UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE GUAYAQUIL

TRABAJO DE GRADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

INGENIERO DE SISTEMAS

CARRERA:

INGENIERÍA DE SISTEMAS

TEMA:

“INDICADORES DE COMPROMISO (IOC) PARA DETECCIÓN DE AMENAZAS EN LA SEGURIDAD INFORMÁTICA CON ENFOQUE EN EL CÓDIGO MALICIOSO”

AUTOR:

Ponce Larreátegui Jimmy Gregorio

TUTOR:

Msg. Joe Llerena Izquierdo

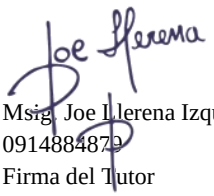
Abril 2021

GUAYAQUIL-ECUADOR

Declaratoria de Responsabilidad

Yo, Jimmy Ponce autor del artículo académico “Indicadores de Compromiso (IoC) para detección de amenazas en la Seguridad Informática con enfoque en el Código Malicioso” certifico que todo el contenido de esta investigación y las conclusiones es absoluta responsabilidad del autor.

Jimmy Ponce
C.I. 0918234923



Msig. Joe Llerena Izquierdo
0914884879
Firma del Tutor

INDICADORES DE COMPROMISO (IOC) PARA DETECCIÓN DE

AMENAZAS EN LA SEGURIDAD INFORMÁTICA CON ENFOQUE EN EL CÓDIGO MALICIOSO

Jimmy Ponce Larreategui[1][0000-0002-7759-6303], Darío Huilcapi Subia[1][0000-0003-4603-0566] and Joe Llerena Izquierdo[1][0000-0001-9907-7048]

[1]Universidad Politécnica Salesiana Sede Guayaquil, Ecuador
jponce@est.ups.edu.ec, dhuilcapi@ups.edu.ec,jllerena@ups.edu.ec

Abstract. Las amenazas informáticas evolucionan en el tiempo con ataques sofisticados, el vector de ataque más utilizado es la utilización de Malware para acceder a su objetivo sin autorización. El problema es que existen ataques llamados de Dia Cero (0days), no se tiene análisis previo del código por lo tanto los indicadores de compromiso (IoC) son menos efectivos; la nueva amenaza debe analizarse y generar los IoC. El objetivo es determinar la importancia de los Indicadores de Compromiso para minimizar los incidentes de seguridad de las infraestructuras informáticas en las organizaciones mediante reportes de plataforma de intercambio online. La metodología utilizada es la exploración de contenido documental relacionado a temas de Indicadores de Compromiso, la deducción y el uso de estadísticas de Malware más relevantes en el robo de información. Los resultados son: Análisis de los tipos de IoC para generación de niveles de impacto, Determinación de herramientas informáticas para el análisis de código, y Niveles de importancia de IoC para identificar el tipo de artefacto malicioso. Se concluye que los ciberdelincuentes siempre están un paso adelante, los ataques son más sofisticados y buscan formas de evadir la seguridad de las organizaciones; los IoC son efectivos, pero tienen sus limitaciones; en el análisis se obtuvo IoCs que permiten identificar por medio de los artefactos las amenazas para su posterior bloqueo; las herramientas mostradas nos permiten visualizar los indicadores para automatización y mejora en los tiempos de verificación; los niveles de importancia indica el impacto de una vulnerabilidad en el código malicioso que utiliza técnicas de explotación.

Keywords: Indicators of Commitment, Threat detection, Informatic security, Malicious code

1 Introducción

La evolución del Malware plantea un gran desafío porque los ataques son más sofisticados e identificar un malware conocido o desconocido es la piedra angular en la seguridad; los autores de malware utilizan diferentes técnicas de evasión para pasar desapercibidos y aumentar la efectividad del ataque; algunas firmas de antivirus reconocen que la cantidad de violaciones de seguridad va en aumento cada año. Los usuarios son las victimas principales del ciberdelincuente, los atacantes utilizan técnicas de Ingeniería social; los ciberdelincuentes para realizar estas actividades buscan siempre ocultar sus comunicaciones y su identidad para no ser descubiertos; por tal motivo siempre es

importante contar con plataformas de seguridad como Sistemas de Detección de Intrusos y antivirus de última generación para poder detectar malware moderno [1].

