

SOC (Security Operations Center)

Módulo 5 – Herramientas



EDR - Ejercicios

Sheila Fernández Cisneros – 24/06/2024

Ejercicios EDR (“Endpoint Detection and Response”)

En estos ejercicios, debemos enfocarnos en analizar las diferentes alertas, sin basarnos exclusivamente en responder las preguntas (pueden servir de guía si alguien se atasca).

Los ejercicios de este módulo requieren tener un conocimiento documentado de como elaborar un informe tras recibir un incidente de seguridad. Debido a que no se detalla el tipo de informe que se requiere, se tomará en cuenta estas distinciones.

Para realizar un informe tras un incidente de seguridad, éste seguirá los protocolos normalizados de trabajo que tenga establecidos la empresa que lo emita y además puede ir acompañado por un informe no técnico y otro técnico con mas detalles de dicho incidente.

Otro factor a tener en cuenta a la hora de emitir un informe es el destinatario, este puede ser un destinatario interno (familiarizado con los protocolos de trabajo internos), un departamento técnico o un cliente externo. De todos modos, el informe general de respuesta a incidentes de seguridad debe recoger toda la información mas relevante y apto para cualquier destinatario.

Por otro lado, el informe técnico proporcionará más detalles técnicos o un análisis más exhaustivo de los resultados de dicho incidente.

Informe Técnico

El informe técnico es detallado y específico, adecuado para un destinatario interno dentro de la empresa, como el equipo de TI, el equipo de seguridad o la gerencia responsable de la ciberseguridad. Este informe contiene:

- Descripción detallada del incidente.
- Resultados de análisis técnicos.
- Medidas tomadas y recomendaciones específicas.
- Detalles de herramientas y técnicas de análisis.

Informe No Técnico

El informe no técnico es más general y explicativo, adecuado tanto para un destinatario interno que no necesariamente tiene un profundo conocimiento técnico (como la gerencia no técnica) como para un destinatario externo (como clientes o socios que utilizan los servicios de seguridad del SOC). Este informe contiene:

- Descripción clara y concisa del incidente.
- Resultados de análisis explicados en términos comprensibles.
- Acciones tomadas de manera comprensible.
- Recomendaciones prácticas y específicas.

Ejemplos de Uso

Interno (Técnico):

- **Destinatario:** Equipo de Seguridad de la Información, Administradores de Sistemas.
- **Propósito:** Proveer detalles técnicos para implementar medidas correctivas y mejorar la postura de seguridad interna.

Interno (No Técnico):

- **Destinatario:** Alta Gerencia, Departamento de Recursos Humanos.
- **Propósito:** Informar sobre el incidente y las acciones tomadas sin entrar en detalles técnicos complejos.

Externo (No Técnico):

- **Destinatario:** Clientes que utilizan servicios de seguridad gestionada.
- **Propósito:** Mantener la transparencia y confianza, proporcionar una explicación clara del incidente y las medidas de mitigación sin revelar detalles técnicos internos sensibles.

Tarea 1:

Imagina que trabajas en un SOC como analista de Nivel 1. Recibes una alerta en la que se describe el incidente que se muestra a continuación:

Alerts		LINK(S):	TO:	FIRST SEEN	LAST SEEN
FROM:	info@skillbrick.com	https://offe...	equipo1@gmail.com	10/06/24 12:58	10/06/24 12:58
					
Description – Phishing					
<ul style="list-style-type: none">- Message ID: <0.0.F.6A9.1DAC09780B1AA62.0@mail45.euc1.acems3.com>- From: "Skillbrick" <info@skillbrick.com>- To: <equipo1@gmail.com>- Subject: 50% de descuento - Cómo utilizar la IA en el trabajo- IP Sender: 217.8.118.45- Link(s): hxxps(:)//offentligautbildningar61088.emlnk9(.)com/l(.).php?x=3DZy~GDEV3bM DaB6zAy9W(.)dvAaAlvNLyw-w2YXbLUnmbEKB_- Oy.OeNy2HVzj_bvlvYyYoHHI3me6m- QR(s): None- Attached File(s): None					

Realiza un pequeño informe basándote al menos en las siguientes cuestiones:

- **¿De qué tipo de alerta se trata?**
- **¿Es maliciosa la IP del remitente (IP Sender)? (Para ello, utiliza VirusTotal)**
- **El enlace que se encuentra en el e-mail, ¿se considera malicioso? (Para ello, utiliza VirusTotal). Ten en cuenta que el link que se encuentra en la Figura anterior está sanitizado. Investiga además en qué consiste la sanitización de links. (No se debe acceder nunca a un link que puede ser malicioso, por lo que se recomienda tener cuidado)**
- **Tras analizar tanto la IP del remitente como el link adjunto en el e-mail, ¿podemos decir que se trata de un falso positivo, o por el contrario es un intento de phishing? ¿Por qué?**

A continuación, se detallará lo que podría ser un ejemplo de informe técnico, el cual podría ajustarse a la finalidad del ejercicio incluyendo una nota aclaratoria sobre la sanitización de enlaces que pide el enunciado del mismo.

Informe Técnico de Incidente de Seguridad

SOC - Centro de Operaciones de Seguridad

Fecha: 26/06/2024

Analista: Sheila Fernández

Asunto: Informe de Incidente de Seguridad - Alerta de Phishing

Hora del Análisis: 26/06/2024, 12:00 CEST

Descripción del Incidente

- **Tipo de Incidente:** Phishing
- **Fecha y Hora de Detección:** 10/06/2024 12:58
- **Descripción del Incidente:** El día 10 de junio de 2024 a las 12:58 horas, se recibió una alerta en el Centro de Operaciones de Seguridad (SOC) indicando un posible intento de phishing. La alerta fue generada por el sistema de monitoreo de correo electrónico y contenía la siguiente información:

Mensaje ID: 0.O.F.6A9.1DAC09780B1AA62.0@mail45.euc1.acems3.com

Remitente: "Skillbrick" info@skillbrick.com

Destinatario: equipo1@gmail.com

Asunto: 50% de descuento - Cómo utilizar la IA en el trabajo

IP del Remitente: 217.8.118.45

Enlace(s) sanitizado:

hxxps(:)//offentligautbildningar61088.emlnk9(.)com/lt(.)php?x=3DZyGDEV3bM
DaB6zAy9W(.

)dvaAaAlvNLyww2YXbLUnmbEKB_0y.0eNy2HVzj_bvlvYyVoHHl3me6m

Códigos QR: Ninguno

Archivos Adjuntos: Ninguno

Primera vez visto: 10/06/2024 12:58

Última vez visto: 10/06/2024 12:58

Análisis del Incidente

El análisis de la IP y URL se realizaron en diferentes plataformas de seguridad en línea para obtener una evaluación completa de posibles amenazas.

1. Análisis de la IP

VirusTotal

- **IP 217.8.118.45:**
 - **Último Análisis:** Hace 17 horas
 - **Detecciones:** 0/93 proveedores de seguridad. No se detectaron actividades maliciosas.
 - **AS 16509 (AMAZON-02)**
 - **AS 16509:** El número de Sistema Autónomo (Autonomous System Number, ASN). Un AS es un conjunto de IPs administradas por una o más redes que siguen la misma política de enrutamiento.
 - **AMAZON-02:** El nombre del Sistema Autónomo, en este caso, pertenece a Amazon. Este nombre indica que la IP es administrada por Amazon Web Services (AWS).
 - **Detalles del WHOIS:**
 - **Rango de IP:** 217.8.0.0 - 217.255.255

- **Organización:** RIPE Network Coordination Centre (RIPE NCC)
- **Ubicación:** Amsterdam, Países Bajos
- **Historial de resoluciones DNS:**
 - Resolución más reciente: mail45.euc1.acems3.com

AbuseIPDB

- **IP 217.8.118.45:**
 - No se encontraron registros de abuso.
 - **ISP:** ActiveCampaign LLC
 - **Tipo de Uso:** Data Center/Web Hosting/Transit
 - **Dominio:** activecampaign.com
 - **Ubicación:** Frankfurt am Main, Hesse, Alemania

2. Análisis de la url contenida en el email

Enlace Desanitizado:

https://offentligautbildningar61088.emlnk9.com/lt/.php?x=3DZy~GDEV3bMDaB6zAy9W.dvAaAlvNLyw-w2YXbLUunmbEKB_-0y.0eNy2HVzj_bvlvYyYoHHI3me6m

Sanitización de Enlaces

La sanitización de enlaces consiste en transformar los enlaces potencialmente peligrosos para prevenir que se haga clic en ellos accidentalmente. En este caso, el enlace ha sido "sanitizado" utilizando "hxps" y paréntesis para reemplazar los puntos, lo que evita que el enlace sea directamente clicable.

VirusTotal

- **Último Análisis:** Momentos antes del análisis.
- **Detecciones:** 0 de 95 proveedores de seguridad marcaron el enlace como malicioso.
- **Detalles Técnicos:**
 - **Redireccionamientos:** Múltiples redireccionamientos detectados.
 - **Código de Estado HTTP:** 307: Código de estado de la respuesta HTTP enviado por el servidor al solicitar la URL que se está estudiando.
 - **Dirección IP del Servidor:** 54.225.69.136

URLVoid

- **Dominio:** offentligautbildningar61088.emlnk9.com
 - **Último Análisis:** Hace 5 días
 - **Detecciones:** 0/40
 - **Registro de Dominio:** 02-06-2014 (hace 10 años)
 - **IP:** 54.225.69.136
 - **Reverse DNS:** ec2-54-225-69-136.compute-1.amazonaws.com
 - **ASN:** AS14618 AMAZON-AES
 - **Ubicación del Servidor:** Ashburn, Virginia, Estados Unidos

Análisis de la IP del enlace del email: 54.225.69.136

VirusTotal

- **Último Análisis:** Hace 10 días
- **Detecciones:** 0/93 proveedores de seguridad. No se detectaron actividades maliciosas.
- **AS 14618 (AMAZON-02)**
- **Detalles del WHOIS:**
 - **Rango de IP:** 54.224.0.0 - 54.255.255.255
 - **Organización:** Amazon Technologies Inc. (AT-88-Z)
 - **Ubicación:** Estados Unidos
- **Historial de resoluciones DNS:**
 - Resolución más reciente: luxe-marketing.acemlnb.com

AbuseIPDB

- No se encontraron registros de abuso.
- **ISP:** Amazon Technologies Inc.
- **Tipo de Uso:** Data Center/Web Hosting/Transit
- **Dominio:** amazonaws.com
- **Ubicación:** Ashburn, Virginia

Conclusión

El análisis de la IP y la URL sospechosa muestra que no se detectaron amenazas por parte de VirusTotal y URLVoid. Sin embargo, la presencia de múltiples redireccionamientos y el uso de un código de estado 307 (Temporary Redirect) indican una posible táctica evasiva común en ataques de phishing. La IP está asociada a Amazon Web Services, lo cual no descarta su uso potencial en actividades maliciosas. Se recomienda seguir monitoreando esta IP y URL, bloquear temporalmente el dominio sospechoso y educar a los usuarios sobre los riesgos asociados a redireccionamientos en correos electrónicos sospechosos.

Acciones a tomar: Recomendaciones

Con la información proporcionada por los distintos servicios consultados, se deben tomar las siguientes acciones para garantizar la seguridad de la red y mitigar posibles amenazas.

1. Investigación Adicional de Redireccionamientos

- **Acción:** Seguir y analizar todos los redireccionamientos detectados desde la URL inicial hasta el destino final.
- **Herramientas:** Utilizar cURL para realizar solicitudes HTTP y capturar el flujo completo de redirección, y Wireshark para analizar el tráfico de red.

2. Monitoreo y Bloqueo Temporal

- **Acción:** Bloquear temporalmente el dominio offentligautbildningar61088.emlnk9.com y la IP 54.225.69.136 en el firewall y sistemas de filtrado de correo electrónico para prevenir acceso hasta que se complete el análisis.
- **Justificación:** Aunque no se detectaron amenazas por los proveedores de seguridad, la presencia de múltiples redireccionamientos y el uso de un código de estado 307 son motivos de precaución.

3. Educación y Alerta a los Usuarios

- **Acción:** Informar a los usuarios sobre el incidente potencial y recordarles las mejores prácticas para identificar y reportar correos electrónicos sospechosos.
- **Herramientas:** Comunicados internos y sesiones de formación.

4. Análisis Detallado de Logs

- **Acción:** Revisar los logs del sistema de correo electrónico y del firewall para detectar cualquier tráfico relacionado con la URL o la IP sospechosa.
- **Herramientas:** SIEM (Splunk, LogRhythm) para buscar patrones de tráfico y actividad inusual.

5. Implementación de Medidas de Seguridad Adicionales

- **Acción:** Revisar y mejorar las políticas de seguridad relacionadas con el filtrado de correos electrónicos y la gestión de redirecciones HTTP.
- **Herramientas:**
 - Proofpoint Email Protection o Mimecast para mejorar la seguridad del correo electrónico.
 - Actualización de reglas en el firewall para gestionar mejor las redirecciones HTTP.

6. Reevaluación de la URL y la IP a Intervalos Regulares

- **Acción:** Continuar monitoreando la URL y la IP en servicios de reputación a intervalos regulares para detectar cualquier cambio en su estatus de seguridad.
- **Justificación:** Las amenazas pueden emerger después del análisis inicial, por lo que es crucial seguir monitoreando.

Resumen de Acciones Inmediatas

1. **Seguir y analizar redireccionamientos** para verificar la legitimidad del destino final.
2. **Investigar la URL y la IP** en bases de datos adicionales de reputación y seguridad.
3. **Bloquear temporalmente** el dominio y la IP en el firewall y sistemas de filtrado de correo electrónico.
4. **Informar y educar a los usuarios** sobre el incidente potencial.
5. **Revisar logs del sistema** para detectar cualquier tráfico relacionado.
6. **Revisar y mejorar políticas de seguridad** para el filtrado de correos y gestión de redirecciones.
7. **Monitorear regularmente** la URL y la IP en servicios de reputación.

Estas acciones garantizarán una respuesta exhaustiva y proactiva ante el potencial riesgo identificado.

Firma: Sheila Fernández, Analista SOC N1, 26/06/2024

Este informe está dirigido al equipo de seguridad y a la administración de TI para la evaluación y acción inmediata.

Anexos

- **Anexo 1: Análisis de la IP en Virus Total.**
- **Anexo 2: Detalles de la IP en Virus Total.**
- **Anexo 3: Análisis de la IP en abusePDB.**

- **Anexo 4: Detalles de la IP en abusePDB.**
- **Anexo 5: Análisis de la url en VirusTotal.**
- **Anexo 6: Detalles de la url por VirusTotal**
- **Anexo 7: Análisis de la url en URLVOID**
- **Anexo 8: Análisis de la IP del enlace incluido en el email por VirusTotal**
- **Anexo 9: Análisis de la IP del enlace del email en URLVOID**

Anexo 1: Análisis de la IP en Virus Total: captura de pantalla mostrando que 0 de 93 proveedores de seguridad marcaron la IP como maliciosa.

No security vendor flagged this IP address as malicious

217.8.118.45 (217.8.118.0/24)
AS 16509 (AMAZON-02)

Community Score: 0 / 93

REANALYZE SIMILAR GRAPH API

US Last Analysis Date: 17 hours ago

DETECTION DETAILS RELATIONS COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis		Do you want to automate checks?	
Abusix	✓ Clean	Acronis	✓ Clean
ADMINUSLabs	✓ Clean	Allabs (MONITORAPP)	✓ Clean
AlienVault	✓ Clean	alphaMountain.ai	✓ Clean
Antiy-AVL	✓ Clean	benkow.cc	✓ Clean
BitDefender	✓ Clean	Blueliv	✓ Clean
Certego	✓ Clean	Chong Lua Dao	✓ Clean
CINS Army	✓ Clean	CMC Threat Intelligence	✓ Clean
CRDF	✓ Clean	Criminal IP	✓ Clean
Cyble	✓ Clean	CyRadar	✓ Clean
desenmascara.me	✓ Clean	DNS8	✓ Clean
Dr.Web	✓ Clean	EmergingThreats	✓ Clean
Emsisoft	✓ Clean	ESET	✓ Clean
ESTsecurity	✓ Clean	Fortinet	✓ Clean
G-Data	✓ Clean	Google Safebrowsing	✓ Clean
GreenSnow	✓ Clean	Heimdal Security	✓ Clean
IPsum	✓ Clean	Juniper Networks	✓ Clean
K7AntiVirus	✓ Clean	Lionic	✓ Clean
Malwared	✓ Clean	MalwarePatrol	✓ Clean
malwares.com URL checker	✓ Clean	OpenPhish	✓ Clean

Anexo 2: Detalles de la IP en Virus Total: Información adicional sobre la asignación de la IP.

