TRABAJO DE GRADO

DEMOSTRACIÓN DE LA APLICABILIDAD DEL PROYECTO MITRE ATT&CK A TRAVÉS DE UN PROCESO DE EMULACIÓN DE ADVERSARIOS

JUAN CARLOS LÓPEZ MONTENEGRO

SERGIO RODRÍGUEZ ANDRADE

UNIVERSIDAD CATÓLICA DE COLOMBIA

FACULTAD DE INGENIERÍA

PROGRAMA DE ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

BOGOTÁ D.C

AÑO

2020

TRABAJO DE GRADO

DEMOSTRACIÓN DE LA APLICABILIDAD DEL PROYECTO MITRE ATT&CK A TRAVÉS DE UN PROCESO DE EMULACIÓN DE ADVERSARIOS

JUAN CARLOS LÓPEZ MONTENEGRO

SERGIO RODRÍGUEZ ANDRADE

Trabajo de grado presentado para optar al título de Especialista en Seguridad de la Información

Docente

DIEGO OSORIO REINA
M.SC. EN SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

UNIVERSIDAD CATÓLICA DE COLOMBIA

FACULTAD DE INGENIERÍA

PROGRAMA DE ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

BOGOTÁ D.C

AÑO

2020

Dedicatoria

A la persona más importante en mi vida Ana María Montenegro, Madre, amiga y confidente, mis hermanas personas incondicionales en mi trayectoria personal y profesional.

Juan Carlos López Montenegro

A mi esposa y a mis hijos por ser el complemento de mi vida, gracias por su comprensión y apoyo durante todo este tiempo, y en especial a mi mamá, por asumir el papel de madre y padre a la vez, gracias por inculcarme valores y principios, por enseñarme a enfrentar la vida con valentía.

Sergio Rodríguez Andrade

Agradecimientos

A la universidad católica de Colombia por presentarnos docentes incomparables, Tutores Ingeniero Fernando Pérez por su incondicional apoyo, Ingeniero Diego Osorio Reina por ampliarnos un mundo fascinante orientado en la ciberseguridad.

TABLA DE CONTENIDO

Pág.

LISTA DE ILUSTRACIONES

LISTA DE TABLAS

LISTA DE MATRICES

LISTA DE GRAFICAS

1. INTRODUCCIÓN

Los ataques cibernéticos ocurren cada vez con más rapidez, evolución y difusión en cuestión de segundos logran vulnerar sistemas, por colocar un ejemplo, unos de los malware más catastróficos que existen en la actualidad (Ransomware - Filecoder), es ejecutado con el objetivo principal de secuestrar la información, para luego chantajear la víctima y solicitar un monto de dinero en bitcoins como condición para liberar la información.

Para prevenir estas amenazas las organizaciones gastan recursos implementando nuevos modelos de seguridad, donde los equipos de seguridad de la información luchan por reaccionar a tiempo, sin embargo, los atacantes aprendieron a moverse con nuevas técnicas sofisticadas evadiendo muchas posibles defensas, como las humanas, las ubicadas en el perímetro, en la red o en la estación de trabajo.

Es por lo que Mitre Corporation desde sus inicios, ha dedicado esfuerzos en investigar y producir soluciones para un mundo seguro, destacándose la base de datos mundial de vulnerabilidades CVE (Comon Vulnerabilities and Exposure), y en ese sentido ha documentado y catalogado el comportamiento de los ciber adversarios bajo sus técnicas y tácticas, consolidándolos en una matriz denominada ATT&CK (Adversarial Tactics, Techniques & Common Knowledge), para que cualquier organización, sin importar su tamaño y tipo de negocio, pueda identificar sus reales amenazas y tomar medidas para estar un paso delante del cibercrimen.

Mitre extendió aún más su trabajo involucrando la emulación de adversarios, con el Software Mitre Caldera, el objetivo es verificar las defensas de una organización simulando la información de Mitre ATT&CK, específicamente los ataques de grupos de ciberdelincuentes identificados y catalogados en ATT&CK.

2. GENERALIDADES

1. LÍNEA DE INVESTIGACIÓN

En el programa se trabaja sobre Software Inteligente y Convergencia Tecnológica.

2. PLANTEAMIENTO DEL PROBLEMA

A pesar de las múltiples estrategias del actual ecosistema de soluciones de seguridad de la información y ciberseguridad, compuesto por aspectos procedimentales y técnicos, como normativas, estándares, regulaciones, políticas, sistemas de gestión, directrices, buenas prácticas, guías y una gran variedad de controles técnicos de múltiples fabricantes, todos encaminados a un solo objetivo, la protección de la información. La sociedad tecnológica está siendo víctima de ciberdelincuentes y amenazas informáticas, ocurriendo hoy en día, secuestros informáticos de ciudades, corporaciones y ciudadanos, robo y publicación de millones de registros confidenciales, espionaje, desviación de fondos bancarios, robos electrónicos de millones de dólares y un incesante intento de engañar a los seres humanos a través de correos electrónicos con fines delincuenciales.

2.2.1 Antecedentes del problema

El cibercrimen es la mayor amenaza para todas las empresas en el mundo y uno de los mayores problemas de la humanidad. El impacto en la sociedad se refleja en números, la organización Cybersecurity Ventures quien se especializa en investigar el actual entorno de cibercrimen e incluso sus implicaciones económicas, “predicen que el cibercrimen le costará al mundo más de $6 billones anuales para 2021 frente a $ 3 billones en 2015". [36]

Para cualquier organización, este tipo de conductas incluye daños y destrucción de datos, chantaje, ransomware, robo de dinero, pérdida de productividad, robo de información clasificada, fraude cibernético, intrusiones no autorizadas, criptominería, Ransomware, APTS (amenazas persistentes avanzadas) y una consecuencia aún mayor, pérdidas económicas y de reputación.

Solo basta con verificar ataques como el que sufrió la cadena de Hoteles Marriot, en el que se filtró información personal de aproximadamente 500 millones de clientes o la brecha de seguridad de la multinacional Yahoo que afectó a más de 3.000 millones de cuentas de usuarios en todo el mundo y por supuesto, como no olvidar la compañía de reputación financiera de ciudadanos de US, Equifax que sufrió un incidente que dio a los cibercriminales acceso a datos de 143 millones de ciudadanos americanos.

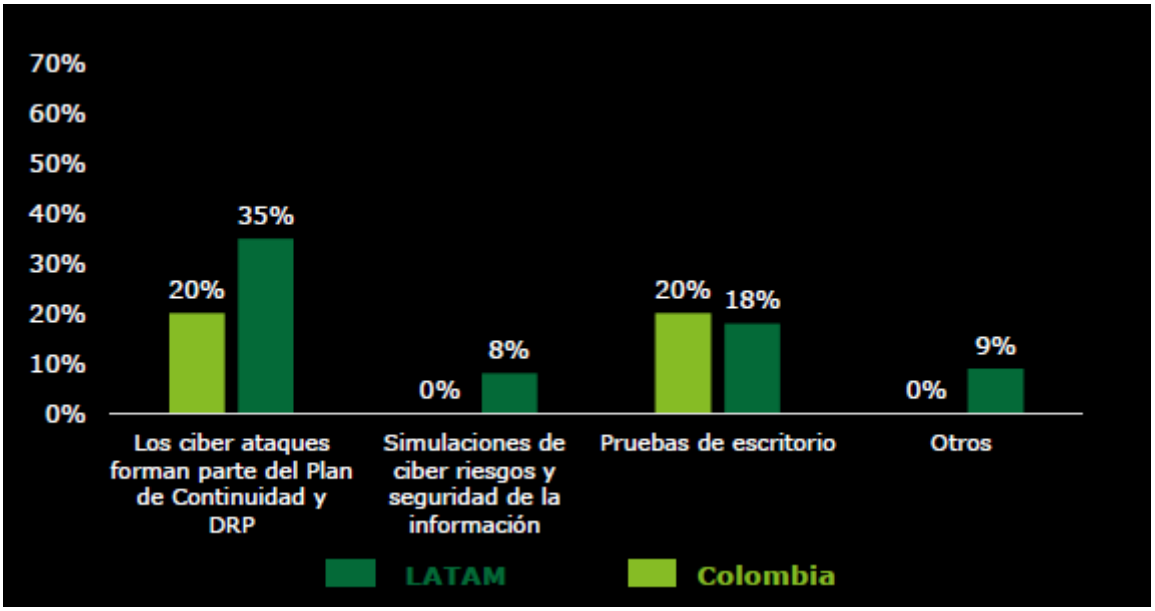
Para redondear las cifras la organización Deloitte, realizó en el mes de abril del 2019 un estudio regional para América Latina y el caribe (AL&C) identificando las siguientes amenazas:

1. “4 de cada 10 organizaciones sufrieron un incidente de ciberseguridad en los últimos 24 meses.
2. Las organizaciones en América Latina están incrementando sus presupuestos dedicados a gestionar ciber riesgos y seguridad de la información.
3. Las organizaciones cuentan con capacidades limitadas de monitoreo de ciberseguridad e inteligencia de amenazas.
4. Casi 7 de cada 10 organizaciones han implementado un programa de concientización en ciberseguridad.” [3]

Este estudio regional para América Latina y el caribe (AL&C) también revela que más de la mitad de las organizaciones en AL&C no han incorporado el ciber espacio dentro de sus programas de continuidad de negocio, y sólo un 3% de las organizaciones realiza algún tipo de simulación de un incidente en los activos que interactúan con el ciberespacio, para validar su nivel de preparación y respuesta” [4].

Las empresas asumen que una vez se aplican las acciones o los controles para mitigar las amenazas de acuerdo con sus sistemas de gestión de seguridad y procesos de evaluación de riesgos, estos funcionaran de forma correcta pero como se evidencia en el estudio regional para América Latina y el caribe (AL&C), no se realizan pruebas para validar que tan efectivas son ante una amenaza real, esto se plasma en la ilustración 1.

Ilustración 1. Ciberseguridad como Parte del Programa de Continuidad de Negocios por la firma Deloitte



Fuente: DELOITTE,Deloitte "Ciber Riesgos y Seguridad de la Información en América Latina & Caribe Tendencias 2019".{En línea}. {10 septiembre de 2019} disponible en: (https://www2.deloitte.com/content/dam/Deloitte/co/Documents/risk/Cyber%20Survey%20LATAM%20-%20Colombia%20v2.pdf) 33 P.

En Colombia el monto de pérdidas varía según el tamaño de la empresa, pero está en un rango entre 120 millones a 5.000 millones de pesos, cifras reportadas por la fiscalía general de la nación de acuerdo con la publicación realizada por el CCTI (Cámara Colombiana de informática y telecomunicaciones), en el estudio de tendencias del cibercrimen en Colombia.

"Actualmente, el 45.5% de las denuncias se hacen por canales virtuales y en el transcurso de 2019, se han reportado 28.827 incidentes de ciberseguridad empresarial en el país, de los cuales 17.531 casos han sido denunciados ante la fiscalía." [1]

"En los últimos 2 años se han reportado 52.901 denuncias, donde la mayoría de los hurtos se realizan utilizando medios informáticos con 31.058 denuncias y el robo de identidad con 8.037 denuncias, las principales ciudades que reportan estos incidentes son Bogotá con 5.308, Cali 1.190 y Medellín 1.186". [2]

2.2.2 Pregunta de investigación

A pesar de los múltiples controles que proporciona la disciplina de la seguridad de la información, la sociedad está siendo víctima de una creciente avalancha de

violaciones de seguridad, ¿Qué estrategias debería tomar las organizaciones para ir un paso adelante de los ciberdelincuentes, y así elevar sus niveles de defensa?

2.2.3 Variables del problema

Sistemas de detección y atención de incidentes: Nivel de preparación que tiene la organización frente a un incidente y la forma en la que detecta una posible violación, el cual modificara los niveles de detección en sus defensas de acuerdo con la emulación de adversarios.

Riesgo: Esta variable se modifica de acuerdo a lo observado en el comportamiento de la emulación de adversarios, las vulnerabilidades y amenazas detectadas en los sistemas expuestos a los APT, reducirán su probabilidad de ocurrencia y el impacto en la organización ACME.

3. JUSTIFICACIÓN

El presente proyecto pretende contribuir al desarrollo de nuevas técnicas de ciberdefensa, debido a que el panorama actual es catastrófico y las estimaciones a futuro son negativas. Sin importar que muchas organizaciones contemplan un plan de buenas prácticas como normativas, legislaciones, controles, así como la adquisición de sistemas para la seguridad, como lo son, Firewall, Antivirus, IPS, IDS, prevención de fuga de información, cifrado y continúan siendo víctimas de cibercriminales o ciberterroristas.

Razón por la cual se plantea implementar una nueva estrategia como la que presenta el framework MITRE ATT&CK e implementando el sistema de emulación de adversarios Mitre CALDERA (Cyber Adversary Language and Decision Engine for Red Team Automation), cuyo objetivo es probar soluciones de seguridad en estaciones de trabajo final y servidores, ayudando a detectar técnicas identificadas a nivel mundial por profesionales de la primera línea de batalla contra los cibercriminales, comprobando y mejorando las defensas antes de que un atacante las explote.

Para concluir por políticas de confidencialidad de la organización se oculta su nombre real, y para el desarrollo de este proyecto se denomina **ACME**, no obstante la empresa donde se despliega el proyecto MITRE CALDERA está legalmente constituida en Colombia y su negocio es la venta de software de ciberseguridad, uno de los autores de este proyecto labora en esta organización.

4. OBJETIVOS

1. OBJETIVO GENERAL

Comprender el proyecto Mitre ATT&CK y demostrar su aplicación a través de procesos de emulación de adversarios.

2. OBJETIVOS ESPECÍFICOS

- Comprender el framewok MITRE ATT&CK.
- Utilizar la base de conocimientos de MITRE ATT&CK para identificar comportamientos utilizados por adversarios.
- Realizar una prueba de concepto de emulación de adversarios soportada en MITRE ATT&CK con la herramienta MITRE CALDERA simulando tres APT´S.
- Utilizar la retroalimentación de los ejercicios MITRE CALDERA para elevar la posición de defensa de la organización evaluada.
- Dar visibilidad de la existencia del proyecto MITRE ATT&CK.

5. MARCOS DE REFERENCIA

1. MARCO CONCEPTUAL

Cuando se habla de retos en ciberseguridad uno de los problemas es determinar qué actor está detrás de los ataques, comúnmente conocido como Ciberdelincuente, cuáles son sus motivaciones, y sobre todo preguntarse ¿cómo logró sobrepasar los controles de seguridad de la organización?

Actualmente las industrias de ciberseguridad han venido desarrollando nuevos sistemas de defensa con el propósito de aumentar la visibilidad y perfilando de adversarios, una de ellas es la organización Mitre con su Framework ATT&CK (Adversary tactics, techniques and common knowledge), el cual consiste en un repositorio de información que contiene técnicas, tácticas y procedimientos que suelen utilizar los ciberatacantes, información recolectada a partir de observaciones del mundo real, permitiendo así comprender el comportamiento de adversarios.

Mitre ATT&CK permite que las capacidades defensivas mejoraren ya que se cuenta con un enfoque holístico involucrando los siguientes casos de uso.

- **Simulación de adversarios**: permite simular técnicas y tácticas de los APT (Advanced Persistent Threat) para MItre son (conjuntos de actividades de intrusión relacionadas con un nombre común en la comunidad de seguridad como por ejemplo APT41, APT19)
- **Pruebas de funcionalidad de soluciones de seguridad**: los casos más usados son las verificaciones de detección y prevención de las soluciones de seguridad de la organización.
- **Entendimiento de un ciberataque**: cuando se realiza un monitoreo de seguridad los primeros pasos es detectar eventos observados y atarlos a una cadena de acciones de un adversario.
- **Threat Hunting** cuyo inicio fue para inteligencia militar se basa en el proceso de búsqueda de amenazas persistentes capaces de evadir las soluciones de seguridad existentes

Teniendo en cuenta los factores determinantes anteriormente explicados, la organización Mitre creó un software con licencia apache 2.0 (libre de pago, pero con limitaciones), de emulación de adversarios llamado CALDERA que se soporta sobre Mitre ATT&CK, cuyo propósito es ayudar a las organizaciones a incrementar sus niveles de defensa en ciberseguridad ahorrando recursos y automatizando tareas de emulaciones de adversarios.

2. MARCO TEÓRICO

Para abordar este proyecto es necesario hablar de otros modelos de adversarios y poder dar otros enfoques existentes, las cuales pueden ayudar a las organizaciones para tener esquemas de protección basados en métodos científicos orientados a la caza de amenazas o el denominado threat hunting.

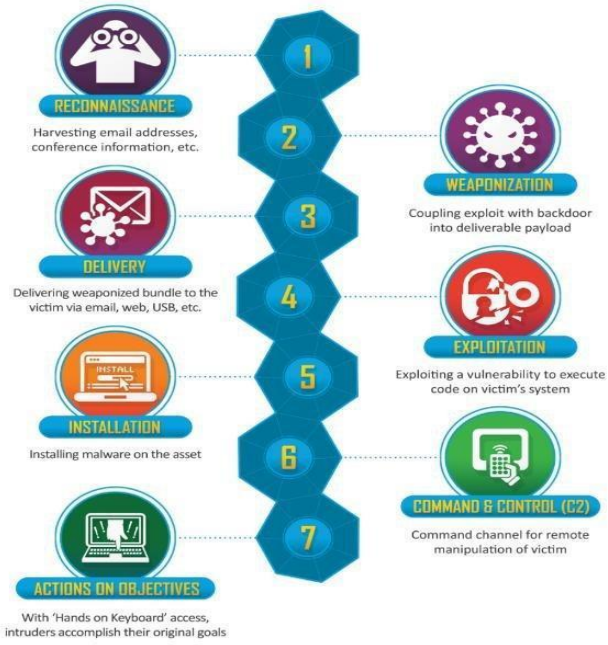
2.2.1. Modelos de adversarios.

Entre los modelos más conocidos está, Cyber Kill Chain de Lockheed Martin, el ciclo de vida de Mandiant Attack, cabe aclarar que el objetivo es demostrar la efectividad de Mitre ATT&CK.

2.2.2. Cyber kill chain de lockheed martin

Uno de los primeros modelos conocidos es la cadena de Cyber kill chain desarrollado Lockheed Martin este modelo describe las actividades de un ciberdelincuente desde su inicio hasta la finalización del ataque.

Ilustración 2. Fases de ataque en la cadena Cyber Kill Chain



Fuente: Lockheed Martin Corporation,Lockheed Martin Corporation "the Cyber Kill Chain".{En línea}. {10 septiembre de 2019} disponible en: (https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html)

Las técnicas están dadas para describir los ataques y se compone de 7 tácticas que son las siguientes:

1. Reconocimiento: El atacante estudia su objetivo, identifica sus vulnerabilidades.

2. Armamento: El atacante diseña un malware para acceder al organismo objetivo.

3.Entrega: Hay que hacer llegar el malware al objetivo, hay que infectar al objetivo.

4. Explotación: El malware se ejecuta dentro de la organización y consigue el acceso deseado por parte del atacante.

5.Instalación: Habitualmente un atacante requiere de acceso continuo a su objetivo, para ello instala puertas traseras o vías de acceso a la red de su objetivo.

