2023

Informe malware - SmokeLoader

VI CIBERSECURITY FULLSTACK BOOTCAMP
NEREA GÓMEZ BARRASA

1. RESUMEN EJECUTIVO

Este documento presenta una evaluación detallada de "SmokeLoader", un malware del tipo backdoor que ha evolucionado a lo largo de los años, perfeccionándose con el objetivo de eludir detecciones convencionales.

"SmokeLoader" se distingue por su enfoque en campañas de spam y phishing, a menudo propagándose a través de archivos ZIP o RAR que albergan componentes maliciosos. Sus capacidades abarcan desde el robo de credenciales hasta actividades más sofisticadas como el minado de criptomonedas y la distribución de ransomware y otras aplicaciones maliciosas. La continua adaptación y sofisticación de sus tácticas hacen que su detección sea cada vez más desafiante.

El proceso de análisis se ha llevado a cabo empleando múltiples herramientas en distintas fases. Inicialmente, se recurrió a herramientas en línea como VirusTotal, Viper, y Joesandbox para obtener datos estáticos del malware y realizar una primera evaluación de la muestra.

Para un entendimiento más profundo y avanzado, se ha utilizado CAPEv2, la última iteración del framework de CAPE Sandbox. Esta herramienta de código libre automatiza el análisis dinámico del malware, proporcionando una visión detallada de su comportamiento y funcionalidades.

El análisis de la red se ha llevado a cabo utilizando Virustotal y Tria.ge, donde se realizaron escaneos exhaustivos de diversas IPs y URLs sospechosas con el objetivo de identificar y mapear las posibles botnets asociadas al malware.

El evento analizado ha sido registrado en MISP (Malware Information Sharing Platform & Threat Sharing), consolidando así la información obtenida. Esta integración contribuye a la colaboración y compartición de inteligencia de amenazas en la comunidad de ciberseguridad.

Este enfoque multifacético, combinando análisis estáticos y dinámicos, escaneo de red, y colaboración a través de plataformas como MISP, permite una comprensión integral de las amenazas planteadas por "SmokeLoader". Esta

metodología no solo facilita la detección y mitigación efectiva, sino que también contribuye al conocimiento y la prevención de futuras amenazas emergentes.

HERRAMIENTAS UTILIZADAS
PEstudio
Virustotal
Joesandbox
Intezer
Tria.ge
Viper
CAPE

ENLACES DE INTERÉS:

Viper

MISP: id 17

2. CARACTERÍSTICAS DEL MALWARE – ANÁLISIS ESTÁTICO

A continuación, se muestran algunas propiedades estáticas del fichero analizado.

El hash del malware es el siguiente:

SHA256	82d763b6cd97ca240a291c90b8de517232b92cbbe5b593549a61547a30eebf19
MD5	fc5e9ebe857d45fa5f578593342ede53
SHA1	6604067c66d1ef3e30c4563d0a8a8b41b9f9ea5c

Tenemos dos payloads que también se han analizado, sus hashes son los siguientes.

