Análisis y prevención del Ransomware en la Universidad de Guayaquil

Jéssica Yépez-Holguín, Jorge Alvarado-Chang[a], Mirella Ortíz-Zambrano[a], Narcisa Acosta-Sánchez[a]
[a] Facultad de Ciencias Matemáticas y Física, Carrera de Ingeniería en Sistemas Computacionales, Universidad de Guayaquil
jessica.yepezh@ug.edu.ec, jorge.alvaradoch@ug.edu.eco, mirella.ortizz@ug.edu.ec, narcisa.acostasa@ug.edu.ec

Resumen

El ataque de tipo cibernético *Ransomeware* es uno de los delitos informáticos que más ha crecido en el 2017, provocando la pérdida de información y paralizando a instituciones públicas y privadas. A nivel mundial, compañías de seguridad cibernética y otras organizaciones establecen medidas y prevenciones. El presente análisis tiene el interés de evaluar si en la Universidad de Guayaquil, como entidad pública, existen las medidas que permitan enfrentar esta creciente amenaza para lo cual se realizó una encuesta a los administradores de cómputo con el objeto de analizar si se encuentran preparados ante este tipo de ataque.

Palabras clave: Amenaza, Análisis, Ataque, *Ransomeware*, Prevención, Seguridad

Abstract

The cybernetic attack Ransomeware is one of the computer crime that has grown the most in 2017, causing the loss of information and paralyzing public and private institutions. Globally, cyber security companies and other organizations establish measures and precautions. The present analysis has the interest of evaluating if the University of Guayaquil, as a public entity, the measures exist that allow to face this growing threat for which a survey was carried out to the computer administrators in order to analyze if they are prepared before This type of attack.

Keywords: Threats, Analysis, Attack, Ransomware, Prevention, Security

I. INTRODUCCIÓN

Los virus son capaces de hacer daño, reproducirse y mutar, se asemejan con los virus biológicos, todo lo cual parece ser el origen de su nombre. Esto precisamente ha convertido a los virus en una verdadera pesadilla para las redes y sus usuarios. *Ransomware*s un tipo de *malware* (código malicioso) que consiste en invadir los sistemas informáticos de manera silenciosa para cifrar los datos y posteriormente pedir un rescate monetario para liberarlos. Aunque este tipo de ataque no es nuevo, estudios recientes alertan del peligro, indicando que desde el 2015 hasta el 2016 es el ataque que más se ha incrementó [1], es uno de los delitos informáticos que más ha crecido en el último año, provocando la pérdida de información y paralizando a las pequeñas y grandes instituciones, siendo importante tomar medidas preventivas para evitar sus consecuencias.

A nivel mundial, compañías de seguridad cibernética y organizaciones establecen medidas y prevenciones. Latinoamericano está exento de este malware [2], países como Brasil, Argentina [3], Uruguay [4], Chile [5], también han tenido ataques del tipo Ransomware comprometiendo sistemas e información de manera más vulnerable al sector público. En Ecuador algunas Compañías han sufrido ataques de este tipo [6], pero no se cuenta con estadísticas para cuantificarlas.

Estas amenazas que antes no eran consideradas, hoy en día son un riesgo latente que puede afectar, incluso a usuarios en su hogar, comprometiendo su información personal, como también afectan al sector público o privado [7]. Como ejemplo en uno de los últimos ataques registrados, MongoDB que es una compañía de base de datos y ofrece servicios a otras grandes empresas como Amazon, Telefónica, eBay, gobierno, fue afectada en sus servidores de base de datos y como ésta hay muchas organizaciones que en alguna medida han sido afectadas [8], pero que por temas de seguridad y de imagen comercial en el mercado, omiten reconocer que no contaban con las medidas de seguridad suficientes. En la actualidad existen métodos y herramientas que podrían minimizar este riesgo, pero el peligro radica en que no se le da la prioridad que el caso amerita; ya sea por desconocimiento o por falta de recursos, estos sectores no aplican medidas para protegerse del riesgo [9].