Gran parte del malware creado está dirigido al robo de datos importantes como números de tarjetas de crédito, contraseñas y aplicaciones bancarias; estos ataques son tan sigilosos que pasan por desapercibidos por los usuarios y una vez los atacantes tienen accesos a plataformas bancarias realizan transferencias no autorizadas; existen malware para computadores personales, dispositivos móviles y dispositivos de IoT [2].

El enfoque para la detección de código malicioso se divide en dos, uno basado en el comportamiento y otro basados en firmas; el análisis de malware se divide en dos clacificaciones: el análisis dinámico y análisis estático, con estos resultados se procede a generar los indicadores de compromiso (IoC); la generación de estos indicadores de compromiso ayuda a las empresas, organizaciones y gobiernos a detectar intrusiones por medio de malware [3].

Existen varios grupos en Internet conocidos como APT (Advanced Persistent Threat) que realizan ataques sofisticados dirigidos a empresas, estados y países, ellos roban todo tipo de información confidencial y secretos de estados; el espionaje corporativo es afectado por varias campañas de malware, aquí entran los indicadores de compromisos como una herramienta útil para la identificación y detección; la detección es parte del proceso de manejo de incidentes [4].

Este documento busca explicar de forma clara y la importancia que tienen los Indicadores de Compromiso en el mundo de la seguridad; las empresas venden productos o servicios por medio de Internet y por esta razón son un objetivo de ataque; las plataformas de intercambio de indicadores son muy importantes para los departamentos de seguridad de cada organización [3].

El problema es que existen ataques llamados de Dia Cero (0days), no se tiene análisis previo del código por lo tanto los IoC son menos efectivo; la nueva amenaza debe analizarse y generar los IoC.

Pregunta de hipótesis: ¿Por qué es necesario analizar indicadores de compromiso (IoC) para detectar amenazas en la Seguridad Informática con un enfoque en el Código Malicioso?

Para identificar y detectar el tipo de amenaza existente en la red se utiliza los IoC; el análisis del código y los Indicadores de Compromiso recolectados servirán para detecciones futuras de una misma familia de Malware; estos indicadores son compartidos en los grupos de intercambio abiertos de la comunidad.

El objetivo es determinar la importancia de los Indicadores de Compromiso para minimizar los incidentes de seguridad de las infraestructuras informáticas en las organizaciones mediante reportes de plataforma de intercambio online.

La metodología utilizada es la exploración de contenido documental relacionado a temas de Indicadores de Compromiso, la deducción, y se utiliza estadísticas de Malware más relevantes en el robo de información.

2 Materiales y Métodos

Los Indicadores de compromiso permiten identificar la presencia de malware; un IoC se activa e indica que existe un ataque en la infraestructura, ya sea por medio de una vulnerabilidad conocida o desconocida; pueden existir falsos positivos, por tal motivo el departamento de seguridad se encarga de evaluar la alerta de intrusión [5].

Importancia de IoC: Los IoC son una buena estrategia para identificar Malware porque están compuestos de firmas del virus, esto significa seleccionar piezas de código del propio virus para crear los IoC, además seleccionar dominios, direcciones web maliciosas o direcciones IPs que forman parte de la comunicación y administración del ataque con el objetivo de prevenir e identificar las amenazas. El Ransomware es el código malicioso que secuestra información a cambio de bitcoin por el rescate, entre los más frecuente están Ransom.Cryptolocker, Winlocker, Ransom.Locky, Cryptowall, Teslacrypt, Torrent-locker. El Ransonware afecta a varios sectores de la industria como educación 13%, sectores gubernamentales 23%, sectores financieros 13%, sectores sanitarios 3.5% y sectores públicos 3.4% [6].

