UNODC
Oficina de las Naciones Unidas contra la Droga y el Delito

Viena, 14/04/2020

CIBERDELITO Y COVID-19: Riesgos y Respuestas

CONSIDERACIONES CLAVE

- **El ciberdelito evoluciona y crece como resultado de la pandemia del COVID-19.** El fraude cibernético, la extorsión y el abuso sexual infantil en línea tienen como objetivo a las personas, mientras que el*malware* (software malicioso) afecta a los sistemas informático (incluyendo sistemas de hospitales). La creciente difusión de desinformación continuará confundiendo al público y obstaculizando la implementación de respuestas basadas en ciencia.
- **El teletrabajo ha aumentado el universo de potenciales víctimas del ciberdelito. Los usuarios toman mayores riesgos en línea mientras están en casa, lo cual, inintencionalmente, expone los sistemas informáticos de sus empresas frente a delincuentes.** A través del *pshising* (fraude cibernético) se puede llegar a obtener acceso con fines maliciosos a sistemas informáticos críticos, lo cual puede ser aprovechado por ciberdelincuentes y otros actores.
- **El número de operadores de justicia especialistas en combate del ciberdelito será reducido durante la mayor parte del año 2020.** Los ciberdelincuentes explotarán aquellos vacíos operativos que detecten. Sin embargo, de forma contraintuitiva, esta situación creará oportunidades tácticas y estratégicas para los operadores de justicia.

Contexto

1. Este reporte provee una imagen de las amenazas del ciberdelito en el contexto de la pandemia del COVID-19. El mismo ha sido elaborado a partir de informes confidenciales de todo el mundo provistos a UNODC por parte de policías, gobiernos, ONG, academia, prensa, sector privado, así como fuentes abiertas durante los primeros días de abril de 2020. Al final de cada sección temática se presentan recomendaciones.

Estado de la Situación: El Ciberdelito, Evolucionando, Incrementando y Vulnerando

2. Alrededor del mundo, están siendo implementadas fuertes medidas de distanciamiento social. Esto ha derivado en un mayor uso de la comunicación digital por parte de autoridades públicas, negocios e individuos. Muchas personas no están familiarizadas con el uso de la tecnología de la información a esta escala. Este contexto presenta una cantidad amplia, atractiva y vulnerable de potenciales víctimas que pueden ser explotadas por ciberdelincuentes. La combinación del teletrabajo y enseñanza en línea ha producido que haya un mayor número de usuarios de Internet, quienes conocen menos sobre las amenazas en línea y que son especialmente proclives a tomar mayores riesgos al hacer uso de las

tecnologías de la información cuando se encuentran en casa, en comparación a cuando se encuentran en el trabajo o la escuela

3. Los ciberdelincuentes han hecho que sus modos operandi evolucionen con el propósito de explotar las vulnerabilidades sociales, legales y psicológicas asociadas al COVID19. Los niños de edad escolar están siendo seleccionados como blancos de forma masiva por parte de agresores sexuales en línea, esto aplica tanto para niños que recién comienzan a hacer uso del Internet, como aquellos que poseen más experiencia. Esta situación incluye a delincuentes que pretenden agredir a niños a través del *grooming*[1] (persuasión en línea) o *sextortion*[2] (extorsión sexual en línea), lo cual están consiguiendo a través de la infiltración masiva en clases en línea,[3] lo cual se conoce ahora como "*zoom-bombing*".
4. Los ciberdelincuentes crecientemente están aprovechándose del miedo que el COVID-19 genera entre la población, vendiendo en Internet curas falsas y defraudando en línea a través de la venta de sanitizantes para manos y equipamiento médico de protección personal, medicinas y productos higiénicos que en realidad no existen. Otros tipos de fraude reportados son la promoción de servicios como oportunidades de inversiones poco seguras (incluyendo criptomonedas), así como consultas y diagnósticos médicos incorrectos. Uno de los principales sitios web de pornografía ofreció suscripción gratuita a los usuarios de un país, lo cual ha incrementado el riesgo de descarga de *malware* y de *sextortion*.
5. Los adultos de edad avanzada, quienes, en muchos casos, se encuentran menos sensibilizados sobre los riesgos que existen en el Internet, son perfilados y buscados específicamente por ciberdelincuentes, para que descarguen y reenvíen a sus amigos y familia correos electrónicos spam que contienen vínculos infectados con *ransomware* (software malicioso para el secuestro de datos), así como desinformación. Asimismo, los ciberdelincuentes continuamente extorsionan a sus víctimas, argumentando que saben (y que revelarán) sobre el supuesto hábito de sus víctimas respecto al acceso a pornografía en línea.
6. Los ataques tipo *business email compromise*[4] (que consisten en correos electrónicos provenientes de cuentas que pretenden ser de un alto oficial de la organización afectada), se basan en el uso de la ingeniería social, facilitada por el sentido de urgencia creado por la pandemia, con el propósito de provocar la transferencia de fondos hacia una cuenta bancaria controlada por criminales, probablemente en el extranjero, o hacia un monedero (cuenta en criptomoneda). Asimismo, el *business email compromise* está siendo utilizado para obtener información sensible para fines maliciosos, como el espionaje.
7. En foros en la web oscura se continúa vendiendo información obtenida a través de acceso no autorizado a sistemas (incluyendo información privada de oficiales de alto rango y celebridades). Delincuentes que son nuevos en el ciberdelito están buscando asesoría de ciberdelincuentes establecidos para conocer cómo explotar la pandemia del COVID-19 para obtener ganancias. Algunos ciberdelincuentes han tratado de disuadir a otros de sus similares para que no afecten con ataques distribuidos de denegación

