

EL CIBERESPACIO, EL NUEVO RETO QUE VIENE AFRONTANDO LA MARINA.



TENIENTE PRIMERO RAMÓN JÁUREGUI IPARRAGUIRRE

Máster en Ciberdefensa por la Universidad de Alcalá de Henares, Licenciado en Ciencias Marítimo Navales por la Escuela Naval del Perú, Licenciado en Ingeniería Industrial por la Universidad de Piura, cuenta con Segunda Especialidad Profesional de Ingeniería de Sistemas por la Escuela Superior de Guerra Naval y una especialización en Tecnologías de la Información por la Universidad Peruana de Ciencias Aplicadas. Ha sido docente de Ciberseguridad de la Escuela Naval del Perú.

RESUMEN

El autor presenta al ciberespacio y su problemática, expone las radican en él y enfatiza el empleo de malware como un vector de ataque. Define APT (amenazas persistentes avanzadas) y describe el impacto que estas puede generar en los intereses de una nación y como esto ha ocasionado que el ciberespacio se considere como dominio para la guerra.

PALABRAS CLAVE

Ciberespacio, ciberdefensa, ciberseguridad, seguridad digital, malware, APT, ciberamenazas.

ABSTRACT

The author presents cyberspace and its problems, exposes the lies in it and emphasizes the use of malware as an attack vector. It defines APT (advanced persistent threats) and describes the impact that these can generate in the interests of a nation and how this has caused cyberspace to be considered as a domain for war.

KEYWORDS

Cyberspace, cyberdefense, cybersecurity, digital security, malware, APT,

El pasado 2 de agosto la Comandancia de Ciberdefensa de la Marina de Guerra del Perú celebró su tercer aniversario de creación. Desde su instauración esta Comandancia viene realizan operaciones militares constantemente, las veinticuatro horas del día y los siete días de la semana. Estás operaciones son diferentes a las convencionales y están orientadas a identificar y neutralizar las amenazas de un ciberespacio complejo y que, junto a ellas, están en mutación y evolución permanente.

El Ciberespacio

Si bien, las generaciones actuales han crecido de cara a la tecnología y se encuentran familiarizadas con ella, pese a ello no todos pueden comprender la magnitud de un término como ese, en su gran mayoría consideran que, el ciberespacio es sólo el internet. Sin embargo,

para otro grupo es una conjunción de elementos: computadoras, servidores, equipos de conectividad, cables de red u ondas electromagnéticas y un sin número de líneas de código de programación, los cuales interactúan entre sí.

Según la norma ISO/IEC 27023:2012[1] (ISO, Internacional Organization for Standardization, 2012) es "el entorno complejo resultante de la interacción de personas, software y servicios en Internet a través de dispositivos tecnológicos y redes conectadas a ella". En consecuencia, este nuevo dominio contempla: componentes geográficos, componentes de redes físicas y lógicas, interfaces y ciber identidades. En ese sentido, entidades como el INCIBE[2] plantean dividirlo en tres capas: Capa física, Capa Lógica y Capa Social; como puede apreciarse en la figura Nro. 1.

Es importante recalcar la consideración de las ciber identidades (usuario y dominios) como parte de su estructura; asignándole una capa exclusiva para representar la interacción que existe entre el ciberespacio y las personas, grupos, organizaciones, u otros tipos entidades. En esta capa se asignan los privilegios y restricciones para el empleo del medio y sus recursos.

Una característica esencial de estas identidades es la impersonalidad, esto implica el potencial de anonimidad de las personas que las utilizan y se manifiesta en la incapacidad para determinar o atribuir actos realizados en o mediante el ciberespacio. Por otra parte, una persona puede asociarse a diversas organizaciones empleándolas. Estas dos consideraciones pueden apreciarse en la Figura Nro. 2.

El ciberespacio, como tal es un entorno

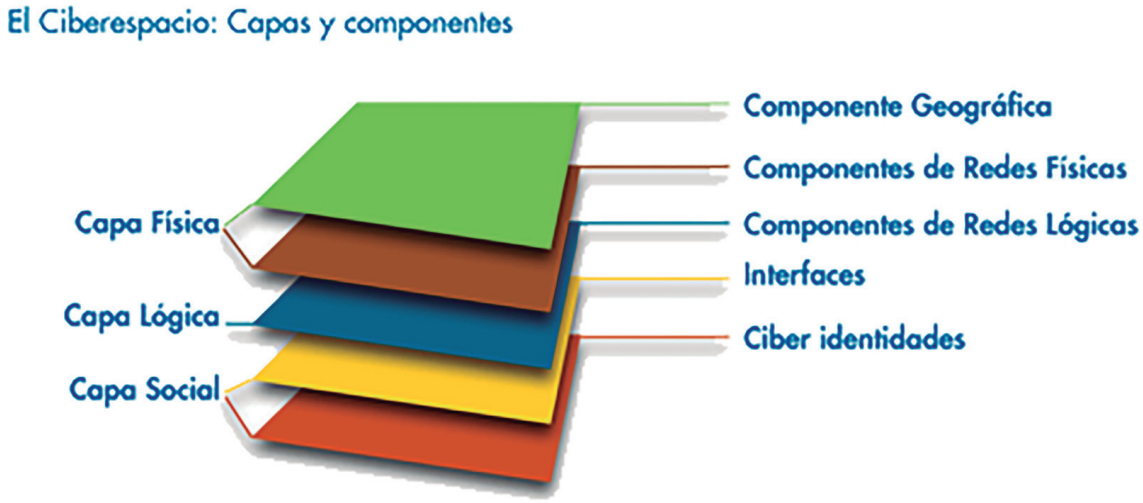


Figura Nro. 1: El ciberespacio: capas y componentes. (INCIBE, Instituto Nacional de Ciberseguridad de España, 2012).

