Inteligente de la red de ordenadores de Defensa informa en el análisis del Adversario y Campañas

Cadenas de intrusiones Kill

Eric M. Hutchins *, Michael J. Cloppert †, Rohan M. Amin, Ph.D. ‡

Lockheed Martin Corporation

Resumen

herramientas de defensa de red convencionales, tales como los sistemas de detección de intrusos y el enfoque anti-virus en el componente de vulnerabilidad de riesgos, y la metodología de respuesta a incidentes tradicional presupone una intrusión exitosa. Una evolución en los objetivos y sofisticación de intrusiones en la red de ordenadores ha hecho que estos enfoques Insu fi ciente para ciertos actores. Una nueva clase de amenazas, apropiadamente llamada la "amenaza persistente avanzada" (APT), representa adversarios con buenos recursos y formados que llevan a cabo campañas de intrusión plurianuales destinados a información altamente sensible de seguridad económica, de propiedad, o nacional. Estos adversarios lograr sus objetivos mediante herramientas avanzadas y técnicas diseñadas para derrotar a los mecanismos de defensa de la red informática más convencionales. técnicas de defensa de red que aprovechar los conocimientos sobre estos adversarios pueden crear un bucle de retroalimentación de inteligencia, lo que permite defensores para establecer un estado de superioridad de la información que disminuye la probabilidad de que el adversario de éxito con cada intento de intrusión posterior. El uso de un modelo de cadena de matanza para describir las fases de intrusiones, los indicadores de la cadena adversario matanza de mapeo para Defender cursos de acción, la identificación de patrones que enlazan intrusiones individuales en campañas más amplias, y la comprensión de la naturaleza iterativa de la recogida de información constituyen la base de defensa de la red informática de inteligencia impulsada (CND). Institucionalización de este enfoque reduce la probabilidad de éxito adversario, informa a la inversión y la defensa de la red de recursos asignación de prioridades, y produce métricas relevantes de rendimiento y e cacia y ss.

palabras clave: respuesta a incidentes, detección de intrusos, la inteligencia, la amenaza, APT, defensa de la red informática

1. Introducción

Mientras han existido redes informáticas mundiales, por lo que los usuarios maliciosos intención de explotar vulnerabilidades. Las primeras evoluciones de las amenazas a las redes de ordenadores que participan código propaga por sí mismo. Los avances en el tiempo en la tecnología antivirus significativamente reducen este riesgo automatizado. Más recientemente, una nueva clase de amenazas, intento en el compromiso de los datos para el avance económico o militar, surgió como el mayor elemento de riesgo que enfrentan algunas industrias. Esta clase de amenaza que se le ha dado el apodo de "amenaza persistente avanzada", o APT. Hasta la fecha, la mayoría de las organizaciones se han basado en las tecnologías y procesos implementados para mitigar los riesgos asociados a los virus y gusanos automatizados que no su dirección de fi cientemente centrado, operada manualmente intrusiones APT.

APT Recientemente se han observado y que se caracteriza por la industria y el gobierno de Estados Unidos. En junio y julio de 2005, el Centro de Seguridad de Infraestructura Coordinación Nacional del Reino Unido (UK-NUSCC) y los EE.UU.

* eric.m.hutchins@lmco.com

† michael.j.cloppert@lmco.com

‡ rohan.m.amin@lmco.com

Computer Emergency Response Team (US-CERT) emitió boletines técnicos que describen alertas, mensajes de correo electrónico de ingeniería social dirigidos a la información que caen troyanos ex infiltrado sensible. Estas intrusiones fueron durante un periodo fi significativo de tiempo, eludieron capacidades cortafuego convencional y anti-virus, y los adversarios para cosechar información sensible (UK-NUSCC, 2005; US-CERT, 2005) habilitados. Epstein y Elgin (2008) de la revista Business Week describen numerosas intrusiones en la NASA y otras redes gubernamentales donde los actores de la APT no se habían detectado y exitoso en la eliminación de la información sensible diseño del cohete de alto rendimiento. En febrero de 2010, iSec Partners observó que los enfoques actuales, tales como antivirus y parches no son su cientes FFI, los usuarios finales están dirigidos directamente, y los agentes de amenaza son sensibles después de la propiedad intelectual (Stamos, 2010).

Antes de los EE.UU. Comité de Servicios Armados Subcomité de Terrorismo, amenazas no convencionales y capacidades, James Andrew Lewis, del Centro de Estudios Estratégicos e Internacionales testi fi cado que las intrusiones se produjeron en varias agencias del gobierno en 2007, incluyendo el Departamento de Defensa, el Departamento de Estado y el Departamento de Comercio, con la intención de recopilación de información (Lewis, 2008). Con específica de la ciudad sobre la naturaleza de las operaciones de la red de ordenadores según los informes, procedentes de China, los informes de 2008 y 2009 al Congreso de la Comisión Económica y de Seguridad Estados Unidos-China se resume la presentación de informes de las intrusiones dirigidas contra los sistemas militares, gubernamentales y contratistas estadounidenses. Una vez más, los adversarios fueron motivadas por el deseo de recopilar información confidencial (Comisión Estados Unidos-China Economic Review y Seguridad, 2008, 2009). Finalmente,

Los avances en las herramientas de gestión de la infraestructura han permitido a las mejores prácticas de aplicación de parches y el endurecimiento de toda la empresa, lo que reduce las vulnerabilidades de más fácil acceso en los servicios de red. Sin embargo, los actores de la APT continuamente demuestran la capacidad para afectar los sistemas mediante el uso de herramientas avanzadas, malware personalizado y exploits de “día cero” que antivirus y parches no pueden detectar o mitigar. Las respuestas a las intrusiones APT requieren una evolución en el análisis, procesos y tecnología; es posible anticipar y mitigar futuras intrusiones basados en el conocimiento de la amenaza. Este artículo describe un enfoque centrado en la amenaza de inteligencia impulsada para estudiar las intrusiones desde la perspectiva de los adversarios. Cada fase discreta de la intrusión se asigna a cursos de acción para la detección, mitigación y respuesta. La frase “cadena de destrucción” describe la estructura de la intrusión, y el modelo correspondiente guía a análisis para informar a la inteligencia de seguridad accionable. A través de este modelo, los defensores pueden desarrollar mitigaciones resistentes contra intrusos e inteligentemente prioridad a las inversiones en nuevas tecnologías o procesos. análisis de la cadena Kill ilustra que el adversario debe progresar con éxito a través de cada etapa de la cadena antes de que pueda alcanzar su objetivo deseado; sólo una mitigación interrumpe la cadena y el adversario. A través de la respuesta de inteligencia impulsada, el defensor puede lograr una ventaja sobre el agresor para adversarios calibre APT. los defensores pueden desarrollar mitigaciones resistentes contra intrusos e inteligentemente prioridad a las inversiones en nuevas tecnologías o procesos. análisis de la cadena Kill ilustra que el adversario debe progresar con éxito a través de cada etapa de la cadena antes de que pueda alcanzar su objetivo deseado; sólo una mitigación interrumpe la cadena y el adversario. A través de la respuesta de inteligencia impulsada, el defensor puede lograr una ventaja sobre el agresor para adversarios calibre APT. los defensores pueden desarrollar mitigaciones resistentes contra intrusos e inteligentemente prioridad a las inversiones en nuevas tecnologías o procesos. análisis de la cadena Kill ilustra que el adversario debe progresar con éxito a través de cada etapa de la cadena antes de que pueda alcanzar su objetivo deseado; sólo una mitigación interrumpe la cadena y el adversario. A través de la respuesta de inteligencia impulsada, el defensor puede lograr una ventaja sobre el agre

Este trabajo se organiza de la siguiente manera: la sección dos de este trabajo los documentos de trabajo relacionados en modelos basados fase de la estrategia de defensa y contramedidas. La tercera sección presenta una red de ordenadores modelo de defensa de inteligencia impulsada (CND) que incorpora análisis fi c intrusión amenaza especí y mitigaciones defensivas. La cuarta sección presenta una aplicación de este nuevo modelo de estudio de un caso real, y la sección cinco resume el papel y es una reflexión sobre el futuro estudio.

