

El modelo Diamond de Análisis de intrusiones

Sergio Caltagirone

sergio.caltagirone@cciatr.org

Andrew Pendergast

andrew.pendergast@cciatr.org

Christopher Betz

christopher.betz@cciatr.org

" Los analistas de inteligencia debe ser consciente de su proceso de razonamiento. Ellos deben pensar en cómo hacen juicios y llegar a conclusiones, no sólo sobre los juicios y conclusiones mismos ".

Richards J. Heuer Jr. [1]

" Análisis de intrusiones se trata tanto de tcpdump como la astronomía con los telescopios"

Chris Sanders [2]

Resumen

En este trabajo se presenta un novedoso modelo de análisis de intrusiones integrado por los analistas, derivado de años de experiencia, pidiendo a la simple pregunta, "¿Cuál es el método subyacente a nuestro trabajo?" El modelo establece el elemento atómico básico de cualquier actividad de intrusión, el evento, compuesto por cuatro características principales: adversario, la infraestructura, la capacidad, y la víctima. Estas características son de borde conectado representación de sus relaciones subyacentes y dispuestos en la forma de un diamante, dando el modelo de su nombre: el modelo Diamond. Es más de fi ne adicionales meta-características para apoyar construcciones más alto nivel, tales como la vinculación eventos juntos en hilos de actividad y además de coalescencia eventos y los hilos en grupos de actividad. Estos elementos, el evento, hilo, y el grupo, todo ello contribuye a un modelo fundamental e integral de la actividad de intrusos en torno a los procesos analíticos. Captura los conceptos esenciales del análisis de intrusiones y operaciones adversario al tiempo que permite la flexibilidad modelo fl expandirse y abarcar nuevas ideas y conceptos. El modelo establece, por primera vez, un método formal la aplicación de principios científicas a análisis de intrusión - en particular los de la medición, la capacidad de prueba, y la repetibilidad

- proporcionando un método integral de documentación de la actividad, síntesis, y la correlación. Este enfoque fi científica y simplicidad produce mejoras en cacia analítica e ff, ciencia e FFI, y la precisión. En última instancia, el modelo proporciona oportunidades para integrar inteligencia en tiempo real para la defensa de la red, la automatización de la correlación entre los eventos, la clasificación de eventos con la confianza en las campañas adversario, y las operaciones de pronóstico adversario mientras que la planificación y mitigación de juego estrategias.

Contenido

1. Introducción	5
2. Trabajo relacionado	6
3 Introducción al modelo de diamante	7
4 Diamond Evento	8
4.1 adversario.	11
4.2 Capacidad.	12
4.2.1 comando y control (C2).	13
4.3 Infraestructura.	13
4.4 La víctima.	14
4.4.1 Vulnerabilidades y Exposiciones.	14
4.5 de eventos Meta-Funciones.	15
4.5.1 Marca de tiempo.	15
4.5.2 Fase.	15
4.5.3 Resultado.	dieciséis
4.5.4 Dirección.	17
4.5.5 Metodología.	17
4.5.6 Recursos.	17
4.5.7 Ampliaciones Meta-Feature.	18
5 Modelo Diamante Extended	19
5,1 político-social.	20
5.1.1 Relaciones Adversario persistente.	20
5.1.2 Cyber-Victimología.	23
5.1.3 Espacio compartido amenaza.	24
5.2 Tecnología.	24
6 Indicadores contextuales	25
7 Analytic pivotante	26
7.1 Enfoques 'Centrado'.	26
7.1.1 Enfoque centrado en las víctimas.	26
7.1.2 Enfoque de Capacidades centrada.	28
7.1.3 Enfoque Centrado en Infraestructura.	29
7.1.4 Enfoque Centrado adversario.	29
Enfoque 7.1.5 político-social centrada.	29
7.1.6 Enfoque centrado en la tecnología.	30
Tema 8 Actividad	30
8.1 Proceso adversario.	36
8.2 Soporte analítico Hipótesis.	36
8.3 Actividad Ataque-Graph.	39
9 grupos de actividades	40

9.1 Paso 1: Problema Analytic.	42
9.2 Paso 2: Selección de características.	43
9.3 Paso 3: Creación.	45
9.3.1 Actividad de grupo Ejemplo Creación.	46
9.4 Paso 4: Crecimiento.	46
9.5 Paso 5: Análisis.	49
9.6 Paso 6: Rede definición.	49
9.7 Grupo Actividad familias.	49
10 Planificación y Gaming	51
11 Trabajo Futuro	54
12 Conclusión	55

Lista de Figuras

1 Un evento de diamante.	9
2 Un diamante Extended Evento.	19
3 Relaciones adversario-víctima.	21
4 grado de persistencia Spectrum.	22
5 Analytic Ejemplo pivotante Uso del diamante.	27
6 Diamante actividad de los hilos Ejemplo.	31
7 Proceso Diamond adversario Ejemplo.	37
8 Actividad-Attack Graph Ejemplo.	39
9 Actividad Grupo Creación.	47
10 Actividad Crecimiento Grupo.	48
11 Diamond Modelo / Kill Curso Cadena de Acción Matriz Ejemplo.	53

1. Introducción

La disciplina de análisis de intrusión ha existido desde el descubrimiento de la primera intrusión.¹

piratas informáticos externos y expertos de la maliciosos, en su mayoría con astucia, infiltrado y el ataque de intrusos mientras que los analistas y administradores de sistemas trabajan para descubrir, entender y frustrar sus acciones oper-. Las preguntas quedan pocos cambios, desde la época de la disciplina: el quién, qué, cuándo, dónde, por qué y cómo. Históricamente, estas preguntas informadas de respuesta a incidentes para hacer frente a la actividad a mano, pero carecían de los defensores de los modelos y marcos para la documentación de la actividad, síntesis, y la correlación necesaria para responder a una pregunta de la creciente importancia: lo hará el retorno adversario como parte de una campaña coordinada? Sin embargo, la cuestión en última instancia conduce organizaciones fuera de la mitigación táctica (la lucha contra la actividad) y hacia la mitigación estratégica (lucha contra el adversario) lo que aumenta el costo de la mitigación y el costo del adversario para llevar a cabo las operaciones.

En este trabajo se presenta un novedoso modelo de análisis de intrusiones integrado por los analistas, derivado de años de experiencia, pidiendo a la simple pregunta, "¿Cuál es el método subyacente de nuestro trabajo?" Llega a su nombre, el modelo del diamante, por su sencilla organización de los aspectos más fundamentales de la actividad maliciosa en la forma de un diamante. Nuestro modelo establece, por primera vez, un método formal de aplicar principios científicos a la intrusión de análisis: los de la medición, la capacidad de prueba, y la repetibilidad - proporcionar un método simple, formal y completa de documentación de la actividad, síntesis, y la correlación. Este enfoque científico y simplicidad produce mejoras en cacia analítica e ff, ciencia e FFI, y la precisión.

Nuestro modelo es a la vez simple y complejo, tanto formal como informal, útil para el análisis tanto de información privilegiada y las amenazas externas. De manera informal, los analistas comprender fácilmente el modelo de lo que es útil en el calor de la búsqueda en una base diaria. El modelo es la base de una ontología²

y presenta un marco sobre el cual para descubrir nueva actividad, maximizar las oportunidades de pivote analíticas, se correlacionan y sintetizar nueva información, y perseguir al adversario con el tiempo, a la vez que mejorar la comunicación y documentación.

Formalmente, el modelo es un marco matemático que permite la aplicación de juego, gráfico, y la teoría de cationes / agrupación fi cación para mejorar el análisis y toma de decisiones. La formalidad ofrece varios beneficios: hipótesis analíticas comprobables que garantizan la repetibilidad y precisión de los resultados analíticos, la generación de hipótesis más fácil, la correlación automatizada a través de eventos, para clasificar rápidamente los eventos con confianza en las campañas adversario, y adversario de predicción operaciones mientras que la planificación y mitigación de juego estrategias. En última instancia, este formalismo conduce a la capacidad del modelo para integrar la inteligencia correlacionada de las capacidades de defensa de la red, de fácil evolución a adoptar nuevas infraestructuras adversario, capacidades y procesos.

Lo más importante, el modelo es a propósito genérico y por lo tanto ampliable y flexible. Captura con precisión los conceptos esenciales del análisis de intrusión y operaciones adversario.

¹ En este documento el término "intrusión" se utiliza para denotar toda la actividad malicioso y nefasto atacan a los sistemas y redes de ordenadores.

² El modelo no presenta una nueva ontología, taxonomía, formato de intercambio, o protocolo, sino por su naturaleza fundamental debe ser la base de estos. Este punto de vista es apoyado por otros en [3].

Estos atributos mejoran la utilidad del modelo, lo que le permite crecer y abarcar nuevas ideas y conceptos.

2. Trabajo relacionado

En el análisis de intrusiones, nos encontramos con analistas y expertos como Stoll [4], Bellovin [5], y Cheswick [6] que han sido descubrir y documentar los eventos maliciosos con poca o ninguna formación y herramientas formales. A menudo han confiado en resmas de datos impresos para analizar la actividad y armado sólo con la intuición y la capacidad técnica suprema. Tradecraft su documentación inicial y la narración oral llevaron a muchos analistas por el camino de adversarios de caza. analistas de intrusión modernos siguen esta tradición con destacadas e innovadoras e ff Orts como el Proyecto Honeynet [7].

Northcutt en [8] y otros han fortalecido la formación analítica que muestra ejemplos de actividades de amenazas especi fi cas y proporcionar a los estudiantes la oportunidad de entender las herramientas adversario y Tradecraft. Formación práctica analítica de organizaciones tales como SANS [9] que ahora es una fuente significativa de difusión Tradecraft analítica.

Si bien estas historias, documentos, libros y cursos proporcionan casos sólidos para la enseñanza de los ics meca- de análisis de intrusiones, no lo hacen o ff er el enfoque c científica necesaria para apuntalar el proceso. Sin el modelo subyacente (ya sea formal o informal) para explicar cómo evalúan ana- lysts y entender la actividad maliciosa, e ff Orts evolucionando Tradecraft son di fi culto a imposible.

tangencialmente trabajo adicional se refiere a análisis de intrusiones y el uso de defensa de la red de inteligencia impulsada. Amann, et al., En [10] señala con precisión, "cada vez es más difícil para informar de manera fiable ataques complejos de hoy sin tener contexto externo a la mano. Por desgracia, sin embargo IDS de hoy [sistemas de detección de intrusos] no se pueden integrar fácilmente la inteligencia ..."Su trabajo avanza de manera significativa la capacidad de un IDS para integrar contexto externo e inteligencia de amenazas en tiempo real para aumentar el éxito de detección. Esta es una capacidad crítica para la mitigación del futuro, que complementa el modelo Diamond mediante la identificación de cómo los analistas e ff caz, e fi ciente, y se desarrollan con precisión ese contexto externo e inteligencia para enriquecer la detección.

La 'cadena de muertes' ofrece un modelo altamente reflexiva e ff e influyente de las operaciones adversario que informa directamente las decisiones de mitigación [11]. Nuestro modelo integra su enfoque por fases y complementa análisis de la cadena de muertes por la ampliación de la perspectiva que proporciona granularidad necesaria y la expresión de las complejas relaciones entre la actividad de intrusión. Esto permite que el alcance completo de conocimiento para ser representada en contraposición a solo los indicadores observables de la actividad. Además, nuestro modelo proporciona un método matemático formal para los e ff análisis gráfico reflexivo y agrupación (por ejemplo, la agrupación / clasi fi cación) para resolver muchas clases de problemas analíticos. Esta característica permite que el modelo para apoyar numerosos marcos estrategia complementaria de planificación como el de Inteligencia preparación conjunta del ambiente operacional (JIOPE) [12].

y Model (ADAM) [13], y el desarrollo potencialmente más estrategia “de punta” usando técnicas de computación evolutivas tales como [14].

gráficos de ataque tradicionales intentan generar todas las posibles trayectorias de ataque y las vulnerabilidades para un conjunto dado de recursos protegidos para determinar la mejor relación costo e defensa y ss caz y el mayor grado de protección. gráficos de ataque se originó con “árboles de ataque” de Schneier y se convirtieron en una herramienta de análisis de vulnerabilidad valiosa para desarrollar e caz y siguientes estrategias de defensa en profundidad [15]. Hasta 2005, los gráficos de ataque enfrentaron cultades fi cativos signi di fi cientes en la escalabilidad, surement medi-, y la facilidad de uso [16]. Sin embargo, se han hecho progresos mejorar la escalabilidad para redes de tamaño reales [17, 18], la medición [19], y la facilidad de uso [20]. Nuestro modelo define un nuevo gráfico ataque inteligencia centradas, llamado hilos de actividad, y combina la inteligencia y gráficos tradicionales de ataque en un gráfico de actividad para este partido. gráficos de la actividad de ataque se fusionan análisis de vulnerabilidad dicional tra- con el conocimiento de la actividad adversario. Se integran lo que ha ocurrido con los vectores potenciales y preferidas de ataque que permite más e caz y siguientes análi- sis y la mitigación del desarrollo de la estrategia. En última instancia, permite una mayor e fi ciente de asignación de recursos de defensa. Además, el trabajo previo en [21] ya ha demostrado la aplicabilidad de ataque representa gráficamente directamente en los sistemas de detección de intrusos. Esto permite que los hilos de actividad y procesos adversario desarrolladas en nuestro modelo a ser implementadas directamente en los sistemas de detección de intrusos. de trabajo previa en [21] ya ha demostrado la aplicabilidad de ataque representa gráficamente directamente en los sistemas de detección de intrusos. Esto permite que los hilos de actividad y procesos adversario desarrolladas en nuestro modelo a ser implementadas directamente en los sistemas de detección de intrusos. de trabajo previa en [21] ya ha demostrado la aplicabilidad de ataque representa gráficamente directamente en los sistemas de detección de intrusos. Esto permite que los hilos de actividad y procesos adversario desarrolladas en nuestro modelo a ser implementadas directamente en los sistemas de detección de intrusos.

Muchos sistemas, lenguajes y taxonomías se han desarrollado, que permiten a los analistas para documentar actividades maliciosas e intercambiar indicadores [22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32]. Nuestro modelo no propone una ontología, taxonomía, o protocolo de uso compartido. Sin embargo, en una reciente encuesta de ontologías de seguridad cibernética nuestro modelo es citado como fundamental y sugiere que debería servir como una base sobre la cual a unirse ontologías existentes y construir ontologías futuras [3]. Por otra parte, nuestro modelo es compatible con el argumento de que la integración de la inteligencia verdadera amenaza cibernética debemos escapar de lo que representa una actividad complicada y profundamente relacional como una super fi y simple lista de indicadores técnicos. Se argumenta que para lograr la mitigación estratégica,

3 Introducción al modelo de diamante

En su forma más simple (Figura 1), el modelo describe que una *adversario* despliega una *capacidad* sobre algunas *infraestructura* contra una *víctima*. Estas actividades se denominan *eventos* y son las *características atómicas*. Los analistas o máquinas pueblan los vértices del modelo como los acontecimientos se presen- ten y detectados. Los vértices están vinculadas con los bordes destacando la relación natural entre las características. Pivotando sobre bordes y dentro de los vértices, los analistas exponen más información acerca de las operaciones del adversario y descubre nuevas capacidades, infraestructura y víctimas.

Un evento de fi ne un solo paso en una serie que el adversario debe ejecutar para lograr su objetivo. Como tal, los eventos son de fase ordenada por par adversario-víctima en *hilos de actividad* que representa el flujo de operaciones de un adversario. Ambos *eventos* Y *hilos de actividad* son

elementos necesarios para una comprensión completa de las actividades maliciosas como más reflexiva e ff y mitigación estratégica "requiere una nueva comprensión de las intrusiones a sí mismos, no como eventos singulares, sino más bien como progresiones graduales." [11]

Una vez *hilos de actividad* se establecen, los eventos pueden ser correlacionados a través de las discusiones para identificar las campañas adversario, y se fundieron en *grupos de actividad* para identificar los eventos y las amenazas que comparten características comunes similares. Estas *grupos de actividad* puede ser utilizado para la correlación automática de eventos, así como para los juegos y la planificación de las opciones de mitigación y escenarios que establecen los planes de mitigación estratégicos en la lucha contra el adversario.

Los términos y conceptos antes mencionados se describen con más detalle y se discuten en las secciones siguientes, comenzando con elemento atómico del modelo - el Evento diamante.

4 Diamond Evento

axioma 1 *Por cada evento de intrusión existe un adversario dando un paso hacia una meta deseada mediante el uso de una capacidad sobre la infraestructura contra una víctima para producir un resultado.*

Un evento actividad de tiempo límite discreto de fines restringido a una específica *fase* donde un *sario adver-*, requiriendo externa *recursos*, utiliza una *capacidad* y *metodología* sobre algunas *infraestructura* contra una *víctima* con un dado *resultado*. Por supuesto, no todas las características deben ser conocidas por crear un evento. En casi todos los casos, se espera que la mayoría de las características para ser desconocida y completó sólo después del descubrimiento inicial se obtenga nueva información se revela y se reunió más datos.

Características básicas las características básicas de un evento son: *adversario*, *la capacidad*, *la infraestructura*, y *víctima*.

Meta-**Características** los meta-funciones son: *marca de tiempo* (tanto principio y fin), *fase*, *resultado*, *dirección*, *metodología*, y *recursos*. Los meta-características se utilizan para ordenar los eventos dentro de una *hilo actividad* (§ 8), grupo como eventos de diversas maneras, y el conocimiento de captura crítico siempre que sea posible.

La confianza Valor Cada característica evento, ya sea un núcleo o meta-función, tiene un valor de confianza con asociado. Este valor se deja fin como propósito unde cada implementación modelo puede comprender confianza diferentemente. Además, la confianza es probablemente una función de los valores múltiples, tales como la confianza de una conclusión analítica y / o la exactitud de una fuente de datos. Según sea necesario, el valor de confianza con fin también puede ser detallada como un sub-tupla para capturar mejor los elementos individuales de confianza.

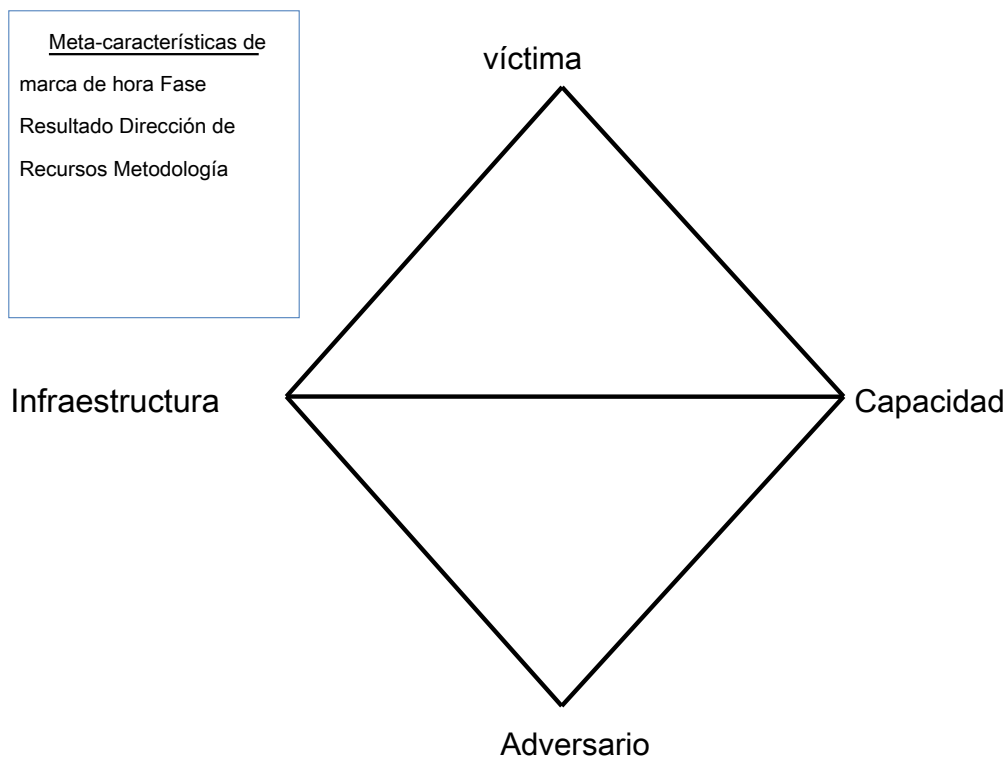


Figura 1: El modelo Diamond de análisis de intrusión, que comprende las características principales de un evento de intrusión: adversario, de capacidad, de infraestructura, y la víctima. Las características fundamentales están vinculados a través de los bordes para representar las relaciones fundamentales entre las características que pueden ser explotadas analíticamente para descubrir y desarrollar el conocimiento de la actividad maliciosa más. Los meta-características se enumeran también, y mientras que las funciones no básicas, destaca su importancia en las funciones de análisis, agrupamiento y de planificación de orden superior.

