912c925163ad3c9fd/details

SHA-256:
b58161c867b2bd6ac4e2332b951b7897efd2b19f696901b078a395ddcf7d134a
Archivo: jre-084621.msi
Tamaño: 101.91 MB

Propiedades:

MD5	7affb9eb1472811a734eafdcec26aff8
SHA-1	47ef71675a2dfae56823d76f459021c023b6bbba
SHA-256	b58161c867b2bd6ac4e2332b951b7897efd2b19f696901b078a395ddcf7d134a
Vhash	6341e08ec6b7dd6583975006796696c0
SSDEEP	24576:rMwBfJu/MjYc9vxkl3tCOfwdU+nmuCvz:rMwBxh/9aOCEwdFS
TLSH	T17C38AE3B78491D32D787BCB91A73BE2E09933D0583ED61459275FC27A06DFB091B42A2

File type	Windows Installer
Magic	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, MSI Installer, Create Time/Date: Mon Jun 21 07:00:00 1999, Name of Creating Application: Windows Installer, Security: 1, Code page: 1252, Template: Intel;1046, Number of Pages: 200, Number of Words: 10, Revision Number: {63b95fb7-64d1-40c1-92f4-cac2524ede97}, Title: Drivers de Sistema de Músicas, Author: Info, Last Printed: Sat Oct 7 22:10:06 2023, Last Saved Time/Date: Sat Oct 7 22:10:06 2023
TrID	Microsoft Windows Installer (86.3%) Windows Installer Patch (8.4%) Kingsoft WPS Office document (alt.) (3.7%) Generic OLE2 / Multistream Compound (1.5%)
File size	101.91 MB (106860032 bytes)

Fuente:
https://www.virustotal.com/gui/file/b58161c867b2bd6ac4e2332b951b7897efd2b19f696901b078a395ddcf7d134a/details

SHA-256:
628b1ba59150a1b66167bec71d16eef23cafc167ffb47c916c69adb2ac372a57
Archivo: 6d7741.msi
Tamaño: 101.91 MB

Propiedades:

MD5	f9946a0868671bb90f05dd9d7b4335cf
SHA-1	b78ae307865a5382a463da70c44447f349e06923
SHA-256	628b1ba59150a1b66167bec71d16eef23cafc167ffb47c916c69adb2ac372a57
Vhash	6341e08ec6b7dd6583975006796696c0
SSDEEP	12288:d+HBwb9X+/Mu3lI7Yc9vIROLIv33XNCSceZg05+vYNHSSy8YiUuRKoy9tmjPyXQ:d+HBwJu/MjYc9vxkI3tCOfwdU+nmuCf
TLSH	T19638AE3B78491D32D787BCB91A73BE2E48933D0583FE61455275BC27A06DFB091B42A2
File type	Windows Installer

Magic	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, MSI Installer, Create Time/Date: Mon Jun 21 07:00:00 1999, Name of Creating Application: Windows Installer, Security: 1, Code page: 1252, Template: Intel;1046, Number of Pages: 200, Number of Words: 10, Revision Number: {5530e306-e902-4ee2-9062-b8d3252915a9}, Title: Planilha de Auxiliar, Author: Settings.bin, Last Printed: Tue Jun 20 18:00:05 2023, Last Saved Time/Date: Tue Jun 20 18:00:05 2023
TrID	Microsoft Windows Installer (86.3%) Windows Installer Patch (8.4%) Kingsoft WPS Office document (alt.) (3.7%) Generic OLE2 / Multistream Compound (1.5%)
File size	101.91 MB (106860032 bytes)

Fuente:
https://www.virustotal.com/gui/file/628b1ba59150a1b66167bec71d16eef23cafc167ffb47c916c69adb2ac372a57/details

SHA-256:
6d4a7488cb559035d5d06d5a94adc76188cd2dfc6a647f8a77da7565e244898c
Archivo:
6d4a7488cb559035d5d06d5a94adc76188cd2dfc6a647f8a77da7565e244898c.msi
Tamaño: 100.90 MB

Propiedades:

MD5	4b44a2a657c208f72dce5f09f5a6838a
SHA-1	484a217993de2380c33a3690122e4df840d17c47
SHA-256	6d4a7488cb559035d5d06d5a94adc76188cd2dfc6a647f8a77da7565e244898c
Vhash	6341e08ec6b7dd6583975006796696c0
SSDEEP	24576:AAUBFJu/MjYc9vxkI3tCOfwdU+nmu6Qqb:AAUBDh/9aOCEwdFY
TLSH	T187389D3B38491D32D387BC790A73BE2E09933D4583EE61455275FC27E16DEB092B42A2
File type	Windows Installer
Magic	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, MSI Installer, Create Time/Date: Mon Jun 21 07:00:00 1999, Name of Creating Application: Windows Installer, Security: 1, Code page: 1252,