2. Trabajo relacionado

Si bien el modelado de las APT y de respuesta utilizando cadenas Kill correspondientes es única, otra fase modelos basados existan estrategias de defensa y contramedidas.

Una publicación del Departamento de Defensa para Juntas Sta ff Estados Unidos describe una cadena de destrucción con las etapas encontramos, fi x, pista, seleccionar, enfrentar y evaluar (Departamento de Defensa de EE.UU., 2007). La Fuerza Aérea de los Estados Unidos (USAF) ha utilizado este marco para identificar las lagunas en inteligencia, vigilancia y capacidad de reconocimiento (ISR) y dar prioridad al desarrollo de los sistemas necesarios (Tirpak, 2000). cadenas de amenazas también se han utilizado para modelar dispositivo explosivo (IED) ataques improvisados (National Research Council, 2007). El IED modelos de cadena de suministro, desde la financiación adversario para atacar ejecución. inteligencia coordinada y defensivos e ff Orts se centraron en cada etapa de la cadena de amenaza de los IED como la forma ideal para contrarrestar estos ataques. Este enfoque también proporciona un modelo para identificación de las necesidades de investigación básica mediante la asignación de la capacidad existente a la cadena. modelos basados fase también se han utilizado para la planificación antiterrorista. El ejército de Estados Unidos describe el ciclo de planificación operativa terrorista como un proceso de siete pasos que sirve como punto de referencia para evaluar la intención y la capacidad de las organizaciones terroristas (Formación ejército de Estados Unidos

y Doctrina de Comando, 2007). Hayes (2008) aplica este modelo para el proceso de planificación antiterrorista para instalaciones militares y principios identi fi ca a ayudar a los comandantes determinar las mejores maneras de protegerse a sí mismos.

Fuera del contexto militar, los modelos basados en fase también se han utilizado en la seguridad de la información de campo. Sakuraba et al. (2008) describen el análisis de Ataque a base secuencial de las contramedidas (ABSAC) marco que se alinea tipos de contramedidas a lo largo de la fase de tiempo de un ataque. El enfoque ABSAC incluye más reactivos contramedidas post-compromiso que la capacidad de detección temprana para descubrir campañas adversario persistentes. En una aplicación de modelos basados de fase para las amenazas internas, Duran et al. (2009) describen una estrategia de detección y contramedidas niveles basado en el progreso de la información privilegiada maliciosos. Willison y Siponen (2009) también se ocupan de las amenazas internas mediante la adaptación de un modelo basado fase llamada situacional de prevención del delito (SCP). SCP modelos delito desde la perspectiva de la junta y siguientes de Ender y luego los mapas de controles para las distintas fases del crimen. Finalmente, la empresa de seguridad Mandiant propone un “ciclo de vida de la explotación”. El modelo Mandiant, sin embargo, no mapa cursos de acción defensiva y se basa en las acciones post-compromiso (MANDIANT, 2010). Mover detecciones y mitigaciones a las fases anteriores de la cadena de intrusión kill es esencial para CND contra actores APT.

3 Inteligencia impulsada por la red de ordenadores de Defensa

defensa de la red informática de inteligencia impulsada es una estrategia de gestión de riesgos que aborda el componente de amenaza de riesgo, análisis de adversarios, sus capacidades, objetivos, doctrina y limitaciones que incorpora. Este es necesariamente un proceso continuo, el aprovechamiento de los indicadores para descubrir nueva actividad con aún más indicadores de apalancamiento. Se requiere una nueva comprensión de los mismos, no como eventos singulares, sino más bien como progresiones graduales intrusiones. En este trabajo se presenta un nuevo modelo de cadena de intrusión kill para analizar las intrusiones y conducir cursos de acción defensiva.

El e ff ect de la CND inteligencia impulsada es una postura de seguridad más resistentes. actores de la APT, por su naturaleza, intento de intrusión después de la intrusión, el ajuste de sus operaciones basadas en el éxito o fracaso de cada intento. En un modelo de cadena de destrucción, sólo uno de mitigación rompe la cadena y frustra el adversario, por lo que cualquier repetición por el adversario es un pasivo que los defensores deben reconocer y apalancamiento. Si los defensores de implementar contramedidas adversarios más rápido que evolucionan, que eleva los costos a un adversario debe gastar para lograr sus objetivos. Este modelo muestra, en contra de la sabiduría convencional, tales agresores no tienen ninguna ventaja inherente sobre los defensores.

3.1 Indicadores y el ciclo de vida del indicador

El elemento fundamental de la inteligencia en este modelo es el *indicador.* Para los fines de este documento, un indicador es cualquier pieza de información que describe objetivamente una intrusión. Los indicadores pueden ser subdivididos en tres tipos:

- Atómica - indicadores atómicos son los que no se puede dividir en partes más pequeñas y conservan su significado en el contexto de una intrusión. Ejemplos típicos Estas son las direcciones IP, direcciones de correo electrónico, y los identificadores de vulnerabilidad.

- computarizada - indicadores calculados son aquellos que se derivan de datos involucrados en un incidente. indicadores calculados comunes incluyen valores hash y expresiones regulares.
- conductual - Los indicadores de comportamiento son colecciones de indicadores calculados y atómicas, a menudo sujetos a salvedad por la cantidad y la lógica posiblemente combinatoria. Un ejemplo sería una declaración como “el intruso podría inicialmente utilizado una puerta trasera que genera la red tra FFI c coincidente [expresión regular] a razón de [cierta frecuencia] a [alguna dirección IP], y luego sustituirlo por uno que coincida con el hash MD5 [valor] una vez que se estableció el acceso “.

El uso de los conceptos en el presente documento, los analistas revelarán indicadores a través del análisis o la colaboración, madurar estos indicadores mediante el aprovechamiento de ellos en sus herramientas, y después utilizarlos cuando se descubre la actividad a juego. Esta actividad, cuando se investigó, a menudo dará lugar a indicadores adicionales que estarán sujetos al mismo conjunto de acciones y estados. Este ciclo de acciones, y los estados de los indicadores correspondientes, forman el ciclo de vida del indicador se ilustra en la Figura 1. Esto se aplica a todos los indicadores de manera indiscriminada, independientemente de su exactitud o aplicabilidad. El seguimiento de la derivación de un indicador dado de sus predecesores puede ser

consume tiempo y problemático si su fi ciente de seguimiento no está en su lugar, por lo tanto, es imperativo que los indicadores sometidos a estos procesos son válidos y aplicables al conjunto de problemas en cuestión. Si no se presta atención a este punto, los analistas pueden hallar a sí mismos la aplicación de estas técnicas a los actores de amenazas para las que no fueron diseñados, o a la actividad benigna por completo.