Un beneficio de este modelo es que proporciona una reflexiva e ff (pero no necesariamente exhaustiva) lista de características que *debería* estar presente en cada evento. Por lo tanto, después de documentar un evento con toda la información disponible cualquier característica vacías son las lagunas de conocimiento fi cados ahora identificaciones que deben fomentar pivotante adicional para cerrar esas brechas.

Un evento, *M*, está formalmente definido como una etiqueta *norte*-tupla donde cada elemento de la tupla es el conocimiento de una característica combinada con un valor de confianza con fi independiente.³

$$E = \langle \langle \text{Adversario}, \text{Confianza}_{\text{adversario}} \rangle, \langle \text{Capacidad}, \text{confianza}_{\text{capacidad}} \rangle, \langle \text{Infraestructura}, \text{Confianza}_{\text{infraestructura}} \rangle, \langle \text{Victim}, \text{Confianza}_{\text{victima}} \rangle, \langle \text{Marca de tiempo}_{\text{comienzo}}, \text{Confianza}_{\text{fecha y hora}_{\text{comienzo}}} \rangle, \langle \text{Marca de tiempo}_{\text{fin}}, \text{Confianza}_{\text{fecha y hora}_{\text{fin}}} \rangle, \langle \text{Fase}, \text{Confianza}_{\text{fase}} \rangle, \langle \text{En consecuencia}, \text{la confianza}_{\text{resultado}} \rangle, \langle \text{Dirección}, \text{Confianza}_{\text{dirección}} \rangle, \langle \text{Metodología}, \text{Confianza}_{\text{metodología}} \rangle, \langle \text{Recursos}, \text{Confianza}_{\text{recursos}} \rangle \rangle$$

Para flexibilidad añadida, la tupla básico se puede ampliar en una jerarquía de anidada pares ordenados (referido como sub-tuplas en el presente documento por simplicidad) para promover de fi ne un conocimiento de características y de captura particular, para la correlación futuro.

Un ejemplo ilustrativo de expansión de la característica víctima para proporcionar una mayor definición de información tal como: la organización que está siendo víctima, la dirección de IP del anfitrión, el nombre del anfitrión (es decir, nombre de host), la aplicación que fue explotada, y el puerto TCP que se utilizó para explotar la aplicación:⁴

³ El evento es una variable de tamaño *norte*-tupla, en lugar de un tamaño fijo, debido a que el modelo no se limita a las características de fi ne aquí y se puede ampliar para incluir otros elementos de interés, como los del diamante extendido §5. Una vez que una organización de fi ne todo su conjunto de características del tamaño tupla será formalmente definida para ese caso particular.

⁴ Tenga en cuenta que en el ejemplo de cada sub-característica de *Victima* tiene un valor de con fi anza independiente, pero también se podría aplicar el modelo en el que uno con valor de confianza es simplemente aplicar a todas las sub-funciones.

$\langle V_{ictim}, Confianza_{victima} \rangle = \langle \langle Organización, Confianza_{organización} \rangle,$

$\langle HostIPAddress, Confianza_{IP} \rangle, \langle Nombre de host,$
 $Confianza_{nombre de host} \rangle, \langle Aplicación, Confianza_{Solicitud}$
 $\rangle, \langle TCPPort, Confianza_{TCPPort} \rangle \rangle$

Para fines analíticos, el evento también puede ser entendido y representado como un gráfico, como se ilustra en la Figura 1. En esta forma los bordes representan las relaciones naturales entre las características de un evento y identificar lo que es normalmente visible / detectable desde la perspectiva de que la función a través de pivotamiento (descrito adicionalmente en § 7). Las características fundamentales (adversario, la capacidad, la infraestructura, y la víctima) conforman una, grafo no dirigido, simple vértice marcado. Un evento organizado gráfico-, *MI*, Es así definido:

$mi_{vértices} = \{ Adversario,$
 $Infraestructura,$
 $Capability, V_{ictim}\}$

$mi_{bordes} = \{\{ Adversario, Capacidad\},$
 $\{ Adversario, Infraestructura\},$
 $\{ Infraestructura, Capacidad\},$
 $\{ Infraestructura, V_{ictim}\},$
 $\{ Capability, ictim V\}\}$

4.1 Adversario

axioma 2 Existe un conjunto de adversarios (insiders, los extranjeros, los individuos, grupos y organizaciones) que tratan de comprometer los sistemas informáticos o redes para fomentar su intención y satisfacer sus necesidades.

Un *adversario* es el actor / organización responsable de la utilización de una capacidad contra la víctima para lograr su propósito. conocimiento adversario es generalmente difícil de alcanzar y esta característica es probable que estar vacío para la mayoría de eventos - al menos en el momento del descubrimiento.

La mayoría de las veces cuando se analizan los aspectos técnicos de un evento, que se refiere simplemente al operador adversario como el adversario. Sin embargo, la distinción entre el operador y el adversario cliente es importante para entender la intención, la atribución, la adaptabilidad y la persistencia al ayudar a enmarcar la relación entre un adversario y un par víctima. Por lo tanto, hemos encontrado estas distinciones importantes: ⁵

operador adversario Esta es la “hacker” real o persona (s) llevar a cabo la actividad de intrusión.

adversario al cliente Esta entidad se encuentra a beneficiarse de la actividad llevada a cabo en la intrusión. Puede ser el mismo que el *operador adversario*, o puede ser una persona o un grupo separado.

Por ejemplo, un cliente podría adversario con los recursos necesarios, a veces Erent di ff u operadores Erent di ff simultáneamente directos, cada uno con sus propias capacidades y la infraestructura, a una víctima frecuente la realización de objetivos comunes o separadas. ⁶ Para contrastar, un operador solitario adversario puede tener acceso a un menor número de capacidades y puntos de infraestructura para llevar a cabo sus actividades, mientras que también carece de la capacidad para eludir la mitigación sencilla.

Conocimiento de las motivaciones y los recursos de los que un operador adversario y su cliente, si es que existe como una entidad separada, ayudará a medir la verdadera amenaza y riesgo para la víctima que resulta en más e caz y siguientes de mitigación.

Informando a estas motivaciones son las necesidades socio-políticas que se explican más adelante en el Diamond Plus (con § 5).

4.2 Capacidad

los *capacidad* característica se describen las herramientas y / o técnicas del adversario se utiliza en el evento. La flexibilidad del modelo permite la capacidad de ser descrita en su fi cliente fidelidad. Nos proponemos para la capacidad de entenderse en sentido amplio y incluyen todos los medios a un ff ect a la víctima de los métodos más manuales “no sofisticados” (por ejemplo, adivinar la contraseña manual) a las técnicas automatizadas más sofisticados.

capacidad capacidad Todas las vulnerabilidades y exposiciones que pueden ser utilizados por la capacidad individual, independientemente de su víctima se consideran *capacidad*.

⁵ Si bien se sugieren algunas distinciones y categorías de características a lo largo de este trabajo tan útil para el análisis de todos los días, no pretende ser completa se hace o sugerencia de que estas distinciones forman una ontología o taxonomía, ni son éstos requeridos por el modelo.

⁶ Varias actividades orquestados por una autoridad superior pueden ser modelados y organizados dentro del modelo como grupo de actividad Familias (§ 9.7).

Arsenal adversario juego completo de un adversario de capacidades, y por lo tanto la capacidad combinada de sus capacidades individuales, es el *el arsenal de adversary*.

Si se conoce la capacidad de la capacidad que se debe documentar como una sub-tupla de la capacidad así como las rutas potenciales en un gráfico de actividad de ataque (§ 8.3). Esta documentación inicial de las capacidades de un adversary puede crecer con el tiempo con el análisis de la actividad de grupo (§ 9.5) que culmina en el conocimiento de su arsenal. Esta es información valiosa en las decisiones y la planificación que permite una para cursos adversario potencialmente pronóstico de acción y reacción de mitigación.

4.2.1 comando y control (C2)

De mando y control (C2) es el ejercicio de la autoridad y dirección sobre activos por un comandante [33]. En el análisis de intrusos, esto significa que los canales, estructuras de comunicación, señales, protocolos, y el contenido hacia o desde el adversario destinado a causar efecto (por ejemplo, obtener acceso, deliberadamente eliminar el acceso, exfiltrado de datos, enviar paquetes de ataque) progresando adversario hacia la consecución de su metas.

Mientras comando y control pueden adoptar muchas formas, se determina en última instancia por el capability en uso. En términos de pivotamiento analítica (§ 7), un analista pivotes más de C2 descubriendo la comunicación entre la infraestructura y las víctimas. Por lo tanto, para los fines de nuestro modelo, mando y control se entiende mejor como una sub-función de la capacidad.

4.3 Infraestructura

los *infraestructura característica* describe las estructuras físicas y / o lógicas de comunicación adversario usa para entregar una capacidad, mantener el control de las capacidades (por ejemplo, de mando y de control de / C2), y efecto resultados de la víctima (por ejemplo, exfiltrado datos). Al igual que con las otras características, la infraestructura puede ser tan específica o amplia como sea necesario. Los ejemplos incluyen: direcciones de Protocolo de Internet (IP), nombres de dominio, direcciones de correo electrónico, el código Morse fl cenizas de la luz de correo de voz de un teléfono visto desde el otro lado de una calle, los dispositivos USB que se encuentra en un estacionamiento y se inserta en una estación de trabajo, o la comprometedoras emanaciones de hardware (por ejemplo, Van Eck Phreaking [34]) se recogieron mediante un puesto de escucha cerca. Nos encontramos las siguientes distinciones función de infraestructura a ser razonable para la mayoría de los propósitos del análisis de intrusiones.

Tipo 1 Infraestructura Infraestructura que está totalmente controlado o propiedad de adversario o que pueden estar en la proximidad física.

Tipo 2 Infraestructura Infraestructura que está controlado por un (Witting o involuntario) intermediario. Por lo general, esta es la infraestructura que una víctima verá como el adversario. Sirve para ocultar el origen y la atribución de la actividad. Tipo 2 in- infraestructura

concluye anfitriones zombi, servidores de plataforma de malware, nombres de dominio maliciosos, los puntos de salto-a través de correo electrónico, cuentas comprometidas, etc.

Proveedores de servicio Las organizaciones que (consciente o inconscientemente) proporcionan servicios ical crit- disponibilidad del adversario Tipo 1 y Tipo 2 infraestructura (por ejemplo, proveedores de servicios Internet, registradores de dominios, proveedores de correo web).

4.4 Víctima

UNA víctima es el objetivo del adversario y contra quien vulnerabilidades y exposiciones son explotados y capacidades utiliza. Al igual que con otras características, una víctima puede describirse en cualquier forma necesaria y apropiada: organización, persona, dirección de correo electrónico de destino, dirección IP, dominio, etc. Sin embargo, es útil para definir la personalidad víctima y sus activos por separado, ya que servir di ff Erent funciones analíticas. personae víctima son útiles en el análisis no **técnica tales como Cyber-victimología (§ 5.1.2) y socio-políticos (enfoques centrados § 5.1) mientras que los activos de las** víctimas están asociados con los enfoques técnicos comunes, tales como análisis de vulnerabilidad.

víctima Persona víctima Personae son las personas y organizaciones en la mira cuyos activos están siendo explotados y atacado. Estos incluyen nombres de organizaciones, nombres de las personas, las industrias, los roles de trabajo, intereses, etc.

activos víctima bienes de las víctimas son la superficie de ataque y consisten en el conjunto de redes, sistemas, anfitriones, direcciones de correo electrónico, direcciones IP, cuentas de redes sociales, etc. contra la cual el adversario dirige sus capacidades. bienes de las víctimas a menudo existen tanto dentro como fuera del control de una persona y la visibilidad, pero aún están disponibles para la orientación por un adversario. Los ejemplos más comunes de esto incluyen cuentas de correo web y el almacenamiento de datos basado en la nube.

Un activo víctima puede ser el objetivo final (por ejemplo, la víctima) en un evento y luego aprovechado como la infraestructura en otros eventos (probable Tipo 2 Infraestructura como se describe anteriormente en § 4.3). De esta manera, siempre se debe tener cuidado de que el objetivo aparente de la actividad puede no ser necesariamente la víctima.

4.4.1 Vulnerabilidades y Exposiciones

axioma 3 Cada sistema, y por extensión todos los activos víctima, tiene vulnerabilidades y exposiciones.

capacidades adversario explotan las vulnerabilidades y exposiciones definido por el axioma 3 a fi II cumplir su propósito. flexibilidad del modelo permite que éstos sean define como un sub-característica de la víctima. Estos pueden ser descritos como ampliamente como “falta de educación del usuario causando hipervínculos transmitidas por correo electrónico a hacer clic” o como específico como CVE [35] para encajar los requisitos de documentación del evento.

Las susceptibilidades víctima El conjunto de vulnerabilidades y exposiciones de una víctima susceptibles a la explotación que se conoce como la *susceptibilidades víctima*.

En nuestro modelo la lista de susceptibilidades víctima se expresan fácilmente como un sub-tupla de la víctima. Esta información es **valiosa cuando se compara con la capacidad de la capacidad y el arsenal adversario (§ 4.2) para determinar las opciones de mitigación**. Al igual que con la capacidad de la capacidad, esto puede ser alternativamente o conjuntiva describe usando gráficos de actividad de **ataque (ver § 8.3)**.

4.5 de eventos Meta-Characterísticas

Los meta-eventos características amplían el modelo ligeramente para incluir no crítica, pero importante, los elementos de eventos de diamante. Los meta-funciones descritas aquí son las que nos encontramos más útil, pero el modelo no se limita a estos. Los que implementar o extender nuestro modelo puede desear añadir meta-funciones adicionales para capturar otros elementos críticos de la información asociada a un evento.

4.5.1 Marca de tiempo

Cada evento está simbolizada con una fecha y / u hora que se produjo. Puede ser tan específico como sea necesario o se expresa como un rango de valores que indican el inicio y final del evento. Las marcas de tiempo son una parte integral de agrupar las actividades maliciosas como la marca de tiempo permite una fi con reducida confianza en el conocimiento en el tiempo (es decir, una función de la descomposición) como la probabilidad de adversario cambios aumentan con el tiempo. Además, las marcas de tiempo combinados con una colección de eventos adversario lo largo del tiempo pueden conducir a otras formas únicas de análisis, tales como el establecimiento de la periodicidad y la deducción patrón de su vida útil como en [6].

4.5.2 Fase

axioma 4 *Cada actividad maliciosa contiene dos o más fases que deben ser éxito-totalmente ejecutada en sucesión para alcanzar el resultado deseado.*

actividad maliciosa no sucede en un solo evento, sino más bien dos o más eventos. Otros han proporcionado su evidencia fi ciente para apoyar la conclusión de que toda la actividad de intrusión debe considerarse como una cadena de eventos [11, 36, 15]. Por ejemplo, primero un adversario debe hallar la

víctima (por lo general el uso de la investigación y / o de barrido) y luego descubrir una gran cantidad vulnerables, seguido por la explotación, el establecimiento de comando y control, y por último por las operaciones de algún tipo. A menudo, las capacidades Erent di FF y a veces infraestructura ff Erent di se utilizan a través de las fases de una intrusión. Como mínimo una víctima primero debe ser ed identi fi (que podría ser tan simple como la selección de una dirección IP al azar) y luego una acción realizada.

Nuestro modelo puede utilizar cualquier modelo escalonado de las operaciones adversario (tales como [11, 36, 15]).⁷

Más tarde, esto se convierte en una característica significativa como el *fase* del evento describe su ubicación en el hilo de la actividad (§ 8).

Mientras axioma 4 garantiza un conjunto de fases para cada actividad, no ha habido consenso o evidencia de que existe un conjunto de fases que satisfacen la caracterización de toda la actividad malicioso. De hecho, la existencia de tantos actividad de fi niciones de múltiples fases sugiere De otro modo, por ejemplo [36, 11]. Por lo tanto, vamos a suponer que los usuarios del diamante pueden de fi ne fases no esenciales para alguna actividad.

Formalmente, las fases, *PAG*, se definen como una ordenada *norte*- tupla, donde *norte* es el número de fases de un usuario modelo tiene definido como necesario y su cliente FFI para describir todos los posibles eventos y la fase de cada evento es uno, y sólo uno, elemento de la tupla ordenada *PAG*:

$$P = \langle pag_1, pag_2, \dots, pag_{norte} \rangle$$

Dónde:

- *norte* ≥ 2 (existe al menos dos fases como es requerido por el axioma 4)
- *pag* es una fase en la cadena de operaciones adversario
- *pag₁* es la primera fase de las operaciones de un adversario
- *pag_{n+1}* se ejecuta posterior una fase a *pag_{norte}*

4.5.3 Resultado

Aunque no siempre serán conocidos los resultados y post-condiciones de las operaciones de un adversario, o tienen un valor fi anza alto cuando se les conoce, son útiles para capturar. Es particularmente útil para buscar en todas las operaciones de un adversario para determinar su tasa de éxito con capacidades particulares o en contra de subconjuntos de las víctimas. Una colección de post-condiciones también puede proporcionar una visión más amplia de intención adversario. Hay varias maneras de documentar potencialmente el resultado. Un método es utilizar la 3-tupla *< Éxito, el fracaso, Desconocido >*.

Otra es la de separarlo por los fundamentos de seguridad: confidencialidad comprometida, Integridad

⁷ La identificación de una fase para cada evento no es esencial para mantener el conocimiento y correlacionar eventos, pero es útil para fines de planificación de mitigación y análisis de la cadena de muertes.

Comprometida, y disponibilidad comprometida. Mientras que otro enfoque podría documentar todas las post-condiciones resultantes del evento, como la orientación información obtenida (en la etapa de reconocimiento) o contraseñas exfiltrado más tarde útil en ataques de máscaras. Además, se podría utilizar una taxonomía existente para los resultados de ataque tales como las categorías Cohen describe en [26].

4.5.4 Dirección

los *direccionalidad* de un evento es importante cuando se considera las opciones de mitigación y la colocación de detección. Esta meta-característica es típicamente útil para describir eventos basados en la red, pero también puede ser útil para describir eventos basados en host también. En general, existen siete valores posibles para esta función: Víctima-a-Infraestructura, Infraestructura-a-Víctima, Infraestructura-a-Infraestructura, Adversario-a-Infraestructura, Infraestructura-a-adversario, bidireccional o Desconocido. Al mantener esta información y teniendo en cuenta la actividad dirección del adversario con el tiempo mejores decisiones sobre qué combinación de sólo externa, orientada al exterior-, o acciones de detección y mitigación-internos hacia funcionarían mejor para hacer frente al adversario.

