Propuesta de mejora del sistema PhisHunter para notificaciones que alerten la suplantación de dominios web oficiales.

Monsalve Guarín Néstor Fernando, González Ardila Eymard Alejandro, Caballero Martínez Johan Alexander, Pinzón Mateus Juan David y Perez Cañon Juan Sebastian

Especialización en Seguridad Informática, Fundación Universitaria Compensar

Propuesta de Consultoría

María Fernanda Montero Molina

15 de noviembre de 2024

Esta obra está bajo una Licencia Creative Commons Atribución-NoComercial-CompartirIgual 4.0 Internacional.

Propuesta de mejora del sistema PhisHunter, para notificaciones que alerte suplantación de dominios web oficiales.

Monsalve Guarín Néstor Fernando, González Ardila Eymard Alejandro, Caballero Martínez Johan Alexander, Pinzón Mateus Juan David y Perez Cañon Juan Sebastian

Trabajo de grado presentado como requisito parcial para optar al título de:
Especialización en Seguridad Informática

Director (a):

María Fernanda Montero Molina

Línea de Investigación:
Descriptiva – Consultoría Seminario de Grado
Grupo de Investigación:
Especialización en Seguridad Informática

Fundación Universitaria Compensar
Especialización en Seguridad Informática
Bogotá D.C, Colombia
2024

Resumen

Este documento presenta una propuesta de mejora para la aplicación PhisHunter, enfocada en implementar notificaciones a través de Telegram para detectar suplantación de dominios web. Actualmente, PhisHunter permite a los administradores analizar y gestionar correos electrónicos sospechosos, asignando una puntuación de amenaza y priorizando las respuestas. La mejora propuesta busca optimizar la comunicación y agilizar la respuesta ante incidentes de phishing, enviando alertas instantáneas a los administradores mediante Telegram. Esta integración no solo aumentará la capacidad de respuesta, sino que también facilitará una gestión más eficiente de las amenazas, contribuyendo a una mayor seguridad y protección de la información en la organización.

Palabras clave: Phishing, seguridad e información

Abstract

This document p This proposal presents an enhancement to the PhisHunter application, focused on implementing notifications via Telegram to detect web domain spoofing. Currently, PhisHunter allows administrators to analyze and manage suspicious emails, assigning a threat score and prioritizing responses. The proposed enhancement seeks to optimize communication and streamline response to phishing incidents by sending instant alerts to administrators via Telegram. This integration will not only increase responsiveness, but also facilitate more efficient threat management, contributing to greater security and protection of information in the organization.

Keywords: Phishing, security and information

Contenido

Resumen 3
Abstract 4
Introducción 6
Antecedentes y Justificación 6
Formulación de problema 7
Objetivo general 8
Objetivos específicos 8
Alcances y limitaciones 8
Alcances 8
Limitaciones 9
1. Marco teórico 9
1.1 Phishing: Concepto y Evolución 9
1.2 PhisHunter: Herramienta de Detección en Tiempo Real 10
1.2.1 Automatización de Alertas con la API de Telegram 10
1.3 Marco Regulatorio sobre Phishing 10
1.3.1 Regulación en Colombia: 10
1.3.2 Regulación Internacional: 11
2. Diseño Metodológico 11
2.1 Fase 1: Diagnóstico inicial 13
2.2 Fase 2: Análisis de Efectividad y Propuesta de Mejora 14
2.3 Fase 3: Implementación de la API de Telegram en un Entorno Controlado 15
3. Arquitectura de aplicación 15
4. Diagrama Funcional 17
5. Conclusión 18
6. Recomendaciones 19
7. Referencias 21

Comentado [MFMM1]: En el capítulo 2 solo se presenta una fase 2.1, cuántas fases son?

Introducción

En el dinámico campo de la ciberseguridad, la identificación y mitigación de amenazas emergentes son fundamentales para mantener la integridad y la confidencialidad de los datos. Un análisis reciente en LATAM muestra que aproximadamente el 30% de las organizaciones experimentaron al menos un incidente de seguridad durante 2023, siendo los sectores de gobierno, tecnología y finanzas los más afectados. El phishing, una técnica de ingeniería social que engaña a las víctimas para que divulguen información sensible mediante la suplantación de identidad, sigue siendo una de las amenazas más prevalentes y sofisticadas en el ámbito digital. Este tipo de ataques ha evolucionado de simples correos electrónicos de engaño a campañas dirigidas y altamente sofisticadas, lo que dificulta su detección y mitigación.

Para enfrentar este desafío, es fundamental mejorar la capacidad para identificar en tiempo real dominios asociados con actividades de phishing. En este contexto, herramientas como PhisHunter, que se basa en CertStream, juegan un papel crucial. PhisHunter permite la detección inmediata de dominios recién registrados que podrían estar involucrados en actividades maliciosas. En esta propuesta se presenta una solución automatizada para enviar notificación de estos eventos, a través de la integración con la API de Telegram, esta propuesta optimiza la capacidad de respuesta ante incidentes y facilita una comunicación rápida y efectiva con los equipos de seguridad.