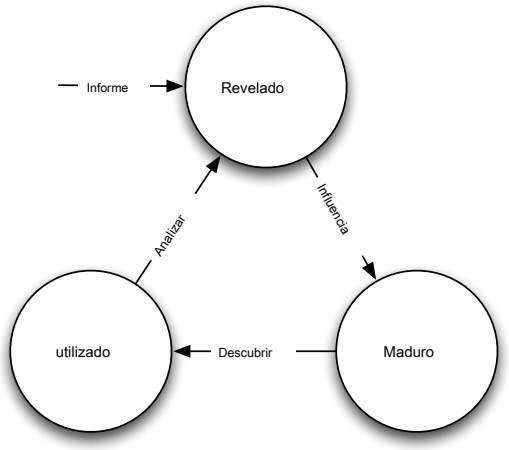

Figura 1: estados y transiciones del ciclo de vida del indicador

Cadena 3.2 de intrusiones Kill

Una cadena de destrucción es un proceso sistemático para apuntar y participar un adversario para crear ECTS ff e deseadas. militar de Estados Unidos orientación doctrina de fi nes los pasos de este proceso como fi nd, fi x, pista, objetivo, enganche, evaluar (F2T2EA): objetivos adversario fi nd adecuado para el acoplamiento; fi x su ubicación; rastrear y observar; apuntar con el arma o activo para crear ECTS e ff deseada adecuada; participar adversario; evaluar ECTS ff e (Departamento de Defensa de EE.UU., 2007). Este es un proceso integrado de extremo a extremo descrito como una “cadena”, ya que cualquier uno de fi ciencia interrumpirá todo el proceso.

Ampliando este concepto, este trabajo presenta un nuevo modelo de cadena de matanza, uno especí fi camente para las intrusiones. La esencia de una intrusión es que el agresor debe desarrollar una capacidad de carga de romper un límite de confianza, establecer una presencia dentro de un entorno de confianza, ya partir de esa presencia, tomar acciones hacia sus objetivos, se están moviendo lateralmente dentro del medio ambiente o la violación de la confidencialidad, integridad o disponibilidad de un sistema en el medio ambiente. La cadena de intrusión kill se define como de reconocimiento, emplazamiento de armas, la entrega, la explotación, la instalación, mando y control (C2), y las acciones sobre los objetivos.

Con respecto al ataque a la red de ordenador (CNA) o espionaje red informática (CNE), las de fi niciones para estas fases de la cadena de matanza son los siguientes:

1. reconocimiento - Research, identi fi cación y selección de objetivos, a menudo representado como gatear
   sitios web de Internet, tales como resúmenes de congresos y listas de correo para direcciones de correo electrónico, relaciones sociales, o información sobre las tecnologías específicas.
2. militarización - Acoplar un troyano de acceso remoto con un exploit en una carga útil de entrega,
   típicamente por medio de una herramienta automatizada (Weaponizer). Cada vez más, los datos de aplicaciones cliente archivos tales como archivos de formato de documento portátil (PDF) o Microsoft O fi cina documentos sirven como la entrega en armas.
3. entrega - La transmisión del arma para el entorno de destino. Los tres más prevalente
   vectores de suministro para cargas útiles en armas por parte de agentes de la APT, según lo observado por el Equipo de Respuesta a Incidentes Lockheed Martin ordenador (LM-CIRT) para los años 2004-2010, son adjuntos de correo electrónico, páginas web y medios extraíbles USB.
4. Explotación - Después de que el arma se entrega al anfitrión víctima, la explotación desencadena código de intrusos.
   Muy a menudo, la explotación se dirige a una vulnerabilidad de aplicación o sistema operativo, pero también podría explotar más simplemente los propios usuarios o aprovechar una función del sistema operativo que se auto-ejecuta el código.

5. instalación - La instalación de un troyano de acceso remoto o puerta trasera en el sistema permite que la víctima
   adversario para mantener la persistencia en el medio ambiente.

6. Mando y control (C2) - Típicamente, hosts comprometidos deben baliza de salida a una
   servidor de controlador de Internet para establecer un canal C2. el malware APT requiere especialmente la interacción manual en lugar de la actividad de conducta automáticamente. Una vez que el canal C2 establece, intrusos tienen “las manos en el teclado” acceso al interior del entorno de destino.

7. Acciones sobre Objetivos - Sólo ahora, después de avanzar a través de los primeros seis fases, pueden los intrusos
   tomar acciones para lograr sus objetivos originales. Típicamente, este objetivo es datos ex filtración que implica la recogida, la codificación y la extracción de información desde el entorno víctima; violaciónes de integridad de los datos o la disponibilidad son objetivos potenciales. Como alternativa, los intrusos sólo se pueden desear acceder a la caja de la víctima inicial para su uso como un punto de salto para comprometer sistemas adicionales y moverse lateralmente dentro de la red.

3.3 Líneas de actuación

La cadena de intrusión kill se convierte en un modelo para la inteligencia procesable cuando los defensores alinean capacidades defensivas de la empresa a la específica procesa un adversario se compromete a orientar dicha empresa. Los defensores pueden medir el rendimiento, así como el correo cacia y siguientes de estas acciones, y el plan de inversión hojas de ruta para rectificar cualquier brechas de capacidad. Fundamentalmente, este enfoque es la esencia de la CND inteligencia impulsada: basar las decisiones de seguridad y mediciones en un profundo conocimiento del adversario. La Tabla 1 muestra un curso de la matriz de acciones mediante las acciones de detectar, negar, interrumpir, degradar, engañar, y destruir la doctrina de las operaciones de información del Departamento de Defensa (IO) (Departamento de Defensa de Estados Unidos, 2006). Esta matriz representa en la fase de explotación, por ejemplo, que los sistemas de detección de intrusiones en el host (HIDS) puede pasivamente

detectar exploits, parches *niega* explotación por completo, y la prevención de ejecución de datos (DEP) puede *interrumpir*
la hazaña una vez que se inicia. Ilustrando el espectro de las capacidades de los defensores pueden emplear, la matriz incluye sistemas tradicionales como los sistemas de detección de intrusiones de red (NIDS) y las listas de control de acceso fi cortafuegos (ACL), sistema de endurecimiento mejores prácticas como el registro de auditoría, sino también los propios usuarios vigilantes que pueden detectar actividades sospechosas.

