Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

Grupo de Hacktivistas expone emails de fuerzas de seguridad pública Latinoamericanas.

30/Septiembre/2022

Contenido

Introducción

Los archivos de la Secretaría de la Defensa Nacional de México; Policía y Fuerza Armada de El Salvador, así como de carteras de seguridad de otros países fueron víctimas de un ataque cibernético, afirmó el presidente de la nación azteca Andrés Manuel López Obrador.

GUACAMAYA HACKS

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2022_09_30_02
Clasificación de alerta:	Noticia
Tipo de Impacto:	Medio
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	09/30/2022
Es día cero (0 day):	No

RESUMEN

Fueron 6 terabytes de información filtrada, que equivale a 36 millones de documentos PDF, 1.5 millones de fotos o 3 mil horas de video, según detalló el grupo de hackers "Guacamaya" en su cuenta de twitter.

Sin precisar cuándo ocurrieron los ataques, López Obrador confirmó las versiones de prensa sobre el hackeo de los sistemas informativos de la Secretaría y la extracción de varios archivos que incluyen informes sobre su estado de salud y el fracaso de la operación para capturar a un hijo de Joaquín “El Chapo” Guzmán ocurrida en 2019.

“No hay nada que no se sepa”, dijo López Obrador en su conferencia matutina al restarle importancia al evento e indicó que el ataque ocurrió durante un cambio del sistema de comunicación de la Secretaría de la Defensa Nacional de México (Sedena), pero no precisó fechas.

En el El Salvador accedieron a los correos electrónicos de la Policía Nacional y militares, pero se desconocen por el momento más detalles.

El ataque a los sistemas fue realizado por un grupo de piratas informáticos conocido como Guacamaya que también efectuó acciones similares a instituciones de seguridad policial y militar en varios países de América Latina.

En Chile los piratas informáticos intervinieron los correos electrónicos de los jefes de Estado Mayor Conjunto de las Fuerzas Armadas.

Estado Mayor Conjunto de las Fuerza Armadas de Chile

Cerca de 400.000 correos electrónicos hackeados por Guacamaya del Estado Mayor Conjunto de las Fuerzas Armadas de Chile, que asesoran al Ministro de Defensa de Chile. Son responsables de velar por que las Direcciones y Departamentos se manejen adecuadamente para el personal, la inteligencia, las operaciones y la logística.

El caché de correos electrónicos abarca más de cinco años, ofreciendo las miradas más detalladas sobre el liderazgo, las operaciones y los intereses del ejército chileno.

Este es el primer lanzamiento de una nueva serie de Guacamaya - Fuerzas Represivas. Las publicaciones posteriores de Fuerzas Represivas incluirán datos policiales y militares de México, Perú, Salvador, Chile, Colombia.

LANZAMIENTO

Estado Mayor Conjunto de las Fuerza Armadas de Chile

Cerca de 400.000 correos electrónicos hackeados por Guacamaya del Estado Mayor Conjunto de las Fuerzas Armadas de Chile, que asesoran al Ministro de Defensa de Chile.