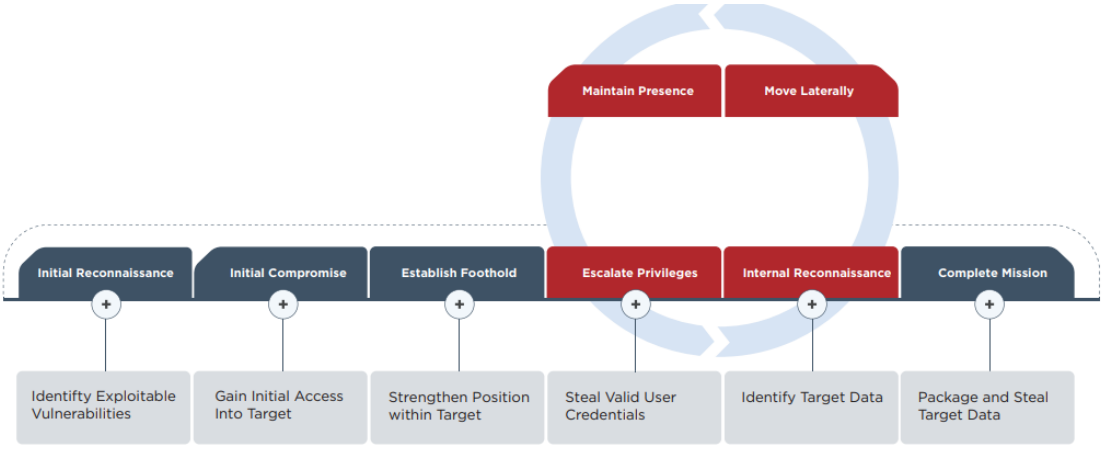
6. C&C: El malware instalado debe permitir realizar acciones complejas dentro de la infraestructura del objetivo.

7. Exfiltración: Finalmente los atacantes extraen información del objetivo, normalmente información crítica y de alto valor.

2.2.3 El ciclo de vida de mandiant attack

El ciclo de vida de Mandiant Attack construido por la organización FireEye, proporciona un modelo de ataque Cibernético que describe el ciclo de vida de un ataque desde la experiencia vista por esta organización, el objetivo de este ciclo de vida es la detección temprana de adversarios.

Ilustración 3. Ciclo de vida de Mandiant Attack



Fuente: FireEye, FireEye "Threat Research".{En línea}. {22 febrero de 2020} disponible en:(https://www.fireeye.com/blog/threat-research/2019/09/sharpersist-windows-persistence-toolkit.html)

Las fases aplicadas son**:**

1. Reconocimiento inicial: el adversario utiliza técnicas de investigación sobre la organización.

2. Compromiso inicial: el adversario ejecuta con éxito código malicioso en uno o más sistemas. Lo probable es que esto ocurra a través de la ingeniería social.

3. Establecer un Rollback Los adversarios se aseguran de conservar un control continuo sobre un sistema comprometido.

4. Escalada de privilegios: los adversarios obtienen un mayor beneficio escalando privilegios mediante el DUMP de hash de contraseña.

5. Reconocimiento interno: El adversario explora el entorno de la víctima para comprender mejor el entorno.

6. Moverse lateralmente: paso crítico en las compañías usa sus credenciales obtenidos en la elevación de privilegios para moverse de un sistema a otro dentro del entorno comprometido.

7. Mantener la presencia: Garantiza el acceso continuo al entorno. Los métodos comunes incluyen instalación de múltiples variantes de puertas traseras Caballos de troya (RAT).

8. Misión completa: El ciberdelincuente logra su objetivo, robar propiedad intelectual, datos financieros, información crítica, identificación personal.

2.2.4 ¿Por qué Mitre ATT&CK?

“El marco de ciberseguridad de Mitre ATT&CK, es una base de conocimiento de las tácticas y técnicas utilizadas por los atacantes, continúa ganando terreno a medida que los proveedores, empresas y proveedores de servicios de seguridad adoptan y adaptan el marco a sus defensas.” [7]

A diferencia de marcos de seguridad más conocidos como Cyber Kill Chain de Lockheed Martin, o el ciclo de vida de Mandiant Attack, Mitre ATT&CK se diferencia y toma ventaja ya que detalla cómo se puede ejecutar un ataque de un adversario, proporcionando mayor información. La cadena Kill Chain de Lockheed Martin, por ejemplo, proporciona las diferentes fases de un ataque, como lo vería un defensor:

“Solo están escaneando una red como una fase de reconocimiento (aún no han logrado entrar, o tal vez hayan entrado y se hayan movido por la red, y ahora están filtrando datos”. [8]

Esto ayuda al defensor a poder realizar una detección y saber las capacidades de respuesta y poder identificar qué tan lejos están en la red y qué tan lejos ha llegado su ataque.

Una debilidad de Lockheed Martin Kill Chain es que la información de los ataques no es muy completa desde la perspectiva del adversario, por el contrario, el modelo Mitre ATT&CK brinda detalles del completo desarrollo de la amenaza. El modelo Mitre ATT&CK explica detalladamente cómo se puede ejecutar un ataque, cómo se obtiene acceso inicial y cómo se mantiene un ataque persistente. Cuenta con todos estos elementos que permiten a las organizaciones rastrear las técnicas y tácticas que emplean los adversarios en una red para detectar y monitorear las respuestas disponibles.

Además, proporciona un fortalecimiento de habilidades de ciberseguridad que facilitan el elegir o seleccionar qué tecnologías de detección, monitoreo y prevención se pueden implementar para remediar estos inconvenientes.

3. MARCO JURÍDICO

Este proyecto busca utilizar leyes y artículos colombianos orientadas a la seguridad de la información como base primordial, es por esto por lo que la ley 1273 de 2009 cuyo objetivo es “declarar conductas relacionadas con el manejo de datos personales se blinden jurídicamente” [10] evitando que un ciberdelincuente utilice los siguientes puntos:

1- Artículo 269A: ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO. El que, sin autorización o por fuera de lo acordado

2- Artículo 269B: OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático,

3- Artículo 269C: INTERCEPTACIÓN DE DATOS INFORMÁTICOS

4- Artículo 269D: DAÑO INFORMÁTICO

5- Artículo 269E: USO DE SOFTWARE MALICIOSO. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso

6- Artículo 269F: VIOLACIÓN DE DATOS PERSONALES. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue,

modifique o emplee códigos personales

7- Artículo 269G: Suplantación de sitios web para capturar datos personales. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes

Es por esto por lo que la emulación de adversarios ayudará a las organizaciones al cumplimiento de leyes y normativas locales puesto que se verifica las posibles fallas de su área de seguridad corporativa contra riesgos y vulnerabilidades antes de que un ciberdelincuente las encuentre protegiendo la confidencialidad, integridad y disponibilidad del activo más importante de las organizaciones la información.

4. ESTADO DEL ARTE

La organización Mitre realizó un experimento en un entorno de investigación en el año 2010 llamado Fort Meade de MITRE (FMX), en donde se evidenció que no se tenía una clasificación sistemática del comportamiento adversario como parte de la ejecución de ejercicios estructurados de emulación. A partir de esta necesidad fue creado ATT & CK.

FMX se desarrolló realizando pruebas en tiempo real, lo cual permitió a los investigadores lograr acceder al entorno de la red corporativa de MITRE, para implementar herramientas, probar y clasificar ideas sobre cómo detectar mejor las amenazas.

A partir de esto, MITRE comenzó a investigar diferentes fuentes de datos y análisis de procesos dentro de FMX, para detectar las amenazas persistentes avanzadas (APT) de una manera más eficaz aplicando un pensamiento de "asumir las consecuencias". Los ejercicios de este experimento cibernético se realizaron en unas bases periódicas para emular a los adversarios dentro del entorno altamente sensible, y a la defensa que era efectuada para probar hipótesis analíticas contra los datos recopilados.

El objetivo de estos ejercicios era corregir mediante mejoras, la detección al momento de que la amenaza se efectuaba y lograba penetrar las redes empresariales a través del descubrimiento de telemetría y análisis de comportamiento. La métrica principal para el éxito fue "¿Qué tan bien lo estamos haciendo detectando un comportamiento adversario documentado?” [37] Para trabajar eficazmente hacia ese objetivo, se aclaró que era útil clasificar el comportamiento observado en los grupos adversarios relevantes del mundo real y utilizar la información para llevar a cabo ejercicios controlados que emulen a estos dentro del ambiente FMX.

Ambos equipos, el de emulación de adversario (para el escenario de desarrollo) y el defensor (para la medición analítica del progreso) utilizaron ATT & CK, que los convirtió en una fuerza impulsora dentro de la investigación FMX.

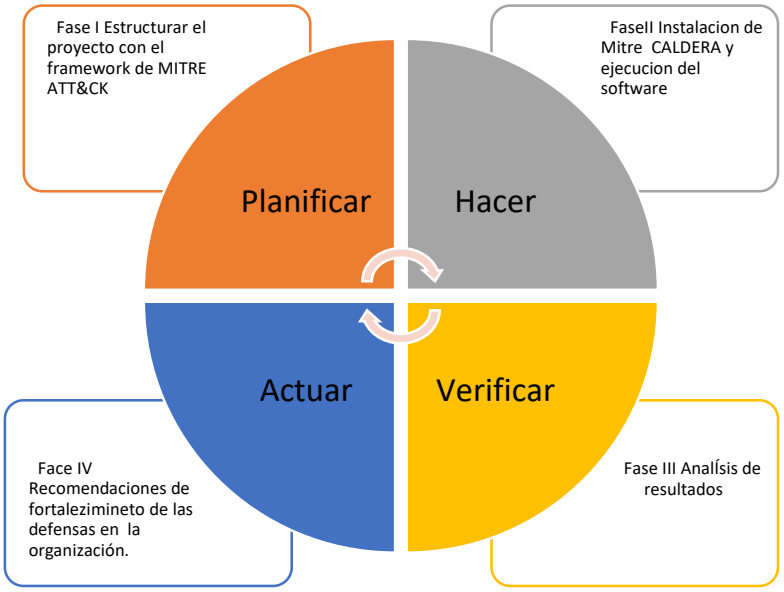
ATT & CK realizó su primer modelo en septiembre de 2013, centrándose especialmente en el entorno empresarial de Windows. Con el transcurso del tiempo se fue perfeccionando aún más a través de la investigación y los desarrollos internos, una vez se obtuvo una mejora inminente se realizó el lanzamiento de forma pública en mayo de 2015 con 96 técnicas organizadas bajo 9 tácticas. Desde la fecha anterior, ATT & CK ha experimentado una evolución y crecimiento teniendo en cuenta las colaboraciones y contribuciones de la comunidad de ciberseguridad a nivel mundial. Partiendo de la metodología base utilizada para llevar a cabo el primer modelo ATT & CK, se creó un complemento de la fuente de conocimiento llamado PRE-ATT & CK, que se enfoca en el comportamiento “a la izquierda del exploit" antes del ataque. En abril de 2018, Enterprise ATT & CK amplió su base de conocimiento donde incluye 219 técnicas en Windows, Linux y Mac” [38], en 2019 se liberó ATT&CK mobile y en el 2020 durante la ejecución del presente proyecto se liberó el framework beta para sub-técnicas.

6. METODOLOGÍA

Este proyecto se centra en una metodología cualitativa, basándose en aspectos observables y comportamentales como la recolección de indicadores de la herramienta Mitre Caldera, con la que se pretende llegar a un resultado de creación de nuevos protocolos y contramedidas de aseguramientos de Ciberseguridad para la organización ACME, teniendo como objetivo principal la simulación adversaria.

6.1. FASES DEL TRABAJO DE GRADO

Ilustración 4. Fases de trabajo



Fuente: Autores

FASE I. Estructurar el proyecto con framework de MITRE ATT&CK: Se recolectará toda la información de que es Mitre ATT&CK como principio base de este proyecto.

FASE II. Instalación de mitre caldera y ejecución de software: Fase de selección de técnicas y tácticas para verificar las defensas, ejecutando los agentes en estaciones de trabajo y servidores.

FASE III. Análisis de resultados: Con esta fase se estudiarán los resultados encontrados en las estaciones de trabajo y así documentar los sistemas de defensa con problemas detectados.

FASE IV. Recomendaciones para aumentar los niveles de defensa de la

organización: Con esta fase se realiza recomendaciones para mitigar las falencias detectadas en la emulación de adversarios, con el fin de aumentar las defensas en la organización ACME basados en recomendaciones de MITRE ATT&CK.

6.2. INSTRUMENTOS O HERRAMIENTAS UTILIZADAS

Las herramientas que se van a utilizar son las siguientes:

1. Servidor Principal: Servidor con sistema operativo Ubuntu, en donde se instalará el software Mitre Caldera.

2. Host de destino: Equipos con sistema operativo Windows (server, workstation) en los que se desplegará los agentes de Mitre Caldera para realizar las pruebas.

3. Controlador de Dominio: Servidor principal de una red donde se establece una estructura jerárquica que relaciona diferentes componentes de la misma como son los grupos, usuarios, conjunto de usuarios, políticas, permisos y privilegios.

4. Mitre Caldera: Software que se utiliza para probar soluciones de seguridad de punto final y evaluar la postura de seguridad de una red frente a las técnicas adversas comunes posteriores al compromiso contenidas en el modelo ATT & CK.

5. Internet: Se requiere internet para descargar las principales actualizaciones en el proceso de instalación de Caldera.

6. Matriz Mitre: incluye las técnicas y tácticas que contienen las plataformas de Windows, Linux y MAC, que se utilizan para guiarse en los métodos de ataque conocidos.

7. Microsoft Office: Software que contiene una suite completa de herramientas ofimáticas como Word, Excel, Powerpoint, Project, entre otras; que es usado para la parte de documentación y elaboración del anteproyecto.

6.3. POBLACIÓN Y MUESTRA

Para conocer la población y muestra se efectuará los siguientes análisis.

6.3.1. Población

Segmentación de la población: La población se encuentra conformada por 10 equipos asignados por la organización ACME para realizar la fase de implementación del proyecto.

6.3.2. Muestra

Método de la significancia: Para determinar el tamaño adecuado de la muestra se hace uso del método probabilístico de significancia. Este método se usa cuando se conoce el tamaño de la población, aplicando la siguiente fórmula:

$$\mathbf{n} = \frac{\mathbf{Z^2 * p * q * N}}{\mathbf{e^2(N-1) + Z^2 * p * q}}$$

N = tamaño de la población
Z = nivel de confianza
p = probabilidad de éxito, o proporción esperada
q = probabilidad de fracaso (1-p)
e = Margen de error

Solución:
Tamaño de la población (N)= 10
Nivel de confianza = 95%
Margen de error e =1%
P = 0.5 por defecto
Q= 1-0.5 = 0.5

$$n = \frac{95^2 \times 0.5 \times 0.5 \times 10}{1^2(10-1) + 95^2 \times 0.5 \times 0.5}$$

n = 9.96 ≈ 10
El tamaño de la muestra da como resultado 10

6.3.3. Diagnóstico de la muestra

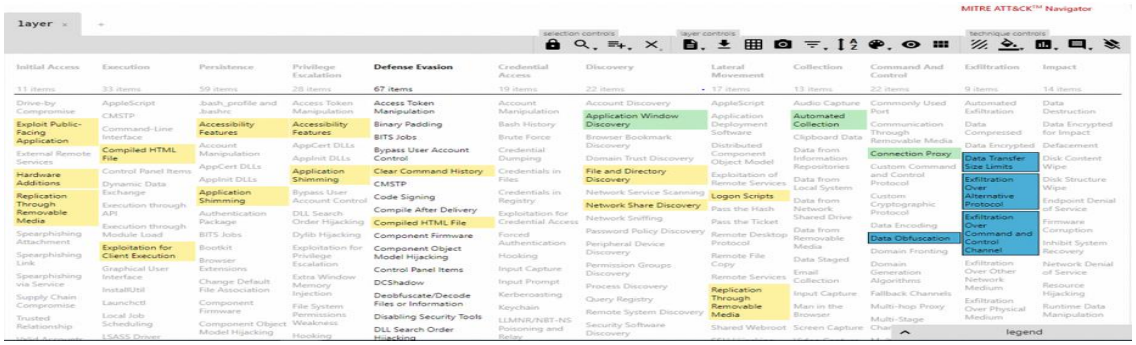
Se debe implementar el software de Mitre Caldera en las 10 estaciones de trabajo que se asignan por la organización ACME.

6.4. Alcances y limitaciones

Se pretende dar visibilidad del framework Mitre ATT&CK y la herramienta Mitre Caldera como una solución o recurso innovador en ciberseguridad, diferente a los ya conocidos (ISO 27001, PCI-DSS, antivirus, proxies, firewalls, IPS, IDS, etc) para evaluar el nivel de defensas de una organización; por otra parte brindar un conocimiento sobre amenazas informáticas, ayudar a describir las acciones adversas de forma estándar, realizando un seguimiento donde se asocien con las técnicas y tácticas de ATT&CK (ilustración 5) por las que son conocidos. Expuesto lo anterior, se busca mejorar los procesos de defensa identificando el origen de las debilidades, evidenciando y dando a conocer los riesgos y los posibles impactos que estos puedan representar, para aplicar controles operacionales en las políticas de seguridad de la organización.

El alcance de este proyecto está relacionado con los objetivos generales y específicos ya nombrados, se implementará una POC en la cual se validarán las defensas de las estaciones de trabajo en la organización ACME con herramientas de emulación de adversarios, donde se entregará un informe de lo detectado junto a las técnicas y tácticas utilizadas. De acuerdo a las políticas de la organización, la emulación de adversarios utilizando Mitre Caldera, solo se puede ejecutar en un máximo de 10 equipos. De igual forma las tácticas y técnicas empleadas se limitan a las establecidas por el fabricante Mitre.

Ilustración 5. Tácticas y Técnicas de Mitre



Fuente: Welivesecurity, Welivesecurity "Cómo utilizar MITRE ATT&CK".{En línea}.{10 septiembre de 2019} disponible en:(https://www.welivesecurity.com/la-es/2019/06/06/como-utilizar-mitre-attck-repositorio-tecnicas-procedimientos-ataques-defensas)

7. PRODUCTOS A ENTREGAR

Este trabajo de grado está bajo el contexto del objetivo general y específicos, los productos a entregar son:

- Documentación de la ejecución: Para este punto se demuestra la ejecución de las técnicas LAZARUS, APT41, ATP19 en la organización ACME.

- Resultados: Se presentará datos de las diferentes técnicas y tácticas ejecutadas en nueve estaciones de trabajo y un servidor para evidenciar la posible falla de seguridad.

- Recomendaciones: se presentará recomendaciones según MITRE para lograr un mejor aseguramiento de los sistemas de defensa que tiene las estaciones de trabajo, servidores.

- Artículo IEEE: Se presentará artículo a la comunidad en general realizando el desarrollo de la emulación de adversarios a través de la emulación de adversarios.

8. ENTREGA DE RESULTADOS E IMPACTOS

8.1 ¿QUE ES ATT & CK?