1. ISO/IEC 27023:2012: Information technology — Security techniques — Guidelines for cybersecurity. Norma de estandarización que proporciona orientación para mejorar el estado de la ciberseguridad, destacando los aspectos únicos de esa actividad y sus dependencias en otros dominios de seguridad
2. INCIBE: Instituto Nacional de Ciberseguridad de España, sociedad dependiente del Ministerio de Asuntos Económicos y Transformación Digital a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial.

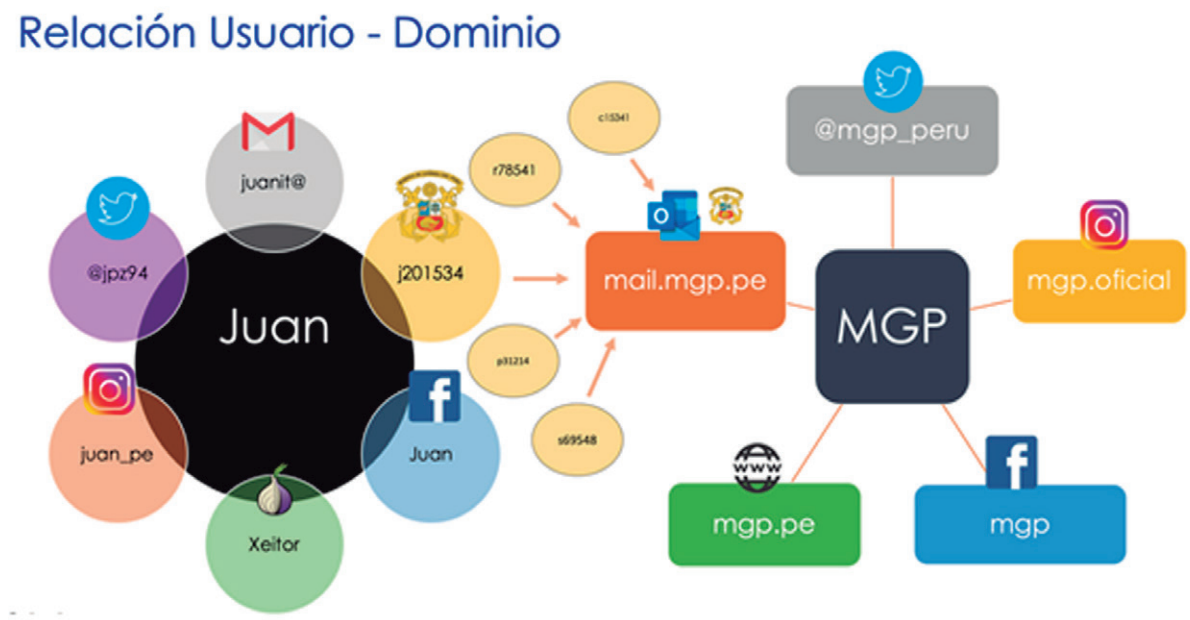


Figura Nro. 2: Relación usuario - dominio (Jáuregui Iparraguirre, Capa lógica y Social, 2020).

atípico y presenta características diferentes a los entornos físicos tradicionales. La relación, "espacio-tiempo" es una de ellas, pues contrastada con el medio físico convencional, es prácticamente imperceptible para el usuario, ofreciéndole acceso a redes y servicios geográficamente distantes en segundos o fracciones de estos. Visto desde una perspectiva distinta, esta rápida interconexión concede al atacante la facultad de afectar una infraestructura informática determinada desde cualquier parte del mundo, prácticamente en tiempo real. En ese sentido, considerando la anonimidad antes expuesta, podemos concluir que, la ventana de tiempo para detectar y reaccionar ante una ciberamenaza es extremadamente corta y las posibilidades de identificar adecuadamente la autoría, es compleja.

Otro aspecto por considerar es la dependencia que le ha generado el ciberespacio a la humanidad, esto a través del empleo exponencial de las tecnologías de la información y comunicaciones, aplicables a personas, sociedad civil, la academia y principalmente a organizaciones del Estado, entre ellas las Fuerzas Armadas. Estas herramientas de hardware y software mejoran día a día para ofrecer una amplia gama de funcionalidades que, fortalecen esa dependencia. En el caso puntual de los sistemas de información, se diseñan y programan para cada proceso del modelo negocio, permitiendo su automatización total o parcial, recopilando, procesando y produciendo su información de utilidad y gran valor para una mejor toma de decisiones y de la gestión de recursos.

Estas condiciones y características son propicias para cualquier actor de interés que pueda constituirse como una amenaza. Estos actores, se encuentran en todos los niveles, ellos analizan sus objetivos para identificar sus vulnerabilidades o brechas

de inseguridad que, tras ser explotadas les permitan afectar la integridad, confidencialidad y disponibilidad de la información o infraestructuras informáticas de sus objetivos. El impacto causado puede variar desde comprometer el servicio de correo electrónico de una persona natural hasta afectar el funcionamiento de un complejo sistema de control para una infraestructura crítica.