DETALLES DEL CONJUNTO DE DATOS

PAÍSES	Chile
TIPO	Cortar
FUENTE	Guacamaya
TAMAÑO DEL ARCHIVO	366 GB

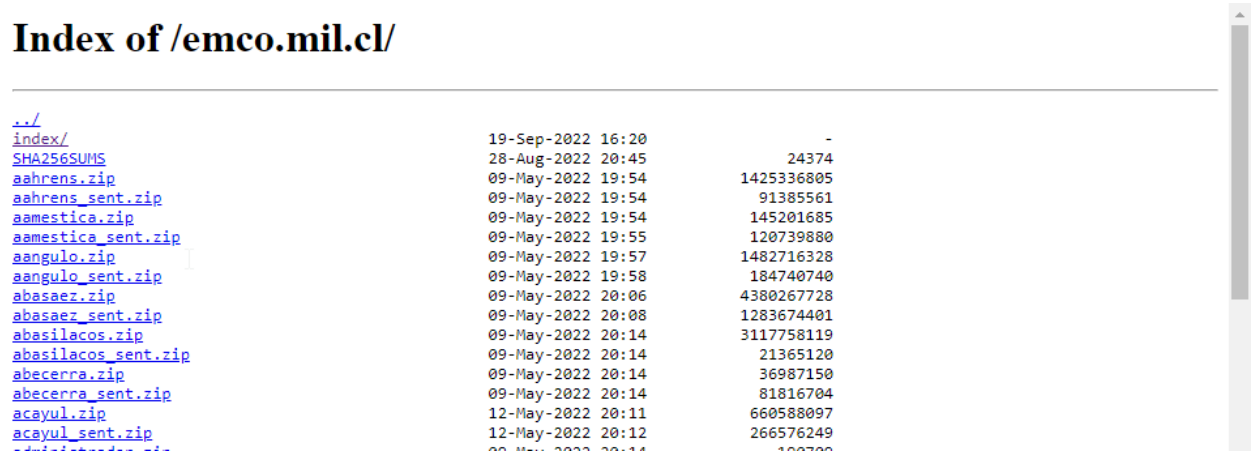
DESCARGAS (Cómo descargar)

En Perú, ingresaron a los correos electrónicos de los jefes conjuntos y del ejército y en Colombia hackearon los correos del Comando General de las Fuerzas Armadas. Sin embargo, el ataque más contundente se dio en la Sedena donde lograron acceder a numerosos archivos.

La distribución de las filtraciones es la siguiente:

- Policía Nacional Civil de El Salvador 4TB
- Fuerzas Militares de Colombia 275GB
- Fuerza Armada de El Salvador 50GB
- CCFFAA de Perú 35GB
- Ejercito del Perú 70GB

Los correos electrónicos filtrados son accesibles mediante un archivo/enlace de Torrent o directamente en la página de Guacamaya Hacks.



Index of /emco.mil.cl/

../		
index/	19-Sep-2022 16:20	-
SHA256SUMS	28-Aug-2022 20:45	24374
aahrens.zip	09-May-2022 19:54	1425336805
aahrens_sent.zip	09-May-2022 19:54	91385561
aamestica.zip	09-May-2022 19:54	145201685
aamestica_sent.zip	09-May-2022 19:55	120739880
aangulo.zip	09-May-2022 19:57	1482716328
aangulo_sent.zip	09-May-2022 19:58	184740740
abasaez.zip	09-May-2022 20:06	4380267728
abasaez_sent.zip	09-May-2022 20:08	1283674401
abasilacos.zip	09-May-2022 20:14	3117758119
abasilacos_sent.zip	09-May-2022 20:14	21365120
abecerra.zip	09-May-2022 20:14	36987150
abecerra_sent.zip	09-May-2022 20:14	81816704
acayul.zip	12-May-2022 20:11	660588097
acayul_sent.zip	12-May-2022 20:12	266576249

El ataque fue realizado usando la vulnerabilidad de ProxyShell para acceder a los servidores Exchange de las organizaciones.

El grupo hacktivista Guacamaya ha liberado 6 TB de emails de la Secretaría de la Defensa Nacional de México

El acceso a esta información está reservado para periodistas e investigadores.

Secretaría de la Defensa Nacional de México

6 TB of emails hacked by Guacamaya from the Secretaría de la Defensa Nacional de México (SEDENA) (Secretariat of National Defense of Mexico).

Limited Distribution

Due to the sensitivity of the data and at the request of the source, the data is only being provided to journalists and researchers.