4.5.5 Metodología

los *metodología* meta-característica permite un analista para describir la clase general de actividad, por ejemplo: lanza-phish correo electrónico, ataque de entrega de contenido, syn flood, exploración de puertos, etc. Como con otros tipos de entidad, esto también permite que más de una definición de fi como sea necesario. Por ejemplo, un correo electrónico de phishing maliciosos con malware adjunto puede clasificarse tanto como un "e-mail lanza-phishing" y un "ataque de entrega de contenido." Mientras que un correo electrónico de phishing con un hipervínculo que lleva al usuario a un sitio web malicioso puede clasificarse tanto como un "email lanza-phish" y "usuario-redirect explotar." categoriza Este método mejor eventos y permite en indicadores comparación evento independiente tanto para un solo adversario ya través de adversarios para agrupar (§ 9) y los propósitos de mitigación.

Varias taxonomías existentes podrían ser fácilmente incorporadas a esta característica la reducción e ff ORT y aumentar la interoperabilidad con los marcos existentes. Algunos ejemplos incluyen Snort classtypes [37] y muchos estudios más formales [25, 29, 26, 28].

4.5.6 Recursos

axioma 5 Cada evento de intrusión requiere uno o más recursos externos para ser satisfechas antes del éxito.

los *recursos* meta-función muestra uno o más recursos externos caso requiere ser satisfecha. Los recursos son de entenderse en sentido amplio como cualquier y todos los elementos de soporte sobre el que el evento, y por lo tanto cada-feature meta núcleo-y, depende. Este meta-función se vuelve importante cuando las estrategias de mitigación del centro de gravedad de recursos en restricciones y se consideran así como la identificación de lagunas en el conocimiento y la comprobación de hipótesis, como se describe más adelante en § 8.2.

Obviamente, este meta-característica podría ser concebido como abarcando un número de elementos intratables. Sin embargo, al igual que con las otras características del modelo del diamante no requiere integridad, solamente su fi ciencia. Por lo tanto, una organización sólo tiene que enumerar los recursos necesarios para su ejecución sea ff e caces para su uso (s) en particular.

Ejemplo recursos incluyen:

- Software (por ejemplo, Metasploit, sistemas operativos, software de virtualización)
- El conocimiento (por ejemplo, cómo ejecutar metasploit, dónde obtener exploits)
- Información (por ejemplo, un nombre de usuario / contraseña podría enmascarse)
- Hardware (por ejemplo, estaciones de trabajo, servidores, módems)
- Los fondos (por ejemplo, el crédito para la compra de dominios)
- Instalaciones (por ejemplo, electricidad, vivienda)
- Acceso (por ejemplo, una ruta de red desde el host origen a la víctima y viceversa, una dirección y una red de acceso IP enrutables de un Proveedor de Servicios de Internet (ISP))

4.5.7 Ampliaciones Meta-Feature

Varios meta-características se han descrito, que el trabajo bien integrado dentro del modelo. Hay muchas otras características meta-a un evento de intrusión maliciosa que puede ser considerada para su inclusión en función de las **necesidades de la organización: *fuentes de datos* (la fuente de los datos que capturado o detecta el evento), *autor* (el analista-autor del evento), *Método de detección* (la herramienta, la técnica o la capacidad de que detecta el evento malicioso), *firma de detección* (la firma o heurística que detectó el evento malicioso), etc.** La adición de meta-cionales características adiciones mejorará el modelo permitiendo a los usuarios, analistas y organizaciones para mantener la información importante asociada a un evento para su uso futuro (como el correo ff ec- tivo de abastecimiento o crédito por el descubrimiento / autoría, fi nir análisis re, confianza intervalos comprensión, control de calidad, etc.).

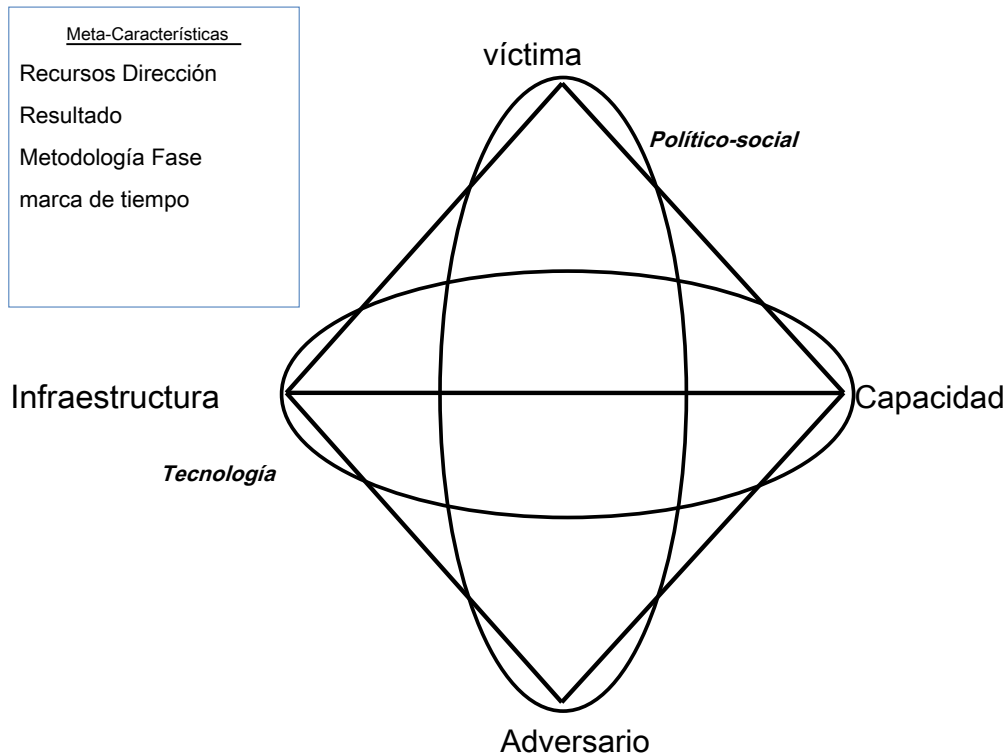


Figura 2: El modelo Diamond extendida ilustra las características únicas social-política y tecnología. Estas características ponen de relieve las relaciones especiales entre el adversario-Víctima (a través de los social-política necesidades, aspiraciones y motivaciones del adversario y la capacidad de la víctima para cumplir esas necesidades) y la Capacidad-Infraestructura (a través de la tecnología utilizada para permitir su comunicación).

5 Modelo Diamante Extended

Como se describió anteriormente, el modelo Diamond se extiende fácilmente para incluir otras características necesarias. Como se ilustra en la Figura 2, dos meta-rasgos fundamentales adicionales de cualquier actividad de intrusiones son: la *Político-social* meta-función de la determinación de la relación adversa-víctima y el *Tecnología* meta-función que permite tanto la infraestructura y capacidades. Estas dos características únicas superposición otras dos características estrechamente definir una relación: uno establecido a través del eje adversario-víctima, el otro a través del eje capacidad de infraestructura.

5,1 político-social

axioma 6 *Una relación siempre existe entre el adversario y su víctima (s) incluso si distante, EUNIÓN fl, o indirecta.*

pares adversario víctima se basan en una relación productor-consumidor que son in-derpinned por las necesidades socio-políticas y las aspiraciones del adversario (por ejemplo, para generar ingresos, para ganar la aceptación en la comunidad hacker, para **convertirse en una potencia hegemónica, para aumentar negocio utilidades**). **La relación indica la necesidad (s) del adversario y la capacidad de la víctima para satisfacer la necesidad (s) de finir la intención adversario** (por ejemplo, el espionaje económico, tradición cional espionaje, fraude criminal, ataque de denegación de servicio, sitio web de la desfiguración). La víctima proporciona, sin saberlo, un "producto" (por ejemplo, recursos informáticos y de ancho de banda como un zombi en una red de bots, un objetivo de la publicidad, la información sensible industrial o de negocios para el espionaje económico, la información financiera y nombre de usuario / contraseñas, por fraude), mientras que los adversarios "consume" su producto.

Intención A pesar de que intención es un aspecto crítico de entender la actividad de intrusos y debe informar fuertemente las decisiones de mitigación, no se incluye como una característica meta de alto nivel fundamental del diamante, pero bene fi mejor como una característica en un socio-política sub-tupla permitiendo además uno a la hipótesis de las necesidades y aspiraciones de orden superior.

5.1.1 Relaciones Adversario persistentes

Axiomas 2 y 6 se pueden combinar para indicar que hay adversarios y que inexplicablemente establecer una relación con su víctima (s). Sin embargo, no todos los barcos PARENTESCO adversario y la víctima son iguales. Algunos adversarios ejecutan "rotura de cristales" operaciones sin la preocupación por el acceso o datos más allá de lo que está inmediatamente disponible sin preocuparse por la pérdida de acceso en cualquier momento. Otros adversarios obstinadamente persisten en sus Orts ff e contra algunas de las víctimas, incluso en la cara de la acción de mitigación sustancial. Algunos adversarios incluso ir tan lejos como para tomar represalias contra los que mitigar sus actividades [6]. La persistencia del adversario para continuar para obtener acceso y / o la información de una víctima es una posible, aunque importante, la caracterización de la relación adversa-Víctima.

Como tal, y la evidencia dada de ambas relaciones persistentes y no persistentes, el siguiente axioma puede postula:

⁸ El término político-social se elige cuidadosamente para categorizar el amplio conjunto de necesidades y aspiraciones de la mayoría de los adversarios, que incluye, pero no se limita a, los individuos, asociaciones, colectivos organizados débilmente, grupos jerárquicos, no estatales y actores estatales. Sus necesidades se pueden describir en términos generales, tanto en términos sociales y políticos. Se podría argumentar que la política es una extensión de las necesidades sociales, la de los individuos que organizan bajo la autoridad de satisfacer los deseos colectivos. Sin embargo, sentimos que separa estos dos términos produce el mejor equilibrio de diálogo en el grupo individual / no estatal necesidades con las necesidades de la autoridad (por ejemplo, gubernamentales o militares) y cómo esas necesidades informar a la selección víctima y, por tanto, las decisiones de mitigación.



Figura 3: Un diagrama de Venn que ilustra el conjunto de todas las relaciones adversario-víctima como definido por axiomas 2 y 6, así como el subconjunto de relaciones adversario persistentes definido por el axioma 7.

axioma 7 Existe un subconjunto del conjunto de adversarios que tienen la motivación, recursos y capacidades para sostener ECTS e ff maliciosos durante un período significativo de tiempo frente a una o más víctimas al resistirse Orts ff mitigación e. Adversario víctima rela- ciones en este sub-conjunto se denominan relaciones adversario persistentes.

Adversario persistente UNA *adversario persistente* es un adversario que satisface el axioma 7 en una relación adversario-víctima en particular.

La Figura 3 ilustra la relación entre el conjunto completo de adversario-víctima relaciones definida por axiomas 2 y 6 y el sub-conjunto de adversarios persistentes como definido por axioma 7. La colocación de una relación adversario-víctima a uno de estos conjuntos es determinado por la satisfacción de Axiom 7.

No es necesario que debido a un adversario es persistente contra una de las víctimas son persistentes en contra de todas las víctimas. Por ejemplo, en una actividad adversario puede tener acceso, determinar que no hay valor, y dejar sin tener en cuenta la persistencia. Sin embargo, en otra actividad adversario puede persistir durante mucho más tiempo con el fin de obtener más valor. Desde la otra perspectiva, una víctima puede ser acogida a varios adversarios de los cuales algunos pueden ser persistentes, mientras que otros son no persistentes. Por lo tanto, la persistencia o no persistencia se determina por el par adversario-víctima en particular.

Fleeting Enduring

Figura 4: grado de persistencia Spectrum ilustra que no todos los persistentes relaciones adversario son iguales, pero en vez caen en un espectro entre REUNIÓN fl y duradera. Cuando una relación adversa-víctima en particular cae en el espectro es una función de muchos elementos y también cambia con el tiempo.

Por otra parte, la persistencia no es una característica binaria ni estático. Aunque es bien sabido que muchas intrusiones persistentes pueden ser mitigados mediante medidas técnicas, como en Stoll [4], en Cheswick "Berferd" [6] ilustra que algunos adversarios resisten medidas técnicas e intentos vergonzosos incluso públicas. En el caso de "Berferd", mitigación por último se consigue mediante una llamada telefónica a las madres de los hackers. Por lo tanto, el grado de persistencia varía y se propone la siguiente corolario:

corolario 1 Existe diversos grados de persistencia adversario predicada sobre los fundamentos de la relación adversa-Víctima.

los grado de persistencia describe la fuerza de motivación y capaci- dades del adversario, así como la ORT y siguientes y los recursos e un adversario expenderá a mantener su correo ff ect. El grado de persistencia se manifiesta a lo largo de un espectro entre REUNIÓN fl a la más perdurable, como se ilustra en la Figura 4, y en muchos casos determina la cantidad de e ff ORT y recursos un defensor requiere para resistir la persistencia. Cuanto más fuerte es la motivación y la capacidad del adversario y el más resistentes que son a la mitigación equivale a una relación persistente más duradero moviéndose hacia la derecha del espectro.

Tradicionalmente, la mitigación se ha limitado a los medios técnicos que giran alrededor de la capaci- dad del adversario y ha tenido poco impacto en su motivación y los recursos resultantes en el adversario regresar poco después de ser retirado de la víctima. Al hacer que la relación política-social y sus necesidades y aspiraciones asociadas una parte clave de la actividad maliciosa, el diamante permite la aplicación de los dominios no tradicionales, tales como la psicología, Inology crim-, victimología, marketing, comportamiento del consumidor, y la economía para expandir la mitigación opciones. En particular, se sustenta la toma de decisiones del adversario y su preferencia percibida destacando las variables y aspectos que pueden ser controlados y en influido a favor de la defensa, además de opciones técnicas tradicionales.

Los siguientes son algunos de los elementos de la relación adversario-víctima que determinan el grado de persistencia:

- La fuerza relativa de las necesidades del adversario, que la víctima ful LLS fl en comparación con otras necesidades
- El riesgo adversario percibe tanto a la continuación ECTS e ff

- El costo del adversario requiere para mantener e ff etc.
- La singularidad de la víctima para satisfacer una necesidad particular
- La continua satisfacción de la necesidad por la víctima
- El nivel de e ff Ort y recursos defensor gasta para resistir la persistencia

Para ambas relaciones adversario persistentes o no persistentes, la colocación en el espectro es única para cada par adversario-víctima. Para facilitar la consulta y el análisis, y sin menosprecio a la complejidad y el espectro continuo **representa, por lo general consideran dos clases de víctimas en el espectro: las víctimas de oportunidad y víctimas de interés.**

Víctima de Oportunidad Una víctima que es un producto prescindible en las operaciones de un adversario, donde la pérdida de acceso probablemente no se dio cuenta ni hacer que el adversario a gastar recursos para recuperar el acceso. Las víctimas en este otoño clase al lado izquierdo del espectro persistencia hacia la "REUNIÓN fl", así como en el conjunto de relaciones no persistente. Estas víctimas fueron atacados inicialmente probablemente porque eran vulnerables y disponibles en el momento adecuado.

Víctima de interés Un bien no fungible donde el acceso continuo proporciona un valor suficiente para un adversario que la pérdida de acceso causaría aviso y adversario gastaría recursos recuperar el acceso a la o las víctimas relacionadas. Las víctimas en este otoño clase al lado derecho del espectro persistente hacia la "perdurable".

Es importante destacar que una relación adversa-Víctima persistente no es estático en el espectro - que puede cambiar. El hecho de que una víctima inicialmente comienza como REUNIÓN fl y una víctima de oportunidades no significa que no puedan desplazarse más tarde. Por ejemplo, si la víctima es explotada inicialmente con un gusano propaga por sí mismo, pero los NDS adversario fi la víctima es mayor al valor de una mercancía, que podría convertirse en una víctima de interés moviéndose hacia la derecha a lo largo del espectro hacia la "perdurable".

5.1.2 Cyber-Victimología

Nuestro modelo es único en que se coloca a la víctima y el adversario en un espacio equivalente y pone de relieve la relación normalmente tácito entre los dos. Además, como nuestro modelo se amplía para abarcar muchos adversarios y **víctimas a través Hilos de actividad (§ 8) y Grupos de actividad (§ 9)** podemos empezar a dibujar en la experiencia de la criminología y la victimología que conduce a importantes preguntas tales como:

- ¿Por qué fue víctima de una entidad en particular?

- ¿Hay un conjunto común de las víctimas?
- ¿Las víctimas comparten un rasgo común?
- Podemos deducir la intención del conjunto de las víctimas?
- ¿Quién podría haber otros, todavía desconocidas, las víctimas?
- ¿Quién tiene las necesidades y la intención de victimizar a este conjunto de organizaciones?

Es importante destacar que, con un mejor modelo de la victimología, podemos empezar a examinar los métodos de Con- tering adversario haciendo víctimas menos atractiva y predecir las futuras víctimas. Esto permite que una organización para maximizar los recursos de detección adecuada, al igual que un detective se centra en la población de más alto riesgo y el área de la delincuencia concentrada en lugar de patrullar áreas al azar. 9

Los recientes ataques “riego hoyos” 10 ilustrar cómo adversarios utilizan este concepto de perfil a sus víctimas con el fin de colocar un exploit en el lugar más lucrativo. Por ejemplo en abril de 2013 una reciente hazaña por etapas en los sitios web relacionados con activistas tibetanos-trataron de explotar cualquier visitante con un navegador vulnerables [40]. Sin embargo, **como alternativa, si la función político-social se utiliza e ff caz en conjunción con el enfoque centrado en la víctima (§ 7.1.1),** algunos lugares riego hoyos se pueden predecir y específicos de detección / mitigación puesto en marcha para anticiparse a la actividad maliciosa.

5.1.3 Espacio amenaza compartida

Si dos o más víctimas comparten suficientes características que satisfagan las necesidades de uno o más adversarios entonces están en un “espacio amenaza compartida.” A principios de identificación de espacio amenaza compartida es una piedra angular para la mitigación estratégica y proactiva. Por ejemplo, los ataques dirigidos contra uno de los miembros permiten el espacio amenaza colectiva para pronosticar y predecir futuros ataques. Por otra parte, el intercambio de la información sobre amenazas es más lucrativo con los más propensos a ser afectados por un adversario similar.

5.2 Tecnología

Además de la función de meta-político-social, la *tecnología* meta-función también pone de relieve una relación especial y se extiende por dos características fundamentales: la capacidad y la infraestructura. Esta

9 Un estudio de la criminología interesante reveló que un aumento en la cobertura de árboles dentro de los barrios urbanos estadísticamente correlacionada con una reducción de la delincuencia [38]. Podría existir un paralelismo potencial para la actividad de intrusos?

10 ataques de riego hoyos son una metodología donde el adversario compromete sitios web legítimos que creen su clase pretendido de víctimas visitará este modo explotarlos. La analogía y término se extrae de leones que ponen en espera para emboscar presa en un abrevadero [39].

representa la tecnología de conexión y permitiendo la infraestructura y la capacidad de operar y comunicarse.

Por ejemplo, si el malware instalado resuelve dominios y se comunica a través de HTTP, las tecnologías utilizadas son: Protocolo de Internet (IP), Protocolo de control de transporte (TCP), Protocolo de Transferencia de Hipertexto (HTTP) y el Sistema de Nombres de Dominio (DNS). Mediante el análisis de la tecnología y su potencial de anomalías / mal uso, un analista descubre nueva actividad **maliciosa independientemente de la infraestructura y la capacidad subyacente (también conocido como el *centrada en la tecnología enfoque***

§ 7.1.6). Además, la comprensión de las tecnologías implicadas en la actividad adversario ayudar en la identificación de los lugares más adecuados de detección, tipos de datos y capacidades.

