UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

Universidad Politécnica de San Luis Potosí

Ingeniería en Tecnologías de la Información

Actividad 18

Análisis de intrusiones con el modelo diamante

Integrantes:

Coronado Noriega Jesús Olaf	178991
De La Rosa Rodríguez Erik	177700
González Reyes Felipe de Jesús	181134
Mendoza Aguado Karina	179859
Serrano Zermeño Leonardo	177301
Pérez Ventura Juan Alejandro	180370

Materia:

CNO V: Seguridad Informática

Docente:

Servando López Contreras

San Luis Potosí, S.L.P.
15 de mayo de 2026

Índice

1. Introducción **3**

2. Objetivos **3**

2.1. Objetivo general 3

2.2. Objetivos específicos 3

3. Parte 01. Comprensión del modelo diamante **4**

4. Parte 02. Análisis de evento con el modelo diamante **5**

4.1. Escenario base 5

4.2. Descomposición del incidente en eventos 6

4.2.1. Evento 1. Detección de malware en equipo víctima 6

4.2.2. Evento 2. Identificación de dominios C2 dentro del malware 7

4.2.3. Evento 3. Resolución de dominios C2 a direcciones IP externas 7

4.2.4. Evento 4. Múltiples hosts conectándose a las IP externas 8

4.2.5. Evento 5. WHOIS/IP revela posible origen del atacante 8

5. Identificación de elementos en el escenario **9**

5.1. ¿Quién es el adversario en este escenario? 9

5.2. ¿Cuál es la capacidad utilizada? 9

5.3. ¿Qué tipo de infraestructura se emplea? 9

5.4. ¿Quién es la víctima primaria? 9

5.5. ¿Existe evidencia de movimiento lateral? 10

6. Parte 03. Relación con la Cyber Kill Chain **10**

7. Parte 04. Hilos de actividad **11**

7.1. Escenario tipo APT 11

7.2. Diagrama de hilos de actividad 12

7.3. Descripción de los hilos 12

8. Síntesis del análisis diamante **13**

9. Recomendaciones de respuesta y contención **13**

10. Conclusión **14**

Referencias **15**

1. Introducción

El presente documento desarrolla la **Actividad 18: Análisis de intrusiones con el modelo diamante**. El propósito es identificar, estructurar y correlacionar eventos de ciberataques mediante el Modelo Diamante del Análisis de Intrusiones, relacionando sus elementos principales con la Cadena de Eliminación Cibernética, conocida como *Cyber Kill Chain*.

El escenario analizado describe una organización que detecta comportamiento anómalo en un equipo: la víctima identifica malware, el malware contiene dominios de Comando y Control, dichos dominios resuelven a direcciones IP externas, los registros muestran múltiples hosts conectándose a esas IP y la información WHOIS/IP sugiere un posible origen del atacante. A partir de esos datos, se construye un análisis técnico que separa los elementos del modelo, clasifica los eventos, identifica el adversario probable y explica la relación entre dos hilos de actividad.

2. Objetivos

2.1. Objetivo general

Aplicar el Modelo Diamante del Análisis de Intrusiones para identificar, estructurar y correlacionar eventos de ciberataques, relacionándolos con la Cadena de Eliminación Cibernética para comprender el comportamiento del adversario.

2.2. Objetivos específicos

1. Identificar y clasificar los elementos del modelo: adversario, capacidad, infraestructura y víctima.
2. Analizar un incidente realista y descomponerlo en eventos de intrusión.
3. Relacionar los eventos detectados con fases de la *Cyber Kill Chain*.
4. Representar los hilos de actividad y explicar la relación de pivote entre una víctima primaria y una segunda víctima.

3. Parte 01. Comprensión del modelo diamante

El Modelo Diamante permite analizar un evento de intrusión mediante cuatro elementos centrales: **Adversario**, **Capacidad**, **Infraestructura** y **Víctima**. La utilidad del modelo está en que obliga a no ver el incidente como un evento aislado, sino como una relación entre quién ataca, con qué medios, por dónde opera y contra quién se dirige la actividad.