RELEASE

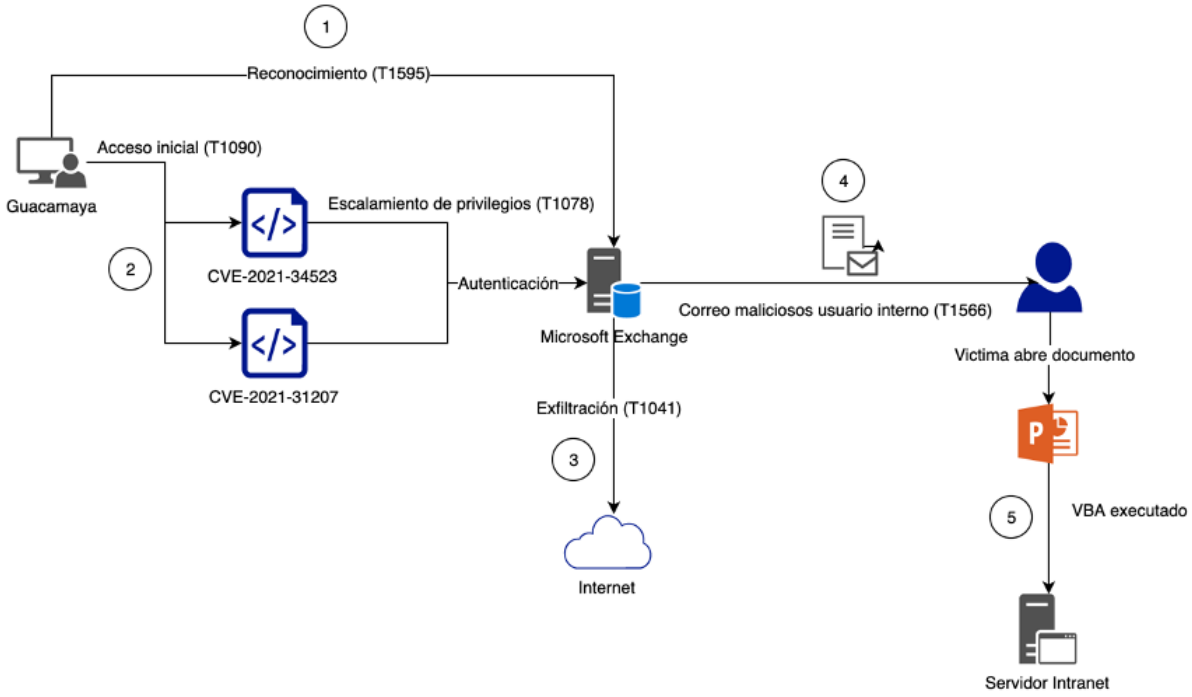
Secretaría de la Defensa Nacional de México

6 TB of emails hacked by Guacamaya from the Secretaría de la Defensa Nacional de México (SEDENA) (Secretariat of National Defense of Mexico).

DATASET DETAILS

Adicional, se tiene conocimiento sobre la liberación de 175,000 emails del ejército de Perú, 300,000 emails de las fuerzas militares de Colombia, 250,000 emails pertenecientes a la Fuerza Armada de El Salvador y 10 Millones Emails de Policía Nacional Civil de El Salvador.

Se presenta la línea de eventos que desencadenaron el ataque exitoso a las infraestructuras vulneradas:



RECOMENDACIONES

- Se sugiere aplicar las mitigaciones brindadas por Microsoft para evitar ser victima de ProxyShell en sus servidores Exchange.

- Asegúrese de que sus servidores estén protegidos por software Antivirus y políticas de navegación adecuadas a nivel de firewall.

- Mantener monitoreo activo sobre todo tráfico sospechoso en red para poder realizar bloqueos a IPs no deseadas y sospechosas.

- Cerrar los puertos para Powershell remoto.

- Recuerde a sus colaboradores no descargar ficheros o ingresar a enlaces de correos sospechosos que puedan recibir si desconocen la identidad real del remitente.

Noticia Completa

https://devel.group/blog/dia-cero-en-exchange/

https://devel.group/blog/guacamaya-hacks-libera-correos-robados-mediante-vulnerabilidad-en-exchange/

CONTACTOS DE SOPORTE

Correo electrónico: cert@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757
El Salvador: +(503) 2249 4252
Honduras: +(504) 2283 5904
República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://www.devel.group/reporta-un-incidente