Este *Software* malicioso, cada vez es más inteligente ya que aprovecha los errores de *software* [10]; existe evidencia que demuestra que los atacantes rápidamente innovan modificaciones e incluso realizan ataques personalizados, que hacen más efectiva la intromisión, además se conoce que es imposible que el software esté 100% libre de errores, de esta manera no estamos exentos de ser potencialmente atacados [11-14]. Existen casos en Instituciones con altos estándares de seguridad que han terminado siendo víctimas del ataque, además con el internet de las cosas (IOT) [15], cada vez es más probable que los ataques alcancen nuevos niveles [16-18]. El ataque *Ransomware* puede potencialmente llegar apoderarse de circuitería Industrial donde el ataque podría causar daños técnicos e incluso daños a la integridad física de las personas [19]. Lo más

novedoso de este malware es que también podría realizar ataques en la nube con el riesgo de pérdida de información, lo cual por consiguiente podría generar cuantiosas pérdidas de no tomar las medidas de seguridad correspondientes.

De acuerdo a esta investigación, la seguridad perimetral en el Ecuador debe realizarse a nivel de red para prevenir ataques de hackers, intrusiones o robos de información, no solo en conexiones remotas sino también a nivel de contenidos que impidan el ingreso de códigos maliciosos, *spam* y contenidos webs no deseados [20]. El nivel de seguridad en las empresas de la ciudad de Guayaquil, están directamente relacionadas con las políticas y planes de seguridad que dispongan, ya que, para las mismas, la seguridad no es un producto final, si no, un proceso continuo [21]. Por tal razón, conociendo de antemano que Ecuador es un país en desarrollo y que posee limitaciones técnicas y económicas, el presente análisis, tiene el interés de conocer en qué situación se encuentra la Universidad de Guayaquil para enfrentar esta creciente amenaza y si se han tomados medidas a fin de prevenir un posible ataque del tipo *Ransomware* con la finalidad de precautelar la información de las diferentes facultades y evitar la pérdida de información académica cuyo valor es incalculable [22-23].

II. MÉTODO

Todo trabajo investigativo, necesita tomar ciertas decisiones para gestionarlo, la realización de este trabajo se desarrolla bajo las modalidades de investigación descriptiva, exploratoria, bibliográfica y de campo, utilizando la técnica de la entrevista a los actores principales en el área de la informática en la Universidad de Guayaquil, como es el caso de los Analistas Informáticos de cada una de las Facultades, Docentes que ejercen la función de administrar centros de cómputo o son responsables de un área de cómputo y alumnos de últimos semestres de Ingeniería en Sistemas y Networking, quienes tienen cargos administrativos y/o experiencia profesional. En cuanto al sector público se ha focalizado el caso de la Universidad de Guayaquil y se ha preparado un cuestionario que permita discernir si la misma está preparada, en cuanto a las seguridades informáticas necesarias para prevenir un ataque del tipo *Ransomware* [24-26].

La información que se recabe mediante el instrumento de la encuesta permitirá obtener información complementaria para obtener un parámetro de comparación con otros sectores públicos y privados del medio y que podrían servir de banco de datos para una investigación más profunda o para ampliar esta misma investigación en un futuro cercano.

III. ANÁLISIS DE RESULTADOS

Realizada la encuesta de evaluación en la Universidad de Guayaquil, los datos indican que el 82% de los encuestados conoce el tipo de ataque *Ramsomware* y sus posibles consecuencias; que en un 71% los administradores utilizan Sistemas Operativos y antivirus actualizados, y usan software debidamente licenciado en alrededor de un 53% [27]; que un 53% utiliza administradores de contraseña, y que en general un 76% de los usuarios utiliza contraseñas diferentes para acceder a diferentes sitios web; que un 47% no guarda datos personales en el navegador y que en el mismo porcentaje utilizan bloqueador de anuncios para evitar *malware;* la encuesta evidenció además, que un 29% apenas alcanza como aspecto descuidado el uso de contraseñas Fuertes [28]. La encuesta demostró que en un 65%, los usuarios acceden para realizar sus compras y transacciones bancarias a sitios seguros y que un 59% entiende los riesgos de descargar software que no es de confianza, entiéndase copias no autorizadas, software modificado o autores de origen desconocido; en cuanto a las políticas de seguridad de uso de memorias portátiles y dispositivos externos que pueden acceder a la red organizacional la encuesta evidenció que los administradores la implementan en un 35%;en cuanto a los archivos adjuntos que reciben en sus correos de contactos no conocidos o incluso conocidos, un 59% dijo que tienen precaución con respecto al manejo de dicho contenido; Otro 59% dijo que utilizan el acceso a un wifi seguro, en cambio un 53% dijo que los servicios de red de sistema operativo están en servicio y son utilizados; La encuesta demostró que un 29% ha implementado el uso de encriptación de datos y tráfico de red; Finalmente, un 53% de los administradores encuestados tienen implementado políticas de respaldo y plan de contingencias. Todos estos datos se ilustran en la figura 1, cuya zona azul indica los niveles de seguridad implementados y la zona roja indica las debilidades que son amenazas que podrían ser aprovechadas por el *malware*.