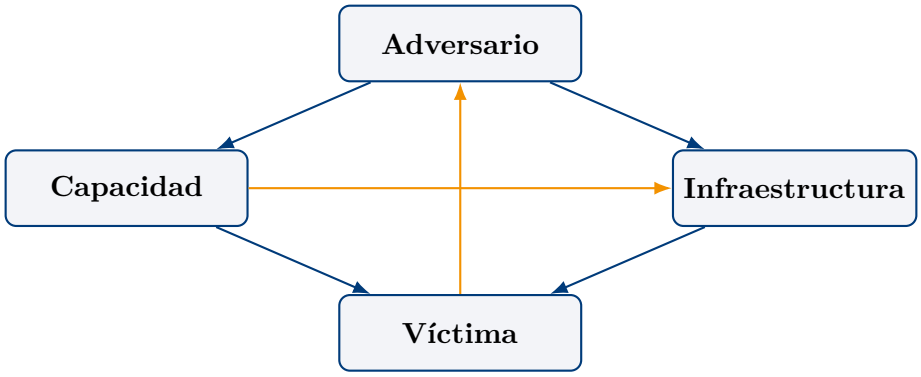

Figura 1: Representación conceptual del Modelo Diamante del Análisis de Intrusiones.

Elemento	Descripción	Ejemplo práctico
Adversario	Entidad responsable de conducir o dirigir la intrusión. Puede ser un atacante individual, grupo criminal, actor interno malicioso, grupo APT o un operador externo que controla la campaña.	Operador que envía phishing a un administrador y controla dominios C2 para mantener comunicación con los equipos comprometidos.
Capacidad	Herramientas, técnicas, procedimientos y recursos técnicos usados para ejecutar la intrusión. Incluye malware, scripts, exploits, credenciales robadas y métodos de evasión.	Malware con comunicación C2, correo de phishing, ejecución de payload y posible uso del host comprometido como proxy.
Infraestructura	Sistemas, redes, dominios, direcciones IP, servidores, servicios o cuentas que permiten al adversario operar la intrusión.	Dominios de Comando y Control, IP externas, servidor de phishing, infraestructura de red usada para recibir conexiones desde los hosts infectados.
Víctima	Persona, equipo, sistema, cuenta, red u organización afectada por la actividad del adversario. Puede haber víctima primaria y víctimas posteriores.	Administrador que recibe el phishing, equipo inicialmente infectado y segunda víctima atacada mediante pivoting desde el host comprometido.

Tabla 1: Elementos principales del Modelo Diamante.

4. Parte 02. Análisis de evento con el modelo diamante

4.1. Escenario base

Una organización detecta comportamiento anómalo en un equipo. El análisis revela lo siguiente:

1. La víctima detecta malware.
2. El malware contiene dominios de Comando y Control, también conocidos como C2.
3. Los dominios resuelven a direcciones IP externas.
4. Los registros muestran múltiples hosts conectándose a esas IP.
5. La información WHOIS/IP revela un posible origen del atacante.

4.2. Descomposición del incidente en eventos

Para evitar una interpretación superficial, el incidente se divide en eventos. Cada evento se describe mediante metacaracterísticas: marca de tiempo, fase, resultado, dirección, metodología y recursos.

4.2.1. Evento 1. Detección de malware en equipo víctima

Metacaracterística	Descripción del evento
Marca de tiempo	T1 - Primer momento en que el equipo de seguridad identifica comportamiento anómalo en el host.
Fase	Instalación / Persistencia inicial observada.
Resultado	Se confirma la presencia de malware en el equipo víctima, lo que indica compromiso del endpoint.
Dirección	Desde el adversario hacia la víctima; en la observación defensiva, desde el host comprometido hacia el monitoreo interno.
Metodología	Análisis de alertas, revisión de endpoint, inspección de procesos, archivos sospechosos o indicadores generados por EDR/antivirus.
Recursos	Equipo víctima, agente de seguridad, hash del archivo, proceso malicioso, bitácoras del sistema.