6 Indicadores contextuales

Los indicadores son aquellos elementos de información utilizadas por los sistemas y analistas para detectar ad- operaciones versario. En el curso normal del negocio, los indicadores se cargan en los sistemas de detección que alerta a los analistas actividad potencial adversario. Los indicadores tradicionales se han limitado a los detalles técnicos. Algunos han extendido estos para incluir metadatos adicionales [32]. Sin embargo, es el momento de que los indicadores se extienden para incluir elementos que son no técnico, de comportamiento y de naturaleza conceptual que aumentan, pero no se implementan directamente por, la detección automatizada.

Indicador contextuales UNA *indicador contextual* es un elemento de información se coloca en el contexto de operaciones de un adversario enriquecer tanto la detección y análisis. Diamante indicadores contextuales derivados asegurar la relación entre los elementos y su papel se conservan y conceptos analíticos tales como las necesidades adversario y la intención son totalmente incorporado la producción de un contexto más completa.

Por ejemplo, en un indicador tradicional enfoque de la infraestructura dirección IP de un adversario es un elemento común. Gracias a este modelo como base para una ontología, esta dirección IP se puede colocar en contexto que proporciona el analista no sólo el conocimiento de la infraestructura adversario (probablemente una alerta de detección), sino también el conocimiento de los tipos / clases de víctimas previamente comprometidas y, posiblemente, los elementos de información adversario estaba intentando poner en riesgo (por ejemplo, documentos de planificación de negocios, propiedad intelectual). El uso de este conocimiento mejorado, el analista está armado, no sólo para detectar y con fi rmar la intrusión (disponible con los indicadores tradicionales), sino también determinar si son parte de una campaña adversario, información que **pueden ser objetivo por el adversario, § 5.1).**

Este contexto permite a la organización a tomar mucho más estratégica de mitigación. Por ejem plos, la organización puede ahora permitir la detección fi c adversario especí y mitigación de los activos que contienen información de valor, desarrolle una campaña de mitigación prolongada (tal como uno descrito en [11]), identificar y comunicarse con socios de la *el espacio amenaza compartida (§ 5.1.3)*

para desarrollar planes de mitigación conjuntas, e intercambiar indicadores no técnicos, etc.

7 Analytic pivotante

Pivotante es la técnica analítica de la extracción de un elemento de datos y la explotación de ese elemento, en conjunción con fuentes de datos, para descubrir otros elementos relacionados. En última instancia, es pivotante sobre la tarea analítica fundamental de la prueba de hipótesis. Cada elemento de un evento de intrusión genera sus propias hipótesis que requieren pruebas para fortalecer, debilitar o cambiar la hipótesis. Pivotante es la tarea de descubrir elementos relacionados (evidencia) que informan a la hipótesis y también generan nuevas hipótesis a sí mismos. Pivotante éxito se basa en el analista para comprender la relación entre los elementos y su capacidad de explotar con éxito un elemento de datos y fuentes de datos (por ejemplo, si tengo esta información, combinada con esta fuente de datos, entonces puedo hallar esto...).

El modelo Diamond apoya fundamentalmente analítica pivotante y es una de sus características más fuertes. De hecho, el diamante fue revelada originalmente después de explorar escenarios de pivote. Las características fundamentales están estructurados como un 'diamante' con la conexión de bordes destacando oportunidades de pivote para iluminar otros elementos de las operaciones de un adversario. Con un punto del diamante, posiblemente, el analista puede descubrir y desarrollar las otras características conectadas.¹¹

Utilizando la Figura 5 como un ejemplo: (pivote 1) una víctima descubre malware en su red, (pivote 2) el malware se invierte la exposición de la-comando y control (C2) de dominio, (pivote 3) el dominio se resuelve la exposición de la dirección IP subyacente de alojamiento controlador del malware, (de pivote 4) registros de fi cortafuego se examinan esclarecedores otros equipos comprometidos en la la red de la víctima para establecer comunicaciones con la dirección IP del controlador de malware ahora revelada, y finalmente (pivote 5) el registro de la dirección IP revela detalles adversario potencial que ofrecen la atribución del adversario.

7.1 Enfoques 'Centrado'

El modelo se presta a varios conceptos de análisis Tradecraft intrusión enfocado. Estos se conocen como 'centrada' se acerca a medida que se centran en un rasgo específico de la Diamond con el fin de descubrir nuevas actividades maliciosas y revelar la actividad relacionada con las otras características conectados y la función en sí.

7.1.1 Enfoque centrado en las víctimas

La mayoría de las organizaciones, a través de la red normal y la vigilancia de acogida, detección y operaciones de defensa, están ejerciendo un enfoque centrado en las víctimas. Con este enfoque, el análisis de datos

¹¹ El éxito no está garantizado por el diamante. Sólo se pone de manifiesto que es posible, no lo que es cierto.

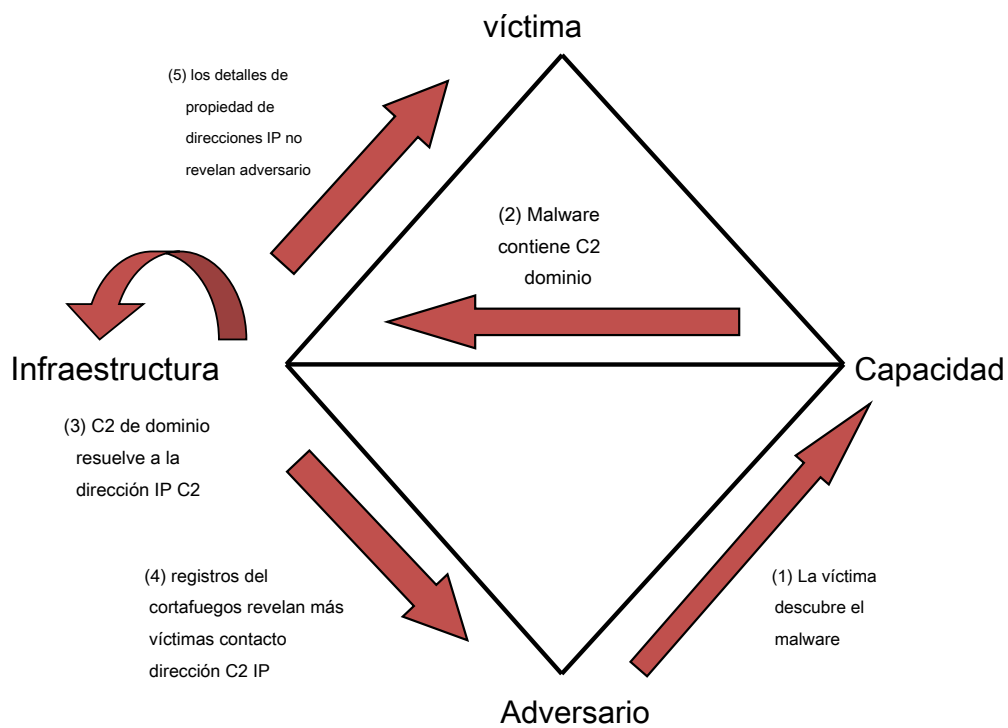


Figura 5: pivote analítico usando el diamante se ilustra. Una de las características más potentes del diamante, pivote analítico permite un analista para explotar la relación fundamental entre las características (resaltado por los bordes entre las características) para descubrir nuevos conocimientos de la actividad maliciosa.

relacionados con una posible víctima revela los otros elementos relacionados (y Diamond-unidas): capacidades maliciosas e infraestructura. El Honeynet Project es un excelente ejemplo de este enfoque. Mediante el establecimiento de una figura de acogida especialmente con la intención de ser víctimas están invitando a los adversarios para explotar el anfitrión, revelando sus capacidades e infraestructura que puede ser publicado para la mitigación y la educación [7].

Otro ejemplo interesante del enfoque centrado en las víctimas es donde los analistas monitoreados servicios para los usuarios del Himalaya que se cree ser el blanco de un adversario muy capaz [41]. Esto, según lo predicho por el modelo del diamante, producido nueva información sobre capacidades maliciosas e infraestructuras como el adversario atacó a los usuarios de la red supervisada. Curiosamente, este enfoque centrado en las víctimas se combinó con el enfoque social centrado en la política (§ 7.1.5) que permite a los investigadores para llegar a un adversario específico mediante la predicción de su víctima, lo que aumenta sus posibilidades de éxito y la adición de atribución confianza.

7.1.2 Enfoque de Capacidades Centrada

El enfoque centrado en la capacidad explota las características de una capacidad de descubrir esos otros elementos relacionados en las operaciones adversario: víctimas que se utiliza esa capacidad en contra, la infraestructura de apoyo a la capacidad, la tecnología que permite la capacidad, pistas sobre otras capacidades relacionadas, y (posibles) pistas para adversario. Los resultados de este enfoque son más frecuentes con los informes de los proveedores de antivirus.

Como primer ejemplo, el análisis por Symantec y CrySyS proporciona un enlace de Stuxnet a Duqu basado en varias características y técnicas comunes empleadas en el código que sugiere un autor común. En este caso, estas características son tan avanzadas que les llevó a girar hasta la característica adversario para deducir posibles adversarios responsable. Este es un ejemplo de una capacidad de pivote adversario, usando el meta-función social-política para reforzar la confianza en la atribución [42].

Como un segundo ejemplo, el análisis de Kaspersky de "Octubre Rojo" proporciona una excelente estudio de caso en el análisis centrada en la capacidad con múltiples pivotes. Aquí el trabajo se inicia con la capacidad de malware y se ingeniería inversa para la tecnología (HTTP, cifrado RC4, compresión zlib), estructuras C2, y la infraestructura. A continuación se usó la capacidad en combinación con su base de datos de detección de anti-virus de víctimas (de pivote-víctima-a capacidad) para detectar "sobre 1000 di ff Erent" asociado fi les que también se invierte para identificar otros infraestructura (capacidad-a-pivote infraestructura) que fueron luego "sinkholed" ¹² identificar a las víctimas globales (de pivote-infraestructura de la víctima). Cada víctima fue además identi fi cado en cuanto a su posición socio-política (por ejemplo, embajada, gobierno, militar, energía), presumiblemente para permitir al lector a inferir posibles adversarios que habría adecuación a las exigencias socio-políticas que utilizan cibernética victimología (§ 5.1.2) [43].

¹² "Sinkholing" es una técnica agresiva defensa de las posiciones públicas de adquisición de la infraestructura para la mitigación del adversario (el adversario ya no puede usar lo que no controla) y análisis (software malicioso y las víctimas siguen comunicándose a la infraestructura ahora controlada defensa-).

7.1.3 Enfoque Centrado en Infraestructura

El enfoque centrado en la infraestructura se centra en la infraestructura maliciosa del adversario. A partir de este elemento de otros elementos relacionados pueden ser descubiertos: víctimas en contacto con la infraestructura, la capacidad de ser entregados o controlados con la infraestructura, otra infraestructura relacionada (tal como direcciones IP resuelta por dominios maliciosos), y (posibles) pistas sobre el adversario, incluidos aquellos que puede estar en control directo de la infraestructura.¹³

El equipo de comandos Cinco demostró un enfoque muy centrado en la infraestructura en su investigación SKHack [44]. Si bien los detalles iniciales fueron recogidos de software malicioso descubierto durante la respuesta, los autores utilizaron las resoluciones de dominios conocidos de devolución de llamada a IP ad-vestidos y luego giran a la información de registro WHOIS para descubrir muchos otros dominios con un solicitante de registro común (infraestructura-a-adversario pivote). Luego éxito-infraestructura totalmente mapeado que no había sido utilizada en el ataque pero fue probablemente controlada por la misma posicionamiento adversario para las acciones defensivas preventivos (por ejemplo, el bloqueo de acceso a la red a aquellos dominios antes de su uso operativo).

7.1.4 Enfoque Centrado Adversario

Se podría teorizar que el enfoque centrado en el adversario es el más difícil de los diversos enfoques centrados-. Se trata de seguimiento de un adversario directamente a descubrir su estructura y capacidades tura. Por supuesto, esto será probablemente el método más conveniente, pero está limitada por la necesidad de acceso. Por ejemplo, la Oficina Federal de Investigaciones (FBI) supervisa la actividad de las conversaciones telefónicas y de módem de los "Phonemasters" piratería grupo que se identifica el alcance total de sus operaciones incluyendo otros personajes adversario involucrados, así como sus víctimas, las capacidades y infraestructura [45]. Sin embargo, uno debe ser advertido por los cuentos de otros que hacen un seguimiento muy de cerca adversarios y pagan un precio [46].

7.1.5 Enfoque social-político-Centered

El enfoque de la política centrada en el social es único. Solo, que no conduce directamente a los nuevos elementos o indicadores, sino que saca provecho de una relación adversa-víctima esperada a la hipótesis de que puede ser una víctima y lo que pueden ser sus adversarios, o, alternativamente, que pueden ser un adversario y sus víctimas esperados. Esto puede dar lugar a los elementos que pueden ser explotadas utilizando el enfoque adversario centrada o centrado en la víctima para obtener detalles tácticos.

¹³ Los analistas suelen explotar el enlace adversario infraestructura mediante la exportación de información de registro, pero a menudo se ven frustrados por información falsa. Sin embargo, la información falsa (por ejemplo, como el que en un registro de dominio) puede ser útil si el adversario utiliza la información de proporcionar constantemente una persona común que se puede controlar y / o rastrear entre los eventos maliciosos

conclusiones analíticas tomadas de la correlación de la actividad de intrusos y de la vida real los acontecimientos políticos son en realidad bastante común. Ya en 1990 Cheswick correlaciona la actividad de intrusión contra su red a la Guerra del Golfo de 1990 a 1991 [6]. Más recientemente los 2008 Georgia ataques DDoS y ataques sostenidos contra grupos pro-Tíbet se han correlacionado con acontecimientos políticos actuales [47, 48]. Sin embargo, la cautela eterna que la correlación no es causalidad debe ser atendida.

7.1.6 Enfoque centrado en la tecnología

El enfoque centrado en la tecnología permite a un analista para apuntar potencial mal uso o el uso anómalo de una tecnología para descubrir infraestructura y las capacidades que utilizan tales técnicas previamente desconocido. Monitorear y detectar anomalías en el sistema de nombres de dominio (DNS) ha sido un método popular y fructuosa de la aplicación del enfoque centrado en la tecnología para descubrir nueva actividad maliciosa [49, 50]. Otros han explorado anomalías en cabeceras de los paquetes en las redes de back-óseas [51].

Tema 8 Actividad

Axiom 4 establece que un adversario no opera en un solo evento contra una víctima, sino más bien en una cadena de acontecimientos causales dentro de un conjunto de fases ordenadas en el que, en general, cada fase debe ser ejecutado **con éxito para alcanzar su intención**. ¹⁴ Un *hilo actividad* es un gráfico fase ordenada dirigido donde cada vértice es un acontecimiento y los arcos (es decir, bordes dirigidos) identificar relaciones causales entre los eventos. Los arcos están etiquetados con la analítica con fi anza establecer la relación causal, si la trayectoria es Y (necesario) o OR (opcional - no hay más de un camino potencial de un evento), si el arco es real o hipótesis, así como con la información o recurso el **evento anterior proporciona lo que se requiere para que ocurra el próximo evento**. ¹⁵ Los hilos están organizadas verticalmente de tal manera que cada hilo describe todos los eventos causales un adversario ejecutado contra una víctima específica (sin embargo, la implementación del modelo define la función víctima) dirigidas colectivamente en fi ful llenado intención del adversario. Por lo tanto, cada hilo es específico para un par adversario-víctima - aunque en muchos casos los hilos de actividad sólo se pueden variar ligeramente entre víctimas como

¹⁴ Como se indica en § 4.5.2, el conjunto de fases pueden incluido fases no esenciales para una actividad determinada y por lo tanto

no toda la actividad puede ajustarse a la serie completa de fases disponibles. Por lo tanto, decimos que *generalmente* cada fase debe ser ejecutado con éxito para alcanzar una intención, pero no es necesariamente válida para todas las fases a través de toda la actividad.

¹⁵ Tanto Y / O y requiere / proporciona conceptos se han incorporado a los modelos anteriores y ambos son útiles en los modos di ff Erent de desarrollo de la estrategia de mitigación. caminos de ataque conjuntivas y disyuntivas son tomados de la obra original de Schneier en Ataque árboles [15] y es útil para la accesibilidad, optimización de la ruta, y otras técnicas de análisis de gráfico para desarrollar estrategias de mitigación. El concepto de gráficos de ataque centradas en los recursos ha sido tomada de [52] y útil en el desarrollo de estrategias de mitigación restricción de recursos. Esto no quiere decir que tanto debe ser utilizado en conjunto, sino más bien proporciona la máxima oportunidad de aplicar técnicas y siguientes Erent di para su posterior comparación, ya que ni se ha demostrado ser óptima por sí mismos en la generación de estrategias de mitigación. Las salidas de estas técnicas se pueden comparar utilizando un modelo de soporte de decisión, tal como ADAM para pesar sus diversos riesgos, costes y beneficios [13]. Para apoyar esto, y como se describe originalmente por Schneier en [15], los arcos también pueden incluir ponderación, prioridad, u otros ERS cuantificadores.

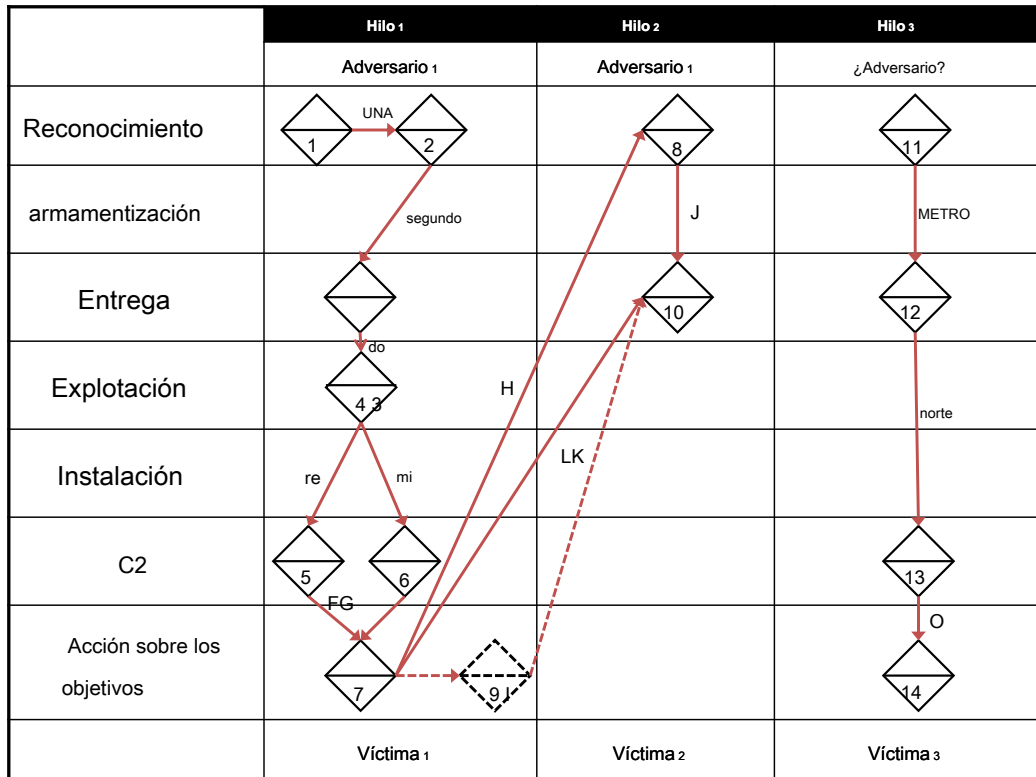


Figura 6: una visualización de ejemplo de hilos de actividad que ilustran eventos de diamante que están unidas verticalmente (dentro de una sola víctima) y horizontalmente (a través de víctimas) a través de arcos dirigidos que designan una relación causal entre los eventos (es decir, este evento se produjo porque de, y posterior a, este evento). En la figura, las líneas continuas representan elemento real de información de apoyo de la evidencia y las líneas de trazos representan elementos hipótesis. Ver Tabla 1 para las descripciones de eventos y en la Tabla 2 para las descripciones de arco.