Los actores antes mencionados pueden ser simples ciberdelincuentes, grupos de crimen organizado, hacktivistas[3], hasta estados y agencias de inteligencia; cada uno de estos ostenta una capacidad y objetivos claramente diferentes entre sí. Asimismo, los recursos que disponen para realizar sus acciones y la sofisticación de los mecanismo o técnicas que se empleen en ellas, lo cual se verá reflejado en el impacto que puedan generar. (Aguirre Ruiz, 2020)

Los mecanismos y técnicas para realizar un ciberataque son tan variados como la cantidad de vulnerabilidades de cada uno de los elementos que componen una infraestructura informática. Asimismo, el conocimiento para realizarlos es de fácil acceso, ya que está disponible en fuentes abiertas. Resta reconocer y analizar el objetivo para establecer el mejor curso de acción y el vector de ataque hacia este.

El Malware o código malicioso

Entre los mecanismos antes mencionados tenemos al malware[4], quizás la herramienta más versátil y utilizada para perpetrar un ataque. Su funcionalidad, está limitada a su finalidad y la inventiva de su creador. Por otra parte, su distribución está sujeta a técnicas complementarias, principalmente técnicas de ingeniería social que se centran en el factor humano y sus debilidades. Como desventaja tenemos que, su vida útil es corta, pues está estrechamente vinculada a la vigencia de la vulnerabilidad, sobre la cual se ha diseñado y lo inadvertido que sea su comportamiento ante las herramientas de seguridad que haya implementado la víctima o la organización a la cual pertenece; he de afirmar que mientras no se ponga en evidencia su efectividad será muy alta.

La clasificación de un malware suele enmarcar sus aspectos funcionales; ello significa que, al analizar el comportamiento sobre la víctima. Este ejecutará sentencias que le permitirán alcanzar un estado deseado por el atacante, en función a esto se le asignará una clasificación.

Como se observa en la Figura Nro. 3, la organización B.Secure[5], agrupa la mayoría de los malware en tres categorías básicas. Sin embargo, estas categorías no son mutuamente excluyentes. Por citar un ejemplo, un programa malicioso puede utilizar técnicas para facilitar su distribución dentro de la red objetivo, como un virus y también establecer conexiones remotas de comando y control con el atacante, como un troyano; considerando la imagen anterior puede atribuírsele dos categorías de primer nivel en simultaneo: "malware destructivo" y "malware de control".

Otra forma de clasificar el malware es no establecer niveles y adoptar como criterio la funcionalidad más preponderante. En

3. Hactivistas: proviene del término hacktivismo, el cual refiere al uso de computadoras y redes de informática como una forma de rendir protesta con fines políticos
4. Malware: Programa malicioso y ajeno al sistema operativo que se ejecuta sin consentimiento del usuario para realizar ajeno acciones puntuales.
5. BSecure, Empresa de nacionalidad colombiana con más de dos décadas de trayectoria y especializada en ofrecer servicios de ciberseguridad y seguridad de la información. "Tipos de Malware más comunes", https://www.b-secure.co/recursos/infografias/tipos-mas-comunes-de-malware.

