Konstantin Asmolov*

Los piratas informáticos norcoreanos son un tema ineludible de discusión teniendo en cuenta la reciente exageración sobre ellos una vez más. Por lo tanto, vale la pena investigar los errores de los que han sido acusados y hasta qué punto son culpables una vez más.

El 30 de mayo de 2019, la estación de radio Voice of America informó que, en opinión de las agencias de inteligencia de EE. UU., la RPDC, enfrentando dificultades económicas debido a sanciones impuestas, estaba participando en ataques cibernéticos contra bancos y otras instituciones financieras para obtener dinero. Erin Cho, directora del Centro Nacional de Integración de Ciberseguridad y Comunicaciones (una agencia del Departamento de Seguridad Nacional), señaló que los ciberataques norcoreanos apuntaban a las monedas virtuales, un medio relativamente nuevo para robar dinero.

La ex asesora principal del Departamento de Estado de los Estados Unidos, Balbina Hwang, también atrajo la atención con sus **declaraciones** en agosto de 2019. La profesora visitante en la Universidad de Georgetown habló sobre una historia de Associated Press que "citó un informe del Consejo de Seguridad de las Naciones Unidas" sobre el uso del ciberespacio por parte de Corea del Norte por lanzar "ataques cada vez más sofisticados para robar fondos de instituciones financieras e intercambios de criptomonedas para generar ingresos. El más afectado fue Corea del Sur, víctima de 10 ataques cibernéticos de Corea del Norte, seguido de India con tres ataques y Bangladesh y Chile con dos cada uno".

Resulta que "Bithumb de Corea del Sur, uno de los mayores intercambiadores de criptomonedas en el mundo, fue atacado al menos cuatro veces". Se produjeron dos ataques en febrero y julio de 2017, cada uno con pérdidas de aproximadamente $ 7 millones, "mientras que un ataque de junio de 2018 condujo a una pérdida de $ 31 millones y un ataque de marzo de 2019 a una pérdida de $ 20 millones".

El 13 de septiembre de 2019, el Departamento del Tesoro de los Estados Unidos impuso sanciones contra los grupos de piratería de la RPDC: el Grupo Lazarus y dos de sus subsidiarias, Bluenoroff y Andariel. Según el Departamento del Tesoro, en 2014, el Grupo Lazarus fue responsable del ataque cibernético contra Sony Pictures y también de infectar 300,000 computadoras con virus en 150 países de todo el mundo. Bluenoroff logró robar $ 1,1 mil millones de varias instituciones financieras, incluidos $ 80 millones del banco central de Bangladesh. Andariel es sospechoso de crímenes contra el gobierno y la infraestructura de Corea del Sur, y también de intentar robar **información militar** clasificada .

A finales de septiembre de 2019, los expertos de la compañía de ciberseguridad Kaspersky detectaron anteriormente el spyware Dtrack, diseñado por el Grupo Lazarus, en redes de organizaciones financieras indias y centros de investigación. Este malware puede proporcionar acceso a un dispositivo que ha infectado permitiendo que los datos se carguen o descarguen de él. El spyware es algo similar a DarkSeoul, vinculado a un ataque cibernético contra Corea del Sur en 2013.

En octubre de 2019, Patrick Wardle, el investigador principal de seguridad de Jamf (un proveedor de software para la plataforma Apple), dijo que los piratas informáticos, que se cree que están patrocinados por Corea del Norte, habían "encontrado una nueva forma de atacar Apple Macs". Lo hicieron mediante el uso de una aplicación falsa de comercio de criptomonedas. Para agregar legitimidad al software, el grupo incluso creó JMT Trading, una compañía líder "con un sitio web oficial".

En enero de 2020, la compañía rusa de ciberseguridad Kaspersky informó que el Grupo Lazarus había acumulado grandes cantidades de criptomonedas al usar Telegram, una popular aplicación de mensajería que usa su propio protocolo de seguridad patentado. De hecho, se pueden encontrar enlaces a grupos alojados por usuarios maliciosos de Telegram en muchos **sitios web** falsos . Además, el Grupo Lazarus continúa diseñando y lanzando numerosos sitios web fraudulentos (como por ejemplo, Union Crypto Trader) que parecen ser plataformas comerciales para criptomonedas o hosts ICO (Oferta inicial de monedas) pero, en realidad, se utilizan para robar información confidencial de los usuarios. El malware desarrollado por el grupo Lazarus también es "capaz de cargarse en la memoria de los dispositivos (RAM) exclusivamente, evitando los discos duros", lo que lo hace aún más **peligroso** .

.

