Metodología para el análisis de incidentes de ciberseguridad o ciberataques durante las acciones de ciberdefensa de las infraestructuras críticas de la defensa nacional – infoscopia –

Director de Proyecto: Julio C. Liporace[a] jcliporace@est.iue.edu.ar

Adrián Buscaglia[a] abuscaglia@est.iue.edu.ar

Pablo Croci[a] pcroci@est.iue.edu.ar

Nicolás Díaz Pais[a] ndiazpais@est.iue.edu.ar

Darío Fernández[a] dfernandez@est.iue.edu.ar

Verónica Ferreyra[c] vferreyra@fuerzas-armadas.mil.ar

Ignacio Martín Gallardo[ab] igallardo@est.iue.edu.ar

Elvira Quiroga[ab] equiroga@est.iue.edu.ar

Fernando Vera Batista[a] verabatista@est.iue.edu.ar

César D. Cicerchia[a] cdcicerchia@est.iue.edu.ar

a. Facultad de Ingeniería del Ejército (FIE), Ejército Argentino – Universidad de la Defensa Nacional

b. Centro de Investigación y Desarrollo de Sistemas Operacionales (CIDESO), Dirección General de Investigación y Desarrollo (DIGID) - Ejército Argentino

c. Comando Conjunto de Ciberdefensa (CCCD), Estado Mayor Conjunto de las Fuerzas Armadas

RESUMEN

El desarrollo actual de la Ciberseguridad y la Ciberdefensa está apoyado en el empleo de procedimientos reactivos de detección, mitigación y remediación, que se aplican cuando el efecto de la agresión sobre una Infraestructura Crítica del Sistema de Defensa Nacional (ICSDN) ya ocurrió. Se ha adoptado un enfoque derivado de las normativas de Seguridad de la Información, como las formuladas por el estándar internacional ISO/IEC 27000. El aporte original de esta línea de investigación se basa en proponer una nueva metodología de Ciberdefensa, desarrollando un abordaje proactivo hacia las amenazas antes que éstas comprometan la infraestructura crítica, a fin de sorprender al agresor mediante una defensa dinámica y reducir sus posibilidades de éxito.

Las líneas de investigación de InFoscopia tienen como alcance desarrollar una metodología proactiva de análisis de eventos que ocurren antes de que el objetivo cibernético haya sido comprometido. Se enfocará en las ICSDN estratégicas (servicios esenciales de energía, transporte, financieros, comunicaciones e informática, alimentos, agua, químicos, nuclear o espacial) y de capacidades militares.

Contribuirá al desarrollo de procedimientos proactivos por parte de los grupos de respuesta del tipo Computer Security Incident Response Team (CSIRT) o Centro de Operaciones de Ciberdefensa, encargados de la protección de las ICSDN.

Palabras Clave: *Informática Forense. Informatoscopia. Ciberseguridad. Ciberdefensa. Ciberataque. Infraestructura Crítica.*

CONTEXTO

La reciente Directiva de Política de Defensa Nacional [1] destaca que, en la atención del riesgo de "Ataques externos a objetivos estratégicos", el Sistema de Defensa Nacional debe focalizarse en "aquellas infraestructuras cuyo funcionamiento resulte crítico para el cumplimiento de las funciones vitales del Estado Nacional, su Defensa Nacional, el ejercicio de la soberanía y el resguardo de la vida y la libertad de sus habitantes."

El Ejército Argentino (EA), desde hace veinte años patrocina la construcción de su propio sistema de comando y control (SC2) para sus brigadas. Los SC2 son de naturaleza socio – técnica y complejos en su concepción y diseño (Clay, 2007). Por sus características y su finalidad de empleo, constituyen una ICSDN (Dean, 2013). Por otra parte, el EA ha proporcionado los recursos humanos formados como

[1] Decreto 703/2018. DECTO-2018-703-APN-PTE - Directiva de Política de Defensa Nacional. Aprobación. https://www.boletinoficial.gob.ar/pdf/pdfAnexoPrimera/5568234A01.pdf/20180731/0

Ingenieros Militares o en Sistemas de Computación, para la creación y constitución del Comando Conjunto de Ciberdefensa[2].

En base a estos antecedentes, el grupo de trabajo del proyecto InFoscopia es responsable de abordar esta línea de investigación. Para su organización ha recibido el aporte de conocimiento de docentes y graduados de la Especialización en Criptografía y Seguridad Teleinformática y de Ingeniería en Informática, ambas carreras de la misma unidad académica. Asimismo, los docentes son investigadores categorizados con trayectoria en otros proyectos de investigación de la FIE o docentes con experiencia en investigación aplicada al desarrollo tecnológico precompetitivo de sistemas militares.

