Swascan
TINEXTA GROUP

APT NEL CONFLITTO HAMAS-ISRAELE

www.swascan.com
info@swascan.com

Sommario

CONTESTO

Nella quinta dimensione, il cyberspazio dove si combatte – o, perlomeno, dove fino a poco tempo fa si è combattuto – una parte considerevole del conflitto tra Hamas e Israele, tutto tace da giorni. Da quando i negoziatori delle due parti hanno cominciato a incontrarsi a Doha, le offensive cyber contro Israele – e alcuni Paesi occidentali che si erano schierati a fianco di Tel Aviv – che hanno caratterizzato la prima fase delle operazioni, accompagnando il blitz terroristico del 7 ottobre, sembrano essere improvvisamente cessate. Le attività dei 150 gruppi cyber pro-Hamas censiti da Swascan – parte del polo italiano per la cybersicurezza di Tinexta Group – nei primi dieci giorni di guerra, residenti in Marocco, Algeria, Sudan, Yemen e in Iran, sono nettamente affievolite, se non scomparse in alcuni casi.

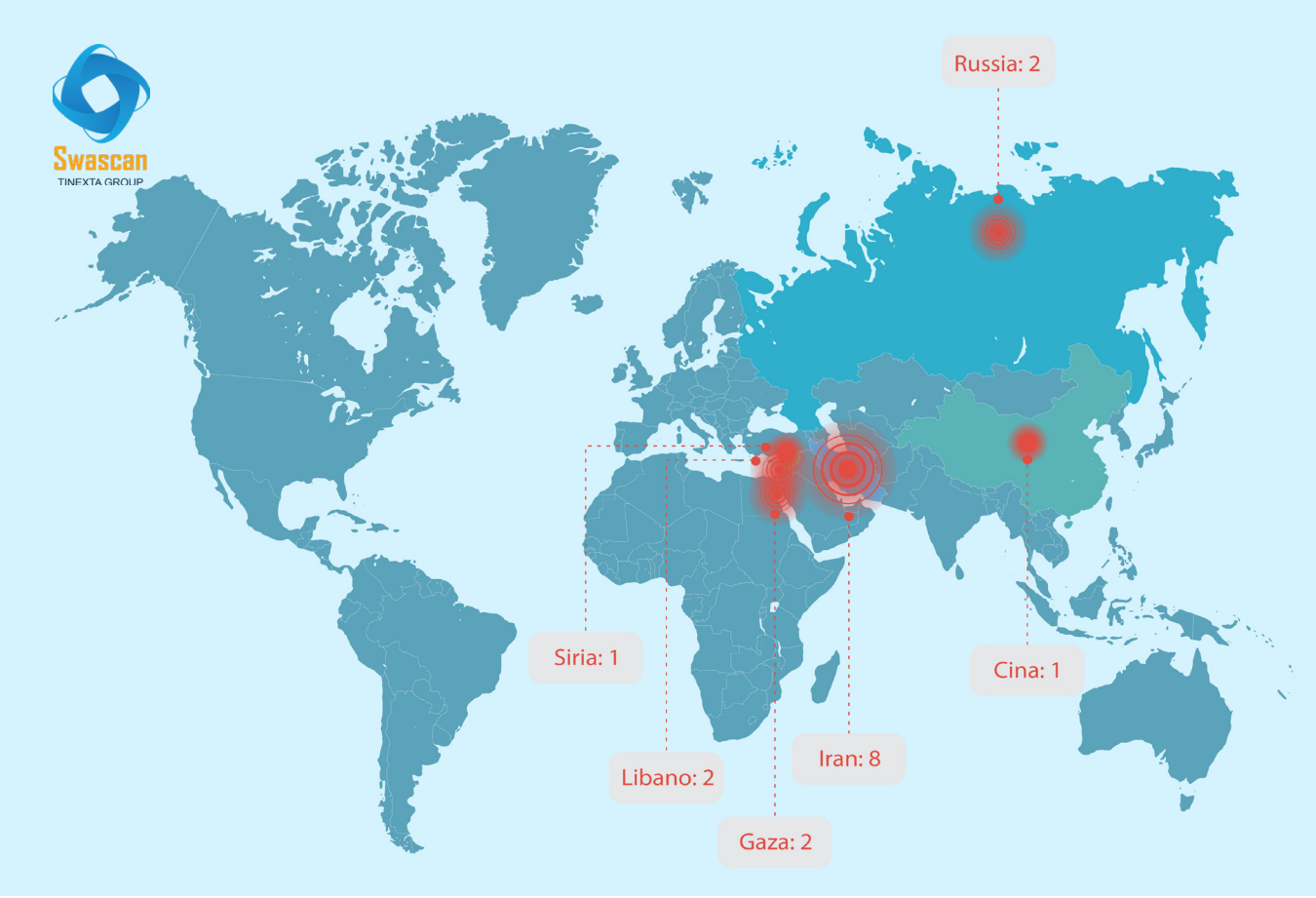
Da un lato una guerra partecipata, spesso realtà di cani sciolti dediti al proselitismo antisraeliano in rete e alla diffusione di fake news, dall'altro una guerra ibrida con riferimento a collettivi dotati di una organizzazione, di una strutturata matrice ideologica con competenze tecnologiche e informatiche basilari per effettuare attacchi di DDoS e web defacement, ma potenziate da "suggerimenti" e "indicazioni" da parte di utenti, probabilmente cybersoldier, che hanno pubblicato target da colpire con tanto di vulnerabilità da sfruttare e codici da usare.