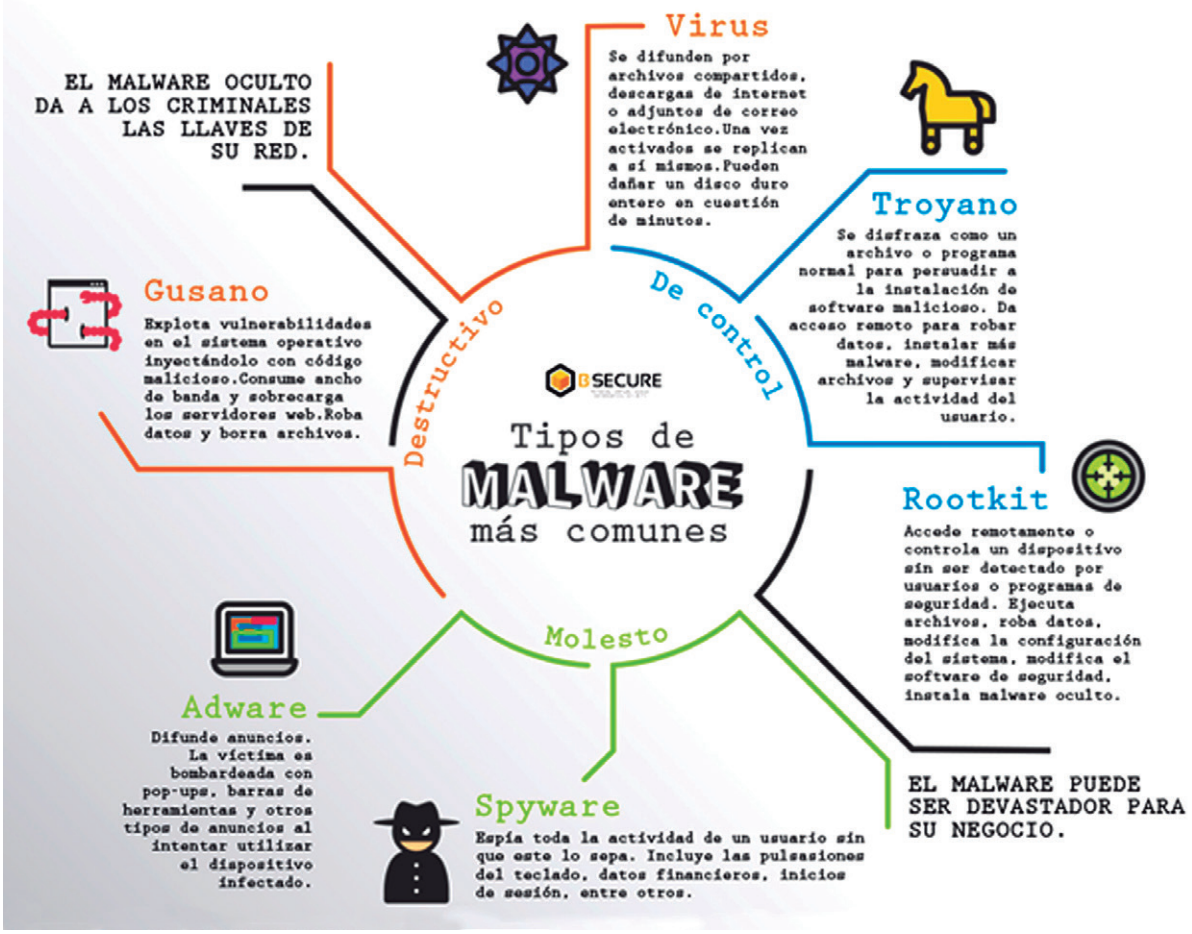


Figura Nro. 3: Tipos de malware más conocidos. (B-Secure, s.f.).

ese aspecto, la cantidad de tipos que pueden establecerse pueden aumentar conforme se ideen nuevas maneras de afectar la ciberseguridad. Siendo los más comunes los que se detallan en la Figura Nro. 4.

Como indica en la investigación "Desarrollo de un sistema de análisis e ingeniería inversa de código malicioso" (Bermejo Higuera, 2015), entre las principales acciones que realiza un código malicioso, señala lo siguientes:

- Envío de correo a gran escala. El malware obtiene el sistema direcciones de correo electrónico para utilizarlo como medio de propagación.
- Eliminación de archivos. Suele borrar archivos clave sin los cuales el ordenador o un servidor no puede arrancar o funcionar correctamente; por ejemplo, en sistemas Windows: boot.ini, ntdetect. com, ntldr, ntoskrnl.exe y otros archivos de arranque.
- Modificación de archivos. El software intenta modificar archivos para incluir troyanos en archivos ejecutables o actualizaciones de Windows
- Modificación de claves del registro u otro tipo de datos de configuración.

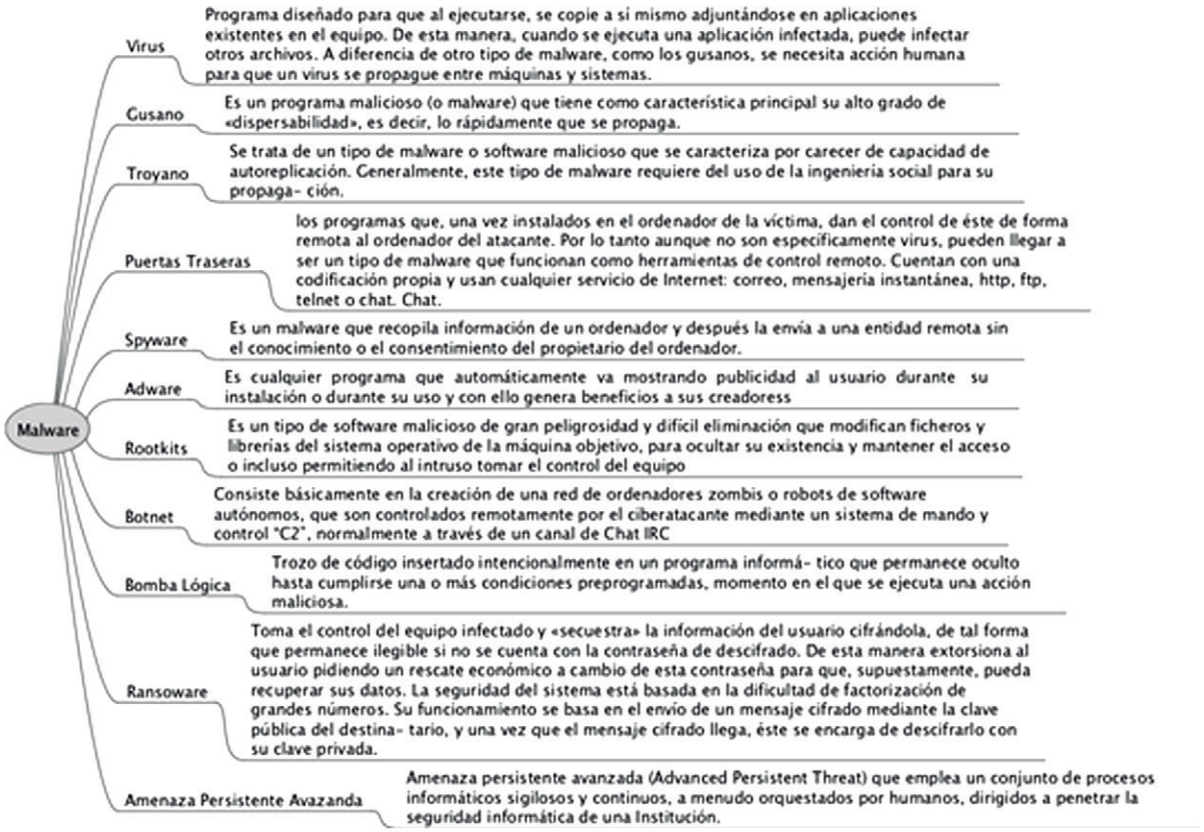


Figura Nro. 4: Tipos de malware (Jáuregui Iparraguirre, Aplicación de la Metodología de Análisis de Malware para la APT DARKCOMET, 2018).