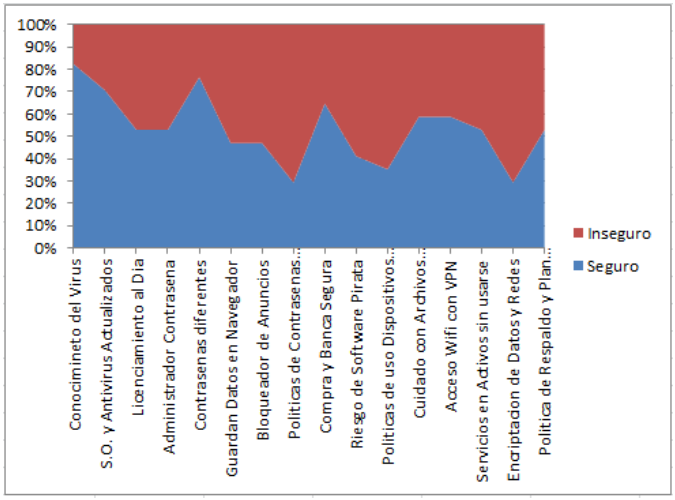

Figura. 1. Resumen de Resultado de la Encuesta de Seguridad Informática

En la figura 2, se resume el promedio total de seguridad vs. Inseguridad en la Universidad de Guayaquil, y a pesar de que un 54% evidencia un factor de seguridad implementado [29], el otro 46% demuestra que existen factores de riesgo poténciales que pueden permitir el ingreso del *Ransomware* a la red de la entidad, siendo lo más relevante que ninguno de los encuestados tiene implementado un sistema de seguridad que garantice al 100% la seguridad de las redes. Al tratarse de una sola organización, todo el sistema de seguridad es tan fuerte como su nodo más vulnerable, esto quiere decir que dadas las características de contaminación un ataque tipo *Ransomware* solo necesita un mínimo de inseguridad para penetrar la organización y causar daños dentro de ella [30-31].

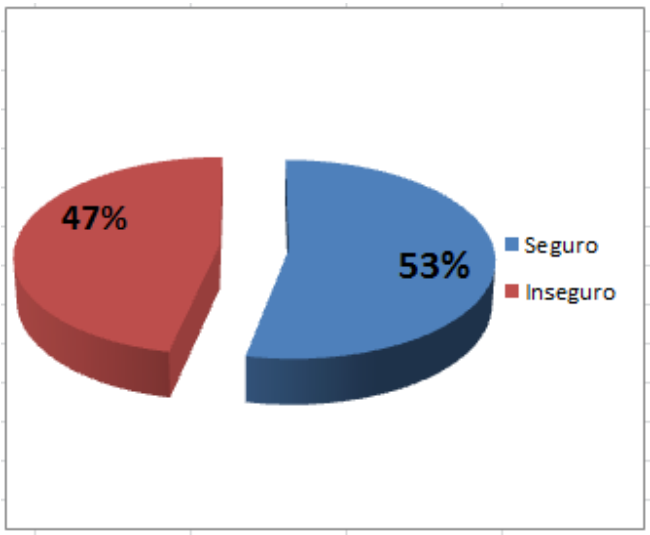

Figura. 2. Total General de Resultado de la Encuesta de Seguridad Informática

IV. Conclusiones

Ante el gran número de ciberataques que se producen diariamente y de manera creciente en cualquier parte del mundo y con el atractivo de la nuevas tecnologías, que el *Ransomware* aprovecha para explorar técnicas que le permiten secuestrar la información de los equipos y que sólo la devuelve a cambio de un rescate monetario, del cual no se tiene ninguna garantía que se cumpla, el enfoque de este proyecto cuestiona, si la Universidad de Guayaquil, se encuentra preparada para un ataque malicioso de esta naturaleza[32].