Σ 217.8.118.45

No security vendor flagged this IP address as malicious

217.8.118.45 (217.8.118.0/24)
AS 16509 (AMAZON-02)

Community Score: 0 / 93

Detection Details Relations Community

[Join our Community](#) and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Basic Properties

Network	217.8.118.0/24
Autonomous System Number	16509
Autonomous System Label	AMAZON-02
Regional Internet Registry	ARIN
Country	US
Continent	NA

Whois Lookup

NetRange: 217.0.0.0 – 217.255.255.255
 CIDR: 217.0.0.0/8
 NetName: 217-RIPE
 NetHandle: NET-217-0-0-0-1
 Parent: ()
 NetType: Allocated to RIPE NCC
 Organization: RIPE Network Coordination Centre (RIPE)
 RegDate: 2000-06-05
 Updated: 2009-03-25
 Comment: These addresses have been further assigned to users in
 Comment: the RIPE NCC region. Contact information can be found in
 Comment: the RIPE database at <http://www.ripe.net/whois>
 Ref: <https://rdap.arin.net/registry/ip/217.0.0.0>
 ResourceLink: <https://apps.db.ripe.net/search/query.html>
 ResourceLink: whois.ripe.net
 OrgName: RIPE Network Coordination Centre
 OrgId: RIPE
 Address: P.O. Box 10096
 City: Amsterdam

Whois Lookup

OrgId: RIPE
 Address: P.O. Box 10096
 City: Amsterdam
 PostalCode: 1001EB
 Country: NL
 Updated: 2013-07-29
 Ref: <https://rdap.arin.net/registry/entity/RIPE>
 ReferralServer: whois://whois.ripe.net
 ResourceLink: <https://apps.db.ripe.net/search/query.html>
 OrgTechHandle: RN029-ARIN
 OrgTechName: RIPE NCC Operations
 OrgTechPhone: +31 20 535 4444
 OrgTechEmail: hostmaster@ripe.net
 OrgTechRef: <https://rdap.arin.net/registry/entity/RN029-ARIN>
 OrgAbuseHandle: ABUSE3850-ARIN
 OrgAbuseName: Abuse Contact
 OrgAbusePhone: +31205354444
 OrgAbuseEmail: abuse@ripe.net
 OrgAbuseRef: <https://rdap.arin.net/registry/entity/ABUSE3850-ARIN>

Google results

About 2 results (0.11 seconds) Sort by: Relevance

IP address information (217.8.0.0 - IP/Domain Lookup
en.ntnths.net
... 217.8.118.45 217.8.118.46 217.8.118.47 217.8.118.48 217.8.118.49 217.8.118.50 217.8.118.51 217.8.118.52 217.8.118.53 217.8.118.54 217.8.118.55 217.8.118.56 ...

IP 주소 정보 (118.45.0.0 - 118.45.255.255) - 모든 IP 주소 정보
kr.ntnths.net
... 217.8.118.45 217.9.118.45 217.10.118.45 217.11.118.45 217.12.118.45 217.13.118.45 217.14.118.45 217.15.118.45 217.16.118.45 217.17.118.45 217.18.118.45 ...

Q Search for "217.8.118.45" on Google ENHANCED BY Google

DETECTION DETAILS RELATIONS COMMUNITY

[Join our Community](#) and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Passive DNS Replication (1)

Date resolved	Detections	Resolver	Domain
2024-03-07	0 / 93	VirusTotal	mail45.euc1.acems3.com

Historical Whois Lookups (2)

Last Updated	Organization	Email
+ 2024-06-25	RIPE Network Coordination Centre	abuse@ripe.net
+ 2020-06-30	RIPE Network Coordination Centre	abuse@ripe.net

Graph Summary

Anexo 3: Análisis de la IP en abusePDB:

AbuseIPDB » 217.8.118.45

Check an IP Address, Domain Name, or Subnet
e.g. 37.222.61.117, microsoft.com, or 5.188.10.0/24

37.222.61.117

217.8.118.45 was not found in our database

ISP	ActiveCampaign LLC
Usage Type	Data Center/Web Hosting/Transit
Hostname(s)	mail45.euc1.acems3.com
Domain Name	activecampaign.com
Country	Germany
City	Frankfurt am Main, Hessen

*IP info including ISP, Usage Type, and Location provided by IP2Location.
Updated monthly.*

[REPORT 217.8.118.45](#) [WHOIS 217.8.118.45](#)

Anexo 4: Detalles de la IP en abusePDB:

mail45.euc1.acems3.com

Subdomains

- mail42.apse2
- mail41.euc1
- mail54.use1
- mail124.euc1
- mail40.euc1
- mail217.euc1
- s10
- mail138.use1
- mail143
- mail205.apse2
- mail54.apse2
- mail130.euc1
- mail50.use1
- mail208.apse2
- mail42-184
- mail40.use1
- mail55.use1
- mail37.euc1
- mail148
- mail136.euc1
- mail45.euc1
- mail218.apse2
- mail121.apse2
- mail208.euc1
- mail155
- mail206.apse2
- mail50.apse2
- mail124.apse2
- mail43.euc1
- mail44.apse2
- mail49.apse2
- mail131.apse2
- mail215.euc1
- mail153
- mail216.apse2
- s2
- mail36.use1
- mail47.euc1
- mail39.euc1
- mail46.euc1
- mail135.euc1
- mail220.euc1
- mail123.use1
- s12
- mail214.use1
- mail47.use1
- mail48.euc1
- mail42-193
- s15
- mail122.apse2
- mail219.use1
- mail121.euc1
- mail213.apse2
- mail38.euc1
- mail134.euc1
- mail212.euc1
- mail4-188
- mail51.euc1
- mail120.apse2
- mail52.apse2
- mail125.apse2
- mail135.use1
- mail137.use1
- mail211.use1
- mail49.euc1
- s6
- mail215.use1
- mail220.use1
- mail214.apse2
- mail207.euc1
- mail136.use1
- mail132.apse2
- mail42-175
- mail205.euc1
- mail210.euc1
- mail139.use1
- mail123.apse2
- mail205.use1
- mail221.euc1
- mail38.apse2
- mail212.use1
- mail208.use1
- mail41.apse2
- mail42.use1
- mail124.use1
- s19
- s5
- mail131.euc1
- mail204.euc1
- mail222.apse2
- mail129.use1
- s16
- mail137.euc1
- mail129.apse2
- mail44.euc1
- mail131.use1
- mail210.use1
- mail55.euc1
- s13
- mail42-191
- mail50.euc1
- mail219.euc1
- mail43.use1
- mail127.euc1
- s18
- mail54.euc1
- mail211.euc1
- mail139.apse2
- mail211.apse2
- mail134.apse2
- mail39.use1
- mail218.euc1
- s20
- mail216.euc1
- mail206.use1
- mail222.euc1
- mail44.use1
- mail46.use1
- mail219.apse2
- mail42-172
- s1
- mail133.use1
- mail42-178
- mail45.apse2
- mail145
- mail213.use1
- mail38.use1
- mail129.euc1
- mail126.apse2
- mail40.apse2
- mail150
- mail214.euc1
- mail53.apse2
- mail46.apse2
- mail48.apse2
- mail217.apse2
- mail125.euc1
- mail133.apse2
- mail129.use1
- www
- mail45.use1
- mail42-183
- mail120.euc1
- mail53.euc1
- mail221.apse2
- s3
- mail126.euc1
- mail139.euc1
- mail126.use1
- mail42.euc1
- mail218.use1
- mail223.use1
- s9
- mail37.apse2
- mail39.apse2
- mail122.euc1
- mail43.apse2
- mail147
- mail204.use1
- s7
- mail130.apse2
- mail135.apse2
- mail151
- mail221.use1
- mail123.euc1
- mail204.apse2
- mail122.use1
- mail125.use1
- mail210.apse2
- mail154
- mail122.use1
- mail48.use1
- mail51.apse2
- mail128.euc1
- mail220.apse2
- mail52.euc1
- mail41.use1
- mail138.euc1
- s17
- mail223.euc1
- mail42-181
- mail47.apse2
- s14
- s11
- mail51.use1
- mail140
- mail37.use1
- mail216.use1
- mail42-176
- mail36.apse2
- mail133.euc1
- mail152
- mail207.apse2
- s4
- mail42-180
- mail55.apse2
- mail209.use1
- mail206.euc1
- mail213.euc1
- mail209.euc1
- mail120.use1
- mail138.apse2
- mail132.euc1
- mail223.apse2
- mail53.use1
- s8
- mail207.use1
- mail204.apse2
- s7
- mail130.apse2
- mail135.apse2
- mail151
- mail221.use1
- mail123.euc1

Current DNS Records

A	AAAA	MX	TXT	NS	SOA
217.8.118.45	n/a	n/a	n/a	n/a	n/a

Want useful, structured WHOIS and DNS data like this? Check out **SecurityTrails**

Raw Whois Results for 217.8.118.45

```
% This is the RIPE Database query service.  
% The objects are in RPSL format.  
%  
% The RIPE Database is subject to Terms and Conditions.  
% See https://apps.db.ripe.net/docs/HTML-Terms-And-Conditions  
  
%ERROR:201: access denied for 2604:a880:400:d0:0:0:40e7:1001  
%  
% Sorry, access from your host has been permanently  
% denied because of a repeated excessive querying.  
% For more information, see  
% https://apps.db.ripe.net/docs/FAQ/#why-did-i-receive-an-error-201-access-denied  
  
% This query was served by the RIPE Database Query Service version 1.112.1 (BUSA)
```

This page displays the publicly-available WHOIS data for 217.8.118.45, which belongs to an unknown organization.

Anexo 5: Análisis de la url en VirusTotal: captura de pantalla mostrando que 0 de 95 proveedores de seguridad marcaron el enlace como malicioso.

We have changed our Privacy Notice and Terms of Use, effective July 18, 2024. You can view the updated [Privacy Notice](#) and [Terms of Use](#).

No security vendors flagged this URL as malicious

https://offentligautbildningar6188.emlnk9.com/lt/.php?x=3DZy-GDEV3bMDaB6zAy9W.dvAaAlvNLyw-w2YxbLUunmbEKB_-0y.0eNy2HVzj_bvlVYy0HHI3me6m

Community Score: 0 / 95

Detection | Details | Community

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendor	Analysis	Do you want to automate checks?
Abusix	Clean	Clean
ADMINUSLabs	Clean	Clean
AlienVault	Clean	Clean
Antiy-AVL	Clean	Clean
benkow.cc	Clean	Clean
BlockList	Clean	Clean
Certego	Clean	Clean
CINS Army	Clean	Clean
CRDF	Clean	Clean
Cyble	Clean	Clean
desenmascara.me	Clean	Clean
Dr.Web	Clean	Clean
Emsisoft	Clean	Clean
ESTsecurity	Clean	Clean
Forcepoint ThreatSeeker	Clean	Clean
G-Data	Clean	Clean
GreenSnow	Clean	Clean
IPSum	Clean	Clean
Acronis	Clean	Clean
Allabs (MONITORAPP)	Clean	Clean
alphamountain.ai	Clean	Clean
Artists Against 419	Clean	Clean
BitDefender	Clean	Clean
Blueliv	Clean	Clean
Chong Lua Dao	Clean	Clean
CMC Threat Intelligence	Clean	Clean
Criminal IP	Clean	Clean
CyRadar	Clean	Clean
DNS8	Clean	Clean
EmergingThreats	Clean	Clean
ESET	Clean	Clean
Feodo Tracker	Clean	Clean
Fortinet	Clean	Clean
Google Safebrowsing	Clean	Clean
Heimdal Security	Clean	Clean
Juniper Networks	Clean	Clean

Anexo 6: Detalles de la url en VirusTotal: Información adicional sobre redireccionamientos, categoría y recursos del enlace.

The screenshot shows the URLVoid analysis interface for the provided URL. Key findings include:

- Community Score:** 0 / 95
- No security vendors flagged this URL as malicious.**
- URL:** https://offentligautbildningar6188.emlnk9.com/l/.php?x=3DZy~GDEV3bMDaB6zAy9W.dvAaAlvNLyw-w2YXbLUunmbEKB_-0y.0eNy2Hvzj_bvlVYyYoHHI3me6m
- Status:** 307
- Last Analysis:** a moment ago
- Detection:** No malicious vendors flagged the URL.
- Categories:** Sophos, Forcepoint ThreatSeeker (parked domains, web and email marketing)
- History:** First Submission: 2024-06-26 10:04:48 UTC; Last Submission: 2024-06-26 10:04:48 UTC; Last Analysis: 2024-06-26 10:04:48 UTC
- HTTP Response:** Final URL: https://offentligautbildningar6188.emlnk9.com/l/.php?x=3DZy~GDEV3bMDaB6zAy9W.dvAaAlvNLyw-w2YXbLUunmbEKB_-0y.0eNy2Hvzj_bvlVYyYoHHI3me6m
- Serving IP Address:** 54.225.69.136
- Status Code:** 307
- Body Length:** 14 B
- Body SHA-256:** 5316717f872a3b46022c0c6b37009e1a18df8809a0cd70a58d8c47fd97f9919c
- Headers:**

Header	Value
cache-control	public, max-age=2628000
location	https://offentligautbildningar6188.activehosted.com/l/.php?x=3DZy~GDEV3bMDaB6zAy9W.dvAaAlvNLyw-w2YXbLUunmbEKB_-0y.0eNy2Hvzj_bvlVYyYoHHI3me6m
date	Wed, 26 Jun 2024 10:04:51 GMT
content-length	0
x-envoy-upstream-service-time	2
server	istio-envoy
- HTML Info:**
 - Meta Tags:** color-scheme: light dark
- Redirection chain:** https://offentligautbildningar6188.emlnk9.com/l/.php?x=3DZy~GDEV3bMDaB6zAy9W.dvAaAlvNLyw-w2YXbLUunmbEKB_-0y.0eNy2Hvzj_bvlVYyYoHHI3me6m

Anexo 7: Análisis de la url en URLVOID:

Report Summary	
Website Address	Offentligautbildningar&1088.emlnk9.com
Last Analysis	5 days ago Rescan
Detections Counts	0/40
Domain Registration	2014-06-02 10 years ago
Domain Information	WHOIS Lookup DNS Records Ping
IP Address	54.225.69.136 Find Websites IPVoid Whois
Reverse DNS	ec2-54-225-69-136.compute-1.amazonaws.com
ASN	AS14618 AMAZON-AES
Server Location	(US) United States
Latitude\Longitude	39.0469 / -77.4903 Google Map
City	Ashburn
Region	Virginia

Anexo 8: Análisis de la IP del enlace del email en VirusTotal

We have changed our Privacy Notice and Terms of Use, effective July 18, 2024. You can view the updated [Privacy Notice](#) and [Terms of Use](#).

0 / 93

No security vendor flagged this IP address as malicious

54.225.69.136 (54.225.0.0/16)
AS 14618 (AMAZON-AES)

US | Last Analysis Date: 10 days ago

Community Score

DETECTION **DETAILS** **RELATIONS** **COMMUNITY (2)**

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

				Do you want to automate checks?	
0xSl_f3d	?	Unrated	Abusix	?	Unrated
Acronis	?	Unrated	ADMINUSLabs	?	Unrated
AI Labs (MONITORAPP)	?	Unrated	AlienVault	?	Unrated
alphaMountain.ai	?	Unrated	AlphaSOC	?	Unrated
Antiy-AVL	?	Unrated	ArcSight Threat Intelligence	?	Unrated
AutoShun	?	Unrated	berkow.cc	?	Unrated
Bfore.Ai PreCrime	?	Unrated	BitDefender	?	Unrated
Bkav	?	Unrated	Blueliv	?	Unrated
Certego	?	Unrated	Chong Lua Dao	?	Unrated
CINS Army	?	Unrated	Cluster25	?	Unrated
CMC Threat Intelligence	?	Unrated	CRDF	?	Unrated
Criminal IP	?	Unrated	CSIS Security Group	?	Unrated
Cyan	?	Unrated	Cyble	?	Unrated
CyRadar	?	Unrated	desenmascara.me	?	Unrated
DNS8	?	Unrated	Dr.Web	?	Unrated
EmergingThreats	?	Unrated	Emsisoft	?	Unrated

Passive DNS Replication (200) ⓘ			
Date resolved	Detections	Resolver	Domain
2024-06-30	0 / 93	VirusTotal	luxe-marketing.acemlnb.com
2024-06-30	0 / 93	VirusTotal	cambiar.emlnk9.com
2024-06-30	0 / 93	VirusTotal	blondedollyimageconsulting.emlnk.com
2024-06-30	0 / 93	VirusTotal	trustinsoft.acemlnb.com
2024-06-30	0 / 93	VirusTotal	pmdalliance.acemlnb.com
2024-06-30	0 / 93	VirusTotal	parentpoweredpbc.acemlnb.com
2024-06-30	0 / 93	VirusTotal	serquo.emlnk9.com
2024-06-30	0 / 93	VirusTotal	hfbbwwx1vhcw.acemlna.com
2024-06-30	0 / 93	VirusTotal	phychoi467250.emlnk9.com
2024-06-30	0 / 93	VirusTotal	travelmilesplus.emlnk9.com

...