Antecedentes y Justificación

PhisHunter es una aplicación diseñada para detectar ataques de phishing en tiempo real. El phishing es una técnica de ingeniería social utilizada por ciberdelincuentes para obtener información confidencial, como contraseñas y datos bancarios, mediante la suplantación de una entidad confiable. Este tipo de ataque ha aumentado significativamente en los últimos años, afectando tanto a individuos como a organizaciones.

La detección en tiempo real de phishing es esencial para minimizar el impacto de estos ataques. PhisHunter utiliza algoritmos avanzados mediante APIS de CertStream para identificar dominios sospechosos y alertar a los administradores de seguridad de posibles amenazas. Sin embargo, la efectividad de una herramienta de seguridad no solo depende de su capacidad para detectar amenazas, sino también de la rapidez y eficiencia con la que comunica estas detecciones.

La implementación de notificaciones a través de Telegram en PhisHunter se justifica por varias razones:

Rapidez y Eficiencia: Telegram es una plataforma de mensajería instantánea que permite la entrega rápida de mensajes. Al integrar notificaciones de PhisHunter con Telegram, los usuarios pueden recibir alertas de phishing en tiempo real, lo que les permite tomar medidas inmediatas para proteger su información (Mozilla Foundation, 2021).

Accesibilidad: Telegram es una aplicación ampliamente utilizada y accesible en múltiples dispositivos, incluyendo smartphones, tablets y computadoras. Esto asegura que los usuarios puedan recibir notificaciones sin importar el dispositivo que estén utilizando en ese momento (Ciberseguridad LATAM, 2022).

Seguridad: Telegram ofrece características de seguridad robustas, como la encriptación de extremo a extremo y la autenticación de dos factores. Estas características complementan la misión de PhisHunter de proteger a los usuarios contra amenazas de seguridad (Kaspersky, 2021).

Interactividad: A través de Telegram, se pueden implementar bots que no solo envíen notificaciones, sino que también interactúen con los usuarios, proporcionando información adicional y recomendaciones sobre cómo proceder ante una amenaza detectada (Fernandez, 2024).

Adopción y Usabilidad: La integración con una plataforma familiar y de uso común como Telegram puede aumentar la adopción y el uso de PhisHunter, ya que los usuarios no necesitarán aprender a usar una nueva aplicación para recibir alertas (Mozilla Foundation, 2021).

Formulación de problema

A pesar de los avances en la detección de ataques de phishing en tiempo real, la efectividad de herramientas de seguridad como PhisHunter se ve limitada por la ausencia de un sistema de notificaciones eficiente y accesible. Actualmente el uso de PhisHunter en SONDA, los administradores de seguridad no reciben alertas de manera inmediata ni en una plataforma que les resulte familiar y fácil de usar, lo que puede retrasar la respuesta ante amenazas de phishing y aumentar el riesgo de comprometer información sensible.

Comentado [MFMM2]: Incluir citas de referencias consultadas (apellido, año)

Comentado [MFMM3]: Incluir que en SONDA se está utilizando actualmente Phishunter

Comentado [MFMM4R3]:

Objetivo general

Automatizar procesos de PhisHunter que identifique y notifique la suplantación de dominios web oficiales de empresas, con el fin de proteger a los usuarios contra fraudes en línea y salvaguardar la reputación e integridad de las marcas.

Objetivos específicos

Implementar la integración de la API de Telegram en la herramienta PhisHunter, utilizando los lenguajes de programación actuales (PHP, MySQL, HTML, JS) para automatizar el envío de notificaciones de nuevos dominios de phishing detectados.

Configurar alertas personalizables que permitan a los administradores de seguridad recibir notificaciones basadas en palabras clave o categorías específicas, adaptadas a las necesidades de cada cliente.

Optimizar el proceso de monitoreo al reducir la dependencia de supervisión manual, de modo que los equipos de seguridad reciban alertas inmediatas sin necesidad de acceder constantemente a la plataforma.

Evaluar la eficacia de las notificaciones en Telegram mediante un periodo de prueba, analizando su impacto en la reducción de tiempos de respuesta y en la detección oportuna de amenazas de phishing.

Alcances y limitaciones

Alcances

Cobertura en la detección de dominios de phishing: La herramienta permite monitorear dominios en tiempo real, proporcionando alertas inmediatas a través de Telegram sobre posibles amenazas de phishing que involucren marcas o palabras clave relevantes para cada cliente.

Automatización de alertas personalizadas: Mediante la integración con Telegram, administradores de seguridad según criterios específicos, como el tipo de amenaza o palabras clave identificadas, mejorando la precisión y relevancia de las alertas.

Reducción en la dependencia de monitoreo manual: La función de notificaciones de Telegram permitirá a los administradores de seguridad mantener una vigilancia continua sin

necesidad de acceder constantemente a la plataforma, optimizando la respuesta ante incidentes de phishing y permitiendo una reacción rápida.