Dagli attacchi alle app israeliane di allerta, ammutolite in coincidenza con i lanci dei primi razzi da parte di Hamas all'alba del 7 ottobre, all'oscuramento delle pagine online del quotidiano Jerusalem Post e della Israel Electric Corporation, via via fino agli assalti informatici ai siti del governo israeliano e del Mossad, tutto sembra dissolto come neve al sole. Se i cani sciolti possono aver continuato a operare in una attività di proselitismo nei diversi canali social, gli attacchi informatici veri e propri sono di fatto cessati o più probabilmente non hanno avuto successo grazie alla supremazia digitale israeliana, che ha ripreso il sopravvento dopo la sorpresa iniziale e soprattutto spiazzata da uno scontro di guerra asimmetrica digitale. L'inabissamento dei gruppi più strutturati, quali Anonymous Sudan, gli iraniani di Cyber Av3ngers e gli hacktivisti islamici antisemiti di AnonGhost, sembra avere un curioso parallelo con il disimpegno sul campo di battaglia reale dei gruppi sostenuti dall'Iran, in primis Hezbollah.

Il regime degli ayatollah ha esplicitamente tolto in questa guerra il sostegno ad Hamas, reo a suo dire di non aver avvertito Teheran del blitz del 7 ottobre, da parte delle compagini presenti sul terreno del conflitto. Inoltre, così come hanno accompagnato gli esordi del conflitto, le ostilità informatiche sembrano essere cessate proprio nel momento della trattativa per il rilascio degli ostaggi e del vero

e proprio cessate il fuoco. A conferma di quanto tali realtà, per quanto mascherate e dissimulate nel mondo del dark e deep web, agiscano in stretta sintonia con le direttive dei governi di riferimento. E, in particolare, dell'Iran. Non dobbiamo però dimenticare che i vari gruppi ATP cyber, gruppi di hacker non esplicitamente sponsorizzati da alcuni Stati, come sempre sono all'opera attraverso discrete azioni di cyber-espionage o per garantirsi la "persistenza" nelle realtà informatiche di asset strategici, non solo potenzialmente israeliani ma anche e soprattutto nei Paesi occidentali.

Distribuzione Geografica gruppi APT



Settori più colpiti da gruppi APT

COSA SONO I GRUPPI APT

Secondo il NIST, un APT è un gruppo di threat actor che possiede livelli sofisticati di competenza e risorse significative che gli consentono di creare opportunità per raggiungere i propri obiettivi utilizzando molteplici vettori di attacco. Questi obiettivi includono tipicamente la creazione e l'estensione di punti d'appoggio all'interno dell'infrastruttura informatica delle organizzazioni prese di mira allo scopo di esfiltrare informazioni, minare o impedire aspetti critici di una missione, di un programma o di un'organizzazione, oppure posizionarsi per realizzare questi obiettivi in futuro. I gruppi APT: perseguono i loro obiettivi ripetutamente per un lungo periodo di tempo; si adattano agli sforzi dei difensori per resistere; sono determinatati a mantenere il livello di interazione necessario per realizzare i loro obiettivi.