InFoscopia es un proyecto acreditado por el Programa de Acreditación y Financiamiento de Proyectos UNDEFI, convocado mediante Resolución Rectoral 154/18 de la Universidad de la Defensa Nacional (UNDEF). El financiamiento del proyecto está sustentado por parte de la FIE, mediante la asignación de cargos y horas de investigación de los docentes integrantes del grupo de trabajo, y de la UNDEF, por medio de un subsidio UNDEFI que se renueva anualmente.

Durante las actividades de investigación se intercambiarán conocimientos y experiencias con los siguientes grupos de investigación: Grupo de Investigación del CriptoLAB de la FIE / UNDEF; Grupo de Investigación Sistemas Operativos e Informática Forense de la Facultad de Ingeniería de la Universidad FASTA (sede Mar del Plata).

Por su parte, La Facultad de Ingeniería del Ejército, así como la Facultad de Ingeniería de la Universidad FASTA son miembros fundadores de la Red Universitaria de Informática Forense (UNIF). Esta red constituye un apoyo fundamental para el Grupo de Investigación.

1. INTRODUCCIÓN

Las Infraestructuras Críticas del Sistema de Defensa Nacional (ICSDN) constituyen recursos diversos y complejos, aunque en la actualidad todas tienen uno o más componentes de TIC (Edwards, 2014). Desde la perspectiva del Estado, se debe considerar una infraestructura como aquel conjunto de medios técnicos, servicios e instalaciones necesarios para el desarrollo de las actividades básicas de la sociedad. En este sentido, la mayoría de esas actividades proveen servicios esenciales de carácter estratégico a la sociedad, al gobierno y a los habitantes en su conjunto, tanto sean prestados por organizaciones de gestión pública como privada (Baggett & Simpkins, 2018).

La interrupción o perturbación severa de su funcionamiento, ocasionaría graves efectos sobre el normal desarrollo de las actividades básicas de la sociedad; por tal motivo deben ser consideradas infraestructuras críticas y su defensa, aún en tiempo de paz, es un deber fundamental del Estado. La componente TIC de cualquier ICSDN puede ser afectada desde el Ciberespacio, con un elevado y creciente riesgo que debe ser analizado y prevenido frente a un número importante de amenazas cibernéticas, cuyo comportamiento es dinámico, cambiante y de difícil predicción (Johnson, 2015).

Las amenazas cibernéticas progresan en su acción ofensiva, evolucionando entre las siguientes etapas (The Mitre Corporation, 2018):

- Exploración o Reconocimiento inicial.
- Adquisición intrusiva de servicios o procesos computacionales de la infraestructura / Desarrollo de herramientas acordes a la debilidad a ser explotada.

[2] http://www.fuerzas-armadas.mil.ar/Dependencias-CIBDEF.aspx

- Entrega o distribución
- Compromiso Inicial.
- Uso indebido / Escalamiento de Privilegios.
- Reconocimiento interno.
- Movimiento lateral.
- Establecimiento de la persistencia (consolidación).
- Ejecución de la Misión o cumplimientos de Objetivos.
- Exfiltración.

El conocimiento tecnológico que proporciona la Informática Forense, la Informatoscopia y su apoyo en las Ciencias de la Computación tiene su campo de aplicación en la Justicia (Consejo General del Poder Judicial (CGPJ) et al., 1996). Esta capacidad se sustenta en el empleo de técnicas científicas y analíticas especializadas sobre la infraestructura tecnológica y se desarrolla con la finalidad de identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal, en el marco de un delito informático que es objeto de investigación judicial. Es decir que estas disciplinas actúan *ex post*, luego de ocurrido un delito (Domínguez, 2013).

En la Ciberdefensa tienen prioridad la mitigación, contención o respuesta inmediata para detener los efectos de una ciberagresión o ciberataque, manteniendo el objetivo de la recolección de evidencias de la vulneración de los sistemas y preservar las pruebas, pero dejándolo en segundo orden de prioridad (Intelligence and National Security Alliance (INSA), 2018). Sin embargo, los métodos y herramientas de la Informática Forense pueden resultar de utilidad para apoyar el proceso de gestión de incidentes de Ciberseguridad y Ciberdefensa, pero bajo otra metodología enfocada en una acción proactiva, antes que el efecto de la agresión llegue a su punto culminante (Colbaugh & Glass, 2011).

