Informe

Técnico

Malware de la Semana

COLCERT IN-20250513-021

TLP:CLEAR

Durante la semana anterior **se identificó una campaña activa de phishing que utiliza archivos .rar que contienen mensajes de correo electrónico (.eml) maliciosos.**Estos correos incluyen enlaces disfrazados mediante Microsoft SafeLinks* y servicios de redirección como Google URL Redirect, los cuales conducen a sitios fraudulentos diseñados para la captura de credenciales.

Aunque esta actividad se origina como una campaña de phishing, su propósito final es inducir al usuario a ejecutar un archivo malicioso; por lo tanto, se clasifica como una amenaza de tipo malware.

Información Técnica de la Muestra

- **Nombre del archivo**: ls "____IMPORTANT____ – Server Expiry ID_NIS33JKY6JYEUXL7EUXLRQN2UVLJUN2PCSEMPS4RQL.rar"
- **Tamaño:** 14.7 KB
- **Tipo:** Archivo .rar comprimido
- **Análisis dinámico:** Trellix IVX Cloud Sandbox
- **Resultado:** Malicioso
- **Perfiles utilizados:** winxp-sp3m, win10x64m

Identificadores de Hash (IoC)

Tipo	Valor
MD5	2ba59a1b0f12ba1866f5e2c6340ff281
SHA1	12fb00a5eb864380f097a9e96071044d24632f95
SHA256 (.rar)	8fff991a0636533d645603c208b656622196f3effa61563e0777c5b0498476e3
SHA256 (.eml)	6dc2fd7c9e24e03367fdef3c65d849085392ae9039728c6d6ed25565e972f34f

URLs Maliciosas Completas

A partir de la decodificación manual del .eml con herramientas en Parrot OS, **se extrajeron las siguientes URLs activas:**

hxxps[:]//jyb[.]dk/section/#~JQ~3L3htmQkSrFSGGpauyIlLHDb4blyAUGYZrYz3G==DW3EGONDpH4Yo0u7jUlli0sbof7B05JqWXjL3v

hxxps[:]//www[.]google[.]com/url?q=hxxps%3A%2F%2Fjyb[.]dk%2Fsection%2F&sa=D&sntz=1&usg=AOvVaw3eZ_c8tv32tWtZM_-WJFI1

hxxps[:]//nam10[.]safelinks[.]protection[.]outlook[.]com/?url=hxxps%3A%2F%2Fwww[.]google[.]com%2Furl%3Fq%3Dhxxps%253A%252F%252Fjyb[.]dk%252Fsection%252F%26sa%3DD%26sntz%3D1%26usg%3DAOvVaw3eZ_c8tv32tWtZM_-WJFI1

COLCERT

Técnicas MITRE ATT&CK Observadas

ID	Técnica	Descripción y Evidencia del Caso
T1566.001	Phishing: Spearphishing Attachment	El ataque se inicia con un correo electrónico que incluye un archivo .rar malicioso con nombre técnico y urgente. Esta táctica busca engañar al usuario para que descargue y abra el contenido.
T1204	User Execution	El ataque requiere la interacción del usuario, quien debe extraer el .rar, abrir el .eml incluido y hacer clic en los enlaces incrustados. Sin esta acción, no se activa la cadena maliciosa.
T1568.002	Command and Control over Application Layer Protocol: Web Services	El .eml contiene enlaces SafeLinks que redirigen a URLs de phishing alojadas en el dominio jyb.dk. Se emplea infraestructura legítima (Microsoft SafeLinks, Google Redirect) para evadir detección y facilitar el C2.
T1027	Obfuscated Files or Information	El archivo .rar comprimido, protegido por política, y el uso de redireccionamientos como SafeLinks y Google obfuscate las URLs reales, dificultando su detección automática por sistemas de seguridad.

Análisis de Evidencia - Parrot OS

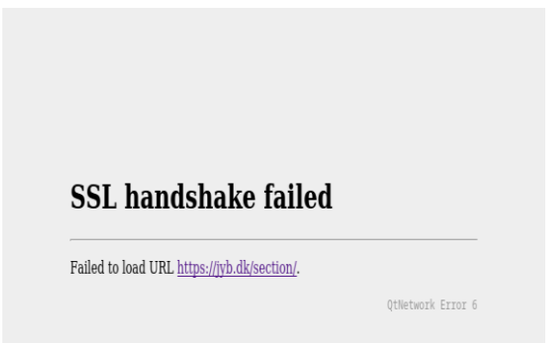
Se utilizó el siguiente entorno y herramientas para el análisis:

- **Entorno:** Máquina virtual con Parrot OS
- **Herramientas:** cat, grep, python3, quopri, curl, cutycapt, xvfb.

Pasos realizados

- **Decodificación del .eml:** Se utilizó quopri para decodificar el contenido en formato quoted-printable.
- **Extracción de URLs:** Con grep y python3, se identificaron y decodificaron las URLs embebidas.
- **Verificación de redirecciones:** Se utilizó curl para seguir las redirecciones y confirmar la estructura de evasión.
- **Captura de pantalla:** Se empleó cutycapt junto con xvfb para capturar la imagen del sitio malicioso.

Resultado de la captura



Interpretación:

Este error indica que el navegador o herramienta utilizada no pudo establecer una conexión segura HTTPS con el sitio web, posiblemente debido a un certificado autofirmado o inválido en el servidor, lo cual es común en infraestructuras maliciosas.

