EL USO DEL
CIBERTERRORISMO
EN LA GUERRA HAMAS - ISRAEL

INTRODUCCIÓN

El 7 de octubre 2023, durante las festividades judías de Shabat y Simjá Torah, Hamás sacudió al mundo al invadir Israel desde Gaza ingresando a través de diferentes puntos. Los resultados fueron devastadores: la mayor cantidad de judíos asesinados en un solo día desde el Holocausto Nazi. Hamás atacó a familias civiles, tomó por asalto y secuestró a cientos de otros civiles que fueron llevados como rehenes a Gaza. La evidencia sugiere que el Hamás se estaba preparando otra “segunda fase” de ataques dirigidos contra los habitantes de Israel. En respuesta a esta masacre sin precedentes y al secuestro de otros, las fuerzas israelíes invadieron Gaza con el objetivo establecido de destruir a Hamás.

En la esfera de Internet, los atroces ataques dispararon una ola de publicaciones, imágenes, memes, ataques ciberterroristas y videos en los medios sociales, así como también en la denominada red oscura y sitios adyacentes. El Proyecto de Odio y Terrorismo Digital del Centro Simon Wiesenthal (CSW) , monitorea las actividades de más de 7.000 grupos, individuos y canales online, muchos de los cuales apoyan a Hamás y otros grupos terroristas. Este informe explorará la explosión de la actividad ciberterrorista contra objetivos judíos e israelíes a raíz del ataque del 7 de octubre y expondrá a algunos de los actores y grupos clave que han caudsao perturbaciones y amenazas significativas a la seguridad personal.

¿ QUÉ ES EL CIBER-TERRORISMO?

Ciber ataques contra Israel apuntan primariamente a sistemas críticos para la infraestructura, teléfonos y contactos de emergencia, sistemas de alerta Homefront Command y sectores de energía, servicios de telecomunicaciones y transporte. Actores de Nación- Estado como Irán, Rusia, China, Corea del Norte y muchos otros que apoyan a terroristas palestinos son perpetradores significantes. Utilizan tácticas como phishing, negación del servicio, filtrado de datos, ataques de fuerza bruta y explotan las conocidas vulnerabilidades del sistema IT.

Los ciberataques contra Israel se dirigen principalmente a infraestructuras críticas, sistemas telefónicos y de contacto de emergencia, sistemas de alerta del Homefront Command, energía, servicios públicos, telecomunicaciones y sectores de transporte. Los actores estado-nación, particularmente de Irán, Corea del Norte, Rusia, China y otros que apoyan a los terroristas palestinos, son perpetradores importantes. Utilizan tácticas como phishing, denegación de servicio, fugas de datos, ataques de fuerza bruta y explotan las vulnerabilidades conocidas del sistema de TI (Tecnología Informática).

Además, tras la masacre del 7 de octubre en Israel, ha habido un aumento de los ataques ciberterroristas y de ciberamenazas contra sitios judíos. El Sistema de Monitoreo Cibernético del Antisemitismo, operado por el Ministerio de Asuntos de la Diáspora israelí, informó que los llamados en línea a la violencia contra Israel, los sionistas y los judíos después de la operación Espadas de Hierro de las FDI han aumentado en un 1200%. En noviembre 2023 la Tecnología Check Point Software informó , " vimos un incremento aproximadamente del 20 % en ciber ataques en Israel durante la guerra, incluido más del 50 % cuando se trata de ataques a sectores del gobierno, hasta ahora no vimos un incremento semejante en ningún otro lugar a nivel global."

Fig. 1: The Returnees (Los Retornados) -Telegram

Trabajamos, gracias a Dios, con total calma y constancia, y
encontramos en Dios nuestra fuerza, y a través de Su voluntad y capacidad, la victoria será la aliada de la resistencia.
Levantamos la cabeza con confianza, confirmando que el enemigo ha fracasado completamente a la hora de afrontar los ataques de la unidad cibernética.

Los grupos ciberterroristas se han sumado a la lucha y lanzaron sus propios ataques contra sitios web israelíes. En particular, se han identificado actores específicos de amenazas cibernéticas, entre ellos: un actor con sede en Gaza conocido como Storm-1133 que ha atacado a los sectores israelíes de energía, defensa y telecomunicaciones; un grupo vinculado a Irán, Imperial Kitten, que apunta al sector tecnológico de Medio Oriente, incluido Israel; y The Returnees, un colectivo de hackers que apuntó tanto a la infraestructura como a ciudadanos individuales israelíes. El frente cibernético de la guerra ha tenido un

impacto aún más amplio con países como Estados Unidos e India que también han sido atacados por su apoyo a Israel.