De acuerdo a los resultados obtenidos mediante el instrumento encuesta se pudo determinar que la Universidad de Guayaquil debe fortalecer nuevos aspectos de la seguridad, que posiblemente no fueron necesarios en otro momento [33]. Se deduce del análisis de la encuesta, por la variación de las respuestas en la misma institución, que la política de seguridad no se cumple de manera homogénea en todas las áreas informáticas de la entidad, una capacitación de seguridad a todos los colaboradores de las diferentes áreas puede ayudar en este sentido a elevar los niveles de seguridad, mitigando en un porcentaje más elevado el riesgo de un ataque [34]; como un factor importante para la prevención de un ataque del tipo *Ransomware* sugerimos también realizar un análisis tecnológico de los equipos y capacidad del software de seguridad implementados, para determinar en qué medida, un mejoramiento de los mismos, permitan apoyar las políticas de seguridad necesarias para contrarrestar esta amenaza[35-37].

Este proyecto deja abierta varios tópicos para que futuros investigadores puedan profundizar en el tema realizando nuevos análisis y levantamiento de información con resultados y precisiones más altas. Se podría decir que este proyecto ha servido para sumergirnos en un mundo el cual aún tiene mucho que decir y hacer. Por ello se considera que en tal sentido ha sido muy útil ya que de cara al futuro se tendrá una base sólida y un referente con el que se podrá contar en futuras investigaciones.

Agradecimientos

Agradecemos la colaboración de Informáticos, Docentes y Alumnos de la Universidad de Guayaquil, quienes de una u otra forma aportaron con este trabajo de investigación, sin los cuales no se hubiera podido completar los objetivos planteados. “El conocimiento es poder, y responsables somos de su divulgación”

Referencias

[1] BPS Business Publications Spain S.L. (2017). El ransomware se incrementó un 752% en 2016 | Informes | Seguridad | Computing. https://doi.org/1096142002501

[2] Manuel Silva, “Casos de ransomware en Chile han aumentado un 131% respecto al año anterior - FayerWayer,” *27 abril 2017*, 2017. [Online]. Available: https://www.fayerwayer.com/2017/04/casos-de-ransomware-en-chile-han-aumentado-un-131-respecto-al-ano-anterior/. [Accessed: 23-Jul-2017].

[3] TELAM, “En Argentina se reportaron 2.400 casos del RansomwareWannaCry - Télam - Agencia Nacional de Noticias,” *17/05/2017*, 2017. [Online]. Available: http://www.telam.com.ar/notas/201705/189366-en-argentina-se-reportaron-2400-casos-del-ransomware-wannacry.html. [Accessed: 23-Jul-2017].

[4] CristophScholz-Flickr, “El ransomware: un virus que ataca cada vez más a todos los internautas | Seguridad, Infraestructura, Uruguay,” *Mayo 14, 2017 05:00*, 2017. [Online]. Available: http://www.elobservador.com.uy/el-ransomware-un-virus-que-ataca-cada-vez-mas-todos-los-internautas-n1070668. [Accessed: 23-Jul-2017].

[5] TELETRECE, "Malware Hunter Team cifra en 379 los ataques con ransomware | Tele 13," *17:50 hrs. Viernes 12, Mayo 2017*, 2017. [Online]. Available: http://www.t13.cl/noticia/nacional/malware-hunter-team-cifra-al-menos-379-ataques-ransomware-chile. [Accessed: 23-Jul-2017].

[6] ANDERSSON BOSCÁN, "Ecuador y casi 100 países sufren ciberataque extorsivo," *13 MAY 2017*, 2017. [Online]. Available: http://www.expreso.ec/actualidad/ecuador-y-casi-100-paises-sufren-ciberataque-extorsivo-HJ1319548. [Accessed: 23-Jul-2017].

[7] IEEE, "Keeping your Data Safe in the Age of Breaches and Ransomware - IEEE Transmitter," *OCTOBER 14, *, 2016. [Online]. Available: http://transmitter.ieee.org/keeping-data-safe-age-breaches-ransomware/. [Accessed: 28-Jun-2017].