Hashes de la Captura de Pantalla

Los siguientes hashes fueron generados para la imagen capturada:

- **MD5:** 16ba29cba826b59baeabee003d21e80a
- **SHA1:** ecad997ecbb3a48731a457a5ac501695591cbe15
- **SHA256:** 51663ee1d9355538acb167294a762f4e6c999aff07ae368aca17486e84fe8eea

Nombre de Variante Detectada

La muestra se alinea con **una variante del malware de phishing catalogado como *Phish.LIVE.DTI.URL***, identificado por múltiples firmas y comportamientos en análisis dinámico. Su estructura y evasión se asemejan a campañas observadas anteriormente relacionadas con **captura de credenciales vía correo corporativo**.

Recomendaciones Técnicas de Mitigación

A nivel de red

- **Bloquear** dominios:
  1. jyb.dk
  2. safelinks.protection.outlook.com
  3. www.google.com/url
- **Implementar** inspección HTTPS con decodificación SSL.
- **Aplicar** reglas de proxy/IDS para detectar patrones de SafeLinks y redirecciones sospechosas.

A nivel de endpoint

- **Implementar** detección basada en hash y análisis heurístico:

.rar→8fff991a0636533d645603c208b656622196f3effa61563e0777c5b0498476e3

.eml→6dc2fd7c9e24e03367fdef3c65d849085392ae9039728c6d6ed25565e972f34f

- **Desplegar** políticas automáticas para poner en cuarentena archivos comprimidos protegidos por contraseña.
- **Revisar** actividad en carpetas %AppData%, %Temp%, y procesos que abran .eml fuera de Outlook..

Concienciación institucional

- **Alertar** a usuarios sobre correos de expiración de cuentas o servidores con adjuntos sospechosos.
- **Capacitar** en verificación de enlaces, incluso si provienen de servicios legítimos como Microsoft SafeLinks.
- **Implementar** simulaciones periódicas de phishing técnico para medir conciencia y respuesta.

Inteligencia y coordinación

- **Registrar** IoCs en plataformas como MISP, Trellix Insights, AlienVault OTX.
- **Compartir** información con entidades nacionales (CERT/CSIRT) si se detectan campañas similares.

Vector de Ataque (Gráfico)

Paso A: Correo con archivo .rar

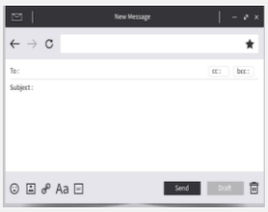
- El atacante envía un **correo electrónico malicioso** que aparenta ser legítimo (por ejemplo, alertas administrativas, expiración de servidores, etc.).
- El mensaje contiene un **adjunto .rar**, que puede estar protegido por contraseña o simplemente disfrazado con un nombre técnico para evadir filtros de spam.

Paso B: Usuario es inducido a descargar y extraer

- El usuario, engañado por el contenido del mensaje, **descarga el archivo .rar** y lo **extrae** manualmente.
- Este paso requiere **interacción del usuario**, por lo tanto, se clasifica bajo la técnica MITRE **T1204 – Ejecución por el usuario**.

Paso C: .eml malicioso

- Dentro del .rar se encuentra un **archivo .eml** (formato de mensaje de correo electrónico).
- El archivo .eml **simula ser un mensaje legítimo**, muchas veces con asuntos urgentes o técnicos para generar presión.



Paso D: Usuario abre .eml

- Al abrir el archivo .eml, el usuario ve un correo que contiene enlaces ofuscados mediante servicios como SafeLinks o redirecciones de Google.
- Técnicamente, esta táctica busca evadir mecanismos de detección automatizados de seguridad en gateways de correo y filtros web (**MITRE T1027 – Ofuscación**).

Paso E: Enlace SafeLinks / Google Redirect

- El usuario hace clic en los enlaces dentro del .eml, los cuales están disfrazados con URLs como:
  - https[:]//nam10[.]safelinks[.]protection[.]outlook[.]com/?url=https%3A%2F%2Fwww[.]google[.]com…
  - https[:]//www[.]google[.]com/url?q=https%3A%2F%2Fjyb[.]dk%2Fsection%2F&sa=…
- Estas redirecciones permiten ocultar el destino real hasta que se realiza el clic.
- Técnica asociada: **MITRE T1568.002** – C2 vía Web Services.

Paso F: Redirección a jyb.dk

- Finalmente, la redirección lleva al usuario al dominio malicioso final:
- https://jyb.dk/section/#~JQ~3L3htmQkSrFSGGpauyIlLHDb4bIyAUGYZrYz3G==DW3EGONDpH4Yo0u7jUlli0sbof7B05JqWXjL3v
- Esta página puede simular un formulario de inicio de sesión, página institucional o captura de información.

- **Paso G: Captura de credenciales**
- El usuario introduce sus credenciales en el formulario falso, sin saber que está proporcionando su información a los atacantes.
- En este punto, se completa el objetivo principal del atacante: robo de credenciales.

Herramientas de Análisis Utilizadas

- Parrot OS Security Edition
- Pestudio
- curl & wget
- Script personalizado en Bash
- Python
- sha256sum / sha1sum / md5sum
- QEMU/KVM + Virt-Manager

Fuentes Oficiales

- MITRE ATT&CK Framework - https://attack.mitre.org
- Trellix (McAfee) Sandbox Analysis **-** https://www.trellix.com
- Outlook SafeLinks Documentation **-** https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/atp-safe-links