	Template: Intel;1046, Number of Pages: 200, Number of Words: 10, Revision Number: {a56c0428-5aad-4a68-ba1c-cf9588205c44}, Title: Gerenciamento de Arquivos, Author: Settings.dat, Last Printed: Mon Mar 6 22:05:07 2023, Last Saved Time/Date: Mon Mar 6 22:05:07 2023
TrID	Microsoft Windows Installer (89.6%) Windows Installer Patch (8.7%) Generic OLE2 / Multistream Compound (1.5%)
File size	100.90 MB (105803776 bytes)

Fuente:
https://www.virustotal.com/gui/file/6d4a7488cb559035d5d06d5a94adc76188cd2dfc6a647f8a77da7565e244898c/details

VII. RECOMENDACIONES:

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

- **Implementar la detección de amenazas avanzadas:** dada la naturaleza sofisticada de Chae$ 4 y su capacidad para evadir las medidas de seguridad tradicionales, es crucial para invertir a través de los sistemas de detección. Esta exploración del sistema emplean la detección de anomalías de analítica basada en el comportamiento para identificar y responder a las características únicas de los ataques Chae$ 4.

- **Fortalecer la seguridad de las aplicaciones web:** Chae$ 4 se dirige a los bancos de plataforma prominentes, lo que hace que la seguridad de las aplicaciones web sea primordial. Realice pruebas regulares de penetración de evaluación de seguridad para aplicaciones web, especialmente si están vinculadas a transacciones financieras. Asegúrese de que los parches de seguridad para los sistemas de gestión de contenido de marco web se apliquen de inmediato para evitar vulnerabilidades que Chae$ 4 puede explotar.

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

TA0011 Command and Control	**TA0005** Defense Evasion	**TA0003** Persistence	**TA0002** Execution
TA0006 Credential Access	**TA0010** Exfiltration	**T1218** System Binary Proxy Execution	**T1053** Scheduled Task/Job
T1053.005 Scheduled Task	**T1059.006** Python	**T1059** Command and Scripting Interpreter	**T1027** Obfuscated Files or Information
T1055.001 Dynamic-link Library Injection	**T1555.003** Credentials from Web Browsers	**T1555** Credentials from Password Stores	**T1055** Process Injection
T1568.002 Domain Generation Algorithms	**T1568** Dynamic Resolution	**T1041** Exfiltration Over C2 Channel	**T1218.007** Msiexec

Fuente: https://www.hivepro.com/new-variant-of-chaes-malware-chae-4-targeting-financial-and-logistics-sectors/

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:

- **The Hacker News (2023).** *New Python Variant of Chaes Malware Targets Banking and Logistics Industries*; recuperado de: https://thehackernews.com/2023/09/new-python-variant-of-chaes-malware.html

- **Hive Pro (2023).** *New Variant of Chaes Malware 'Chae$ 4' Targeting Financial and Logistics Sectors*; recuperado de: https://thehackernews.com/2023/09/new-python-variant-of-chaes-malware.html

- **Morphisec (2023).** *Chae$ 4: New Chaes Malware Variant Targeting Financial and Logistics Customers;* recuperado de: https://blog.morphisec.com/chaes4-new-chaes-malware-variant-targeting-financial-and-logistics-customers

- **Virus Total (2023).** *5a5fec.msi*, recuperado de: https://www.virustotal.com/gui/file/d1885b4f515cea0d5c262c8d0b19db9c1cb7bc98efe761c4021fc4e40a9584d6

- **Virus Total (2023).** *55c7c7.msi*, recuperado de: https://www.virustotal.com/gui/file/05b10fc19273045a3e70fa0057873643af289db75878949912c925163ad3c9fd

- **Virus Total (2023).** *jre-084621.msi*, recuperado de: https://www.virustotal.com/gui/file/b58161c867b2bd6ac4e2332b951b7897efd2b19f696901b078a395ddcf7d134a

- **Virus Total (2023).** *6d7741.msi*, recuperado de: https://www.virustotal.com/gui/file/628b1ba59150a1b66167bec71d16eef23cafc167ffb47c916c69adb2ac372a57

- **Virus Total (2023).** *6d4a7488cb559035d5d06d5a94adc76188cd2dfc6a647f8a77da7565e244898c.msi*, recuperado de: https://www.virustotal.com/gui/file/6d4a7488cb559035d5d06d5a94adc76188cd2dfc6a647f8a77da7565e244898c