ISSN: 2981-3506

BOLETÍN Nº 11

BOGOTÁ JULIO-SEPTIEMBRE DE 2024

ESICI
Escuela de Inteligencia y Contrainteligencia
Brigadier General Ricardo Charry Solano

BOLETÍN ESTRATÉGICO MULTIDISCIPLINAR

MEDIDAS DE PROTECCIÓN ESTRATÉGICA CONTRA RANSOMWARE EN INFRAESTRUCTURAS CRITICAS EN EL EJERCITO NACIONAL DE COLOMBIA

Escrito por: *ST. Vargas Soto Carlos Manuel*
Orientado por: *Julián Camilo Guevara Cardona*

Resumen: En la era digital actual, las infraestructuras críticas del Ejército Nacional de Colombia enfrentan crecientes amenazas cibernéticas, siendo el ransomware una de las más peligrosas. Estos ataques no solo pueden paralizar operaciones militares esenciales, sino también comprometer la seguridad nacional. Este boletín explora estrategias efectivas, basadas en investigaciones académicas para fortalecer la defensa contra el ransomware en el contexto militar colombiano.

Antecedentes en Colombia sobre el Rasomware:

A

El primer antecedente se presenta en el año 2018 a la empresa Carvajal Tecnología y Servicios, una empresa colombiana de soluciones de tecnología, que fue víctima de un ataque de Ransomware y a la vez comprometió su infraestructura tecnológica. Este incidente impactó a diversas entidades que dependían de sus servicios tecnológicos. ***(Fuente: VENTASDESEGURIDAD.COM-VER HOSTING WEB, 2018)***

B

El ataque más reciente se presentó en septiembre de 2023, la empresa de servicios de telecomunicaciones IFX Networks sufrió un ataque de Ransomware que afectó a numerosas entidades en Colombia y otros países de América Latina. La suspensión de los servicios de IFX tuvo un impacto considerable, especialmente en empresas y organismos gubernamentales que dependían de sus servicios de internet y conectividad. ***(Fuente: EL TIEMPO.COM-VER HOSTING WEB, 2023)***

RANSOMWARE

El Ransomware se mantiene como uno de los ataques preferidos por los cibercriminales. Esta modalidad criminal, con la que se secuestra información de una compañía, Gobierno o usuario para cobrar un rescate, tiene en alerta al continente americano, ante una ola de ataques que ha puesto a prueba sus relativamente inmaduros sistemas de ciberseguridad gubernamentales que dependían de sus servicios de internet y conectividad.

(Fuente: FORBES, 2023)

TÉCNICAS DE CIBERDELINCUENTES

En el ciberespacio hay diferentes técnicas utilizadas por los ciberdelincuentes, entre las más importantes se conocen las siguientes cuatro:

1 PHISHING

El phishing es una técnica en la que los atacantes envían correos electrónicos o mensajes que parecen provenir de fuentes confiables para engañar a las víctimas y hacer que revelen información confidencial, como contraseñas o datos bancarios.

(Fuente: VERIZON, 2023)

3 MOVILIDAD LATERAL

La movilidad lateral es una técnica utilizada por los ciberdelincuentes para moverse dentro de una red comprometida después de haber obtenido acceso inicial. Este movimiento les permite expandir su control y buscar datos sensibles o sistemas críticos.

(Fuente: ZIMBA & WANG,Z, 2019)

2 VULNERABILIDAD CSRF

La vulnerabilidad CSRF (Cross-Site Request Forgery), también conocida como "falsificación de solicitud en sitios cruzados", es una técnica en la que un ciberdelincuente engaña a un usuario autenticado para que realice acciones no deseadas en una aplicación web en la que está autenticado.