Para abordar el ATT&CK se conoce como Tácticas, Técnicas y Conocimiento Común de Adversarios fue desarrollado por la organización MITRE, el objetivo es describir y categorizar comportamientos adversos basados en observaciones de ciberataques en todo el mundo, su estrategia se basa en los siguientes ítems:

- Que es una táctica**:**

“Las tácticas representan el "por qué" de una técnica o sub-técnica ATT & CK. Es el objetivo táctico del adversario: la razón para realizar una acción, Por ejemplo, un adversario puede querer obtener acceso de credenciales.” [19].

- Que es una Técnica:

“Las técnicas representan "cómo" un adversario logra un objetivo táctico al realizar una acción.” [20]

Ejemplo un adversario puede realizar conductas de DUMP para lograr el acceso a las credenciales.

- Sub-técnicas:

“Las sub-técnicas son una descripción más específica del comportamiento del adversario utilizado para lograr un objetivo. Describen el comportamiento en un nivel más bajo que una técnica” [21].

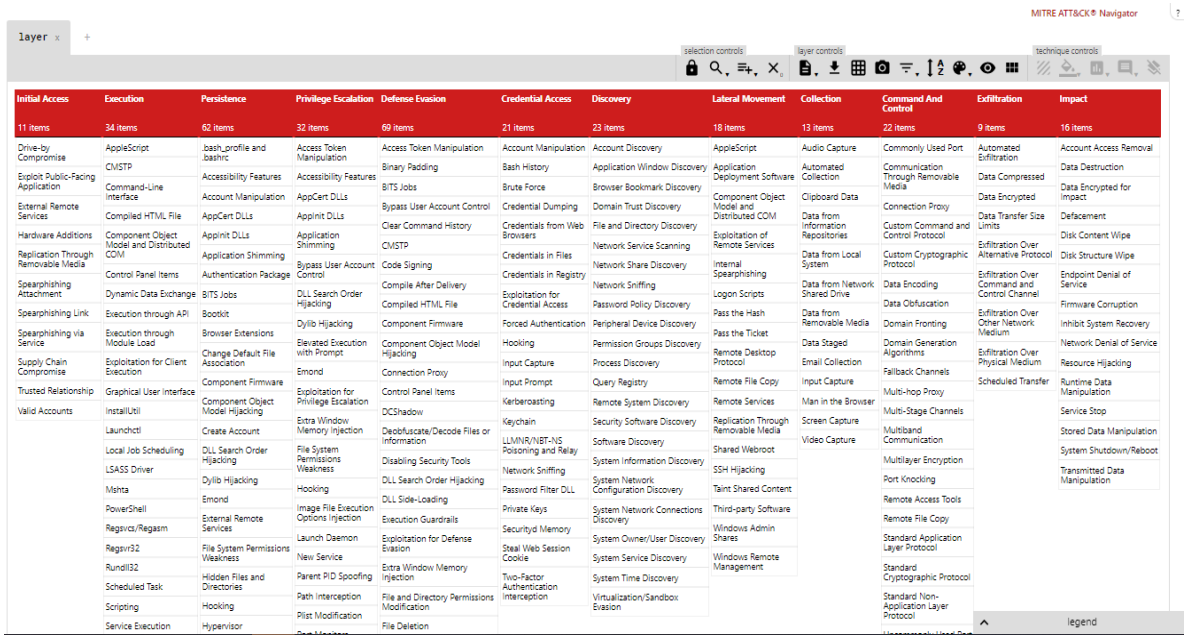
Por ejemplo, un adversario puede realizar conductas de DUMP a las credenciales accediendo a los servicios de la Autoridad de Seguridad Local (LSA).

- Los procedimientos

“Son la implementación específica que el adversario usa para técnicas o sub-técnicas” [22]. Por ejemplo, un procedimiento podría ser un adversario que usa PowerShell para inyectar en lsass.exe y realizar conductas de DUMP a credenciales.

La Matriz ATT&CK contiene 12 tácticas (sección de color Rojo) y las filas (sección de color blanco) contienen 331 técnicas, clasificadas según el modo operandi que utiliza los Ciber terroristas. se demuestran en la ilustración 6.

Ilustración 6. Matriz ATT&CK para empresas



Fuente: The MITRE Corporation. MITRE ATT&CK and ATT&CK "Enterprise Matrix".{En línea}.{22 febrero de 2020} disponible en:(https://attack.mitre.org/matrices/enterprise/)

8.1.1 ¿Qué es mitre caldera?

Es un proyecto con fines investigativos desarrollado por la organización MITRE. El cual elaboró un software que se basa en el marco de seguridad cibernética de MITRE ATT & CK, con el fin de ejecutar de forma sencilla ejercicios autónomos de simulación de ataques. También es usado para ejecutar simulaciones manuales del equipo rojo o una respuesta automática a incidentes.

Componentes de Caldera

"El sistema central: Este es el código marco, que consta de lo que está disponible en este repositorio. Se incluye un servidor asíncrono de comando y control (C2) con una API REST y una interfaz web.

Plugins: Estos son repositorios separados que cuelgan del marco central, proporcionando funcionalidad adicional. Los ejemplos incluyen agentes, interfaces GUI, colecciones de TTP y más." [6]

8.1.2 Metodología de emulación

La metodología utilizada para la emulación de adversarios con mitre Caldera en la organización ACME, se basa en los siguientes procesos.

Ilustración 7. Procesos de Mitre

Fuente: The MITRE Corporation, attack.mitre.org "GETTING STARTED WITH".{En línea}.{22 febrero de 2020} disponible en: (https://www.mitre.org/sites/default/files/publications/mitre-getting-started-with-attack-october-2019.pdf) página 26

1. Recopilar información sobre amenazas: En esta fase se verificará la selección de un adversario en función del core del negocio de organización ejemplo Farmacéutica tecnología, banca, retail.

2. **Técnicas de extracción**: En esta fase se selecciona la información, las técnicas se van a especificar para verificar los puntos de ataque que se consideran débiles en la organización.

3. **Analizar y organizar**: Con la información recolectada sobre el adversario y cómo operan, se debe organizar esa información en su flujo operativo de una manera que sea fácil de crear planes de emulación.

4. **Desarrollar herramientas y procedimientos**: descubrir cómo implementar el comportamiento es importante se debe considerar los siguientes puntos,

- ¿La técnica que se utilizó según el contexto del entorno?
- ¿Qué herramientas se puede usar para replicar estos TTP (táctica, técnicas y procedimientos)?

5. **Emular al adversario**: En esta fase se utilizará Mitre Caldera para emular los adversarios o APT´S. Una vez que se lleva a cabo todo este proceso, se verificará cuáles son las técnicas que se ejecutaron, y probaron las defensas contra los comportamientos del mundo real.

8.2. EMULACIÓN DE ADVERSARIOS

Para comenzar la emulación de adversarios se inicia con la instalación de Mitre CALDERA en un servidor virtual proporcionado por la organización ACME, para ver características del servidor ver tabla 2, en las primeras versiones de la herramienta, no se encontraba información sobre el proceso de instalación, para lo cual se realizó pruebas de ensayo y error de ejecución, los resultados para la instalación son los siguientes:

1. Instalar dependencias que utiliza CALDERA

   apt-get -y install python3-dev python3-pip git-core mongodb

2. Asegúrarse de que las herramientas de configuración estén actualizadas

   ```
   pip3 install --upgrade setuptools
   ```

3. Download CALDERA

   ```
   apt intall git

   git clone https://github.com/mitre/caldera
   ```

4. Instalar CALDERA. cd importante estar dentro de directorio caldera**/caldera**:

   ```
   pip3 install -r requirements.txt
   ```

5. Preparar base de datos

   ```
   echo "replSet = caldera" >> /etc/mongodb.conf
   ```

   Reinicie el servicio de base de datos systemctl restart mongodb.service.

6. Ejecute caldera desde el directorio **caldera/caldera**.

   ```
   python3 caldera.py
   ```

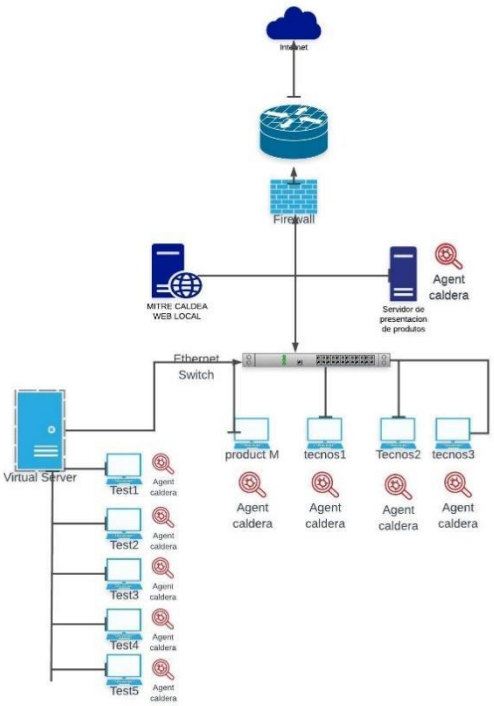
En las últimas versiones de caldera la versión 2.6, versión en el cual se basa este proyecto, el proceso de instalación es más sencillo, solo basta con tener

dependencias de PIP3 y python3-pip los comandos ejecutados para tener CALDERA son los siguientes:

```
mitre@mitre-virtual-machine:~$ sudo su
[sudo] contraseña para mitre:
root@mitre-virtual-machine:/home/mitre# history
    1  apt get pip3
    2  apt get install pip3
    3  git clone
    4  apt install git
    5  git clone --branch master https://github.com/mitre/caldera --recursive
    6  cd caldera/
    7  pipi3 install
    8  apt install pip3
    9  apt install python3-pip
   10  pip3 install -r requirements.txt
   11  python server.py
   12  python3 server.py
```

Para la ejecución de los ATP´S se dispone de una infraestructura donde se contempla máquinas físicas y virtuales de la organización ACME como se observa en la ilustración 8, que **por políticas de confidencialidad no se puede dar información adicional, por supuesto en la ejecución de técnicas y tácticas realizadas por la herramienta CALDERA no se mostraron en su totalidad ya que se obtiene información crítica de la organización, los APT LAZARUS, APT 41, APT 19 se diferenciaron debido a que estos grupos tienen como objetivos industrias orientadas a tecnología**, estas máquinas pertenecen al área de tecnología de la organización y son máquinas que están en uso cotidiano. También se obtuvo acceso a un servidor de virtualización donde están alojadas máquinas virtuales y su objetivo en la organización es probar software como si estuviera en entornos de producción.

Ilustración 8. Esquema de conectividad de estaciones de trabajo analizar.



Fuente: Autores

8.2.1 Características de las máquinas

Entorno físico

Tabla 1. Especificaciones técnicas entorno físico

Nombre	OS	RAM	Procesador	Disco Duro	Antivirus
Product M	Windows 10 actualizado	20	Intel Core I7 8 generación	SSD 512	SI
TECNOS1	Windows 10 actualizado	20	Intel Core I7 8 generación	SSD 512	SI
TECNOS2	Windows 10 actualizado	20	Intel Core I7 8 generación	SSD 512	SI
TECNOS3	Windows 10 actualizado	20	Intel Core I7 8 generación	SSD 512	SI

Fuente: Autores

Entorno virtual

Virtualizado vmware 6.7

Tabla 2. Especificaciones técnicas en entorno virtual

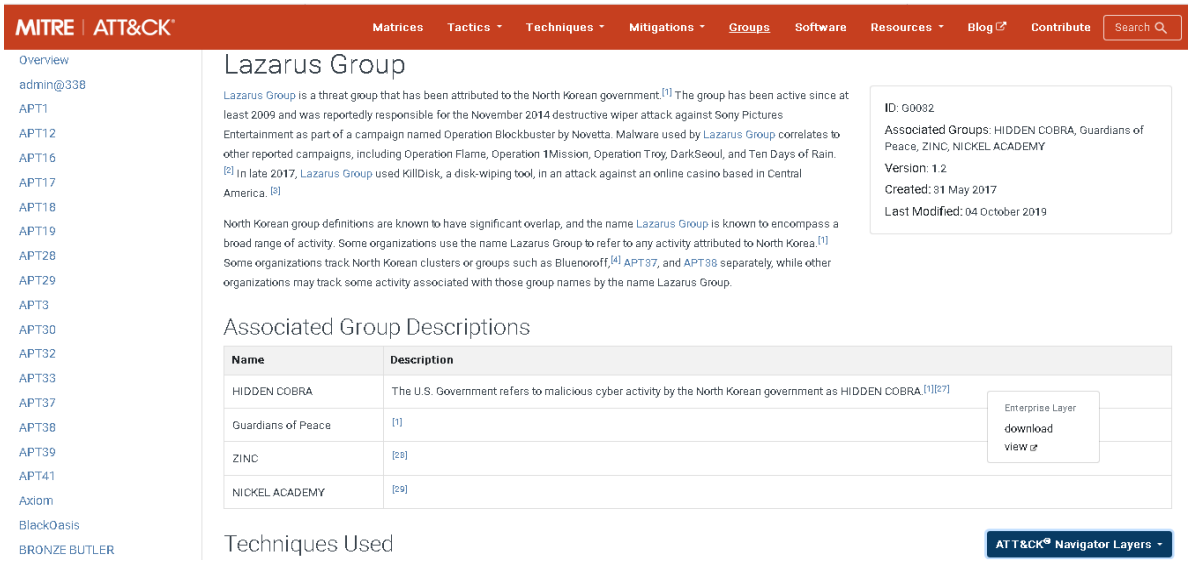
Nombre	OS	RAM	Procesador	Disco Duro	Antivirus
Test1	Windows 10 actualizado	4	INTEL XEON 2 CORES	DD 80 GB	SI
Test2	Windows 10 actualizado	4	INTEL XEON 2 CORES	DD 80 GB	SI
Test3	Windows 10 actualizado	4	INTEL XEON 2 CORES	DD 80 GB	SI
Test4	Windows 10 actualizado	4	INTEL XEON 2 CORES	DD 80 GB	SI
Test5	Windows 10 actualizado	3	INTEL XEON 2 CORES	DD 80 GB	SI
MITRE CALDERA	UBUNTU 18.02	6	INTEL XEON 2 CORES	DD 100 GB	NO

Fuente: Autores

8.2.2 Extracción de apt´s desde ATT&CK

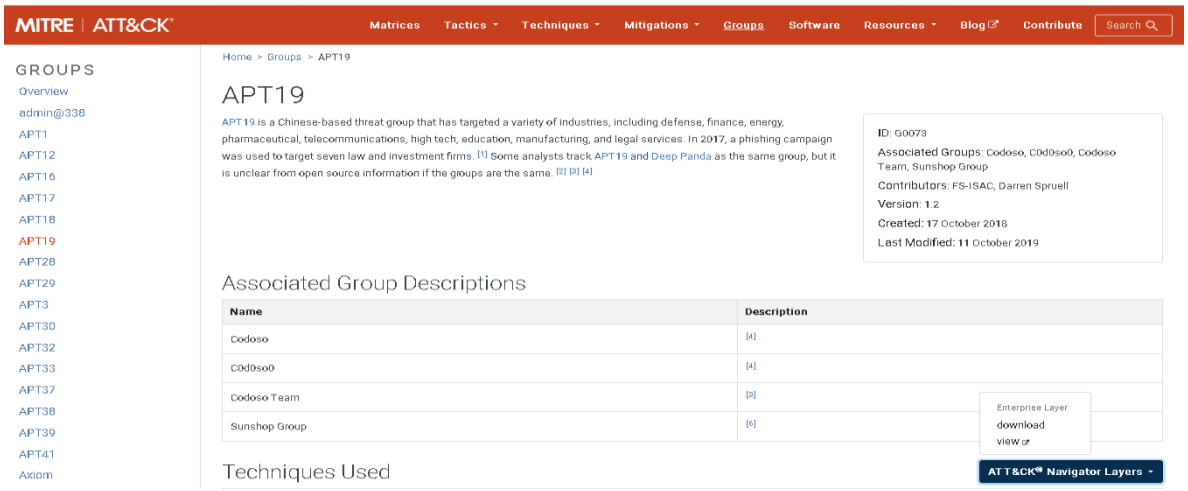
Las APT Lazarus (ilustración 9), APT 19 (ilustración 10), APT 41 (ilustración 11) se encuentran en el sitio oficial de Mitre ATT&CK https://attack.mitre.org/groups/, al seleccionar cada una de las ATP mencionadas, se muestra una descripción de las técnicas y tácticas utilizadas, como también la opción de descarga en formato JSON, con el fin de poder cargarlo en Mitre Caldera.