Communicating Files (2) ⓘ			
Scanned	Detections	Type	Name
2024-04-25	0 / 62	PDF	Gmail - A @caixa analisou seu perfil.pdf
2024-06-20	0 / 66	PDF	hamis-mvm-oldal-6673e66edc04e.pdf

Historical Whois Lookups (2) ⓘ			
Last Updated	Organization	Email	
+ 2024-04-25	Amazon Technologies Inc.	abuse@amazonaws.com	
+ 2021-10-29			

Historical SSL Certificates (3) ⓘ			
First seen	Subject	Thumbprint	
+ 2024-01-13	acemlna.com	1a6bf0c82daa6601632ebdfbe171385473e333e2	
+ 2022-05-28	pma.victor.instamaven.co	a726718985e1874cd35bf6669c105d0ff8bd6d94	
+ 2021-10-25	m	3a0a51b95a8fb081fb035e457cefc8572c31066c	

Graph Summary ⓘ			
 10+ resolutions	 2 communicating files		

Anexo 9: Análisis de la IP del enlace del email en AbusePDB

AbuseIPDB » 54.225.69.136

The screenshot shows the AbuseIPDB search results for the IP address 54.225.69.136. The search bar at the top contains the IP address. Below the search bar, a message states "54.225.69.136 was not found in our database". A table provides the following details:

ISP	Amazon Technologies Inc.
Usage Type	Data Center/Web Hosting/Transit
Hostname(s)	ec2-54-225-69-136.compute-1.amazonaws.com
Domain Name	amazon.com
Country	United States of America
City	Ashburn, Virginia

IP info including ISP, Usage Type, and Location provided by IP2Location. Updated monthly.

At the bottom, there are two buttons: "REPORT 54.225.69.136" and "WHOIS 54.225.69.136".

Una vez realizado los informes me gustaría comentar cierta información encontrada tras el análisis. Es importante destacar que la dirección IP del enlace contenido en el email es importante analizarla por varios motivos.

1. Ayuda a identificar el proveedor de servicios de la dirección IP. En este caso, indica que la IP pertenece a la infraestructura de Amazon Web Services.
2. **Ubicación y Propiedad de la Red:** Proporciona detalles sobre la ubicación y la entidad propietaria de la red que utiliza la IP, lo que puede ser útil para determinar la reputación y la confiabilidad.
3. **Evaluación de Riesgos:** Saber que una IP pertenece a un proveedor grande y confiable como Amazon puede influir en la evaluación del riesgo, aunque también es importante recordar que los atacantes pueden utilizar servidores en proveedores legítimos para actividades maliciosas.

En el contexto de un análisis de seguridad, si una dirección IP está asociada con el AS 16509 AMAZON-02, se puede inferir que esta IP está alojada en Amazon Web Services. Sin embargo, es necesario seguir investigando y no asumir automáticamente que la IP es segura solo por pertenecer a AWS, ya que los servicios en la nube son frecuentemente utilizados por tanto por negocios legítimos como por actores maliciosos para hospedar sus operaciones.

Tarea 2:

Imagina que trabajas en un SOC como analista de Nivel 1. Recibes una alerta en la que se describe el incidente que se muestra a continuación:

Alerts

HOST: equipo2 **NETWORK:** 10.125.0.1



FIRST SEEN
23/05/2024 10:30

LAST SEEN
23/05/2024 10:30

Description - Responder

- **Host IP:** 10.124.76.132
- **EPS Prevention:** false
- **EPS Prevention Success:** NotSet
- **Fake Hostnames:**
gxAKryuQzCxesO8oElChV,TnQdSZyr4pszBDJzM34A,Damw7wfvUKRmEh9t
- **Hostname:** equipo2
- **Responder IP Address:** 10.125.0.1
- **Responder MAC Address:** 08-35-71-08-9E-53

Realiza un pequeño informe basándote al menos en las siguientes cuestiones:

- ¿En qué consisten este tipo de ataques?
- ¿Qué riesgos suponen estos ataques?
- ¿Qué recomendaciones daría al cliente con respecto a esta alerta?

Este tipo de informe siguiendo las preguntas que pide el enunciado se podría realizar del siguiente modo.

Informe Técnico de Incidente de Seguridad

SOC - Centro de Operaciones de Seguridad

Fecha: 26/06/2024

Analista: Sheila Fernández

Asunto: Informe de Incidente de Seguridad - Alerta de Spoofing y Configuración de EPS

Descripción del Incidente

El día 23 de mayo de 2024 a las 10:30 horas, se recibió una alerta en el Centro de Operaciones de Seguridad (SOC) indicando un posible incidente de seguridad en uno de los endpoints de la

red. La alerta fue generada por la solución de seguridad del endpoint (EPS) y contenía la siguiente información:

- **Host IP:** 10.124.76.132
- **EPS Prevention:** false (La prevención de seguridad del endpoint no está activada)
- **EPS Prevention Success:** NotSet (No se ha configurado un estado de éxito o fallo para la prevención)
- **Nombres de Host Falsos:**
 - gxAKryuQzCxesO8oElChV
 - TnQdSZyr4pszBDJzM34A
 - Damw7wfvUKRmEh9t
- **Nombre del Host:** equipo2
- **Dirección IP del Respondedor:** 10.125.0.1
- **Dirección MAC del Respondedor:** 08-35-71-08-9E-53
- **Primera vez visto:** 23/05/2024 10:30
- **Última vez visto:** 23/05/2024 10:30

Análisis de la alerta

1. Tipo de Alerta

El incidente reportado parece ser un ataque de spoofing o suplantación de identidad, donde se utilizan nombres de host falsos para enmascarar la identidad real del dispositivo comprometido. La alerta también indica que la prevención de seguridad del endpoint (EPS) no está habilitada en el dispositivo afectado, lo que facilita la ejecución del ataque.

2. Análisis de la IP

VirusTotal

- **IP Analizada:** 10.125.0.1
- **Detecciones:** Ninguna de las fuentes de seguridad marcó la IP como maliciosa.
- **Último Análisis:** Hace un mes.
- **Detalles de los Motores de Seguridad:**
 - Todos los motores de seguridad (como Fortinet, Kaspersky, McAfee, etc.) no han indicado ninguna actividad maliciosa relacionada con esta IP.

AbuseIPDB

- **IP Analizada:** 10.125.0.1

- **Resultado:** La IP 10.125.0.1 no fue encontrada en la base de datos de AbuseIPDB.
- **Nota Importante:**
 - 10.125.0.1 es una dirección IP privada, utilizada únicamente en entornos de red internos.
 - Cualquier actividad abusiva que se detecte proveniente de una IP interna suele ser causada por un componente interno de la red o por un error/malconfiguración.
 - Se debe tener cuidado al manejar IPs internas para evitar bloqueos innecesarios que podrían afectar el funcionamiento de la red interna.

2. Riesgos Asociados

Los riesgos asociados con este tipo de ataques son los siguientes:

- **Acceso No Autorizado:** El atacante puede obtener acceso no autorizado a la red y a datos sensibles.
- **Pérdida de Datos:** Los datos críticos pueden ser robados o alterados.
- **Interrupción del Servicio:** El ataque puede causar interrupciones en los servicios críticos.
- **Daño a la Reputación:** La reputación de la organización puede verse afectada negativamente.
- **Impacto Económico:** Los costos asociados con la respuesta al incidente y la restauración de los sistemas pueden ser significativos.

Análisis de los resultados

El hecho de que la IP 10.125.0.1 sea una dirección IP privada utilizada dentro de la organización sugiere que la actividad sospechosa detectada está ocurriendo dentro de la red interna de la empresa. Esto puede tener varias implicaciones y puntos de acción clave.

Implicaciones del Uso de una IP Privada

1. **Possible Amenaza Interna:**
 - La actividad sospechosa puede estar siendo generada por un dispositivo comprometido dentro de la red interna, lo que podría indicar la presencia de un atacante interno o un dispositivo infectado por malware.
2. **Errores de Configuración:**
 - La alerta podría ser el resultado de una configuración incorrecta en los dispositivos de red, lo que permite actividades que no deberían estar ocurriendo. Esto puede incluir configuraciones erróneas de DNS, DHCP o de seguridad.

3. Movimientos Laterales:

- Un atacante que haya comprometido un dispositivo dentro de la red interna podría estar utilizando esta IP para moverse lateralmente a través de la red, intentando comprometer otros dispositivos y servicios internos.

4. Simulaciones de Pruebas de Seguridad:

- La actividad podría ser parte de una prueba de seguridad interna (como una simulación de ataque o un ejercicio de red team) llevada a cabo sin el conocimiento de todos los equipos.

Conclusión

La alerta recibida indica una posible suplantación de identidad y una configuración inadecuada de la seguridad del endpoint. Es crucial tomar medidas inmediatas para activar la prevención EPS y asegurar todos los endpoints dentro de la red. Implementando las recomendaciones mencionadas, se mitigarán los riesgos asociados y se fortalecerá la postura de seguridad de la organización.

Recomendaciones

1. Verificar la Configuración del Endpoint:

- Asegurarse de que la configuración de prevención esté habilitada en el endpoint afectado. Esto puede requerir una revisión y activación de las funcionalidades necesarias en la política de seguridad.

2. Revisar Políticas de Seguridad:

- Comprobar las políticas de seguridad para asegurar que todos los endpoints estén configurados correctamente y utilicen todas las medidas de prevención disponibles.

3. Audituar Otros Endpoints:

- Realizar una auditoría exhaustiva de otros endpoints para asegurar que no se encuentren en una situación similar, es decir, con la prevención deshabilitada.

4. Actualizar y Configurar Correctamente EPS:

- Actualizar el software de seguridad del endpoint y configurarlo correctamente para asegurar que todas las funcionalidades preventivas estén activas y operativas.

5. Investigación del Host Comprometido:

- Llevar a cabo una investigación exhaustiva del host con la IP 10.124.76.132 para determinar el alcance del compromiso y tomar medidas correctivas apropiadas.

6. Bloquear IP y Hostnames Falsos:

- Bloquear la dirección IP 10.124.76.132 y los nombres de host falsos identificados en los sistemas de firewall y de detección de intrusos para prevenir futuros accesos malintencionados.

7. Monitoreo Interno Estricto y Continuo:

- Implementar una vigilancia estrecha del tráfico interno utilizando herramientas de monitoreo de red y sistemas de detección de intrusiones.
- Establecer un monitoreo continuo y auditorías regulares para detectar y responder rápidamente a futuros incidentes.

8. Revisión de Configuraciones de Red:

- Verificar y ajustar las configuraciones de red para asegurar que no haya malconfiguraciones que puedan ser explotadas.
- Implementar segmentación de red para limitar el alcance de cualquier posible movimiento lateral de un atacante.

9. Capacitación en Seguridad:

- Proveer capacitación continua en seguridad a todo el personal para mejorar la concienciación sobre amenazas y respuestas adecuadas.

10. Simulaciones y Pruebas Regulares:

- Realizar simulaciones de ataques y pruebas de seguridad internas regularmente para identificar y corregir vulnerabilidades antes de que puedan ser explotadas por atacantes reales.

Estas medidas ayudarán a mitigar los riesgos asociados con este tipo de ataques y fortalecerán la postura de seguridad de la organización.

Firma: Sheila Fernández, Analista SOC N1, 26/06/2024

Anexos: Capturas de pantalla con los resultados del análisis de la IP

 0 / 93

No security vendor flagged this IP address as malicious

10.125.0.1 private

Last Analysis Date
1 month ago

Detection Details Relations Community

[Join our Community](#) and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Security vendors' analysis		Do you want to automate checks?		
0xSl_f33d	?	Unrated	?	Unrated
Acronis	?	Unrated	?	Unrated
AI Labs (MONITORAPP)	?	Unrated	?	Unrated
alphaMountain.ai	?	Unrated	?	Unrated
Antiy-AVL	?	Unrated	?	Unrated
AutoShun	?	Unrated	?	Unrated
Bfore.Ai PreCrime	?	Unrated	?	Unrated
Bkav	?	Unrated	?	Unrated
Certego	?	Unrated	?	Unrated
CINS Army	?	Unrated	?	Unrated
CMC Threat Intelligence	?	Unrated	?	Unrated
Criminal IP	?	Unrated	?	Unrated
Cyan	?	Unrated	?	Unrated
CyRadar	?	Unrated	?	Unrated
DNS8	?	Unrated	?	Unrated
EmergingThreats	?	Unrated	?	Unrated
Ermes	?	Unrated	?	Unrated
ESTsecurity	?	Unrated	?	Unrated
Fortinet	?	Unrated	?	Unrated
Google Safebrowsing	?	Unrated	?	Unrated
Gridinsoft	?	Unrated	?	Unrated
Hunt.io Intelligence	?	Unrated	?	Unrated

AbuseIPDB » 10.125.0.1

Check an IP Address, Domain Name, or Subnet
e.g. 37.222.61.117, microsoft.com, or 5.188.10.0/24

37.222.61.117

10.125.0.1 was not found in our database

Important Note: 10.125.0.1 is a private IP address, and is only used in internal network environments. Any abusive activity you see coming from an internal IP is either coming from within your network itself, or is the result of an error or misconfiguration.

With this in mind, we present the reports on this page for entertainment and testing purposes only. If you mistakenly blacklist an internal IP, you will not have a good day!

Tarea 3:

Imagina que trabajas en un SOC como analista de Nivel 1. Recibes una alerta en la que se describe el incidente que se muestra a continuación:

Alerts

FILE HASH: 311edf744...	HOST: equipo3	FIRST SEEN 10/06/24 12:58
 → 		LAST SEEN 10/06/24 12:58

Description – Malicious Binary

- **Hostname:** equipo3
- **Host IP:** 10.57.24.131
- **OS Version:** Windows 11 x64
- **File Hash:**
311edf744c2e90d7bfc550c893478f43d1d7977694d5dcecf219795f3eb99b86

Realiza un pequeño informe basándote al menos en las siguientes cuestiones:

- Analiza esta alerta utilizando VirusTotal. ¿Se considera malicioso el hash?
- Tras analizar el hash, ¿ante qué tipo de malware estamos?
- ¿Para qué sistema operativo está hecho este malware?
- ¿A qué grupo criminal corresponde este malware?

En este caso he querido realizar los dos tipos de informes mencionados con anterioridad, un informe no técnico y otro técnico con un análisis mas detallado de los resultados obtenidos. Comenzaremos con el informe no técnico.

Informe de Incidente de Seguridad

SOC - Centro de Operaciones de Seguridad

Fecha: 26/06/2024

Analista: Sheila Fernández

Asunto: Informe de Incidente de Seguridad - Alerta de Malware

Descripción del Incidente

El día 10 de junio de 2024 a las 12:58 horas, se recibió una alerta en el Centro de Operaciones de Seguridad (SOC) indicando un posible incidente de seguridad en uno de los endpoints de la red. La alerta fue generada por las herramientas de monitoreo de seguridad y contenía la siguiente información:

- **Archivo Sospechoso:** VLC.exe
- **Hash del Archivo:**
311edf744c2e90d7bfc550c893478f43d1d7977694d5dcecf219795f3eb99b86
- **Host Afectado:** equipo3
- **IP del Host:** 10.57.24.131
- **Versión del Sistema Operativo:** Windows 11 x64

Análisis del Incidente

1. Identificación del Malware

El hash 311edf744c2e90d7bfc550c893478f43d1d7977694d5dcecf219795f3eb99b86 fue analizado utilizando VirusTotal, donde el archivo VLC.exe fue clasificado como malicioso por 67 de 74 motores antivirus.