El último incidente posiblemente relacionado con piratas informáticos de la RPDC ocurrió en enero de 2020 cuando 16 programadores informáticos de Corea del Norte "descubrieron que trabajaban ilegalmente en Camboya" y posteriormente se les ordenó abandonar el país . Sin embargo, pronto salió a la luz que no eran piratas informáticos sino personal temporal de TI que trabajaba para una "operación china de juego en la red".

El 17 de febrero de 2020, ESTsecurity (una empresa de ciberseguridad con sede en Seúl) informó que un grupo vinculado a Corea del Norte probablemente fue responsable de piratear el teléfono inteligente perteneciente a Thae Yong-ho, un ex diplomático de la RPDC que desertó a Corea del Sur en 2016. los hackers usaron "spear phishing" para acceder a su nuevo nombre, mensajes de texto, fotografías y otra información. Según los expertos en seguridad, sus patrones de ataque "fueron similares a los utilizados anteriormente por los grupos de piratería de Corea del Norte", como Geumseong121, que atacaron "los sitios web de los departamentos gubernamentales, las organizaciones relacionadas con Corea del Norte y los **medios de comunicación"**

.
". El nombre del grupo es bastante patriótico. También existe la posibilidad de que algún otro equipo de piratas informáticos "usó tales patrones de ataque para dar la impresión de ser un grupo norcoreano". Según Mun Chong-hyun de ESTsecurity, Geumseong 121 creía que, en opinión de los expertos surcoreanos, con el respaldo de las agencias de inteligencia de la RPDC, era capaz de piratear teléfonos móviles de ciudadanos de la República de Corea, como Thae Yong-ho, cuyo trabajo está relacionado con Corea del Norte y la política exterior. Mun Chong-hyun también señaló que los correos electrónicos y mensajes de phishing contenían, por ejemplo, "un archivo adjunto que, al hacer clic, dirigía al lector a un sitio web disfrazado como el sitio web de una organización de derechos humanos de Corea del Norte con sede en los EEUU, una vez que los usuarios fueron atraídos a dicho sitio web,

2 de marzo de 2020. El Departamento de Justicia de Estados Unidos acusó a dos ciudadanos chinos, Tian Yinyin y Li Jiadong, de lavado de dinero. Fueron acusados □□por robar más de $ 100 millones como resultado de dos ataques cibernéticos. Pero, según una investigación conjunta realizada por la inteligencia de EE. UU. y las agencias policiales de Corea del Sur, a partir de finales de 2017, los piratas informáticos norcoreanos han robado criptomonedas de los intercambios y luego han lavado aproximadamente $ 250 millones con la ayuda de ciudadanos chinos. Se cree que los fondos se utilizaron para financiar el programa de armas nucleares de Corea del Norte. No fue la primera vez que se hicieron tales acusaciones. En 2017, Estados Unidos alegó que la empresa china Mingzheng International Trading Ltd "facilitó" transacciones monetarias prohibidas en nombre de un banco norcoreano. Los fiscales "dijeron que buscarían **sanciones**
".

El 23 de marzo de 2020, la Policía de Chipre emitió una advertencia pública diciendo que habían recibido una serie de quejas sobre llamadas telefónicas que parecían venir de Corea del Norte, ya que los números comenzaron con 00850 (el código de país de la RPDC). Había motivos para creer que se trataba de una "estafa que llevaba a los destinatarios" a **cobrar de más**
.

Desafortunadamente, todos estos informes desconcertantes no proporcionan ninguna evidencia para respaldar sus afirmaciones. Y hace algún tiempo, el autor realizó su propia investigación sobre tales incidentes. Y simplemente nos gustaría recordar a nuestros lectores sobre los resultados.

- La afirmación de que los patrones de ataque fueron similares a los utilizados por otros grupos de Corea del Norte no está justificada. Después de todo, dado que hay pocas herramientas de piratería únicas, la mayoría de los hackers tienen un arsenal limitado a su disposición. Es una práctica común para ellos usar los patrones de ataque de los demás para no solo ahorrar tiempo, sino también desviar y echar la culpa a otra parte. Teniendo en cuenta el hecho de que la participación de Corea del Norte en los ataques anteriores no fue probada, la llamada evidencia podría llegar a ser una extrapolación. De este modo, se crea un círculo vicioso, a medida que se multiplica un reclamo "altamente probable" y, por alguna razón, esta incertidumbre no se refleja en las conclusiones extraídas, y la participación de la RPDC se considera un hecho "incontrovertible".
- El uso por los hackers de expresiones lingüísticas típicamente norcoreanas tampoco prueba la participación de la RPDC. Después de todo, cualquier grupo criminal puede optar por utilizar dicho lenguaje (por ejemplo, Chollima) para ocultar sus huellas y engañar a las agencias de la ley.
- Ocultar las direcciones IP o la suplantación de identificador de llamadas son herramientas comunes utilizadas por los estafadores. De hecho, una VPN (una red privada virtual) le permite cambiar su ubicación aparente.
- Las discusiones sobre la piratería de redes aparentemente seguras que no están conectadas a Internet (como, por ejemplo, los sistemas bancarios) generalmente hacen la pregunta "¿Pero cómo es eso posible?". Es necesario introducir un virus de alguna manera, y esto es posible cuando un dispositivo está conectado a Internet. Si una red no puede infectarse de esta manera, entonces probablemente esté involucrado un saboteador (no malware). Otra posibilidad es que el sistema en cuestión no estaba completamente seguro o aislado del mundo exterior debido a un alto nivel de incompetencia.
- Las acusaciones públicas en la línea de 'X podría haber estado involucrado en Y' son meras especulaciones si no están respaldadas por evidencia. Las declaraciones, como "grupos con vínculos con Pyongyang", también se incluyen en la misma categoría, ya que es importante demostrar esa relación. Después de todo, simplemente decir 'los piratas informáticos atacan a los enemigos de la RPDC' no es evidencia. Además, el Grupo Lazarus,