Limitaciones

Dependencia de palabras clave para detección: La efectividad de la herramienta depende de la precisión de las palabras clave configuradas. Si las palabras clave no son exhaustivas o específicas, pueden omitirse ciertos dominios de phishing, lo que limita la cobertura de la detección.

Limitación en la cobertura de fuentes: Aunque PhisHunter utiliza CertStream para detectar dominios, está limitado a los certificados monitoreados en esta plataforma. Esto podría dejar fuera posibles amenazas de phishing que no emitan certificados reconocidos o utilicen métodos alternativos de validación.

Posibles demoras en notificaciones por conectividad de Telegram: La funcionalidad de notificaciones en tiempo real depende de la conectividad y funcionamiento estable de la API de Telegram. Interrupciones en este servicio o limitaciones de uso intensivo de la API podrían afectar la entrega de alertas oportunas.

Dio formato: Fuente: Sin Negrita

1. Marco teórico

1.1 Phishing: Concepto y Evolución

El phishing ha evolucionado significativamente desde sus primeras apariciones, pasando de simples ataques de correo electrónico a complejas campañas dirigidas que utilizan técnicas avanzadas para evitar su detección. Los ataques de phishing modernos no solo imitan marcas y entidades conocidas con gran precisión, sino que también emplean técnicas de ingeniería social sofisticadas para engañar a las víctimas. Estos ataques pueden tener consecuencias devastadoras, incluyendo la exposición de datos personales, la pérdida financiera y el compromiso de sistemas críticos.

Comentado [MFMM5]: Incluir citas de las referencias consultadas

Las técnicas de phishing han progresado para incluir ataques dirigidos y personalizados, conocidos como spear phishing, que son diseñados específicamente para engañar a individuos o grupos específicos. Este aumento en la sofisticación de los ataques subraya la necesidad de soluciones de detección y respuesta temprana. PhisHunter, como herramienta avanzada en la detección de phishing, proporciona una respuesta efectiva al

identificar dominios potencialmente peligrosos antes de que puedan causar daños significativos, evitando que se propaguen mediante el monitoreo continuo (Rodríguez, 2021).

1.2 PhisHunter: Herramienta de Detección en Tiempo Real

PhisHunter es una herramienta especializada en la vigilancia y detección de dominios potencialmente involucrados en phishing. Utiliza CertStream, un servicio que proporciona un flujo continuo de certificados digitales emitidos por autoridades de certificación. Este flujo permite a PhisHunter identificar rápidamente nuevos dominios que podrían estar asociados con actividades de phishing. La herramienta está configurada para filtrar dominios basados en palabras clave relevantes, lo que permite una detección más precisa y específica.

La información sobre los dominios detectados se almacena en una base de datos MySQL, facilitando su análisis y seguimiento a lo largo del tiempo. Esta capacidad de almacenamiento y análisis continuo permite a los equipos de seguridad realizar investigaciones más profundas y mantener un registro de dominios sospechosos para futuras referencias.

1.2.1 Automatización de Alertas con la API de Telegram

La automatización de procesos es vital para una respuesta rápida y eficiente ante incidentes. PhisHunter propone integrarse con Telegram para enviar alertas automatizadas a los responsables de seguridad cuando se detecte un nuevo dominio sospechoso. Telegram es una plataforma de mensajería segura que permite la creación de bots para la gestión de notificaciones en tiempo real, lo que facilita una comunicación instantánea y efectiva.

La automatización de alertas en Telegram permite reducir tiempos de respuesta y minimizar la intervención manual, proporcionando datos como fecha y hora de detección, URL del dominio, IP de origen y resultados de búsqueda. Esto permite a los equipos de seguridad actuar de forma proactiva, reduciendo el tiempo de uso de dominios de phishing por los atacantes, y mejorando significativamente la capacidad de respuesta ante estas amenazas.

1.3 Marco Regulatorio sobre Phishing

1.3.1 Regulación en Colombia:

En Colombia, la regulación sobre delitos informáticos, incluido el phishing, está enmarcada en la Ley 1273 de 2009. Esta legislación penaliza el uso indebido de sistemas informáticos y establece sanciones para actividades delictivas relacionadas con la seguridad

informática. La Ley 1273 es un componente clave en la estrategia nacional contra los delitos cibernéticos, proporcionando una base legal para la persecución de delitos como el phishing.

Adicionalmente, Colombia bajo la ley 1928 de 2018 hace parte del Convenio de Budapest, sobre Ciberdelincuencia, que establece un marco internacional para la cooperación en la lucha contra el ciberdelito. Este convenio facilita la colaboración entre países para combatir actividades delictivas transnacionales, incluyendo el phishing.

1.3.2 Regulación Internacional:

A nivel internacional, el phishing está regulado bajo diversas normativas y convenios. El Convenio de Budapest proporciona un marco legal para la cooperación internacional en la lucha contra el ciberdelito, incluyendo la criminalización del phishing. Además, el Reglamento General de Protección de Datos (GDPR) de la Unión Europea exige a las organizaciones que implementen medidas adecuadas para proteger los datos personales, lo que incluye la identificación y mitigación de ataques de phishing.