Figura 2: AnonGhost (8 de Octubre) - Telegram

Ciber amenazas, ciber ataques y ciber terrorismo contra Israel no son un fenómeno nuevo. Sin embargo. el CSW monitoreó un pico significativo en la actividad de los actores de ciber amenazas, tanto antes como después del 7 de octubre 2023.

El CSW identificó al menos 40 entidades de ciber terrorismo que participaron y colaboraron en ciber ataques dirigidos contra Israel. Estos grupos y sus colaboradores se adjudicaron la responsabilidad por ataques a numerosos dominios de Internet israelíes. Algunos de estos grupos proveyeron con regularidad detalles de los ataques que llevaron a cabo así como de la información que obtuvieron. También compartieron imágenes gráficas y videos del conflicto y junto a la justificación por sus creencias y acciones.

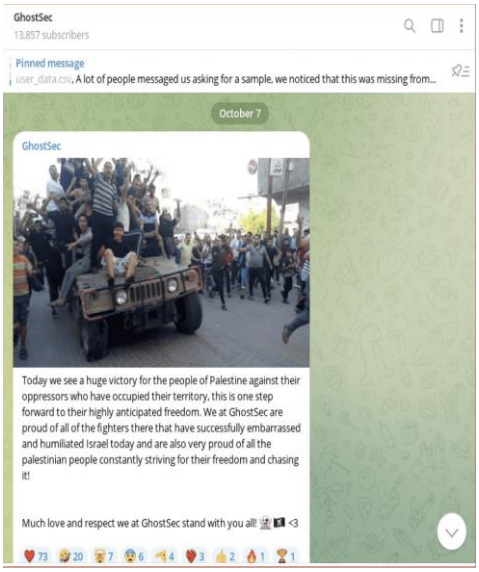

Figura 3: Actor de amenazas cibernéticas Ghostsec - Telegram

Cabe señalar que el impacto de los ataques ciberterroristas en la sociedad israelí a lo largo de esta guerra ha sido profundo y ha causado estrés, ansiedad, inseguridad y daños financieros. Los ataques ciberterroristas en Israel han provocado interrupciones en el servicio, daños físicos e incluso riesgo de muerte o lesiones corporales, como resultado de interrupciones en el sistema telefónico de emergencia. El impacto psicológico de las amenazas cibernéticas puede rivalizar con el del terrorismo tradicional al infundir miedo en las poblaciones civiles.

A continuación se analizan algunos de los actores más prolíficos del ciberterrorismo:

ANONYMOUS SUDAN

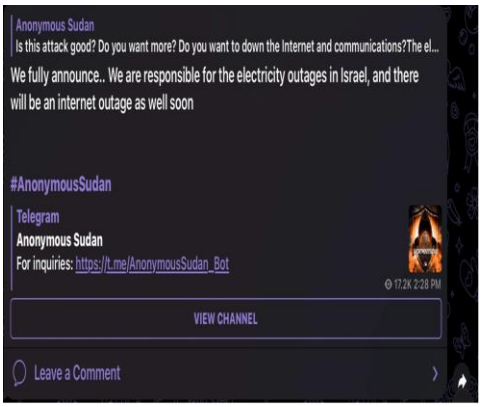

Figura 4: Anonymus Sudan (Abril 1993) - Telegram

Anonymous Sudan es un grupo de hackers de base pro-palestina y pro-rusa con supuestos orígenes en Sudan. Desde principios de 2023, participaron en una variedad de acciones disruptivas, incluidos ataques distribuídos de denegación de servicio (DDoS) contra objetivos en Israel, Suecia, Dinamarca, Estados Unidos, Australia y otros países donde ellos creen que existe actividad anti -musulmana y anti -palestina.
Los ataques DDoS inundan el servidor atacado con tráfico, eliminando así efectivamente su capacidad de operar. Anonymous Sudan es una entidad multilingüe y multiplataforma. En abril y mayo de 2023, Anonymous Sudan lanzó ataques contra el sistema de defensa israelí conocido como Cúpula de Hierro. El 7 de octubre de 2023 el grupo hacktivista pro-palestino Team Bangladesh, anunció su apoyo a Hamás y su alineamiento con Anonymous Sudan, utilizando hashtags pro-palestinos incluídos #FreePalestine y #OpIsraelV2.