Algunos tipos de malware intentan desactivar anti-virus, anti-spyware, firewall y otros tipos de software para poder realizar una mayor explotación y uso no autorizado.

- Degradación del rendimiento. El software malicioso puede provocar problemas de rendimiento en el sistema afectado, por ejemplo el gusano W32.Korgo.F produce problemas de rendimiento en la red.
- Inestabilidad del sistema. El software malicioso puede provocar problemas de estabilidad en el sistema afectado.
- Robo de información corporativa y confidencial. Por ejemplo, el gusano W32.Korgo.F al funcionar como puerta trasera permitiendo accesos no autorizados.
- Modificación de la configuración de seguridad. El software modifica la configuración de seguridad y abre puertos para permitir el uso no autorizado. Por ejemplo el gusano W32. Netsky.Y abre una puerta trasera en el puerto 82.

Amenazas persistentes avanzadas

Las acciones antes mencionadas varían de acuerdo con el tiempo, aumentando esta

lista y haciéndola cada vez más compleja. Como detalla el portal Wired[6] en su artículo "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History" (WIRED, 2011), el salto evolutivo más grande registrado por un malware se evidenció el 17 de junio del 2010, cuando Sergey Ulasen, Jefe de la División Antivirus de la Empresa de seguridad informática VirusBlokAda en Minsk, en base a una muestra obtenida de la computadora de uno de sus clientes, se apodera del virus que la infecta y observa que, esta usa un exploit de tipo "día cero" para propagarse.

VirusBlokAda contactó a Microsoft para informarle sobre la vulnerabilidad y evidenciar la necesidad de un parche de seguridad, el cual se puso en servicio el 12 de julio de ese año. VirusBlokAda hizo público el descubrimiento en un foro de seguridad, así las compañías de antivirus de todo el mundo se apresuraron a tomar muestras del malware, al cual Microsoft denominó como "Stuxnet", por la combinación de nombres de dos archivos encontrados en el código y que eran parte del proceso de infección ".stub y MrxNet. sy". (SYMANTEC, 2010)

Stuxnet, estaba diseñado para establecer un canal encriptado de comunicaciones de comando y control con un servidor remoto, mediante una conexión reversa, siendo la primera vez en la historia en emplearse esta técnica. Esta funcionalidad facultaba al atacante de analizar el entorno y mediante el control remoto del equipo, realizar acciones de extracción de información o búsqueda de otros equipos de interés para saltar hacia ellos y también poder controlarlos. El conjunto de bondades y los métodos que se emplearon para desplegarlo hicieron que Stuxnet sea catalogado como la primera Amenaza Persistente Avanzada (APT, por sus siglas en inglés), que es el escalón más alto en la clasificación de un ataque, no sólo por el impacto que este puede generar en una organización o la variedad de funcionalidades que puede llegar a tener, sino por la gran complejidad de técnicas y procedimientos que se realizan previa, durante y posteriormente a la realización del ataque.

Este tipo de amenazas requieren una gran inversión para su diseño y creación, demandando incluso sofisticados trabajos de Inteligencia Militar, lo cual no es una capacidad habitual en los atacantes individuales o grupos hacktivistas de recursos limitados, sino que es propio de organizaciones Gubernamentales o Agencias de Inteligencia.

La multinacional Kaspersky[7] señala que "Hay dos maneras de ver la APT, como concepto y como persona, por un lado, se refiere a una especie de ciberataque sofisticado, muy preciso por otra parte puede referirse a aquellos grupos, normalmente patrocinados por los estados que son los responsables del lanzamiento de dichas campañas maliciosas". (KASPERSKY, 2013)

Como bien se señala en el artículo "Advanced Persistent Threats" (SYMANTEC, 2016), el proceso general que se realiza al desplegar una APT consta de las siguientes fases:

I. Incursión: Buscará generar el acceso dentro de la red objetivo y se realiza principalmente mediante la aplicación de técnicas de ingeniería social.

II. Descubrimiento: Una vez dentro de la

7. Kaspersky, empresa multinacional fundada en 1997 en Rusia, especializada en brindar productos y servicios de ciberseguridad a entidades públicas y privadas a nivel mundial.