Ilustración 9. APT Lazarus



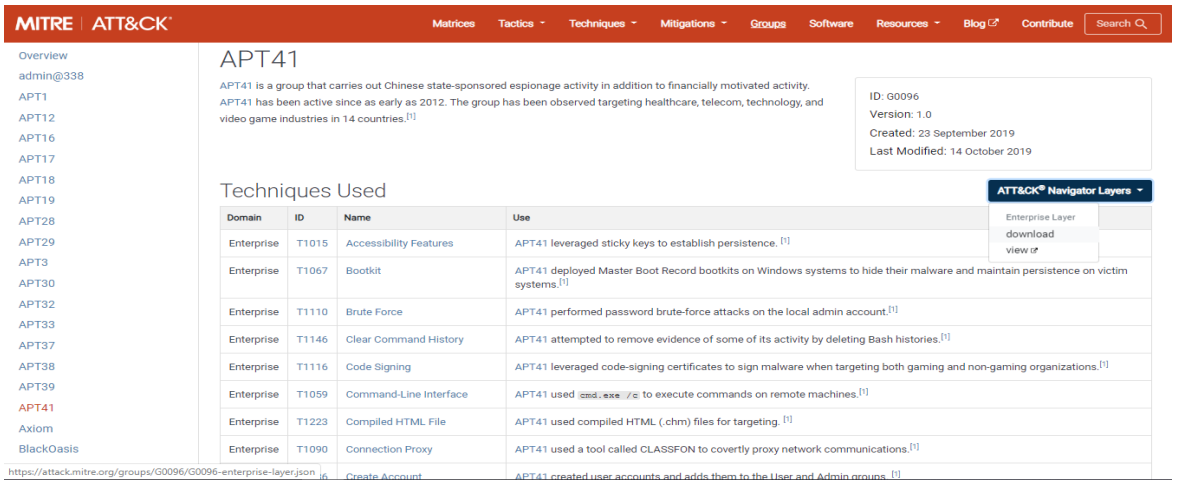
Fuente: The MITRE Corporation, attack.mitre.org "Lazarus Group".{En línea}.{22 febrero de 2020} disponible en: (https://attack.mitre.org/groups/G0032/)

Ilustración 10. APT 19



Fuente: The MITRE Corporation, attack.mitre.org "Lazarus Group".{En línea}.{22 febrero de 2020} disponible en: (https://attack.mitre.org/groups/G0079/)

Ilustración 11. APT 41

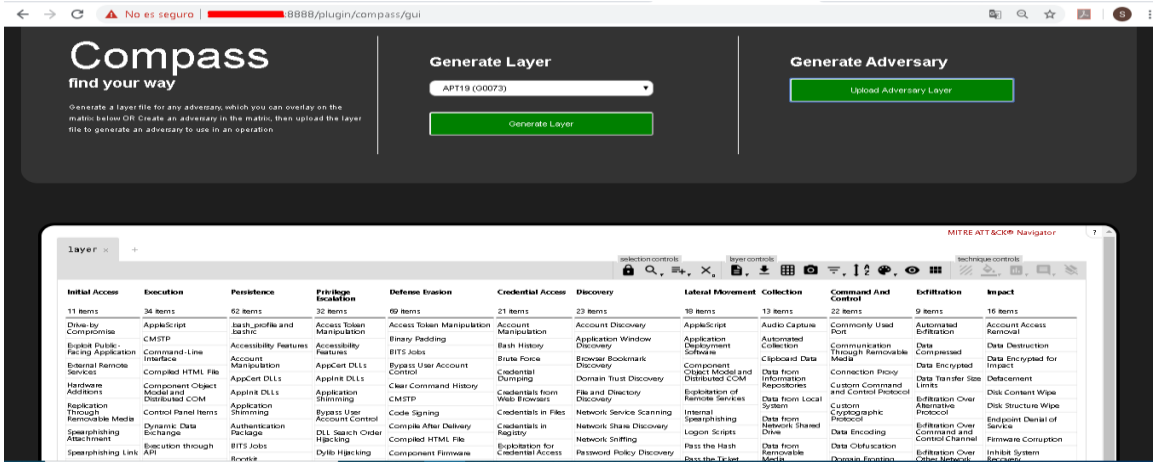


Fuente: The MITRE Corporation, attack.mitre.org "Lazarus Group".{En línea}.{22 febrero de 2020} disponible en: (https://attack.mitre.org/groups/G0096/)

8.2.3 Carga de APT

El complemento Compass como se observa en la ilustración 12, permite ver y agregar nuevos adversarios desde la matriz ATT & CK los modelos de adversario son extraídos en formato .JSON directamente de la página de Mitre, un ejemplo es el link que se proporciona a continuación el cual descarga el ATP41 https://attack.mitre.org/groups/G0096/G0096-enterprise-layer.json para después cargarlo al sistema MITRE

Ilustración 12. Carga de APT vista desde Mitre Caldera

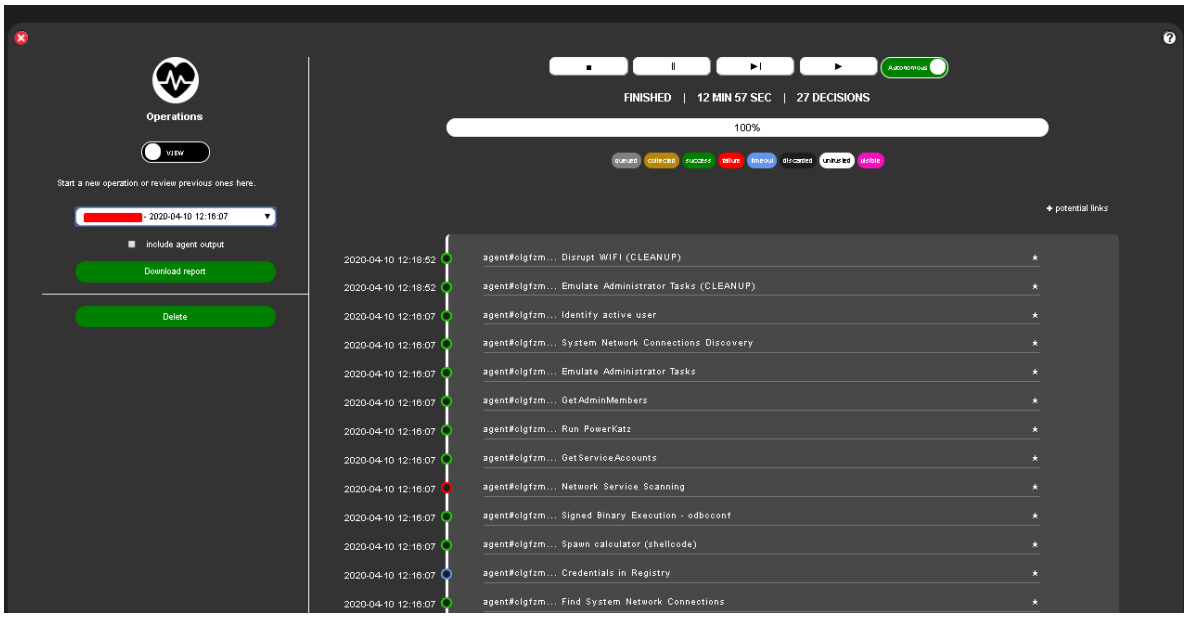


Fuente: Autores

8.2.4 Visualización de ejecución de Mitre Caldera

Para la ejecución de los adversarios la herramienta CALDERA muestra puntos verdes que significan que las técnicas se cumplieron, los puntos de color rojo muestran que la tarea se entregó, pero la defensa de las estaciones de trabajo reaccionó y bloqueo, los puntos azules hacen referencia en que la tarea se entrega para ejecutar la técnica, pero genera un timeout (ilustración 13).

Ilustración 13. Técnicas Ejecutadas



Fuente: Autores

8.3 Ejecución de APT LAZARUS

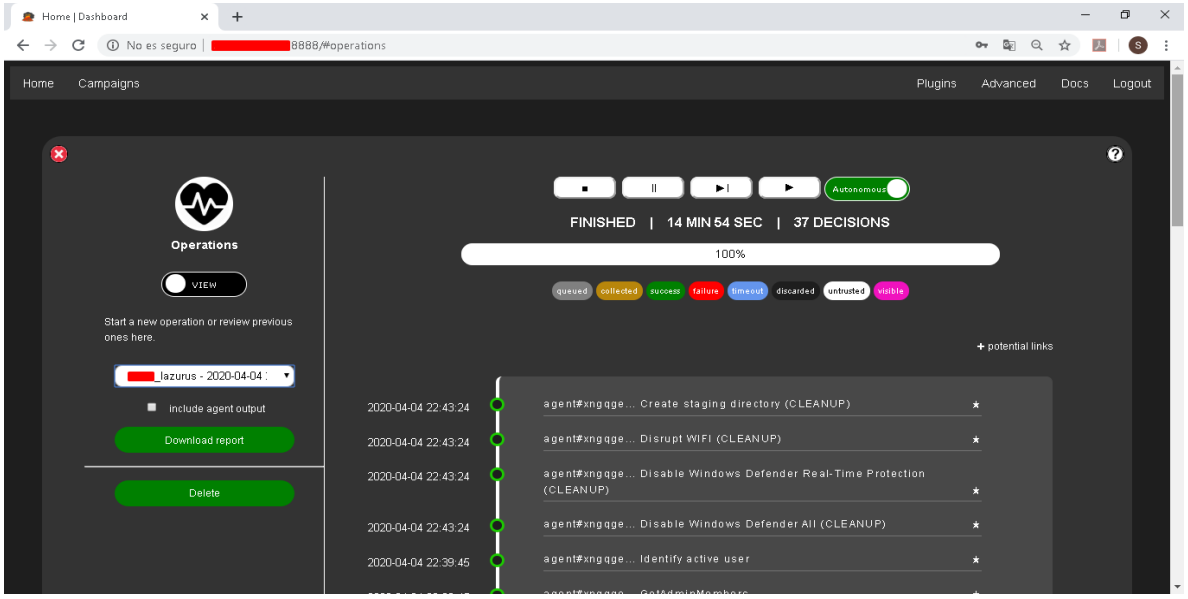
¿Qué es Lazarus?

El Grupo Lazarus ha estado activo aproximadamente desde el año 2019, sus amenazas se han atribuido al gobierno de corea del norte. De acuerdo con informes presentados fue responsable del ataque wiper, que representaba una campaña denominada Operation Blockbuster por Novetta el cual tuvo fines destructivos y se efectuó en noviembre del 2014 contra Sony Pictures Entertainment.

Se detectó que el malware utilizado en esta campaña ya había sido utilizado con anterioridad en otras campañas conocidas como: Operation Flame, Operation 1Mission, Operation Troy, DarkSeoul y Ten Days of Rain.

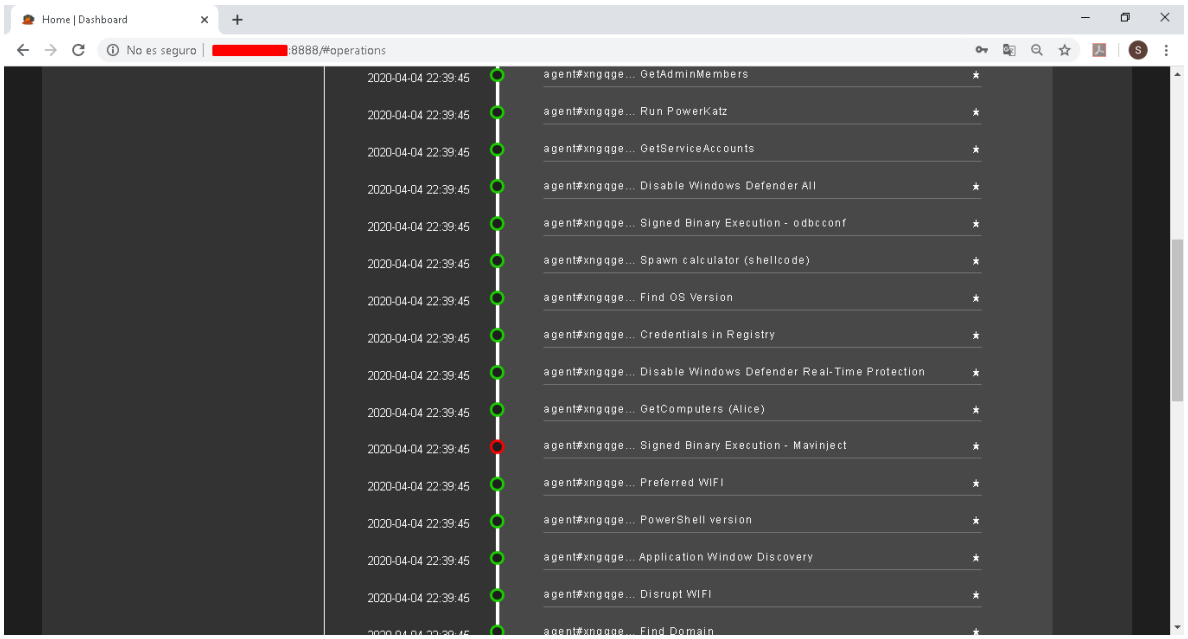
Lazarus utilizó una herramienta de limpieza de disco, para efectuar en el 2017 un ataque en América Central contra un casino en línea. Los grupos de Corea del Norte tienen un reconocimiento significativo, y es de conocimiento público que el grupo Lazarus realiza diversas actividades. Diferentes organizaciones resaltan el nombre del grupo Lazarus para referirse a cualquier actividad efectuada por Corea del Norte, y otras organizaciones individualizan las actividades y las categorizan a otros grupos llamados Bluenoroff, APT37 y APT38. Ejecución de APT Lazarus desde Mitre Caldera (ilustración 14, 15, 16).

Ilustración 14. Ejecución de APT Lazarus desde Mitre Caldera



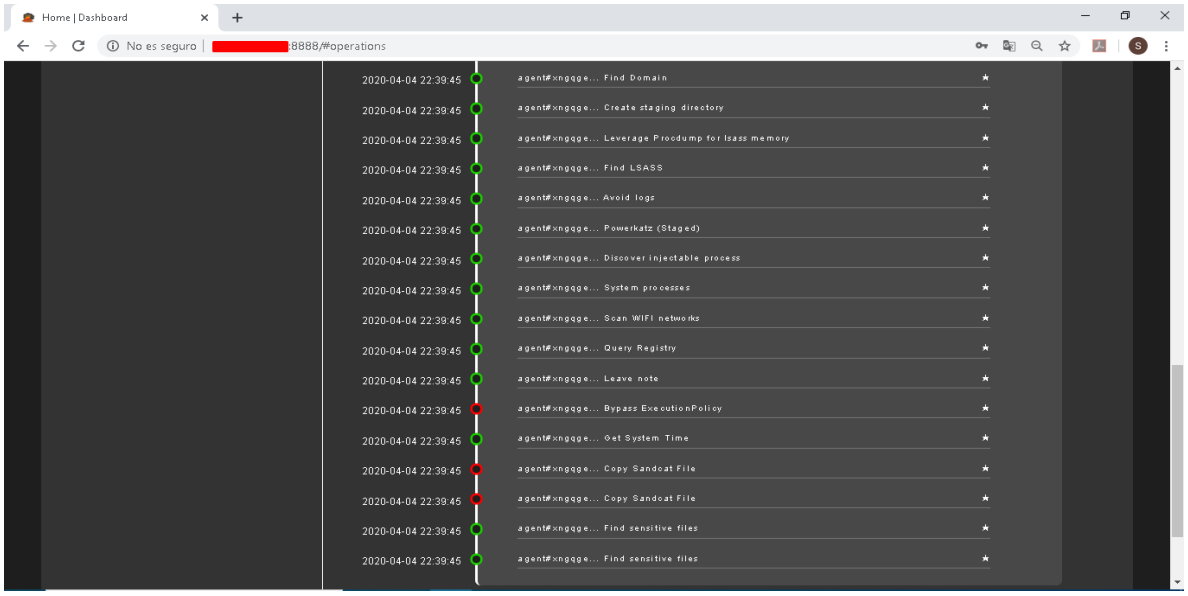
Fuente: Autores

Ilustración 15. Ejecución de APT Lazarus desde Mitre Caldera



Fuente: Autores

Ilustración 16. Ejecución de APT Lazarus desde Mitre Caldera

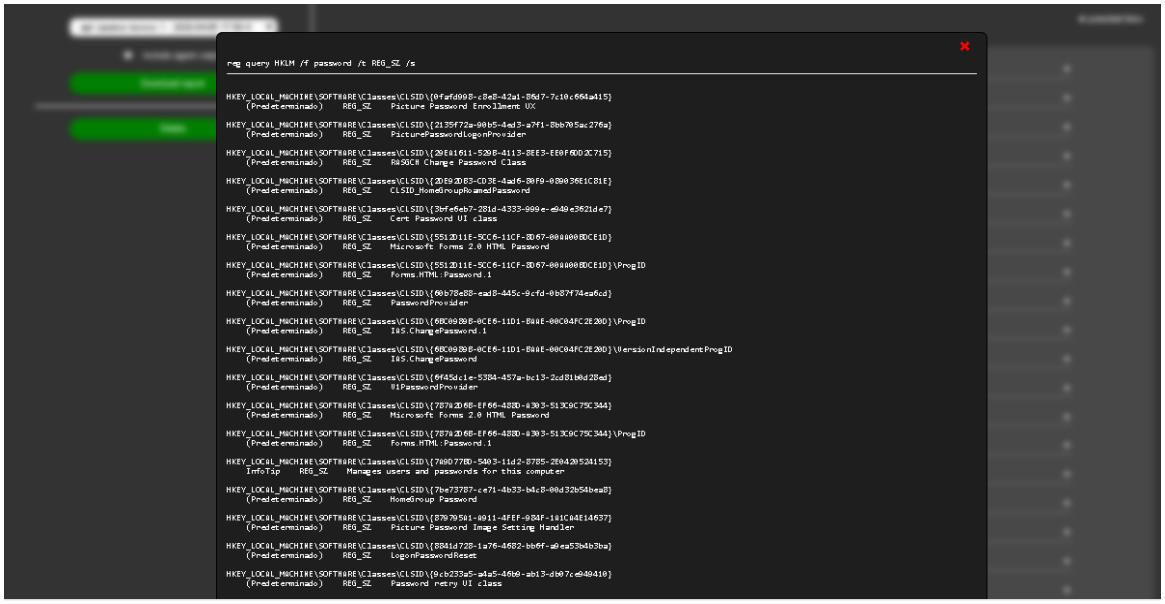


Fuente: Autores

8.3.1 Resultados de la ejecución de la APT LAZARUS

Las credenciales que son utilizadas por el sistema o algún programa son almacenadas en el registro de Windows, algunas veces estas credenciales son utilizadas para acceder a sesiones de forma automática, las rutas de estas credenciales quedan en evidencia al ejecutar la técnica T1003 Credentials Duping como se muestra en la ilustración 17.

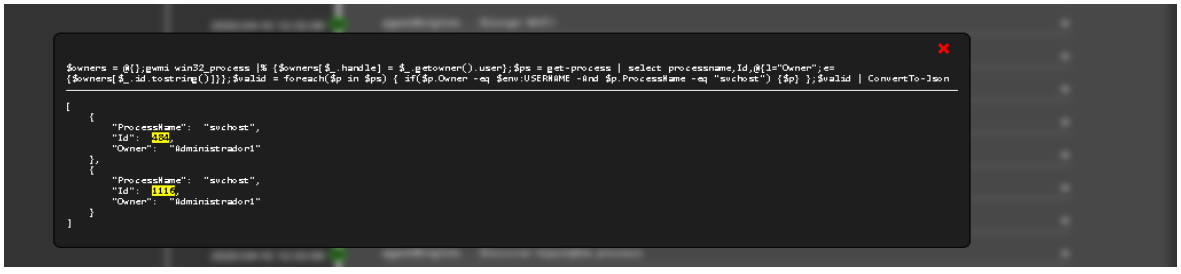
Ilustración 17. Credentials in Registry



Fuente: Autores

Al conocer los procesos que se están ejecutando en un sistema operativo como se observa en la ilustración 18, un atacante puede inyectar código arbitrario en servicios legítimos y así evadir la detección de productos de seguridad, esto se evidencia en la técnica T1057 Process Discovery.

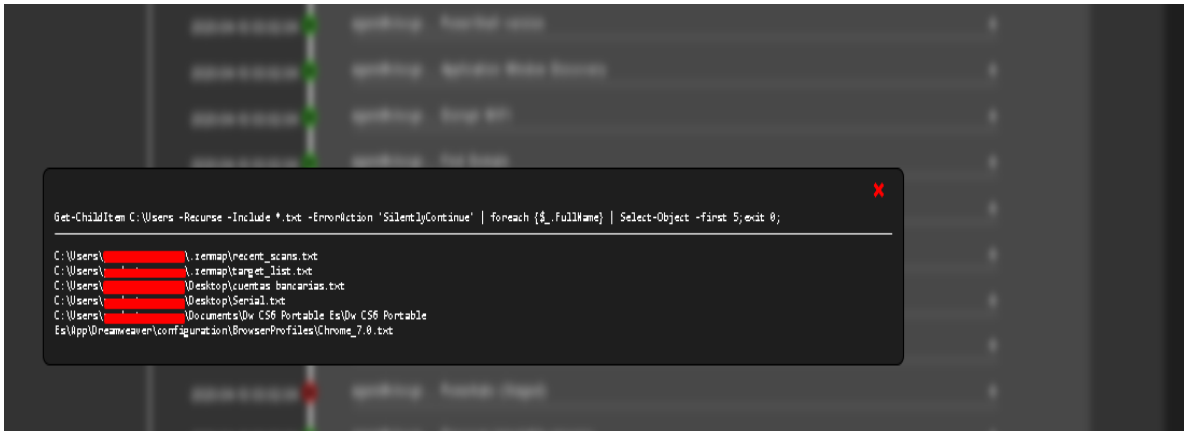
Ilustración 18. Discover injectable process



Fuente: Autores

En la ilustración 19, se evidencia como la APT Lazarus mediante la técnica T1005 Data From Local System, ejecuta un comando con el fin de encontrar archivos confidenciales, el cual se efectuó de forma correcta.

