UNIVERSIDAD DE COSTA RICA

MTI Henry Lizano Mora, director del Centro de Informática de la UCR. Foto Laura Rodríguez.

Por el MTI Henry Lizano Mora, director del Centro de Informática de la UCR

Voz experta: Taxonomía del malware, el caso Ransomware Conti

A propósito de los ataques informáticos a las instituciones públicas costarricenses: ¿de qué se trata, quién los hace y cómo evitarlos?

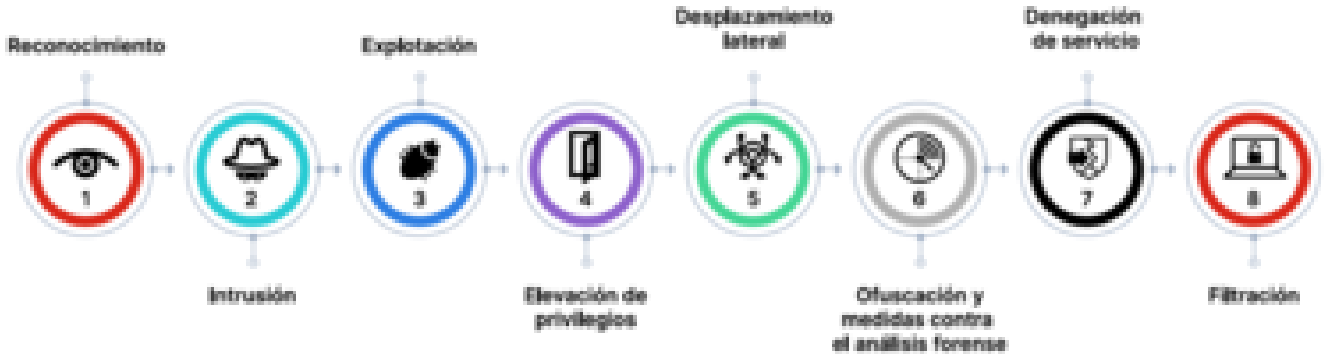
5 MAY 2022 Ciencia y Tecnología

Mucho se ha hablado en los últimos días sobre los ciberataques a las instituciones públicas, iniciando por la denegación de algunos de sus servicios importantes. Es por eso que, para comprender realmente la magnitud de lo que está ocurriendo más allá de la conocida afectación, nos dimos a la tarea de presentar cómo está compuesto este tipo de malware (software malicioso) y algunas de las implicaciones de las Amenazas Persistentes Avanzadas (Advanced Persistent Threats), mejor conocidas como APT por sus siglas en inglés.

Un APT como el que hoy en día flagela nuestro país no solo se trata de un único malware, sino de un conjunto de estos dirigidos estratégicamente por un grupo criminal, con el fin de solicitar un rescate por la información secuestrada.

El Ransomware es la herramienta por excelencia y de allí su nombre, un vocablo compuesto del inglés ransom o “rescate” y ware de malware; es decir, un programa informático malicioso para solicitud de rescate cuyo único objetivo es la extorsión a cambio de la información. Se solicita el pago, normalmente en criptomonedas, para evitar el rastreo de la transacción.

Según (Dargahi et al., 2019), para que un Ransomware se propague en una organización y provoque una afectación importante, se debe seguir una serie de pasos explicados por el modelo Cyber Kill Chain (CKC), presentado en la imagen y que se describirán posteri



ormente:

En primera instancia, los grupos criminales utilizan técnicas de **ingeniería social** o de reconocimiento; según el modelo ontológico de (Mouton et al., 2016), es la puerta de la intrusión, para la que se utilizan diversas técnicas por antonomasia: el pretexting o pretexto llamativo para una persona o inclusive la organización, un tema que haga sentido e interese para luego dar paso al ya conocido phishing o "pesca", logrando obtener de manera voluntaria información relevante.