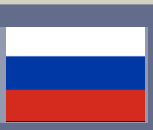
A cosa si riferisce il codice alfanumerico?

Le organizzazioni che conducono ricerche sulle APT assegnano nomi/numeri alle APT al momento della scoperta. Poiché più di un'organizzazione è impegnata nella ricerca sulle minacce costanti evolutive, possono esserci sovrapposizioni tra le minacce costanti evolutive e possono esserci più nomi per una singola minaccia costitutiva. Per esempi di elenchi di APT, vedere MITRE ATT&CK's® Groups

SCHEDE RIASSUNTIVE APT

COZY BEAR

Russia



Attiva dal: **2008**

Conosciuto come:

APT 29 (Mandiant), Cozy Bear (CrowdStrike), The Dukes (F-Secure), Group 100 (Talos), Yttrium (Microsoft), Iron Hemlock (SecureWorks), Minidionis (Palo Alto), CloudLook (Kaspersky), ATK 7 (Thales), ITG11 (IBM), Grizzly Steppe (US Government) together with Sofacy, APT 28, Fancy Bear, Sednit, UNC2452 (FireEye), Dark Halo (Volexity), SolarStorm (Palo Alto), StellarParticle (CrowdStrike), SilverFish (Prodaft), Nobelium (Microsoft), Iron Ritual (SecureWorks), Cloaked Ursa (Palo Alto), BlueBravo (Recorded Future), Midnight Blizzard (Microsoft)

Paesi vittime:

Australia, Azerbaigian, Bielorussia, Belgio, Brasile, Bulgaria, Canada, Cecenia, Cile, Cina, Cipro, Danimarca, Francia, Georgia, Germania, India, Irlanda, Israele, Italia, Giappone, Kazakistan, Kirghizistan, Lettonia, Libano, Lituania, Lussemburgo, Messico, Montenegro, Paesi Bassi, Nuova Zelanda, Polonia, Portogallo, Romania, Russia, Singapore, Slovacchia, Slovenia, Spagna, Corea del Sud, Svizzera, Tailandia, Turchia, Uganda, Emirati Arabi Uniti, Regno Unito, Ucraina, USA, Uzbekistan, NATO.

Settori Osservati:

Aerospaziale, Difesa, Istruzione, Energia, Finanza, Governo, Sanità, Forze dell'Ordine, Media, Organizzazioni Non Governative (ONG), Farmaceutico, Telecomunicazioni, Trasporti, Think Tank e Settore delle Immagini.

Particolarità:

ampia gamma di strumenti malware personalizzati, tra cui MiniDuke, CosmicDuke, OnionDuke, CozyDuke, CloudDuke, SeaDuke, HammerDuke, PinchDuke e GeminiDuke e campagne di spear-phishing su larga scala.

WIZARD SPIDER

Russia 

Attiva dal: **2014**

Conosciuto come:

Wizard Spider (CrowdStrike), Grim Spider (CrowdStrike), TEMP.MixMaster (FireEye), Gold Blackburn (SecureWorks), Gold Ulrick (SecureWorks), ITG23 (IBM), DEV-0193 (Microsoft), Periwinkle Tempest (Microsoft)

Paesi vittime:

Worldwide.

Settori Osservati:

Difesa, finanza, governo, sanità, telecomunicazioni.

Particolarità:

originariamente orientato verso frodi finanziarie nel 2016, ha successivamente ampliato il proprio raggio d'azione, diventando un'entità altamente avanzata con un vasto e potente arsenale, gestendo diverse famiglie di ransomware con modalità operative differenziate.

AL QASSAM

Iran 

Attiva dal: **2012**

Conosciuto come:

Cyber fighters of Izz Ad-Din Al Qassam (self given), Qassam Cyber Fighters (self given), QCF (self given) Fraternal Jackal (CrowdStrike)

Paesi vittime:

USA

Settori Osservati:

Finanziario

Particolarità:

DESERT FALCON

Gaza– Sponsor Hamas 

Attiva dal: **2011**

Conosciuto come:

Desert Falcons (Kaspersky), APT-C-23 (Qihoo 360), Two-tailed Scorpion (Qihoo 360), Arid Viper (Palo Alto), ATK 66 (Thales), TAG-CT1 (Recorded Future) Mantis (Symantec)

Paesi vittime:

Europa: Albania, Belgio, Bosnia ed Erzegovina, Danimarca, Francia, Germania, Grecia, Italia, Paesi Bassi, Norvegia, Portogallo, Romania, Russia, Svezia, Ucraina.