a) B65B.exe

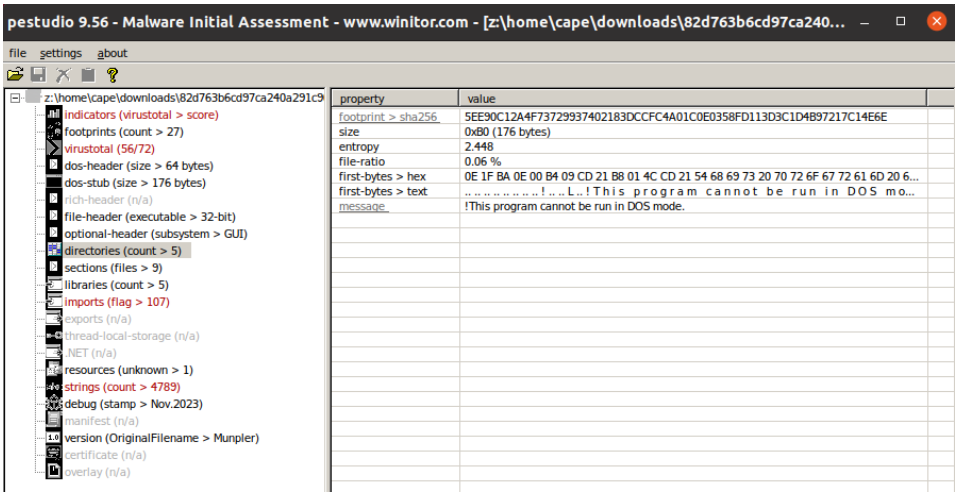
SHA256	0f6db13c0239ca113c19ebeaec8f3243572fd365c3396eff1777115bc08849a1
MD5	33a60439e95f0dfc10016075f97aeb0c
SHA1	fb3595f8a5f9c243e5ad108ff11bc5cb2400ec2b

b) 3928.exe

SHA256	076abc443c05871e2e638ec146f791b06084aafb9dc200410c6aaaacef934239
MD5	e0e783bba2f8e3f0d2da2bded27eceed
SHA1	a723dea176c400de9bdd169b703eb283032ed2cb

A través de PEstudio, tenemos información general de la muestra de malware.

Se nos proporcionan todos estos apartados e información:



3. COMPORTAMIENTO DEL MALWARE

En el análisis dinámico de la muestra mediante CAPEv2, se revela que el malware bajo escrutinio exhibe una sofisticada variedad de técnicas diseñadas para eludir la detección, manipular la gestión de permisos y seguridad, así como controlar la entrada/salida de archivos. Estas tácticas incluyen el uso de scripts como *sleep, SetThreadIdealProcessor, SetKernelObjectSecurity, GetSdlHandle…*

Como se mencionó previamente, este malware se clasifica como una *backdoor,* focalizándose en recopilar información sobre la inicialización del programa y el entorno, mientras monitorea la consola del sistema mediante funciones como *GetcommandLineA* y *ReadConsoleOutputCharacterW.* Su enfoque principal reside en la manipulación del sistema a través de la consola y la recopilación de datos, incluyendo la identificación del alias de la consola, la adaptación al sistema operativo correspondiente, la obtención de datos sobre

usuarios, ventanas y escritorios, la manipulación y carga de bibliotecas DLL, y el control del manejo de archivos.

Adicionalmente, el malware puede abrir el manejo de hilos para la memoria, evitando así escribir en la consola simultáneamente con la víctima o viceversa, asegurando la efectividad de sus acciones. En relación a las secciones, destaca la presencia de una sección *.text* con una entropía significativamente alta, y la importación de librerías KERNEL32 y USER32, ambas vinculadas a la gestión de memoria y la interfaz de usuario.

En términos más concretos, el malware busca recopilar información exhaustiva sobre el sistema operativo, su versión, conexiones de red, archivos, librerías y alias de usuarios. Posteriormente, emplea diversas técnicas para manipular la consola, orientadas a alterar datos de respaldo y obtener información sobre distintos perfiles de usuario. Todo sugiere que el objetivo final de esta amenaza es el robo de credenciales.

En relación a los dos payloads asociados al malware, presentan un comportamiento notablemente similar. Estos componentes miden el tiempo para sincronizar acciones, acceden a archivos, implementan funciones anti-debugging y contienen dos archivos ejecutables entre sus scripts*: Lameros.exe* (nombre original del archivo) y *Bastard.exe* (nombre interno). En términos de secciones, se destaca la presencia de una *.text* con un nivel de entropía elevado.

Es plausible que estos payloads estén diseñados para evitar la detección del malware principal, incorporando funcionalidades anti-debugging y anti-sandbox en su arsenal defensivo.

