15-5-2026

Act 18. Modelo diamante

Lopez Lopez Josue Emmanuel 182078
Mata Martinez Aaron Efraim 179419
Rodriguez Hernandez Edgar Omar 177888
Rodriguez Morin Estefano Alessandro 178584
Ros Padilla Ivan 177573
Salinas Carrillo Mauricio Josafat 177406
UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSI
PROFESOR: SERVANDO LOPEZ CONTRERAS

Parte 01. Comprensión del modelo (Caso Canvas - Mayo 2026)

Elemento	Descripción	Ejemplo práctico (Caso Canvas 2026)
Adversario	El actor o grupo responsable del ataque.	ShinyHunters: Grupo de ciberdelincuencia de élite que reapareció para realizar este ataque masivo y extorsión pública.
Capacidad	Herramientas, técnicas y procedimientos (TTPs) utilizados.	Explotación de vulnerabilidad en cuentas "Free-for-Teacher" y uso de fallos de día cero (0-day) en el sistema de tickets de soporte para escalar privilegios.
Infraestructura	Recursos lógicos que conectan al adversario con la víctima.	Infraestructura de AWS (Amazon Web Services) de Instructure, dominios de C2 ocultos y la red TOX para las comunicaciones de extorsión.
Víctima	El objetivo principal y secundarios del ataque.	Canvas (Instructure) como víctima primaria; casi 9,000 instituciones educativas y sus 275 millones de usuarios como víctimas secundarias.

Adversario:

Se mostraron muy activos en redes sociales (como X) publicando capturas de pantalla de los paneles de administración de Canvas para presionar el pago.

Infraestructura:

El punto crítico fue el acceso a los *buckets* de almacenamiento en la nube donde residían los 3.65 TB de datos.

Capacidad:

No fue un simple robo de contraseñas, sino un encadenamiento de vulnerabilidades que les permitió tomar control de los portales de inicio de sesión de las escuelas.

Parte 02. Análisis de evento (Modelo Diamante: Caso Canvas Mayo 2026)

Metacaracterística	Descripción del evento
Marca de tiempo	30 de abril al 12 de mayo de 2026. El ataque inicial fue el 30/04; la segunda intrusión y defacement ocurrieron el 07/05, con cierre de negociaciones el 11/05.
Fase	Acciones sobre los objetivos (Exfiltración y Extorsión). El evento incluyó el robo de 3.65 TB de datos y el compromiso de los portales de inicio de sesión (*defacement*).
Resultado	Exitoso (Crítico). ShinyHunters logró la exfiltración masiva y forzó a Instructure a pagar un rescate para evitar la filtración de 275 millones de registros.
Dirección	Multidireccional. *Outbound* para la exfiltración de los 3.65 TB y *Inbound* para el compromiso de los portales de login (330 instituciones afectadas directamente).

Metodología	Explotación de vulnerabilidad en cuentas "Free-for-Teacher". Usaron estas cuentas para escalar privilegios y acceder a sistemas de soporte/producción.
Recursos	Vulnerabilidad de día cero en tickets de soporte, infraestructura de almacenamiento AWS, y plataforma de comunicación cifrada TOX para la negociación.

Volumen de datos:

3.65 Terabytes (uno de los robos más grandes en el sector educativo).

Impacto:

Afectó a casi 9,000 escuelas a nivel mundial en plena semana de exámenes finales.

Persistencia:

Lo más interesante para el modelo es que el atacante volvió a entrar el 7 de mayo para burlarse de los parches de seguridad de la empresa, demostrando que aún tenían acceso (infraestructura comprometida no saneada).

Parte 03. Relación con la Kill Chain

Evento	Fase Kill Chain
Envío de phishing	Entrega (Delivery): Los atacantes enviaron correos dirigidos a personal con cuentas "Free-for-Teacher" para obtener credenciales iniciales.

Detección de malware	Instalación (Installation): Se refiere al momento en que el sistema detecta la presencia de scripts maliciosos o herramientas de persistencia dejadas por el grupo.
Ejecución del malware	Explotación (Exploitation): El código malicioso aprovecha la vulnerabilidad de día cero en el sistema de tickets de soporte para elevar privilegios.
Conexión a C2	Comando y Control (C2): El canal establecido para que ShinyHunters enviara comandos a la infraestructura de Canvas y coordinara la exfiltración.

Aunque la tabla cubre los puntos básicos, el incidente de mayo de 2026 tuvo una fase de Acciones sobre los objetivos muy marcada:

- **Exfiltración:** El robo de los 275 millones de registros.
- **Extorsión:** El uso de la red TOX para negociar el pago del rescate tras demostrar que tenían el control de los portales de login.

Parte 04. Hilos de actividad

Hilo 1: Compromiso Inicial (Víctima 1 - Administrador)

Este hilo representa la entrada al entorno de Canvas. El adversario establece su cabeza de playa.