Ilustración 19. Find sensitive files



Fuente: Autores

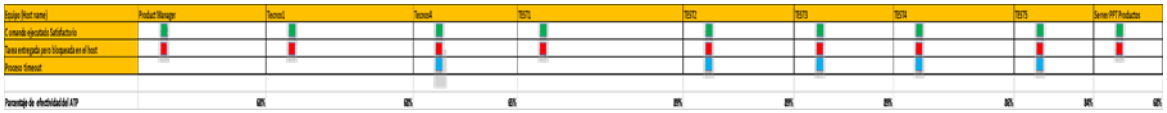
8.3.2 Matriz con operaciones ejecutadas APT LAZARUS

La capacidad de ejecución del APT LAZARUS como se observa en la matriz 1, contiene puntos de referencia de colores como: verde, representa la ejecución exitosa de la táctica, rojo tarea no realizada pero sí entregada y azul que significa que se agotó el tiempo de espera, el color amarillo representa todas las técnicas y tácticas que tiene el APT extraídas desde el ATT&CK cabe resaltar que no todas las técnicas y tácticas están disponibles en la herramienta Mitre Caldera. En la tabla 3 se observa el porcentaje de efectividad y ejecución del APT en cada una de las estaciones de trabajo y servidor.

Matriz 1. Técnicas y tácticas mapeadas por ejecución de Mitre Caldera para Lazzarus

Fuente: Autores

Tabla 3. Resultados APT Lazarus



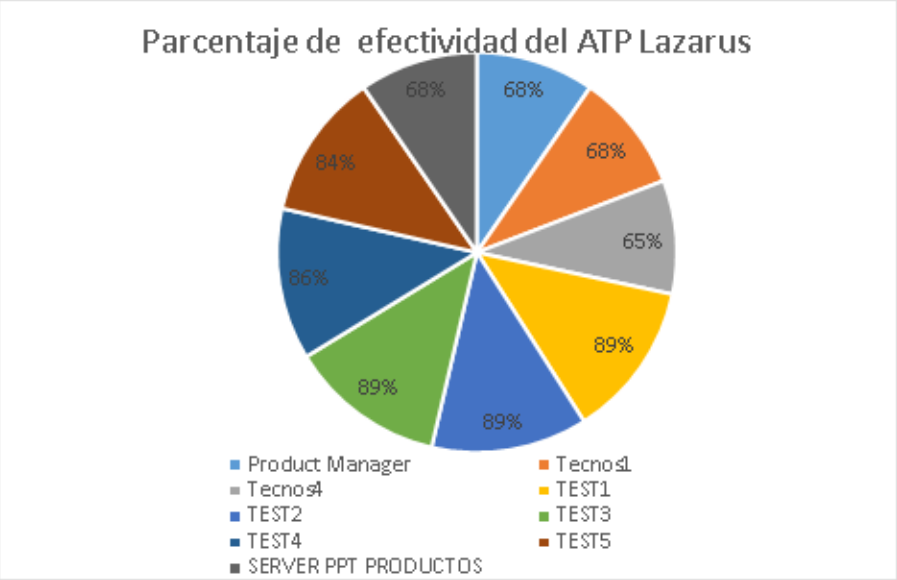
Fuente: Autores

8.3.2 Resultado

El software de MITRE CALDERA tiene 37 técnicas del APT Lazarus cargadas en sus sistemas de emulación de adversario, de un total de 65 que se encuentran referenciadas en ATT&CK, esto nos da como resultado que el porcentaje de ejecución de técnicas cargadas en caldera sobre el total del APT lazarus, tiene un porcentaje de efectividad del 57%

En la gráfica 1 se observa el nivel de efectividad del APT LAZARUS sobre las estaciones de trabajo y servidor de manera individual, donde se obtiene un promedio de ejecución del 77%, dando como resultado que la organización ACME está en un nivel Bajo en la detección de este APT.

Grafica 1. Porcentaje de efectividad APT Lazarus

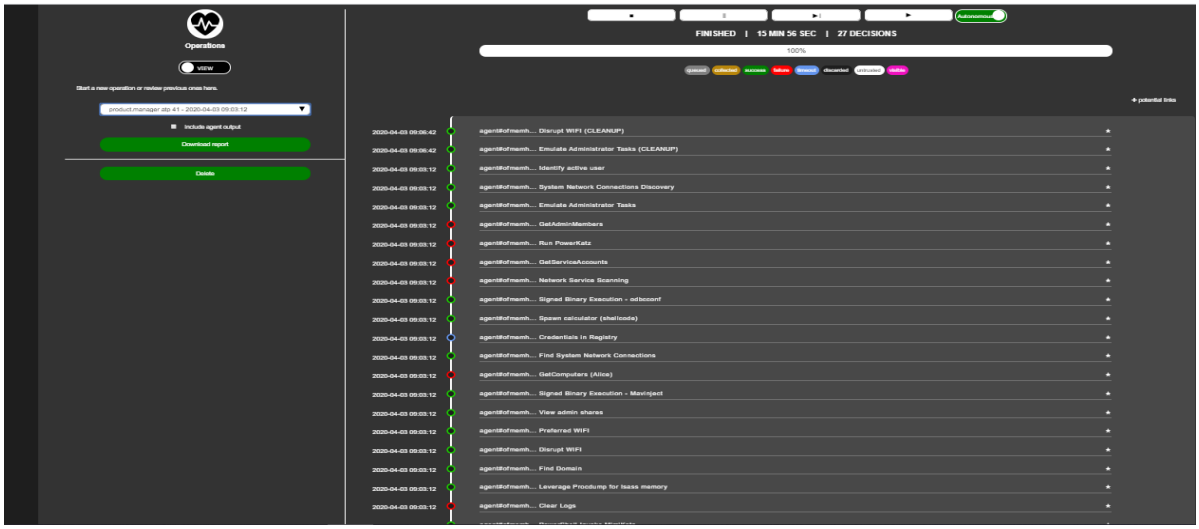


Fuente: Autores

8.4. EJECUCIÓN DE APT 41

APT41 es un grupo que comete acciones de espionaje, las cuales son patrocinadas por el estado chino, el objetivo de sus actividades son obtener ganancias financieras. Este grupo ha estado activo desde de 2012, sus principales objetivos son organizaciones de salud, telecomunicaciones, tecnología y videojuegos.

Ilustración 20. Ejecución de APT 41 desde Mitre Caldera



Fuente: Autores

8.4.1 Resultados de la ejecución de la APT41

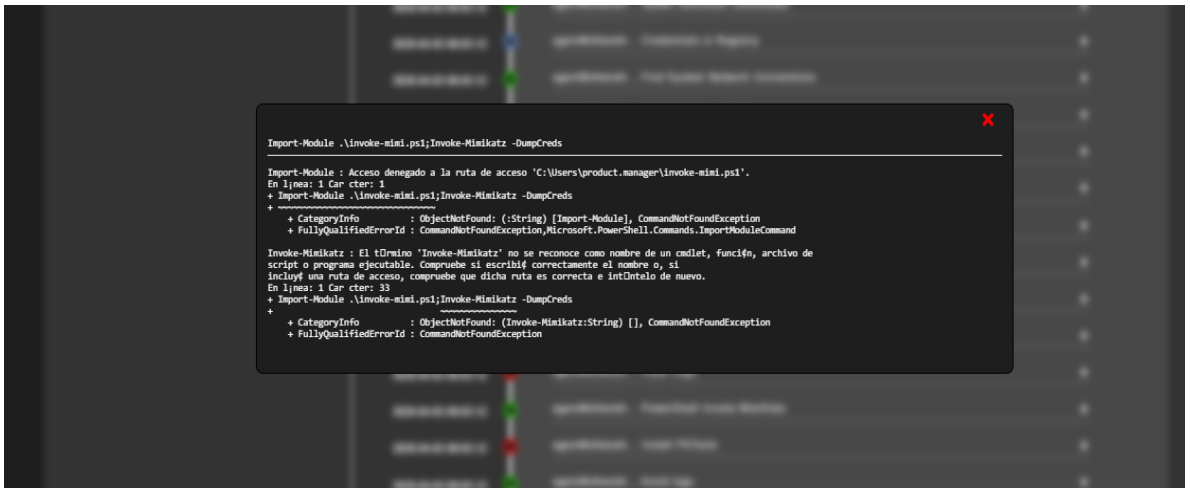
En la ilustración 21 se puede observar una de las técnicas T1046 Network Service Scanning del ATP41, la cual realiza un scan sobre las redes Wifi de los objetivos, con el escaneo de la red se obtiene detalles de configuración de servicios, características de la red etcétera.

Ilustración 21. Scan WIFI networks

Fuente: Autores

Mimikatz es un software cuyo objetivo es obtener inicios de sesión y contraseñas de cuentas de Windows en texto sin formato, esta técnica no se logró, puesto que los sistemas de antivirus bloquean su ejecución como se ve en la ilustración 22 es identificada como Credential Dumping T1003.

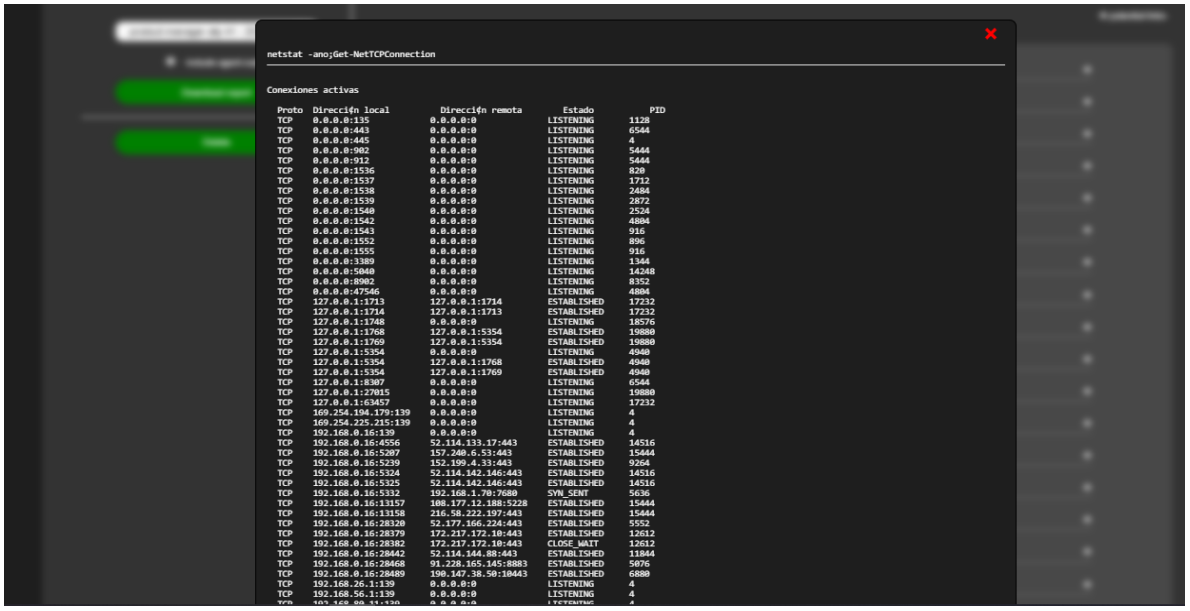
Ilustración 22. Powerkatz (Staged)



Fuente: Autores

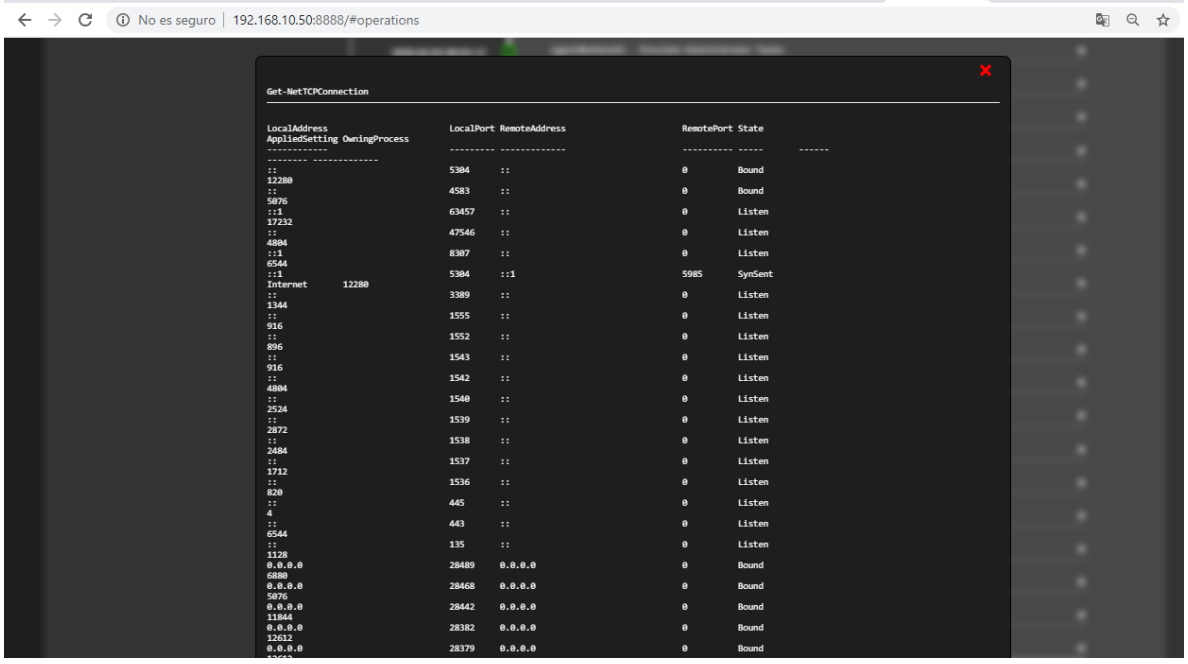
Los adversarios intentan obtener una lista de conexiones de red hacia o desde el sistema comprometido realizando consultas y así evaluar futuros movimientos laterales, en la ilustración 23 y 24 se muestra cómo se verifica las conexiones activas que tienen las estaciones de trabajo identificado con la técnica System Network Connections Discovery T1049.

Ilustración 23. System Network Connections



Fuente: Autores

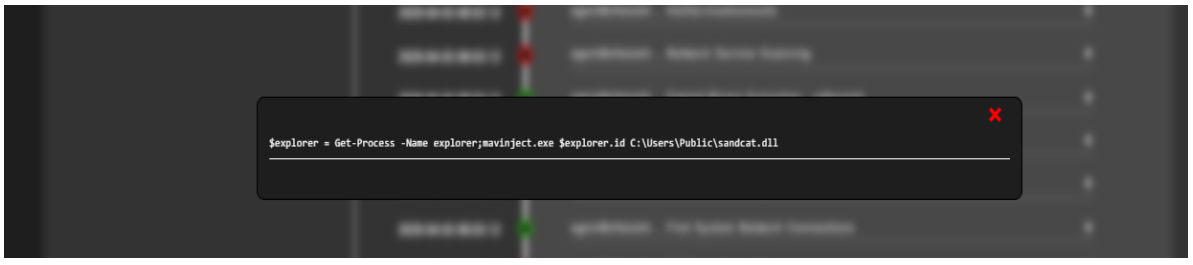
Ilustración 24. Find System Network Connections



Fuente: Autores

ODBCCONF.exe es una herramienta de línea de comandos que permite configurar controladores ODBC como nombres de fuentes de datos, CALDERA lo ejecuta de forma silenciosa, el archivo se carga en la memoria principal (RAM) el proceso Mavinject.exe es una utilidad de Windows que permite la ejecución de código, el cual se puede utilizar para ingresar una DLL en un proceso en ejecución como se observa en la ilustración 25 e identificado con la técnica Signed Binary Proxy Execution T1218.

Ilustración 25. Signed Binary Execution - odbcconf

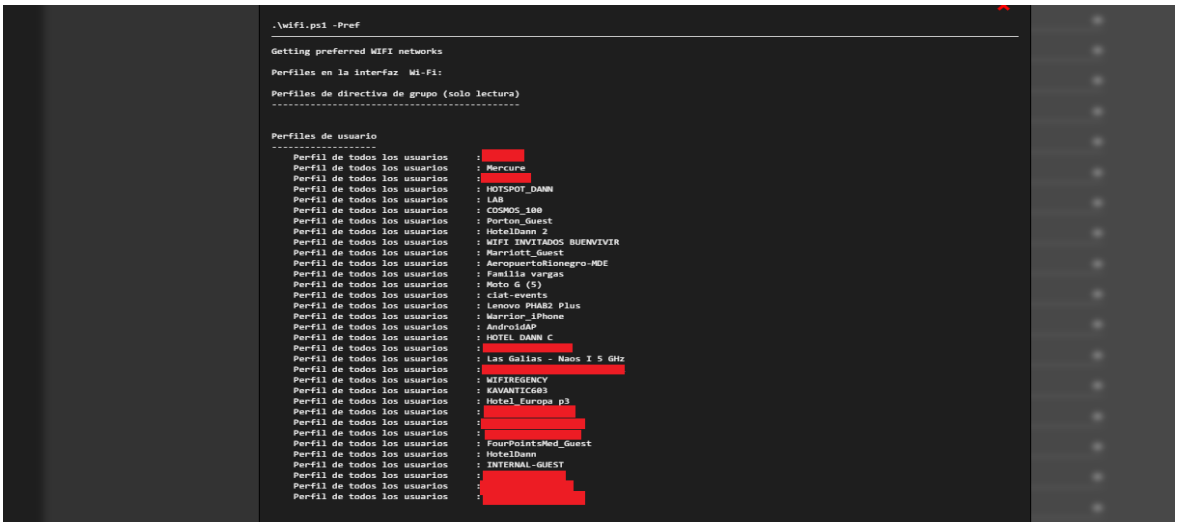


Fuente: Autores

Otras de las técnicas de los ciberdelincuentes es System Network Connections Discovery T1049 la cual se encarga de verificar el historial de conexiones WIFI realizadas, en la ilustración 26 se puede apreciar, redes públicas, Aeropuertos,

Hoteles, esto con el fin de descubrir movimientos de un equipo portátil en diferentes Access Point analizando la infraestructura de red WIFI.