Tabla 1: Ejemplo Actividad Descripciones hilo de eventos para la Figura 6

Hipótesis Evento / descripción real		
1	Real	Adversario lleva a cabo una búsqueda en la web de la empresa víctima Gad- consigue Inc. recibir como parte de los resultados de su dominio gad- gets.com
2	Real	Adversario utiliza el dominio recién descubierto gadgets.com para una nueva búsqueda "administrador de la red gadget.com" descubriendo remitidos a foros de usuarios que afirman ser los administradores de red de gadget.com revelando sus direcciones de correo electrónico
3	Real	Adversario envía correos electrónicos de phishing de lanza con una troyanizado attachment a los administradores de red de gadget.com revelado en el Evento 2
4	Real	Un administrador de red (NA1) de gadget.com abre el archivo adjunto malicioso ejecutar el cerrado explotar permitiendo para su posterior ejecución de código
5	Real	anfitrión de NA1 explotados en el Evento 4 envía un mensaje HTTP mensaje a una dirección IP registrándolo con un controlador y recibe una respuesta HTTP a cambio
6	Real	Se puso de manifiesto a partir de la ingeniería inversa de malware en el host del NA1 que el malware tiene una dirección IP adicional con fingurar que actúa como una copia de seguridad si el anfitrión primero no responde
7	Real	A través de un mensaje de respuesta HTTP-mando y control enviado al host del NA1, el malware comienza a conexiones de proxy TCP
8	Real	A través de la delegación prevista en el host del NA1, Adversary1 hace una búsqueda en Internet para "la investigación cada vez más importante" y NDS fin la víctima Interesante Research Inc.
9	Hipótesis	Adversary1 comprueba NA1s lista de contactos de correo electrónico para los contactos desde Interesante Research Inc. y descubre el contacto para el interesante Research Inc. principal de investigaciones oficiales
10	Real	Jefe de Investigación oficial del Interesante Research Inc. recibe un correo electrónico de phishing de lanza del vestido de Ad-mail de tu NA1 de Gadget Inc enviado desde el host de NA1 con la misma carga útil como observado en el Evento 3
11	Real	Un adversario exploraciones desconocidos para los servidores web vulnerables, incluyendo Victim3
12	Real	Un exploit para una vulnerabilidad escaneada para previamente en el Evento 10 se entrega a través de la red Victim3
13	Real	El servidor explotado, Victim3, establece un shell remoto al adversario
32		
14	Real	El adversario utiliza el shell remoto para descargar todos los documentos en el directorio privado de Victim3

Tabla 2: Ejemplo actividad de los hilos Descripciones de arco para la Figura 6

La confianza de arco y / o hipótesis / real proporciona una				
	Bajo	Y	Real	Proporciona el dominio de Gadgets Inc., gadgets.com
segundo	Alto	Y	Real	Proporciona objetivos de phishing: direcciones de correo electrónico de la red administra- dores de gadgets.com
do	Alto	Y	Real	[Ninguna]
re	Alto	O	Real	[Ninguna]
mi	Alto	O	Real	[Ninguna]
F	Alto	Y	Real	[Ninguna]
sol	Alto	Y	Real	[Ninguna]
H Medium		Y	Real	Proporciona acceso al proxy de la víctima anterior al motor de búsqueda
yo	Bajo	Y	Hipótesis	El acceso a la lista de contactos de correo electrónico
J	Alto	Y	Real	organización víctima la identificación fi
K	Bajo	Y	Hipótesis	Victima dirección de correo electrónico, nombre y su función identificación
L	Alto	Y	Real	Lanza-phishing de correo electrónico troyanizado
METRO	Alto	Y	Real	Proporciona la salida de los resultados del análisis ful Éxito de la identificación de la Vic- tim servidor web como vulnerables a la explotación
norte	Alto	Y	Real	[Ninguna]
O	Alto	Y	Real	Proporciona la cáscara alejada establecido

adversario consolida la infraestructura, procesos y capacidades para reducir los costos.

Correlación Vertical Es raro el caso de que se conocen todos los eventos en un solo hilo actividad vertical. Además, puede tomar e ff ORT para establecer relaciones causales entre eventos dentro de un hilo que requieren investigación adicional, la recogida de datos y análisis. El proceso analítico de identificar los vacíos de conocimiento, llenando los huecos con nuevos conocimientos, y estableci- ing relaciones causales (y etiquetas de arco asociados) dentro de un solo hilo actividad **adversario-víctima vertical se denomina *correlación vertical*. Por fase-organización de la rosca, también se puede identificar más fácilmente las lagunas de conocimiento donde debería haber ocurrido actividad pero no existe conocimiento de tal (ver § 8.2 para más información).**

Es común que un adversario a utilizar los recursos obtenidos en una sola operación para permitir operaciones futuras o para explotar las relaciones de confianza interna para acceder más profundamente en una red específico - conocido en las pruebas de penetración como pivote y explotación lateral. Por lo tanto, las relaciones causales (arcos) pueden abarcar uno o más hilos horizontalmente. Además, como se ve en la Figura 6, las fases pueden contener más de un evento y arcos puede incluso ir 'hacia atrás' para describir un proceso iterativo mientras que los bordes describen los recursos obtenidos y usados entre eventos.

La correlación horizontal El proceso analítico de vincular causalmente eventos entre hilos verticales a través de pares adversario-víctima, la identificación de las lagunas de conocimiento comunes entre los hilos, y utilizar el conocimiento de un subproceso a lagunas de conocimiento llenar en otro se denomina ***correlación horizontal*. Este proceso también conduce a la identificación de características comunes en las víctimas que puede conducir a la creación de un grupo de actividades en un proceso de fi ne más adelante (§ 9).**

Estos hilos actividad de la forma de un nuevo tipo de gráfico ataque fase ordenada ^{dieciséis} informado por observa- ciones de los acontecimientos reales para predecir la probabilidad y adversario preferencia por caminos particulares. Al igual que con los gráficos de ataque tradicionales, la actividad hilos de actividad de múltiples etapas complejo modelo que puede explotar múltiples vulnerabilidades del sistema y de red. Sin embargo, a diferencia de los gráficos de ataque tradicionales que tratan de enumerar de forma exhaustiva todos los caminos posibles, hilos de actividad de borde modelo knowl- de trayectorias de ataque real y la interdependencia entre y dentro de las roscas. La naturaleza de los hilos de actividad, tal como se define en esta sección, permite para un evento / vértice para satisfacer una o **más de las necesidades de recursos de otro evento (§ 4.5.6) que permiten el caso después de ocurrir. Además, cada vértice es un evento que trae consigo la profundidad de la información un evento proporciona que la información gráfica rico, así como inherentemente más utilizable.**

Formalmente, podemos de fi ne el hilo actividad como un gráfico dirigido, A , dónde $AT = (V, A)$ es un par ordenado de tal manera que:

- $|V| \geq 1$, existe al menos un evento en el hilo ¹⁷

^{dieciséis} gráficos de ataque son una enumeración de todos los caminos posibles a un adversario puede tomar para penetrar las redes de ordenadores logrando su propósito deseado.

¹⁷ Mientras axioma 4 se asegura de que hay al menos dos fases a cada actividad es probable que no todos son

- A es un gráfico infinito
- V es el conjunto de todos los eventos dividida en sub-conjuntos de tal manera que todos los eventos en una cuota de sub-establecer el mismo adversario y víctima y se divide adicionalmente en pag tuplas marcados donde pag es el número de fases de finido y cada evento se coloca en la tupla que coincide con su fase de
- UNA es el conjunto de pares ordenados de tal manera que los arcos $arco(x, y)$ Se define si y sólo si el evento adversario ejecutado con éxito y debido a eventos X y el evento X evento directamente precedido y
- No puede existir más de un arco a cualquier evento. Por ejemplo, dada tres eventos $X, Y, y z$ no puede existir un camino desde X a y $arco(x, y)$ así como un camino desde z a y $arco(z, y)$.
- No puede existir más de un arco de cualquier evento. Por ejemplo, dada tres eventos $X, Y, y z$ no puede existir un camino desde X a y $arco(x, y)$ así como un camino desde X a $arco z(x, z)$.
- No puede existir solamente una trayectoria desde un nodo a otro (es decir, cada arco par ordenado es único dentro de la gráfica). Por ejemplo, dada dos eventos X y y sólo puede existir un camino de X a y $arco(x, y)$.
- Los arcos se marcaron con un 4-tupla $< Confianza, Y / O \text{ hipotético / real, Proporciona } >$ dónde:
 - Confianza: de definición de la analítica confianza en la existencia de una nave causal entre PARENTESCO X y y
 - Y / o : de fin si la ruta de X a y es necesario y requerido para y para tener éxito (Y) o si la trayectoria es una alternativa y la ruta opcional para lograr y desde X (O)
 - Hipotético / Actual: distingue un arco hipotético de un arco real (apoyo pothesis hi- se describe en § 8.2) apoyada por la evidencia
 - Proporciona: de definición de los recursos X proporciona a y para ser coincidente con éxito los requisitos enumerados en el meta-estelar evento recursos (§ 4.5.6)

conocido en el momento de descubrimiento y por lo tanto una rosca actividad puede ser creado inicialmente con un solo evento. La fase (s) vacía y evento (s) que falta se tratan entonces como vacíos de conocimiento.

Proceso 8.1 Adversario

Colectivamente, los hilos verticales y vínculos horizontales e ff caz describen el proceso final- a extremo de un adversario tal como se define por el axioma 4. Esta se enriquece aún más por los propios eventos que contienen las características de las acciones individuales (por ejemplo, la capacidad y la infraestructura utilizado, la metodología específica, los recursos **externos Biosystems**). **En conjunto, estos definen cómo adversario ejecuta sus operaciones, su *modus operandi*.**

Sin embargo, en muchos casos un adversario demostrará una preferencia por ciertos elementos y comportamientos dentro de sus procesos más amplios. Este hecho ha sido identi fi cada y explorado en criminología y es probable que el resultado de la atracción humana a la cómoda y familiar basada en la cultura, el conocimiento, la formación, la experiencia, etc. [53] En las grandes organizaciones, estas preferencias es probable que también llevar por las políticas y los edictos de los líderes. analistas de intrusión suelen identificar estas preferencias a través de elementos comunes a través de una campaña al igual que los investigadores criminales tradicionales a identificar a través de pruebas común entre las escenas del crimen.

La capacidad de identificar y articular estas características comunes y comportamientos adversario es de gran alcance. Con esta **caracterización analistas pueden grupo como-hilos juntos que comparten procesos similares (ver § 9) sin la necesidad de hacer** coincidir las características exactas (por ejemplo, la misma dirección IP, la infraestructura de la misma capacidad) para cada evento. El modelo Diamond de fi ne esto como una *proceso adversario*.

Por ejemplo, la Figura 7 ilustra un proceso adversario definido de eventos 2, 3, 4 y 6 en la Figura 6. Este proceso adversario es generalmente descrito como: un evento de reconocimiento que incluye una búsqueda de la web “administrador de red”, seguido (pero no necesariamente inmediatamente) por la entrega de un correo electrónico con un archivo adjunto de troyanizado, seguido de un específico y conocido explotar en la máquina local (por ejemplo, CVE-AAAA-XXX), y fi nalmente un HTTP post dejando a la víctima. Este hilo se puede utilizar ahora para que coincida contra otros hilos de actividad que exhiben el mismo orden general de los acontecimientos y características.

Formalmente, los procesos adversario se definen como sub-gráficos de una rosca actividad que contienen un sub-conjunto de sus características. Es importante destacar que la sub-gráfico puede ser “elástico” en que puede ser definido de tal manera que los eventos no necesitan mantener su orden estricto a e ff caz coinciden con otro hilo (ilustrado en la Figura 7 como arcos de trazos entre los eventos). En otras palabras, sólo importa que las características se corresponden en el orden general, pero otros eventos pueden existir entre ellos. Alternativamente, un proceso adversario puede ser definido “estrictamente” de tal manera que los eventos deben mantener su orden sin eventos intermedios, o una combinación de los dos.

Soporte analítico 8.2 Hipótesis

Apoyando la generación de hipótesis, la documentación y las pruebas es una de las características más importantes de la rosca actividad y prevé la integración de modelos analíticos formales tales como “El análisis de competir hipótesis” (ACH) [1] y se aplica necesario científica







		Características del proceso
Reconocimiento		búsqueda en la web de "administrador de red" [derivada del producto de 2]
armamentización		
Entrega		Email con el accesorio de troyanizado entregado [derivada del producto de 3]
Explotación		Local específica explotar (por ejemplo, CVE-AAAA-XXX) [derivada del producto de 4]
Instalación		
C2		HTTP POST de la víctima [derivada del producto de 6]
Acción sobre los objetivos		

Figura 7: Un proceso de ejemplo adversario derivado de la rosca actividad se ilustra en la Figura 6. En este proceso, las características de los eventos 2, 3, 4, y 6 se extraen en un sub-proceso que se puede utilizar para que coincida contra otros hilos. Los arcos entre eventos son discontinuos ilustran que mientras que los eventos son todavía de fase ordenada por otros eventos pueden intervenir entre ellos sin interrumpir los criterios de coincidencia.

rigor. El primer paso del análisis es para definir la cuestión que debe abordarse. Una vez que la cuestión es de fi nidas hipótesis pueden ser generados, documentados y probados.

Como se describió anteriormente, mediante la colocación de eventos dentro de un modelo basado en la fase de lagunas de conocimiento **pueden ser más fácilmente identi fi . Desde el axioma 4 establece que la actividad maliciosa es de varias fases, cada fase *debería* contener al menos un evento.**¹⁸ **Un método alternativo de vacío de conocimiento identi fi cación es utilizar los recursos meta-característica (§ 4.5.6).** Entonces, el analista puede preguntar cómo el adversario es fi ul llenando los recursos necesarios para cada caso la generación de las hipótesis necesarias para abordar la cuestión.

Estas hipótesis pueden ser documentados en el hilo actividad y necesariamente di ff eren- ciada de otros eventos. Esta es una característica importante porque uno de los defectos de la mayoría de análisis es la falta de hipótesis documentadas y, además, y de manera más peligrosa, la falta de erentiation di ff entre la hipótesis y hecho. El modelo de actividad-hilo fomenta la generación de hipótesis y documentación aumentar el valor y la precisión de la El conocimiento.

Una vez que las hipótesis se documentan y di ff erentiated, deben ser re definido y probado. Hay varios métodos de prueba de hipótesis que pueden ser utilizados con nuestro modelo para determinar si una hipótesis dada, tanto en sí mismo y, entre otros, es razonable. Por ejemplo, se puede aplicar pruebas de ponderación a las hipótesis que compiten [1], navaja de Occam (por ejemplo, las explicaciones más simples son, en igualdad de condiciones, en general mejores que los complejos)¹⁹, conservadurismo (si la hipótesis 'fi ts' facilitada otros aspectos de la actividad), y otros métodos formales de razonamiento inductivo y deductivo a hipótesis en competencia [1].

Por ejemplo, Evento 10 en la Figura 6 podría enumerar los siguientes en los recursos meta-características: acceso a la red para enviar correo electrónico, el acceso a una cuenta de correo electrónico, la dirección de correo electrónico de destino, el malware troyano para incluir en el correo electrónico, y el conocimiento de su objetivo para crear un correo electrónico que va a pasar por alto filtros y atraer el objetivo de ejecutar el programa malicioso. Ni Evento 7 (acceso al proxy) o eventos (8 resultados) proporcionar los recursos necesarios para enviar un correo electrónico a la o fi cial de Recursos Jefe, en particular su dirección de correo electrónico y el papel (por ejemplo, el conocimiento de la diana). Por lo tanto, Evento 9 es la hipótesis de que la fuente de la información de orientación que permite el correo electrónico más atractivo para ser enviado con el objetivo correcto.

Evento 9 se puede probar en varias maneras. En primer lugar, es muy sencillo y lógico ya que todos sus recursos requeridos se cumplen necesitando No hay más eventos que se plantearon la hipótesis. En segundo lugar, es fi cios 'dentro de las capacidades y el acceso del adversario. En tercer lugar, la evidencia puede ser obtenida (por ejemplo, registros de eventos de host) para determinar si ocurrió hacer la hipótesis medible y comprobable para cumplir con el rigor científico fi co.

Esta forma de documentación se presta para finalmente lograr la repetibilidad en el proceso de análisis de intrusión como otros analistas pueden rastrear independientemente la actividad de gráfico de establecer

¹⁸ Un evento en cada fase no se garantiza como axioma 4 permite para las fases no esenciales.

¹⁹ En nuestro modelo, simple se puede medir fácilmente mediante la comparación de la cantidad de recursos requiere un evento y cuántos de esos son veri fi có dado los acontecimientos actuales frente a tener que formular la hipótesis más eventos que mantener.

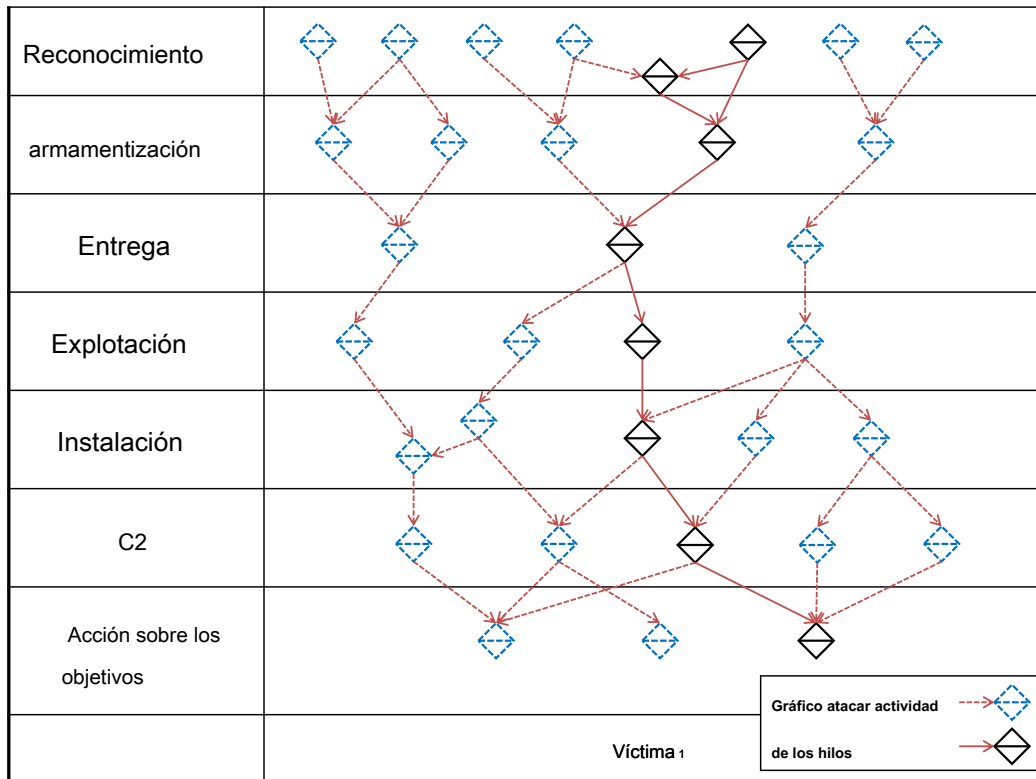


Figura 8: Un ejemplo Actividad-Attack gráfico que ilustra la integración de los conocimientos de las trayectorias reales de ataque adversario con la multitud de caminos de ataque hipotéticos que podrían adoptarse. El uso de un gráfico de actividad-ataque pone de relieve los posibles caminos de un adversario en el futuro, así como las rutas preferidas basadas en el conocimiento actual.

sus propias hipótesis y conclusiones comparándolos con el original. Este proceso se basa la confianza en las conclusiones analíticas y una mayor precisión en los juicios finales.