Análisis estático y dinámico: Para generar un IoC a partir de un archivo malicioso se utiliza dos métodos conocidos como análisis estático y análisis dinámico; el análisis estático analiza malware sin ejecutarlo por medio de herramientas de desensamblado; los análisis dinámicos se ejecutan en VMs [7].

Plataformas de Intercambio de Indicadores de Compromiso:

Existen muchos esfuerzos para caracterizar las amenazas, los indicadores de compromiso y la remediación básica así como su intercambio utilizando STIX (Expresión Estructurada de Información de Amenazas) / TAXII (Intercambio automático de la Información de Inteligencia) y OTX (Open Threat Exchange) creado por la compañía AlienVault [8].

Se recopilaron IoC de artículos de ciberseguridad y se utilizó “Sequence Labelling Model”; este modelo propuesto recopila y administra la información contextual de textos; como resultado se obtuvo un puntaje del 89% de artículos de ciberseguridad en inglés y un 81.8% de artículos de ciberseguridad en chino [5].

Se realizó un enfoque de creación IoCs a través de la teoría de grafos, esta teoría modela sistemas complejos; la teoría de grafos ayuda a modelar cualquier tipo de ataque en red visualizándolo como un único IoC y no como un IoC individual; cada intrusión se agregas como un artefacto en el gráfico y además se agregan sistemas afectados como un servidor, un endpoint o un router [9–11].

Se desarrolló una herramienta llamada YARA para análisis de malware que se generan a partir de ingeniería inversa, las reglas se determinan por varios indicadores de compromiso; permite una detección efectiva de muestras de código malicioso; la automatización de herramientas como Yabin y yarGen mejoran la efectividad incorporando fuzzy hashing method SSDEEP [12].

Para crear este documento se realizaron lecturas de contenido documental relacionado a temas de Indicadores de Compromiso; los dominios en los que el Malware busca conectarse después de infectar el objetivo, así como sus respectivas IP y con estos datos compartirlos a las diferentes fuentes de Threat Intelligence abiertas.

3 Resultados

3.1 Análisis de los tipos de IoC para generación de niveles de impacto mediante las métricas de codificación

Los IoC son artefactos forenses recolectados de una intrusión que son identificados en la red, en un host o equipo; estos IoC ayudan a los profesionales a identificar cualquier tipo de amenazas que indican una brecha de seguridad por medio de una vulnerabilidad, y se recolecta mediante el proceso de análisis; la tabla 1 presenta los tipos de IoC.

Table 1. Tipos de indicadores de compromiso.

Referencia	Tipo	Descripción
[13]	Artefactos Basados en Red	Son recibidos desde servidores, puertos, proxy server, entre los artefactos recolectados tenemos: captura de paquetes, estado de la red y sesiones.
[13]	Artefactos Basados en Host.	Son recibidos desde el equipo, entre los artefactos recolectados tenemos: el registro del sistema y el sistema de archivos.
[14]	Artefactos Basados en Red / IPs	Identificar las IPs del comando y control son claves para identificar una conexión maliciosa.
[14]	Artefactos Basados en Red / URL	Identificar las URLs asociadas a una Botnet y sus IPs relacionadas es punto clave en la detección, para su posterior bloqueo.
[14]	Artefactos Basados en Red/ Puertos y Servicio	Servicios como DNS, HTTP, TCP, UDP, ICMP, FTP, SSH son analizados con sus puertos relacionados, la mayoría puertos altos.
[15]	Artefactos Basados en Host/ Registro	Generar los IoCs de los cambios en el registro (Persistencia) es señal de una computadora infectada
[15]	Artefactos Basados en Host/ Procesos	La revisión de los procesos en estado running es un indicador clave para la identificación de Malware en el sistema incluye revisión de spawning process tree, carga de DLLs y parámetros utilizados.

3.2 Determinación de herramientas informáticas para el análisis de código mediante técnicas estáticas y dinámicas

El análisis estático y dinámico son utilizados para generar los IoC que realiza ingeniería inversa del código malicioso y se utilizan herramientas que identifican direcciones IPs, dominios, creación de archivos, modificación del registro de Windows, entre otros; la tabla 2 presenta las herramientas de análisis.