Interpretación diamante: la víctima directa es el host infectado; la capacidad es el malware; la infraestructura aún no se confirma por completo, pero comienza a inferirse por la necesidad del malware de comunicarse con recursos externos; el adversario todavía no está atribuido nominalmente.

4.2.2. Evento 2. Identificación de dominios C2 dentro del malware

Metacaracterística	Descripción del evento
Marca de tiempo	T2 - Posterior a la extracción o revisión del malware detectado.
Fase	Comando y Control.
Resultado	Se identifican dominios usados por el malware para comunicarse con infraestructura externa controlada por el adversario.
Dirección	Malware en host víctima hacia dominios C2 externos.
Metodología	Análisis estático y dinámico del malware; búsqueda de cadenas, dominios incrustados, consultas DNS y patrones de comunicación.
Recursos	Muestra de malware, dominios C2, sandbox, herramientas de análisis, registros DNS.

Interpretación diamante: la capacidad se vuelve más clara, porque el malware no solo existe, sino que tiene funcionalidad de comunicación externa. La infraestructura queda representada por los dominios C2.

4.2.3. Evento 3. Resolución de dominios C2 a direcciones IP externas

Metacaracterística	Descripción del evento
Marca de tiempo	T3 - Durante la investigación de infraestructura asociada al malware.
Fase	Comando y Control / Infraestructura.
Resultado	Los dominios maliciosos resuelven a IP externas, lo que permite mapear parte de la infraestructura usada por el adversario.
Dirección	Consulta desde la red víctima hacia DNS; resolución hacia IP externa controlada o usada por el atacante.
Metodología	Consulta DNS, enriquecimiento de indicadores, revisión de reputación, análisis de resolución histórica y correlación con tráfico de red.
Recursos	Dominios, direcciones IP externas, registros DNS, firewall, proxy, SIEM y fuentes OSINT.

Interpretación diamante: la infraestructura deja de ser abstracta y se vuelve accionable: dominios e IP externas pueden bloquearse, monitorearse y correlacionarse con otros eventos.

4.2.4. Evento 4. Múltiples hosts conectándose a las IP externas

Metacaracterística	Descripción del evento
Marca de tiempo	T4 - Al revisar logs de firewall, proxy, DNS o SIEM después de identificar los indicadores externos.
Fase	Comando y Control con posible propagación interna o movimiento lateral.
Resultado	Se detecta que el incidente no se limita a un solo equipo; varios hosts internos intentan comunicarse con la misma infraestructura externa.
Dirección	Desde múltiples hosts internos hacia IP externas asociadas a C2.
Metodología	Correlación de eventos en SIEM, búsqueda de indicadores de compromiso en toda la red y análisis de conexiones salientes.
Recursos	Logs de red, direcciones IP internas, IP externas C2, firewall, proxy, DNS, SIEM.

Interpretación diamante: el análisis cambia de un compromiso aislado a una posible campaña dentro de la red. La víctima deja de ser solo un host y pasa a incluir varios equipos internos conectados a la misma infraestructura adversaria.

4.2.5. Evento 5. WHOIS/IP revela posible origen del atacante

Metacaracterística	Descripción del evento
Marca de tiempo	T5 - Durante el enriquecimiento de indicadores externos.
Fase	Análisis de infraestructura / atribución técnica preliminar.
Resultado	Se obtiene información que sugiere un posible origen o proveedor de infraestructura relacionado con el atacante; no constituye atribución definitiva.
Dirección	Desde el analista hacia fuentes de inteligencia externas; relación de infraestructura externa hacia posible adversario.
Metodología	Consulta WHOIS, revisión ASN, geolocalización aproximada, reputación de IP, historial de dominios y correlación con campañas conocidas.
Recursos	Datos WHOIS, ASN, registros históricos, inteligencia de amenazas, reputación de IP y dominios.