2. Tipo de Malware:

- **Etiquetas de amenaza**
 - trojan.lockbit/blackmatter
- **Categorías de Amenaza**
 - **Troyano:** Malware que se disfrazza de software legítimo para engañar a los usuarios y obtener acceso no autorizado a sus sistemas.
 - **Ransomware:** Tipo de malware que cifra los archivos del usuario y demanda un rescate para restaurar el acceso a los datos.
- **Etiquetas de Familia**
 - **LockBit:** Familia de ransomware conocida por su capacidad de cifrar archivos y extorsionar a las víctimas mediante tácticas de doble extorsión.
 - **BlackMatter:** Grupo de ransomware que comparte características con LockBit y otros ransomware notables, enfocado en grandes organizaciones.
 - **Encoder:** Indica que el malware incluye capacidades de cifrado para bloquear el acceso a los archivos de las víctimas.

El análisis confirma que el archivo es una variante del **ransomware**. La mayoría de los motores antivirus lo han clasificado como **LockBit**, aunque algunos también lo asocian con **BlackMatter**. Ambos tipos de ransomware comparten características y métodos de operación similares, como el cifrado de archivos y la extorsión mediante amenazas de publicar datos robados.

3. Sistema Operativo Objetivo

El ransomware LockBit está diseñado específicamente para sistemas operativos **Windows**, en este caso, Windows 11 x64.

4. Grupo Criminal Asociado

El ransomware Lockbit ha sido vinculado principalmente al grupo criminal conocido como **LockBitSupp**. Sin embargo, la presencia de etiquetas que mencionan BlackMatter sugiere que podría haber conexiones o similitudes en el código o las tácticas utilizadas.

Características de LockBitSupp:

1. **Operaciones Profesionales:** Estructura organizativa profesional con soporte técnico y actualizaciones constantes.
2. **Enfoque en Grandes Objetivos:** Objetivos principales son grandes organizaciones e instituciones.

3. **Doble Extorsión:** Cifrado de archivos y exfiltración de datos con amenaza de publicación.
4. **Actualizaciones Constantes:** Mejoras continuas para evadir medidas de seguridad.

Conclusiones

El archivo VLC.exe identificado en el sistema equipo3 es una variante de ransomware que ha sido mayoritariamente identificado como LockBit, aunque con algunas referencias a BlackMatter. Esto indica que podría haber similitudes o evoluciones entre estos dos tipos de ransomware. LockBit es operado por el grupo criminal LockBitSupp, conocido por sus tácticas de doble extorsión y ataques a grandes organizaciones.

Recomendaciones

1. **Aislamiento del Sistema:** Aislar inmediatamente el sistema afectado para prevenir la propagación del ransomware.
2. **Análisis Forense:** Realizar un análisis forense completo del sistema comprometido para identificar el alcance de la infección y los vectores de ataque utilizados.
3. **Restauración de Datos:** Restaurar los sistemas y datos afectados desde copias de seguridad no comprometidas.
4. **Educación y Capacitación:** Capacitar al personal sobre cómo reconocer intentos de phishing y otras tácticas de ingeniería social que puedan llevar a infecciones de malware.
5. **Actualización de Sistemas:** Asegurar que todos los sistemas y software estén actualizados con los últimos parches de seguridad para mitigar vulnerabilidades que puedan ser explotadas por el ransomware.
6. **Implementación de Soluciones de Seguridad:** Utilizar herramientas avanzadas de detección y respuesta ante amenazas (EDR) para monitorear y mitigar actividades sospechosas en tiempo real.

Firma: Sheila Fernández, Analista SOC N1, 26/06/2024

Informe Técnico de Incidente de Seguridad

SOC - Centro de Operaciones de Seguridad

Fecha: 26/06/2024

Analista: Sheila Fernández

Asunto: Informe de Incidente de Seguridad – Alerta de Malware

Descripción del Incidente

El día 10 de junio de 2024 a las 12:58 horas, se recibió una alerta en el Centro de Operaciones de Seguridad (SOC) indicando un posible incidente de seguridad en uno de los sistemas de la red. La alerta fue generada por las herramientas de monitoreo de seguridad y contenía la siguiente información:

- **Archivo Sospechoso:** VLC.exe
- **Hash del Archivo:**
311edf744c2e90d7bfc550c893478f43d1d7977694d5dcecf219795f3eb99b86
- **Host Afectado:** equipo3
- **IP del Host:** 10.57.24.131
- **Versión del Sistema Operativo:** Windows 11 x64

Análisis del Incidente

1. Identificación del Malware

El hash 311edf744c2e90d7bfc550c893478f43d1d7977694d5dcecf219795f3eb99b86 fue analizado utilizando VirusTotal. Los resultados muestran que el archivo VLC.exe es considerado malicioso por 67 de 74 motores antivirus.

2. Tipo de Malware:

- **Etiquetas de amenaza**

- trojan.lockbit/blackmatter
- **Categorías de Amenaza**
 - **Troyano:** Malware que se disfrazza de software legítimo para engañar a los usuarios y obtener acceso no autorizado a sus sistemas.
 - **Ransomware:** Tipo de malware que cifra los archivos del usuario y demanda un rescate para restaurar el acceso a los datos.
- **Etiquetas de Familia**
 - **LockBit:** Familia de ransomware conocida por su capacidad de cifrar archivos y extorsionar a las víctimas mediante tácticas de doble extorsión.
 - **BlackMatter:** Grupo de ransomware que comparte características con LockBit y otros ransomware notables, enfocado en grandes organizaciones.
 - **Encoder:** Indica que el malware incluye capacidades de cifrado para bloquear el acceso a los archivos de las víctimas.

El análisis confirma que el archivo es una variante del **ransomware**. La mayoría de los motores antivirus lo han clasificado como **LockBit**, aunque algunos también lo asocian con **BlackMatter**. Ambos tipos de ransomware comparten características y métodos de operación similares, como el cifrado de archivos y la extorsión mediante amenazas de publicar datos robados.

3. Detalles Técnicos del Análisis

Análisis de VirusTotal

- **Detección:** 67/74 motores antivirus consideran el archivo como malicioso.
- **Tipo de archivo:** PE32 executable (GUI) Intel 80386, for MS Windows.
- **Tamaño:** 145.00 KB.
- **Fecha de Compilación:** 2022-09-13 23:30:57 UTC.
- **Tags:** ransomware, trojan, lockbit, blackmatter.

Análisis de Comportamiento

- **Comportamientos Detectados:**
 - **peexe:** Indica que el archivo analizado es un ejecutable Portable Executable (PE), comúnmente utilizado en sistemas operativos Windows.

- **detect-debug-environment:** Detecta si está siendo ejecutado en un entorno de depuración o análisis. Los atacantes a menudo implementan estas comprobaciones para evadir los análisis automatizados y evitar ser detectados por los investigadores de seguridad.
 - **calls-wmi:** El archivo utiliza Windows Management Instrumentation (WMI) para interactuar con el sistema operativo. WMI se puede usar para recolectar información del sistema, ejecutar comandos o scripts, y realizar tareas administrativas, lo que puede ser malicioso si es usado por malware.
 - **check-user-input:** Monitorea la entrada del usuario. Esto podría ser un intento de registrar pulsaciones de teclas, movimientos del ratón o interacciones con el sistema para robar credenciales u otra información sensible.
 - **long-sleeps:** Realiza largos periodos de espera para evadir análisis automatizados. Esta técnica se usa para evadir la detección por parte de soluciones de seguridad, ya que los análisis automatizados suelen tener un límite de tiempo para determinar si un archivo es malicioso.
- **Sandbox Detections:**
 - **Zenbox:** Clasificado como Malware Stealer Ransom Trojan.
 - **VMRay:** Clasificado simplemente como Malware.

Tácticas y Técnicas MITRE ATT&CK

1. Ejecución (Execution) - TA0002

- **Windows Management Instrumentation (T1047):** l.exe ejecuta una consulta WMI.
- **Command and Scripting Interpreter (T1059):** Acepta argumentos de la línea de comandos.
- **Shared Modules (T1129):** El proceso intenta cargar funciones dinámicamente.

2. Persistencia (Persistence) - TA0003

- **Create or Modify System Process (T1543):** Creación o modificación de procesos a nivel de sistema para ejecutar cargas útiles maliciosas repetidamente.
- **Windows Service (T1543.003):** Creación o modificación de servicios de Windows para persistencia.
- **DLL Side-Loading (T1574.002):** Intenta cargar DLLs faltantes.

3. Escalada de Privilegios (Privilege Escalation) - TA0004

- **Create or Modify System Process (T1543):** Creación o modificación de procesos a nivel de sistema para ejecutar cargas útiles maliciosas repetidamente.

- **Windows Service (T1543.003)**: Creación o modificación de servicios de Windows para persistencia.
- **DLL Side-Loading (T1574.002)**: Intenta cargar DLLs faltantes.

4. Evasión de Defensa (Defense Evasion) - TA0005

- **Direct Volume Access (T1006)**: l.exe accede directamente al volumen "Z".
- **Obfuscated Files or Information (T1027)**: Codificación de datos usando XOR y Base64, cifrado con AES y RC4 KSA.
- **Masquerading (T1036)**: l.exe cambia la apariencia de carpetas.
- **Modify Registry (T1112)**: Añade entradas al registro de inicio de Windows.
- **Virtualization/Sandbox Evasion (T1497)**: Utiliza técnicas de sueño para evadir análisis dinámicos.
- **Impair Defenses (T1562)**: Modificación maliciosa de componentes defensivos del entorno.
- **Disable or Modify Tools (T1562.001)**: Modificación y/o desactivación de herramientas de seguridad.
- **DLL Side-Loading (T1574.002)**: Intenta cargar DLLs faltantes.

5. Acceso a Credenciales (Credential Access) - TA0006

- **OS Credential Dumping (T1003)**: Intenta recolectar información de navegadores (historial, contraseñas, etc.).
- **Input Capture (T1056)**: Crea un objeto DirectInput para capturar pulsaciones de teclas.

6. Descubrimiento (Discovery) - TA0007

- **Application Window Discovery (T1010)**: Monitorea cambios en ventanas de aplicaciones.
- **Query Registry (T1012)**: Interacción con el registro de Windows para recolectar información del sistema.
- **Process Discovery (T1057)**: Consulta la lista de procesos en ejecución.
- **System Information Discovery (T1082)**: Obtiene información detallada del sistema operativo y hardware.
- **File and Directory Discovery (T1083)**: Escribe archivos ini.
- **Virtualization/Sandbox Evasion (T1497)**: Utiliza técnicas de sueño para evadir análisis dinámicos.
- **Security Software Discovery (T1518.001)**: Intenta detectar máquinas virtuales.
- **System Location Discovery (T1614)**: Obtiene la ubicación geográfica del sistema.

7. Recolección (Collection) - TA0009

- **Data from Local System (T1005)**: Intenta recolectar información de navegadores (historial, contraseñas, etc.).

- **Input Capture (T1056):** Crea un objeto DirectInput para capturar pulsaciones de teclas.
- **Data Staged (T1074):** Los adversarios pueden almacenar datos recolectados en un directorio central antes de la exfiltración.

8. Comando y Control (Command and Control) - TA0011

- **Application Layer Protocol (T1071):** Los adversarios pueden comunicarse usando protocolos de capa de aplicación para evitar la detección.

9. Impacto (Impact) - TA0034

- **Data Destruction (T1485):** l.exe elimina múltiples archivos de usuario.
- **Data Encrypted for Impact (T1486):** Renombra 207 archivos añadiendo la extensión ".fihqnbxym" y modifica documentos de usuario.
- **Service Stop (T1489):** l.exe detiene el servicio Windows Security Center mediante la API ControlService.

10. Impacto (Impact) - TA0040

- **Data Destruction (T1485):** l.exe elimina múltiples archivos de usuario.
- **Data Encrypted for Impact (T1486):** Renombra 207 archivos añadiendo la extensión ".fihqnbxym" y modifica documentos de usuario.
- **Service Stop (T1489):** l.exe detiene el servicio Windows Security Center mediante la API ControlService.

Reglas Sigma Detectadas

Reglas Sigma: Son reglas de detección de amenazas escritas en un formato estandarizado (YAML) que identifican patrones sospechosos en los registros de eventos, compatibles con múltiples plataformas de SIEM.

1. **Windows Defender Service Disabled - Registry:**

- Detecta la desactivación del servicio Windows Defender a través del registro.

2. **Change WinEvt Channel Access Permission via Registry:**

- Detecta cambios en los permisos de acceso al canal de eventos de Windows.

3. **Suspicious desktop.ini Action:**

- Detecta accesos inusuales al archivo desktop.ini.

4. **Load of RstrtMgr DLL by an Uncommon Process:**

- Detecta la carga de la biblioteca RstrtMgr DLL por un proceso inusual.

Reglas IDS Detectadas

Reglas IDS: Son reglas específicas utilizadas por sistemas de detección de intrusos (IDS) para identificar y alertar sobre actividades anómalas o maliciosas en el tráfico de red, tales como escaneos de puertos o intentos de explotación.

- **UDP portscan:**
 - Intento de reconocimiento usando escaneo de puertos UDP.

Comunicación de Red

- **Solicitudes HTTP:**
 - <http://crt.sectigo.com/SectigoPublicCodeSigningCAR36.crt>
 - <http://crt.sectigo.com/SectigoPublicCodeSigningRootR46.p7c>
- **Resoluciones DNS:**
 - `_ldap._tcp.dc._msdcs.WIN-5E07COS9ALR`:
 - **Descripción:** Este es un registro de servicio DNS (SRV) utilizado en redes de Active Directory de Microsoft.
 - **Uso:** Indica un servicio LDAP (Lightweight Directory Access Protocol) que opera sobre TCP, y es utilizado para localizar controladores de dominio (DC) dentro de la infraestructura de Active Directory.
 - **Función:** Permite a los clientes de Active Directory encontrar y conectarse a controladores de dominio para autenticación y otros servicios relacionados.
 - `www.microsoft.com`
 - **Descripción:** Este es un dominio ampliamente conocido que apunta al sitio web oficial de Microsoft.
 - **Uso:** Utilizado por navegadores web y otros servicios de red para acceder al contenido y servicios proporcionados por Microsoft.
 - **Función:** Resolver este dominio permite a los usuarios y servicios acceder a la página principal de Microsoft y sus recursos asociados.
 - `crt.sectigo.com`
 - **Descripción:** Este dominio pertenece a Sectigo, una Autoridad de Certificación (CA) que emite certificados digitales.
 - **Uso:** Utilizado por servicios y aplicaciones para verificar y obtener certificados digitales, cruciales para establecer comunicaciones seguras mediante HTTPS y otros protocolos.

- **Función:** La resolución de este dominio permite la validación de certificados digitales para asegurar la comunicación en línea.
 - tsel.mm.bing.net
 - **Descripción:** Este dominio está asociado con Bing, el motor de búsqueda de Microsoft.
 - **Uso:** Utilizado para la carga de imágenes y otros contenidos multimedia en los resultados de búsqueda de Bing.
 - **Función:** La resolución de este dominio permite que los resultados de búsqueda de Bing muestren contenido visual relevante.
- **Tráfico IP:**
 - Varias conexiones TCP y UDP a direcciones IP relacionadas con microsoft.com y otras redes.

Actividades del Sistema de Archivos

1. **Archivos Caídos:**
 - Varias instancias de archivos sospechosos con extensiones .fihqnbxym y .FihqnBxYm.
2. **Acciones del Registro:**
 - Modificaciones en claves del registro bajo HKEY_CLASSES_ROOT, HKEY_CURRENT_USER, y HKEY_LOCAL_MACHINE. Algunas eliminadas, otras abiertas.
3. **Procesos y Servicios:**
 - **Procesos Creados:** procesos creados como:
 - C:\Users\<USER>\AppData\Local\Temp\L.exe
 - C:\Windows\system32\services.exe
 - C:\Windows\system32\svchost.exe -k DcomLaunch -p
 - **Comandos de Shell:** Ejecución de varios comandos de shell para iniciar procesos maliciosos.
 - **Procesos Inyectados:** Inyección en procesos como VLC.exe y ShellExperienceHost.exe.
 - **Servicios Abiertos y Eliminados:** Manipulación de servicios como WinDefend, sppsvc, vss, wscsvc.
4. **Árbol de Procesos:**

- Relación entre varios procesos creados e injectados, indicando cómo el malware se extiende y manipula el sistema.

5. Mutexes y Señales:

- Creación de mutexes para evitar múltiples instancias del malware.

6. Módulos Cargados:

- Módulos en tiempo de ejecución necesarios para las operaciones del malware.

7. Consultas de Propiedades del Sistema:

- Consultas WMI para obtener información del sistema.