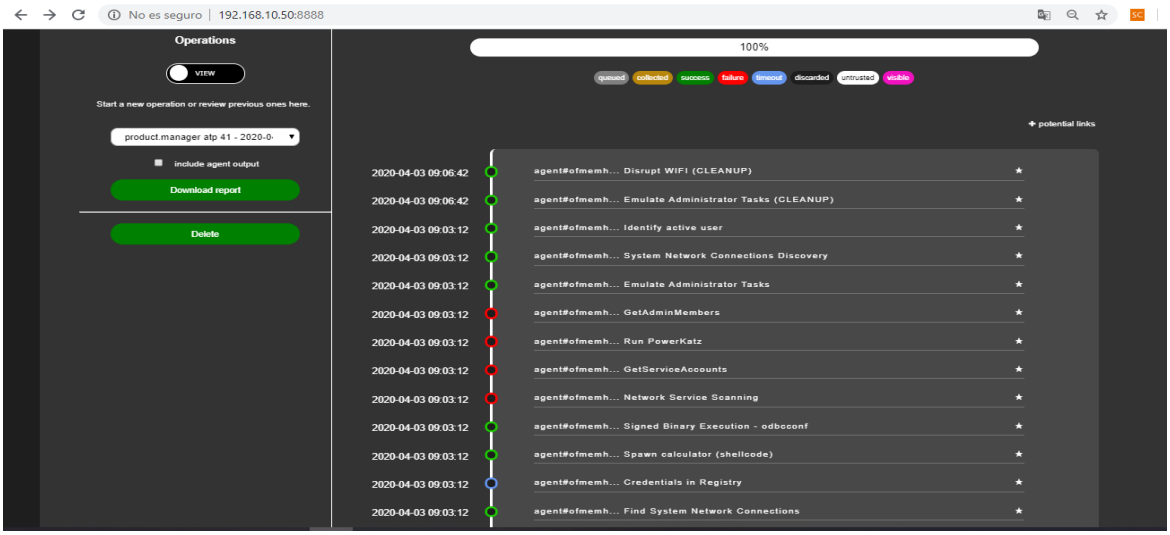
Ilustración 26. Preferred WIFI



Fuente: Autores

Desde mitre caldera, se cuenta con una interfaz de visualización global de ejecución del APT41, mostrando estados de culminación de tareas ejecutadas como se observa en la ilustración 27.

Ilustración 27. Ejecución de APT 41 desde Mitre Caldera

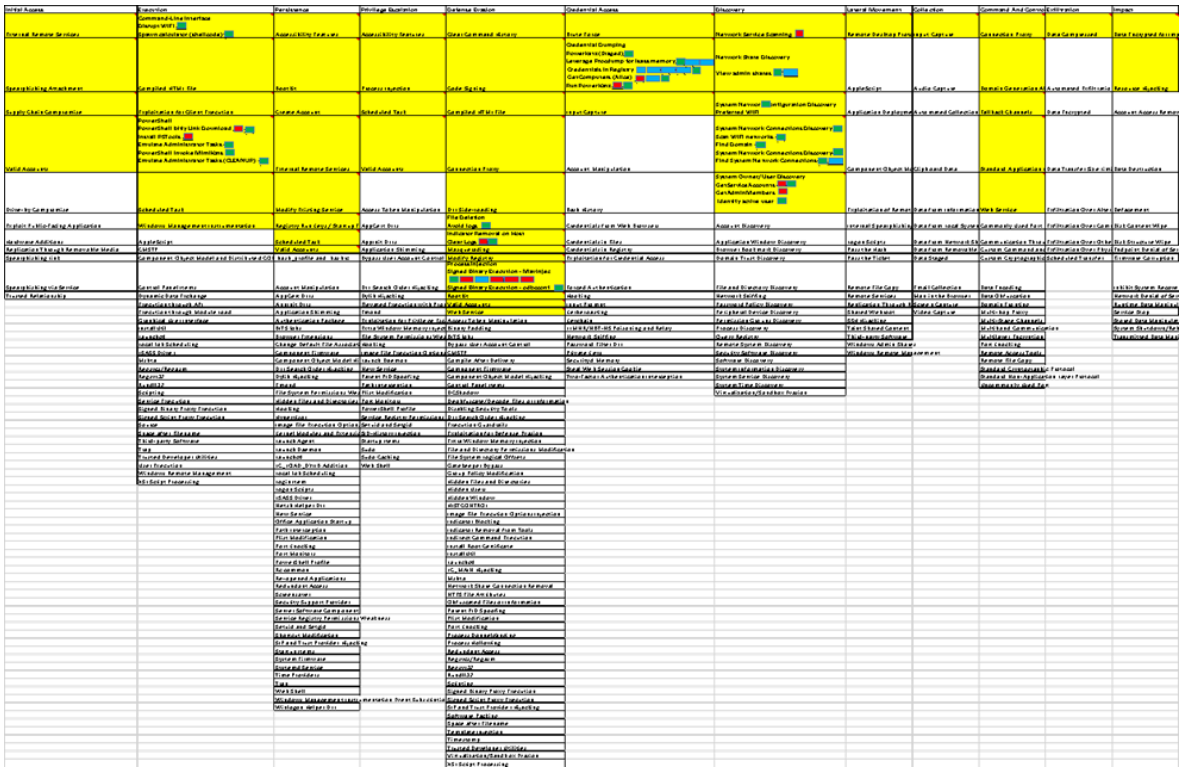


Fuente: Autores

8.4.2 Matriz con operaciones ejecutadas APT41

La capacidad de ejecución del APT41 como se observa en la matriz 2, contiene puntos de referencia de colores como: verde, representa la ejecución exitosa de la táctica, rojo tarea no realizada pero sí entregada y azul que significa que se agotó el tiempo de espera, el color amarillo representa todas las técnicas y tácticas que tiene el APT extraídas desde el ATT&CK cabe resaltar que no todas las técnicas y tácticas están disponibles en la herramienta. En la tabla 4 se observa el porcentaje de efectividad y ejecución del APT en cada una de las estaciones de trabajo y servidor.

Matriz 2. Técnicas y tácticas mapeadas por ejecución de Mitre Caldera para APT41



Fuente: Autores

Tabla 4. Resultado APT 41

Equipo (Host name)	Product Manager	Tecnos1	Tecnos4	TEST1	TEST2	TEST3	TEST4	TEST5	TEC190	SERVER PPT PRODUCTOS
Comando ejecutado Satisfactorio										
Tarea entregada pero bloqueada en el host										
Proceso timeout										
	Product Manager	Tecnos1	Tecnos4	TEST1	TEST2	TEST3	TEST4	TEST5	TEC190	SERVER PPT PRODUCTOS
Parcentaje de ejectividad del ATP	59%	63%	63%	89%	70%	85%	89%	81%	63%	59%

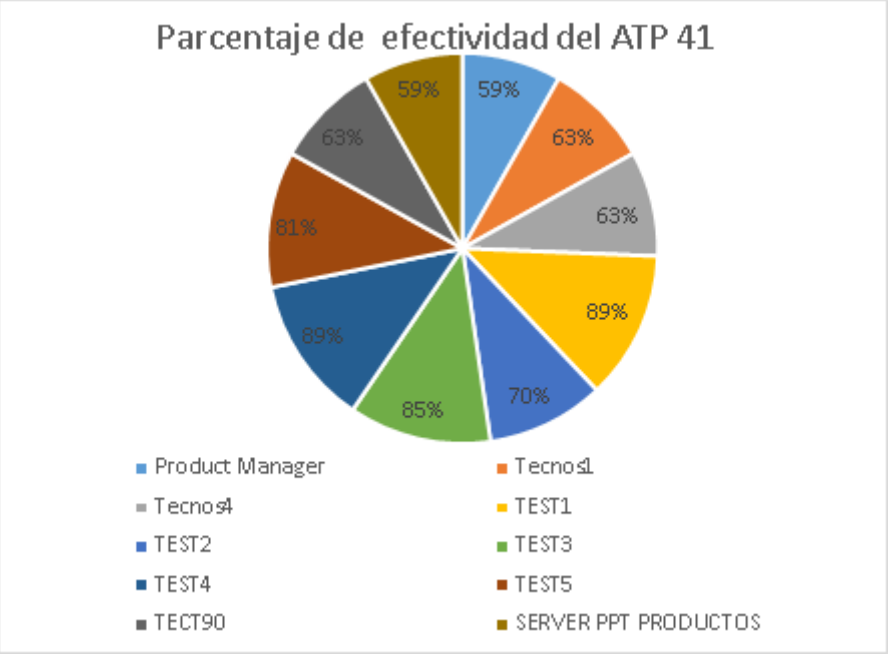
Fuente: Autores

8.4.3 Resultado

El software de MITRE CALDERA tiene 27 técnicas del APT41 cargadas en sus sistemas de emulación de adversario, de un total de 52 que se encuentran referenciadas en ATT&CK, esto nos da como resultado, que el porcentaje de ejecución de técnicas cargadas en caldera sobre el total del APT41 tiene un porcentaje de efectividad del 52%

En la gráfica 2 se observa el nivel de efectividad del APT LAZARUS sobre las estaciones de trabajo y servidor de manera individual, donde se obtiene un promedio de ejecución del 72%, dando como resultado que la organización ACME está en un nivel Bajo en la detección de este APT.

Grafica 2. Porcentaje de efectividad APT 41



Fuente: Autores

8.5 EJECUCIÓN DE APT 19

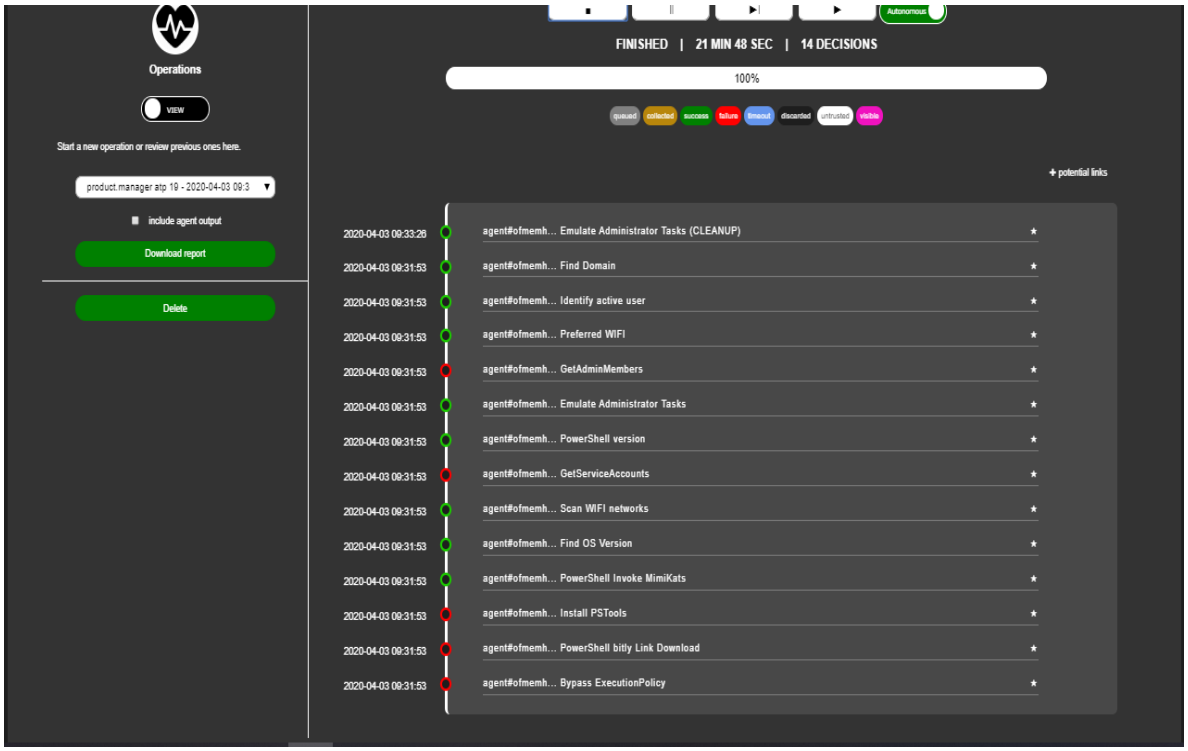
¿Qué es APT 19?

Es un grupo con sede en China cuyo objetivo es realizar amenazas informáticas y efectuarlas en una variedad de industrias, como lo son: defensa, finanzas, energía, farmacéutica, telecomunicaciones, alta tecnología, educación, manufactura y servicios legales. Es reconocido por sus actos debido a que, en el año 2017 realizó una campaña utilizando phishing, la cual estaba dirigida a siete firmas de abogados e inversionistas.

8.5.1 Resultados de la ejecución de la APT19

Desde mitre caldera, se cuenta con una interfaz de visualización global de ejecución del APT19, mostrando estados de culminación de tareas ejecutadas como se observa en la ilustración 28.

Ilustración 28. Ejecución de APT 19 desde Mitre Caldera

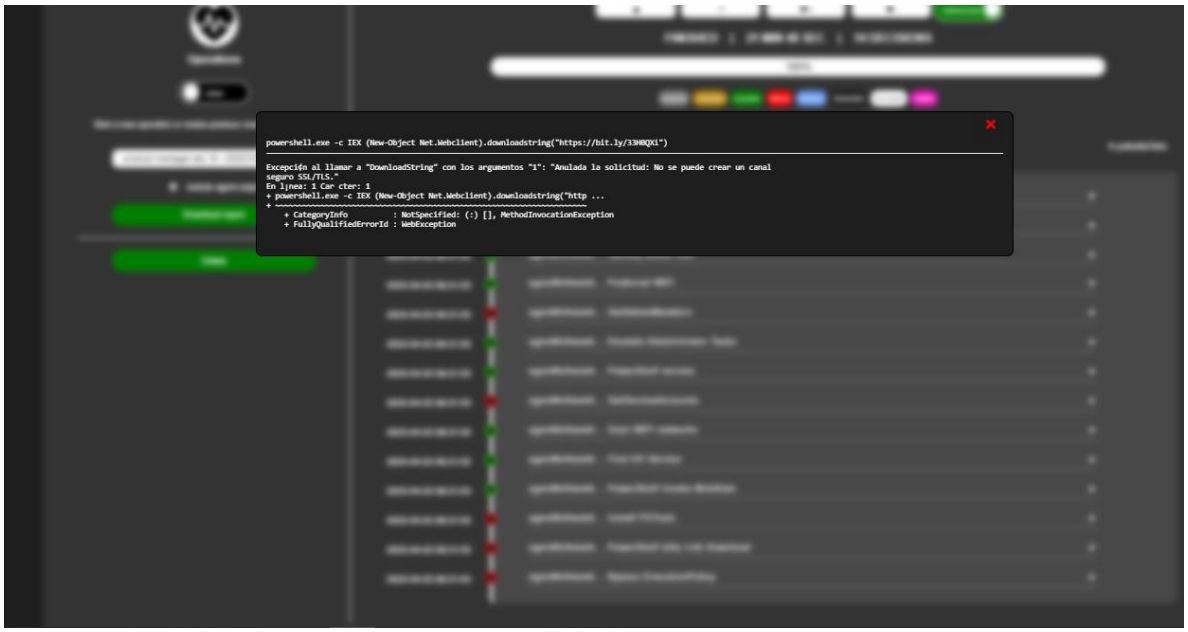


Fuente: Autores

Mitre Caldera ejecuto la operacion por PowerShell bitly Link Download T1086 llamado la ejecución de un comando publicado en un sitio web, pero el sistema

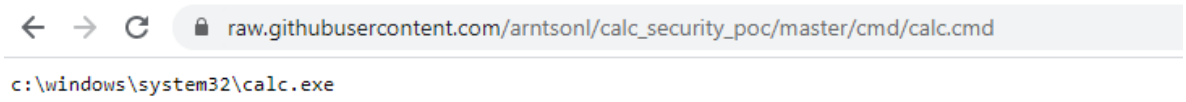
Firewall bloqueo la petición, como se puede observar en la ilustración 29 y 30 https://raw.githubusercontent.com/arntsonl/calc_security_poc/master/cmd/calc.cmd

Ilustración 29. PowerShell bitly Link Download bloqueado por el sistema firewall



Fuente: Autores

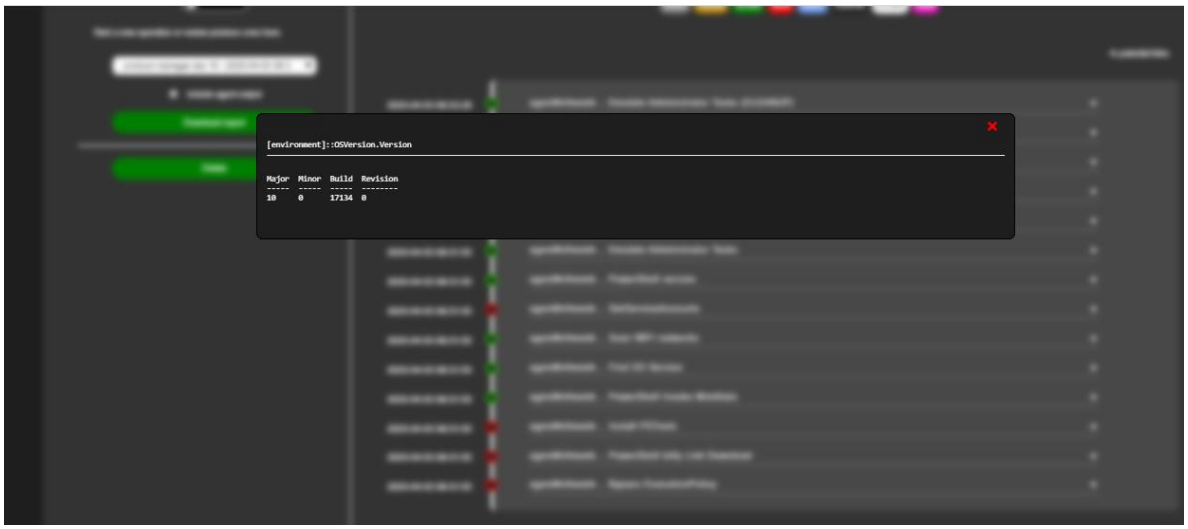
Ilustración 30. Link para ejecución de comando por Powershell



Fuente: raw.gitbusercontent.com

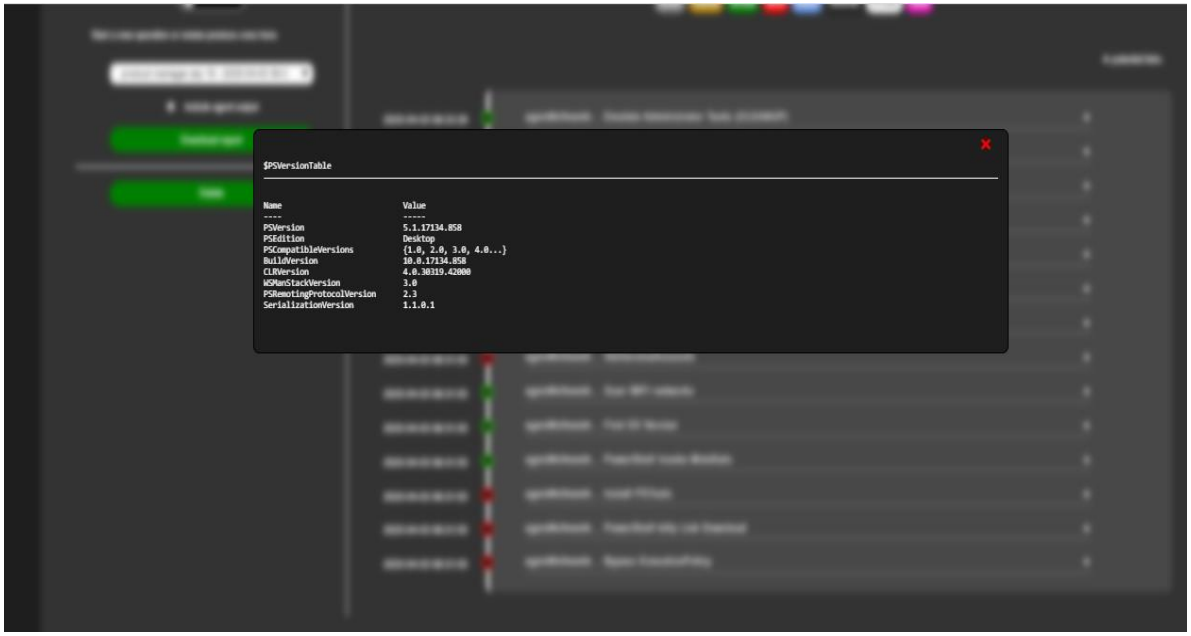
Una de las fases importantes para un ciberdelincuente es la verificación de versiones de OS, esto con el fin de detectar compilaciones anteriores y detectar posibles vulnerabilidades dentro del sistema, como se observa en las ilustraciones 31 y 32 evidenciando la versión del sistema por powershell con técnica T1082.