Estas regulaciones internacionales enfatizan la necesidad de medidas proactivas para la protección de datos y la prevención de ataques de phishing, estableciendo estándares para la seguridad de la información y la cooperación entre jurisdicciones.

2. Diseño Metodológico

El enfoque PHVA establece un ciclo claro con el objetivo de garantizar la efectividad en el desarrollo de proyectos. Este proceso nos permitirá verificar que cada una de las fases del proyecto se ejecute de forma continua, permitiendo la evaluación del comportamiento, funcionamiento con el fin de identificar y corregir fallos de la integración que hemos realizado en el software de SONDA para mitigar y mejorar los tiempos de respuesta y de acción por parte del cliente afectado.

En la Ilustración 1 se presenta las diferentes fases de la metodología PHVA, con el cual se busca la mejora continua en la gestión y optimización de los procesos que se ejecutan en la aplicación PhisHunter, en la **¡Error! No se encuentra el origen de la referencia.** se observa el cronograma de actividades planteadas para el desarrollo e implementación de la mejora de PhisHunter y en la Ilustración 3 se muestran las fases a tener en cuenta en la ejecución de las mejoras e implementación del sistema de notificaciones en PhisHunter

Planear	Hacer	Verificar	Actuar
•Definir objetivos •Identificar requerimientos •Desarrollar un plan de proyecto •Cronograma y asignación de recursos	•Desarrollo de la automatización del software •Integración con el sistema de mensajeria Telegram •Realización de pruebas iniciales	•Monitoreo de rendimiento •Evaluación de resultados •Revisión del desempeño •Revisión de la retroalimentación	•Implementación de mejoras •Documentación y capacitación •Preparación para el despliegue •Revisión periodica

Ilustración 1. Metodología PHVA

	Agosto				Septiembre				Octubre				Noviembre				
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	Recursos necesarios	Impacto esperado
Planteamiento Problema																	
Definir objetivos																	
FASE																	
Actividad 1																	
Analisis conceptual																Conocimiento del sistema actual	Mejora la eficiencia de detección
Estudio de viabilidad																Documentación tecnica, API telegram	confirmar si es posible la integración
FASE 2																	
Diseño de la arquitectura																Software de diagramación	Facilitar la futura implementación
Definicion reglas de negocio																Documentación del sistema	Reducir falsas alarmas
Creación flujos de notificación																Conocimientos de telegram, sistema actual	Mejora en la claridad de la comunicación
FASE 3																	
Evaluación de impacto de la seguridad																Herraientas analisis de seguridad	Integración segura sin comprometer el sistema
Plan de monitoreo y mantenimiento																Herramientas de monitoreo	Mantener la eficacia del sistema
Redacción de la propuesta																Software de documentación	Propuesta bien estructurada
Sutentación																Software de presentación	Obtener feedback

Ilustración 2. Diagrama de proyección de tiempos

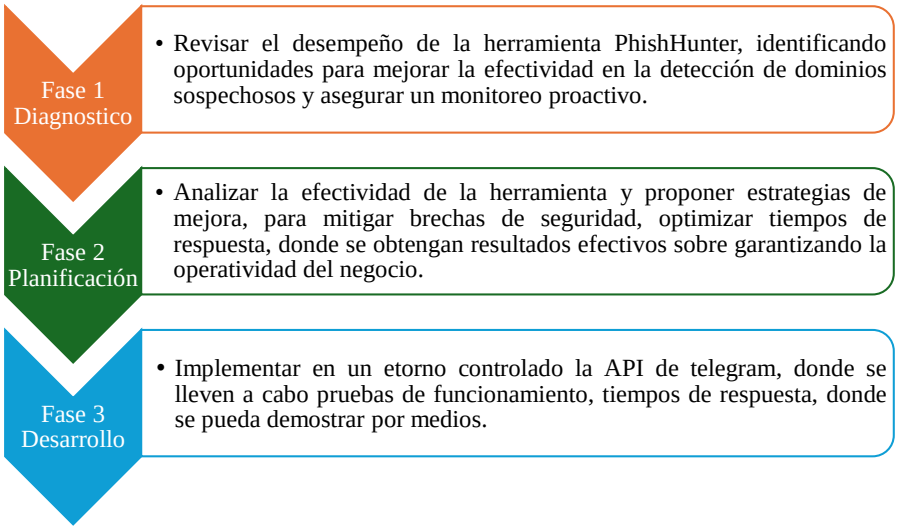


Ilustración 3. Fases desarrollo de tareas

Plan de Trabajo.

2.1 Fase 1: Diagnóstico inicial

Se llevó a cabo un periodo de evaluación exhaustiva de la herramienta PhisHunter durante un tiempo prudente, en el cual se identificaron múltiples dominios asociados a entidades bancarias, sospechosos de actividades de phishing. Este periodo permitió analizar el rendimiento y la precisión de la herramienta en la detección en tiempo real de estos dominios. Además, se implementó un monitoreo constante con inspección visual detallada, lo que ayudó a evaluar la efectividad del sistema en la identificación y alertas tempranas sobre amenazas potenciales, asegurando una respuesta oportuna ante la aparición de posibles ataques de phishing.