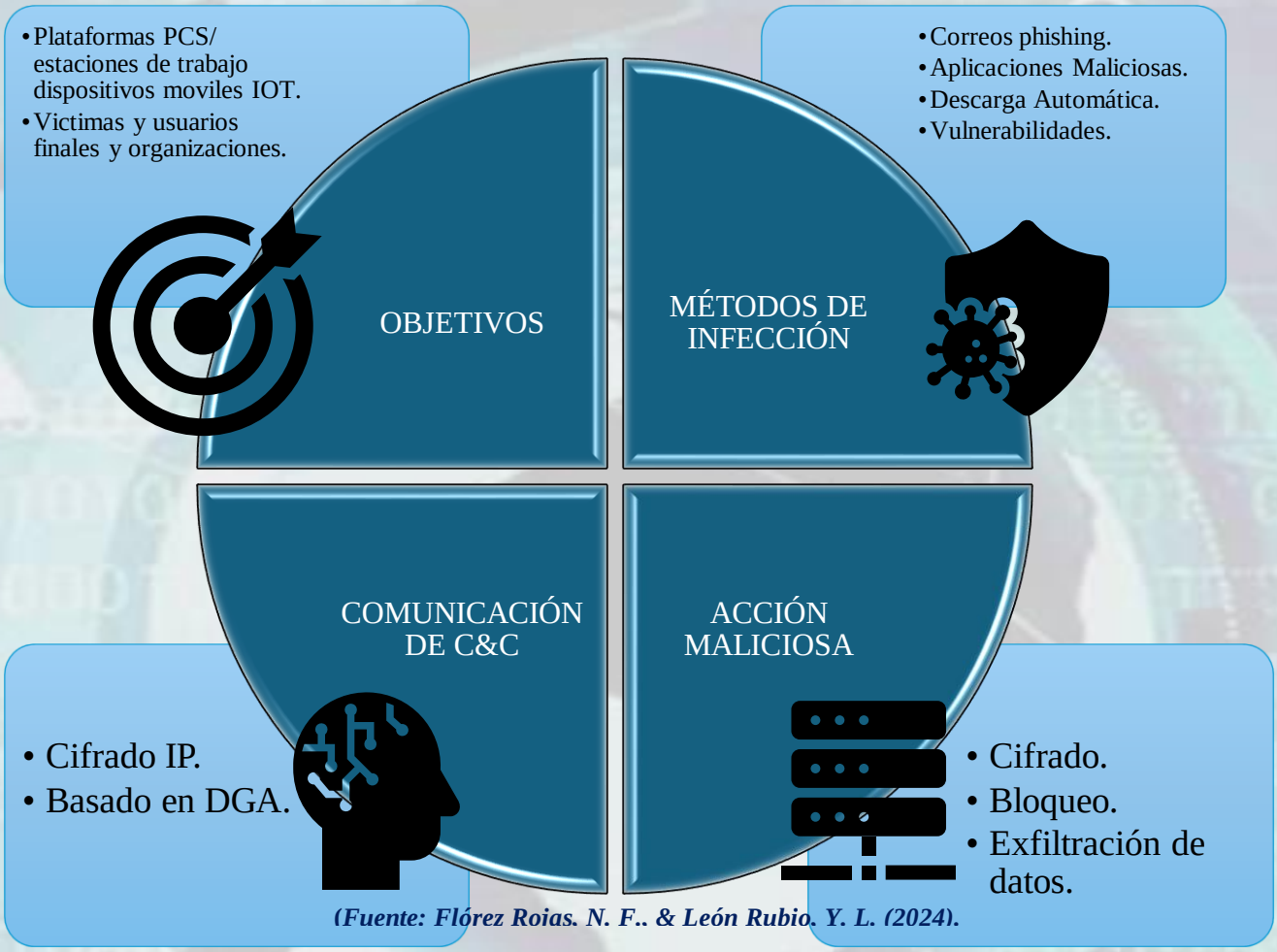
(Fuente: OWASP FOUNDATION, n.d)

4 FUERZA BRUTA

CrowdStrike 2023 Global Threat Report menciona que los ataques de fuerza bruta siguen siendo una técnica común entre los ciberdelincuentes, especialmente contra sistemas mal asegurados.

(Fuente: CROWDSTRIKE, 2023)

TAXONOMÍA DE RANSOMWARE



(Fuente: Flórez Roias. N. F.. & León Rubio. Y. L. (2024).

COMPRENSIÓN DE LA AMENAZA

Para desarrollar una defensa efectiva, es fundamental entender las tácticas, técnicas y procedimientos (TTP) utilizados por los actores de ransomware. Según Martínez et al. (2022) en Revista Colombiana de Seguridad Informática, el 75% de los ataques de ransomware contra entidades gubernamentales comienzan con campañas de phishing dirigidas y explotación de vulnerabilidades no parchadas.

(Fuente: Martínez, L., Gómez, A., & Rodríguez, P. (2022).