La explotación del análisis forense digital y su capacidad de extraer muestras o pruebas de las computadoras, equipos móviles y otros dispositivos es fundamental para descubrir e interpretar datos electrónicos.

Un componente de soporte al desarrollo de la metodología es la "línea de tiempo" que permite mostrar quién hizo, qué y cuándo, de manera de poder afirmar de forma concluyente que la Acción A causó el Resultado B (Amusategui López, 2016).

2. LÍNEAS DE INVESTIGACIÓN Y DESARROLLO

Se identifican dos líneas principales de investigación de interés para InFoscopia; a saber:

- Análisis de amenazas cibernéticas y de tendencias de ciberagresiones a infraestructuras críticas estratégicas, para modelar el comportamiento de agresores cibernéticos que puedan afectar, especialmente, la disponibilidad[3] de las infraestructuras críticas.
- Métodos de análisis forense digital en memoria, de ingeniería inversa de software y de análisis de malware, que puedan extenderse o aplicarse para estudiar procesos "vivos" en dispositivos de datos, red, seguridad informática o soporte. Se consideran de interés para elaborar un conjunto de Indicadores de Amenaza (*Indicators of Threat* - IoTh), por analogía a los Indicadores de Compromiso (*Indicators of Compromise* - IoC).

Para este proyecto, la primera línea de investigación resulta de interés para el modelado del comportamiento del agresor cibernético, especialmente en las etapas previas del ciberataque

[3] *Availability*, adoptada por el estándar internacional ISO/IEC 27000. Se refiere a la "propiedad de la información [o de un sistema] de estar accesible y utilizable cuando lo requiera una entidad autorizada".

(exploración o reconocimiento inicial, adquisición intrusiva de servicios o procesos computacionales de la infraestructura, desarrollo de herramientas ofensivas acordes a la debilidad a ser explotada) y en momento inicial del asalto a la infraestructura, cuando empieza la entrega o distribución de una ciberarma (malware, tramas anómalas de datos, etc).

La segunda línea de investigación tiene interés, entre otros puntos, sobre los métodos de recolección de información disponibles para archivos dependientes de la memoria RAM, como ser la RAM propiamente dicha y el archivo de paginación de los sistemas operativos. También, el análisis de artefactos o piezas de software en tiempo de ejecución, los procesos desatados por el malware o software dañino y el análisis de tráfico en la red, desde y hacia el activo comprometido. Se pretende analizar y comprender eventos en tiempo de ejecución para clasificarlos como normales o anómalos con un grado de confianza aceptable.

El proyecto tiene previsto tres etapas:

- Formulación metodológica para activos bajo entornos Windows en redes Ethernet proponiendo indicadores de amenazas a la disponibilidad. Se validará con pruebas de concepto.
- Ampliación de la metodología para ambientes heterogéneos con dispositivos Linux y medios de redes y seguridad particulares de infraestructuras críticas. Se desarrollará un prototipo experimental.
- Se completará con la experimentación y selección de parámetros definitivos de los indicadores de amenazas definidos.

3. RESULTADOS OBTENIDOS/ESPERADOS

El principal resultado esperado es desarrollar una metodología propia de análisis de eventos o incidentes aplicable a las fases iniciales de una ciberagresión o ciberataque que pudiera ocurrir en uno o más activos esenciales de una ICSDN, con la finalidad de dar respuesta a los siguientes propósitos:

- Detectar cómo y cuándo ocurrió una violación de la protección de una ICSDN.
- Identificar los activos esenciales o sistemas comprometidos y afectados.
- Determinar qué atacantes tomaron o cambiaron procesos.
- Contener y remediar los incidentes que se configuren.
- Desarrollar indicadores y fuentes clave de inteligencia de amenazas.
- Buscar violaciones adicionales usando el conocimiento de las tácticas, técnicas y procedimientos del agresor.

Con respecto a la primera línea, se ha comenzado por adoptar como referencia el marco de trabajo MITRE's Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK), desarrollada y mantenida por la organización estadounidense The Mitre Corporation. Se trata de una base de conocimiento accesible a nivel mundial, sobre tácticas, técnicas y procedimientos que utilizan los agresores cibernéticos.