Table 2. Herramientas y técnicas informáticas.

Referencia	Técnica	Herramienta	Descripción
[16]	Análisis Estático	IdaPro	IdaPro es un disassembler, realiza análisis estático y convierte un ejecutable a código máquina.

[16]	Análisis Estático	Dependency Walker	Dependency Walker escanea módulos de Windows de archivos exe, dll, sys y crea un diagrama de árbol jerárquico.
[17]	Análisis Dinámico	WinDBG	Este Debugger ejecuta código binario cuando no se dispone del código fuente.
[17]	Análisis Dinámico	Process Monitor	Process Monitor visualiza las actividades de un archivo, cambios de registros, procesos y actividades de la red.
[18]	Análisis Hibrido	VxStream Sandbox	Los Sandbox como VxStram realizan híbridos, durante la ejecución recopilan datos junto con un análisis estático importante en el volcado de memoria.
[19]	Análisis Hibrido	Andrubis	Adrubis realiza un análisis estático y todo lo toma como entrada para continuar con el análisis dinámico.

3.3 Niveles de importancia de IoC para identificar el tipo de artefacto malicioso mediante análisis de patrones de comportamiento

Las amenazas siempre evolucionan, después de realizar ataques tradicionales pasan a ser persistentes o llamadas también APT(Advanced Persistent Threat) que afectan a la industria, corporaciones, gobiernos y usuarios finales; en un informe creado por Mandiant comunica la existencia de APT China ha comprometido 141 empresas que abarcan 20 industrias principales [20].

La explotación de un aplicativo es producto de las vulnerabilidades, al ser descubiertas estas son documentadas y expuestas al público en general, a través del CVE (Common Vulnerabilities and Exposures); el CVE suministra un ID estándar para cada vulnerabilidad analizada; Los CVE contienen información limitada y podemos recurrir también a NVD (National Vulnerability Database) [21].

Los niveles de impacto los encontramos en el Common Vulnerability Scoring System (CVSS), se generan una puntuación numérica que refleja la severidad; esta puntuación también se representa de forma cualitativa (Baja, Media, Alta, Critica); CVSS ayuda a las organizaciones a priorizar los procesos de cada empresa en la gestión de vulnerabilidades [22].

El score del CVSS es un numero decimal de 0.0. a 10.0 y está compuesto por tres métricas que representan los atributos de una vulnerabilidad: métrica Base siempre son constantes en el tiempo y en el entorno de usuario; la métrica Temporal que cambian con el tiempo pero no en el entorno de usuario; la métrica de entorno son específicas y relevantes en el entorno de usuario [23].

CVSS v3 es la última versión lanzada en junio 2015 la diferencia con la versión 2 son los tipos de niveles de los parámetros de cada métrica; la métrica base está compuesta por las métricas de explotabilidad, impacto y alcance; La versión 2 está compuesta por 18 niveles y la versión 3 de 22 niveles, contamos con una calculadora web para realizar los cálculos [24].

4 Discusión

En el primer resultado se identifican los tipos de indicadores de compromiso, la clasificación ayuda al analista a identificar mejor los artefactos a recolectar; en el segundo resultado se conocen las herramientas utilizadas para la generación de estos artefactos y la creación del indicador; el tercer resultado da valor a las vulnerabilidades que a su vez son en mayor parte el núcleo del malware para la explotación y la prioridad para la generación de los IoC.

Todas las investigaciones citadas en este artículo concuerdan en la importancia y generación de los Indicadores de compromiso de un ataque; buscando formas de generar estos indicadores automáticamente utilizan incluso métodos como teorías de grafos y redes neuronales; la ayuda que proporciona estos IoC a los departamentos de seguridad son importantes para el manejo de incidentes.