Ilustración 31. Find OS Version



Fuente: Autores

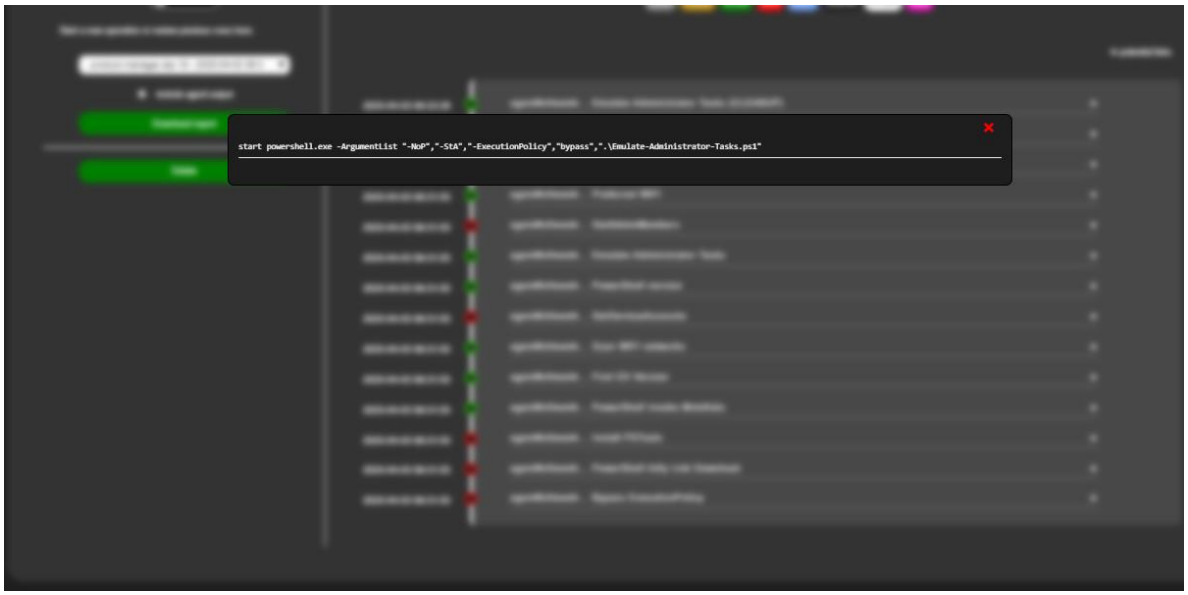
Ilustración 32. PowerShell version



Fuente: Autores

Mitre caldera ofrece una simulación de administrador, la operación se ejecuta a través de powershell técnica T1086 como se ve en la ilustración 33, el código de la emulación se puede observar en CO1.

Ilustración 33. Emulate Administrator Tasks



Fuente: Autores

Powershell script para emular las tareas típicas de administrador del sistema en una empresa

```
# Powershell
script to
emulate
typical
system
administrator
tasks on an
enterprise
```

```
# Run this anywhere you want to emulate an adversary presence


# BaseTask Object Structure
$BaseTaskClass = New-Object psobject -Property @{
    id   = $null
    task = $null
}


# BaseTask constructor
function BaseTask {
    param(
        [Parameter(Mandatory=$true)][Int]$id,
        [Parameter(Mandatory=$true)][String]$task
    )
    $basetask = $BaseTaskClass.psobject.copy()
    $basetask.id   = $id
    $basetask.task = $task
```

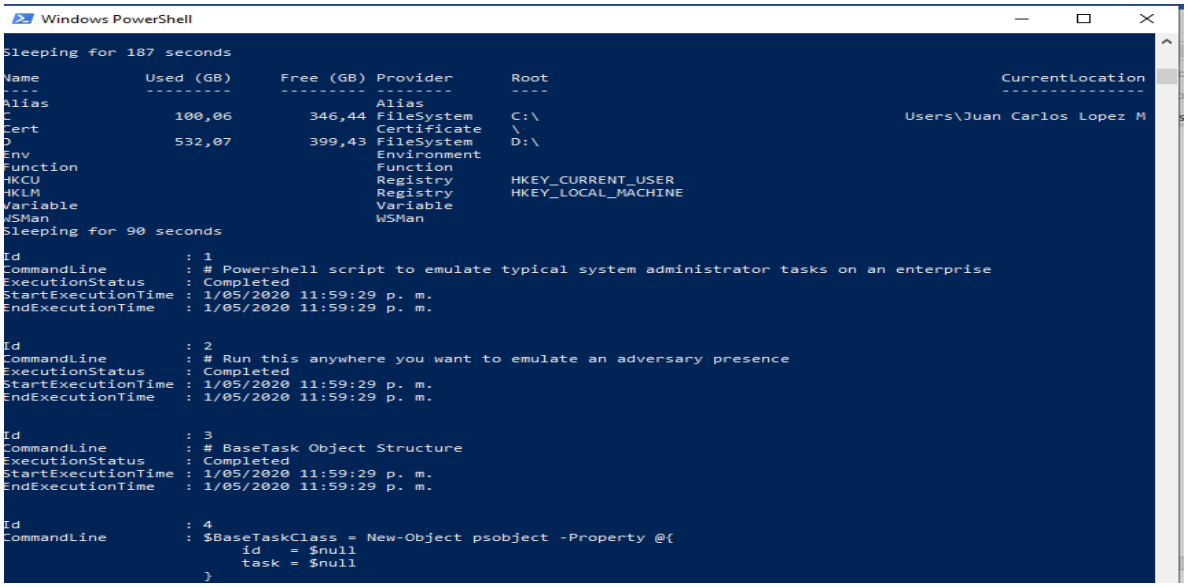
```
    $basetask
}


# BaseTask Execute task function
$BaseTaskClass | Add-Member -MemberType ScriptMethod -Name Execute -value
{
    Invoke-Expression $this.task
}


# Event loop that selects random tasks to execute over a time interval
function eventloop{
    Param(

[Parameter(Mandatory=$true)][System.Collections.ArrayList]$taskObjs
    )
     # Enter randomized task loop
    $minSleep = 10  # 10 seconds
    $maxSleep = 900 # 15 minutes
    while($true) {
        $index = Get-Random -Maximum $taskObjs.Count
        $taskObjs[$index].Execute()
        $sleep = Get-Random -Minimum $minSleep -Maximum $maxSleep
        Write-Host "Sleeping for"$sleep" seconds"
        Start-Sleep -s $sleep
    }
}


# Main
function main{
    Write-Host "+-------------------------------------------------+"
    Write-Host "|                                                 |"
    Write-Host "|---------- Emulating and Administrator ----------|"
    Write-Host "|                                                 |"
    Write-Host "+-------------------------------------------------+"
    $tasks =
        "Get-Process -Verbose",
        "Get-Service -Verbose",
        "Get-ComputerInfo",
        "Get-PSDrive",
        "Get-Command -Name Test-Connection -Syntax",
        "Get-LocalUser",
        "Get-WmiObject -Class Win32_Printer",
        "(New-Object -ComObject
WScript.Network).EnumPrinterConnections()",
        "Get-Command -Noun Item",
        "New-Item -Path $HOME\MyImportantWork -ItemType Directory -
Force`; Get-DnsClient | Out-File -FilePath
$HOME\MyImportantWork\DNSinfo.txt -Force",
        "Get-Host",
        "Get-EventLog -Log `"Application`" | Out-File -FilePath
$HOME\ApplicationLogsForWork.log -Force",
        "Get-ChildItem",
        "Get-History"
```

```
    # Array to store task object
    $taskObjs = [System.Collections.ArrayList]::new()


    # Construct task objects
    for($i=0;$i -lt $tasks.length;$i++){
        $taskObj = BaseTask -id $i -task $tasks[$i]
        $taskObjs.Add($taskObj) > $null
    }


    # Enter randomized task loop
    eventloop($taskObjs)
}


# Call Main to load script
main
```

Co 1 Emulación de administrador https://github.com/mitre/stockpile/blob/master/payloads/Emulate-Administrator-Tasks.ps1 APT41

Este comando se puede implementar de forma ATÓMICA por powershell, ejemplo de la ejecución se evidencia en la ilustración 34.

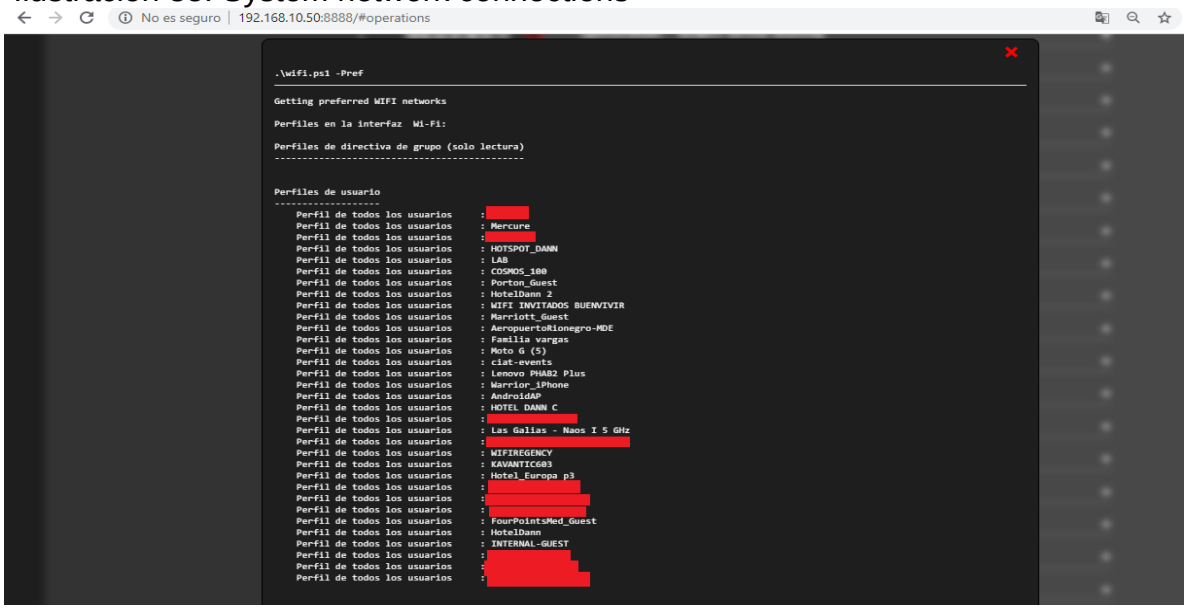
Ilustración 34. Ventana de powershell emulación de usuario administrador



Fuente: Autores

La técnica System Network Connections Discovery T1049 se encarga de verificar el historial de conexiones WIFI realizadas, en la ilustración 35 se puede apreciar, redes públicas, Aeropuertos, Hoteles, esto con el fin de descubrir movimientos de un equipo portátil en diferentes Access Point analizando la infraestructura de red WIFI.

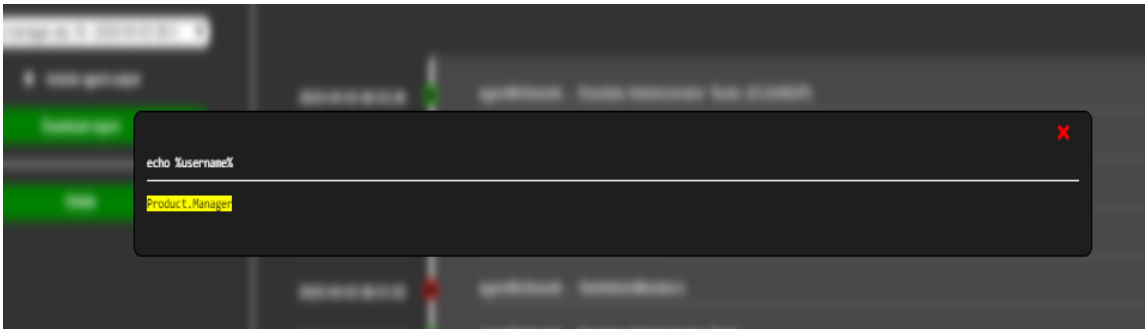
Ilustración 35. System network connections



Fuente: Autores

Por esta técnica de descubrimiento Identify active user T1087, los ciberdelincuentes también verifican los usuarios que tienen sesiones activas en los OS, y así logran conocer su nivel de acceso, como se observa en la ilustración 36.

Ilustración 36. Identify active user

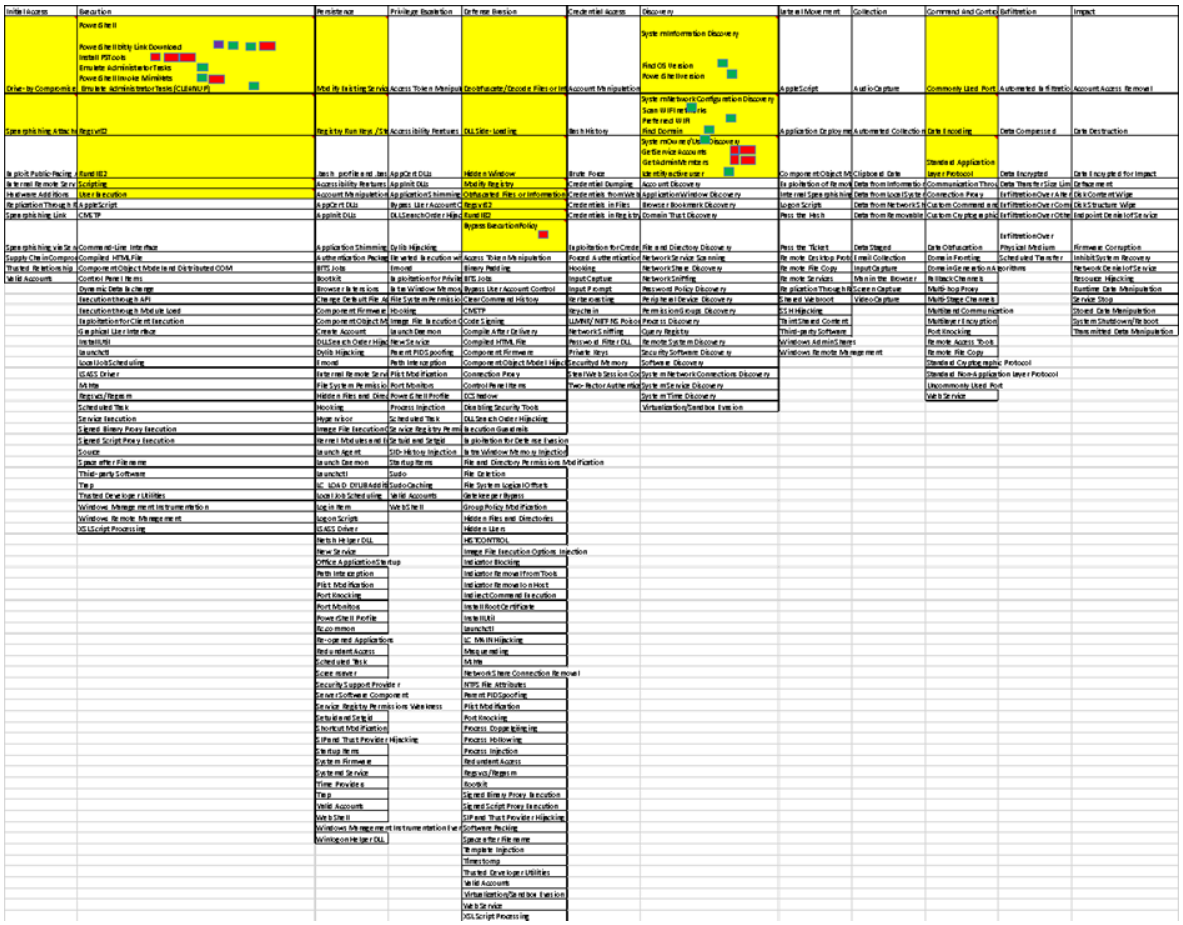


Fuente: Autores

8.5.2 Matriz con operaciones ejecutadas APT19

La capacidad de ejecución del APT 19 como se observa en la matriz 3, contiene puntos de referencia de colores como: verde, representa la ejecución exitosa de la táctica, rojo tarea no realizada pero sí entregada y azul que significa que se agotó el tiempo de espera, el color amarillo representa todas las técnicas y tácticas que tiene el APT extraídas desde el ATT&CK cabe resaltar que no todas las técnicas y tácticas están disponibles en la herramienta Mitre Caldera. En la tabla 5 se observa el porcentaje de efectividad y ejecución del APT en cada una de las estaciones de trabajo y servidor.