Medio Oriente e Africa del Nord: Algeria, Egitto, Iran, Iraq, Israele, Giordania, Kuwait, Libano, Libia, Mali, Mauritania, Marocco, Palestina, Qatar, Arabia Saudita, Sudan, Siria, Turchia, Emirati Arabi Uniti, Yemen.

Asia: Cina, India, Giappone, Pakistan, Taiwan.

Nord America: Canada, Stati Uniti.

Sud America: Messico.

Africa: Zimbabwe.

Settori Osservati:

Infrastrutture critiche, Difesa, Istruzione, Governo, Media, Trasporti.

Particolarità:

il gruppo prende di mira individui di alto profilo palestinesi e israeliani. Utilizza spesso attacchi di phishing e social engineering per infettare i bersagli, e social media come Facebook e Instagram per instaurare rapporti con le vittime. Le vittime delle loro operazioni suggeriscono dunque che il target demografico è costituito da individui associati a gruppi pro-Fatah, organizzazioni governative palestinesi, personale militare e di sicurezza e gruppi di studenti in Palestina.

POLONIUM

Libano 

Attiva dal: **2022**

Conosciuto come:

Polonium (Microsft)
Plaid Rain (Microsoft)

Paesi vittime:

Israele, Libano.

Settori Osservati:

Ingegneria, Difesa, IT, Produzione, Media, Telecomunicazioni.

Particolarità:

Esiste una probabile collaborazione con i servizi di intelligence iraniani, in particolare con il Ministero dell'Intelligence e della Sicurezza dell'Iran (MOIS), come suggerito dalla sovrapposizione delle vittime e dalla similitudine di strumenti e tecniche.

VOLATILE CEDAR

Libano 

Attiva dal: **2012**

Conosciuto come:

Volatile Cedar (Check Point)
Dancing Salome (Kaspersky)
DeftTorero (Kaspersky)

Paesi vittime:

Canada, Egitto, Israele, Giordania, Libano, Russia, Arabia Saudita, Emirati Arabi Uniti, Regno Unito, Stati Uniti e Autorità Palestinese.

Settori Osservati:

Istruzione, Governativo e Hosting.

Particolarità:

I metodi di accesso iniziale osservati con maggiore frequenza si concentrano sulla compromissione dei server web delle vittime attraverso vulnerabilità zero-day per l'installazione di webshells, tra cui ASPXSpy, devilzshell e Caterpillar.

MOLERATS

Gaza– Sponsor Hamas

Attiva dal: **2012**

Conosciuto come:

Molerats (FireEye), Extreme Jackal (CrowdStrike), Gaza Cybergang (Kaspersky), Gaza Hackers Team (Kaspersky), TA402 (Proofpoint), Aluminum Saratoga (SecureWorks), ATK 89 (Thales), TAG-CT5 (Recorded Future)

Paesi vittime:

Afghanistan, Algeria, Canada, Cina, Cile, Danimarca, Egitto, Germania, India, Iran, Iraq, Israele, Giordania, Kuwait, Libano, Lettonia, Libia, Macedonia, Marocco, Nuova Zelanda, Oman, Palestina, Qatar, Russia, Arabia Saudita, Serbia, Slovenia, Somalia, Corea del Sud, Siria, Turchia, Emirati Arabi Uniti, Regno Unito, Stati Uniti, Yemen.

Settori Osservati:

Aerospaziale, Difesa, Ambasciate, Energia, Finanza, Governo, High-Tech, Media, Petrolio e gas, Telecomunicazioni e giornalisti.

Particolarità:

Preferenza notevole per il phishing mirato come metodo di accesso iniziale.

MOSES STAFF

Iran

Attiva dal: **2021**

Conosciuto come:

Moses Staff (self given)
Abraham's Ax (self given)
DEV-0500 (Microsoft)
Cobalt Sapling (SecureWorks)

Paesi vittime:

Cile, Germania, India, Israele, Italia, Turchia, Emirati Arabi Uniti, USA.