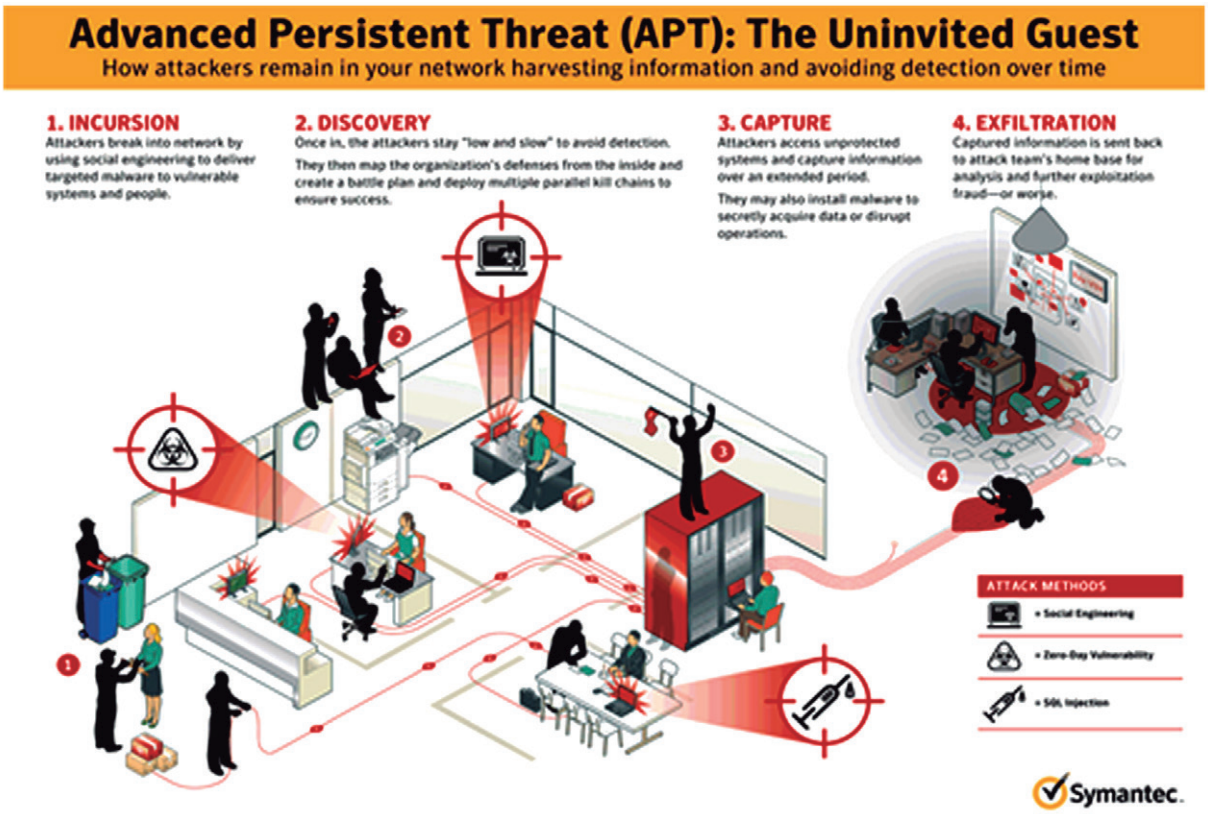


Figura Nro. 5: Amenazas persistentes avanzadas. (SYMANTEC, 2016).

red, la amenaza identificará los activos y se desplegará realizando saltos laterales y ganando privilegios hasta identificar el objetivo principal o de mayor valor.

III. Captura: La amenaza buscará hacerse del activo principal y obtener un usuario con los privilegios necesarios para tomar el control total del activo.

IV. Exfiltración: establecerá un canal que le permita extraer la información de interés, aplicando técnicas de ocultamiento y persistencia[8].

La Figura Nro. 5, describe gráficamente el proceso de una Amenazas persistentes avanzadas (APT). Se presume que, el código fuente de Stuxnet y toda la gama de funcionalidades que contenía, sirvió de base para la creación de nuevas APT, las cuales se hicieron más recurrentes. Prueba de ello son las APT DUQU, FLAME, DARKCOMET, CARETO[9]. Asimismo, se estima que existe un buen número de estas ejecutándose sin ser aún detectadas. Las amenazas de tipo APT, son cada vez más frecuentes, organizadas y complejas. Asimismo, estas se consideran como la

8. Symantec: corporación internacional de origen norteamericano, dedicada a ofrecer servicios y productos de software especializados en cibeseguridad para infraestructuras informáticas. "Advanced Persistent Threats: A Symantec Perspective".
9. DUQU, FLAME, DARKCOMET, CARETO: Amenazas persistentes avanzadas que reutilizaron las fuentes y el modelo de Stuxnet, en los años siguientes a este.

máxima evolución del malware por su diversa polivalencia, pudiendo considerarse como ciberarmas por excelencia y tanto su empleo como desarrollo demandan recursos y capacidades muy onerosas; por ello se presume que puedan estar financiado por organizaciones afines a estados ya que su impacto trasciende la economía una empresa hasta niveles que podrían considerarse estratégicos, incluso políticos.

Como ya se mencionó, el ciberespacio no es ajeno al ámbito militar. La interacción con él es de vital importancia para el comando, control y comunicaciones de las fuerzas; tanto en la parte operacional como la administrativa y logística. Los sistemas de información que se emplean demandan particularidades especiales y se rigen a estrictas políticas de seguridad para mantener un óptimo nivel de confiabilidad, integridad y disponibilidad de las plataformas y su información; siendo esta última por naturaleza clasificada y cuyo riesgo de transgresión significa un alto impacto en la seguridad nacional.