Matriz 3. Técnicas y tácticas mapeadas por ejecución de Mitre Caldera para APT19



Fuente: Autores

. Tabla 5. Resultado APT 19

Equipo (Host name)	Product Manager	Tecnos1	Tecnos4	TEST1	TEST2	TEST3	TEST4	TEST5	TECT90	SERVER PPT PRODUCTOS
Comando ejecutado Satisfactorio	■	■	■	■	■	■	■	■	■	■
Tarea entregada pero bloqueada en el host	■	■	■	■	■	■	■	■	■	■
Proceso timeout	■									
Parcentaje de ejectividad del ATP	64%	71%	71%	43%	86%	93%	93%	93%	63%	59%

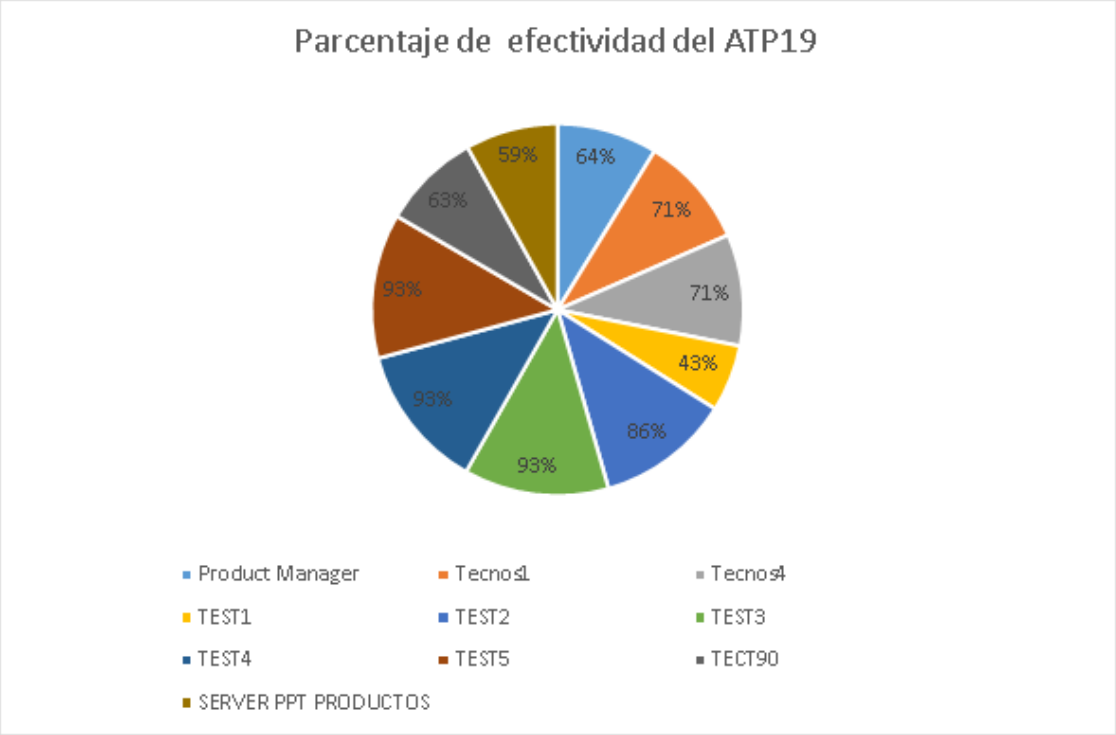
Fuente: Autores

8.5.3 Resultado

El software de MITRE CALDERA tiene 14 técnicas del APT 19 cargadas en sus sistemas de emulación de adversario, de un total de 23 que se encuentran referenciadas en ATT&CK, esto nos da como resultado que el porcentaje de ejecución de técnicas cargadas en caldera sobre el total del APT 19, tiene un porcentaje de efectividad del 61%

En la gráfica 3 se observa el nivel de efectividad del APT 19 sobre las estaciones de trabajo y servidor de manera individual, donde se obtiene un promedio de ejecución del 75%, dando como resultado que la organización ACME está en un nivel Bajo en la detección de este APT.

Grafica 3. Porcentaje de efectividad ATP 19



Fuente: Autores

8.6 RECOMENDACIONES PARA MITIGAR LAS APT EJECUTADAS

Se recomienda realizar las siguientes acciones según el proceso de detección y mitigación de técnicas de Mitre ATT&CK:

Tabla 6. Recomendaciones para APT´S Lazarus,41,19

Técnica	Recomendaciones
T1059 - Command-Line Interface	"Audite y / o bloquee intérpretes de línea de comandos innecesarios mediante el uso de herramientas de la lista blanca de aplicaciones, como Control de aplicaciones de Windows Defender, AppLocker o Políticas de restricción de software, según corresponda." [12]
T1086 – PowerShell	**"Firma de código:** Establezca la política de ejecución de PowerShell para ejecutar solo scripts firmados. **Deshabilitar o eliminar función o programa:** Puede ser posible eliminar PowerShell de los sistemas cuando no sea necesario, pero se debe realizar una revisión para evaluar el impacto en un entorno, ya que podría estar en uso para muchos fines legítimos y funciones administrativas. Deshabilitar / restringir el Servicio WinRM para ayudar a evitar el uso de PowerShell para la ejecución remota. **Gestión de cuenta privilegiada:** Restringir la política de ejecución de PowerShell a los administradores. Tener encuenta que existen métodos para omitir la política de ejecución de PowerShell, según la configuración del entorno." [25]
T1064 – Scripting	**"Aplicación Aislamiento y Sandboxing:** Configurar la configuración de seguridad de Office permite la Vista protegida, para ejecutar dentro de un entorno de espacio aislado y para bloquear macros a través de

	la Política de grupo. Otros tipos de virtualización y microsegmentación de aplicaciones también pueden mitigar el impacto del compromiso. **Deshabilitar o eliminar función o programa**: Desactive las funciones no utilizadas o restrinja el acceso a los motores de secuencias de comandos como VBScript o los marcos de administración de secuencias de comandos como PowerShell.” [30]
T1089- Disabling Security Tools	**“Restringir permisos de archivos y directorios:** Asegurarse de que existan los permisos adecuados de proceso, registro y archivo para evitar que los adversarios deshabiliten o interfieran con los servicios de seguridad. **Gestión de cuentas de usuario:** Asegurarse de contar con los permisos de usuario adecuados para evitar que los adversarios deshabiliten o interfieran con los servicios de seguridad.” [16]
T1055 - Process Injection	Prevención del comportamiento en el punto final. Algunas soluciones de seguridad de punto final se pueden configurar para bloquear algunos tipos de inyección de procesos en función de secuencias comunes de comportamiento que se producen durante el proceso de inyección. [27]
T1003 - Credential Dumping	**“Configuración de Active Directory:** Administre la lista de control de acceso para "Replicar cambios de directorio" y otros permisos asociados con la replicación del controlador de dominio. **Protección de acceso de credenciales:** Con Windows 10, Microsoft implementó nuevas protecciones llamadas Credential Guard para proteger los secretos de LSA que pueden usarse para obtener credenciales a través de formas de descarga de credenciales. No está configurado de manera predeterminada y

	tiene requisitos de sistema de hardware y firmware. Tampoco protege contra todas las formas de dumping de credenciales. **Configuración del sistema operativo:** Considere deshabilitar o restringir NTLM. **Políticas de contraseña:** Asegúrese de que las cuentas de administrador local tengan contraseñas complejas y únicas en todos los sistemas de la red. **Gestión de cuenta privilegiada:** Windows: no coloque cuentas de dominio de usuario o administrador en los grupos de administradores locales en todos los sistemas a menos que estén estrictamente controlados, ya que esto suele ser equivalente a tener una cuenta de administrador local con la misma contraseña en todos los sistemas. Siga las mejores prácticas para el diseño y la administración de una red empresarial para limitar el uso de cuentas privilegiadas en todos los niveles administrativos. **Integridad de proceso privilegiada:** "En Windows 8.1 y Windows Server 2012 R2, active Protected Process Light para LSA. **Entrenamiento de usuario:** Limite la superposición de credenciales entre cuentas y sistemas al capacitar a los usuarios y administradores para que no usen la misma contraseña para varias cuentas." [13]
T1046 - Network Service Scanning	**"Deshabilitar o eliminar función o programa:** Asegúrese de que los puertos y servicios innecesarios estén cerrados para evitar el riesgo de descubrimiento y posible explotación. **Prevención de intrusiones en la red:** Use sistemas de detección / prevención de intrusiones en la red para detectar y

	prevenir escaneos de servicio remoto **Segmentación de red:** Asegúrese de seguir la segmentación de red adecuada para proteger los servidores y dispositivos críticos.” [23]
T1107 - File Deletion T1010- Application Window Discovery T1057 - Process Discovery T1012 - Query Registry T1082 - System Information Discovery T1016 - System Network Configuration Discovery T1033 - System Owner/User Discovery T1124 - System Time Discovery T1005 - Data from Local System T1070 - Indicator Removal on Host T1135 - Network Share Discovery T1049 - System Network Connections Discovery T1074 - Data Staged	“Este tipo de técnica de ataque no se puede mitigar fácilmente con controles preventivos, ya que se basa en el abuso de las funciones del sistema”. [12] [13] [26] [28] [31] [32] [34] [35] [14] [18] [24] [33] [15]
T1105 - Remote File Copy	**“Prevención de intrusiones en la red:** Los sistemas de detección y prevención de intrusiones en la red que usan firmas de red para identificar el tráfico de malware adverso específico o la transferencia de datos inusual sobre herramientas y protocolos conocidos como FTP se pueden

	usar para mitigar la actividad a nivel de red. Las firmas a menudo son para indicadores únicos dentro de los protocolos y pueden basarse en la técnica de ofuscación específica utilizada por un adversario o herramienta en particular, y probablemente serán diferentes en varias familias y versiones de malware. Los adversarios probablemente cambiarán las firmas de la herramienta C2 con el tiempo o construirán protocolos de tal manera que eviten ser detectados por herramientas defensivas comunes.” [29]

Fuente: Autores

9. CONCLUSIONES

El conocimiento de MITRE ATT&CK en este proyecto conlleva a ver un panorama extenso de lo que un ciberdelincuente utiliza habitualmente, refiriéndose a técnicas y tácticas utilizadas en un escenario mundial.

Se logra efectuar de forma sencilla ejercicios autónomos de simulación de adversarios con la herramienta MITRE CALDERA, la cual ofrece un entorno sencillo en sus procesos de instalación cliente-servidor, brinda una interfaz gráfica amigable al usuario final, sus sistemas de creación de adversarios y emulación cuentan con la compatibilidad de base de datos recolectada por su creador MITRE, aunque no tiene todas las técnicas y tácticas debido a que se encuentra en una fase inicial de un proceso de mejora continua.

Se puede evidenciar que al verificar las defensas de la organización ACME estas son susceptibles a las APT´S, la detección de ejecución de comandos es débil, aunque los sistemas de Antivirus lograron contrarrestar los ataques relaciones con payloads del RAT de CALDERA, es recomendable elevar la posición de defensa implementado herramientas de EDR Endpoint detection and response, responsables de analizar, verificar y reportar comportamientos a nivel de ejecución de comandos del sistema operativo. De igual forma fortalecer las herramientas que tiene la organización aplicando las recomendaciones que ofrece MITRE ATT&CK para cada una de las técnicas vistas y mapeadas según el comportamiento de adversarios.

Se pudo anticipar a los pasos de un ataque alertando fallas en los sistemas de defensa cuando se utilizan amenazas avanzadas persistentes (APT´S), que en la actualidad son detectadas después de sufrir un incidente de seguridad por exfiltración de datos, recurriendo a una pérdida de imagen

Uno de los beneficios de implementar el proyecto MITRE CALDERA es que no tiene costo, y la organización ACME no tuvo la necesidad de aumentar su presupuesto para verificar sus sistemas de defensa o contratar un RED TEAM, BLUE TEAM, PURPLE TEAM.

Para finalizar los grandes fabricantes en ciberseguridad están en incorporando en sus soluciones, sistemas de MITRE evaluando las técnicas y tácticas para mejorar los esquemas de detección y respuesta a un incidente de seguridad uno de ellos, MICROSOFT en su suite Microsoft Defender incorporo ATP´s en el cual grabó y alertó de actividades de las estaciones de trabajo que incluyen técnicas y tácticas avanzadas donde los indicadores de compromiso son la escalada de privilegios y robo de credenciales junto a la persistencia, aprovechando sensores profundos como AMSI, WMI y LDAP.

10. BIBLIOGRAFÍA

1 CCIT “Tendencias del cibercrimen en Colombia 2019 - 2020”.{En línea}. {30 de Octubre de 2019} disponible en:(http://www.ccit.org.co/estudios/tendencias-del-cibercrimen-en-colombia-2019-2020/)

2 --------. “Tendencias del cibercrimen en Colombia 2019 - 2020”.{En línea}. {30 de Octubre de 2019} disponible en:(http://www.ccit.org.co/estudios/tendencias-del-cibercrimen-en-colombia-2019-2020/).

3 "DELOITTE,Deloitte “Ciber Riesgos y Seguridad de la Información en América Latina & Caribe Tendencias 2019”.{En línea}. {10 septiembre de 2019} disponible en: (https://www2.deloitte.com/content/dam/Deloitte/co/Documents/risk/Cyber%20Survey%20LATAM%20-%20Colombia%20v2.pdf) 10, 11 P.

4 --------. “Ciber Riesgos y Seguridad de la Información en América Latina & Caribe Tendencias 2019”.{En línea}. {10 septiembre de 2019} disponible en: (https://www2.deloitte.com/content/dam/Deloitte/co/Documents/risk/Cyber%20Survey%20LATAM%20-%20Colombia%20v2.pdf) .

5 ESPITIA, Nicolás. VANZINA, Juan David. Auditoría al cumplimiento de una política de desarrollo seguro basada en la ISO 27001. Bogotá, 2018, 162p. Trabajo de investigación (especialización en auditoria en sistemas de información). Universidad Católica de Colombia. Facultad de Ingeniería.

6 github, “Emulación Adversaria Automatizada”.{En línea}. {31 octubre De 2019} disponible en: (https://github.com/mitre/caldera).

7 "LOSHIN, Peter. “Desafíos y beneficios de usar el marco de Mitre ATT&CK”.{En línea}. {24 septiembre de 2019} disponible en: (https://searchdatacenter.techtarget.com/es/cronica/Desafios-y-beneficios-de-usar-el-marco-de-Mitre-ATTCK).

8 LOSHIN, Peter. “Desafíos y beneficios de usar el marco de Mitre ATT&CK”.{En línea}. {24 septiembre de 2019} disponible en: (https://searchdatacenter.techtarget.com/es/cronica/Desafios-y-beneficios-de-usar-el-marco-de-Mitre-ATTCK).

9 LUBECK,Luis, “Cómo utilizar MITRE ATT&CK: un repositorio de técnicas y procedimientos de ataques y defensas”.{En línea}. {31 octubre De 2019} disponible en: (https://www.welivesecurity.com/la-es/2019/06/06/como-utilizar-mitre-attck-repositorio-tecnicas- procedimientos-ataques-defensas).

10 MINTIC. “Ley 1273 de 2009”.{En línea}. {30 septiembre de 2019} disponible en:(https://www.mintic.gov.co/portal/inicio/3705:Ley-1273-de-2009).

11 Mitre Corporation, “Application Window Discovery ” {En línea}. {25 febrero De 2020} disponible en: (https://attack.mitre.org/techniques/T1010/.).

12 Mitre Corporation, “Command-Line Interface” {En línea}. {24 febrero De 2020} disponible en: (https://attack.mitre.org/techniques/T1059/.).

13 Mitre Corporation, “Credential Dumping” {En línea}. {25 febrero De 2020} disponible en: (https://attack.mitre.org/techniques/T1003/.).

14 Mitre Corporation, “Data from Local System” {En línea}. {26 febrero De 2020} disponible en: (https://attack.mitre.org/techniques/T1005/.).

15 Mitre Corporation, “Data Staged ” {En línea}. {26 febrero De 2020} disponible en: (https://attack.mitre.org/techniques/T1074/.).

16 Mitre Corporation, “Disabling Security Tools” {En línea}. {24 febrero De 2020} disponible en: (https://attack.mitre.org/techniques/T1089/.).

17 Mitre Corporation, “File Deletion” {En línea}. {25 febrero De 2020} disponible en: (https://attack.mitre.org/techniques/T1107/.).

18 Mitre Corporation, “File Deletion” {En línea}. {26 febrero De 2020} disponible en: (https://attack.mitre.org/techniques/T1107/.).

19 Mitre Corporation, “Frequently Asked Questions-tactics"” {En línea}. {22 febrero De 2020} disponible en: (https://attack.mitre.org/resources/faq/.).

20 Mitre Corporation, “Frequently Asked Questions- techniques” {En línea}. {22 febrero De 2020} disponible en: (https://attack.mitre.org/resources/faq/.).

21 Mitre Corporation, “Frequently Asked Questions-sub-techniques” {En línea}. {22 febrero De 2020} disponible en:

(https://attack.mitre.org/resources/faq/.).

22 Mitre Corporation, “Frequently Asked Questions-procedures” {En línea}. {22 febrero De 2020} disponible en: (https://attack.mitre.org/resources/faq/.).

23 Mitre Corporation, “Network Service Scanning” {En línea}. {25 febrero De 2020} disponible en: (https://attack.mitre.org/techniques/T1046/.).

24 Mitre Corporation, “Network Share Discovery ” {En línea}. {26 febrero De 2020} disponible en: (https://attack.mitre.org/techniques/T1135/.).

25 Mitre Corporation, “PowerShell” {En línea}. {24 febrero De 2020} disponible en: (https://attack.mitre.org/techniques/T1086/.).

26 Mitre Corporation, “Process Discovery ” {En línea}. {25 febrero De 2020} disponible en: (https://attack.mitre.org/techniques/T1057/.).

27 Mitre Corporation, “Process Injection” {En línea}. {22 febrero De 2020} disponible en: (https://attack.mitre.org/techniques/T1055/.).

28 Mitre Corporation, “Query Registry ” {En línea}. {25 febrero De 2020} disponible en: (https://attack.mitre.org/techniques/T1012/.).

29 Mitre Corporation, “Remote File Copy ” {En línea}. {26 febrero De 2020} disponible en: (https://attack.mitre.org/techniques/T1105/.).

30 Mitre Corporation, “Scripting ” {En línea}. {24 febrero De 2020} disponible en: (https://attack.mitre.org/techniques/T1064/.).

31 Mitre Corporation, “System Information Discovery ” {En línea}. {25 febrero De 2020} disponible en: (https://attack.mitre.org/techniques/T1082/.).

32 Mitre Corporation, “System Network Configuration Discovery” {En línea}. {25 febrero De 2020} disponible en: (https://attack.mitre.org/techniques/T1016/.).

33 Mitre Corporation, “System Network Connections Discovery” {En línea}. {26 febrero De 2020} disponible en: (https://attack.mitre.org/techniques/T1049/.).

34 Mitre Corporation, “System Owner/User Discovery” {En línea}. {25 febrero De 2020} disponible en: (https://attack.mitre.org/techniques/T1033/.).

35 Mitre Corporation, “System Time Discovery ” {En línea}. {26 febrero De 2020} disponible en: (https://attack.mitre.org/techniques/T1124/.).

36 MORGAN, Steve."2019 Official Annual Cybercrime Report" {En línea}.{3 septiembre de 2019} disponible en: (https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf)

37 STROM,Blake E. APPLEBAUM,Andy.Miller,Doug P.NICKELS,Kathryn C.PENNINGTON,Adam G.THOMAS,Cody B.“MITRE ATT&CK™: Design and Philosophy”.{En línea}. {7 octubre de 2019} disponible en:(https://www.mitre.org/sites/default/files/publications/pr-18-0944-11-mitre-attack-design-and-philosophy.pdf).

38 STROM,Blake E. APPLEBAUM,Andy.Miller,Doug P.NICKELS,Kathryn C.PENNINGTON,Adam G.THOMAS,Cody B.“MITRE ATT&CK™: Design and Philosophy”.{En línea}. {7 octubre de 2019} disponible en:(https://www.mitre.org/sites/default/files/publications/pr-18-0944-11-mitre-attack-design-and-philosophy.pdf).