Conclusiones

El archivo VLC.exe identificado en el sistema “equipo3” es una variante del ransomware que ha sido mayoritariamente identificado como **LockBit**, aunque algunos motores antivirus también lo asocian con **BlackMatter**. Esto sugiere que podría haber similitudes o evoluciones entre estos dos tipos de ransomware. LockBit es operado por el grupo criminal **LockBitSupp**, conocido por sus tácticas de doble extorsión y ataques a grandes organizaciones.

Recomendaciones

1. **Aislamiento del Sistema:** Aislar inmediatamente el sistema afectado para prevenir la propagación del ransomware.
2. **Análisis Forense:** Realizar un análisis forense completo del sistema comprometido para identificar el alcance de la infección y los vectores de ataque utilizados.
3. **Restauración de Datos:** Restaurar los sistemas y datos afectados desde copias de seguridad no comprometidas.
4. **Educación y Capacitación:** Capacitar al personal sobre cómo reconocer intentos de phishing y otras tácticas de ingeniería social que puedan llevar a infecciones de malware.
5. **Actualización de Sistemas:** Asegurar que todos los sistemas y software estén actualizados con los últimos parches de seguridad para mitigar vulnerabilidades que puedan ser explotadas por el ransomware.
6. **Implementación de Soluciones de Seguridad:** Utilizar herramientas avanzadas de detección y respuesta ante amenazas (EDR) para monitorear y mitigar actividades sospechosas en tiempo real.

Firma: Sheila Fernández, Analista SOC N1, 26/06/2024

Anexo: Capturas de pantalla de los resultados de VirusTotal.

67 / 74

67/74 security vendors and 2 sandboxes flagged this file as malicious

311edf744c2e90d7bfc550c893478f43d1d7977694d5dcef219795f3eb99b86

VLC.exe

Community Score

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 13+

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Popular threat label: trojan.lockbit/blackmatter

Threat categories: trojan, ransomware

Family labels: lockbit, blackmatter, encoder

Security vendors' analysis

Vendor	Analysis	Vendor	Analysis
Acronis (Static ML)	Suspicious	AhnLab-V3	Ransomware/Win.LockBit.R521581
Alibaba	Ransom:Win32/Lockbit.7c048ed6	AliCloud	RansomWare:Win/Lockbit.x1glab
ALYac	Trojan.Ransom.LockBit	Antiy-AVL	Trojan[Ransom]/Win32.LockBit.ha
Arcabit	Trojan.Generic.D4592DEB	Avast	Win32:RansomX-gen [Ransom]
Avert Labs	BlackMatter!76B23DD72A88	AVG	Win32:RansomX-gen [Ransom]
Avira (no cloud)	BDS/ZeroAccess.Gen7	BitDefender	Trojan.GenericKD.72953323
BitDefenderTheta	AI-Packer.15A5CA4A1E	Bkav Pro	W32.AIDetectMalware
ClamAV	Win.Ransomware.BlackMatter-9970818-0	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Cybereason	Malicious.72a883	Cylance	Unsafe

Cynet	 ⓘ Malicious [score: 100]	DeepInstinct	 ⓘ MALICIOUS
DrWeb	 ⓘ Trojan.Encoder.31074	Elastic	 ⓘ Windows.Ransomware.Lockbit
Emsisoft	 ⓘ Trojan.GenericKD.72953323 (B)	eScan	 ⓘ Trojan.GenericKD.72953323
ESET-NOD32	 ⓘ A Variant Of Win32/Filecoder.BlackMatte...	Fortinet	 ⓘ W32/Conwise.RCE!tr
GData	 ⓘ Trojan.GenericKD.72953323	Google	 ⓘ Detected
Gridinsoft (no cloud)	 ⓘ Ransom.Win32.Alols1	Ikarus	 ⓘ Trojan-Ransom.LockBit
Jiangmin	 ⓘ Trojan.Generic.hmvpt	K7AntiVirus	 ⓘ Trojan (0059b9cd1)
K7GW	 ⓘ Trojan (0059b9cd1)	Kaspersky	 ⓘ UDS:Trojan-Ransom.Win32.Generic
Kingsoft	 ⓘ Win32.Trojan-Ransom.Generic.a	Lionic	 ⓘ Trojan.Win32.Lockbit.tsvY
Malwarebytes	 ⓘ Generic.Malware.AI.DDS	MAX	 ⓘ Malware (ai Score=89)
MaxSecure	 ⓘ Trojan.Malware.10307848.susgen	McAfee Scanner	 ⓘ Real Protect-LS!76B23DD72A88
Microsoft	 ⓘ Ransom:Win32/Lockbit.RPA!MTB	NANO-Antivirus	 ⓘ Trojan.Win32.Encoder.jtarpu
Palo Alto Networks	 ⓘ Generic.ml	Panda	 ⓘ Trj/Genetic.gen
QuickHeal	 ⓘ Ransom.Lockbit.S29768538	Rising	 ⓘ Ransom.LockBit!1.DFDC (CLASSIC)
Sangfor Engine Zero	 ⓘ Ransom.Win32.Save.LockBit30	SecureAge	 ⓘ Malicious
SentinelOne (Static ML)	 ⓘ Static AI - Malicious PE	Skyhigh (SWG)	 ⓘ BehavesLike.Win32.BlackMatter.cc
Sophos	 ⓘ Mal/EncPk-HM	Symantec	 ⓘ Ransom.Lockbit!g6
Tencent	 ⓘ Trojan-Ransom.Win32.Crypmodng.gz	Trapmine	 ⓘ Malicious.moderate.ml.score
Trellix (FireEye)	 ⓘ Generic.mg.76b23dd72a883d8b	TrendMicro	 ⓘ Ransom.Win32.LOCKBIT.SMYXCJN
Varist	 ⓘ W32/Trojan.DPTH-0027	VBA32	 ⓘ Trojan.Encoder
VIPRE	 ⓘ Trojan.GenericKD.72953323	ViRobot	 ⓘ Trojan.Win32.LockBit.157184.A
Webroot	 ⓘ W32.Ransom.Lockbit	WithSecure	 ⓘ Backdoor.BDS/ZeroAccess.Gen7
Xcitium	 ⓘ Malware@#dr7o0ycvnb	Yandex	 ⓘ Trojan.Filecoder!HJuVfCjCHY
Zillya	 ⓘ Trojan.Filecoder.Win32.26935	ZoneAlarm by Check Point	 ⓘ HEUR:Trojan-Ransom.Win32.Generic
Baidu	 ✓ Undetected	CMC	 ✓ Undetected
SUPERAntiSpyware	 ✓ Undetected	TACHYON	 ✓ Undetected
TEHTRIS	 ✓ Undetected	TrendMicro-HouseCall	 ✓ Undetected
Zoner	 ✓ Undetected	Avast-Mobile	 ⚠ Unable to process file type
BitDefenderFalx	 ⚠ Unable to process file type	Symantec Mobile Insight	 ⚠ Unable to process file type
Trustlook	 ⚠ Unable to process file type	ViriT	—

67 / 74

67/74 security vendors and 2 sandboxes flagged this file as malicious

311edf744c2e90d7bfc550c893478f43d1d7977694d5dcecf219795f3eb99b86
VLC.exe

Community Score: 67 / 74

Size: 145.00 KB | Last Modification Date: 37 minutes ago | EXE

peexe long-sleeps calls-wmi detect-debug-environment checks-user-input

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 13+

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Basic properties

MD5	76b23dd72a883d8b1302bb4a514b7967
SHA-1	338e19e8a3615c29d8a25ebbba66cf5fa0caa2c
SHA-256	311edf744c2e90d7bfc550c893478f43d1d7977694d5dcecf219795f3eb99b86
Vhash	01506666151d7d6567za1z8n27f
Authentihash	f3fc0e59afa08279a168fb950bf29631e74bbeefc8fb62519a53daca3e7c
ImpHash	914685b69f2ac2ff61b6b0f1883a054d
SSDeep	1536:a1zCSAAawczUU8y8gvM+1zGSNAojMP95D1xDtCYU0GsvgtwjECrozUVj3PeAU2:pqJogYkcSNm9V7DtCCGsg+AmYlQhTT
TLSH	T18CE36C21E15EDB3C47718F12726B17DB3EA4D2C0A57847EA40F88BCA59232F4595F
File type	Win32 EXE executable windows win32 pe peexe
Magic	PE32 executable (GUI) Intel 80386, for MS Windows
TrID	Win32 Dynamic Link Library (generic) (25%) Win16 NE executable (generic) (19.1%) Win32 Executable (generic) (17.1%) Win16/32 Executable Delphi generic (7.8%)
Magika	PEBIM
File size	145.00 KB (148480 bytes)

History

Creation Time	2022-09-13 23:30:57 UTC
First Seen In The Wild	2024-05-30 09:21:48 UTC
First Submission	2024-05-29 18:22:29 UTC
Last Submission	2024-06-26 10:05:26 UTC
Last Analysis	2024-06-26 06:22:48 UTC

Names

- VLC.exe
- 311edf744c2e90d7bfc550c893478f43d1d7977694d5dcecf219795f3eb99b86.exe
- phdays.exe
- unknown
- l2.exe
- 2024-05-30_76b23dd72a883d8b1302bb4a514b7967_darkside
- l.exe

Portable Executable Info

Header

Target Machine	Intel 386 or later processors and compatible processors
Compilation Timestamp	2022-09-13 23:30:57 UTC
Entry Point	103535
Contained Sections	6

Sections

Name	Virtual Address	Virtual Size	Raw Size	Entropy	MD5	Chi2
.text	4096	97606	97792	6.61	57ad8095d0d1b2e0663fb3e4405410	616326.06
.text	102400	1385	1536	3.04	0adcc204eb91a7bbe4f95ec65202fe1	161672.45
.rdata	106496	1202	1536	3.66	9264ea7f335858b063b39397d3c51d14	111585.08
.data	110592	44488	40960	7.99	b4988b41cbd71279421d9a56ca7b755	958.1
.pdata	155648	1157	1536	6.67	9758f9fdb118c688711e859a91d23cb	23995.56

Imports

- + gdi32.dll
- + USER32.dll
- + KERNEL32.dll

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 13+

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Contacted URLs (2) ⓘ

Scanned	Detections	Status	URL
2024-06-24	0 / 95	200	http://crt.sectigo.com/SectigoPublicCodeSigningCAR36.crt
2024-06-24	0 / 95	200	http://crt.sectigo.com/SectigoPublicCodeSigningRootR46.p7c

Contacted Domains (4) ⓘ

Domain	Detections	Created	Registrar
crt.sectigo.com	0 / 93	2018-08-16	CSC CORPORATE DOMAINS, INC.
sectigo.com	0 / 93	2018-08-16	CSC CORPORATE DOMAINS, INC.
tsel.mm.bing.net	0 / 93	1997-09-03	MarkMonitor Inc.
www.microsoft.com	0 / 93	1991-05-02	MarkMonitor Inc.

Contacted IP addresses (13) ⓘ

IP	Detections	Autonomous System	Country
13.107.21.200	0 / 93	8068	US
131.253.33.203	0 / 93	8068	US
172.64.149.23	0 / 93	13335	-
192.168.0.17	0 / 93	-	-
192.168.0.32	0 / 93	-	-
192.168.0.67	0 / 93	-	-
192.168.0.78	0 / 93	-	-
20.99.133.109	1 / 93	8075	US
20.99.186.246	0 / 93	8075	US
204.79.197.200	1 / 93	8068	US

• • •

Bundled Files (6) ⓘ

Scanned	Detections	File type	Name
✓ ?	?	file	5f8f6e8fbf6a80d1bc3f9acd19372dca3bcd9f8c8c60f359c2107a45c7e63402
✓ ?	?	file	5e790d86f546811d97dd84b978e903770e14d2106995fb113a1242f12b3b227
✓ ?	?	file	8226ed51e189c255710066c6d7621c034ff5fdb4856de20025a51e642dc73f7
✓ ?	?	file	e29dd4a54c97e59786cb0c5cf1d1d77b234d10bedf88a34ae39c68a9f96c737c
✓ ?	?	file	fed988545b8fa9d1c0be54c86eb1b10d693229fb132f86057bdd67f6e8ceec60
✓ ?	?	file	3f79e113d906307d34b22bf154cf45b283881fb5b57106c7561ed8ee8a64f1142

Dropped Files (462) ⓘ

Scanned	Detections	File type	Name
✓ 2024-05-29	0 / 64	PGP Security Key	decoder.py.FihqnBxYm
✓ 2024-05-29	0 / 64	PGP Security Key	widenvinecdm.dll.sig.FihqnBxYm
✓ 2024-05-29	0 / 64	DOS EXE	test_copy.py.FihqnBxYm
✓ 2024-05-29	0 / 64	DOS EXE	fields_cpython-39.pyc.FihqnBxYm
✓ 2024-05-29	0 / 64	DOS EXE	req_set.py.FihqnBxYm
✓ 2024-05-29	0 / 63	PGP Security Key	test_gzip.py.FihqnBxYm
✓ 2024-05-29	0 / 64	DOS EXE	METADATA.FihqnBxYm
✓ 2024-05-29	0 / 63	DOS EXE	Guernsey.FihqnBxYm
✓ 2024-05-29	0 / 64	DOS EXE	test_ioctl.py.FihqnBxYm
✓ 2024-06-18	1 / 64	ICO	3R9qG8i3Z.ico

• • •

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 13+

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Display grouped sandbox reports

<input checked="" type="checkbox"/> C2AE	△ 0 M 0 W 0 E 0 D 0 P 0	<input checked="" type="checkbox"/> CAPA	△ 0 M 3 W 0 E 0 D 0 P 0
<input checked="" type="checkbox"/> CAPE Sandbox	△ 0 M 8 W 0 E 1 D 11 P 0	<input checked="" type="checkbox"/> Microsoft Sysinternals	△ 0 M 0 W 0 E 2 D 12 P 12
<input checked="" type="checkbox"/> VMRay	△ 1 M 4 W 0 E 1 D 99+ P 0	<input checked="" type="checkbox"/> VirusTotal Jujubox	△ 0 M 0 W 0 E 0 D 1 P 0
<input checked="" type="checkbox"/> Yomi Hunter	△ 0 M 1 W 1 E 0 D 1 P 3	<input checked="" type="checkbox"/> Zenbox	△ 4 M 8 W 0 E 1 D 99+ P 1

Activity Summary Download Artifacts ▾ Full Reports ▾ Help ▾

4 Detections 2 MALWARE 1 STEALER 1 RANSOM 1 TROJAN

Mitre Signatures 6 HIGH 4 LOW 24 INFO

IDS Rules 1 MEDIUM

Sigma Rules 2 HIGH 1 MEDIUM 1 LOW

Dropped Files 460 OTHER 1 DOS.COM 1 ICO 1 PE_EXE 1 CAB 1 COFF

Network comms 2 HTTP 4 DNS 10 IP

Activity Summary Download Artifacts ▾ Full Reports ▾ Help ▾

Behavior Tags calls-wmi checks-user-input detect-debug-environment long-sleeps

Dynamic Analysis Sandbox Detections ▾

- The sandbox Zenbox flags this file as: MALWARE STEALER RANSOM TROJAN
- The sandbox VMRay flags this file as: MALWARE

MITRE ATT&CK Tactics and Techniques ▾

- + Execution TA0002
- + Persistence TA0003
- + Privilege Escalation TA0004
- + Defense Evasion TA0005
- + Credential Access TA0006
- + Discovery TA0007
- + Collection TA0009
- + Command and Control TA0011
- + Impact TA0034
- + Impact TA0040

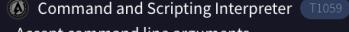
MITRE ATT&CK Tactics and Techniques

— Execution TA0002



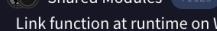
Windows Management Instrumentation T1047

(Process #1) .exe executes WMI query:



Command and Scripting Interpreter T1059

Accept command line arguments

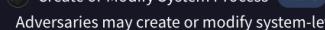


Shared Modules T1129

Link function at runtime on Windows

The process tried to load dynamically one or more functions.

— Persistence TA0003



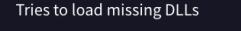
Create or Modify System Process T1543

Adversaries may create or modify system-level processes to repeatedly execute malicious payloads as part of persistence.



Windows Service T1543.003

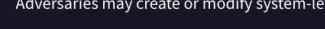
Adversaries may create or modify Windows services to repeatedly execute malicious payloads as part of persistence.



DLL Side-Loading T1574.002

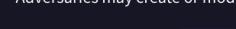
Tries to load missing DLLs

— Privilege Escalation TA0004



Create or Modify System Process T1543

Adversaries may create or modify system-level processes to repeatedly execute malicious payloads as part of persistence.