En este artículo no se ha considerado el tiempo de implementación de laboratorios para el análisis de código malicioso; no se ha considerado costos de herramientas de análisis de pago; ni procedimientos que indiquen buenas prácticas para el análisis de Malware.

5 Conclusiones

Se concluyó que los ciberdelincuentes siempre están un paso adelante, los ataques son más sofisticados y buscan formas de evadir la seguridad de las organizaciones; los IoC son efectivos, pero tiene sus límites; en el análisis se obtuvo IoC que permiten identificar por medio de los artefactos las amenazas para su posterior bloqueo; las herramientas mostradas nos permiten visualizar los indicadores para automatización y mejora en los tiempos de verificación; los niveles de importancia indica el impacto de una vulnerabilidad en el código malicioso utiliza técnicas de explotación para vulnerar los sistemas que son parte del malware.

En busca de mejorar la seguridad y poder identificar a tiempo las amenazas; la creación de Framework, herramientas y plataformas están enfocadas generar con rapidez los indicadores de compromiso; los IoC son utilizados por tipos de plataforma de seguridad como los antivirus y además para toda plataforma de seguridad.

Las herramientas de seguridad por medio de una alerta creada por un indicador de compromiso ayudan a los departamentos encargados en la seguridad de la organización a responder; activa sus procesos de manejo de incidentes y se comienza con la investigación; las fases de análisis, contención, erradicación, recuperación y actividades posteriores son ejecutados al momento de estar comprometidos.

References

1. Khraisat, A., Gondal, I., Vamplew, P., Kamruzzaman, J.: Survey of intrusion detection systems: techniques, datasets and challenges. Cybersecurity. 2, (2019). https://doi.org/10.1186/s42400-019-0038-7

2. Demertzis, K., Iliadis, L.: Computational intelligence anti-malware framework for android OS. Vietnam J. Comput. Sci. 4, 245–259 (2017). https://doi.org/10.1007/s40595-017-0095-3
3. Souri, A., Hosseini, R.: A state-of-the-art survey of malware detection approaches using data mining techniques. Human-centric Comput. Inf. Sci. 8, (2018). https://doi.org/10.1186/s13673-018-0125-x
4. Sudhakar, Kumar, S.: An emerging threat Fileless malware: a survey and research challenges. Cybersecurity. 3, 1–12 (2020). https://doi.org/10.1186/s42400-019-0043-x
5. Long, Z., Tan, L., Zhou, S., He, C., Liu, X.: Collecting indicators of compromise from unstructured text of cybersecurity articles using neural-based sequence labelling. arXiv. 1–8 (2019)
6. Verma, M., Kumarguru, D.P., Deb, S.B., Gupta, A.: Analysing indicator of compromises for ransomware: Leveraging IOCs with machine learning techniques. 2018 IEEE Int. Conf. Intell. Secur. Informatics, ISI 2018. 154–159 (2018). https://doi.org/10.1109/ISI.2018.8587409
7. Murali, R., Ravi, A., Agarwal, H.: A Malware Variant Resistant to Traditional Analysis Techniques. Int. Conf. Emerg. Trends Inf. Technol. Eng. ic-ETITE 2020. 1–7 (2020). https://doi.org/10.1109/ic-ETITE47903.2020.264
8. Rhoades, D.: Machine actionable indicators of compromise. Proc. - Int. Carnahan Conf. Secur. Technol. 2014-Octob, (2014). https://doi.org/10.1109/CCST.2014.6987016
9. A Systems Approach to Indicators of Compromise Utilizing Graph Theory. 2018 IEEE Int. Symp. Technol. Homel. Secur. HST 2018. 16–21 (2018). https://doi.org/10.1109/THS.2018.8574187
10. Llerena, J., Mendez, A., Sanchez, F.: Analysis of the Factors that Condition the Implementation of a Backhaul Transport Network in a Wireless ISP in an Unlicensed 5 GHz Band, in the Los Tubos Sector of the Durán Canton. In: 2019 International Conference on Information Systems and Computer Science (INCISCOS). pp. 15–22. IEEE (2019)
11. López, C., Parra, A.: Análisis técnico de los recursos disponibles de la UEFS Santa María Mazzarello de Guayaquil para el diseño e implementación de un escenario de arquitectura, http://dspace.ups.edu.ec/handle/123456789/10286
12. Naik, N., Jenkins, P., Cooke, R., Gillett, J., Jin, Y.: Evaluating Automatically Generated YARA Rules and Enhancing Their Effectiveness. 2020 IEEE Symp. Ser. Comput. Intell. SSCI 2020. 1146–1153 (2020). https://doi.org/10.1109/SSCI47803.2020.9308179
13. Akram, B., Ogi, D.: The Making of Indicator of Compromise using Malware Reverse Engineering Techniques. 7th Int. Conf. ICT Smart Soc. AIoT Smart Soc. ICISS 2020 - Proceeding. 3–8 (2020). https://doi.org/10.1109/ICISS50791.2020.9307581
14. Rudman, L., Irwin, B.: Dridex: Analysis of the traffic and automatic generation of IOCs. 2016 Inf. Secur. South Africa - Proc. 2016 ISSA Conf. 77–84 (2016). https://doi.org/10.1109/ISSA.2016.7802932
15. Hsiao, S.C., Kao, D.Y.: The static analysis of WannaCry ransomware. Int. Conf. Adv. Commun. Technol. ICACT. 2018-Febru, 153–158 (2018). https://doi.org/10.23919/ICACT.2018.8323680
16. Saurabh: Advance Malware Analysis Using Static and Dynamic Methodology. 2018 Int. Conf. Adv. Comput. Telecommun. ICACAT 2018. 4–8 (2018).