Entrega: En la Ilustración 4 e Ilustración 5 se muestra evidencia de la efectividad de la plataforma en la detección de dominios de phishing, destacando la necesidad de que el especialista en seguridad realice un monitoreo continuo de la herramienta para asegurar una respuesta oportuna ante posibles amenazas.

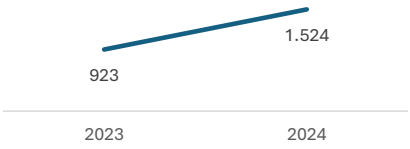


Ilustración 4 Dominios Davivienda

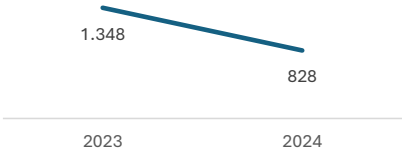


Ilustración 5 Dominios Bancolombia

2.2 Fase 2: Análisis de Efectividad y Propuesta de Mejora

Actividades:

Actualmente, la plataforma permite un monitoreo continuo de dominios de phishing, pero requiere la supervisión constante de un especialista para revisar visualmente cada detección. Se propone optimizar este proceso mediante la integración de notificaciones en tiempo real a través de Telegram, permitiendo que las alertas lleguen directamente al equipo de seguridad sin necesidad de acceder continuamente a la plataforma, lo cual agiliza la respuesta ante posibles amenazas y mejora la eficiencia operativa.

Entrega: Grafico en Ilustración 6 de estimación de tiempos empleados y con reducción al momento de implementar la API de Telegram, tomando como base la formula Tiempo total de análisis = dominios detectados × tiempo por dominio

Comentado [MFMM6]: No está en la tabla de contenido

Con formato: Sangría: Primera línea: 1,25 cm

Comentado [MFMM7]: Incluir resultados del informe y qué análisis se realizó

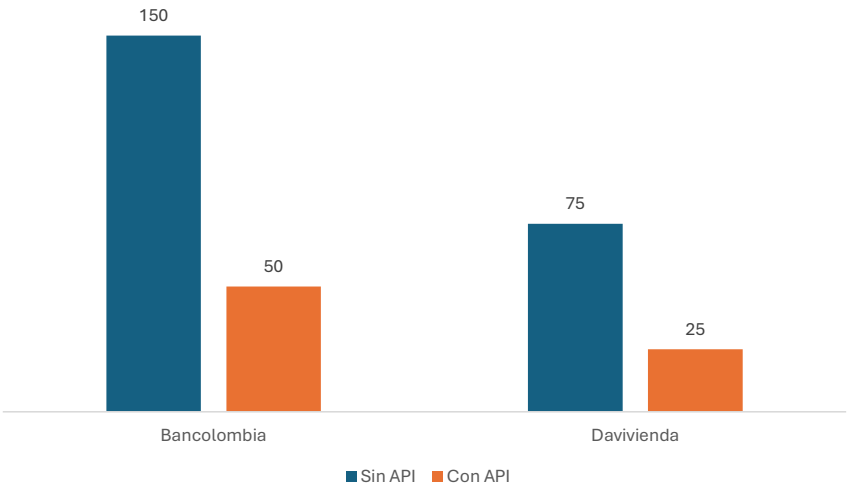


Ilustración 6. Gráfico de reducción de tiempos en detección en minutos de dominios web

2.3 Fase 3: Implementación de la API de Telegram en un Entorno Controlado

Comentado [MFMM8]: No está en la tabla de contenido

Actividades:

Implementar la API de Telegram utilizando los lenguajes de programación actuales de la herramienta (PHP, MySQL, HTML) en un entorno controlado para realizar pruebas exhaustivas de funcionamiento y medir los tiempos de respuesta en la emisión de alertas. Durante esta fase, se recopilarán datos estadísticos sobre el rendimiento de la integración, analizando tanto la precisión como la velocidad de las notificaciones automáticas, además del impacto en la reducción de la supervisión manual. Estos datos permitirán afinar y optimizar el sistema para garantizar que las notificaciones incluyan información completa (fecha, hora de detección, URL, IP de origen) y faciliten una respuesta proactiva por parte del equipo de seguridad ante posibles dominios de phishing.

3. Arquitectura de aplicación

La arquitectura de esta aplicación permite validar dominios en tiempo real usando CertStream. El navegador del administrador de seguridad envía solicitudes al servidor web, que procesa la información y se conecta a la base de datos para obtener o almacenar datos.

CertStream envía actualizaciones de certificados SSL al backend mediante WebSocket, donde un módulo en JavaScript recibe y procesa estos datos. Luego, el validador de dominios analiza los certificados para identificar posibles amenazas. Finalmente, los resultados se almacenan o se muestran en el frontend para el administrador de seguridad como se muestra en Ilustración 7 e Ilustración 8.