4. MITRE

MITRE, una organización sin fines de lucro, se ha destacado como pionera en el desarrollo del marco de conocimiento ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge). Este marco es esencial para analizar y comprender el comportamiento de las amenazas cibernéticas. Los resultados MITRE en el análisis de malware proporcionan una valiosa hoja de ruta que detalla las tácticas, técnicas y procedimientos utilizados por los atacantes. Estos resultados son instrumentales para fortalecer las defensas cibernéticas, permitiendo a las organizaciones adaptar sus estrategias de seguridad de manera precisa y eficaz frente a las amenazas actuales.

Descubrimiento

El malware está en continua búsqueda de información del sistema. Trata de detectar virtualización, alcanzar información sobre la configuración del sistema para adaptarse a la misma e incluso recopilar información de la BIOS.

Tiene diversos mecanismos anti-debugging y anti-sandbox sobre archivos y directorios, enumera procesos y registra todas las peticiones.

Busca también conseguir información sobre los usuarios del sistema.

Acceso credenciales

Realiza *dumping* de credenciales en email y navegadores, es decir, extrae información sensible almacenada en correos electrónicos y en los navegadores. Captura cookies de sesión para obtener acceso no autorizado a cuentas y, además, recopila contraseñas almacenadas de manera insegura en archivos locales.

Ejecución

Se trata de un tipo de malware denominado *dropper*, que instala y ejecuta otro malware para ampliar la amenaza. Crea procesos de manera sigilosa para evadir la detección e implementa técnicas para eludir la detección durante procesos de análisis (*anti-debugging*). También utiliza Powershell como herramienta para llevar a cabo acciones maliciosas.

Colección

Extrae información de correos electrónicos almacenados localmente, recopila datos del sistema local para obtener información y utiliza técnicas de ofuscación para ocultar la información recopilada.

Persistencia

Establece mecanismos para iniciar automáticamente en el inicio de sesión del sistema.

Escalada de privilegios

Realiza inyecciones de código malicioso para obtener privilegios elevados.

Evasión

Opera discretamente en segundo plano para evitar detección (*hide artifacts*), elimina rastros y utiliza tácticas como *InstallUtil.exe* para evadir sistemas de detección.

Implementa medidas para identificar y evadir entornos de sandboxing (*anti-sanbox*) y oculta su presencia mediante técnicas de enmascaramiento.

C&C (Comando y Control)

Despliega alertas para evadir sistemas de detección como Suricata y utiliza tácticas específicas para evadir la detección en el tráfico de red.

Emplea peticiones Powershell para ejecutar comandos maliciosos. Aprovecha la red Tor con múltiples saltos para ocultar la comunicación y también establece comunicación cifrada con el mismo fin.

Impacto

Realiza acciones destructivas sobre archivos almacenados en el sistema y cifra datos sensibles para impedir el acceso no autorizado.

Por su parte, los dos payloads de la muestra tienen comportamientos similares, a lo que MITRE respecta:

Descubrimiento

Ambos implementan estrategias para eludir sistemas de detección y ambientes virtualizados. También desarrollan técnicas específicas para identificar y evadir entornos de sandboxing (*anti-sandbox*).

Realizan también una identificación de procesos, es decir, reconocen y controlan procesos para asegurar un acceso persistente y control continuo.

C&C (Comando y Control)

Manipulan el tráfico de red para realizar comunicación con servidores remotos y llevar a cabo operaciones específicas.

Ejecución

Este proceso lo lleva a cabo solo uno de los dos payloads, el *B65B.exe*, y es el de almacenar ejecutables maliciosos en ubicaciones no convencionales para evadir la detección.

Evasión

Utilizan ambos payloads un camuflaje del malware con procesos o archivos que se asemejan al proceso “explorer” (HTTP). También insertan código malicioso en otro proceso en ejecución para ocultar su presencia y borran rastros y archivos ejecutados para dificultar la detección.

Escala de privilegios

Realizan inyecciones de código malicioso en procesos en ejecución para obtener privilegios elevados.