8.3 Actividad-Ataque Gráfico

Actividad-Ataque Gráfico hilos de actividad y gráficos de ataque tradicionales no son mutuamente excluyentes, sino que responden a las preguntas complementarias. gráficos de ataque identificar y enumerar caminos un adversario *podría* tomar mientras que la actividad roscas de fi ne los caminos un adversario *tiene*

tomado. Estos pueden existir juntos mediante la superposición de los hilos de actividad en la parte superior de un gráfico de ataque tradicional. Nos referimos a este gráfico ataque inteligencia informada como una *gráfico de actividad-ataque*.

El gráfico de la actividad de ataque proporciona varios beneficios:

- Se mantiene la integridad de la gráfica ataque puesta a disposición el alcance completo de análisis gráfico de ataque.
- Se aumenta la cantidad de información contenida en un gráfico de ataque, ya que cada vértice es un evento Diamond rica en características.
- Se aumenta la cantidad de información visual contenida en el gráfico de ataque con poco- a-ninguna reducción en la facilidad de uso.
- Genera pesos más precisos como se conocen opciones atacante reales (y preferencias).
- **Se destaca atacante *preferencias* junto a caminos alternativos.**
- De manera exhaustiva (debido a la naturaleza de los gráficos de ataque) los mapas de caminos alternativos para los escenarios de juego y el desarrollo de campañas de mitigación (por ejemplo, si se toma esta acción, el adversario es probable que tome uno de estos caminos...).
- Como es natural, ayuda a las lagunas de conocimiento fi ll para cualquier hilo un ataque mediante la superposición de la corpus de hilos de ataque horizontalmente relacionados para la comparación. El resultado es más cura CA y la generación de hipótesis más rápido y pruebas durante las investigaciones de respuesta a incidentes en curso.

Figura 8.3 es un ejemplo de un gráfico de actividad-ataque. La figura distingue los caminos conocidos adversario (gráfico de actividad) de los posibles caminos todavía conocidas para ser explotado (gráfico tachuela franco). Esto es muy parecido a consultar tanto pruebas de penetración (por ejemplo, equipo rojo) y la evaluación de la vulnerabilidad (por ejemplo, el equipo azul) resulta al mismo tiempo para trazar el mejor curso de acción.²⁰

En última instancia, los hilos de actividad y gráficos de la actividad de ataque permiten una mejor estrategia de mitigación sarrollo de- medida **que se integran tanto en seguridad de la información y la inteligencia de amenazas de manera cohesiva. Integran lo *tiene* con lo ocurrido *podría*** permitiendo que se produzca una estrategia tanto a contrarrestar la amenaza actual y plan para la reacción E ff adversario caz en la lucha contra futuros movimientos del adversario. Esta planificación integrada también conduce a una mayor e fi ciente utilización de recursos como acciones gación mitiga pueden ser diseñados para contrarrestar la amenaza actual, así como la amenaza futura al mismo tiempo.

9 grupos de actividades

actividad del Grupo Un *grupo de actividad* es un conjunto de eventos de diamante y los hilos de actividad aso- ciados por similitudes en sus características o procesos y ponderado por la confianza. Una actividad

²⁰ Si el enfoque gráfico de actividad-ataque sería un método útil para la integración de los resultados reales del equipo rojo y azul para el análisis no se aprovecha, pero una pregunta interesante e izquierda para el trabajo futuro.

grupo tiene dos propósitos: (1) un marco para responder a las preguntas analíticas que requieren una amplitud de conocimientos actividad, y (2) el desarrollo de estrategias de mitigación con una intención e ffect más amplio que los hilos de actividad. grupos de actividad son di ff erentiated a partir de hilos de actividad de dos maneras: (1) grupos de actividad contienen ambos eventos y los hilos, y (2) eventos y los hilos en un grupo de actividades se correlacionan por las características y comportamientos similares en lugar de causalmente relacionada (como es el caso de hilos de actividad).

Los analistas que tradicionalmente forman grupos de actividad para identificar a un adversario común detrás de los acontecimientos y las discusiones por lo general utilizando similitudes en infraestructura y capacidades. Sin embargo, el concepto es inherentemente flexible y se extiende para incluir cualquier agrupación sobre la base de similitudes para hacer frente a una multitud de necesidades analíticas y operacionales. La analítica deseada o el resultado operativo determina la aplicación y el tipo de correlación (es decir, la función de agrupamiento) que se utiliza. Thermore Fur-, grupos de actividades no son estáticos - al igual que los adversarios no son estáticas. grupos de actividades deben crecer y cambiar con el tiempo para absorber nuevos conocimientos del adversario, incluidos los cambios en sus necesidades y operaciones. ²¹

Existen seis distintos pasos para los grupos de actividad que rodean proceso:

Paso 1: Problema Analytic El problema analítico particular a ser resuelto a través de agrupación

Paso 2: Selección de características Los procesos de características de eventos y adversario utilizados para formar la base de clasi fi y la agrupación se seleccionan

Paso 3: Creación grupos de actividad se crean a partir del conjunto de eventos e hilos

Paso 4: Crecimiento A medida que nuevos eventos flujo en el modelo, que son clasificarse en los grupos de actividades

Paso 5: Análisis grupos de actividad se analizan para abordar el problema (s) de análisis de fi nido

Paso 6: redefinición Grupos de actividad tienen que ser rede fi nida de vez en cuando para mantener su precisión

Formalmente, definimos un grupo de actividades, AG como un conjunto de eventos y los hilos de actividad que comparten uno o más similitudes en las características o procesos adversario:

²¹ Mientras que la agrupación y clasi fi cación son herramientas poderosas que debe fomentarse como un multiplicador de fuerza analítica, que no dejan de tener sus trampas. esquemas de agrupamiento y clasi fi cación tienen muchas preocupaciones bien documentados. Algunos son de especial preocupación porque los adversarios practican activamente la negación y el engaño en casi todos los paquetes para evadir la detección y análisis. El área de mayor preocupación es llamado sobre fi tting, donde un analista o máquina incluye información no relacionada en los racimos. La razón principal de este error es pobre grupo de fi nición (es decir, débil vector de características). Particularmente en el caso del análisis de intrusos, que se manifiesta en dos actividades se superponen características (por ejemplo, compartiendo una capacidad pública, utilizando el espacio de alojamiento compartido). Esto se complica aún más por la propagación de errores: una vez que un evento no relacionado se incluye en el grupo de fi nición entonces se utiliza para el futuro correlación aumentar el número de eventos no relacionados Para agravar el error inicial. Existen varias técnicas para detectar y evitar el exceso de fi tting [54]. Una comparación de estas técnicas como se aplica a análisis de intrusión está más allá del alcance de este trabajo y se deja para el trabajo futuro. Sin embargo, es un problema digno de mención.

$$AG = \{et_1, et_2, \dots, et_{norte}\}$$

Dónde:

- $norte \geq 1$, debe haber al menos un elemento en un grupo de actividad
- et_{norte} es o bien: Un evento singular o un hilo de actividad tal como se define en § 8
- Todos los eventos o procesos AG compartir uno o más similitudes que satisfacen la función de creación de grupo de actividad se utiliza para dividir los eventos y los hilos (definido en § 9.3)

9.1 Paso 1: Problema Analytic

agrupación actividad se utiliza para resolver una serie de problemas. Estos problemas generalmente requieren deducción y la inferencia basado en un conjunto común de características (es decir, vector de características). Estos problemas son por lo general bastante distinta a requerir un vector de características Erent di ff para cada proble- Lem. 22 Por ejemplo, el vector de características, que serían eventos de grupo y los temas probable adversario (por ejemplo, la atribución) serían no siempre su fi cina para eventos de grupo para descubrir el malware autores / desarrolladores comunes. El problema analítico primero debe ser de fi nido.

Por lo tanto, definimos un problema analítico, PR , como una declaración análisis intrusión problema que requiere agrupamiento y clasificación fi cación (es decir, la agrupación) para abordar en parte o completo.

Algunos ejemplos de problemas analíticos que soportan grupos de actividad:

- Tendencias: ¿Cómo ha cambiado la actividad de un adversario con el tiempo y lo que es el vector de corriente para inferir cambios en el futuro?
- Deducción Intención: ¿Cuál es la intención del adversario?
- Reconocimiento Deducción: ¿Qué acontecimientos y las roscas probabilidades son realizadas por el mismo adversario?
- Capacidades adversario e Infraestructura: ¿Cuál es el conjunto completo de capacida- des observadas y la infraestructura del adversario?
- Cruz-Capacidad La identificación: las capacidades que han sido utilizados por múltiples adversarios?
- Campaña adversario brecha de conocimiento La identificación: ¿Cuáles son las lagunas de conocimiento de la organización a través de la campaña de un adversario?

²² Sin embargo, esto no descarta la posibilidad de que dos o más problemas comparten un vector de características comunes.

- Automatizado Recomendación Mitigación: Cuando se detecta un evento que es adversario detrás del evento y qué acciones pueden / deben tomar? ²³
- Deducción capacidad común de desarrollo: ¿Qué capacidades de mostrar evidencia de los autores / desarrolladores comunes?
- Centro de Gravedad La identificación: ¿Qué recursos y los procesos son los más comunes y fundamentales para una actividad y / o campaña?

9.2 Paso 2: Selección de características

eventos de diamante y los hilos están correlacionados y se agrupan en dos formas complementarias: (1) utilizando diversos **núcleo-evento, meta-, y sub-características (por ejemplo, la infraestructura, la capacidad), y (2) los procesos adversario (§ 8) previamente** definido como grupo de actividad sub-gráficos. Para lograr esto, las características se seleccionan poblar un vector de características de finir los elementos utilizados para eventos de grupo y los hilos.

Es importante destacar que, vectores de características pueden ser tremendamente específico que permite un analista para definir una actividad particular de interés mediante la inclusión de los observables particulares (por ejemplo, direcciones IP, dominios, malware) de tal manera que se forman dos grupos: los eventos y los hilos que forman parte de la actividad, y las que no lo son.

Además, los procesos incluidos en un vector de características son un concepto poderoso para apoyar la actividad de pelado com- no sólo por observable sino también por específico significa irregardless de la infraestructura finco o capacidad. Esto es especialmente eficaz contra adversarios que pueden cambiar la infraestructura y capacidad de los observables (más comunes), pero a menudo mantener un proceso estático semi.

los *espacio de características* se compone de todas las características-meta Core- y de los eventos (por ejemplo, infra- estructura, capacidad, víctima, resultado) (§ 4), así como cualquier proceso de fin adversario NED (§ 8). Desde el espacio de características las **características más relevantes y óptimas son seleccionadas y / o creados** ²⁴ de finir la *vector de características*. Por último, cada una de estas características se pueden combinar con un peso identificación de su importancia relativa en la de finición del grupo. Existen varias técnicas bien conocidas para seleccionar (y posiblemente crear) las características más pertinentes y óptimas [55]. Además discusión de óptima diamante modelo de selección de características / creación de la actividad de grupo se deja como un área para la investigación futura y también estará implementación específica.

²³ **grupos de actividades soporte en tiempo real defensa de la red de inteligencia impulsada.** Como se detectan eventos en tiempo real, las técnicas de clasificación finción de aprendizaje automático se clasificación y eventos que asocian conocidos grupos de actividad aplican. Dado un conjunto de condiciones preestablecidas (por ejemplo, si el evento E es clasificada como grupo de actividad X con > 80% confianza) el sistema puede hacer una recomendación a la red mecanismos de defensa para aplicar las técnicas de reducción a la actividad. De esta manera, las operaciones adversario pueden ser mitigados en tiempo real, incluso si el adversario ha cambiado parte de sus operaciones sin necesidad de defensores para pronosticar el cambio.

²⁴ **creación de la operación (la creación de nuevas características a partir de las características existentes)** se nota porque a menudo los analistas utilizan una función para comparar las características basadas en la actividad de intrusos. Por ejemplo, la dirección IP de un nombre de dominio resuelto puede ser una característica extraída si el IP no existía en la lista de características originales permitiendo ahora eventos que hacen referencia al mismo dominio o sus asociados IP a estar correlacionados.

Tabla 3: Ejemplo Actividad Grupo definición Pasos 1 y 2

Problema analítica	¿Qué eventos e hilos es probable que sean con-
	canalizado por el mismo adversario que utiliza un determinado
	proceso (<i>Proceso</i> ₁)? (por ejemplo, la atribución)
espacio de funciones	<i>Infraestructura</i> _{IP} , <i>Infraestructura</i> _{Dominio} , <i>Capacidad</i> _{Maryland} ₅ , <i>Victim</i> _{IP} , <i>Victim</i> _{Organización} , <i>Metodología</i> , <i>Proceso</i> ₁ , <i>Proceso</i> ₂ , <i>Proceso</i> ₃
vector de características	< <i>Infraestructura</i>_{IP}, <i>Capacidad</i>_{Maryland}₅, <i>Proceso</i>₁ >
Salir	Todos los eventos y las discusiones se agruparán por ilarities sim- en la infraestructura IP, capacidad de hash MD5, y un proceso adverarsy definida de <i>Proceso</i> ₁

Definimos el espacio de características, *FS*, como el conjunto de todos núcleo-, meta-, y sub-características que de eventos fi ne, así como los procesos de cualquiera y todas las adversario.

Además, definimos el vector de características a frente a un problema analítico, *FV_{PR}*, como

$$FV_{PR} = \langle \langle F_1, w_{F_1} \rangle, \langle F_2, w_{F_2} \rangle, \dots, \langle F_{norte}, w_{F_{norte}} \rangle \rangle$$

Dónde:

- *norte* ≥ 1 , debe haber al menos un elemento en el vector de características
- *F_{norte}* $\in FS$, cada característica en el vector de características debe existir en el espacio de características
- *FV* $\subset FS$, el vector de características es un sub-conjunto de la función de espacio
- *F_{norte}* es un elemento necesario para eventos de grupo y los hilos para abordar el problema analítico
PR
- *w_{F_{norte}}* $\in \mathbb{R}$ y $0 < w_{F_{norte}} \leq 1$, el peso es un número real que describe la importancia relativa de *F_{norte}* a todos los demás *F_i*, de tal manera que *w* = 1 es una característica de mayor importancia ²⁵

²⁵ No debería haber ninguna función con un peso dado de cero en el vector de características, ya que ello indicar que la propiedad no tenía importancia. En ese caso, la función no debe incluirse en el vector de características.

9.3 Paso 3: Creación

Los analistas crean inicialmente grupos de actividad a través de un proceso de agrupamiento cognitivo: un analista compara las características de un evento con cada otra (por ejemplo, su vector de características) y usando alguna función de similitud separa los eventos en grupos distintos (es decir, conjuntos) con una confianza con la asociada de los cuales grupo pertenece el evento.

Formalmente, estos grupos se convierten

clases en la que las técnicas de aprendizaje de máquina se pueden aplicar, como clasificación en el crecimiento del grupo de actividades (§ 9.4).

Se espera que una organización tendrá más de un problema analítico definida (vía Paso 1). Por lo tanto, es posible que haya más de una actividad de la función de creación de grupos por ejemplo Diamond Modelo. Por ejemplo, la agrupación eventos por aparente mismo actor-adversario (es decir, agrupar para atribución) y agrupar eventos por la vulnerabilidad víctima (por ejemplo, la agrupación para la ruta de la explotación lo más probable) son diferentes problemas analíticos que requieren funciones distintas. Además, algunos problemas pueden requerir la función de agrupación para colocar cada evento y el hilo en un grupo donde otros pueden permitir valores atípicos (es decir, eventos y roscas que no pertenecen a ningún grupo).

creación de grupo Actividad es un problema general clustering solución de evento y el hilo correlación abordar un problema análisis particular. La función de la agrupación depende de la información anterior, tal como el problema / objetivo analítico y el vector de característica particular que puede ser único para cualquier aplicación dada del modelo de Diamond. Por lo tanto, lo más probable es que no hay una función de creación de grupo de una actividad a resolver todos los problemas de análisis de intrusión. Esperamos que la investigación adicional de definir las funciones de optimización de la agrupación en relación a problemas de análisis de intrusiones, tales como la agrupación de eventos optimizado para la atribución adversario.

Formalmente, definimos una función de creación de grupo de actividad, *AGC* como:

$$AGC(PR, FV_{PR}, ET) \rightarrow AGS$$

$$AGS = \{AG_1, AG_2, \dots, AG_{norte}\}$$

Dónde:

- *PR* es una de finido problema analítico a ser satisfecho por la función de
- *FV_{PR}* es el vector de características, que satisface el problema analítico *PR*
- *ET* es el conjunto de todos los eventos y los hilos que se agrupan
- *AGC* particiones todos los elementos del conjunto de eventos / hilo *ET* en un conjunto de *norte* Grupos de actividad, *AGS*, basado en el vector de características *FV_{PR}*

- La función que comprende *AGC* puede operar a través de todos los elementos dentro del conjunto *ET* utilizando las características y los procesos se define en el *FVPR*²⁶
- *AGS* es el conjunto de grupos de actividad de tal manera que cada grupo de actividad, *AGnorte*, satisface la definición de un grupo de actividades
- Es posible que la función de creación establece ningún grupo porque no existen similitudes, y por lo tanto *norte* ≥ 0

9.3.1 Actividad de grupo Creación Ejemplo

La Figura 9 ilustra cómo una función de creación de grupo de actividad (*AGC*), usando estricta partición con valores atípicos, puede ser definido para responder al problema planteado ejemplo en la sección de características anterior vectorial (§ 9.2) de fi grupos Ning basados en un adversario común propensos a utilizar la misma infraestructura IP, la capacidad, y un proceso de 3 pasos. La ilustración muestra un conjunto nominal de 17 eventos y los hilos (*ES*) que se agrupan de acuerdo a nuestra función y vector de características para crear tres grupos y dos eventos errantes y un hilo errante que no cumplían los criterios de la función y se dejan un-agrupados. Nuestra función agrupan dos hilos en la actividad del Grupo 3.

Para nuestro ejemplo, vamos a decir que la lógica expresada en la función establece que cualquier hilo que contenía el proceso *UNA* → *segundo* → *do* sería un grupo de actividades. Dos o más hilos que coinciden proceso- serían correlacionadas dentro del mismo grupo de actividad si al menos un evento dentro de cada hilo de rosca (no necesariamente dentro del proceso ed especificidad) compartió una IP infraestructura y la capacidad de hash MD5 con al menos medio confianza. Ahora que los datos se organiza para responder a la pregunta analítica, los grupos pueden ser cultivadas (§ 9.4) y se analizaron (§ 9.5) para proporcionar una visión potencialmente responder a la pregunta.

9.4 Paso 4: Crecimiento

Los analistas crecen continuamente grupos de actividad a través de un proceso de reconocimiento de patrón cognitivo imitando confianza ponderado probabilística clasi fi: un analista descubre un evento malicioso, compara el evento a todos los otros eventos conocidos basados en similitudes de características y su confianza con fi, y asociados (es decir, clasificación fi es) el evento con el grupo más similar (es decir, clase) (o, alternativamente, se abstiene de asociación si la confianza con fi no cumple su umbral). Esta acción crece continuamente los grupos de actividad como los eventos y los hilos se caracterizan en los grupos medida que se descubren, detectada o recibida.