[8] A. MARTÍNEZ, "Un enorme ataque de «ransomware» secuestra 32.000 servidores de MongoDB," *10/01/2017 21:53h - Actualizado: 11/01/2017 10:42h.*, 2017. [Online]. Available: http://www.abc.es/tecnologia/redes/abci-enorme-ataque-ransomware-secuestra-32000-servidores-mongodb-201701102153_noticia.html. [Accessed: 23-Jul-2017].

[9] A. Duros Blandos, "Seguridad en Informática," 2013.

[10] H. Orman, "Evil Offspring - Ransomware and Crypto Technology," *IEEE Internet Comput.*, vol. 20, no. 5, pp. 89–94, Sep. 2016.

[11] A. Kharaz, S. Arshad, C. Mulliner, W. Robertson, E. Kirda, and A. Kharraz, "This paper is included in the Proceedings of the 25th USENIX Security Symposium UNVEIL: A Large-Scale, Automated Approach to Detecting Ransomware UNVEIL: A Large-Scale, Automated Approach to Detecting Ransomware."

[12] H. Orman, "Evil Offspring - Ransomware and Crypto Technology," *IEEE Internet Comput.*, vol. 20, no. 5, pp. 89–94, Sep. 2016.

[13] Huilcamaigua Pazuña, S. R. (2017). Aplicación de una metodología para el análisis de los efectos de malware en dispositivos móviles con sistema operativo Android en el Ecuador. Retrieved from http://bibdigital.epn.edu.ec/handle/15000/17495

[14] *Redes seguras (Seguridad informática) - Purificación Aguilera - Google Libros*.

[15] IAN CHANT, "Data Breaches, Compromised Credentials, and Ransomware are Among CIOs and CTOs Top Concerns - IEEE - The Institute," *24 marzo 2017*, 2017. [Online]. Available: http://theinstitute.ieee.org/ieee-roundup/blogs/blog/data-breaches-compromised-credentials-and-ransomware-are-among-cios-and-ctos-top-concerns. [Accessed: 28-Jun-2017].

[16] DAN GOODIN, "WannaCry ransomware tied to prolific Lazarus hacking group by new evidence | Ars Technica UK," *23/5/2017, 05:20*, 2017. [Online]. Available: https://arstechnica.co.uk/security/2017/05/wannacry-ransomware-lazarus-group/. [Accessed: 28-Jun-2017].

[17] ERIC GELLER, "NSA-created cyber tool spawns global attacks — and victims include Russia - POLITICO," *05/12/2017 02:07 PM EDT* , 2017. [Online]. Available: http://www.politico.com/story/2017/05/12/nsa-hacking-tools-hospital-ransomware-attacks-wannacryptor-238328. [Accessed: 28-Jun-2017].

[18] STEVE ORLANDO, "Extortion extinction: Researchers develop a way to stop ransomware," *JULY 7, 2016*, 2016. [Online]. Available: http://news.ufl.edu/articles/2016/07/extortion-extinction-researchers-develop-a-way-to-stop-ransomware.php. [Accessed: 29-Jun-2017].

[19] John Toon, "Simulated Ransomware Attack Shows Vulnerability of Industrial Controls | Research Horizons | Georgia Tech's Research News," *February 13, 2017*, 2017. [Online]. Available: http://www.rh.gatech.edu/news/587359/simulated-ransomware-attack-shows-vulnerability-industrial-controls. [Accessed: 29-Jun-2017].

[20] Jumbo Tene, T. M. (2017). Metodología para el análisis de malware en un ambiente controlado. Retrieved from http://dspace.ups.edu.ec/handle/123456789/14202

[21] O. David López Villa, W. Darío, and R. Gil, "ANÁLISIS Y DESARROLLO DE ESTRATEGIAS PARA LA PREVENCIÓN DEL USO DE LA INGENIERÍA SOCIAL EN LA SOCIEDAD DE LA INFORMACIÓN," *Ing. USBMed*, vol. 4, no. 2, pp. 16–22, 2013.