El malware de muestra exhibe un comportamiento altamente sofisticado y multifacético, revelando una amplia gama de tácticas destinadas a eludir la detección, recopilar información sensible y comprometer la seguridad del sistema. En sus acciones de acceso a credenciales, ejecución, colección, persistencia,

escalada de privilegios, evasión y C&C, el malware demuestra una habilidad excepcional para adaptarse al entorno operativo y manipular activamente sistemas y datos. Los payloads asociados, por su parte, refuerzan estas capacidades al sincronizar acciones, implementar funciones anti-debugging y anti-sandbox, y exhibir comportamientos similares. La combinación de estas características sugiere que el objetivo principal del malware es el robo de credenciales, respaldado por una estructura técnica que busca persistencia, evasión y control remoto eficaces. La adopción de técnicas como inyección de código, ofuscación y comunicación cifrada a través de C&C subraya la amenaza significativa que representa este malware en términos de impacto y persistencia.

5. ANÁLISIS DINÁMICO

Estamos ante un malware sofisticado, enfocándose en sus tácticas y comportamientos específicos, así como en la identificación de firmas, comandos y procesos involucrados. Este malware, clasificado como una *backdoor*, destaca por su capacidad para eludir la detección, manipular la gestión de permisos y seguridad, y ejecutar diversas acciones maliciosas con el objetivo final de robo de credenciales.

El malware exhibe una diversidad de acciones estratégicas. Inicia su actividad recolectando y cifrando información del sistema, abordando tácticas anti-debugging y detectando la virtualización para adaptarse al entorno operativo real. Además, realiza borrados anómalos de archivos y emplea técnicas de anti detección, incluyendo intentos de *sleep* durante el análisis.

El intento de conexión a una IP y puerto inactivo revela una estrategia de evasión de detección, mientras que la preferencia por conexiones HTTPS cifradas dificulta la inspección del tráfico. La utilización de Powershell para enviar datos a un host remoto refuerza la complejidad y sofisticación de sus operaciones.

El malware ejecuta una serie de comandos para llevar a cabo sus acciones maliciosas. Entre ellos, destaca la creación de directorios, la manipulación de archivos y el uso de herramientas como *tasklist* y *PING.EXE*. Los procesos específicos involucrados, como *mscorsvw.exe*, *Perceived.pif*,

conhost.exe, explorer.exe, y *cmd.exe*, demuestran la capacidad del malware para interactuar y manipular el sistema operativo.

Asimismo, se observa la creación de una ventana escondida a través del proceso "288D.exe" en la ruta "C:\Users\ama\AppData\Local\Temp\288D.exe". Este archivo ejecutable utiliza el packer UPX para ofuscar su código. Además, se identifica el cargador de malware "SmokeLoader" asociado al proceso "explorer.exe".

El análisis del proceso árbol revela una secuencia de ejecuciones y asociaciones entre procesos. Destaca la creación de una ventana escondida mediante el proceso "82d763b6cd97ca240a29.exe", la asociación de "explorer.exe" con "SmokeLoader", y la ejecución de "regsvr32.exe" para registrar una DLL.

Adicionalmente, se detecta la ejecución de "A89F.exe", que a su vez inicia "AppLaunch.exe", seguido por la presencia de "WerFault.exe" para monitorear y gestionar errores.

En conjunto, este análisis dinámico revela un malware altamente avanzado y adaptativo, con un enfoque claro en el robo de credenciales. Su capacidad para eludir la detección, manipular procesos y establecer conexiones cifradas presenta un desafío significativo para la seguridad. La identificación de firmas, comandos y procesos específicos proporciona una base sólida para la implementación de contramedidas y fortalecimiento de las defensas contra esta amenaza.