Windows Service T1543.003

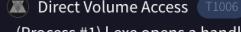
Adversaries may create or modify Windows services to repeatedly execute malicious payloads as part of persistence.



DLL Side-Loading T1574.002

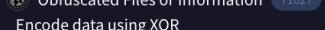
Tries to load missing DLLs

— Defense Evasion TA0005



Direct Volume Access T1006

(Process #1) .exe opens a handle to directly access the volume "Z".



Obfuscated Files or Information T1027

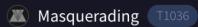
Encode data using XOR

Encode data using Base64

Reference AES constants

Encrypt data using AES

Encrypt data using RC4 KSA



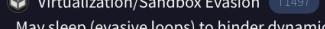
Masquerading T1036

(Process #1) .exe changes the appearance of folder "C:\\$Recycle.Bin\S-1-5-21-245394380-2276627025-4024548581-1000".



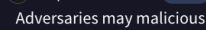
Modify Registry T1112

(Process #1) .exe adds "O:BAG:SYD:(A;;0x1;;;SY)(A;;0x5;;;BA)(A;;0x1;;;LA)" to Windows startup via registry.



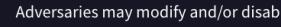
Virtualization/Sandbox Evasion T1497

May sleep (evasive loops) to hinder dynamic analysis



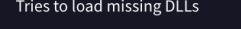
Impair Defenses T1562

Adversaries may maliciously modify components of a victim environment in order to hinder or disable defensive mechanisms.



Disable or Modify Tools T1562.001

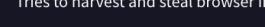
Adversaries may modify and/or disable security tools to avoid possible detection of their malware/tools and activities.



DLL Side-Loading T1574.002

Tries to load missing DLLs

— Credential Access TA0006



OS Credential Dumping T1003

Tries to harvest and steal browser information (history, passwords, etc)



Input Capture T1056

Creates a DirectInput object (often for capturing keystrokes)

— Discovery TA0007	
⌚ Application Window Discovery T1010	Sample monitors Window changes (e.g. starting applications), analyze the sample with the simulation cookbook
⌚ Query Registry T1012	Adversaries may interact with the Windows Registry to gather information about the system, configuration, and installed software.
⌚ Process Discovery T1057	Queries a list of all running processes
⌚ System Information Discovery T1082	Reads software policies An adversary may attempt to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture.
⌚ File and Directory Discovery T1083	Writes ini files
⌚ Virtualization/Sandbox Evasion T1497	May sleep (evasive loops) to hinder dynamic analysis
⌚ Security Software Discovery T1518.001	May try to detect the virtual machine to hinder analysis (VM artifact strings found in memory)
⚠ System Location Discovery T1614	Get geographical location
— Collection TA0009	
⌚ Data from Local System T1005	Tries to harvest and steal browser information (history, passwords, etc)
⌚ Input Capture T1056	Creates a DirectInput object (often for capturing keystrokes)
⌚ Data Staged T1074	Adversaries may stage collected data in a central location or directory prior to Exfiltration.
— Command and Control TA0011	
⌚ Application Layer Protocol T1071	Adversaries may communicate using application layer protocols to avoid detection/network filtering by blending in with existing traffic.

— Impact TA0034	
💣 Data Destruction T1485	⚠ (Process #1).exe deletes multiple user files.
💣 Data Encrypted for Impact T1486	⚠ Renames 207 files by appending the extension ".fihqnbxym". Modifies user documents (likely ransomware behavior)
💣 Service Stop T1489	⚠ (Process #1).exe stops Windows Security Center service by ControlService API. Adversaries may stop or disable services on a system to render those services unavailable to legitimate users.
— Impact TA0040	
💣 Data Destruction T1485	⚠ (Process #1).exe deletes multiple user files.
💣 Data Encrypted for Impact T1486	⚠ Renames 207 files by appending the extension ".fihqnbxym". Modifies user documents (likely ransomware behavior)
💣 Service Stop T1489	⚠ (Process #1).exe stops Windows Security Center service by ControlService API. Adversaries may stop or disable services on a system to render those services unavailable to legitimate users.

Activity Summary

Download Artifacts ▾ Full Reports ▾ Help ▾

Malware Behavior Catalog Tree

- + Anti-Behavioral Analysis OB0001
- + Anti-Static Analysis OB0002
- + Defense Evasion OB0006
- + Discovery OB0007
- + Execution OB0009
- + Persistence OB0012
- + Privilege Escalation OB0013
- + File System OC0001
- + Data OC0004
- + Cryptography OC0005
- + Communication OC0006
- + Operating System OC0008

Capabilities ▽

- + Linking
- + Data-Manipulation
- + Host-Interaction
- + Anti-Analysis
- + Load-Code
- + Collection

Crowdsourced Sigma Rules ▽

CRITICAL 0 HIGH 2 MEDIUM 1 LOW 1

- ⚠️ 🗃 Matches rule Windows Defender Service Disabled - Registry by Ján Trenčanský, frack113, AlertIQ, Nasreddine Bencherchali at Sigma Integrated Rule Set (GitHub)
 - ↳ Detects when an attacker or tool disables the Windows Defender service (WinDefend) via the registry
- ⚠️ 📁 Matches rule Change Winevt Channel Access Permission Via Registry by frack113 at Sigma Integrated Rule Set (GitHub)
 - ↳ Detects tampering with the "ChannelAccess" registry key in order to change access to Windows event channel.
- ⚠️ 🖥️ Matches rule Suspicious desktop.ini Action by Maxime Thiebaut (@0xThiebaut), Tim Shelton (HAWK.IO) at Sigma Integrated Rule Set (GitHub)
 - ↳ Detects unusual processes accessing desktop.ini, which can be leveraged to alter how Explorer displays a folder's content (i.e. renaming files) without changing them on disk.
- ⚠️ 🚨 Matches rule Load Of RstrMgr.DLL By An Uncommon Process by Luc Génaux at Sigma Integrated Rule Set (GitHub)
 - ↳ Detects the load of RstrMgr.DLL (Restart Manager) by an uncommon process. This library has been used during ransomware campaigns to kill processes that would prevent file encryption by locking them (e.g. Conti ransomware, Cactus ransomware). It has also recently been seen used by the BiBi wiper for Windows. It could also be used for anti-analysis purposes by shutting down specific processes.

Crowdsourced IDS rules ▽

- ⚠️ 📡 Matches rule (port_scan) UDP portsweep at Snort registered user ruleset
 - ↳ attempted-recon

Network Communication ▽

HTTP Requests

- + 🌐 GET http://crt.sectigo.com/SectigoPublicCodeSigningCAR36.crt 200
- + 🌐 GET http://crt.sectigo.com/SectigoPublicCodeSigningRootR46.p7c 200

DNS Resolutions

- _ldap_tcp_dc_msdcWIN-5E07COS9ALR
- + www.microsoft.com
- + crt.sectigo.com
- + tsel.mm.bing.net

IP Traffic

- TCP 20.99.133.109:443
- TCP 23.216.8.1.152:80 (www.microsoft.com)
- UDP a83f8110:3208:78d90c3:39b8:8f80:ffff:53
- UDP 192.168.0.17:137
- TCP 131.253.33.203:80
- UDP 192.168.0.78:137
- UDP 192.168.0.67:137
- TCP 20.99.186.246:443
- UDP a83f8110:0:0:1400:0:0:0:53
- UDP 192.168.0.32:137

Memory Pattern Domains

- docs.python.org
- imp.mt48.net
- mail.python.org
- mozillaclampxdirect.com
- www.nike.com
- www.underarmour.com
- www2.hursley.ibm.com

Memory Pattern URLs

- http://mail.python.org/pipermail/idle-dev/2004-December/002307.html
- http://www2.hursley.ibm.com/decimal
- https://docs.python.org/
- https://docs.python.org/3/bugs.html
- https://docs.python.org/3/library/idle.html
- https://imp.mt48.net/static?v=2&partner=firefox_cla&sub1=nike&sub2=us&adv-id=74521&custom-data=2954
- https://imp.mt48.net/static?v=2&partner=firefox_cla&sub1=nike&sub2=us&adv-id=74521&custom-data=2955
- https://imp.mt48.net/static?v=2&partner=firefox_cla&sub1=nike&sub2=us&adv-id=74521&custom-data=2956
- https://imp.mt48.net/static?v=2&partner=firefox_cla&sub1=nike&sub2=us&adv-id=74521&custom-data=2957
- https://imp.mt48.net/static?v=2&partner=firefox_cla&sub1=nike&sub2=us&adv-id=74521&custom-data=2959

▼

Behavior Similarity Hashes

C2AE	53878ae7c240c652e087120bf0c44d20
CAPA	f29d7cd77f34d687a9acd726b4055fdf
CAPE Sandbox	1c308dd62d588c70ebef64b2e1db99fc
Microsoft Sysinternals	9b1f57f55f3340677306015e27d17670
VirusTotal Jujubox	6fc7e20bc0163ad91f641ee388db23c
VMRay	449159b5dc7a0f825f4be8f4790cd6cb
Yomi Hunter	978748c2175ddb54ef24f114248db84b
Zenbox	f5ba99e7ee2f89a3e9195ff042a1a5ca

File system actions ⓘ

Files Opened

- ⌚ C:\\$Recycle.Bin\S-1-5-18\AAAAAAAAAAA
- ⌚ C:\\$Recycle.Bin\S-1-5-18\BBBBBBBBBBB
- ⌚ C:\\$Recycle.Bin\S-1-5-18\CCCCCCCCCCC
- ⌚ C:\\$Recycle.Bin\S-1-5-18\DDDDDDDDDD
- ⌚ C:\\$Recycle.Bin\S-1-5-18\EEEEEEEEE
- ⌚ C:\\$Recycle.Bin\S-1-5-18\FFFFFFFFF
- ⌚ C:\\$Recycle.Bin\S-1-5-18\GGGGGGGGGGG
- ⌚ C:\\$Recycle.Bin\S-1-5-18\HHHHHHHHHHH
- ⌚ C:\\$Recycle.Bin\S-1-5-18\IIIIIIIII
- ⌚ C:\\$Recycle.Bin\S-1-5-18\JJJJJJJJJJ

⌄

Files Written

- ⌚ C:\\$Recycle.Bin\S-1-5-18\AAAAAAAAAAA
- ⌚ C:\\$Recycle.Bin\S-1-5-18\BBBBBBBBBBB
- ⌚ C:\\$Recycle.Bin\S-1-5-18\CCCCCCCCCCC
- ⌚ C:\\$Recycle.Bin\S-1-5-18\DDDDDDDDDD
- ⌚ C:\\$Recycle.Bin\S-1-5-18\EEEEEEEEE
- ⌚ C:\\$Recycle.Bin\S-1-5-18\FFFFFFFFF
- ⌚ C:\\$Recycle.Bin\S-1-5-18\GGGGGGGGGGG
- ⌚ C:\\$Recycle.Bin\S-1-5-18\HHHHHHHHHHH
- ⌚ C:\\$Recycle.Bin\S-1-5-18\IIIIIIIII
- ⌚ C:\\$Recycle.Bin\S-1-5-18\JJJJJJJJJJ

⌄

Files Deleted

- ⌚ C:\\$Recycle.Bin\S-1-5-18\AAAAAAAAAAA
- ⌚ C:\\$Recycle.Bin\S-1-5-18\BBBBBBBBBBB
- ⌚ C:\\$Recycle.Bin\S-1-5-18\CCCCCCCCCCC
- ⌚ C:\\$Recycle.Bin\S-1-5-18\DDDDDDDDDD
- ⌚ C:\\$Recycle.Bin\S-1-5-18\EEEEEEEEE
- ⌚ C:\\$Recycle.Bin\S-1-5-18\FFFFFFFFF
- ⌚ C:\\$Recycle.Bin\S-1-5-18\GGGGGGGGGGG
- ⌚ C:\\$Recycle.Bin\S-1-5-18\HHHHHHHHHHH
- ⌚ C:\\$Recycle.Bin\S-1-5-18\IIIIIIIII
- ⌚ C:\\$Recycle.Bin\S-1-5-18\JJJJJJJJJJ

⌄

Files Copied

- + ⌚ ?(C:\Users\<USER>\AppData\Roaming\Mozilla\Firefox\Profiles\drb6pwbu.default-release\ExperimentStoreData.json
- + ⌚ ?(C:\Users\<USER>\AppData\Roaming\Mozilla\Firefox\Profiles\drb6pwbu.default-release\SiteSecurityServiceState.txt
- + ⌚ ?(C:\Users\<USER>\AppData\Roaming\Mozilla\Firefox\Profiles\drb6pwbu.default-release\activity-stream.discovery_stream.json
- + ⌚ ?(C:\Users\<USER>\AppData\Roaming\Mozilla\Firefox\Profiles\drb6pwbu.default-release\addonStartup.json.lz4
- + ⌚ ?(C:\Users\<USER>\AppData\Roaming\Mozilla\Firefox\Profiles\drb6pwbu.default-release\addons.json
- + ⌚ ?(C:\Users\<USER>\AppData\Roaming\Mozilla\Firefox\Profiles\drb6pwbu.default-release\broadcast-listeners.json
- + ⌚ ?(C:\Users\<USER>\AppData\Roaming\Mozilla\Firefox\Profiles\drb6pwbu.default-release\cert9.db
- + ⌚ ?(C:\Users\<USER>\AppData\Roaming\Mozilla\Firefox\Profiles\drb6pwbu.default-release\compatibility.ini
- + ⌚ ?(C:\Users\<USER>\AppData\Roaming\Mozilla\Firefox\Profiles\drb6pwbu.default-release\containers.json
- + ⌚ ?(C:\Users\<USER>\AppData\Roaming\Mozilla\Firefox\Profiles\drb6pwbu.default-release\content-prefs.sqlite

⌄

Files Dropped

- + FihqnBxYm.ico
- + zzzzzzzzzz
- + bing.url.fihqnbxym
- + bitaddress.pdf.fihqnbxym
- + cover-letter-uidev.docx.fihqnbxym
- + invoice.pdf.fihqnbxym
- + persdata.doc.fihqnbxym
- + personal.xls.fihqnbxym
- + scarrer presentation.ppt.fihqnbxym
- + winrt--{s-1-5-21-4005801669-2598574594-602355426-1001}.searchconnector-ms.fihqnbxym

▼

Registry actions ⓘ

Registry Keys Opened

- ⌚ HKEY_CLASSES_ROOT\FihqnBxYm
- ⌚ HKEY_CLASSES_ROOT\FihqnBxYm\DefaultIcon
- ⌚ HKEY_CURRENT_USER\SOFTWARE\Microsoft\RestartManager\Session0000\ESCount
- ⌚ HKEY_CURRENT_USER\SOFTWARE\Microsoft\RestartManager\Session0000\JSCount
- ⌚ HKEY_CURRENT_USER\SOFTWARE\Microsoft\RestartManager\Session0000\Owner
- ⌚ HKEY_CURRENT_USER\SOFTWARE\Microsoft\RestartManager\Session0000\RRCount
- ⌚ HKEY_CURRENT_USER\SOFTWARE\Microsoft\RestartManager\Session0000\RegFiles0000
- ⌚ HKEY_CURRENT_USER\SOFTWARE\Microsoft\RestartManager\Session0000\RegFiles0001
- ⌚ HKEY_CURRENT_USER\SOFTWARE\Microsoft\RestartManager\Session0000\RegFilesHash
- ⌚ HKEY_CURRENT_USER\SOFTWARE\Microsoft\RestartManager\Session0000\RegProcs0000

Registry Keys Set

- + 🛡 \\Registry\Machine\COMPONENTS\ServicingStackVersions\6.1.7601.24537 (win7sp1_ldr_escrow.191114-1547)
- + 🛡 \\Registry\Machine\Software\Classes\FihqnBxYm\{Default}
- + 🛡 \\Registry\Machine\Software\Classes\FihqnBxYm\DefaultIcon\{Default}
- + 🛡 HKEY_CURRENT_USER\SOFTWARE\Microsoft\RestartManager\Session0000\Owner
- + 🛡 HKEY_CURRENT_USER\SOFTWARE\Microsoft\RestartManager\Session0000\RegFiles0000
- + 🛡 HKEY_CURRENT_USER\SOFTWARE\Microsoft\RestartManager\Session0000\RegFilesHash
- + 🛡 HKEY_CURRENT_USER\SOFTWARE\Microsoft\RestartManager\Session0000\Sequence
- + 🛡 HKEY_CURRENT_USER\SOFTWARE\Microsoft\RestartManager\Session0000\SessionHash
- + 🛡 HKEY_LOCAL_MACHINE\SOFTWARE\Classes\FihqnBxYm\{Default}