La Figura 10 ilustra el crecimiento grupo de actividad: como eventos y los hilos son descubiertos, detectados o recibidos son clasificarse en los diversos grupos de actividad basado en la característica definida de

²⁶ Las operaciones en una función de creación de grupo de actividad son tan amplias como sea necesario y no están obligados a utilizar todos los elementos del vector de características.

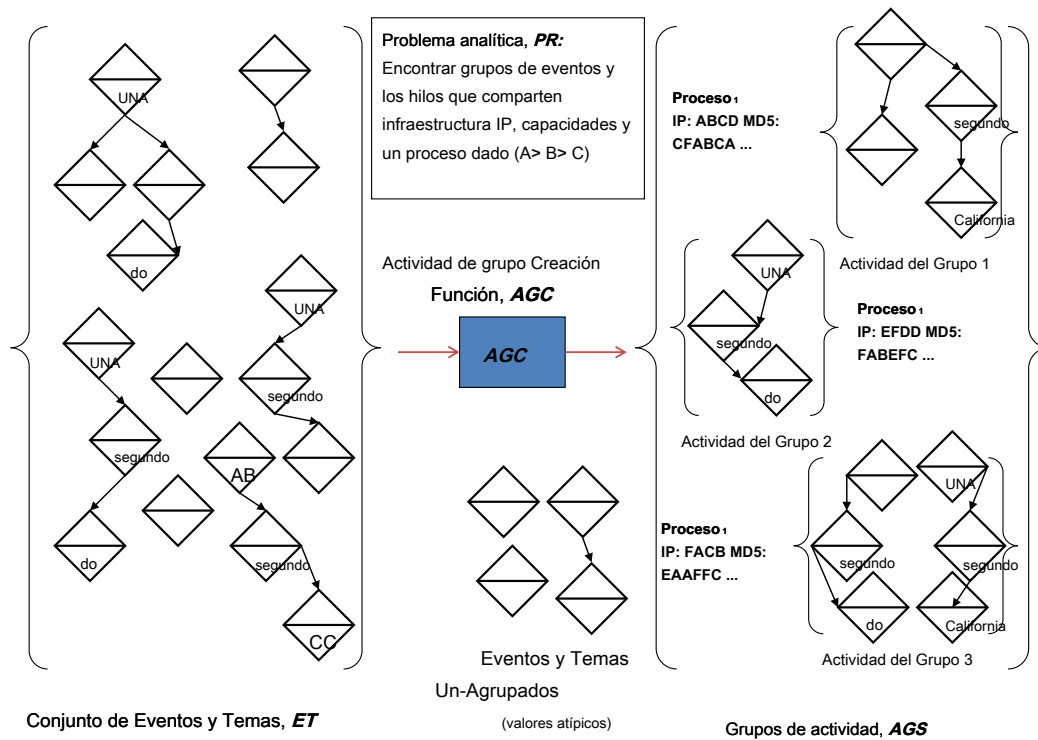


Figura 9: la creación del grupo actividad se ilustra de tal manera que un grupo de eventos y los hilos están agrupados basa en un vector de características definida por: un proceso adversario (*UNA* → *segundo* → *DO*), una capacidad de adaptación de hash MD5, y la dirección IP de la infraestructura. Sobre la base de este vector de características y una función de creación de grupo de actividad (*AGC*) los 17 eventos y los hilos están agrupados en tres grupos con dos eventos y un hilo que no cumplan los criterios de agrupación y se clasifican como valores atípicos.

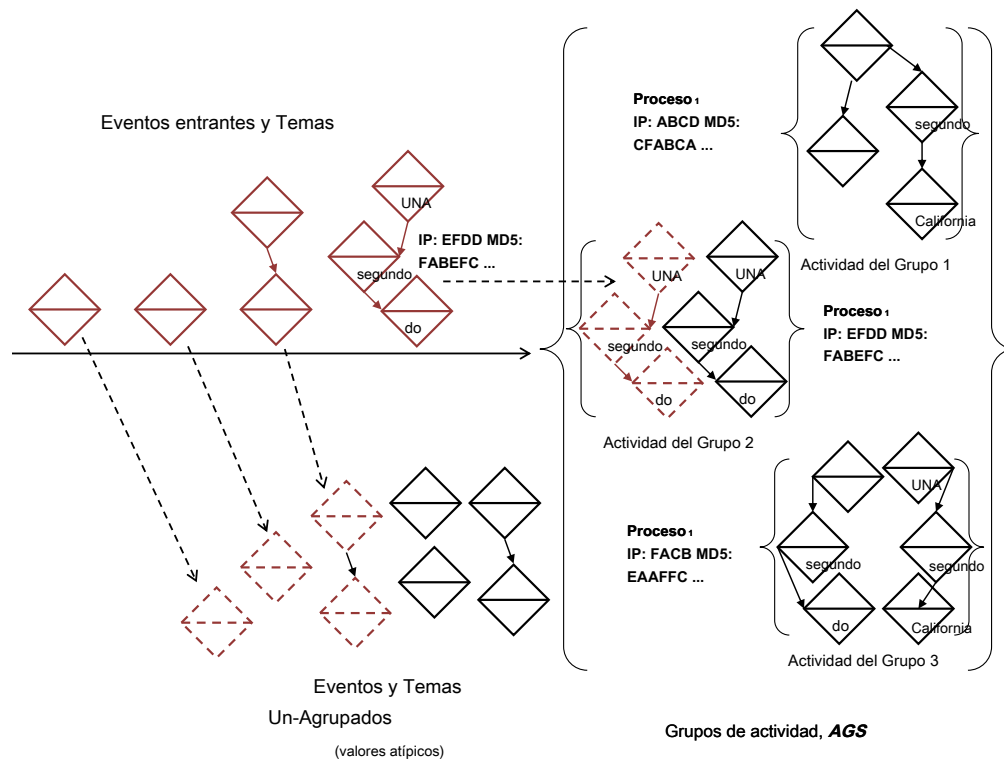


Figura 10: Ilustración Paso 4, Crecimiento Actividad de grupo, eventos y los hilos se descubren, detecta, o se recibe y continuamente clasificados en grupos de actividad existentes basados en la NED vector previamente de función. En este caso, esos eventos y los hilos no emparejan con éxito los criterios son valores atípicos y no agrupados.

vector. En este ejemplo, la reunión de hilo los criterios se clasificad en Actividad Grupo 2 mientras que el otro hilo y eventos son clasificados como valores atípicos.²⁷

9.5 Paso 5: Análisis

Una vez que un grupo de actividad es definido y los eventos y los hilos están agrupados dentro de los grupos que se pueden analizar para abordar el problema específico analítico que se trate. Esto generalmente requiere la aplicación de herramientas y Tradecraft más allá del Modelo Diamante. Por ejemplo, con nuestro ejemplo en la Figura 9 el analista ahora probable examinar cada uno de estos grupos de discernir diferencias y similitudes que exponen nuevos problemas analíticos para ser resueltos. Esto puede incluso conducir a un nuevo examen de la selección de características y la función de agrupación que requiere iniciación (el paso siguiente).

Sin embargo, el analista tiene ahora las herramientas para analizar eventos de intrusión e hilos a través de una escala más grande que incluye: exponiendo potencialmente campañas adversario de largo alcance, la identificación de similitudes entre eventos aparentemente disímiles, reuniendo una lista completa de las capacidades del adversario observados y la infraestructura, el adversario deducir atribución basado en el conjunto víctima (es decir, cyber-victimología § 5.1.2), y muchos otros problemas.

9.6 Paso 6: redefinición

grupos de actividad, como todas las funciones basadas en cationes de agrupamiento y clasificación, fiero desde varios desafíos bien estudiados. Uno de ellos es el supuesto de que el analista puede adecuado describir el vector de características y la función utilizada para clúster - o que su idea de un cluster es correcto para empezar. Otro es sobre racor y la propagación de errores: cuando un analista o un sistema asocia erróneamente un evento a un grupo de propagación y potencialmente magnificar ese error con el tiempo. Por lo tanto, es normal que los grupos de actividades requieren el examen, detección de anomalías, y la redefinición (re-agrupamiento) en el tiempo para descubrir y corregir errores. Además, durante esta redefinición cambios etapa puede (y debe) ser considerados para el vector de características y los pesos y algoritmos asociados para asegurar el error subyacente está corregida. A mano,

9.7 Las familias del grupo de actividades

grupos de actividades son tan variadas como las empresas detrás de la actividad maliciosa. Como tal, la identificación y detección de millones de eventos podría fácilmente de filtro en un gran número de

²⁷ Sin embargo, como se describió anteriormente en el Paso 3, Actividad Grupo Creación (§ 9.3), la función de agrupación es

definido por las necesidades de la analista y el problema analítico particular que se está resuelto y por lo tanto tipos de agrupación alternativa son posibles que pueden no utilizar los valores atípicos pero en su lugar colocar cada hilo y el evento en un grupo.

grupos de actividades, algunas de las cuales interactúan en un nivel superior. Por lo tanto, es necesario veces para desarrollar una jerarquía de grupos de cuál es el modelo de las cada vez más complejas organizaciones detrás de los acontecimientos a fin de abordar cuestiones de orden superior y desarrollar aún más la mitigación estratégica.²⁸

Muy parecido a un grupo de actividades, una familia del grupo de actividades es un conjunto de grupos de actividades que comparten características comunes, excepto que las características comunes de los grupos dentro de una familia probablemente no técnico. Por ejemplo, en el caso del crimen organizado, una financiación común y elemento de tareas pueden ser responsables de múltiples operaciones y, por tanto, varios grupos de actividad

- cada uno de los cuales se realiza un seguimiento y se analizaron por separado - se agrupan dentro de una familia. Esto hace que el cación identi fi, la organización y el desarrollo de estrategias de mitigación de elementos de orden superior, tales como el crimen-jefe en este ejemplo, manejable y más e ff reflexivo.

A efectos de la metodología analítica, las familias del grupo actividad se tratan al mismo proceso de 6 pasos como un grupo de actividades. Deben ser de fi nido, creado, crecido, analizado y redefinido. También tienen vectores de características y funciones de creación, excepto que la función de creación utilizado para el agrupamiento y clasificación opera a través de las características de un grupo entero en lugar de eventos o de hilos separados. Estos términos y las funciones asociadas, características y procesos no necesitan ser re-define como que se han discutido previamente en su totalidad

- excepto para decir que se modi fi cado ligeramente para apoyar características y procesos a través de grupos de actividad.

Formalmente, definimos un grupo familiar actividad como:

$$AGF = \{AG_1, AG_2, \dots, AG_{norte}\}$$

Dónde:

- *norte* ≥ 1 , una familia del grupo de actividades debe contener al menos un grupo de actividad
- *AG_{norte}* satisface la definición de un grupo de actividades
- *AGF* es un conjunto de grupos de actividad que comparten uno o más similitudes
- *AGF* satisface un problema analítico particular,
- *AGF* es el resultado de una función de creación y vector de características que comparan grupos de actividad

²⁸ La prueba de tal organización detrás de la actividad maliciosa es evidente en el caso "Phonemasters" [45] y Brenner argumenta persuasivamente en [56] que los modelos existentes de criminalidad jerárquico organizadas se siguen necesariamente en el ciberespacio, ya que son el método ciento e fi mayor parte de diversas empresas criminales - y ciberespacio será una extensión natural de las actividades delictivas, especialmente los más grandes. Sin embargo, nuestro modelo no se limita a los delitos informáticos, pero extensible a cualquier empresa organizada de la realización de una multitud de actividades cibernéticos maliciosos que son necesarias para el grupo.

10 Planificación y Gaming

Desde una perspectiva de la mitigación, muchas acciones son posibles. Sin embargo, decidir la mejor acción a tomar para establecer o FF adversario es un reto. Acciones cuestan los defensores de dinero y / o el tiempo para poner en práctica y se toman con la expectativa de que la acción impactará adversamente contradictorio e ff Orts.

Nuestro modelo proporciona una comprensión de las dependencias entre los componentes del adversario. Para adversario e ff Orts tengan éxito, roscas completas deben estar disponibles creando un camino BE- interpolar la intención y el resultado. Las ayudas modelo para comprender cómo las acciones del defensor tendrán un impacto en las capacidades del adversario mediante la determinación de los componentes que necesitará un adversario para reemplazar / fi x / re-implementar.

Además, las acciones deben ser elegidos defensor de que los defensores de costes pequeños pero cuestan mucho más adversarios. Claramente, el inverso (es decir, costando el defensor más y el adversario menos) no es deseable desde una perspectiva de la mitigación táctica o estratégica. Acciones que cuestan el defensor más (especialmente significativamente más) deben evitarse si es posible. El costo para el adversario puede ser expresado como el coste (en dinero, recursos, tiempo) para recuperar la capacidad y la infraestructura necesaria para tener una plataforma funcional. costo adversario tiene varios componentes, incluyendo el tiempo de desarrollo, el costo de construcción de infraestructura / hora, retrain- tiempo y costes ing, costo de oportunidad, y los costos incurridos por la pérdida de la disposición. Defender los costos también tienen varios componentes, tales como dinero, tiempo, así como los riesgos legales y éticos que necesitan ser tratados [13].

El modelo Diamond es un concepto fundamental que ayuda a estructurar y fortalecer el análisis para lograr su objetivo final: la mitigación. El Modelo no prescribe estrategia de mitigación o curso de desarrollo de la acción. Estos existen separado del modelo. En lugar de ello, es compatible con muchas formas de toma de decisiones. Las siguientes son las discusiones sobre la aplicabilidad del modelo a los aspectos de varios marcos de toma populares:

Inteligencia preparación conjunta del ambiente operacional (JIOPE) Departamento de Defensa doctrina planificación militar
Conjunto de Inteligencia Preparación del Medio Ambiente erational Op (JIOPE) [12] Estados Unidos es un recurso bien entendida y, a menudo citado que establece un proceso para el uso de la inteligencia para desarrollar cursos de acción. La doctrina reconoce que una estrategia fracasará si se basa únicamente en la fi cación de Nulli adversario tructure y capacidades tura. Más bien, se prescribe un enfoque combinado que también incluye la identificación de los recursos adversario, centros de gravedad, así como las respuestas del adversario y cursos de acción. Este enfoque identi fi ca las zonas óptimas para la mitigación y contrarresta la capacidad del adversario para mantener y reconstruir las capacidades y la infraestructura una vez mitigados. Nuestro modelo es compatible con este tipo de planificación, ya que:

- Ayuda en la identificación de inteligencia y de información a través de las brechas faltante características de eventos y de fase lagunas en hilos de actividad (JIOPE Paso 1, Elemento 6)

- Apoya el desarrollo de un modelo de adversario (JIOPE Paso 3, Elemento 1)
- infraestructura adversario identifica las capacidades y con un enfoque en los recursos (JIOPE Paso 3, elemento 3)
- centros adversario identifica las de la gravedad a través de hilo actividad y grupo de actividad análisis (JIOPE Paso 3, Elemento 4)
- identificaciones objetivos es adversario y estado final a través de análisis de actividad de los hilos, mología victi-, y grupos de actividad (JIOPE Paso 4, elemento 1)
- Determina cursos adversario probables de acción a través de gráfico de actividad-ataque análisis donde los caminos posibles y preferidos de ataque se pueden identificar (JIOPE Paso 4, los elementos 2 y 3)

Matar Análisis de la Cadena El análisis de la cadena Modelo Diamante y muertes son altamente comple- mentaria. Matar análisis de la cadena permite que un analista de "apuntar y comprometer a un adversario para crear ECTS e ff deseados." [11] El diamante permite a los analistas para desarrollar Tradecraft y comprensión con el fin de construir y organizar los conocimientos necesarios para realizar el análisis de la cadena de muertes. Se describen dos métodos de integración de los dos enfoques:

- Una vez que un analista desarrolla una rosca actividad, cursos de acción para cada evento a lo largo de la rosca pueden ser ed fi identi usando el curso de la cadena de destrucción de la matriz de acción. Como se ilustra en la Figura 11, cursos de acción para cada una de las etapas de la cadena Kill se identifican por hilos de actividad 1 y 2 de la Figura 6. La potencia del modelo Diamond es que cursos de acción pueden ser diseñados para abarcar múltiples víctimas y a través de la actividad de un adversario haciendo las acciones aún más potente, ya que reducen aún más la capacidad del adversario.
- grupos de actividades agrupadas por adversario misma probabilidad (es decir, la agrupación por atribución) con el análisis de la mayor característica común situado entre los eventos en un grupo puede proporcionar indicadores clave de la campaña requeridas de la cadena de muertes necesarias para enfocar y priorizar las líneas de acción.

cubierta de la vulnerabilidad La práctica común aseguramiento de la información es analizar un sistema (o red) para las vulnerabilidades, la clasificación de esas vulnerabilidades basado en las preocupaciones fi específicos de la organización (por ejemplo, valor de activo y coste), seguido por la aplicación de la mitigación a esas vulnerabilidades. A través de la generación de los gráficos de la actividad de ataque, este proceso normal de decidir qué caminos de la gráfica para podar por la mitigación (negando **así el uso de la ruta por el adversario) está ahora informado por *preferencia adversario y potencial*. A través del uso de nuestro** modelo, las decisiones tradicionales de aseguramiento de la información ya no son hechas por la hipótesis de adversarios potenciales y sus caminos, sino más bien mediante la inyección de caminos ataque real en el gráfico, así como la proyección de preferencia adversario y potencial. Este enfoque proporciona una protección más completa y aumenta el costo adversario, ya que ahora tienen que desarrollar, entrenar y

	Detectar	Negar	Interrumpir	Degradar	Engañar	Destruir
Reconocimiento	analista de la red	Política para Prevenir Foro de Uso			Crear registros falsos	
armamentización						
Entrega	NIDS, formación de usuarios	Correo electrónico de barrido AV		Hacer cola de correo electrónico	Filtro, pero responderá con el mensaje de fuera de la oficina	
Explotación	HIDS	Parche	DEP			
Instalación						
C2	NIDS	HTTP lista blanca	PELLIZCOS	estrangulamiento HTTP		
Acción sobre los objetivos	Apoderado Detección Firewall ACL		PELLIZCOS	estrangulamiento HTTP	Tarro de miel	

Figura 11: Kill Chain Curso de Acción Matrix deriva de hilos 1 y 2 en la figura 6. Las medidas de mitigación para cada categoría (por ejemplo, interrumpir, degradar, negar) Se identificaron para contrarrestar la cacia e ff de eventos del adversario a lo largo de las fases. Este formato y el proceso de matriz se describen en [11] como un método de identificación de cursos de mitigación de acción para contrarrestar campañas Sary adver- - que ilustra el poder de combinar el modelo de Diamond y Matar análisis de la cadena.

operar más allá de su base de capacidad de corriente.

Juego de azar Parte de cualquier estrategia de mitigación desarrollo reflexivo e ff es engañar al adversario con el fin de predecir su próximo movimiento. De esta manera un defensor puede tanto contrarrestar la actividad actual y pre-posición para la actividad futura contrarrestar de este modo el adversario. La planificación de las dos al mismo tiempo permite que las decisiones económicas que satisfagan ambos requisitos. Nuestro modelo es compatible con los juegos en varias formas para predecir con mayor precisión las respuestas del adversario a presiones ambientales (por ejemplo, acciones, defensor de vulnerabilidad parcheada):

- Permite a los juegos de orden superior en torno a la toma de decisiones humana como los meta-características socio-políticas y la intención son un aspecto integrado (por ejemplo, ¿cuáles son las necesidades y aspiraciones del adversario? ¿Cómo pueden aquellos haber influido o contrarrestado?).
- **A través de hilos y grupos de actividad, la deducción atribución es posible a través de la victimología cibernética (§ 5.1.2)** y otros medios.
- El soporte fundamental de la prueba de hipótesis permite un juego más completa escena- rio mejorar el valor del juego y la precisión de sus resultados.

