Laboratorio BRabbit de CyberDefenders

Categoría : Inteligencia de amenazas
Tácticas : Ejecución, Persistencia, Escalada de privilegios, Comando y control, Impacto
Dificultad : Media

Escenario :

Eres un investigador asignado para ayudar a Drumbo, una empresa que recientemente fue víctima de un ataque de ransomware. El ataque comenzó cuando un empleado recibió un correo electrónico que parecía ser del jefe. Presentaba el logotipo de la empresa y una dirección de correo electrónico conocida. Creyendo que el correo era legítimo, el empleado abrió el archivo adjunto, lo que comprometió el sistema e activó el ransomware, cifrando archivos confidenciales. Tu tarea es investigar y analizar los elementos para descubrir información sobre el atacante.

P1: El correo electrónico de phishing utilizado para enviar el archivo adjunto malicioso mostró varios indicadores de un posible intento de ingeniería social. Reconocer estos indicadores puede ayudar a identificar amenazas similares en el futuro.
¿Cuál es la dirección de correo electrónico sospechosa que envió el archivo adjunto?

Para esta primera pregunta es importante comentar que el archivo es una muestra de Ransomware, por lo que no debes ejecutarlo en tu maquina host, se recomienda un entorno aislado:

```
┌──(root㉿kali)-[/home/karolina/Desktop/temp_extract_dir (2)/218-BRabbit]
└─# cat Warning.txt
Do not run this file as it is real ransomware and could cause significant harm to your system. Executing the file may lead to the encryption
 of your personal data, making it inaccessible without paying a ransom. It could also allow attackers to gain unauthorized control over your
 machine, potentially causing permanent damage or data loss. For your safety, do not interact with this file and delete it immediately. If y
ou must analyze it, only do so in a secure, isolated environment such as a virtual machine.

Password: infected

┌──(root㉿kali)-[/home/karolina/Desktop/temp_extract_dir (2)/218-BRabbit]
└─#
```

Una vez que se descomprime el archivo puedes visualizar el correo electrónico con el comando string:

```
┌──(root㉿kali)-[/home/karolina/Desktop/temp_extract_dir (2)/218-BRabbit]
└─# strings Urget\ Contract\ Action.eml | grep @
Delivered-To: Rafaiel@Drumbo.com
Delivered-To: me@Drumbo.com
 <Rafaiel@Drumbo.com>        (version=TLS1 cipher=ECDHE-ECDSA-AES128-SHA
ARC-Authentication-Results: i=1; mx.google.com;       dkim=pass header.i=@dezoeteinval.co.za
 return@alaho-akbar.dezoeteinval.co.za designates 51.195.254.223 as permitted
 sender) smtp.mailfrom=Return@alaho-akbar.dezoeteinval.co.za;
Return-Path: Return@alaho-akbar.dezoeteinval.co.za
Received-SPF: pass (google.com: domain of return@alaho-akbar.dezoeteinval.co.za designates
Authentication-Results: mx.google.com;       dkim=pass header.i=@dezoeteinval.co.za header.s=smtp
 return@alaho-akbar.dezoeteinval.co.za designates 51.195.254.223 as permitted
 sender) smtp.mailfrom=Return@alaho-akbar.dezoeteinval.co.za;
 h=From:To:Subject:MIME-Version:Date:List-Unsubscribe:Message-ID:Content-Type; i=theceojamessmith@Drurnbo.com; bh=Ii9k8I7YilfzIrtepZOKK1WPxF
o=;
From: =?utf-8?B?RHJ1bWJvwq4=?= <theceojamessmith@Drurnbo.com>
To: "Rafaiel@Drumbo.com" <Rafaiel@Drumbo.com>
X-Google-Original-Message-ID: <←@vevida.net>
X-Google-Sender-Delegation: Rafaiel@Drumbo.comTrusted Sender
List-Unsubscribe: <mailto:unsubscribe@store.ass0005.gogomailbali.eu.org>
Message-ID: <1419576.bWFhcmtrbm9wZmxlckBnbWFpbC5jb20=@iobBeE5>
Sender: =?utf-8?B?RHJ1bWJvwq4=?= <theceojamessmith@Drurnbo.com>
```