▼

Registry Keys Deleted

- ⌚ HKEY_CURRENT_USER\SOFTWARE\Microsoft\RestartManager\Session0000\Owner
- ⌚ HKEY_CURRENT_USER\SOFTWARE\Microsoft\RestartManager\Session0000\RegFiles0000
- ⌚ HKEY_CURRENT_USER\SOFTWARE\Microsoft\RestartManager\Session0000\RegFilesHash
- ⌚ HKEY_CURRENT_USER\SOFTWARE\Microsoft\RestartManager\Session0000\Sequence
- ⌚ HKEY_CURRENT_USER\SOFTWARE\Microsoft\RestartManager\Session0000\SessionHash

Process and service actions ⓘ

Processes Created

- ⌚ "C:\Users\<USER>\AppData\Local\Temp\l.exe"
- ⌚ C:\Windows\system32\services.exe
- ⌚ C:\Windows\system32\svchost.exe -k DcomLaunch -p
- ⌚ %SAMPLEPATH%\311edf744c2e90d7bfc550c893478f43d1d7977694d5dcecf219795f3eb99b86.exe
- ⌚ %SAMPLEPATH%\VLC.exe
- ⌚ %SAMPLEPATH%\l.exe
- ⌚ %SAMPLEPATH%\unknown.exe
- ⌚ C:\Windows\SystemApps\ShellExperienceHost_cw5n1h2txyewy\ShellExperienceHost.exe
- ⌚ "C:\Users\user\Desktop\l.exe"

```

Shell Commands
█ "%SAMPLEPATH%\311edf744c2e90d7bfc550c893478f43d1d7977694d5dcef219795f3eb99b86.exe"
█ "%SAMPLEPATH%\VLC.exe"
█ "%SAMPLEPATH%\Lexe"
█ "%SAMPLEPATH%\unknown.exe"
█ "C:\Windows\SystemApps\ShellExperienceHost_cw5n1h2txyewy\ShellExperienceHost.exe" -ServerName=App.AppXtk181ttxbce2qsex02s8tw7hfxa9xb3t.mca

Processes Injected
█ %SAMPLEPATH%\311edf744c2e90d7bfc550c893478f43d1d7977694d5dcef219795f3eb99b86.exe
█ %SAMPLEPATH%\VLC.exe
█ %SAMPLEPATH%\Lexe
█ %SAMPLEPATH%\unknown.exe

Processes Terminated
█ %windir%\System32\DiIHost.exe /Processid:{AB8902B4-09CA-4BB6-B78D-A8F59079A8D5}
█ wmiadap.exe /F /T /R
█ %SAMPLEPATH%\311edf744c2e90d7bfc550c893478f43d1d7977694d5dcef219795f3eb99b86.exe
█ %SAMPLEPATH%\VLC.exe
█ %SAMPLEPATH%\Lexe
█ %SAMPLEPATH%\unknown.exe
█ C:\Windows\System32\SSVC.exe
█ C:\Windows\System32\svchost.exe
█ C:\Windows\SystemApps\ShellExperienceHost_cw5n1h2txyewy\ShellExperienceHost.exe

```

```

Services Opened
● SecurityHealthService
● Sense
● WdBoot
● WdFilter
● WdNisDrv
● WdNisSvc
● WinDefend
● sppsvc
● vmicvss
● vss
▼

Services Deleted
☒ WinDefend
☒ sppsvc
☒ vss
☒ wscsvc

```

```

Processes Tree
    2700 - %windir%\system32\DllHost.exe /ProcessId:{AB8902B4-09CA-4BB6-B78D-A8F59079A8D5}
    2896 - wmiadap.exe /F /T /R
    2936 - %windir%\system32\wbem\wmiprvse.exe
    2600 - %windir%\servicing\TrustedInstaller.exe
    2508 - %SAMPLEPATH%
    5884 - "C:\Users\<USER>\AppData\Local\Temp\l.exe"
    692 - C:\Windows\system32\services.exe
        ↳ 832 - C:\Windows\system32\svchost.exe -k DcomLaunch -p
        ↳ 5588 - C:\Windows\system32\svchost.exe -k netsvcs -p -s Winmgmt
    3036 - %WINDIR%\explorer.exe
    ▾

Synchronization mechanisms & Signals ⓘ
Mutexes Created
    Local\RstrMgr-3887CAB8-533F-4C85-B0DC-3E5639F8D511-Session0000
    Local\RstrMgr3887CAB8-533F-4C85-B0DC-3E5639F8D511
    NULL

Modules loaded ⓘ
Runtime Modules
    COMBASE.DLL
    CRYPTBASE.DLL
    LOGONCLI.DLL
    NETUTILS.DLL
    NTDLL.DLL
    SAMCLI.DLL
    SRVCLI.DLL
    WKSCLI.DLL
    WS2_32.DLL
    %SAMPLEPATH%\311edf744c2e90d7bfc550c893478f43d1d7977694d5dcecf219795f3eb99b86.exe

```

```

Highlighted actions ⓘ
Calls Highlighted
    CoCreateGuid
    CoCreateInstance
    CoCreateInstanceEx
    CoInitializeEx
    CoInitializeSecurity
    CoSetProxyBlanket
    CoUninitialize
    DsGetDcCloseW
    DsGetDcNameW
    DsGetDcNextW
    ▾

Dataset actions ⓘ
System Property Lookups
    IWbemServices::Connect
    IWbemServices::ExecQuery - ROOT\CIMV2 : SELECT * FROM Win32_ShadowCopy

```

Información adicional del ejercicio

MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) es un marco de referencia y una base de datos completa que documenta las tácticas y técnicas utilizadas por los actores de amenazas en el ámbito de la ciberseguridad. Fue desarrollado por la organización MITRE y se utiliza ampliamente por profesionales de seguridad para entender mejor los métodos de ataque, mejorar las defensas y analizar los incidentes de seguridad.

Principales Componentes del Marco MITRE ATT&CK:

- 1. Tácticas (Tactics):**
 - Representan los objetivos estratégicos que un adversario intenta lograr durante una operación de ataque. Ejemplos de tácticas incluyen Ejecución (Execution), Persistencia (Persistence) y Evasión de Defensa (Defense Evasion).
- 2. Técnicas (Techniques):**
 - Describen las formas específicas en que un adversario logra una táctica. Por ejemplo, dentro de la táctica de Ejecución, una técnica podría ser la Ejecución a través de Windows Management Instrumentation (WMI).
- 3. Subtécnicas (Sub-techniques):**
 - Proporcionan un nivel adicional de detalle bajo las técnicas. Cada técnica puede tener una o más subtécnicas que describen variaciones específicas de la técnica.
- 4. Procedimientos (Procedures):**
 - Ofrecen descripciones detalladas de cómo se utilizan las técnicas en escenarios específicos. Incluyen ejemplos reales de incidentes de seguridad en los que se han utilizado estas técnicas.

Propósitos del Marco MITRE ATT&CK:

- 1. Entendimiento de Amenazas:**
 - Ayuda a los analistas de seguridad a comprender mejor los métodos utilizados por los adversarios y a anticipar posibles ataques.
- 2. Evaluación de Seguridad:**
 - Permite a las organizaciones evaluar la eficacia de sus defensas actuales y realizar pruebas de penetración basadas en las técnicas documentadas.
- 3. Respuesta a Incidentes:**
 - Proporciona un marco común para investigar y responder a incidentes de seguridad, facilitando la identificación de tácticas y técnicas utilizadas por los atacantes.
- 4. Desarrollo de Capacidades de Defensa:**
 - Ayuda en el desarrollo de medidas defensivas específicas para contrarrestar las técnicas utilizadas por los adversarios.

Ejemplo de Tácticas y Técnicas:

- **Ejecución (Execution):** Incluye técnicas como la ejecución a través de WMI (T1047) o el uso de intérpretes de comandos y scripts (T1059).
- **Persistencia (Persistence):** Técnicas como la creación o modificación de procesos del sistema (T1543) y la modificación de servicios de Windows (T1543.003).
- **Evasión de Defensa (Defense Evasion):** Incluye técnicas como el acceso directo al volumen (T1006) y la modificación del registro (T1112).

Recursos Adicionales:

- MITRE ATT&CK Framework: <https://attack.mitre.org/>
- Crowdstrike: <https://www.crowdstrike.com/cybersecurity-101/mitre-attack-framework/>

El marco MITRE ATT&CK es una herramienta esencial para los profesionales de ciberseguridad, ya que proporciona un entendimiento profundo de las tácticas y técnicas de los adversarios, facilitando una mejor preparación y respuesta ante amenazas de seguridad.

Tarea 4:

Imagina que trabajas en un SOC como analista de Nivel 1. Recibes una alerta en la que se describe que el equipo de un usuario de uno de los clients (del departamento de ventas) se ha ejecutado el comando que se muestra en la alerta siguiente:

Alerts	MALICIOUS PROCESS: ipscan.exe	HOST IP: 192.168.1.124	FIRST SEEN 03/06/24 11:52
			LAST SEEN 03/06/24 11:52
Description – Process Monitoring <ul style="list-style-type: none"> - Host IP: 192.168.1.124 - Host Name: equipo4 - Username: equipo4_ventas - Os Version: Windows 10 Pro x64 - Process Command Line: C:\Program Files\Angry IP Scanner\ipscan.exe - Parent Process: C:\windows\Explorer.EXE - Description: T1018: This behavior may indicate adversaries are attempting to get a listing of other systems by IP address, hostname, or other logical identifiers on a network that may be used for Lateral Movement from the current system 			

Realiza un pequeño informe basándote al menos en las siguientes cuestiones:

- ¿De qué se trata esta alerta?
- El comando detectado en esta alerta, ¿en qué consiste?
- Dependiendo de si consideras maliciosa esta acción o si por el contrario consideras que es un falso positivo, ¿qué recomendación le darías al cliente?

Informe de Incidente de Seguridad

SOC - Centro de Operaciones de Seguridad

Fecha: 26/06/2024

Analista: Sheila Fernández

Asunto: Informe de Incidente de Seguridad – Alerta de Actividad Sospechosa

Descripción del Incidente

El día 3 de junio de 2024 a las 11:52 horas, se recibió una alerta en el Centro de Operaciones de Seguridad (SOC) indicando un posible incidente de seguridad en uno de los sistemas de la red. La alerta fue generada por las herramientas de monitoreo de seguridad y contenía la siguiente información:

- **Alerta recibida:** Proceso malicioso: ipscan.exe
- **IP del Host:** 192.168.1.124
- **Nombre del Host:** equipo4
- **Nombre de Usuario:** equipo4_ventas
- **Versión del SO:** Windows 10 Pro x64
- **Primera Detección:** 03/06/24 11:52
- **Última Detección:** 03/06/24 11:52

Descripción del proceso

- **Línea de Comando del Proceso:** C:\Program Files\Angry IP Scanner\ipscan.exe
- **Proceso Padre:** C:\windows\Explorer.EXE
- **Descripción:** T1018: Este comportamiento puede indicar que adversarios están intentando obtener una lista de otros sistemas por dirección IP, nombre de host u otros identificadores lógicos en una red, lo que podría ser usado para movimiento lateral desde el sistema actual.

Análisis de la Alerta

La alerta indica que en el equipo identificado como “equipo4”, perteneciente a un usuario del departamento de ventas, se ha detectado la ejecución del proceso ipscan.exe. Este proceso corresponde a la herramienta “Angry IP Scanner”, la cual es comúnmente utilizada para escanear redes en busca de direcciones IP activas y puertos abiertos.

El comando detectado (C:\Program Files\Angry IP Scanner\ipscan.exe) sugiere que el usuario ejecutó la aplicación Angry IP Scanner desde su ubicación de instalación predeterminada. Esta herramienta puede ser utilizada tanto para fines legítimos, como la administración de red, o para actividades maliciosas, como el reconocimiento previo a un ataque.

Evaluación de la Maliciosidad

La ejecución de ipscan.exe puede ser considerada maliciosa si no está autorizada o si no es una herramienta comúnmente utilizada por el departamento de ventas. Dado que esta herramienta se utiliza para mapear redes, su uso no autorizado puede indicar actividades de reconocimiento potencialmente maliciosas, tales como:

- **Mapeo de la red:** Identificar qué dispositivos están activos en la red.
- **Descubrimiento de puertos abiertos:** Determinar qué servicios están corriendo en los dispositivos de la red.
- **Enumeración de sistemas y servicios:** Obtener información sobre los sistemas operativos y las aplicaciones que están en uso.
- **Preparación para un ataque de movimiento lateral:** Utilizar la información recolectada para moverse lateralmente dentro de la red, accediendo a otros dispositivos.
- **Identificación de vulnerabilidades:** Buscar puntos débiles en la red que pueden ser explotados para obtener acceso no autorizado.

Recomendaciones

Dado que el uso de Angry IP Scanner no es típico en el contexto del departamento de ventas, se recomienda tomar las siguientes acciones:

1. **Confirmar la Legitimidad:** Verificar con el usuario y el departamento de TI si la ejecución de Angry IP Scanner fue autorizada y tenía un propósito legítimo.
2. **Ánálisis Forense:** Realizar un análisis forense del equipo “equipo4” para identificar cualquier actividad inusual o conexiones sospechosas que puedan haber sido realizadas desde o hacia este equipo.

3. **Revisión de Políticas:** Asegurarse de que las políticas de seguridad y de uso de herramientas estén claras y sean comunicadas a todos los empleados. Limitar el uso de herramientas de escaneo de red a personal autorizado.
4. **Monitoreo Adicional:** Incrementar el monitoreo de la red para detectar cualquier otro uso no autorizado de herramientas de escaneo o cualquier comportamiento anómalo que pueda indicar un movimiento lateral o un ataque en curso.

Firma: Sheila Fernández, Analista SOC N1, 26/06/2024

Estas acciones ayudarán a asegurar que la actividad detectada sea legítima o, en caso contrario, a mitigar cualquier posible amenaza a la red y a los sistemas del cliente.

Tarea 5:

Imagina que trabajas en un SOC como analista de Nivel 1. Recibes una alerta en la que se describe el incidente que se muestra a continuación:

Alert

MALICIOUS FILE: setup.exe



HOST: equipo5

FIRST SEEN: 17/04/24 18:42

LAST SEEN: 17/04/24 18:42

Description – Executable Download

- **Download Source:** GitHub Repository
- **User Involved:** equipo5
- **URL:** https://github.com/guillaume-bgd/ul_mapping_correspondants/blob/main/main.py
- **Description:** This rule detects the downloading of executable files from the GitHub repository, which can be a way to introduce malicious and illegitimate programs to the organization

Realiza un pequeño informe basándote al menos en las siguientes cuestiones:

- ¿En qué consiste esta alerta?
- ¿Cuáles son los riesgos que suponen este tipo de acciones?
- Tras analizar la alerta, ¿se debe considerar como una acción maliciosa, o por el contrario debería cerrarse como falso positivo?

- ¿Qué recomendaciones se le podrían dar al cliente ante este tipo de alertas?

Informe de Incidente de Seguridad

SOC - Centro de Operaciones de Seguridad

Fecha: 26/06/2024

Analista: Sheila Fernández

Asunto: Informe de Incidente de Seguridad – Alerta de Descarga Ejecutable

Descripción del Incidente

El día 14 de abril de 2024 a las 18:42 horas, se recibió una alerta en el Centro de Operaciones de Seguridad (SOC) indicando un posible incidente de seguridad en uno de los sistemas de la red. La alerta fue generada por las herramientas de monitoreo de seguridad y contenía la siguiente información:

- **Alerta recibida:** Archivo malicioso: setup.exe
- **Host:** equipo5
- **Primera detección:** 17/04/24 18:42
- **Última detección:** 17/04/24 18:42

Descripción del Proceso

- **Fuente de descarga:** Repositorio de GitHub
- **Usuario involucrado:** equipo5
- **URL:** https://github.com/guillaume-bgd/ul_mapping_correspondants/blob/main/main.py
- **Descripción:** Esta regla detecta la descarga de archivos ejecutables desde el repositorio de GitHub, lo cual puede ser una forma de introducir programas maliciosos e ilegítimos en la organización.

Análisis de la Alerta

La alerta indica que un usuario del equipo equipo5 ha descargado un archivo ejecutable (setup.exe) desde un repositorio de GitHub. La alerta ha sido generada porque la descarga de archivos ejecutables desde fuentes externas, como GitHub, puede ser una vía para introducir software malicioso en la red de la organización.