Figura 5: De Anonymous Sudan (Rusia) – Telegram

Ahora estamos atacando las sirenas en Israel, incluyendo la Cúpula de Hierro. "Buena Suerte Gaza"

Figura 6: De Anonymous Sudan (Rusia) – Telegram

KILLNET

Figura 7: Killnet – Telegram

Gobierno israelí, usted es el culpable de este derramamiento de sangre. En 2022 usted apoyó al régimen terrorista de Ucrania. Traicionaste a Rusia. ¡Hoy Killant os informa oficialmente al respecto! ¡Todos los sistemas del gobierno israelí estarán sujetos a nuestros ataques! SOMOS KILLNET.

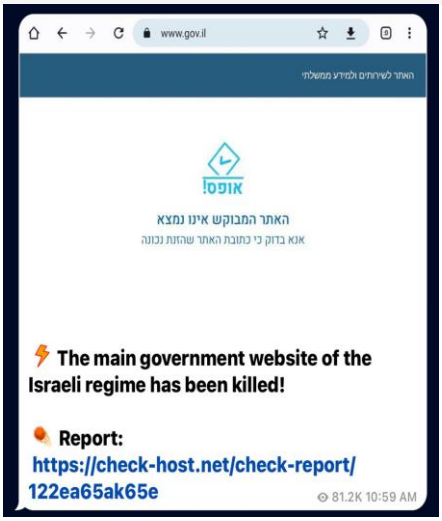

Figura 8: Killnet October 8 – Telegram

El sitio web del Gobierno Israelí está muerto.

Figura 9: Anonymous Sudan – Telegram

Anonymous Sudan y KILLNET están en contra de Israel y de cualquiera que apoye a la Entidad Sionista. Gloria a la resistencia Palestina.

Killnet se unió recientemente a Anonymous Sudan en sus ataques a Israel. Killnet es una entidad multilingüe y multiplataforma. El brazo palestino de Killnet se estableció el 13 de octubre de 2023. Entidades de hackers y ciberterroristas a menudo están influenciadas y motivadas políticamente, y con frecuencia se alinean con ciberhacktivistas patrocinados por el estado. Killnet, vía publicaciones multilingües (inglés, árabe, ruso y hebreo), anunció nuevas intenciones de atacar al gobierno israelí, y Anonymous Sudan emitió amenazas similares. (Ver figuras 8 y 9).

Las entidades de hackers y ciberterroristas suelen estar motivadas e influenciadas políticamente, y con frecuencia se alinean con ciberhacktivistas patrocinados por el Estado. Killnet, a través de publicaciones multilingües (inglés/ruso/árabe/hebreo), anunció nuevas intenciones de atacar al gobierno israelí, y Anonymous Sudan emitió amenazas similares (ver figuras 8 y 9).

Anonymous Sudan y Killnet están en contra de Israel y de cualquiera que apoye la entidad sionista.

GHOSTSEC

Ghostsec es un actor de ciberamenazas y un grupo hacktivista que surgió como una rama del infame grupo de hackers Anonymous. Inicialmente, el grupo se enfocó en esfuerzos de contraterrorismo y en monitorear actividades en línea asociadas con el terrorismo. Obtuvieron prominencia tras el tiroteo de Charlie Hebdo en París en 2015 y el ascenso de ISIS. Anteriormente se dedicaban a frustrar, rastrear e interrumpir la propaganda en línea relacionada con ISIS, y colaboraron con agencias policiales y de inteligencia. Ghostsec ahora ha girado sus actividades hacia ataques contra Israel. Se han alineado con los intereses de Hamás. Sus actividades han impactado principalmente en organizaciones que ellos perciben como anti-Hamás. La campaña se ha dirigido hacia los sectores de energía y defensa israelíes, así como a entidades afiliadas a Fatah, un partido político palestino con sede en Cisjordania que es rival de Hamás.
Uptycs.com, es una compañía de ciber seguridad, que enumera estas actividades recientes atribuidas a Ghostsec:

• En mayo de 2022, el sitio web de HRVAC en Israel fue pirateado, lo que provocó la divulgación de datos personales y de credenciales.

• En junio de 2022, el grupo de hackers atacó con éxito las industrias de telecomunicaciones y electricidad.

• En julio de 2022, los ataques se centraron en las industrias de energía y sistemas de alcantarillado.

• En agosto de 2022, datos militares y datos API del sistema ferroviario quedaron expuestos en una filtración de datos.

• En septiembre de 2022, los dispositivos PLC se convirtieron en el objetivo de los ataques.

• En abril de 2023, los ataques se centraron en la industria de bombas de agua.

• En mayo de 2023, el acceso no autorizado a dispositivos PLC provocó una fuga de datos.