Tabla 1: Matriz de Líneas de Acción

Fase	Detectar	Negar	Interrumpir	Degradar	Engañar	Destruir
Reconocimiento	Analista de la red	firewall ACL				
armamentización	NIDS	PELLIZCOS				
Entrega	filtro Proxy usuario Vigilant		En la línea de AV	hacer cola		
Explotación	HIDS	Parche	DEP			
Instalación	HIDS	cárcel “chroot”	AV			
C2	NIDS	firewall ACL	PELLIZCOS	Pozo de brea	redirección de DNS	
Acciones sobre los objetivos	Registro de auditoría			Calidad de servicio	Tarro de miel	

Aquí, la integridad equivale a la resiliencia, que es el objetivo principal de la defensa cuando se enfrentan a adversarios persistentes que se adaptan continuamente sus operaciones con el tiempo. Las adaptaciones más notables son exploits, particularmente previamente no revelado exploits “día cero”. Los proveedores de seguridad llaman a estos “ataques de día cero”, y tout “protección día cero”. Este enfoque miope no tiene en cuenta que la explotación es más que un cambio en un proceso más amplio. Si los intrusos desplegar un exploit de día cero, pero la reutilización de herramientas observables o infraestructura

en otras fases, que mejora importante es infructuosa si los defensores tienen mitigaciones para las repetidas indicadores. Esta repetición demuestra una estrategia de defensa de la utilización completa indicador alcanza la resistencia y fuerza al adversario para hacer más dif'ıcil y ajustes integrales para lograr sus objetivos. De esta manera, el defensor aumenta el coste del adversario de la ejecución de las intrusiones exitosas.

Los defensores pueden generar métricas de esta capacidad de recuperación mediante la medición del rendimiento y ss e cacia de las acciones defensivas contra los intrusos. Considere una serie ejemplo de los intentos de intrusión desde una sola campaña APT que se producen durante un periodo de tiempo de siete meses se muestra en la Figura 2. Para cada fase de la cadena de destrucción, un diamante blanco indica relevante, pero pasiva, las detecciones estaban en su lugar en el momento de intento de intrusión de ese mes, un diamante negro indica mitigaciones pertinentes estaban en su lugar, y una celda vacía indica que no hay capacidades pertinentes estaban disponibles. Después de cada intrusión, los analistas apalancar nuevos indicadores dan cuenta de actualizar sus defensas, como se muestra por las flechas de color gris.

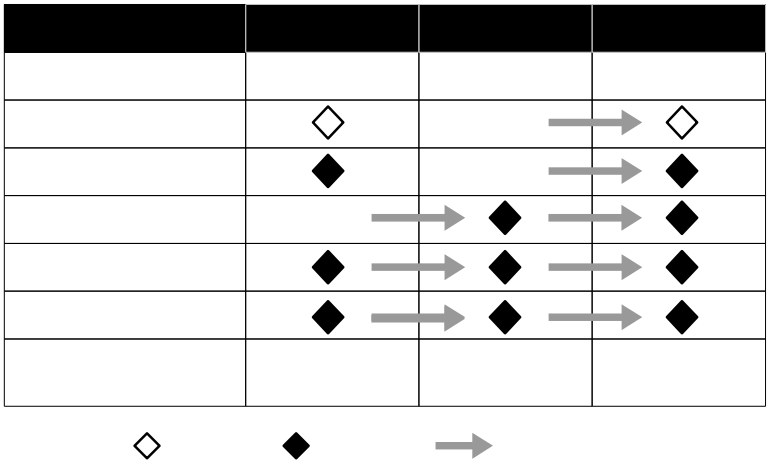

Figura 2: Ilustración de la e ff cacia relativa de las defensas contra intentos de intrusión posteriores

La ilustración muestra, ante todo, que en el último mitigación estaba en su lugar para los tres intentos de intrusión, por lo tanto mitigaciones tuvieron éxito. Sin embargo, también muestra claramente fi cativos erences di ff significantes en cada mes. En diciembre, los defensores de detectar el emplazamiento de armas y bloquean la entrega pero descubren una nueva marca, sin paliativos, de día cero explotar en el proceso. En marzo, el adversario vuelve a utilizar la misma hazaña, sino que evoluciona la técnica y armas en infraestructura de entrega, eludiendo la detección y la prestación de esos sistemas defensivos ine ff ectantes. Para junio, los defensores actualizan sus capacidades de su fi ciente para tener detecciones y mitigaciones laminares de emplazamiento de armas a C2. Al enmarcar métricas en el contexto de la cadena de matanza,

3.4 Reconstrucción de intrusiones

Análisis de la cadena de muertes es una guía para los analistas para entender cuál es la información, y puede ser, disponibles para los cursos de acción defensiva. Es un modelo para analizar las intrusiones de una manera nueva. La mayoría de las intrusiones detectadas proporcionarán un conjunto limitado de atributos acerca de una sola fase de una intrusión. Los analistas todavía debe descubrir muchos otros atributos para cada fase para enumerar el conjunto máximo de opciones para cursos de acción. Además, basado en la detección en una fase dada, los analistas pueden asumir que las fases anteriores de la intrusión ya han ejecutado con éxito. Sólo a través de análisis completo de las fases anteriores, como se muestra en la Figura 3, se pueden tomar acciones en aquellas fases para mitigar ataques futuros. Si no se puede reproducir la fase de entrega de una intrusión, no se puede esperar para actuar en la fase de entrega de intrusiones posteriores de la misma adversario. El proceso de respuesta a incidentes convencional inicia después de nuestra hazaña fase, que ilustra la profecía llenado auto-ful que los defensores son inherentemente e inevitablemente desventaja demasiado tarde. La incapacidad para reconstruir totalmente todas las fases de intrusión da prioridad a las herramientas, tecnologías y procesos para llenar este vacío. Los defensores deben ser capaces de mover su detección y análisis de la cadena de destrucción y lo más importante para implementar cursos de acción a través de la cadena de destrucción. Para que una intrusión a ser económico, adversarios deben volver a utilizar las herramientas y la infraestructura. Al entender completamente una intrusión, y el aprovechamiento de la inteligencia La incapacidad para reconstruir totalmente todas las fases de intrusión da prioridad a las herramientas, tecnologías y procesos para llenar este vacío. Los defensores deben ser capaces de mover su detección y análisis de la cadena de destrucción y lo más importante para implementar cursos de acción a través de la cadena de destrucción. Para que una intrusión a ser económico, adversarios deben volver a utilizar las herramientas y la infraestructura. Al entender completamente una intrusión, y el aprovechamiento de la inteligencia La incapacidad para reconstruir totalmente todas las fases de intrusión da prioridad a las herramientas, tecnologías y procesos para llenar este vacío. Los defensores deben ser capaces de mover su detección y análisis de la cadena de destrucción y lo más importante para implementar cursos de acción a través de la cadena de destrucción. Para que

Figura 3: detección de fase tardía

sobre estas herramientas y la infraestructura, los defensores obligan a un adversario a cambiar todas las fases de su intrusión a fin de lograr con éxito sus objetivos de intrusiones posteriores. De esta manera, los defensores de la red utilizan la persistencia de intrusiones adversarios contra ellos para lograr un nivel de resistencia.

Tan importante como análisis exhaustivo de compromisos de éxito es la síntesis de las intrusiones sin éxito. Como defensores recogen datos sobre adversarios, van a empujar la detección de las últimas fases de la cadena de muertes en los anteriores. Detección y prevención en las fases pre-compromiso también requiere una respuesta. Los defensores deben recopilar tanta información sobre la intrusión mitigada como sea posible, para que puedan sintetizar lo que podría haber sucedido deben eludir futuras intrusiones la actualidad e caz y siguientes protecciones y detecciones (ver Figura 4). Por ejemplo, si un correo electrónico malicioso dirigido se bloquea debido a la re-uso de un indicador conocido, la síntesis de la cadena de destrucción restante podría revelar un nuevo explotar o puerta trasera contenido en el mismo. Sin este conocimiento, las futuras intrusiones, entregados por medio di ff Erent, pueden pasar desapercibidos.