En el año 2020, la compañía de seguridad informática ESET[10] publicó el "Security Report Latinoamérica 2020", en el cual señala que, en promedio el 60% de empresas en la región ha registrado incidentes de seguridad, presentando una mayor frecuencia en países como Ecuador y Paraguay, como se aprecia en la Figura Nro. 6. Asimismo, indica que los tres incidentes de seguridad con mayor recurrencia son: infecciones de malware con un 30%, acceso indebido a aplicaciones y/o bases de datos con un 18% y ataques de ingeniería social con un 15%. Técnicas estrechamente relacionadas a las fases de una APT. (ESET, 2020)

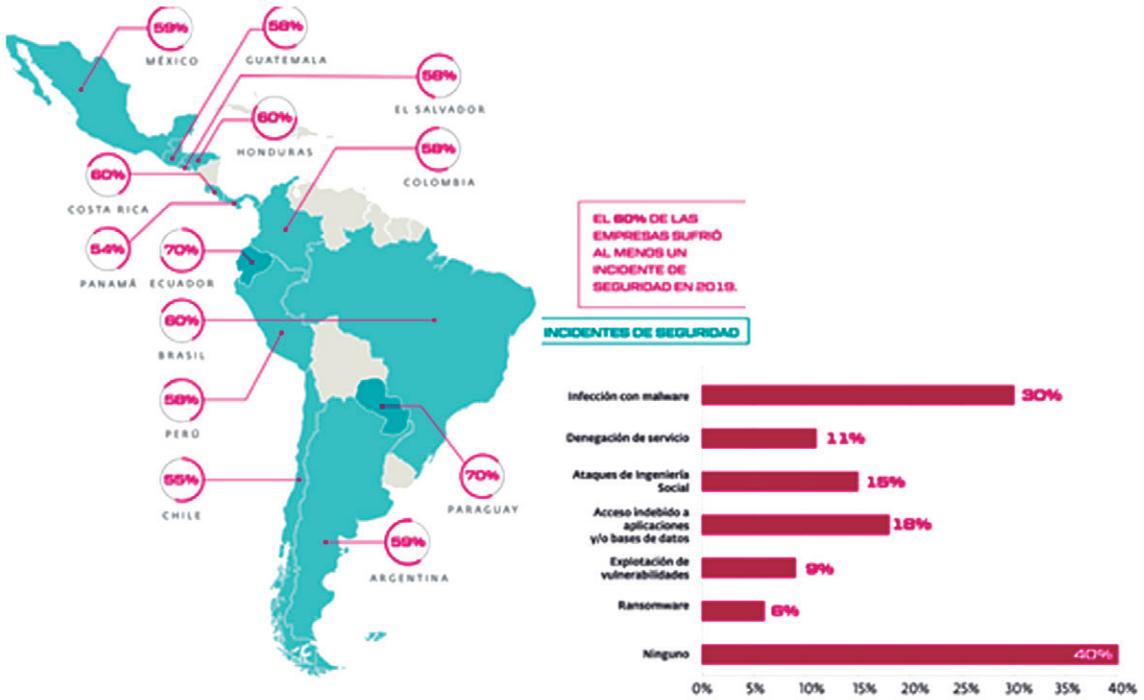


Figura Nro. 6: Empresas con incidentes de seguridad por país de la región (ESET, 2020).

10. ESET: Compañía de seguridad fundada en el año 1992 en Eslovaquia, produce software de ciberseguridad comercializado a nivel mundial con mas de 110 millones de usuarios registrados.

Por otra parte, en el año 2018 se presentó el caso "APT38". Esta amenaza afectó los sistemas bancarios de 13 países. En América, habría ocasionado pérdidas cercanas a los $100 millones en Chile, en adición fue identificada en países como Estados Unidos, Brasil y Uruguay. El impacto global del incidente se aprecia en la Figura Nro. 7.

En el documento de análisis "APT38Un-usualSuspects", realizado por la Empresa FireEye[11] se señala que la APT tiene la capacidad de reconocer los sistemas bancarios y emplear las operaciones SWIFT[12] para perpetrar el ataque; asimismo, establece posibles conexiones con el gobierno de Corea del Norte y el grupo Lazarus[13], al cual ya se le han atribuido otros de ataques como el malware de espionaje

Conclusión

En ese sentido, por el nivel de impacto que puede alcanzar un ciberataque y sumado a la coyuntura global, es necesario a considerar al ciberespacio como parte del teatro operaciones, asumiéndolo como el quinto dominio de la guerra. Al respecto, países como Estados Unidos, China, España, Brasil, Italia, Alemania, entre otros más; han confiado a sus Fuerzas Armadas