Bluenoroff y Andariel son nombres muy inusuales para los grupos de hackers, en comparación con Geumseong121, teniendo en cuenta lo aislada que está Corea del Norte como nación.

- De hecho, hay debates en curso sobre de dónde es el Grupo Lazarus entre los expertos. Es especialmente agradable escuchar la palabra "Chollima" en referencia a sus subgrupos. Chollima es un mítico caballo alado capaz de viajar 400 km por día. Durante mucho tiempo, el animal simboliza la velocidad del desarrollo económico de Corea del Norte, que, durante al menos dos años, se ha multiplicado por 10. Por lo tanto, hoy en día, es costumbre referirse a tal progreso con la expresión "Mallima".

Curiosamente, no solo el cibercrimen está en aumento en la propia Corea del Norte, donde hay más de 600,000 usuarios de teléfonos móviles, las estafas telefónicas también se están **exten diendo** allí. Según los desertores de la RPDC, los delincuentes a menudo "fingen ser agentes de la ley o supervisores financieros" que amenazan con arrestar a las personas a las que apuntan si no pagan. "Tales estafas clásicas todavía funcionan porque las víctimas no se atreven a cuestionar la identidad de los **supuestos** funcionarios del gobierno".

Con toda probabilidad, los piratas informáticos de Corea del Norte son responsables de las llamadas "campañas de phishing diseñadas para obtener contraseñas y otra información personal" una vez que una víctima abre un enlace o un archivo adjunto enviado en un mensaje. En septiembre de 2019, dicha correspondencia con el malware se envió a "personas que trabajan en el **campo** de Corea del Norte ". Estos tipos de ataques, que usan direcciones de correo electrónico que parecen pertenecer a "personas que trabajan en asuntos de Corea del Norte", comenzaron en 2010.

Según un informe de Palo Alto Networks, Inc. (una empresa de seguridad cibernética) emitido en enero de 2020, "un grupo de piratas informáticos sospechosos de estar vinculados a Corea del Norte" había atacado a "una agencia del gobierno de EE. UU. con un tipo de malware ". Ellos "enviaron correos electrónicos con seis documentos diferentes de Microsoft Word en ruso que contenían macros maliciosas con el objetivo de dar a los atacantes el control sobre las **co mputadoras** de los destinatarios ".

Las últimas "campañas de correo electrónico malicioso" **ocurrieron** a fines de febrero de

2020.

En resumen, una situación interesante aparentemente está tomando forma. Las sanciones impuestas contra la RPDC están obligando a la nación a buscar nuevas formas de generar ingresos. Y dado que el uso de tecnologías digitales no está prohibido por ellos y también es difícil de monitorear, Corea del Norte aparentemente ha comenzado a confiar en este sector. Cualquier trabajo realizado por especialistas de TI de la RPDC y el software desarrollado por ellos no están cubiertos por sanciones. Y Pyongyang ha comenzado a aprovechar esto, por ejemplo, utilizando aplicaciones de transferencia de dinero (diseñadas de manera similar a los análogos chinos) que permiten a los usuarios eludir los procedimientos bancarios estándar para enviar y recibir dinero.

Claramente, hay un impulso para cerrar tales herramientas y reforzar el bloqueo digital, por lo tanto, los informes sobre piratas informáticos. Pero para cada acción, hay una reacción igual y opuesta, y es posible que, al igual que en las profecías autocumplidas, los mitos sobre los hackers norcoreanos se conviertan en realidad.

**PhD en Historia, Investigador principal del Centro de Estudios Coreanos del Instituto de Estudios del Lejano Oriente de la Academia de Ciencias de Rusia*