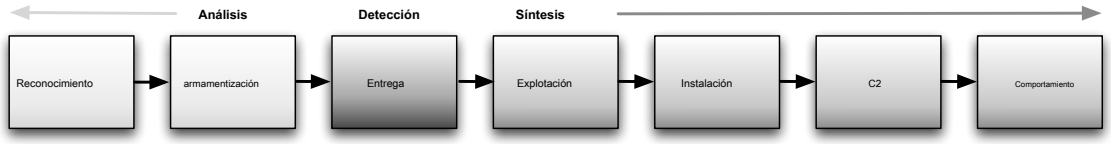

Figura 4: Detección de fase anterior

Análisis de Campaña 3.5

A nivel estratégico, el análisis de múltiples cadenas de intrusión de matar con el tiempo va a identificar elementos comunes e indicadores que se solapan. Figura 5 ilustra cómo altamente dimensional correlación entre dos intrusiones a través de múltiples fases de la cadena de matanza puede ser identi fi. A través de este proceso, los defensores reconocerán y campañas de intrusión fi ne, y que une quizás años de actividad de una amenaza persistente en particular. Los indicadores más consistentes, las campañas de indicadores clave, proporcionan centros de gravedad de los defensores para priorizar el desarrollo y uso de los cursos de acción. La figura 6 muestra cómo las intrusiones pueden tener diversos grados de correlación, pero la en puntos fl exión donde los indicadores más frecuentemente alinear identificar estos indicadores clave. Estos indicadores menos volátiles se pueden esperar para ser coherentes, predecir las características de futuras intrusiones con mayor confianza la mayor frecuencia se observan. De esta manera, la persistencia de un adversario se convierte en una responsabilidad que la defensa puede aprovechar para reforzar su postura.

El objetivo del análisis de la campaña principio es determinar los patrones y comportamientos de los intrusos, sus tácticas, técnicas y procedimientos (TTP), para detectar “cómo” que operan en vez de fi camente “qué” que hacen. El objetivo de la defensa es menos atribuir positivamente la identidad de los intrusos no sea para evaluar sus capacidades, doctrina, objetivos y limitaciones; atribución intruso, sin embargo, bien puede ser un producto secundario de este nivel de análisis. Como defensores estudian nueva actividad de intrusión, ya sea que se vincularlo a las campañas existentes o quizás identificar un nuevo conjunto de comportamientos de una amenaza desconocida hasta entonces y hacer un seguimiento como una nueva campaña. Los defensores pueden evaluar su postura defensiva en relación sobre una base de campaña por campaña, y en base al riesgo evaluado de cada uno, desarrollar líneas estratégicas de actuación para cubrir cualquier hueco.

Otro objetivo fundamental del análisis de la campaña es entender la intención de los intrusos. En la medida en que los defensores pueden determinar las tecnologías o personas de interés, pueden empezar a entender los objetivos de la misión adversarys. Para ello es necesario intrusiones de tendencias a través del tiempo para evaluar la orientación y los patrones de examinar de cerca los datos ex infiltrado por los intrusos. Una vez de nuevo este resultados de los análisis

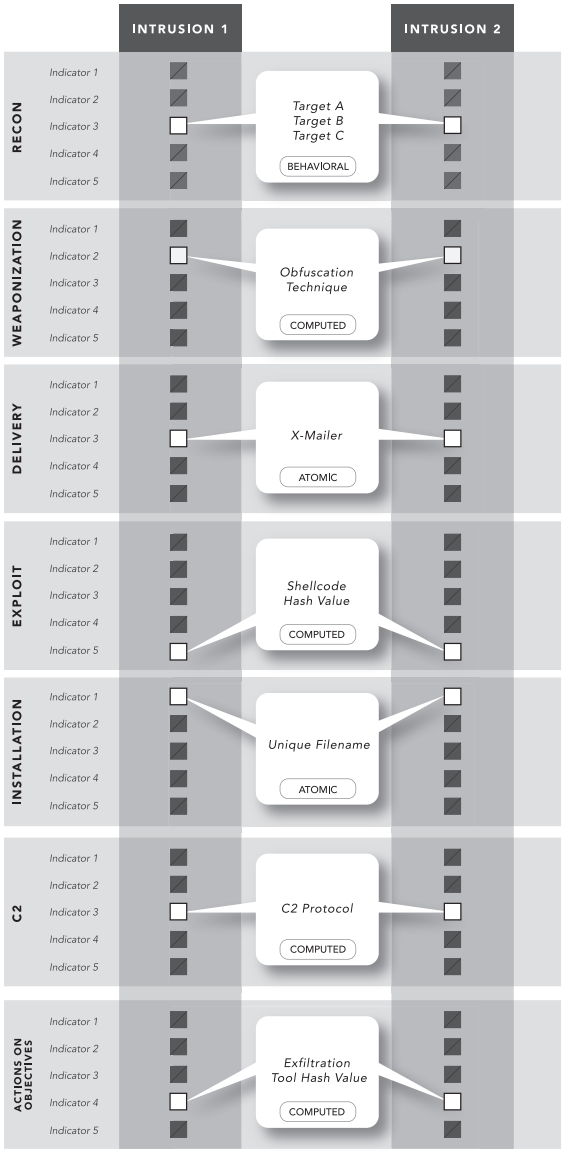

Figura 5: Los indicadores comunes entre las intrusiones

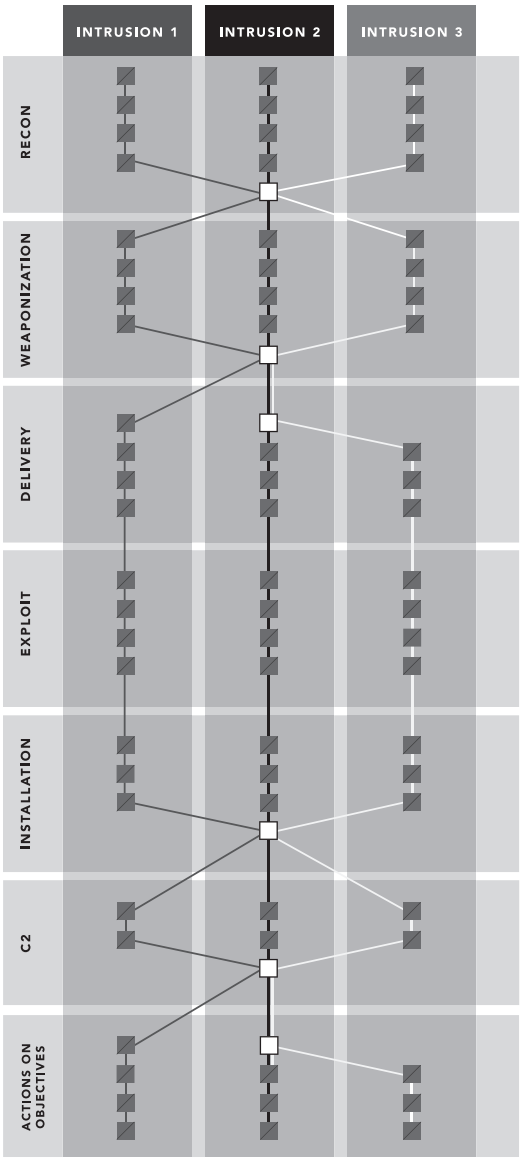

Figura 6: Campaña de indicadores clave

en una hoja de ruta para dar prioridad a las medidas de seguridad muy concretas para defender a estas personas, las redes o tecnologías.