- **Evento 1:** Envío y apertura de Phishing dirigido. (**Fase:** Entrega)
- **Evento 2:** Instalación de malware tras la ejecución del archivo adjunto. (**Fase:** Instalación)
- **Evento 3:** El malware contacta al servidor C2 del atacante para recibir instrucciones. (**Fase:** Comando y Control)
- **Evento 4:** Configuración del host como **Proxy/Jump box**. El atacante ahora tiene un pie dentro de la red interna de la organización.

Hilo 2: Movimiento Lateral (Víctima 2 - Servidor de Base de Datos)

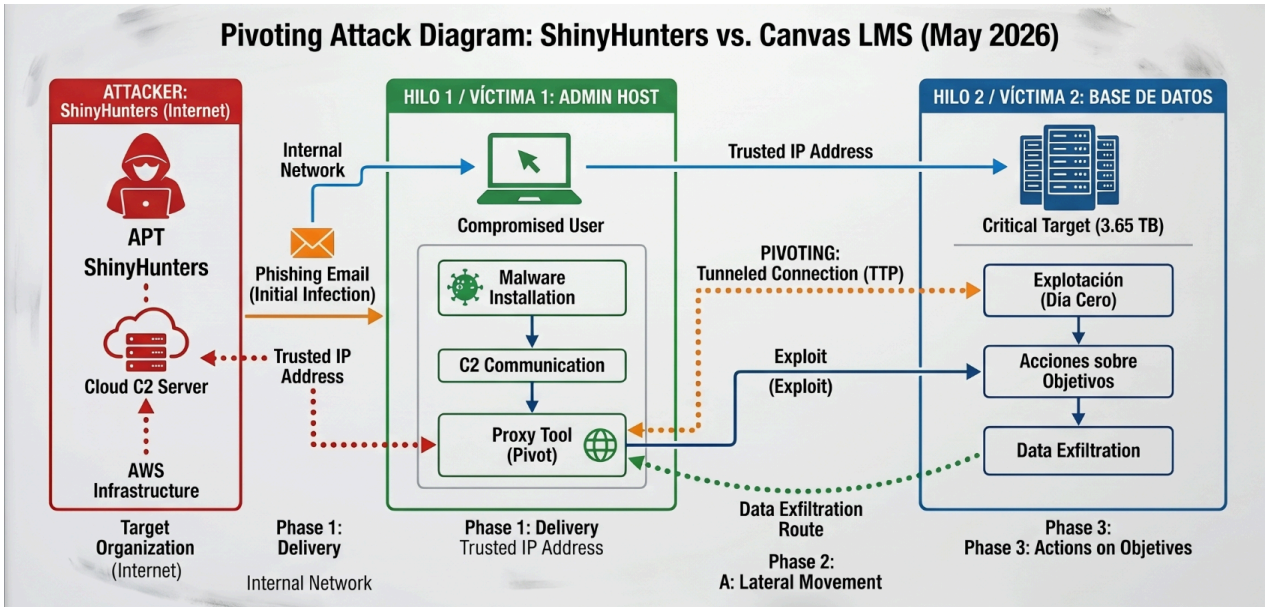
Aquí es donde el atacante utiliza la infraestructura de la Víctima 1 para atacar a la Víctima 2, evadiendo firewalls perimetrales.

- **Evento 1:** Escaneo de red interna desde el host comprometido (Víctima 1). (**Fase:** Reconocimiento interno)
- **Evento 2:** Explotación de vulnerabilidades o uso de credenciales robadas para acceder al servidor. (**Fase:** Explotación)
- **Evento 3:** Extracción de los 3.65 TB de datos hacia el exterior a través del túnel creado en el Hilo 1. (**Fase:** Acciones sobre los objetivos)

Relación entre ambos: Pivoting (Salto)

La relación se define como un **Ataque Transversal**. El diamante de la Víctima 1 se conecta con el de la Víctima 2 a través del vértice de **Infraestructura**.

> **Explicación del Pivoteo:** El host de la Víctima 1 deja de ser solo un objetivo y se convierte en **Infraestructura del Atacante**. Para la Víctima 2, el "atacante" parece ser el Administrador (Víctima 1), ocultando el verdadero origen de ShinyHunters.



Referencias Bibliográficas

- **Caltagirone, S., Pendergast, A., & Betz, C.** (2013). *The Diamond Model of Intrusion Analysis*. Center for Cyber Threat Intelligence and Threat Hunter Intelligence. Recuperado de http://www.activeresponse.org/wp-content/uploads/2013/07/diamond_model.pdf
- **Hutchins, E. M., Cloppert, M. J., & Amin, R. M.** (2011). *Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains*. Lockheed Martin Corporation.
- **Instructure Security Operations.** (2026, mayo). *Incident Response Report: May 2026 External Breach and Data Exfiltration*. official Instructure Security Blog.
- **Krebs, B.** (2026, 12 de mayo). *ShinyHunters strikes again: The Canvas LMS 3.65TB data breach explained*. Krebs on Security.
- **MITRE ATT&CK.** (2024). *Technique: Lateral Movement through Proxying (T1090)*. Recuperado de https://attack.mitre.org/techniques/T1090/
- **The Hacker News.** (2026, mayo). *Canvas LMS targeted by ShinyHunters: Millions of student records at risk*. Recuperado de https://thehackernews.com