https://doi.org/10.1109/ICACAT.2018.8933769
17. Aslan, O., Samet, R.: Investigation of possibilities to detect malware using existing tools. Proc. IEEE/ACS Int. Conf. Comput. Syst. Appl. AICCSA. 2017-Octob, 1277–1284 (2018). https://doi.org/10.1109/AICCSA.2017.24
18. Shrivastava, G., Kumar, P.: SensDroid: Analysis for Malicious Activity Risk of Android Application. Multimed. Tools Appl. 78, 35713–35731 (2019). https://doi.org/10.1007/s11042-019-07899-1
19. Choudhary, M., Kishore, B.: HAAMD: Hybrid Analysis for Android Malware Detection. 2018 Int. Conf. Comput. Commun. Informatics, ICCCI 2018. 18–21 (2018). https://doi.org/10.1109/ICCCI.2018.8441295
20. Quader, F., Janeja, V., Stauffer, J.: Persistent threat pattern discovery. 2015 IEEE Int. Conf. Intell. Secur. Informatics Secur. World through an Alignment Technol. Intell. Humans Organ. ISI 2015. 179–181 (2015). https://doi.org/10.1109/ISI.2015.7165967
21. Chen, Q., Bao, L., Li, L., Xia, X., Cai, L.: Categorizing and Predicting Invalid Vulnerabilities on Common Vulnerabilities and Exposures. Proc. - Asia-Pacific Softw. Eng. Conf. APSEC. 2018-Decem, 345–354 (2018). https://doi.org/10.1109/APSEC.2018.00049
22. 022 Time-Related Vulnerability Lookahead Extension to the CVE.pdf
23. Feutrill, A., Ranathunga, D., Yarom, Y., Roughan, M.: The Effect of Common Vulnerability Scoring System Metrics on Vulnerability Exploit Delay. Proc. - 2018 6th Int. Symp. Comput. Networking, CANDAR 2018. 1–10 (2018). https://doi.org/10.1109/CANDAR.2018.00009
24. Ando, E., Kayashima, M., Komoda, N.: A proposal of security requirements definition methodology in connected car systems by CVSS V3. Proc. - 2016 5th IIAI Int. Congr. Adv. Appl. Informatics, IIAI-AAI 2016. 894–899 (2016). https://doi.org/10.1109/IIAI-AAI.2016.95