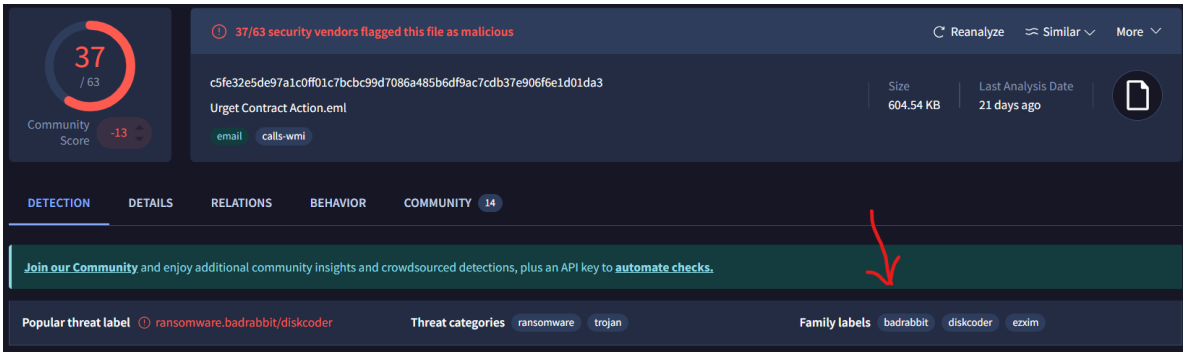
P2: El ransomware se identificó como parte de una familia de malware conocida. Determinar su nombre de familia puede proporcionar información crucial sobre su comportamiento y las estrategias de remediación.
¿Cuál es el nombre de familia del ransomware identificado durante la investigación?

Para esta parte puedes cargar el archivo .ml en alguna pagina de inteligencia de amenazas como Virus Total, Hibryd Análisis, Anu.run etc, en mi caso genere el Hash MD5 y solo copie ese valor en Virus Total:

```
┌──(root㉿kali)-[/home/karolina/Desktop/temp_extract_dir (2)/218-BRabbit]
└─# md5sum Urget\ Contract\ Action.eml
048c02e929690bcb0a537d08e71f6b50  Urget Contract Action.eml

┌──(root㉿kali)-[/home/karolina/Desktop/temp_extract_dir (2)/218-BRabbit]
└─#
```

Lo que nos da como resultado:



Las familias a las cuales hace referencia el malware.

P3: Tras su ejecución, el ransomware ingresó un archivo en el sistema comprometido para iniciar su carga útil. Identificar este archivo es esencial para comprender su proceso de infección.
¿Cómo se llama el primer archivo que ingresó el ransomware?

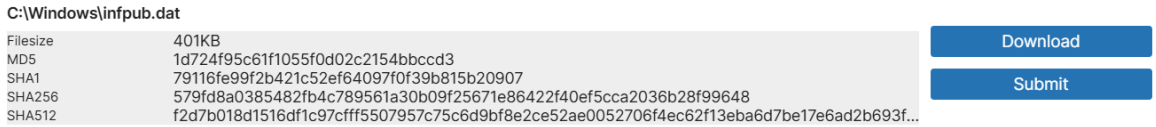
Para este punto necesite realizar mucha investigación, hasta que llegue a este informe:

https://tria.ge/250108-m3erpaxjh1/behavioral1

Aquí podemos ver el árbol de procesos y por lo tanto el nombre del archivo:

P4: Dentro del archivo descargado, el malware contenía artefactos codificados, incluyendo nombres de usuario y contraseñas que podrían proporcionar pistas sobre su origen o configuración.
¿Cuál es el único nombre de usuario encontrado en el archivo descargado?