Sin embargo, no es la única técnica para obtener datos relevantes; lo son también el Vishing, que es similar al phishing pero mediante llamadas telefónicas, muy conocidas en nuestro contexto como las llamadas de "La Reforma"; el Baiting gancho o cebo que consiste en dejar supuestamente olvidados en lugares públicos dispositivos de almacenamiento secundario como llaves "maya", discos externos, entre otros, para que los transeúntes los recojan, los utilicen en sus dispositivos y comprometan sus equipos; y por último, menos conocido pero psicológicamente muy efectivo es el "Quid pro quo" del latín una "cosa por otra", que se refiere por ejemplo a una llamada de personal de soporte técnico que indica que se debe atender su equipo de manera remota, pero para esto necesita el usuario y contraseña de su equipo.

Todos los casos anteriores son conocidos como vectores de ataque, pero lo son también el reconocimiento de vulnerabilidades relacionadas con sistemas operativos y programas desactualizados, aseguramiento de las plataformas de Tecnologías de Información (TI) a nivel de aplicativos, infraestructura y redes de comunicaciones, así como contar con las soluciones de ciberseguridad adecuadas.

El segundo paso es la intrusión, que el 98% de las veces se da por correos electrónicos con adjuntos comprometidos; de allí la importancia de identificar cuando un correo electrónico es malicioso, sobre todo si es un subtipo de phishing de mayor impacto conocido como whaling o ballenera, que se refiere a pesca masiva, en este caso los correos suplantan a un superior jerárquico reconocido de la organización.

El tercer paso es la explotación de los sistemas computacionales desde adentro, para dar paso a la elevación de privilegios o toma de control. Este punto es especialmente importante puesto que además de controlar el dispositivo, el malware puede iniciar el desplazamiento lateral o explotación de otros equipos en la misma red aprovechando vulnerabilidades similares, pero esta vez con los permisos y autorizaciones del equipo afectado. En este punto inicia la afectación exponencial y posterior ofuscación o encubrimiento de comunicaciones con los servidores de mando o C2 (Command and Control), así como el control del grupo criminal en espera de la señal del ataque orquestado, mejor conocida como denegación de servicio y posterior exfiltración de datos.

Ransomware Conti

Una vez explicado el modo de operación general de los ciberataques, es pertinente analizar el caso particular de operación del grupo criminal detrás del Ransomware Conti.

Este grupo de origen ruso llamado **Trickbot Group** según (WSJ, 2022), opera sistemáticamente de la siguiente manera: en primera instancia utiliza el phishing con el objetivo de infectar los dispositivos de la entidad con un troyano, un tipo de malware que hace alusión a la historia del caballo de Troya.

Se presenta como un programa aparentemente legítimo e inofensivo, normalmente utiliza el malware **Emotet** que a su vez permite la introducción de otro malware más específico conocido como **TrickBot**, mucho más agresivo que encaja dentro de la denominación de botnet (red de robots), este es un software malicioso que convierte los dispositivos en zombi; es decir, trabaja en adelante para el grupo criminal para habilitar el ingreso del ransomware Conti que utiliza la modalidad de doble extorsión: Exfiltrar información confidencial de las víctimas previo al cifrado y amenazar con publicar dicha información a menos que se pague el monto de dinero exigido.

Por consiguiente, el cifrado de archivos genera afectaciones importantes en bases de datos, respaldos e información no estructurada como archivos de ofimática y archivos de sistemas operativos, como resultado se obtiene la denegación de servicio como sucedió en el caso del Ministerio de Hacienda, que a la fecha ha provocado afectaciones importantes sobre todo en la declaración de impuestos y el servicio de aduanero, con implicaciones directas en las importaciones y exportaciones, y afectaciones relacionadas.

Según el último reporte de Cripto Crimen 2022 emitido por la organización especializada Chainalysis, el grupo TrickBot recibió pagos en el 2020 por más de $70 millones y en el 2021 por más de $200 millones, sin embargo, a marzo de este año solo había percibido $13.5 millones, razones por las que posiblemente han ofrecido descuentos.

El Wall Street Journal (WSJ, 2022) indica que, según investigaciones del FBI, TrickBot es un grupo criminal a la baja, debido a las pocas ganancias percibidas durante este año, pero que ha aumentado su actividad luego del inicio del conflicto armado entre Ucrania y Rusia.