El payload *B65B.exe* revela un conjunto de firmas y comportamientos distintivos que reflejan su funcionalidad avanzada y adaptativa. Al enumerar procesos en ejecución y crear procesos en localizaciones sospechosas, el payload demuestra una estrategia proactiva para evadir la detección y mantener la persistencia en el sistema. La generación de tráfico de red en respuesta al proceso de inyección sugiere operaciones de Comando y Control (C&C), mientras que su capacidad para detectar la presencia de antivirus y entornos de virtualización subraya su sofisticación en la evasión de medidas de seguridad convencionales. La conexión vía HTTP al dominio "legdfls2369.com:80" señala

una comunicación activa con un servidor remoto, revelando una posible canalización de datos hacia y desde el sistema comprometido.

En el proceso árbol, la ejecución de "B65B.exe" desencadena una cadena de eventos, incluyendo la asociación con el cargador de malware SmokeLoader a través de "explorer.exe" y la ejecución de subprocesos, destacando la complejidad y la cooperación entre componentes maliciosos.

Los comandos utilizados, como la ejecución de exploradores y tareas específicas en la carpeta del usuario, indican la ejecución de operaciones específicas y la manipulación activa del entorno del sistema.

Similar al primer payload, el 3928.exe también presenta firmas y comportamientos significativos. El acceso a un archivo desde la carpeta pública y la enumeración de procesos en ejecución señalan la búsqueda de información del entorno operativo. La creación de procesos en localizaciones sospechosas y la generación de tráfico de red en respuesta a la inyección indican tácticas de evasión y posibles operaciones de C&C.

La detección de antivirus y entornos de virtualización demuestra una adaptabilidad similar a la del primer payload. La conexión vía HTTP al dominio "legdfls2369.com:80" confirma la interacción continua con un servidor remoto.

En el proceso árbol, la ejecución de "3928.exe" se asocia con el cargador de malware SmokeLoader a través de "explorer.exe" y "svchost.exe", subrayando la colaboración entre distintos componentes maliciosos.

En resumen, ambos payloads exhiben una complejidad y sofisticación notables en sus acciones, indicando una clara coordinación en sus objetivos y estrategias.

6. ANÁLISIS DE RED

Análisis de botnets asociadas al malware

El comportamiento intrusivo del malware en consideración nos ha proporcionado una rica fuente de datos, aunque su enfoque evasivo ha presentado desafíos en el rastreo. La muestra de malware, como previamente

examinado, establece múltiples conexiones con el objetivo de eludir la detección, lo que añade complejidad al seguimiento de su trayectoria. A pesar de estas tácticas evasivas, se ha implementado un escaneo exhaustivo de IPs y URLs sospechosas en un esfuerzo por identificar la botnet subyacente al malware.

El resultado de estas investigaciones revela la presencia de dos botnets distintas, identificadas como "pub1" y "autm", distribuidas a través de diversos dominios. Este hallazgo proporciona una visión más clara de la infraestructura utilizada por los actores maliciosos, permitiéndonos comprender mejor la magnitud y sofisticación de la amenaza.

Análisis de conexiones maliciosas

El malware, al realizar conexiones extensas, demuestra una estrategia deliberada para dificultar la identificación y el seguimiento. Las conexiones, aunque enmascaradas, han sido escudriñadas meticulosamente para discernir patrones y establecer correlaciones con botnets específicas. Este análisis de conexiones es esencial para comprender la infraestructura subyacente y puede proporcionar pistas valiosas sobre el propósito y el alcance de las actividades maliciosas.

Mapeo de botnets

La identificación de las botnets "pub1" y "autm" bajo varios dominios representa un avance significativo en el entendimiento del ecosistema malicioso. El mapeo detallado de estas botnets podría incluir la recopilación de información sobre su estructura, alcance geográfico, y métodos de comunicación. Este proceso es esencial para implementar medidas de mitigación específicas y colaborar con las autoridades pertinentes en la desarticulación de estas redes maliciosas.