[22] Jaramillo Barea, F. X., & Xavier, F. (2012). Delitos informáticos prevención modificación y creación de nuevos tipos penales. Retrieved from http://repositorio.upacifico.edu.ec/handle/40000/55

[23] Daza Rosado, G. A., & Antonio, G. (2015). FORTALECIMIENTO DE SEGURIDAD DEL CENTRO DE DATOSDE LA CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES, ANÁLISIS DE POLÍTICAS DE SEGURIDAD INFORMÁTICA PROPUESTA DE PROTECCIÓN ENDPOINT Y CONTROL DE ACCESO A LA RED¨. Retrieved from http://repositorio.ug.edu.ec/handle/redug/10281

[24] Guamán Sinchi, B. V., & Vinicio, B. (2015). Anatomía de un ataque Informático. Retrieved from http://dspace.uazuay.edu.ec/handle/datos/5046

[25] López Fierro, J. F. (2016). Estudio y propuesta de diseño para la arquitectura de seguridad perimetral de campus, caso de estudio data center para el Municipio del Distrito Metropolitano de Quito. Retrieved from http://repositorio.puce.edu.ec/handle/22000/12582

[26] Lara Ponce, C. A., & Antonio, C. (2015). Estudio de una auditoría en seguridad informática aplicando la Norma Internacional de calidad total ISO 27001 para la empresa Maint de la ciudad de Guayaquil. Retrieved from http://repositorio.ug.edu.ec/handle/redug/6978

[27] R. A. Guibourg, "CAPÍTULO 22 INFORMÁTICA JURÍDICA," vol. 1, pp. 791–823.

[28] Dr. Joaquín Alarcón Fidalgo, "Boletín del Grupo Internacional de Trabajo 'Nuevas Tecnologías, Prevención y Seguro' Nº 8-2011," vol. 35, p. 348, 2011.

[29] V. Pascual, O. Director, and D. Vico, "Trabajo Fin de Máster presentado por."

[30] Rodríguez, J. A., Oduber, J., & Mora, E. (2007). Actividades rutinarias y cibervictimización en Venezuela (Tema central). 2017-06. Retrieved from http://repositorio.flacsoandes.edu.ec/handle/10469/12242#.WXfV3oQ1-Uk

[31] R. Brewer, "Ransomware attacks: detection, prevention and cure," *Netw. Secur.*, vol. 2016, pp. 5–9, 2016.

[32] Hurtado Sandoval, M. E., &MendañoMendaño, L. A. (2016). Implementación de técnicas de hacking ético para el descubrimiento y evaluación de vulnerabilidades de la red de una cartera de Estado. Retrieved from http://bibdigital.epn.edu.ec/handle/15000/16836

[33] Ian Chant, "The Institute: The Cybersecurity Talent Shortage Is Here, and It's a Big Threat to Companies – IEEE Cybersecurity," *12 April 2017*, 2017. [Online]. Available: https://cybersecurity.ieee.org/blog/2017/04/13/the-institute-the-cybersecurity-talent-shortage-is-here-and-its-a-big-threat-to-companies/. [Accessed: 23-Jul-2017].

[34] AMANDA DAVIS, "Potential Consequences for Cybersecurity Specialists Who Report Vulnerabilities - IEEE - The Institute," *17 octubre 2016*, 2016. [Online]. Available: http://theinstitute.ieee.org/technology-topics/cybersecurity/potential-consequences-for-cybersecurity-specialists-who-report-vulnerabilities. [Accessed: 23-Jul-2017].

[35] J. K. Lee, S. Y. Moon, and J. H. Park, "CloudRPS: a cloud analysis based enhanced ransomware prevention system," *J. Supercomput.*, vol. 73, no. 7, pp. 3065–3084, Jul. 2017.

[36] Paredes Valdivieso, H. R. (2010). Implementación de un sistema de gestión central y unificada sobre seguridad en ambientes Microsoft en el Laboratorio de Tecnologías de Información y Comunicación (LTIC) de la Facultad de Ingeniería. Pontificia Universidad Católica Del Ecuador. Retrievedfrom http://repositorio.puce.edu.ec/handle/22000/3424

[37] A. Abril, J. Pulido, and J. A. Bohada, "Análisis de Riesgos en Seguridad de la Información," *Ciencia, Innovación y Tecnol.*, vol. 1, no. 0, pp. 39–53, 2014.