Ahora bien, este grupo criminal no solamente se le atribuye Conti, sino que ofrece Ransomware as a Service (RaaS) o Ransomware Como Servicio en la Dark Web o web oscura, inclusive cuenta con un modelo de ganancias en el cual ofrece hasta un 5% de la recompensa obtenida, cuenta con empleados formales presenciales y con teletrabajo. Otro de sus Ransomware muy utilizado por este grupo es **Ryuk** con beneficios menores a los $50 millones en el 2021.

Así las cosas, Conti no es la única amenaza. Según (Kshetri et al., 2022), en el 2021 la corporación CNA Financial pagó $40 millones por la afectación de PhoenixLocker; JBS USA pagó $11 millones por el ransomware Revil; Colonial Pipeline pagó $4.5 millones por DarkSide, este ransomware tuvo beneficios el año pasado por más de $150 millones según (Chainalysis,2022) y ExaGrid pagó por la afectación de Conti $2.6 millones, a pesar de que la demanda original fue de $7 millones.

Ahora bien, si estas organizaciones pagaron por el rescate de la información, salta la duda: ¿por qué no pagar?; muy sencillo, porque si un individuo u organización paga el rescate de la información no hay garantía de que la recupere, inclusive en algunos casos de pago reportado se indica que la recuperación de los datos fue parcial o inclusive inservible;

además, si está dispuesto a pagar seguirá siendo blanco de afectaciones por su disposición al pago.

¿Cómo evitar el ransomware definitivamente?

La respuesta es la misma a la pregunta: ¿cómo eliminar el crimen organizado en el país?; siempre que se detiene a un líder de una banda criminal alguien toma su lugar. Por consiguiente, indiferentemente de las acciones en ciberseguridad, se debe hacer un esfuerzo importante como sociedad costarricense en la cultura de hábitos digitales saludables, reforzar las competencias digitales en identificación de los riesgos ya mencionados como la ingeniería social, identificar por ejemplo cuando un correo es malicioso y cuándo es seguro, es fundamental y muy sencillo.

Aunado a esto, desde el punto de vista de las organizaciones, seguir la implementación de una estrategia de Zero Trust Network Access (ZTNA) o de Confianza Cero en Línea con (Rose et al., 2020), esta confianza cero se debe llevar al ámbito social en materia de tecnologías de comunicación; es decir, desconfiar de un correo electrónico desconocido, de la llamada urgente o de los enlaces extraños, por mencionar algunas buenas prácticas.

Por consiguiente, (Yeoh et al., 2022) presenta un marco de referencia de factores críticos en materia de ciberseguridad sumamente relevantes, en relación con el éxito de la ciberseguridad en las organizaciones, desde un punto de vista interno: de procesos relacionado con la auditoria, desarrollo de competencias, identificación de riesgo y amenazas, y la estrategia de seguridad.

En este último punto es preocupante ya que en el análisis realizado por el PROSIC en referencia al abordaje del tema de ciberseguridad del presidente electo Rodrigo Chávez es muy escaso.

Luego, en relación con la organización, el conocimiento de sus miembros y una cultura pro-seguridad son fundamentales. Por último, la infraestructura de software y hardware deben estar alineados a las políticas de seguridad.

Por lo anterior, resulta fundamental cambiar la percepción de que la ciberseguridad es un gasto y verlo más bien como una inversión en la protección de **uno de los activos más valiosos de cualquier organización: su información**.

¿Cómo aborda a lo interno la UCR el tema de ciberseguridad?

En el caso de la Universidad de Costa Rica (UCR), hemos implementado una serie de acciones para mitigar los ataques de intrusión y explotación de vulnerabilidades.