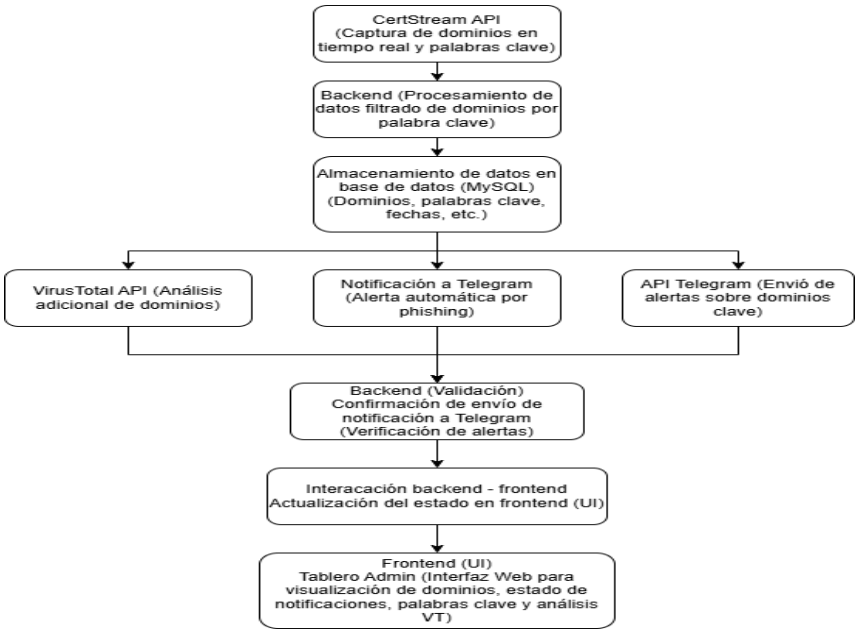


Ilustración 7. Arquitectura de funcionamiento de PhisHunter

Con la integración de Telegram, se implementa el proceso de notificaciones mediante un bot, el cual permita notificar a la mayor brevedad posible, la suplantación de dominios web.

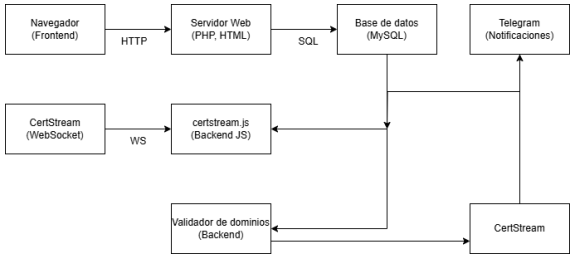


Ilustración 8. Arquitectura de PhisHunter con integración de API Telegram

4. Diagrama Funcional

En la Ilustración 9 se presenta la nueva funcionalidad de la aplicación PhisHunter en conjunto con la integración de notificaciones por Telegram.

Comentado [MFMM9]: Referenciar la ilustración 6

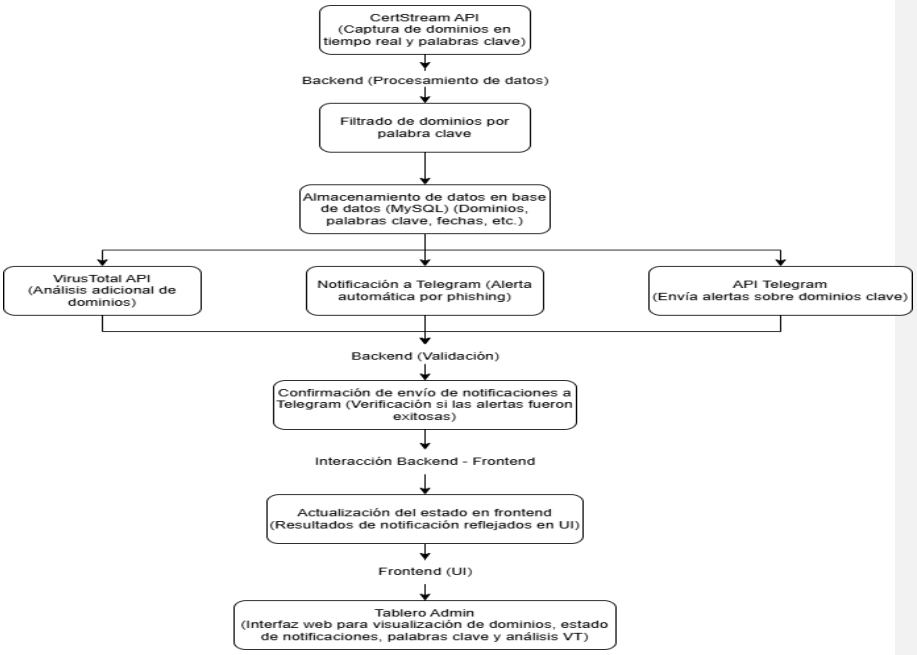


Ilustración 9. Diagrama funcional nueva versión de PhisHunter

Para implementar la integración con Telegram en el aplicativo PhisHunter, se realizó un análisis de los requisitos de notificación de los dominios. Se desarrolló una API que permite enviar alertas automáticas a través de Telegram, asegurando que los administradores de seguridad reciban notificaciones de nuevas detecciones en tiempo real. Se configuraron los requisitos necesarios como lo es el bot que recibirá las notificaciones. Las pruebas se llevaron a cabo en un ambiente de desarrollo aislado y se utilizaron casos de prueba específicos para verificar la funcionalidad y la robustez del sistema. Finalmente, tras ajustes y validaciones, se logró una comunicación eficaz y directa con los usuarios.