Interpretación diamante: este evento fortalece el análisis de infraestructura y puede apoyar una hipótesis de adversario, pero debe tratarse con cautela porque la infraestructura

puede estar comprometida, alquilada o deliberadamente usada como falsa bandera.

5. Identificación de elementos en el escenario

5.1. ¿Quién es el adversario en este escenario?

El adversario es el actor que opera la campaña de intrusión y controla o utiliza la infraestructura de Comando y Control. No es correcto afirmar un nombre específico con la información disponible; lo técnicamente sólido es describirlo como un **actor externo o grupo organizado** que despliega malware, administra dominios C2 y posiblemente busca mantener presencia dentro de la red. La información WHOIS/IP permite formular una hipótesis de origen, pero no basta para una atribución concluyente.

5.2. ¿Cuál es la capacidad utilizada?

La capacidad principal es el **malware con comunicación C2**. También forman parte de la capacidad el phishing dirigido, la ejecución del payload, los mecanismos de persistencia, la comunicación hacia dominios externos, el uso de infraestructura para control remoto y, en el escenario APT, el uso del host comprometido como proxy para atacar a una segunda víctima.

5.3. ¿Qué tipo de infraestructura se emplea?

Se emplea infraestructura externa compuesta por dominios C2, direcciones IP externas, posibles servidores de comando, servicios DNS y recursos asociados al envío de phishing. Además, cuando el host comprometido se usa como proxy, ese equipo pasa a formar parte de la infraestructura operacional del adversario, porque facilita el pivote hacia otra víctima.

5.4. ¿Quién es la víctima primaria?

La víctima primaria es el **equipo inicialmente comprometido**, asociado al usuario o administrador que recibió el phishing y ejecutó el malware. En un plano más amplio, la organización también es víctima, pero para el análisis diamante conviene separar la víctima inicial del resto de activos afectados.

5.5. ¿Existe evidencia de movimiento lateral?

Sí existe evidencia razonable de posible movimiento lateral o propagación interna, porque los logs muestran múltiples hosts conectándose a las mismas IP externas. Además, el escenario APT indica que el host comprometido se usa como proxy para atacar una segunda víctima. Esto representa una relación de *pivoting*: el adversario aprovecha el primer compromiso para ampliar su alcance dentro o hacia otro objetivo.

6. Parte 03. Relación con la Cyber Kill Chain

La *Cyber Kill Chain* permite ordenar los eventos de una intrusión en fases. La clasificación siguiente relaciona los eventos del escenario con la fase más representativa de la cadena.

Evento	Fase Kill Chain	Justificación
Detección de malware	Instalación / Persistencia	La detección confirma que el malware ya está presente en el equipo, por lo que el atacante superó fases previas y consiguió instalar o ejecutar capacidad maliciosa.
Envío de phishing	Entrega	El phishing es el medio usado para entregar el vector inicial al usuario objetivo, normalmente mediante correo, enlace o archivo malicioso.
Conexión a C2	Comando y Control	El malware intenta comunicarse con dominios o IP externas para recibir instrucciones, reportar estado o mantener control remoto.
Ejecución del malware	Explotación / Instalación	La ejecución activa la capacidad maliciosa en el host; dependiendo del caso, puede representar explotación inicial o instalación del payload.
Múltiples hosts conectándose a IP externas	Acciones sobre objetivos / Movimiento lateral posterior	El patrón sugiere que el adversario amplió su actividad a varios equipos o utilizó la misma infraestructura para controlar más de un host.

Tabla 2: Relación de eventos del escenario con fases de la Cyber Kill Chain.

Análisis: el incidente no debe verse como una alerta única de malware. La secuencia muestra una progresión: entrega del phishing, ejecución del malware, establecimiento de C2, expan-

sión a múltiples hosts y enriquecimiento de infraestructura. Esa progresión permite priorizar contención, erradicación y búsqueda de indicadores en toda la red.

7. Parte 04. Hilos de actividad

7.1. Escenario tipo APT

Con base en el escenario APT propuesto, la actividad se organiza así:

- Phishing dirigido a administrador.
- Ejecución de malware.
- Conexión a C2.
- Uso del host comprometido como proxy.
- Ataque a segunda víctima.