• En octubre de 2023, se produjo un ataque a bombas de agua junto con la implementación del ransomware (secuestro de datos) GhostLocker.

• Durante noviembre de 2023, este grupo lanzó continuamente ciberataques contra Israel en respuesta a presuntos crímenes de guerra.

Figura 10: Ghostsec – Telegram

CYB3R DRAGONZ

Poco se sabe sobre la procedencia del actor de la ciber amenaza de Cyb3r Dragonz. A principios de octubre publicaron una encuesta en su canal de Telegram preguntando a los usuarios a qué país debían apoyar. El 83 % de los 392 respondientes votaron por "Palastina [sic]" , y el 17 % votó por Israel.

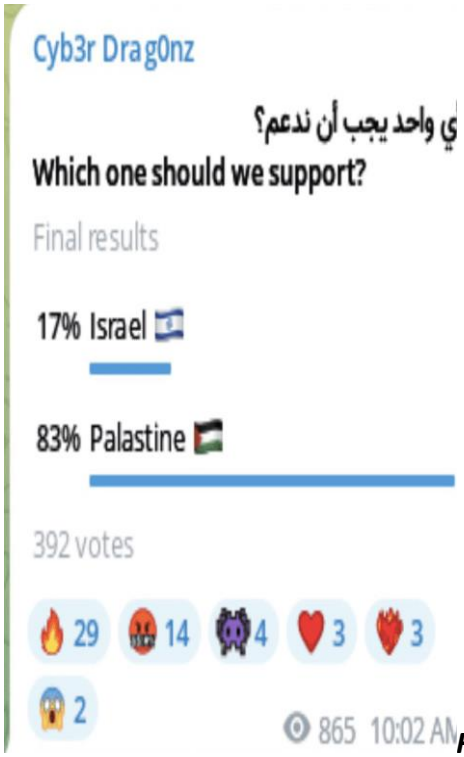

Figura 11: Cyb3r DragOnz – Telegram

Figura 12: Cyb3r DragOnz – Telegram

Figura 13: Cyb3r DragOnz – Telegram

Figura 14: Cyb3r DragOnz – Telegram

Grupos de ciber terroristas pro-palestinos también apuntaron sus ataques hacia ciudadanos y simpatizantes israelíes. Filtraron información personal y alentaron a partidarios y simpatizantes a apuntar a cuentas de redes sociales para acosar a los usuarios con mensajes pro palestinos.

ESFUERZOS PRO ISRAELÍES

La multiplataforma Garuna Ops se alineó con Israel y en el proceso cometió numerosos ataques contra intereses de Yemen, Bangladesh y algunos palestinos. Han declarado públicamente que realizarían ataques a cualquier gobierno o país que exhibiese apoyo a Hamás o Palestina.

Figura 15: Garuna Ops (Octubre 7, 2023) – X (ex Twitter)

WE RED EVILS

We Red Evil es un incipiente grupo de hackers israelí multiplataforma que emergió en octubre 2023. El grupo se hizo conocido por sus ataques dirigidos a países y sitios pro-Hamás y pro-palestinos. Han violentado exitosamente los sistemas de aquellos afiliados al Cuerpo de la Guardia Revolucionaria Iraní, e impactaron en la red de electricidad y la infraestructura en Irán.

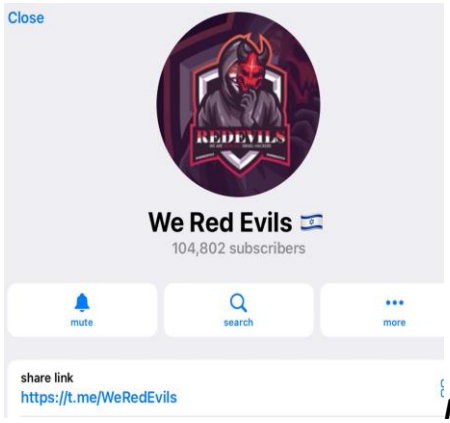

Figura 16: We Red Evils - Telegram

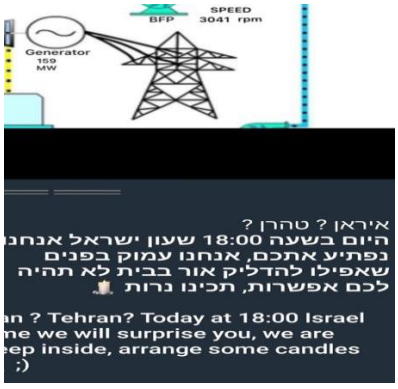

Figura 17: We Red Evils - X (ex Twitter)

CONCLUSIÓN

El ciberterrorismo está desempeñando un papel importante en la guerra entre Israel y Hamás, donde Hamás y sus partidarios explotan las vulnerabilidades de los sistemas de defensa israelíes, que dependen de la tecnología. Al planificar la masacre del 7 de octubre, Hamás investigó zonas con una cobertura mínima de cámaras y luego utilizó drones para lanzar granadas, perturbando así el aparato de vigilancia de Israel y aumentando la naturaleza letal de sus ataques.