[1] https://www.esafety.gov.au/parents/big-issues/unwanted-contact
[2] https://www.esafety.gov.au/key-issues/image-based-abuse/take-action/deal-with-sextortion
[3] https://tcrn.ch/3buz3gW
[4] https://www.trendmicro.com/vinfo/us/security/definition/business-email-compromise-(bec)

de servicio (DDOS) o con *malware* a hospitales ni a laboratorios donde se prueban vacunas. Agresores sexuales de niños se mantienen discutiendo sobre cuáles redes sociales o sitios para intercambiar imágenes son los más viables para encontrar niños a quienes abusar. Los ciberdelincuentes también continúan debatiendo sobre cómo identificar y enfrentar policías que se encuentran realizando trabajo encubierto en línea.

8. Además del ciberdelito más tradicional, grupos que realizan amenazas persistentes avanzadas continúan evolucionado y explotando la pandemia. Las amenazas persistentes avanzadas tienen como blanco la infraestructura crítica nacional, e incluyen entre sus blancos a hospitales y laboratorios de desarrollo de vacunas, sus instrumentos incluyen *malware*, *ransomware* y ataques D-DOS. La motivación de esta clase de ataques no está basada simplemente en beneficios económicos, dado que el *malware* en muchas ocasiones busca obtener acceso a credenciales de ingreso y otra información sensible con valor de inteligencia.
9. Buena parte de la ciberdelincuencia relacionada al COVID-19 está basada en el uso de *phishing* a través de correo electrónico como vector inicial de la infección. Cuando la gente hace click en un link o en un documento, su cuenta queda vulnerada. Dicha vulneración puede ser evidente para la víctima, sin embargo, la mayor parte de veces, la vulneración queda encubierta lo cual facilita al ciberdelincuente establecer y mantener un acceso a largo plazo sobre dicha cuenta, la organización y la tecnología de la información asociada. Además de obtener información sensible, los actores que constituyen amenazas persistentes avanzadas pueden alterar sitios web, modificar detalles de documentos, eliminar información y diseminar desinformación.
10. **UNODC recomienda que los gobiernos y el sector privado aumenten la implementación de campañas públicas de sensibilización, que sean culturalmente respetuosas y fáciles de comprender. Otro elemento clave de la respuesta, es el establecimiento de números telefónicos dedicados a la denuncia anónima de casos de abuso sexual infantil en línea. También recomendamos que las actualizaciones de seguridad informática sigan siendo continuamente aplicadas y que la información digital sea constantemente respaldada.**

<u>Capacidad reducida de los operadores de justicia y resiliencia social</u>

11. En muchos países, el personal especializado en combatir el ciberdelito ha cesado de investigar casos de ciberdelito con el objetivo de apoyar las medidas gubernamentales contra la propagación del COVID-19, por ejemplo, en la implementación de cuarentenas. Asimismo, hay casos de operadores de justicia especializados en ciberdelito contagiados. Se espera que en las próximas semanas la capacidad para combatir el ciberdelito se vea reducida, lo cual afectará el margen de maniobra de los estados para contrarrestar nuevas y crecientes amenazas cibernéticas.
12. En muchos países, los procesos investigativos y judiciales han sido afectados, dado que no es posible satisfacer la necesidad de realizar dichos procesos en persona como consecuencia de las medidas de salud pública. En este sentido, algunos países rápidamente han implementado procesos judiciales en línea.

13. La desinformación en relación con el virus continúa esparciéndose, primordialmente a través de redes sociales y servicios de mensajería instantánea encriptados. Las empresas de redes sociales se han visto también afectadas por el teletrabajo de su personal, el cual es un factor que obstaculiza hacerle frente al gran volumen de contenido de desinformación, asimismo afecta la forma en que estas empresas implementan políticas internas y se adaptan al impacto de diferentes legislaciones nacionales.
14. La desinformación y los ataques a la infraestructura crítica nacional merman la confianza pública en las autoridades y debilitan la efectiva aplicación de medidas de salud y seguridad pública.
15. **UNODC recomienda que los procesos judiciales continúen en línea, en aquellos casos que sea posible, a la vez que se garantice el respeto a estándares y normas internacionales, al debido proceso y al estado de derecho.**
16. **También recomendamos que las empresas de redes sociales hagan más para combatir la difusión de la epidemia de desinformación alrededor del COVID-19, al mismo tiempo que se proteja la libertad de expresión. La ciencia y las respuestas basadas en evidencia deben estar al centro de la respuesta al COVID-19. Todos tenemos un rol fundamental que desempeñar en esto.**