4 Estudio de caso

Para ilustrar el beneficio de estas técnicas, un estudio de casos observados por el Equipo de Respuesta a Incidentes Lockheed Martin ordenador (LM-CIRT), en marzo de 2009, de tres intentos de intrusión por un adversario que se considera. A través del análisis de las cadenas de intrusión matar y robusta madurez indicador, los defensores de red detectada con éxito y mitigados una intrusión aprovechar una vulnerabilidad de “día cero”. Todos los tres intrusiones apalancados una táctica APT común: objetivo de correo electrónico malicioso (TME) entregado a un conjunto limitado de individuos, que contiene un archivo adjunto en armas que se instala una puerta trasera que inicia las comunicaciones salientes a un servidor de C2.

4.1 Intento de intrusión 1

El 3 de marzo de 2009, LM-CIRT detecta un archivo adjunto sospechoso dentro de un correo electrónico de discutir una próxima Instituto Americano de Aeronáutica y Astronáutica de conferencia (AIAA). El correo electrónico afirma que es de una persona que legítimamente trabajó para AIAA, y fue dirigido a sólo 5 usuarios, cada uno de los cuales habían recibido similares TME en el pasado. Los analistas determinan el archivo adjunto malicioso, tcnom.pdf, sería explotar un conocido, pero sin parches, la vulnerabilidad en Adobe Acrobat Portable Document Format (PDF): CVE-2009-0658, documentada por Adobe el 19 de febrero de 2009 (Adobe, 2009), pero no se parcheado hasta marzo

10, 2009. Una copia de los encabezados de correo electrónico y seguimiento cuerpo.

> Recibido: (qmail 71864 invocada por uid 60001); Mar 03 Mar 2009 15:01:19 +0000 Recibido: desde [60.abc.xyz.215] por web53402.mail.re2.yahoo.com a través de HTTP; Mar 03 Mar 2009 07:01:18 -0800 (PST) Fecha: mar, 03 de Mar 2009 07:01:18 -0800 (PST) De: Anne E ... < dn ... etto@yahoo.com > Asunto: Comités técnicos Para AIAA: [ELIMINADO]
>
> Responder-a: dn ... etto@yahoo.com
> Mensaje-id: < 107017.64068.qm@web53402.mail.re2.yahoo.com > MIME-Version: 1.0
>
> X-Mailer: YahooMailWebService / 0.7.289.1
> Tipo de contenido: multipart / mixed; boundary = "Boundary_ (ID_Hq9CkDZSoSvBMukCRm7rsg)" X-YMail-OSG:
>
> Por favor, envíe una copia (fotocopias son aceptables) de esta forma, y una copia de la hoja de vida del candidato a: Comité Técnico AIAA nominaciones de 1801 Alexander Bell Drive, Reston, VA 20191. El número de fax es 703 / 264-
>
> Formulario 7551. También se puede enviar a través de nuestro sitio Web en el interior www.aiaa.org, AIAA, comités técnicos

Dentro del PDF en armas fueron otros dos archivos, un archivo PDF benigno y un ejecutable (PE) de instalación portátil de puerta trasera fi l. Estos archivos, en el proceso de emplazamiento de armas, se codifica utilizando un algoritmo trivial con una clave de 8 bits almacenada en la shellcode explotar. Al abrir el PDF, código shell explotando CVE-2009-0658 sería descifrar el binario de instalación, lo coloca en el disco como C: \ Documents and Settings \ [nombre de usuario] \ Configuración local \ fssm32.exe, e invocarlo. El código shell también podría extraer el PDF benigna y mostrarlo al usuario. Los analistas descubrieron que el PDF benigna era una copia idéntica de uno publicado en el sitio en AIAA http://www.aiaa.org/pdf/inside/tcnom.pdf, acciones adversario de reconocimiento revelador.

el instalador fssm32.exe sería extraer los componentes de puerta trasera incrustados dentro de sí mismo, ahorrando EXE y archivos como HLP C: \ Archivos de programa \ Internet Explorer \ IEUpd.exe y IEXPLORE.HLP. Una vez activo, la puerta trasera enviaría los datos de latido al servidor C2 202.abc.xyz.7 a través de peticiones HTTP válidos. Tabla 2 articula la ed fi identi, los indicadores correspondientes por fase. Debido al éxito mitigaciones, el adversario nunca se llevó a cabo acciones sobre los objetivos, por lo tanto, esa fase está marcada “N / A”.

Tabla 2: Intrusión Intento 1 Indicadores

Fase	indicadores
Reconocimiento	[Lista de destinatarios] Archivo Benigna: tcnom.pdf
armamentización	algoritmo de cifrado trivial: Clave 1
Entrega	dn ... etto@yahoo.com IP Aguas abajo: 60.abc.xyz.215 Asunto: Comités Técnicos AIAA [Cuerpo del correo electronico]
Explotación	CVE-2009-0658 [Shellcode]
Instalación	C: \ ... \ fssm32.exe C: \ ... \ IEUpd.exe C: \ ... \ IEXPLORE.HLP
C2	202.abc.xyz.7 [petición HTTP]
Acciones sobre los objetivos	N / A

4.2 Intrusión Intento 2

Un día más tarde, fue ejecutado otro intento de intrusión TME. Los analistas identificarían características sustancialmente similares y vincular este intento y el día anterior para una campaña común, pero los analistas también tomó nota de una serie de di ff erences. Las características habilitadas repetidas defensores para bloquear esta actividad, mientras que las nuevas características proporcionan los analistas de inteligencia adicional para construir resiliencia con otros cursos de detección y mitigación de acción.

> Recibido: (qmail 97721 invocada por uid 60001); 4 Mar 2009 14:35:22 -0000 Message-ID: <
> 552620.97248.qm@web53411.mail.re2.yahoo.com >
> Recibido: desde [216.abc.xyz.76] por web53411.mail.re2.yahoo.com a través de HTTP; Mie 04 Mar 2009 06:35:20 PST
>
> X-Mailer: YahooMailWebService / 0.7.289.1 Fecha: Miér 4 Mar 2009
> 06:35:20 -0800 (PST) De: Anne E ... < dn ... etto@yahoo.com >
> Responder a: dn. ..etto @ yahoo.com
>
> Asunto: Conferencia defensa del misil séptimo Anual US A: [EXPURGADO]
> MIME-Version: 1.0
>
> Content-Type: multipart / mixed; boundary = "= 0-760892832-1236177320: 97.248"
>
> Bienvenido a la 7ª Conferencia Anual de Defensa de Misiles de EE.UU.