Comentado [MFMM10]: Describir qué se presenta en cada ilustración

En la Ilustración 10 se muestra el funcionamiento adecuado de las notificaciones de Telegram al identificar un nuevo dominio.

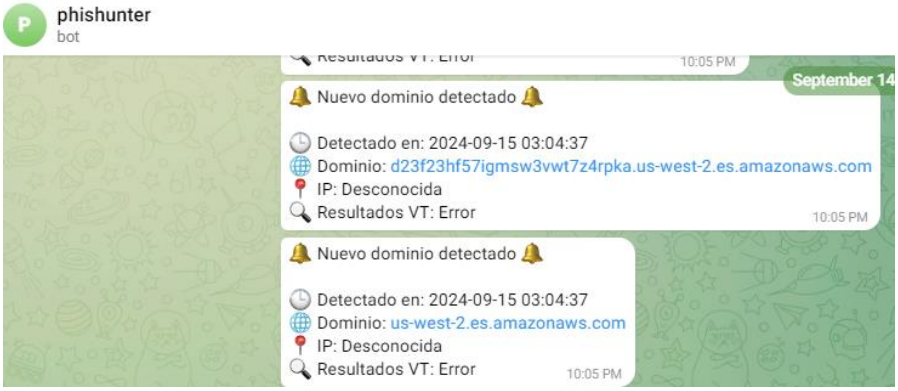


Ilustración 10. Chat de notificación de suplantación de dominios

5. Conclusión

- La integración de PhisHunter con la API de Telegram supone un avance importante en la detección y respuesta al phishing, permitiendo alertas en tiempo real que mejoran la capacidad de respuesta y cumplen con estándares de ciberseguridad nacionales e internacionales. Con esta implementación, las notificaciones sobre suplantación de dominios se enviarán desde el perfil administrador, proporcionando una solución proactiva para proteger a usuarios y organizaciones frente a amenazas en constante evolución.
- La propuesta de mejora en el proceso de gestión de PhisHunter destaca la importancia de una respuesta rápida ante incidentes de phishing. La integración con Telegram, permite obtener notificaciones en tiempo real, representa una mejora significativa al proceso actual. Esta optimización reduce la dependencia de la supervisión manual, agilizando la reacción ante potenciales amenazas y cumpliendo con el objetivo de mejorar los tiempos de respuesta.
- Se realizó un diagnóstico exhaustivo de PhisHunter, donde permitió identificar áreas de mejora, especialmente en la precisión de detección y en la necesidad de notificaciones automáticas. Esta evaluación fue crucial para justificar los cambios propuestos y asegurar que la herramienta cumple con sus objetivos de protección y prevención en tiempo real.
- La integración de notificaciones en tiempo real no solo mejora la capacidad de respuesta, sino que también reduce el riesgo de pérdida de datos o daños a la

reputación de la organización al poder mitigar amenazas de phishing de forma inmediata.

- El proyecto PhisHunter y sus mejoras contribuyen de manera efectiva a los objetivos estratégicos de seguridad de los clientes, como la protección de datos y la integridad de la información. Al mejorar los procesos de detección y respuesta, PhisHunter se alinea con los estándares de seguridad y las normativas regulatorias vigentes.
- El proyecto fomenta la implementación de mejoras continuas al utilizar la metodología PHVA (Planear, Hacer, Verificar y Actuar), lo que permite ajustar y optimizar constantemente el sistema en función de nuevas amenazas y avances tecnológicos. Este enfoque asegura que PhisHunter mantenga su efectividad y relevancia en el tiempo.

6. Recomendaciones

- Se recomienda establecer un plan de capacitación regular para el equipo de seguridad, asegurando que estén al tanto de las funcionalidades y nuevas capacidades del sistema PhisHunter. Esto ayudará a maximizar el uso de la herramienta y a que el equipo esté preparado para reaccionar con rapidez y precisión ante cualquier incidente.
- La elección de Telegram ha sido una eficaz, pero es importante, considerar la integración de PhisHunter con otras plataformas de comunicación o mensajería de texto utilizadas en la organización, con el objetivo de aumentar la accesibilidad y asegurar que las alertas lleguen al equipo sin importar la plataforma preferida de cada usuario.
- La seguridad de la integración con Telegram es crucial, para evitar cualquier posible brecha o incidente de seguridad, por este motivo, es indispensable contar con ciertos procesos de pruebas de penetración periódicas en la API y aplicar protocolos de seguridad robustos, como autenticación de dos factores y cifrado adicional, para minimizar riesgos.
- El proceso de integración de PhisHunter junto a Telegram requieren conectividad a Internet, por este motivo, es recomendable diseñar y plantear un plan de contingencia para casos de interrupción en el servicio. Esto podría incluir notificaciones alternativas, como mensajes SMS o correos electrónicos, para asegurar que el equipo de seguridad reciba las alertas incluso en situaciones de conectividad limitada.