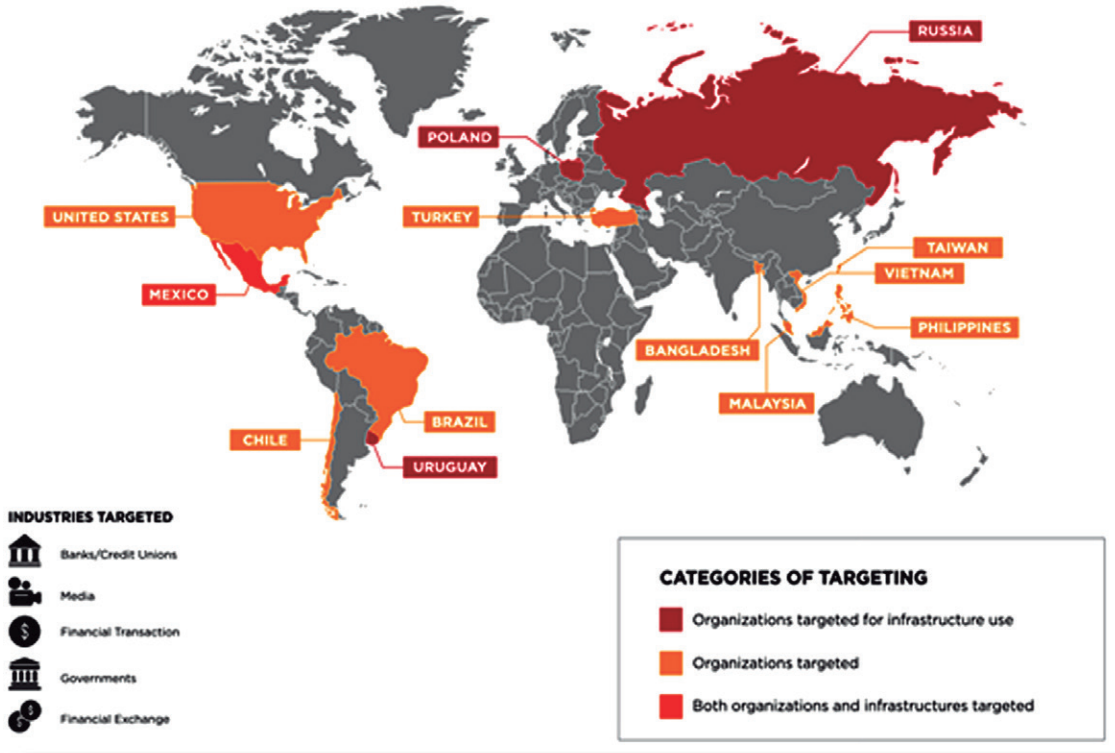


Figura Nro. 7: APT38 global targeting (FireEye, 2018).

11. FireEye: Empresa de origen estadounidense, dedicada a la producción y comercialización de soluciones de hardware y software de ciber-seguridad, detección de amenazas y análisis de riesgos. cibers"APT38Un-usualSuspects", disponible en https://content.fireeye.com/apt/rpt-apt38
12. SWIFT: Es un sistema de mensajería interbancario de transferencias transfronterizas que se utilizan en la mayoría de los bancos del mundo.
13. Lazarus: Grupo cibercriminal acusado de delitos como espionaje, extorsión y la distribución del malware a gran escala.

la implementación y/o fortalecimiento de capacidades de ciberdefensa; las cuales empleán en operaciones militares para alcanzar objetivos en los diferentes niveles de la guerra o en pro del resguardo de la ciberseguridad de sus naciones.

Finalmente, la Marina de Guerra del Perú ha contado, desde hace más de dos décadas, con políticas y procedimiento de seguridad de la información y comunicaciones destinadas a garantizar un correcto nivel de aseguramiento de la infraestructura informática y de comunicaciones institucional. Sin embargo, la gran complejidad y evolución de las amenazas en el ciberespacio demandó que, en el año 2018, el Alto Mando Naval dispusiese la creación de la Comandancia de Ciberdefensa de la Marina. Este órgano de línea tiene la misión de planear y conducir operaciones militares de defensa del ciberespacio, explotación de amenazas cibernéticas y respuesta; para asegurar el empleo efectivo de este dominio y contribuir al esfuerzo en la guerra. (Marina de Guerra del Perú, s.f.)

Este, es el nuevo reto que ha asumido la Institución de cara a su bicentenario. Un reto que, como siempre, sabrá afrontar y continuará contribuyendo a garantizar la seguridad e integridad de la Nación. Así lo exige esa consigna permanente, aquella que se grita a viva voz cada día a orillas de cripta del Gran Almirante Miguel Grau y que dice: "Seguid su ejemplo".

Bibliografía

- INCIBE, Instituto Nacional de Ciberseguridad de España. (2012). La Ciberseguridad Nacional, un compromiso de todos. Madrid, Madrid, España.
- Aguirre Ruiz, J. (2020, Marzo 10). Fundamentos de Ciberseguridad. Callao, Lima, Perú.
- Jáuregui Iparraguirre, R. (2020, Mayo 8). Capa lógica y Social. Callao, Lima, Perú.
- Jáuregui Iparraguirre, R. (2018, Abril 23). Aplicación de la Metodología de Análisis de Malware para la APT DARKCOMET. Lima, Lima, Perú.
- Bermejo Higuera, J. (2015, 6 12). DESARROLLO DE UN SISTEMA DE ANALISIS E INGENIERIA INVERSA DE CODIGO MALICIOSO. Madrid, Madrid, España.
- KASPERSKY. (2013, 06 11). ¿Qué es una APT? Retrieved from kaspersky.es: https://www.kaspersky.es/blog/que-es-una-apt/966/
- WIRED. (2011, 11 7). How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History. Retrieved from WIRED.COM : https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/
- B-Secure. (n.d.). https://www.b-secure.co . Retrieved from Tipos de Malware más comunes: https://www.b-secure.co/recursos/infografias/tipos-mas-comunes-de-malware
- ISO, Internacional Organization for Standardization. (2012). ISO/IEC 27032:2012 Information technology — Security techniques — Guidelines for cybersecurity. Retrieved from https://www.ISO.ORG : https://iso.org
- ESET. (2020). Security Report Latinoamérica 2020. Latinoamérica.
- FireEye. (2018). APT38 Un-usual Suspects. California, California, Estados Unidos.
- SYMANTEC. (2016). Advanced Persistent Threats: A Symantec Perspective. Disponible. Estados Unidos de América.
- SYMANTEC. (2010, 09 30). W32.Stuxnet Dossier. Estados Unidos de América.
- Marina de Guerra del Perú. (n.d.). LA COMANDANCIA DE CIBERDEFENSA . Retrieved from https://www.marina.mil.pe: https://www.marina.mil.pe/es/organos/comciberdef/comandancia/