Consecuencias potenciales

El descubrimiento de múltiples botnets asociadas al malware indica un potencial impacto significativo en términos de alcance y sofisticación. Estas redes de bots pueden ser utilizadas para diversas actividades maliciosas, desde el robo de información sensible hasta ataques coordinados más amplios. La

evaluación de las consecuencias potenciales es crucial para anticipar y contrarrestar posibles amenazas emergentes.

En resumen, la identificación de las botnets "pub1" y "autm" proporciona una visión detallada de la infraestructura subyacente al malware analizado.

7. RESUMEN GENERAL

El malware en cuestión ha sido vinculado al grupo UAC-0006, el cual resurgió hace unos meses para llevar a cabo ataques de phishing dirigidos a Ucrania, empleando señuelos financieros. Este colectivo de hackers, conocido como UAC-0006, ha estado en el radar de la ciberseguridad desde 2013 hasta julio de 2021. El modus operandi del grupo implica comúnmente el uso de cargadores de archivos JavaScript en la fase inicial de sus ataques.

Los patrones de comportamiento característicos de este adversario se centran en la obtención de acceso a servicios bancarios remotos. El robo de credenciales de autenticación, como contraseñas, claves o certificados, constituye una de sus metas principales. Posteriormente, el grupo lleva a cabo acciones como realizar pagos no autorizados, utilizando, por ejemplo, la ejecución directa del bot HVNC desde los sistemas comprometidos. La campaña actual se destaca por su enfoque en el phishing y su utilización de señuelos financieros como anzuelo, marcando la continuación de las actividades del grupo UAC-0006 en el panorama de amenazas cibernéticas.

El malware en cuestión se revela como una amenaza altamente avanzada centrada en el robo de credenciales. Clasificado como una *backdoor*, su comportamiento multifacético destaca por su capacidad para eludir la detección, manipular permisos y seguridad, y ejecutar acciones maliciosas con enfoque preciso en la recopilación de información sensible.

En el acceso a credenciales, el malware utiliza tácticas sofisticadas como la recopilación y cifrado de datos del sistema, implementando estrategias anti-debugging y detección de virtualización para adaptarse al entorno operativo real. La estrategia de evasión es evidente a través de intentos de conexión a IPs

inactivas y la preferencia por conexiones HTTPS cifradas, añadiendo capas adicionales de complejidad a sus operaciones.

El uso de Powershell para la transferencia de datos a un host remoto subraya la sofisticación en la comunicación y control de la amenaza. Además, la ejecución de comandos específicos, manipulación de archivos y procesos, junto con la creación de una ventana escondida a través del proceso "288D.exe", ilustran la habilidad del malware para interactuar y manipular activamente el sistema operativo.

En el ámbito de la infección, el malware emplea técnicas como la inyección de código y la ofuscación utilizando el packer UPX. La asociación con el cargador de malware "SmokeLoader" a través del proceso "explorer.exe" añade otra capa de complejidad a sus operaciones. La combinación de estas tácticas, respaldada por funciones anti-debugging y anti-sandbox en los payloads asociados, subraya la amenaza sustancial que representa en términos de impacto y persistencia, evidenciando una estructura técnica sólida y altamente adaptativa.

8. MITIGACIÓN Y RECOMENDACIONES

Mitigación efectiva posterior al ataque del malware

Ante un ataque de malware, la respuesta inmediata y bien ejecutada es esencial para minimizar los daños y restaurar la integridad del entorno digital. Las siguientes acciones detallan un enfoque integral para la mitigación de los efectos posteriores a un ataque:

Identificación y aislamiento: La identificación y aislamiento de sistemas comprometidos deben ser ejecutados de manera diligente para evitar la propagación del malware dentro de la red. La velocidad en esta respuesta es clave para contener la amenaza y prevenir daños adicionales.

Restauración desde copias de seguridad confiables: La recuperación de información y sistemas debe basarse en copias de seguridad confiables y actualizadas. Es fundamental verificar que los respaldos estén libres de cualquier rastro de malware

antes de proceder con la restauración, asegurando así la integridad de los datos recuperados.