Settori Osservati:

Energia, Finanza, Governo, Produzione, Trasporti, Servizi.

Particolarità:

Interessanti somiglianze tra Moses Staff e Abraham's Ax.

AGRIUS

Iran 

Attiva dal: **2020**

Conosciuto come:

Agrius (SentinelLabs), DEV-0227 (Microsoft), Black-Shadow (Kaspersky), SharpBoys (?), AMERICIUM (Microsoft), Pink Sandstorm (Microsoft)

Paesi vittime:

Hong Kong, Israele, Sud Africa.

Settori Osservati:

Istruzione, Servizi.

Particolarità:

Recenti rapporti lo hanno associato al Ministero dell'Intelligence e della Sicurezza iraniano (MOIS).

COMMENT CREW

Cina 

Attiva dal: **2006**

Conosciuto come:

Comment Crew (Symantec), Comment Panda (CrowdStrike), TG-8223 (SecureWorks), APT 1 (Mandiant), BrownFox (Symantec), Group 3 (Talos), Byzantine Hades (US State Department), Byzantine Candor (US State Department), Shanghai Group (SecureWorks) GIF89a (Kaspersky)

Paesi vittime:

Belgio, Canada, Francia, India, Israele, Giappone, Lussemburgo, Norvegia, Singapore, Sudafrica, Corea del Sud, Svizzera, Taiwan, Emirati Arabi Uniti, Regno Unito, USA, Vietnam.

Settori Osservati:

Aerospaziale, Chimico, Edile, Difesa, Educazione, Energia, Ingegneria, Intrattenimento, Finanziario, Alimentare e Agricolo, Governativo, Sanitario, High-Tech, IT, Manifatturiero, Media, Minerario, Organizzazioni no-profit, Ricerca, Satelliti, Telecomunicazioni, Trasporti, Legale.

Particolarità:

Il gruppo di minacce cinese è stato associato al 2° Ufficio del Dipartimento di Stato Maggiore Generale (GSD) del 3° Dipartimento dell'Esercito di Liberazione del Popolo Cinese (PLA), comunemente noto come Unità 61398.

COPYKITTENS

Iran 

Attiva dal: **2012**

Conosciuto come:

CopyKittens (Trend Micro)
Slayer Kitten (CrowdStrike)

Paesi vittime:

Germania, Israele, Giordania, Arabia Saudita, Turchia, USA.

Settori Osservati:

Difesa, Istruzione, Governo, IT e Media

Particolarità:

Affidamento su tecniche di social engineering per ingannare i potenziali obiettivi prima dell'infezione. Ciò che distingue questo gruppo è la sua abitudine a mantenere un basso profilo e il suo rifiuto di utilizzare strumenti altamente sofisticati o sfruttare vulnerabilità zero-day.

MADI

Iran 

Attiva dal: **2011**

Conosciuto come:

Madi (Kaspersky)
Mahdi (Kaspersky)

Paesi vittime:

Australia, Ecuador, Grecia, Iran, Iraq, Israele, Mozambico, Nuova Zelanda, Pakistan, Arabia Saudita, Svizzera, Stati Uniti e Vietnam.

Settori Osservati:

istruzione, ingegneria, finanza, governo, petrolio e gas, e think tank.

Particolarità:

Il gruppo ha effettuato una campagna che ha coinvolto 800 vittime in Iran, Israele e in diverse nazioni in un arco temporale di otto mesi: le vittime erano prevalentemente uomini d'affari coinvolti in progetti critici per l'infrastruttura in Iran e Israele, istituti finanziari israeliani, studenti di ingegneria nel Medio Oriente e diverse agenzie governative attive nella regione.

MAGIC HOUND

Iran 

Attiva dal: **2012**

Conosciuto come:

Magic Hound (Palo Alto), APT 35 (Mandiant), Cobalt Illusion (SecureWorks), Cobalt Mirage (SecureWorks), Charming Kitten (CrowdStrike), TEMP.Beanie (FireEye), Timberworm (Symantec), Tarh Andishan (Cylance), TA453 (Proofpoint), Phosphorus (Microsoft), TunnelVision (SentinelOne), UNC788 (FireEye), Yellow Garuda (PWC), Educated Manticore (Check Point), Mint Sandstorm (Microsoft), Ballistic Bobcat (ESET)

Paesi vittime:

Afghanistan, Brasile, Canada, Egitto, Iran, Iraq, Israele, Giordania, Kuwait, Marocco, Pakistan, Arabia Saudita, Spagna, Siria, Turchia, Emirati Arabi Uniti, Regno Unito, Stati Uniti, Venezuela e Yemen.