EVALUACIÓN DE RIESGOS Y VULNERABILIDAS

La identificación y evaluación continua de riesgos son esenciales para proteger las infraestructuras críticas. Pérez y López(2023), en el Journal de Defensa Nacional, destacan como una empresa de energía eléctrica debe someterse a revisiones constantes para prevenir ataques a los sistemas de seguridad de la empresa por parte del desarrollador del ingeniero de sistemas, aplicando una matriz de chequeo en el administrador de tareas.

(Fuente: Pérez, M., & López, S. (2023).

IMPLEMENTACIÓN DE TECNOLOGÍAS DE DEFENSA

Adoptar tecnologías avanzadas es clave para detectar y responder rápidamente a incidentes de ransomware. García et al. (2023) en Tecnología y Seguridad Militar, enfatizan el uso de soluciones de detección y respuesta extendida (XDR) y la inteligencia artificial para la identificación temprana de amenazas, reduciendo significativamente el tiempo de respuesta ante un ataque.

(Fuente: García, F., Ramírez, T., & Sánchez, J. (2023).

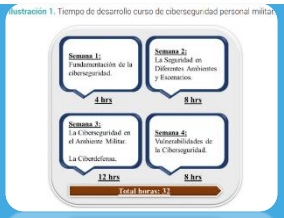
ISSN: 2981-3506

BOLETÍN Nº 11

BOGOTÁ JULIO-SEPTIEMBRE DE 2024

DESARROLLO DE UN PLAN DE RESPUESTA Y RECUPERACIÓN

Tener un plan bien estructurado de respuesta y recuperación es vital para minimizar el impacto de un ataque de ransomware. Según Ramírez y Torres (2022), en el Boletín de Estrategia de Seguridad, la realización de simulacros regulares y la capacitación continua del personal militar son prácticas esenciales para garantizar una respuesta eficaz y coordinada. ***(Fuente: Ramírez, C., & Torres, E. (2022)***



FORMACIÓN Y CONCIENCIACIÓN DEL PERSONAL

El factor humano es una de las primeras líneas de defensa contra el ransomware. González (2021), en Revista de Ciberseguridad Militar, destaca que programas de formación continua y campañas de concienciación han demostrado reducir en un 65% la probabilidad de éxito de phishing dirigidos a personal militar.

(Fuente: González, R. (2021)

COLABORACIÓN Y COMPARTICIÓN DE INFORMACIÓN

La colaboración entre diferentes ramas del gobierno y aliados internacionales es crucial para combatir amenazas cibernéticas. Hernández y Castro (2023) en Estudios de Seguridad Nacional subrayan la importancia de establecer canales seguros para la compartición de información sobre amenazas y mejores prácticas entre las fuerzas armadas y agencias de inteligencia.

(Fuente: Hernández, J., & Castro, M. (2023).

COPIAS DE SEGURIDAD FRECUENTES

Aplicar las reglas 3-2-1: tres copias de seguridad de los datos en dos medios diferentes y una de esas copias en un lugar distinto y seguro.

VERIFICAR FUENTES DE EMAIL

Comprobar la dirección de email del remitente con los contactos antes de abrir cualquier enlace o descargar cualquier elemento de su correo electronico.

¿CÓMO PROTEGERSE DE UN RANSOMWARE?

Aun no se ha descubierto un antídoto contra la infección por un ransomware.

MARCAR SITIOS WEB COMO FAVORITOS

Marcar las páginas web de confianza y visitadas con más frecuencia evitará introducir direcciones equivocadas.

ACTUALIZAR SOFTWARE DE SEGURIDAD

Un software de seguridad actualizado añade una capa adicional de seguridad. Actualizarlo regularmente puede protegerlo contra las últimas variantes de ransomware.

(Fuente: Córdoba Bahamon, J. A. (2016).)

La protección contra el ransomware en las infraestructuras críticas del Ejército Nacional de Colombia requiere una estrategia integral que combine la comprensión de las amenazas, la evaluación continua de riesgos, la implementación de tecnologías avanzadas, la planificación de respuesta y recuperación, la formación del personal y la colaboración interinstitucional. Adoptando estas medidas estratégicas basadas en investigaciones académicas, el Ejército Nacional fortalece significativamente su resiliencia frente a ataques de ransomware.