La dirección de correo electrónico enviando era común tanto a la actividad de marzo de 3 y 4 de marzo, pero la materia, la lista de destinatarios, nombre del archivo adjunto, y lo más importante, la dirección IP aguas abajo (216.abc.xyz.76) difería. El análisis del PDF adjunto, MDA_Prelim_2.pdf, revelado un algoritmo idéntico cifrado emplazamiento de armas y la clave, así como shellcode idéntica a explotar la misma vulnerabilidad. El instalador PE en el PDF fue idéntico al usado el día anterior, y el PDF benigna fue una vez más una copia idéntica de un expediente en el sitio web de la AIAA (http://www.aiaa.org/events/missiledefense/MDA_Prelim_09.pdf). El adversario nunca se llevó a cabo acciones hacia sus objetivos, por lo tanto, esa fase se marcó de nuevo “N / A”. Un resumen de los indicadores de los primeros dos intentos de intrusión se proporciona en la Tabla 3.

Tabla 3: Intrusión Intentos 1 y 2 Indicadores

Fase	Intrusión 1	Intrusión 2
Reconocimiento	[Lista de destinatarios] Archivo Benigna: tcnom.pdf	[Lista de destinatarios] Archivo Benigna: MDA_Prelim_09.pdf
armamentización	algoritmo de cifrado trivial: Clave 1	
Entrega	IP aguas abajo: 60.abc.xyz.215 Asunto: Comités Técnicos AIAA [Cuerpo del correo electronico]	IP aguas abajo: 216.abc.xyz.76 Asunto: 7º Anual de Defensa de Misiles Conferencia [Cuerpo del correo electrónico]
	dtto@yahoo.com dn ...	
Explotación	CVE-2009-0556 [Shellcode]	
Instalación	C: \ ... \ fssm32.exe C: \ ... \ IEXPLORE.HLP C: \ ... \ fssm32.exe C: \ ... \ IEUpd.exe C: \ ... \ IEXPLORE.HLP	
C2	202.abc.xyz.7 [petición HTTP]	
Acciones sobre los objetivos	N / A	N / A

4.3 Intento de intrusión 3

Más de dos semanas después, el 23 de marzo de 2009, un significativamente di ff Erent intrusión fue identi fi cado debido a la superposición indicador, aunque mínimo, con intrusiones 1 y 2. Este correo electrónico contiene un PowerPoint fi l que explotaba una vulnerabilidad que no lo era, hasta ese momento, conocida a los defensores de los proveedores o de red. La vulnerabilidad fue reconocido públicamente 10 días más tarde por Microsoft como aviso de seguridad 969136 e identi fi cado como CVE-2009-0556 (Microsoft, 2009b). Microsoft publicó un parche el 12 de mayo de 2009 (Microsoft, 2009a). En esta campaña, el adversario hizo un cambio signi fi cativo en el uso de una marca nueva, “día cero” explotar. Los detalles del seguimiento de correo electrónico.

> Recibido: (qmail 62698 invocada por uid 1000); Lun 23 Mar 2009 17:14:22 +0000 Recibido: (qmail 82085 invocada por uid 60001); Lun 23 Mar 2009 17:14:21 +0000 Recibido: desde [216.abc.xyz.76] por web43406.mail.sp1.yahoo.com a través de HTTP; Lun 23 Mar 2009 10:14:21 -0700 (PDT) Fecha: Lun 23 Mar 2009 10:14:21 -0700 (PDT) De: Ginette C ... < ginette.c ... @ yahoo.com > Asunto: Celebridades sin maquillaje a: [redactado]
>
> Mensaje-id: < 297350.78665.qm@web43406.mail.sp1.yahoo.com > MIME-Version: 1.0
>
> X-Mailer: YahooMailClassic / 5.1.20 YahooMailWebService / 0.7.289.1 Content-type: multipart / mixed; boundary = "Boundary_ (ID_DpBDtBoPTQ1DnYXw29L2Ng)"
>
> <Cuerpo del correo electrónico en blanco>

Este correo electrónico contiene una nueva dirección de envío, la nueva lista de destinatarios, marcadamente di ff Erent contenido benigna se muestra al usuario (de “defensa antimisiles” a “maquillaje de famosos”), y el archivo adjunto malicioso de PowerPoint contenía un exploit completamente nuevo. Sin embargo, los adversarios utilizan la misma dirección IP aguas abajo,
216.abc.xyz.76, para conectarse al servicio de correo web como solían en Intrusos 2. La fi PowerPoint le fue en armas usando el mismo algoritmo que los dos intrusiones anteriores, pero con una llave di ff Erent de 8 bits. El instalador PE y de puerta trasera se encontró que eran idénticas a las dos intrusiones anteriores. Un resumen de los indicadores de los tres intrusiones se proporciona en la Tabla 4.

Aprovechando la inteligencia de adversarios en los defensores de red habilitados primer intento de evitar la intrusión de un conocido de día cero explotar. Con cada intento de intrusión consecutivo, a través de análisis completo, se descubrieron más indicadores. Un sólido conjunto de líneas de acción para mitigar los defensores habilitado subsecuente

Tabla 4: Intrusión Intentos 1, 2, y 3 Indicadores

Fase	Intrusión 1	Intrusión 2	Intrusión 3
Reconocimiento	[Lista de destinatarios] benigna PDF	[Lista de destinatarios] benigna PDF	[Lista de destinatarios] benigna PPT
armamentización	algoritmo de cifrado algoritmo de		
	Tecla 1		clave 2
Entrega	[Asunto del correo electrónico] [Cuerpo del correo electrónico]	[Asunto del correo electrónico] [Cuerpo del correo electrónico]	[Asunto del correo electrónico] [Cuerpo del correo electrónico]
	dtto@yahoo.com dn ...		ginette.c ... @ yahoo.com
	60.abc.xyz.215	216.abc.xyz.76	
Explotación	CVE-2009-0658 [Shellcode]		[PPT 0-día] [shellcode]
Instalación	C: \ ... \ fssm32.exe C: \ ... \ EXPLORE.HLP		
C2	202.abc.xyz.7 [petición HTTP]		
Acciones sobre los objetivos	N / A	N / A	N / A

intrusiones momento de la entrega, incluso cuando adversarios desplegado una previamente no vista explotan. Además, a través de este enfoque diligente, defensores obligaron al adversario para evitar todos los indicadores maduros para lanzar con éxito una intrusión de ahí en adelante.

Siguiendo la metodología de respuesta a incidentes convencional puede haber sido e ff reflexivo en la gestión de sistemas comprometidos por estas intrusiones en entornos completamente bajo el control de los defensores de la red. Sin embargo, esto no habría mitigado el daño causado por un activo móvil comprometida que se moviera fuera del entorno protegido. Además, al centrarse sólo en post-compromiso ECTS e ff (los que después de la fase de Exploit), un menor número de indicadores están disponibles. Simplemente usando una puerta trasera Erent di ff e instalador podría eludir las detecciones y mitigaciones disponibles, lo que permite el éxito adversario. Al impedir compromiso en el lugar primero, el riesgo resultante se reduce de una manera inalcanzable a través del proceso de respuesta a incidentes convencional.