Los ataques de piratas informáticos y ciberterroristas por parte de grupos y actores de estados-nación a través de ataques proxy (inspirados por Irán y otros), contra infraestructura crítica israelí como los medios de comunicación, la energía, los servicios públicos, las telecomunicaciones y el transporte, han crecido exponencialmente. Si bien las tácticas de ciberterror observadas no se consideran altamente sofisticadas, han sido disruptivas y es probable que se comparta información más confidencial en canales cerrados. A pesar de su falta de sofisticación, estos ataques son altamente eficaces para sembrar el miedo. El impacto del ciberterrorismo en la sociedad israelí es multifacético y afecta tanto el bienestar psicológico de las personas como la confianza del público en las instituciones encargadas de mantenerlos seguros. Los efectos psicológicos de las ciberamenazas pueden ser muy graves e inducir estrés, ansiedad e inseguridad.

Las amenazas del ciberterrorismo también son importantes para economías altamente digitalizadas como Israel. El aumento de los ciberataques posterior al 7 de octubre también ha provocado un aumento de las operaciones cibernéticas y las amenazas contra comunidades e instituciones judías, musulmanas y árabe-estadounidenses. Los componentes de ciberterrorismo y ciberguerra de esta guerra han añadido una nueva dimensión a este conflicto, lo que demuestra la creciente importancia de la ciberseguridad en la guerra moderna. Mitigar o eliminar el ciberterrorismo tanto en esta guerra como en la más amplia situación global del siglo XXI, requerirá un abordaje internacional del tipo “todos manos a la obra”, utilizando los recursos y activos tecnológicos de los países tomados como objetivo y de sus aliados.

El CSW continúa monitoreando e informando sobre las actividades de los ciberterroristas y las amenazas que representan para Israel y las comunidades e instituciones judías.

FUENTES UTILIZADAS

- https://www.washingtonpost.com/national-security/2023/11/12/hamas-planning-terror-gaza-israel/
- https://cybernews.com/cyber-war/israel-redalert-breached-anonghost-hamas/
- https://www.washingtonpost.com/politics/2023/10/11/largest-cyberattack-its-kind-recently-happened-heres-how/
- https://www.jpost.com/diaspora/antisemitism/article-768393
- https://www.csoonline.com/article/1249135/cyberattacks-on-israel-intensify-as-the-war-against-hamas-rages-check-point.html
- https://www.wired.com/story/israel-hamas-war-hacktivism/
- https://techcrunch.com/2023/10/09/hacktivism-erupts-in-response-to-hamas-israel-war/
- https://thehackernews.com/2023/10/gaza-linked-cyber-threat-actor-targets.html
- https://thehackernews.com/2023/11/iran-linked-imperial-kitten-cyber-group.html
- Gross, M. L., Canetti, D., & Vashdi, D. R. (2016). The psychological effects of cyber terrorism. *The Bulletin of the atomic scientists*, 72(5), 284–291. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5370589/
- https://www.uptycs.com/blog/ghostlocker-ransomware-ghostsec
- https://www.washingtonpost.com/world/2023/10/17/israel-hamas-war-reason-explained-gaza/
- https://www.politico.com/news/2023/10/10/israel-hamas-technology-failure-00120667
- https://www.politico.com/news/2023/10/15/hackers-israel-hamas-war-00121593
- https://www.politico.com/news/2023/10/10/israel-hamas-technology-failure-00120667
- https://cloudsecurityalliance.org/blog/2022/09/26/the-ongoing-cyber-threat-to-critical-infrastructure/
- https://www.securityweek.com/cyberterrorist-attacks-unsophisticated-effective-former-fbi-agent/
- https://academic.oup.com/cybersecurity/article/3/1/49/2999135
- Ibid.
- https://homeland.house.gov/wp-content/uploads/2023/11/2023-11-15-HRG-Testimony.pdf
- https://www.politico.com/news/2023/10/15/hackers-israel-hamas-war-00121593