11 Trabajo Futuro

Reconocemos que el modelo del diamante en la actualidad es altamente cognitiva y manual. Estamos dispuestos a aceptar esto porque es, como su nombre lo indica, un modelo a ser estudiado y re fi ne definida con respecto sólo para capturar con precisión el proceso de análisis de intrusión. Sin embargo, en última instancia, somos pragmáticos y reconocer que el modelo será mucho más útil una vez que se desarrollan deficiencias automatización y e fi. Como tal, esperamos haber proporcionado información sobre su ciente FFI y citas de correos relacionados ff Orts para motivar a los futuros trabajos en esta línea.

Uno de estos automatización de gran valor sería la integración del modelo de diamante en herramientas ana- líticas que son ambos alimentados de forma automática con la inteligencia de los sensores de la red, así como los informes externos de otras organizaciones, **especialmente aquellas dentro de un espacio amenaza compartida (§ 5.1.3).** Sin embargo, esperamos que todavía serán necesarios los analistas de intrusión a la entrada de nuevos datos de inteligencia y supervisan los alimentos automatizados. Para ello será necesario el trabajo en la facilidad de uso para aumentar, en lugar de impedir, la analítica de obra flujo. Por otra parte, esto también podría provocar automático acoplado y la generación de hipótesis formal y las pruebas que proporciona la evaluación inmediata de las conclusiones analíticas.

Para lograr esto, debe haber un protocolo para compartir indicadores contextuales y la inteligencia de amenazas para integrar rápidamente la información de todas estas fuentes. Vemos el modelo Diamond como base para la consecución de este y la mejora de nuevo o protocolos y lenguajes formales existentes (como [30, 27, 22, 24, 32]) para hacerlos más contextual y relacional. Esto también es probable que requieren más re fi namiento de las taxonomías. El mismo modelo Diamond

proporciona la oportunidad de definir las características y sub-características en un estrato interminable de información. Sin embargo, las implementaciones diferentes del modelo podrían conflictuar en sus definiciones. Por lo tanto, volver a más refinamiento de los sub-modelos para cada característica y sub-característica, mediante fundamentos taxonómicos es crítica [25].

También hay varios elementos diversos que se han descrito como que requiere el futuro ORT, tales como:

- La definición de vectores de características y algoritmos de agrupación / clasificaciones para determinados problemas analíticos
- El potencial de integración de prueba de penetración y salida de evaluación de la vulnerabilidad en gráficos de actividad de ataque
- Métodos de prevención sobre flujos de eventos de análisis de intrusión durante la agrupación / clasificación
- Un examen minucioso y definición de eventos sub-funciones como una taxonomía
- La evaluación de las variables y aspectos a determinar grados de persistencia
- Una comprensión más profunda de la esfera político-social y su papel en la toma de decisiones de mitigación, incluyendo la contabilidad para las necesidades y aspiraciones adversario

Por último, el propósito del modelo es lograr más reflexividad y en última instancia, un análisis preciso para permitir la planificación, la estrategia y la toma de decisiones para defender las redes. Por lo tanto, si bien hemos mostrado cómo el modelo se puede utilizar con varios marcos de planificación, cada uno de ellos podría ser un trabajo en sí mismo y hay muchos otros modelos a tener en cuenta.

Por ejemplo, una ruta potencial para generar más reflexividad y estrategias de mitigación creativas sería extender el trabajo de [14] y tratar el hilo de actividad como un grupo de cromosomas en un entorno depredador-presa co-evolutiva usando algoritmos genéticos. Este enfoque ha demostrado previamente promesa y los hilos de actividad modelar un algoritmo genético crédito préstamos cromosoma de buen comportamiento a este concepto.

12 Conclusión

En este trabajo se presenta el Modelo de diamante de análisis de intrusión. Comenzó con el elemento atómico de toda la actividad de intrusión, el evento, y sus características principales (adversario, víctima, infraestructura y capacidad) organizados en la forma de un diamante. Este evento fue más luego definido con sub-funciones y características meta-permitiendo que contenga y relacionar todos los aspectos de un evento malicioso. Desde el caso deducimos varias aproximaciones de funciones centradas para ayudar en la categorización de Tradecraft analítica existente y el desarrollo de nuevos Tradecraft. El modelo extrajo adicionalmente nuevos entendimientos sobre la actividad maliciosa como la importancia de la relación social-política entre adversario y la víctima y los grados

de la persistencia.

Además, el modelo Diamond capturó la esencia de la actividad de intrusión como un conjunto de eventos causales relacionados en una rosca actividad documentar el proceso de extremo a extremo de la versario Ad. Es importante destacar que estos hilos se aumentan aún más con los gráficos de ataque para crear un nuevo enfoque a la tecnología inteligente de seguridad de la información tradicional llamados gráficos de actividad de ataque teniendo en cuenta los ataques adversarios reales, así como los caminos posibles y preferidas. Las roscas y los eventos son luego se unieron en grupos de actividades que abordan los problemas alytic an- más amplias y permiten a las campañas de mitigación más estratégicos a desarrollar. Por último, los grupos de actividad puede ser jerárquica y organizada en la que las familias mejor modelo de sofisticación CATed organizaciones adversario.

El modelo también se ha demostrado que es altamente complementaria con los modelos de decisión, incluyendo la preparación conjunta de Inteligencia del espacio de batalla, la cadena de muertes, la cobertura tradicional vulnerabilidad de seguridad de la información, y los enfoques de juego adversario plan- mitigación múltiples Ning y.

El análisis de intrusiones durante mucho tiempo ha sido considerada como un arte para ser aprendido y practicado, en lugar de una ciencia que ser estudiado y re fi nido. Prueba de ello está en todas partes: desde el enfoque en los resultados analíticos más que en el proceso y los principios, a la transmisión de conocimientos a través de historias y estudios de casos. Sin embargo, acercarse a él sólo como un arte ha demorado mucho mejoras y una mayor comprensión de frenar la evolución de la mitigación de amenazas que se basa en e fi ciente, e caz y siguientes, y un análisis preciso. Sin saberlo, los analistas han utilizado el modelo Diamond durante décadas, pero han carecido el marco completo para comprender, mejorar y enfocar sus Orts ff e.

Es hora de reconocer que la disciplina es un arte y una ciencia. El modelo Diamond aborda este reto de frente en la integración del arte y la ciencia del análisis de intrusión. El modelo Diamond captura con precisión y organiza los conceptos básicos y fundamentales que subyacen en todo lo que los analistas de intrusión hacen y cómo se sintetiza y se utiliza para la mitigación y la defensa de la red de análisis de intrusiones. Se ha logrado sus objetivos de ser a la vez un soporte analítico cognitiva informal y un marco formal de la aplicación de los conceptos matemáticos y computacionales para el análisis de intrusiones. Sin embargo, su mayor contribución es que finalmente se aplica el científico rigor fi co y los principios de medición, la capacidad de prueba, y repetibilidad al dominio que permite el análisis de intrusiones para ser más reflexivo e ff, e fi ciente, y precisa que conduce a más rápido, más e ff caz,

referencias

[1] Richards J. Heuer Jr. *Psicología de Análisis de Inteligencia*. Agencia Central de Inteligencia, 1999.

[2] Chris Sanders. Los 10 mandamientos de análisis de intrusión.

[EN LÍNEA] [http:](http://)

//chrisanders.org/2011/01/the-10-commandments-of-intrusion-analysis/,
Enero de 2011.

- [3] Leo Obrsta, Penny Chaseb, y Richard Markelo FF a. El desarrollo de una ontología de la ciberdominio de seguridad. En Paulo CG Costa y Kathryn B. Laskey, editores, *Actas de las tecnologías semánticas para Inteligencia, Defensa y Seguridad (STIDS) 2012*, páginas 49-56, octubre de 2012. [En línea] <http://ceur-ws.org/Vol-966/>.
- [4] Clifford Stoll. Acechando el hacker astuto. *Communications of the ACM*, 31 (5): 484-497, De mayo de 1988.
- [5] Steve Bellovin. Hay dragones. En *3er Simposio de Seguridad Usenix UNIX*, Baltimore, MD, EE.UU., Septiembre de 1992.
- [6] Bill Cheswick. Una noche con Berferd. En *Los cortafuegos e Internet Seguridad*, Capítulo 10. Addison-Wesley, Reading, MA, EE.UU., 1994.
- [7] Lance Spitzer. El proyecto Honeynet: atrapando a los piratas informáticos. *Seguridad y Privacidad*, página 15, abril de 2003.
- [8] Stephen Northcutt, Mark Cooper, Matt Fearnow, y Karen Frederick. *Intrusión Firmas y Análisis*. New Riders Publishing, Indianapolis, IN, USA, 2001.
- [9] SANS. [EN LÍNEA] <http://www.sans.org>.
- [10] Bernhard Amann, Robin Sommer, Aashish Sharma, y Seth Hall. Un lobo solitario sin más: Apoyo de detección de intrusiones de red con inteligencia en tiempo real. En *15a Conferencia Internacional sobre Investigación en ataques, intrusiones y defensas*, páginas 314-333, Berlín, Heidelberg, 2012. Springer-Verlag.
- [11] Eric M. Hutchins, Michael J. Cloppert, y Rohan M. Amin. Inteligente de la comunidad: defensa de la red putadora informado por el análisis de las campañas adversario y cadenas de intrusiones Kill. En L. Armistad, editor, *Conferencia Internacional sobre la Guerra de Información y Seguridad*, volumen 6, páginas 113-125. Conferencias académicas Internacional, Academic Publishing internacionales ilimitadas, 2011.
- [12] Departamento de Defensa de Estados Unidos. *Conjuntas Tácticas, Técnicas y Procedimientos para Conjunta Inteligencia Preparación del ambiente operacional (JP 2-01,3)*, Junio de 2009.
- [13] Sergio Caltagirone y Deborah Frincke. ADAM: algoritmo de defensa activa y modelo. En NR Wyler y G. Byrne, editores, *Agresiva Red de Autodefensa*, páginas 287-311. Syngress Publishing, Rockville, MD, EE.UU., 2005.
- [14] Sergio Caltagirone. La evolución de las estrategias de defensa activa. Informe Técnico CSDS-DF-TR-05-07, Universidad de Idaho, Moscow, ID, EE.UU., 2005.

- [15] Bruce Schneier. árboles de ataque. *Dr. Dobbs Journal*, 24 (12): 21-29, 1999.
- [16] Richard Paul Lippmann y Kyle William Ingols. Una revisión comentada de exámenes de años anteriores en los gráficos de ataque. Informe Técnico PR-IA-1, Instituto de Tecnología de Massachusetts, Lincoln Laboratory Lexington, 2005.
- [17] Xinming Ou, Wayne Boyer, y Miles McQueen. Un enfoque escalable para atacar gráfico Generacion. En *Actas de la 13ª Conferencia ACM sobre Computación y comunicaciones de seguridad*, páginas 336-345. ACM, 2006.
- [18] Kyle Ingols, Richard Lippmann, y Keith Piwowarski. ataque práctico gráfico de generación ción para la defensa de la red. En *22da Computer Security Conferencia Aplicaciones, ACSAC'06*, páginas 121-130. IEEE 2006.
- [19] Lingyu Wang, Tania Islam, Tao largo, Anoop Singhal, y Sushil Jajodia. Un ataque gráfico basado en medida de seguridad probabilístico. En *Datos y Aplicaciones de Seguridad XXII*, páginas 283-296. Springer, Berlin Heidelberg, 2008.
- [20] John Homero, Ashok Varikuti, Xinming Ou, y Miles McQueen. La mejora de ataque visualización gráfica a través de la reducción de datos y agrupación ataque. En *La visualización de la seguridad informática*, páginas 68-79. Springer, Berlin Heidelberg, 2008.
- [21] Sebastián Roschke, Feng Gheng, y Christopher Meinel. El uso de informa- vulnerabilidad gráficos ción y de ataque para la detección de intrusos. En *Actas de la 6ª Conferencia Internacional sobre la Seguridad de la Información y Seguridad (IAS 2010)*, páginas 104 - 109, At-Lanta, GA, EE.UU., 2010. IEEE Press.
- [22] Vocabulario para la grabación de eventos y el intercambio de incidente (VERIS). [EN LÍNEA] <http://www.veriscommunity.net>.
- [23] ThreatConnect. [EN LÍNEA] <http://www.threatconnect.com>.
- [24] Un lenguaje estructurado de información de inteligencia amenaza cibernética (Stix). [EN LÍNEA] <http://stix.mitre.org>.
- [25] John D. Howard y Pascal Meunier. El uso de un lenguaje común para la seguridad informática la información del incidente. En Seymour Bosworth y ME Kabay, editores, *Manual de Seguridad ordenador*, capítulo 3, páginas 3.1-3.22. John Wiley & Sons, Nueva York, NY, EE.UU., cuarta edición, 2002.
- [26] Frederick B. Cohen. *La protección y la seguridad en la autopista de la información*. Juan Wiley & Sons, Nueva York, Nueva York, EE.UU., 1995.
- [27] Steven T. Eckmann, Giovanni Vigna, y Richard A. Kemmerer. STATL: Un ataque idioma para detección de intrusos basado en estado. *Diario de la seguridad informática*, 10 (1): 71-163, 2002.

- [28] Frederick B. Cohen. ataques al sistema de información: un esquema de clasificación preliminar. *Computadoras y Seguridad*, 16 (1): 29-46, 1997.
- [29] John D. Howard y Thomas A. Longstaff. Un language común para la seguridad informática incidents. Technical Report SAND98-8667, Sandia National Laboratories, October 1998.
- [30] Frederic Cuppens and Rodolphe Ortalo. LAMBDA: A language to model a database for detection of attacks. In *Proceedings of the Third International Workshop, RAID 2000*, pages 197–216, Berlin, Heidelberg, 2000. Springer-Verlag.
- [31] Michel Cedric and Ludovic Me. ADELE: An attack description language for knowledge-based intrusion detection. In *Trusted Information*, number 65, pages 353–368. Springer US, 2002.
- [32] Sophisticated indicators for the modern threat landscape: An introduction to OpenIOC. [ONLINE] [http://openioc.org/resources/An Introduction to OpenIOC.pdf](http://openioc.org/resources/An%20Introduction%20to%20OpenIOC.pdf).
- [33] Command and control. In *Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms*, page 103. US Department of Defense, March 2009.
- [34] Wim Van Eck. Electromagnetic radiation from video display units: An evesdropping risk? *Computers & Security*, 4(4):269–286, 1985.
- [35] MITRE. Common vulnerabilities and exposures. [ONLINE] <http://cve.mitre.org/>.
- [36] Stuart McClure, Joel Scambray, and George Kurtz. *Hacking Exposed*. McGraw-Hill Osborne Media, 4th edition, 2003.
- [37] classtype. In *Snort Users Manual 2.9.3*, page 179. The Snort Project, May 2012.
- [38] Austin Troya, J. Morgan Grove, and Jarlath O’Neil-Dunne. The relationship between tree canopy and crime rates across an urban-rural gradient in the greater Baltimore region. *Landscape and Urban Planning*, 106(3):262–270, June 2012.
- [39] Will Gragido. Lions at the watering hole – the “VOHO” affair. [ONLINE] <http://blogs.rsa.com/lions-at-the-watering-hole-the-voho-affair>, July 2012.
- [40] Kurt Baumgartner. Winnti-stolen digital certificates re-used in current watering hole attacks on Tibetan and Uyghur groups. [ONLINE] [http://www.securelist.com/en/blog/208194218/Winnti Stolen Digital Certificates Re Used in Current Watering Hole Attacks on Tibetan and Uyghur Groups](http://www.securelist.com/en/blog/208194218/Winnti_Stolen_Digital_Certificates_Re_Used_in_Current_Watering_Hole_Attacks_on_Tibetan_and_Uyghur_Groups), April 2013.
- [41] Matthias Vallentin, Jon Whiteaker, and Yahel Ben-David. The gh0st in the shell: Network security in the Himalayas. [ONLINE] <http://www.eecs.berkeley.edu/~yahel/>

papers/network-security-in-the-himalayas-cs294-28.pdf.

- [42] Symantec Security Response. W32.Duqu: The precursor to the next Stuxnet. [ONLINE] [http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32 duqu the precursor to the next stuxnet. pdf](http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf), November 2011. –
- [43] Red October: Diplomatic cyber attacks investigation. [ONLINE] [http://www.securelist.com/en/analysis/204792262/Red October Cyber Attacks Investigation](http://www.securelist.com/en/analysis/204792262/Red_October_Cyber_Attacks_Investigation), 2013. – –
- [44] Command Five Pty Ltd. SK Hack by an advanced persistent threat. [ONLINE] [http://www.commandfive.com/papers/C5 APT SKHack.pdf](http://www.commandfive.com/papers/C5_APT_SKHack.pdf), September 2011.
- [45] D. Ian Hopper and Richard Stenger. Large-scale phone invasion goes unnoticed by all but FBI. *CNN*, December 1999. [ONLINE] [http://edition.cnn.com/1999/TECH/ computing/12/14/phone.hacking/](http://edition.cnn.com/1999/TECH/computing/12/14/phone.hacking/).
- [46] Nate Anderson. How one man tracked down Anonymous – and paid a heavy price. *Ars Technica*, February 2011. [ONLINE] <http://www.arstechnica.com/tech-policy/2011/02/how-one-security-firm-tracked-anonymousand-paid-a-heavy-price/>.
- [47] Jose Nazario. Georgia DDoS attacks – a quick summary of observations. [ONLINE] <http://ddos.arbornetworks.com/2008/08/georgia-ddos-attacks-a-quick-summary-of-observations>, August 2008.
- [48] Brian Krebs. Cyber attacks target pro-Tibet groups. *Washington Post*, March 2008. [ONLINE] [http://www.washingtonpost.com/wp-dyn/content/article/ 2008/03/21/AR2008032102605.html](http://www.washingtonpost.com/wp-dyn/content/article/2008/03/21/AR2008032102605.html).
- [49] Bojan Zdrnja, Nevil Brownlee, and Duane Wessels. Passive monitoring of DNS anomalies. In *Proceedings of the 4th International Conference on Detection of Intrusions and Malware and Vulnerability Assessments, DIMVA '07*, pages 129–139, Berlin, Heidelberg, 2007. Springer-Verlag.
- [50] Manos Antonakakis, Roberto Perdisci, Wenke Lee, Nikolas Vasiloglou, II, and David Dagon. Detecting malware domains at the upper DNS hierarchy. In *Proceedings of the 20th USENIX Conference on Security, SEC'11*, pages 27–27, Berkeley, CA, USA, 2011. USENIX Association.
- [51] Wolfgang John and Tomas Olovsson. Detection of malicious traffic on back-bone links via packet header analysis. *Campus-Wide Information Systems*, (25):342–358, 2008.
- [52] S. Templeton and K. Levitt. A requires/provides model for computer attacks. In *Proceedings of the 2000 Workshop on New Security Paradigms*, New York, NY, USA, 2001. ACM Press.

- [53] Crime pattern analysis: An investigative tool. In Michael J Palmiotto, editor, *Critical Issues in Criminal Investigation*, pages 59–69. Pilgrimage, 2nd edition, 1988.
- [54] Douglas M. Hawkins. The problem of overfitting. *Journal of Chemical Information and Computer Sciences*, (10):1–12, 2004.
- [55] Huan Liu and Hiroshi Motoda. *Feature Selection for Knowledge Discovery and Data Mining*. Kluwer Academic Publishers, Norwell, MA, USA, 1998.
- [56] Susan W. Brenner. Organized cybercrime? how cyberspace may affect the structure of criminal relationships. *North Carolina Journal of Law & Technology*, 4(1), Fall 2002.