Análisis

a. *La pandemia del COVID-19 representa un reto global sin precedentes que afecta a toda la sociedad. Mucha gente ha transferido sus actividades físicas a operaciones en línea, de forma similar han operado los delincuentes. Al mismo tiempo que el ciberdelito incrementa en complejidad y las víctimas incrementan en cantidad, en algunos países los operadores de justicia están siendo trasladados a realizar otras funciones. El impacto económico del COVID-19 implica otra capa más de complejidad tanto para los pueblos como para los gobiernos. Una tormenta perfecta que ofrece oportunidades para la cibercriminalidad se avecina.*
b. *En la media que el COVID-19 y las amenazas de la ciberdelincuencia vinculadas a esta crisis son globales, en esa misma medida las respuestas deben ser globales: combatir el ciberdelito en una jurisdicción reduce el nivel riesgo a nivel global. Información sobre nuevas amenazas y nuevos tipos de delitos, como el análisis de Europol sobre el COVID19 y la evaluación de amenazas cibernéticas de INTERPOL, deben ser continuamente compartidas a nivel internacional y sin retrasos, las líneas telefónicas dedicadas al reporte anónimo de casos de abuso sexual infantil en línea constituyen una herramienta crítica de empoderamiento del pública para contrarrestar esta amenaza.*
c. *Considerando los obstáculos al trabajo policial proactivo y reactivo, prevemos que la capacidad para investigar activamente el ciberdelito se verá afectada al corto plazo, en especial en países con recursos limitados incluso antes de la pandemia. Los ciberdelincuentes, incluyendo los grupos de amenazas avanzadas persistentes, continuarán explotando esta situación. Se debe incrementar la difusión de información sobre arrestos exitosos o disrupción de actividades de ciberdelincuentes. Operaciones de alto impacto, como el reciente cierre en una semana de quince proveedores de servicios criminales*

dedicados a ataques D-DOS en los Países Bajos,[5] son útiles para visibilizar el impacto de este tipo de operaciones, y recordarles a los ciberdelincuentes que otras operaciones como estas continúan implementándose alrededor del mundo. De forma contraintuitiva, los ciberdelincuentes pueden tomar más riesgos en línea en la medida que creen que la posibilidad de ser detectados ha disminuido, En este sentido, las investigaciones policiales especializadas deben continuar sin bajar el ritmo.

d. *La diplomacia pública y la sensibilización son críticas para la prevención y estas deben empoderar a grupos vulnerables, especialmente a niños y adultos de edad avanzada. Las acciones contra la desinformación deben proveen información verificada, creíble y útil. Esto debe ser hecho de forma transparente y con rendición de cuentas.*
e. *Todas las acciones para combatir el ciberdelito deben ser proporcionadas, legales, sujetas a rendición de cuentas y necesarias. La tecnología está siendo utilizada por muchos gobiernos para monitorear, identificar y rastrear potenciales pacientes con COVID-19. Este trabajo esencial debe permanecer bajo escrutinio, con una supervisión clara, para garantizar que las medidas de vigilancia sean cesadas una vez se logre el control de la propagación. Ahora es el momento de construir confianza digital con el público, de trabajar juntos para enfrentar las mayores amenazas de nuestro tiempo y de construir confianza a nivel internacional.*
f. *Ahora no es el momento de reducir la inversión en operadores de justicia especialistas en combatir el ciberdelito. La capacidad para combatir el ciberdelito constituye un componente esencial para proteger la infraestructura crítica nacional, mantener a los niños seguros en línea, empoderar a la industria, asegurar los hospitales y apoyar a la recuperación económica del COVID-19.*
g. *El personal especialista de UNODC en combatir el ciberdelito se encuentra disponible, alrededor del mundo, para apoyar a los Estados Miembros en el combate al ciberdelito, 24 horas del día, 7 días a la semana. Los recursos de diplomacia pública de UNODC están disponibles en: https://www.unodc.org/unodc/en/covid-19.html, estos incluyen vínculos a una sesión de Instagram Live con la Enviada del Secretario General sobre Juventud, a asesoría sobre protección en línea para el personal de las Naciones Unidas y a una evento de iSEEK Live sobre ciberseguridad para la Secretaria General de las Naciones Unidas.*

Diseminación: este reporte (UNODC/CMLS/COVID19/Cyber1) puede ser compartido sin referencia previa al autor.

FIN

[5] https://www.zdnet.com/article/dutch-police-take-down-15-ddos-services-in-a-week/