7.2. Diagrama de hilos de actividad

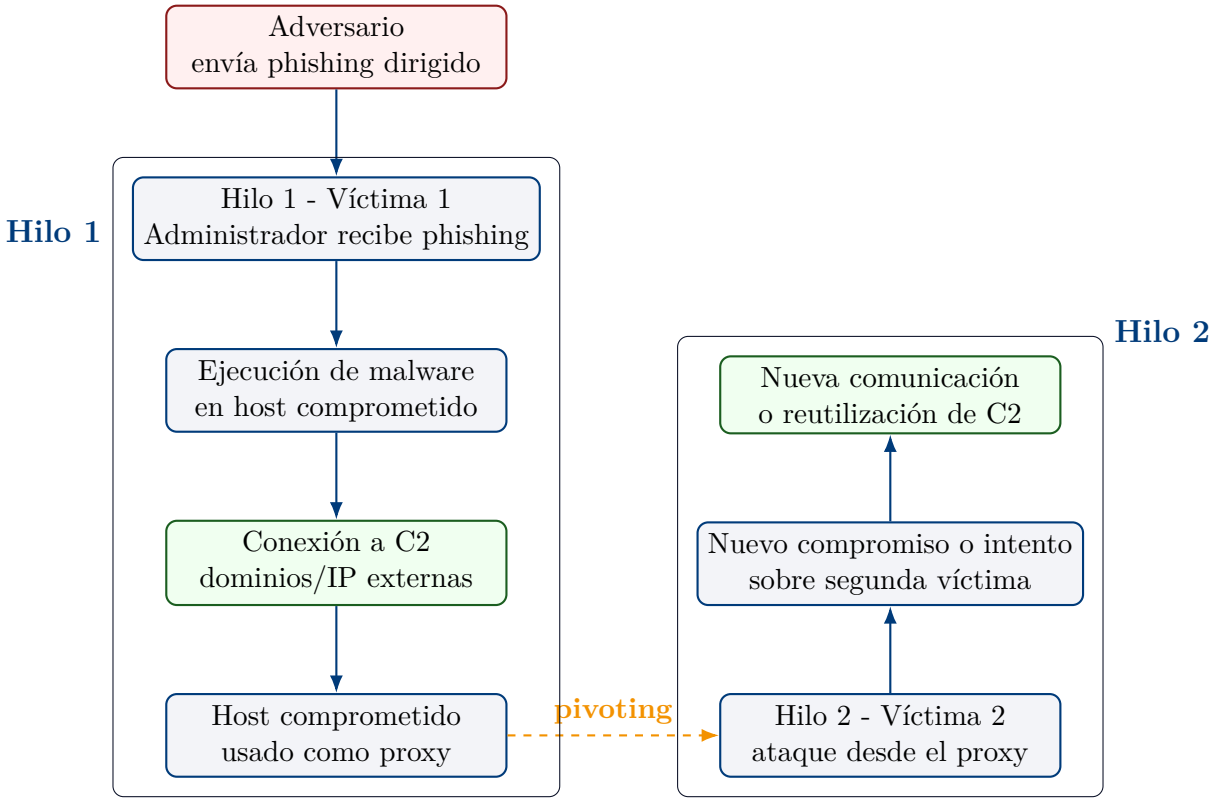

Figura 2: Hilos de actividad y relación de pivoting entre Víctima 1 y Víctima 2.

7.3. Descripción de los hilos

Hilo 1 - Víctima 1. El primer hilo inicia con un phishing dirigido a un administrador. El usuario recibe el mensaje, el malware se ejecuta en su equipo y el host establece comunicación con dominios/IP de Comando y Control. A partir de ese punto, el adversario obtiene una posición operacional dentro del entorno de la víctima. En el modelo diamante, la víctima es el administrador o su host, la capacidad es el malware, la infraestructura son los dominios/IP C2 y el adversario es el operador de la campaña.