- Desarrollar y mantener un manual de procedimientos actualizado para el equipo de seguridad lo cual ayudará a estandarizar la respuesta ante incidentes de phishing. Este manual debe incluir instrucciones sobre cómo reaccionar a alertas de PhisHunter, así como protocolos de comunicación y escalación para casos críticos.
- Para una gestión centralizada y un análisis más profundo de las alertas de seguridad, se recomienda considerar la integración de PhisHunter con una plataforma SIEM, donde permitiría consolidar las alertas en un solo sistema y mejorar la correlación de eventos para detectar patrones de ataque complejos.

7. Referencias

Origen y evolución de las técnicas de phishing en el mundo • Sello Legal Abogados. (n.d.). Retrieved November 12, 2024, from https://sellolegal.com/blog/origen-y-evolucion-de-las-tecnicas-de-phishing-en-el-mundo/

Ávila Niño, F. Y., & Rincón Núñez, P. M. (2023). Inclusión de la formación en prevención y atención de delitos informáticos en la educación policial. *Revista Educación*. https://doi.org/10.15517/revedu.v47i2.53905

Estancona Pérez, A. A. (2023). FINANCIAL INSTITUTIONS LIABILITY IN CASE OF BANK ACCOUNTS HACKING. IN PARTICULAR, "PHISING" CASES. *Actualidad Jurídica Iberoamericana*, 18.

Kitsios, F., Chatzidimitriou, E., & Kamariotou, M. (2023). The ISO/IEC 27001 Information Security Management Standard: How to Extract Value from Data in the IT Sector. *Sustainability (Switzerland)*, 15(7). https://doi.org/10.3390/su15075828

Ley de delitos informáticos colombiana, el convenio de Budapest y otras legislaciones: Estudio comparativo. (2023). *Revista de Ciencias Sociales*. https://doi.org/10.31876/rcs.v29i2.39981

López Sánchez, J. (2020). Métodos y técnicas de detección temprana de casos de phishing. *Universitat Oberta de Catalunya (UOC)*. Máster En Tecnologías y Seguridad de La Información., TFM.

Moise, A. C. (2024). Procedural Aspects of the Second Additional Protocol to the Council of Europe Convention on Cybercrime. *Bulletin of the Transilvania University of Braşov. Series VII: Social Sciences • Law*. https://doi.org/10.31926/but.ssl.2023.16.65.3.23

Moreno, P., Paucar, C., & Cajas, C. (2022). Regulación global para evitar la suplantación de identidad digital. *Universidad y Sociedad*, 14(6).

Peláez, H., & Riascos, A. (2020). La protección de datos personales y la privacidad en Internet. El caso de Colombia. *Working Paper*, 1(2).

Putra, A. P., & Soewito, B. (2023). Integrated Methodology for Information Security Risk Management using ISO 27005:2018 and NIST SP 800-30 for Insurance Sector.

International Journal of Advanced Computer Science and Applications, 14(4). https://doi.org/10.14569/IJACSA.2023.0140468

Rodríguez, M. P. (2021). Ciberseguridad en la justicia digital: recomendaciones para el caso colombiano. *Revista UIS Ingenierías*, 20(3). https://doi.org/10.18273/revuin.v20n3-2021002

von Grafenstein, M., Kiefaber, I., Heumüller, J., Rupp, V., Graßl, P., Kolless, O., & Puzst, Z. (2024). Privacy icons as a component of effective transparency and controls under the GDPR: effective data protection by design based on art. 25 GDPR. *Computer Law and Security Review*, 52. https://doi.org/10.1016/j.clsr.2023.105924

Consejos de seguridad y privacidad en Telegram. (2021, enero 18). Kaspersky. https://www.kaspersky.es/blog/telegram-privacy-security/24542/

De Nicola, M. (2021, junio 13). *Cómo configurar la privacidad y seguridad en Telegram*. Ciberseguridadlatam.com. https://www.ciberseguridadlatam.com/2021/06/13/como-configurar-la-privacidad-y-seguridad-en-telegram/

Fernández, D. C. (2024, agosto 26). Telegram y la seguridad de los mensajes: Un análisis del cifrado. *Redes Sociales*. https://www.redes-sociales.com/telegram-seguridad-mensajes-cifrado/

(S/f). Mozilla.org. Recuperado el 14 de noviembre de 2024, de https://foundation.mozilla.org/es/privacynotincluded/telegram/