1. Análisis de la URL

Se procedió a analizar la URL en VirusTotal y URLVoid para determinar su legitimidad. El análisis de ambos mostró que la URL de GitHub desde donde se descargó el archivo no fue marcada como maliciosa por ningún proveedor de seguridad.

Riesgos Asociados

Los riesgos asociados con la descarga de ejecutables desde repositorios públicos incluyen:

- **Introducción de malware:** El archivo descargado puede contener virus, troyanos, ransomware u otro tipo de software malicioso que puede comprometer la seguridad de la red y los datos de la organización.
- **Ejecución de código no verificado:** Descargar y ejecutar programas de fuentes externas sin verificarlos adecuadamente puede llevar a la ejecución de código potencialmente dañino.
- **Exposición a vulnerabilidades:** El software descargado puede tener vulnerabilidades que podrían ser explotadas por atacantes para obtener acceso no autorizado a los sistemas de la organización.

Evaluación de la Maliciosidad

Para determinar si esta acción es maliciosa o un falso positivo, se deben considerar los siguientes pasos:

1. **Verificación de la legitimidad del archivo:** Confirmar con el usuario si la descarga del archivo fue intencional y con un propósito legítimo.
2. **Ánalisis del archivo:** Realizar un análisis del archivo setup.exe utilizando herramientas de análisis de malware para verificar si contiene código malicioso.

Según el análisis reciente mostrado en la captura, la URL de GitHub desde donde se descargó el archivo no fue marcada como maliciosa por ningún proveedor de seguridad.

Recomendaciones

1. **Confirmación de la Legitimidad:** Verificar con el usuario y el departamento de TI si la descarga del archivo setup.exe fue autorizada y tenía un propósito legítimo.
2. **Análisis de Seguridad:** Aunque el análisis de la URL no muestra actividad maliciosa, realizar un análisis de seguridad exhaustivo del archivo descargado para asegurar que no contiene software malicioso.
3. **Refuerzo de Políticas de Descarga:** Reforzar las políticas de seguridad que regulan la descarga de archivos ejecutables desde fuentes externas. Asegurarse de que los usuarios solo descarguen software desde fuentes confiables y verificadas.
4. **Educación y Concienciación:** Capacitar a los usuarios sobre los riesgos de descargar y ejecutar archivos desde fuentes no verificadas y la importancia de seguir las políticas de seguridad de la organización.
5. **Monitoreo Continuo:** Implementar mecanismos de monitoreo continuo para detectar y responder rápidamente a actividades sospechosas relacionadas con la descarga y ejecución de archivos.

Firma: Sheila Fernández, Analista SOC N1, 26/06/2024

Anexo: Detalles del Análisis de VirusTotal y URLVOID

Resultados del análisis realizado en VirusTotal:

The screenshot shows the URLVoid analysis interface for the URL https://github.com/guillaume-bgd/ul_mapping_correspondants/blob/main/main.py. The main header indicates 'No security vendors flagged this URL as malicious'. Below this, the URL is listed as https://github.com/guillaume-bgd/ul_mapping_correspondants/blob/main/main.py (github.com) with a status of 404, content type of text/html; charset=utf-8, and last analysis date of 7 days ago. A 'Community Score' of 0/95 is shown with a green progress bar. The interface includes tabs for DETECTION, DETAILS, and COMMUNITY, with the DETECTION tab selected. A call-to-action button 'Join our Community' is present. The 'Security vendors' analysis' section contains 16 entries, each with a vendor name, a green checkmark icon, and the word 'Clean'. The vendors listed are: Abusix, ADMINUSLabs, AlienVault, Antiy-AVL, benkow.cc, BlockList, Certego, CINS Army, CRDF, Cyble, desenmascara.me, Dr.Web, Acronis, AI Labs (MONITORAPP), alphaMountain.ai, Artists Against 419, BitDefender, Blueliv, Chong Lua Dao, CMC Threat Intelligence, Criminal IP, CyRadar, DNS8, and EmergingThreats. A 'Do you want to automate checks?' link is located in the top right corner of this section.

Vendor	Status
Abusix	Clean
ADMINUSLabs	Clean
AlienVault	Clean
Antiy-AVL	Clean
benkow.cc	Clean
BlockList	Clean
Certego	Clean
CINS Army	Clean
CRDF	Clean
Cyble	Clean
desenmascara.me	Clean
Dr.Web	Clean
Acronis	Clean
AI Labs (MONITORAPP)	Clean
alphaMountain.ai	Clean
Artists Against 419	Clean
BitDefender	Clean
Blueliv	Clean
Chong Lua Dao	Clean
CMC Threat Intelligence	Clean
Criminal IP	Clean
CyRadar	Clean
DNS8	Clean
EmergingThreats	Clean

Resultados del análisis en URLVoid:

Report Summary	
Website Address	Github.com
Last Analysis	3 hours ago Rescan
Detections Counts	0/40
Domain Registration	2007-10-09 17 years ago
Domain Information	WHOIS Lookup DNS Records Ping
IP Address	140.82.121.4 Find Websites IPVoid Whois
Reverse DNS	lb-140-82-121-4-fra.github.com
ASN	AS36459 GITHUB
Server Location	 (DE) Germany
Latitude\Longitude	50.1187 / 8.6842 Google Map
City	Frankfurt am Main
Region	Hesse

Tarea 6:

Imagina que trabajas en un SOC como analista de Nivel 1. Recibes una alerta en la que se describe el incidente que se muestra a continuación:

Alert

The diagram illustrates a network connection between two hosts. On the left, a computer monitor icon is labeled "EXTERNAL HOST". A curved arrow points from this host to another computer monitor icon on the right, which is labeled "HOST: equipo6". The word "RDP" is written in blue text next to the arrow, indicating the protocol used for the connection.

EXTERNAL HOST	HOST: equipo6	FIRST SEEN 19/06/24 09:37
		LAST SEEN 19/06/24 09:37

Description – Attempted to login via RDP

- **Hostname:** equipo6
- **Host IP:** 172.10.0.23
- **Number of Failed Attempts:** 10
- **Number of Successful Attempts:** "X"
- **Description:** This rule detects when EventID 4825 triggers. This eventID means that a user was denied the access to Remote Desktop. By default, users are allowed to connect only if they are members of the Remote Desktop Users group or Administrators group

Realiza un pequeño informe basándote al menos en las siguientes cuestiones:

- ¿En qué consiste esta alerta?
- ¿Sería recomendable pedirle al cliente que investigue acerca del incidente para ver si el intento de acceso fue legítimo, o habría que recomendarles directamente que restablezcan las credenciales de ese usuario lo antes posible?
- En caso de que no haya sido un acceso legítimo, ¿qué peligros supone para la empresa?

Comentar qué posibles diferencias habría en los casos en los que “X” fuese 0 o distinto de 0 para el “número de intentos exitosos”.

Informe de Incidente de Seguridad

SOC - Centro de Operaciones de Seguridad

Fecha: 26/06/2024

Analista: Sheila Fernández

Asunto: Informe de Incidente de Seguridad – Alerta de Intento de Acceso por vía RDP

Descripción del Incidente

El día 19 de junio de 2024 a las 09:37 horas, se recibió una alerta en el Centro de Operaciones de Seguridad (SOC) indicando un posible incidente de seguridad en uno de los sistemas de la red. La alerta fue generada por las herramientas de monitoreo de seguridad y contenía la siguiente información:

- **Nombre del Host:** equipo6
- **IP del Host:** 172.10.0.23
- **Número de intentos fallidos:** 10
- **Número de intentos exitosos:** "X"
- **Primera detección:** 19/06/24 09:37
- **Última detección:** 19/06/24 09:37
- **Descripción del Evento:** Esta regla se activa cuando el EventID 4825 se desencadena. Este EventID indica que a un usuario se le denegó el acceso a Escritorio Remoto. Por defecto, los usuarios solo pueden conectarse si son miembros del grupo de Usuarios de Escritorio Remoto o del grupo de Administradores.

Análisis del Incidente

La alerta registrada indica un intento de acceso remoto no autorizado al equipo "equipo6". La detección de múltiples intentos fallidos sugiere un posible ataque de fuerza bruta o un intento de acceso no autorizado.

Número de Intentos Exitosos

El número de intentos exitosos viene determinado con "X", lo cual puede deberse a varias razones:

- **Datos incompletos:** El sistema de monitoreo puede haber registrado los intentos fallidos, pero no ha terminado de procesar o recibir los datos completos sobre los intentos exitosos.
- **Configuración de la alerta:** Puede que la alerta esté configurada para registrar solamente los intentos fallidos y el número de intentos exitosos aún no ha sido registrado en el log o en la alerta generada.
- **Error en la recopilación de datos:** Es posible que haya un error en la herramienta de monitoreo que impide que el número exacto de intentos exitosos se registre correctamente.

Diferencias en el Número de Intentos Exitosos

- **X = 0:** Indica que todos los intentos de acceso fallaron, sugiriendo un intento fallido de ataque de fuerza bruta o acceso no autorizado. Se recomienda reforzar las medidas de seguridad.
- **X > 0:** Indica que al menos un intento de acceso fue exitoso, lo cual es crítico y requiere un análisis forense inmediato para determinar el alcance del compromiso, restablecer las credenciales y revisar los logs para identificar cualquier actividad sospechosa.

Peligros Potenciales para la Empresa

En caso de que el acceso no haya sido legítimo, los peligros potenciales incluyen:

- **Acceso no autorizado a información sensible:** Un atacante podría robar o manipular datos confidenciales.
- **Compromiso de la red interna:** El atacante podría moverse lateralmente dentro de la red, comprometiendo otros sistemas y recursos.
- **Instalación de malware o ransomware:** Un atacante podría instalar software malicioso.
- **Pérdida de confianza y reputación:** Un incidente de seguridad puede dañar la reputación de la empresa y afectar la confianza de los clientes.

Conclusión

La alerta debe ser tratada con la máxima prioridad. Es esencial investigar a fondo el origen de los intentos de acceso y tomar medidas inmediatas para proteger la red y los sistemas afectados. Restablecer las credenciales y reforzar las políticas de seguridad son pasos necesarios para mitigar posibles amenazas y proteger la integridad de la infraestructura de TI de la empresa.

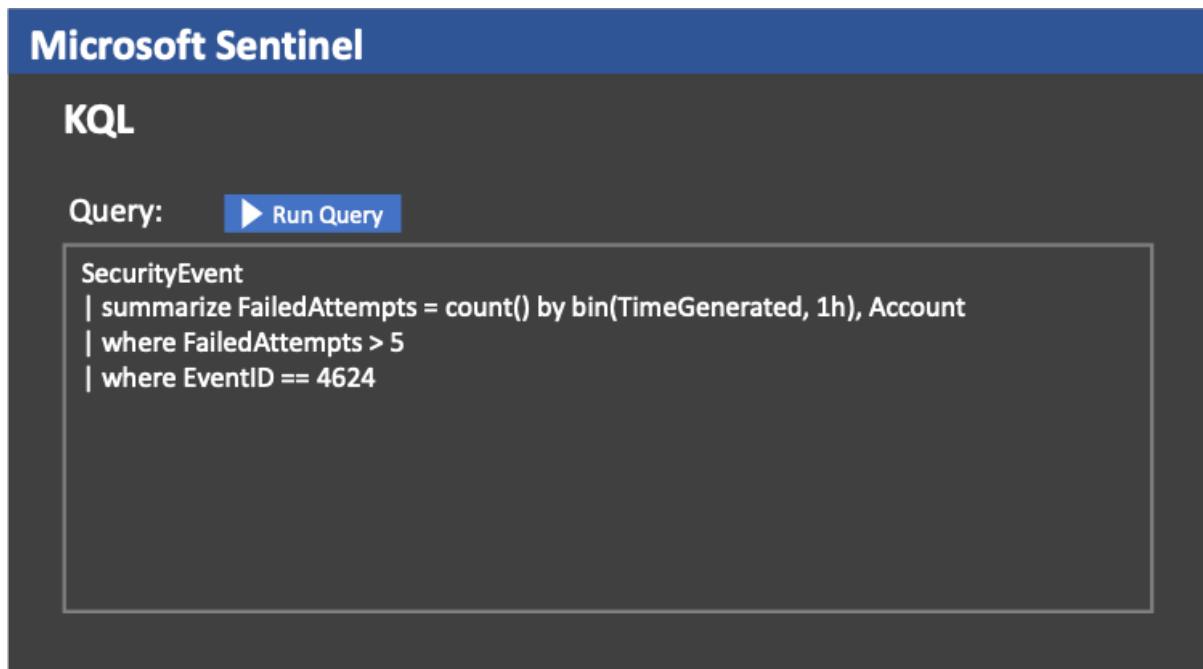
Recomendaciones

1. **Investigación del Incidente:** Llevar a cabo una investigación detallada para determinar si el intento de acceso fue legítimo. Esta investigación debe incluir la revisión de los logs de seguridad y el análisis del tráfico de red asociado.
2. **Restablecimiento de Credenciales:** Independientemente de la legitimidad del acceso, restablecer las credenciales del usuario afectado de inmediato para prevenir accesos no autorizados adicionales.
3. **Fortalecimiento de la Seguridad:** Implementar medidas de seguridad adicionales, tales como la autenticación multifactor, el bloqueo de cuentas después de varios intentos fallidos y la revisión de los permisos de acceso a los sistemas críticos.
4. **Revisión de Configuraciones de Monitoreo:** Verificar y corregir cualquier configuración errónea en las herramientas de monitoreo para asegurar que toda la información relevante se registre correctamente.

Firma: Sheila Fernández, Analista SOC N1, 26/06/2024

Tarea 7:

Imagina que trabajas en un SOC como analista de Nivel 1. Quieres detectar cuándo un usuario intenta iniciar sesión más de 5 veces de manera errónea en un determinado periodo de tiempo. Para ello se hace uso de la siguiente regla definida en lenguaje KQL (“Kusto Query Language”):



The screenshot shows the Microsoft Sentinel interface with the title "Microsoft Sentinel" at the top. Below it, a blue bar says "KQL". Underneath, there's a "Query:" field containing the following KQL code:

```
SecurityEvent  
| summarize FailedAttempts = count() by bin(TimeGenerated, 1h), Account  
| where FailedAttempts > 5  
| where EventID == 4624
```

Next to the "Query:" field is a blue button with a white play icon and the text "Run Query".

Comprueba si esta regla está bien construida y realizará las consultas que se desean hacer. En caso de que se detecte algún error, comente el motivo por el cual se cree que es errónea, describa cómo debería ser para ser correcta y explique el funcionamiento que tiene una vez corregida.

En caso contrario, comente el funcionamiento de la regla.

Análisis de la Regla

Problemas Detectados

- Condiciones Inadecuadas para Filtrado:** El EventID 4624 se refiere a un evento de inicio de sesión exitoso. Para capturar intentos de inicio de sesión fallidos, se debe utilizar EventID correspondiente a fallos de inicio de sesión, como 4625 (que indica un intento de inicio de sesión fallido).

2. **Orden de las Condiciones:** Filtrar por EventID debe realizarse antes de la agregación para asegurar que solo se cuentan los eventos relevantes (fallos de inicio de sesión) y no todos los eventos.

Corrección de la Regla

Para corregir la regla, se deben realizar los siguientes cambios:

1. Filtrar por EventID 4625 antes de la agregación.
2. Asegurarse de contar solo los eventos de intentos fallidos.

La regla corregida debería ser:

SecurityEvent

```
| where EventID == 4625  
| summarize FailedAttempts = count() by bin(TimeGenerated, 1h), Account  
| where FailedAttempts > 5
```

Explicación del Funcionamiento de la Regla Corregida

1. **Filtro Inicial:** | where EventID == 4625
 - Este filtro selecciona solo los eventos que corresponden a intentos de inicio de sesión fallidos.
2. **Agregación y Conteo:** | summarize FailedAttempts = count() by bin(TimeGenerated, 1h), Account
 - Esta línea agrega los datos en intervalos de una hora (bin(TimeGenerated, 1h)) y cuenta el número de intentos de inicio de sesión fallidos (count()) por cada cuenta (Account).
3. **Filtro de Conteo:** | where FailedAttempts > 5
 - Finalmente, este filtro selecciona solo aquellos casos donde el número de intentos de inicio de sesión fallidos en una hora para una cuenta específica es mayor a 5.

Conclusión

La regla original no estaba bien construida para detectar intentos de inicio de sesión fallidos debido al uso del EventID incorrecto y el orden inadecuado de las condiciones. Con la corrección aplicada, la regla ahora funcionará como se desea, detectando usuarios que intentan iniciar sesión más de 5 veces de manera errónea en un periodo de una hora.