Análisis forense exhaustivo: La realización de un análisis forense exhaustivo es esencial para comprender la magnitud del ataque, las tácticas empleadas y las vulnerabilidades explotadas. Este proceso no solo contribuye a la recuperación actual, sino que también fortalece la capacidad de la organización para enfrentar futuros incidentes.

Cambio de credenciales: Dado el intento de robo de credenciales, se debe proceder al cambio inmediato de todas las contraseñas y credenciales que podrían haber sido comprometidas durante el ataque. Este paso crítico refuerza la seguridad y limita el acceso no autorizado.

Monitoreo continuo y alertas en tiempo real: La implementación de un monitoreo continuo permite la detección de actividades anómalas o intentos de reinfección. Las alertas en tiempo real facilitan una respuesta inmediata ante cualquier actividad sospechosa, reforzando la seguridad proactiva.

Actualización y escaneo antivirus: Las soluciones antivirus han de estar actualizadas. Un escaneo exhaustivo en todos los sistemas ayuda a identificar y eliminar cualquier rastro persistente del malware, asegurando un entorno limpio y seguro.

Aplicación de parches y actualizaciones: La aplicación rápida de parches y actualizaciones de seguridad en todos los sistemas es esencial para cerrar las vulnerabilidades que podrían haber sido aprovechadas por el malware. Esta medida fortalece las defensas y reduce futuros riesgos.

Capacitación adicional a empleados: Proporcionar capacitación adicional a los empleados es esencial para internalizar las lecciones aprendidas del ataque. Haciendo hincapié en las buenas prácticas de seguridad y la identificación de posibles amenazas, se fortalece la resiliencia de la organización ante amenazas cibernéticas.

Recomendaciones

Enfrentándonos a la complejidad de los riesgos y amenazas cibernéticas, es imperativo establecer estrategias integrales para mitigar riesgos y fortalecer la postura de seguridad. A continuación, se detallan recomendaciones tanto a nivel de concienciación de los empleados como de medidas técnicas para salvaguardar la integridad del entorno digital:

Formación continua de los empleados: La formación constante de los empleados es un pilar fundamental en la defensa contra amenazas cibernéticas. Se debe mantener a los equipos informados sobre las últimas tácticas empleadas por los atacantes, fomentando la conciencia y la capacidad de respuesta frente a posibles ataques.

Implementación de filtros de correo electrónico: A nivel técnico, se recomienda la implementación de filtros de correo electrónico robustos para neutralizar intentos de phishing. La configuración precisa de estos filtros permite bloquear correos electrónicos maliciosos y reducir drásticamente la posibilidad de que los usuarios interactúen con archivos adjuntos comprometidos.

Segmentación de red: Como medida preventiva avanzada, se sugiere la segmentación de la red. Esta estrategia implica la división de la infraestructura en segmentos independientes, limitando así la propagación de malware en caso de una eventual infección. La segmentación proporciona una capa adicional de defensa, contribuyendo a contener y mitigar el impacto de posibles ataques.

Políticas de respaldo y recuperación: Es esencial implementar políticas de respaldo de manera regular. Asegurarse de contar con procedimientos de recuperación de datos efectivos garantiza la capacidad de restaurar sistemas a un estado seguro en caso de un incidente. La realización periódica de respaldos se convierte en una salvaguarda crucial ante la pérdida de datos.

Análisis proactivo de seguridad: La realización de análisis proactivos y regulares de seguridad constituye una práctica esencial. Identificar posibles vulnerabilidades antes de que se materialicen amenazas permite la mejora continua de las medidas de protección. La vigilancia constante y la adaptación a las dinámicas del panorama de amenazas son clave para mantener la seguridad cibernética robusta y efectiva.

Al integrar estas recomendaciones, se establece un enfoque global que abarca desde la concienciación de los empleados hasta medidas técnicas avanzadas, fortaleciendo así la resiliencia de la organización frente a las amenazas en constante evolución.