ESICI
Escuela de Inteligencia y Contrainteligencia
Brigadier General Ricardo Charry Solano
BOLETÍN ESTRATÉGICO
MULTIDISCIPLINAR

Referencias

Álvarez Calderón, C. E., Ramírez Pedraza, Y. E., Ruiz Tinoco, D., Rosanía Miño, N. A., Gómez Martínez, J. C., Sánchez Duque, D. P., ... & Urbano Morales, Ó. J. (2022). Escenarios y desafíos de la seguridad multidimensional en Colombia.

Antonio, J., & Bahamón, C. (s/f). MALWARE: UNA PUERTA A LA CIBERCRIMINALIDAD.

Beaman, C., Barkworth, A., Akande, T. D., Hakak, S., & Khan, M. K. (2021). Ransomware: Recent advances, analysis, challenges and future research directions. *Computers & security*, *111*, 102490.

Camacho, J. D. (2016). EVOLUCIÓN DE LA CIBERDEFENSA Y LA SEGURIDAD DE LA INFORMACIÓN EN COLOMBIA.

Castañeda, J. E. R., Tello, J. S., Cárdenas, E. E., & Pineda, V. G. (2023). Identificación de herramientas para prevenir el cryptojacking. Una aproximación de literatura desde el caso de Colombia. *Revista Científica Epistemia*, *7*(1), 99-110.

Córdoba Bahamon, J. A. (2016). *Malware: una puerta a la cibercriminalidad* (Bachelor's thesis, Universidad Piloto de Colombia).

CrowdStrike. (2023). *2023 Global Threat Report*. CrowdStrike. https://www.crowdstrike.com/resources/reports/global-threat-report/

De, S., De, S., & Información, L. A. (s/f). Folker Narvaez-Proyecto de investigación.

Flórez Rojas, N. F., & León Rubio, Y. L. (2024). El Increíble Impacto del Ransomware en Colombia.

García, F., Ramírez, T., & Sánchez, J. (2023). *Tecnologías avanzadas para la defensa contra ransomware en el ámbito militar*. Tecnología y Seguridad Militar, 10(2), 150-168.

González, R. (2021). *Impacto de la concienciación en ciberseguridad dentro de las fuerzas militares*. Revista de Ciberseguridad Militar, 5(1), 33- fifty.

Hernández, J., & Castro, M. (2023). *La importancia de la colaboración interinstitucional en la lucha contra el ransomware*. Estudios de Seguridad Nacional, 12(2), 110-128.

Leyton Garzón, E. O. (2021). Lineamientos estratégicos para la defensa de la infraestructura critica en el comando de apoyo operacional de comunicaciones y ciberdefensa del Ejército Nacional de Colombia.

Martínez, L., Gómez, A., & Rodríguez, P. (2022). *Análisis de las tácticas de ransomware en entidades gubernamentales colombianas*. Revista Colombiana de Seguridad Informática, 14(3), 89-104.

Niño, F. Y. Á. (2023). Ransomware, una amenaza latente en Latinoamérica. Intersedes, 24(49), 92-119.

O'Gorman, G., & McDonald, G. (2012). *Ransomware: A growing menace*. Arizona, AZ, USA: Symantec Corporation.

OWASP Foundation. (n.d.). *Cross-Site Request Forgery (CSRF)*. OWASP. https://owasp.org/www-community/attacks/csrf

Pérez, M., & López, S. (2023). *Marcos de evaluación de riesgos para infraestructuras críticas militares*. Journal de Defensa Nacional, 18(1), 45-67.

Ramírez, C., & Torres, E. (2022). *Estrategias de respuesta y recuperación ante ransomware en entornos militares*. Boletín de Estrategia de Seguridad, 7(4), 200-215.

Richardson, R., & North, M. M. (2017). Ransomware: Evolution, mitigation and prevention. *International Management Review*, *13*(1), 10.

Rosas Prado, A. F. (2022). El cibercrimen en Colombia y su evolución en los últimos dos años (2020-2021).

Sierra, M. E. O. (2023). Propuesta de capacitación virtual para promover la cibercultura en el Ejército Nacional de Colombia. Revista Ciberespacio, Tecnología e Innovación, 2(4), 147-167.

Teymourian, K., & Mann, M. (2020). The role of scripting languages in advanced persistent threats: A case study of PowerShell. Computers & Security, 91, 101702. https://doi.org/10.1016/j.cose.2020.101702

Verizon. (2023). *2023 Data Breach Investigations Report*. Verizon. https://www.verizon.com/business/resources/reports/dbir/