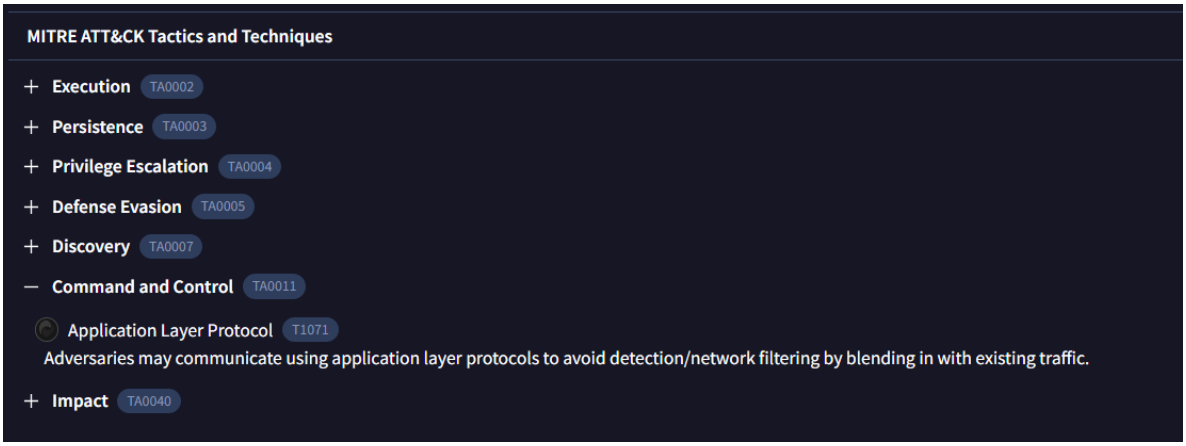
Para esto hay que descargar el archivo en tu MV, importante que sea un entorno aislado:



Una vez descargado, con el comando strings info.dat vamos a ver varios nombres de usuarios:

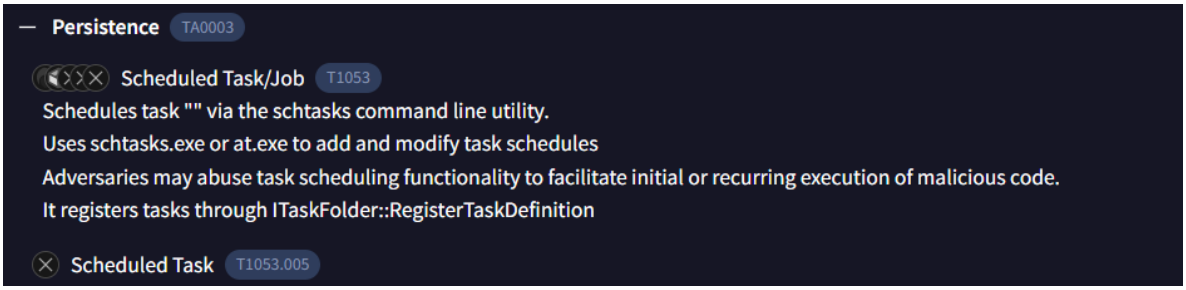
P5: Tras su ejecución, el ransomware se comunicó con un servidor C2. Reconocer sus técnicas de comunicación puede ayudar a mitigar el ataque.
¿Qué subtécnica de MITRE ATT&CK describe el uso de protocolos web por parte del ransomware para enviar y recibir datos?

Para esto basta con preguntar en Google cual es la subtenica de MITRE y realizar un poco de investigación, sin embargo, también en el Behavior de Virus total podemos observar las técnicas, en este caso de C2:



P6: Los mecanismos de persistencia son un sello distintivo del ransomware sofisticado. Identificar cómo se logró la persistencia puede facilitar la recuperación y la prevención de reinfecciones.
¿Cuál es el ID de la subtécnica MITRE ATT&CK asociado con la técnica de persistencia del ransomware?

Lo mismo que en el punto anterior en la parte de Behavior de VT en Persistence vamos a ver las Técnicas, o bien puedes investigar directo en Google:

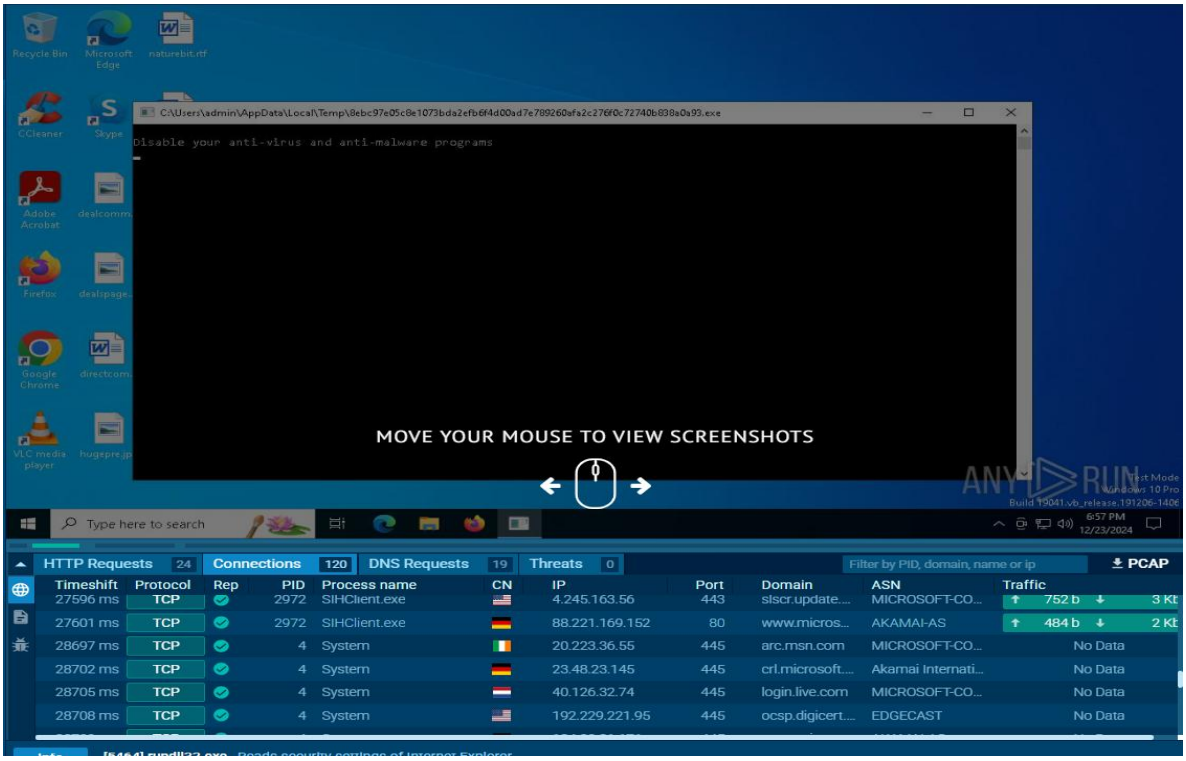


P7:Como parte de su cadena de infección, el ransomware creó tareas específicas para garantizar su funcionamiento continuo. Reconocer estas tareas es crucial para la restauración del sistema. ¿Cómo se llaman las tareas creadas por el ransomware durante su ejecución?

Para esta pregunta en el árbol de procesos del triage también se especifica el nombre de las tareas creadas (TN = nombre de la tarea):

*P8: El binario malicioso dispci.exemostró un **mensaje sospechoso** al ejecutarse, instando a los usuarios a desactivar sus defensas. Esta táctica buscaba evadir la detección y permitir la ejecución completa del ransomware. ¿Qué mensaje sospechoso se mostró en la consola al ejecutar este binario?*

En any.Run se puede visualizar un promnt con cade de texto:



P9: Para modificar el Registro de Arranque Maestro (MBR) y cifrar el disco duro de la víctima, el ransomware utilizó un controlador específico. Reconocer este controlador es esencial para comprender el mecanismo de cifrado.
¿Cómo se llama el controlador utilizado para cifrar el disco duro y modificar el MBR?

Para esta pregunta podemos regresar a Virus Total donde analizamos el archivo dispci.exe, en la parte de los Detalles vemos esto:

P10: La atribución es clave para comprender el panorama de amenazas. El ransomware se vinculó a un grupo de ataque conocido mediante sus tácticas, técnicas y procedimientos (TTP).
¿Cuál es el nombre del actor de amenazas responsable de esta campaña de ransomware?

Haber para este punto no se requiere nada del otro mundo únicamente hacer una búsqueda exhaustiva sobre la amenaza todo lo relacionado a BadRabbit, encontraras artículos que los relacionan con otros tipos de malware y con eso encontraras los actores de amenazas.

Por favor si no encuentras esta información Preguntate que estas haciendo aquiiiiiiiiii!

P11: El ransomware impidió el arranque del sistema al corromper componentes críticos. Identificar la técnica utilizada proporciona información sobre su capacidad destructiva.
¿Cuál es el ID de MITRE ATT&CK de la técnica utilizada para corromper el firmware del sistema e impedir el arranque?

Para esto muy sencillo vas a MITRE en el buscador poner la palabra Firmware y ahí lo tienes.

Si te sirvió esta información no olvides irme a seguir a mis redes sociales:

Youtube: https://www.youtube.com/c/Or4kM4cCiberseguridad

Facebook: https://www.facebook.com/orakmac

Instagram: https://www.instagram.com/orackmac/

Tiktok: https://www.tiktok.com/@orackmac