Estas son: la actualización de contraseñas, el bloqueo de direcciones reportadas por el Centro de Atención de Incidentes de Seguridad Informática (CSIRT) del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT), la revisión del estado de actualización de las plataformas institucionales, el acceso a sistemas por medio de una Red Privada Virtual (VPN), verificación de los sistemas de seguridad como el firewall institucional, adopción de XDR (Extended Detection and Response) que permite la correlación de eventos de seguridad y su mitigación, verificación de cumplimiento de seguridad de los dispositivos que se conecten a la RedUCR, emisión y publicación de lineamientos de seguridad, análisis de vulnerabilidad de los sitios web institucionales,

grupos de enfoque con personal de las diversas instancias universitarias, establecimiento de SandBox o caja de arena para el caso de una eventual infección e inspección constante de servidor de nombres de dominio entre otras, así como el plan de acción en caso de que se detecte la presencia de Conti en nuestra institución.

Finalmente, desde esta Universidad hemos emitido algunas de las medidas más relevantes para evitar ser víctima del Ransomware Conti:

- Utilice contraseñas robustas y que sean difíciles de descifrar, cambiarlas periódicamente y si es posible active el MFA o factor múltiple de autenticación. En caso de requerir ayuda, puede contactar al personal de TI de su unidad.
- Respalde la información de manera periódica; en este sentido le instamos a que utilice la solución como OneDrive para respaldos en la nube provista por la Universidad, como parte del licenciamiento de MS Office 365. El OneDrive le advertirá sobre detección de Ransomware y le guiará en la recuperación de versiones anteriores que no estén infectadas.
- Instale una solución de seguridad confiable en sus equipos, que cumpla con las funciones de antispam, webfilter y antivirus.
- Mantenga sus equipos actualizados, tanto el sistema operativo como las aplicaciones que se utilicen.
- Evite abrir archivos adjuntos o enlaces de correos en los que se desconoce al remitente.
- Evite hacer clic en enlaces de descarga de redes sociales o sistemas de mensajería instantánea como Facebook, Twitter, Whatsapp, Telegram, entre otros.
- Active la opción de mostrar en el sistema operativo las extensiones de los archivos que por defecto vienen ocultas, para evitar abrir archivos maliciosos.
- Deshabilite las conexiones de Escritorio Remoto (Protocolo RDP) cuando no sea necesario.
- En caso de extorsión, evite el pago de la recompensa solicitada, ya que esta no asegura la recuperación de la información y podría fomentar que se continúe con el proceso de extorsión.

Realice respaldos constantemente, pero no en unidades de red, pues estas unidades son utilizadas por Conti para cifrar los respaldos.

Proteger nuestra información, así como la información institucional que tenemos bajo nuestra tutela es también una responsabilidad personal. ¡Juntos y juntas cuidamos nuestra salud digital!

Si desea aprender más sobre Ciberseguridad, puede visitar el micrositio: https://ci.ucr.ac.cr/ciberseguridad.

Referencias:

Dargahi, T., Dehghantanha, A., Bahrami, P. N., Conti, M., Bianchi, G., & Benedetto, L. (2019). A Cyber-Kill-Chain based taxonomy of crypto-ransomware features. Journal of Computer Virology and Hacking Techniques, 15(4), 277-305. https://doi.org/10.1007/s11416-019-00338-7

Kshetri, N., Voas, J., & Voas, J. (2022). Ransomware: Pay to Play? Computer, 55(3), 11-13. https://doi.org/10.1109/MC.2021.3126529

Mouton, F., Leenen, L., & Venter, H. S. (2016). Social engineering attack examples, templates and scenarios. Computers & Security, 59, 186-209. https://doi.org/10.1016/j.cose.2016.03.004

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207

¿Desea enviar sus artículos a este espacio?

Los artículos de opinión de *Voz experta UCR* tocan temas de coyuntura en textos de 6 000 a 8 000 caracteres con espacios. La persona autora debe estar activa en su respectiva unidad académica, facilitar su correo institucional y una línea de descripción de sus atestados. Los textos deben dirigirse al correo de la persona de la Sección de Prensa a cargo de cada unidad. En el siguiente enlace, puede consultar los correos electrónicos del personal en periodismo: https://odi.ucr.ac.cr/prensa.html

Henry Lizano Mora
Director del Centro de Informática de la UCR
HENRY.LIZANO@ucr.ac.cr

Etiquetas: ciberseguridad, informatica, malware, software, estafas, conti, tecnologia, computacion.