Entre los primeros resultados de la segunda línea de investigación, por medio del empleo de varias herramientas forenses de análisis de memoria de computadoras con arquitectura *Von Neumann*, se logró validar la técnica de obtención de datos residentes en memoria para el análisis de cadenas de caracteres presentes en tiempo de ejecución. Como continuación de este trabajo, mediante la utilización de la herramienta *Sysmon* (de la suite *Sysinternals* de Microsoft) se pretende estudiar el comportamiento de los activos bajo condiciones normales de operación y compararlos con los efectos de eventos asociados a la fase previa de los ciberataques. La finalidad es obtener información detallada sobre las creaciones de procesos, conexiones de red y cambios en el tiempo de creación de archivos. Al recopilar los eventos que se generan, se podrá realizar el análisis en vivo de los *Logs* para identificar actividades anómalas y comprender cómo operan los intru-

sos y el *malware* en la red de una infraestructura crítica, de manera de encontrar posibles Indicadores de Amenazas (IoTh) en un momento previo al compromiso de la disponibilidad del activo (*weaponization* en el *framework* PRE-ATTACK de Mitre).

4. FORMACIÓN DE RECURSOS HUMANOS

El Grupo de Investigación tiene conocimientos y experiencia sobre Informática Forense, Ciberseguridad, Ciberdefensa, Redes de Información, Sistemas Operativos, Sistemas de Control, Sistemas Electrónicos, Ingeniería de Software y Programación.

La estructura del equipo de trabajo está conformada por dos docentes e investigadores del posgrado de Especialización en Criptografía y Seguridad Teleinformática, tres docentes e investigadores de Ingeniería en Informática. Además, un tecnólogo posgraduado en la especialización mencionada, con dos tesis de posgrado aprobadas, vinculadas al proyecto; actualmente, realiza el Doctorado en Ciencias Informáticas con tesis afín al proyecto. El grupo se completa con dos tecnólogos especializados en sistemas operativos y redes de computadoras, y un tercer tecnólogo con experiencia en incidentes de ciberseguridad. A partir de este año, se han incorporado dos alumnos de la carrera de Ingeniería en Informática y uno de Ingeniería Electrónica que desarrollarán tesinas de grado vinculadas al proyecto.

La formación de recursos humanos es un objetivo del proyecto y está reflejado en la constitución del grupo, donde se integran los conocimientos de docentes muy experimentados y jóvenes, alumnos de ingeniería, personal técnico y tecnólogos de tres laboratorios asociados al proyecto (CriptoLab y CIDESO / Ejército; InFo-Lab / Universidad FASTA). Por último, se previeron otorgar becas de doctorado, postgrado y grado e incorporar pasantes en el marco de la Red UNIF.

5. BIBLIOGRAFÍA

Amusategui López, J. M. (22 de Dic de 2016). *Universitat Oberta de Catalunya.* Obtenido de http://openaccess.uoc.edu/webapps/o2/bitstream/10609/60765/6/jamusateguiTFM1216memoria.pdf

Baggett, R. K., & Simpkins, B. K. (2018). *Homeland Security and Critical Infrastructure Protection, 2nd Edition.* Santa Barbara, California. USA: Praeger Security International.

Clay, W. (2007). *Network Centric Operations: Background and Oversight Issues for Congress.* CRS Report for Congress.

Colbaugh, R., & Glass, K. (15 de Ago de 2011). *IEEE Xplore Digital Library.* (P. o. Informatics, Ed.) doi:10.1109/ISI.2011.5984062

Consejo General del Poder Judicial (CGPJ) et al. (31 de Dic de 1996). *CITA.ES.* Obtenido de http://cita.es/apedanica/INFORMAT.HTM

Dean, S. E. (2013). *Cyber Defense: Securing Military Systems and Critical Civilian Infrastructure from an Electronic 9/11.* Hampton Roads International Security Quarterly.

Domínguez, F. L. (2013). *Introducción a la Informática Forense.* Madrid. España: Ra-Ma.

Edwards, M. (2014). *Critical Infraestructurre Protection.* Ankara, Turquía: IOS Pres BV.

Intelligence and National Security Alliance (INSA). (31 de Ago de 2018). *Intelligence and National Security Alliance.* Obtenido de https://www.insaonline.org/wp-content/uploads/2018/08/INSA-Managing-Cyber-Attack-Critical-Infrastructure.pdf

Johnson, T. A. (2015). *Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare.* St.Louis, Missouri. USA: CRC Press.

The Mitre Corporation. (22 de Nov de 2018). *MITRE ATT&CK*. Obtenido de https://attack.mitre.org/