5 Resumen

defensa de la red informática de inteligencia impulsada es una necesidad a la luz de las amenazas persistentes avanzadas. Como convencional, centrado procesos de vulnerabilidad-son insu fi ciente, la comprensión de la amenaza en sí, su intención, la capacidad, la doctrina, y los patrones de funcionamiento se requiere para establecer la capacidad de recuperación. La cadena de intrusión kill proporciona una estructura para analizar intrusiones, extraer indicadores y conducir cursos defensivas de acciones. Por otra parte, este modelo da prioridad a la inversión de los vacíos de capacidad, y sirve como marco de referencia para medir el cacia e ff de las acciones de los defensores. Cuando los defensores consideran que el componente de amenaza de riesgo para aumentar la resistencia contra las APT, pueden convertir la persistencia de estos actores en un pasivo, lo que disminuye la probabilidad de que el adversario de éxito con cada intento de intrusión.

La cadena de destrucción muestra una asimetría entre agresor y defensor, cualquier componente repetido por el agresor es un pasivo. La comprensión de la naturaleza de la repetición para los adversarios dado, ya sea por conveniencia, las preferencias personales, o la ignorancia, es un análisis de costo. Modelización de la relación t fi coste-beneficio a los intrusos es un área para la investigación adicional. Cuando ese coste-beneficio es decididamente desequilibrada, es tal vez un indicador de la superioridad de la información de un grupo sobre otro. Modelos de superioridad de la información puede ser valiosa para el ataque a la red informática y el desarrollo de la doctrina explotación. Finalmente, este documento presenta un modelo de cadena de intrusiones kill en el contexto de espionaje ordenador. Intrusiones pueden representar un problema más amplio de clase. Esta investigación puede solaparse fuertemente con otras disciplinas, como contramedidas IED.

referencias

Adobe. APSA09-01: Actualizaciones de seguridad disponibles para Adobe Reader y Acrobat de la versión 9 y anteriores, Febrero de 2009. URL http://www.adobe.com/support/security/advisories/apsa09-01.html.

F. Duran, SH Conrad, GN Conrad, DP Duggan, y EB retenida. La construcción de un sistema de información privilegiada de Seguridad. *IEEE Seguridad y Privacidad,* 7 (6): 30-38, 2009. doi: 10.1109 / MSP.2009.111. Keith Epstein y Ben Elgin. Red de infracciones de seguridad plaga de la NASA, de noviembre de 2008. URL http: //www.businessweek.com/print/magazine/content/08_48/b4110072404167.htm.

LTC Ashton Hayes. La defensa contra el desconocido: Antiterrorismo y el ciclo de planificación del Terrorismo. *los Guardián,* 10 (1): 32-36, 2008. URL http://www.jcs.mil/content/files/2009-04/041309155243_ spring2008.pdf.

Bryan Krekel. La capacidad de la República Popular de China a realizar un Ciber Guerra y Computadora Red de Explotación, de octubre de 2009. URL http://www.uscc.gov/researchpapers/2009/ NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved% 20Report_16Oct2009.pdf.

James Andrew Lewis. Enfoques holísticos a la seguridad cibernética para habilitar la Red de Operaciones Centrales, abril 2008. URL http://armedservices.house.gov/pdfs/TUTC040108/Lewis_Testimony040108.pdf.

Mandiant. M-Trends: La amenaza persistente avanzada, enero de 2010. URL http: //www.mandiant. com / productos / servicios / M-tendencias.

Microsoft. Boletín de seguridad de Microsoft MS09-017: Una vulnerabilidad en Microsoft PowerPoint o fi cina se pudo Permitir la ejecución remota de código (967340), 2009a mayo. URL http://www.microsoft.com/technet/ seguridad / boletín / ms09-017.mspx.

Microsoft. Informativo sobre seguridad de Microsoft (969136): Una vulnerabilidad en Microsoft o fi cina PowerPoint podrían Permitir la ejecución remota de código, Abril 2009b. URL http://www.microsoft.com/technet/security/ asesoramiento / 969136.mspx.

Sarandis Mitropoulos, Dimitrios Patsosa, y Christos Douligeris. Sobre el manejo y respuesta a incidentes: Un enfoque del estado de la técnica. *Computadoras y Seguridad,* 5: 351-370, julio de 2006. URL http://dx.doi.org/ 10.1016 / j.cose.2005.09.006.

Instituto Nacional de Estándares y Tecnología. Special Publication 800-61: Incidente de seguridad informática Guía de manipulación, de marzo de 2008. URL http://csrc.nist.gov/publications/PubsSPs.html.

Consejo nacional de investigación. Contrarrestar la amenaza de artefactos explosivos improvisados: Investigación Básica Oportunidades (abreviado versión), 2007. URL http://books.nap.edu/catalog.php?record_id= 11953.

T. Sakuraba, S. Domyo, Bin-Hui Chou, y K. Sakurai. Exploración de las contramedidas de seguridad a lo largo de la secuencia de ataque. En *Proc. En t. Conf. Seguridad de la Información e ISA Aseguramiento de 2008,* páginas 427-432, 2008. doi: 10.1109 / ISA.2008.112.

Alex Stamos. “Aurora” Recomendaciones de respuesta, de febrero de 2010. URL https: //www.isecpartners. com / archivos / iSEC_Aurora_Response_Recommendations.pdf.

John A. Tirpak. Encontrar, arreglar, Pista, seleccionar, enfrentar Evaluar. *Aire Force Magazine,* 83: 24-29, 2000. URL http: //www.airforce-magazine.com/MagazineArchive/Pages/2000/July%202000/0700find.aspx.

UK-NUSCC. Nacional de Infraestructura Centro de Coordinación de la Seguridad: Targeted Troya ataques de correo electrónico, Junio de 2005. URL https://www.cpni.gov.uk/docs/ttea.pdf.

Entrenamiento del Ejército de Estados Unidos y el Comando de Doctrina. Una guía militar al terrorismo en la vigésima primera Siglo, agosto de 2007. URL http://www.dtic.mil/srch/doc?collection=t3&id=ADA472623.

US-CERT. Técnica de Seguridad Cibernética Alerta TA05-189A: Targeted Troya ataques de correo electrónico, de julio de 2005. URL http://www.us-cert.gov/cas/techalerts/TA05-189A.html.

Estados Unidos-China Económico y Comisión de Revisión de Seguridad. 2008 Informe al Congreso de la Comisión Económica y de Seguridad Estados Unidos-China, de noviembre de 2008. URL http://www.uscc.gov/annual_ informe / 2008 / annual_report_full_08.pdf.

Estados Unidos-China Económico y Comisión de Revisión de Seguridad. 2009 Informe al Congreso de la Comisión Económica y de Seguridad Estados Unidos-China, de noviembre de 2009. URL http://www.uscc.gov/annual_ informe / 2009 / annual_report_full_09.pdf.

Departamento de Defensa estadounidense. Publicación Conjunta 3-13 Operaciones de Información, de febrero de 2006. URL http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf.

Departamento de Defensa estadounidense. Publicación Conjunta 3-60 Targeting conjunta, de abril de 2007. URL http: //www.dtic. mil / doctrine / new_pubs / jp3_60.pdf.

Robert Willison y Mikko Siponen. La superación de la información privilegiada: la reducción del crimen informático empleado situacional a través de la prevención del delito. *Communications of the ACM,* 52 (9): 133-137, 2009. doi: http://doi.acm.org/10.1145/1562164.1562198.