Hilo 2 - Víctima 2. El segundo hilo inicia cuando el host de la primera víctima se usa como proxy o punto de pivote. Esto permite al adversario atacar a otra víctima aparentando que la actividad proviene de un sistema ya ubicado dentro del entorno comprometido. El uso del primer host como infraestructura es crítico: la víctima 1 deja de ser solo afectada y pasa a convertirse también en recurso operativo del atacante.

Relación entre ambos hilos. La relación principal es el **pivoting**. El adversario compro-

mete primero un equipo con mayor probabilidad de acceso, como el de un administrador, y luego aprovecha esa posición para alcanzar una segunda víctima. Esta relación muestra por qué es insuficiente limpiar solo el equipo donde se detectó el malware; también se deben revisar conexiones internas, autenticaciones recientes, tráfico hacia C2, reglas de firewall, movimientos de credenciales y otros hosts con los mismos indicadores.

8. Síntesis del análisis diamante

Elemento	Aplicación al escenario
Adversario	Actor externo o grupo organizado que opera la campaña, controla infraestructura C2 y usa phishing/malware para comprometer hosts.
Capacidad	Malware, phishing dirigido, comunicación C2, posible persistencia y uso de host comprometido como proxy.
Infraestructura	Dominios C2, IP externas, registros DNS, servidores asociados, recursos de envío de phishing y host comprometido usado como infraestructura intermedia.
Víctima	Administrador y host inicialmente comprometido; posteriormente, segunda víctima atacada mediante pivoting.
Relación crítica	El host de la primera víctima se transforma en punto de apoyo para ampliar la intrusión, lo que evidencia continuidad operacional del adversario.

Tabla 3: Síntesis de los elementos del Modelo Diamante aplicados al escenario.

9. Recomendaciones de respuesta y contención

Aunque la actividad se centra en el análisis, una interpretación completa debe proponer acciones de respuesta. Para este escenario, se recomiendan las siguientes medidas:

1. Aislar el host comprometido para evitar nuevas comunicaciones con C2.
2. Bloquear dominios e IP externas identificadas en firewall, proxy y DNS.
3. Buscar los mismos indicadores de compromiso en todos los hosts de la organización.
4. Revisar autenticaciones recientes del administrador afectado y forzar rotación de credenciales.

5. Analizar si el host comprometido realizó conexiones internas anómalas hacia otros equipos.
6. Confirmar si existe movimiento lateral o uso del equipo como proxy.
7. Recolectar evidencia forense antes de eliminar archivos, procesos o artefactos relevantes.
8. Fortalecer controles contra phishing dirigido mediante MFA, capacitación y protección de correo.

10. Conclusión

El Modelo Diamante permitió estructurar el incidente de forma más precisa que una simple lista de alertas. La detección de malware, la presencia de dominios C2, la resolución hacia IP externas y la conexión de múltiples hosts forman una secuencia coherente de intrusión. El análisis muestra que el adversario utilizó capacidades técnicas como phishing, malware y comunicación C2, apoyándose en infraestructura externa y, posteriormente, en un host comprometido como recurso de pivote.

La relación con la *Cyber Kill Chain* confirma una progresión desde la entrega inicial del ataque hasta el establecimiento de comando y control y la posible expansión hacia una segunda víctima. Por ello, la respuesta no debe limitarse a eliminar el malware del primer equipo. Es necesario investigar la infraestructura, buscar indicadores en toda la red, revisar cuentas privilegiadas y comprobar si existió movimiento lateral.

En conclusión, el escenario corresponde a una intrusión con comportamiento compatible con una campaña dirigida o APT básica, donde la correcta correlación de eventos permite comprender el comportamiento del adversario y priorizar acciones de contención, erradicación y monitoreo.

Referencias

Caltagirone, S., Pendergast, A., & Betz, C. (2013). *The Diamond Model of Intrusion Analysis*. Center for Cyber Intelligence Analysis and Threat Research.

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.

MITRE. (s. f.). *ATT&CK: Enterprise Matrix*. MITRE Corporation.