Settori Osservati:

difesa, energia, finanza, governo, sanità, informatica, produzione, petrolio e gas, tecnologia e telecomunicazioni.

Particolarità:

Utilizzo di tecniche di impersonation al fine di rubare credenziali.

SUBGROUP: DEV-0270, NEMESIS KITTEN

Iran 

Attiva dal: **2022**

Conosciuto come:

DEV-0270 (Microsoft)
Nemesis Kitten (CrowdStrike)
DireFate (BAE Systems)

Paesi vittime:

Settori Osservati:

Particolarità:

Le informazioni di intelligence fornite da Microsoft identificano DEV-0270 come un sottogruppo dell'attore iraniano PHOSPHORUS, noto per le sue attività sponsorizzate dallo stato. Le campagne ransomware associate a DEV-0270 sono state collegate a operazioni dannose di rete presumibilmente condotte per conto del governo iraniano.

OILRIG

Iran 

Attiva dal: **2014**

Conosciuto come:

OilRig (Palo Alto), APT 34 (FireEye), Helix Kitten (CrowdStrike), Twisted Kitten (CrowdStrike), Crambus (Symantec), Chrysene (Dragos), Cobalt Gypsy (SecureWorks), TA452 (Proofpoint), IRN2 (Area 1), ATK 40 (Thales), ITG13 (IBM), EUROPIUM (Microsoft), Hazel Sandstorm (Microsoft)

Paesi vittime:

Azerbaijan, Bahrain, Cina, Egitto, Iraq, Israele, Giordania, Kuwait, Libano, Mauritius, Oman, Pakistan, Qatar, Arabia Saudita, Turchia, Emirati Arabi Uniti, Regno Unito, USA.

Settori Osservati:

Aviazione, Chimico, Istruzione, Energia, Finanza, Governo, High-Tech, Alberghiero, Petrolio e gas, Telecomunicazioni.

Particolarità:

Una delle caratteristiche salienti di questi attacchi recenti è l'adozione di tattiche avanzate di social engineering: i threat actor si sono spostati da offerte di lavoro fasulle a un nuovo approccio, presentandosi come fornitori di servizi legittimi.

OPERATION VICELEAKER

[Unknown]

Attiva dal: **2018**

Conosciuto come:

Operation ViceLeaker (Kaspersky)

Paesi vittime:

Israele

Settori Osservati:

Individui di diverso profilo

Particolarità:

il principale metodo di diffusione di ViceLeaker è attraverso la distribuzione diretta di applicazioni compromesse inviate direttamente alle vittime designate tramite messaggi su Telegram o WhatsApp.

SPHINX

[Unknown]

Attiva dal: **2014**

Conosciuto come:

Sphinx (Qihoo 360)
APT-C-15 (Qihoo 360)

Paesi vittime:

Egitto, Israele

Settori Osservati:

Organizzazioni politiche e militari

Particolarità:

PAT BEAR

Siria

Attiva dal: **2015**

Conosciuto come:

Pat Bear (Qihoo 360)
APT-C-37 (Qihoo 360)
Racquet Bear (CrowdStrike)

Paesi vittime:

Egitto, Israele

Settori Osservati:

Difesa

Particolarità:

Sono state notate somiglianze tra i gruppi di minacce Molerats e APT-C-37. Entrambi i gruppi si concentrano sulla regione del Medio Oriente e del Nord Africa, con particolare attenzione. La tattica di avvicinarsi alle vittime attraverso il phishing, utilizzando documenti esca in arabo legati alla situazione politica della zona, è comune a entrambi.

I GRUPPI

Cozy bear

L'Advanced Persistent Threat (APT) noto come Cozy Bear, ha un'ampia gamma di nomi (APT29 (Mandiant), Cozy Bear (CrowdStrike), The Dukes (F-Secure), Group 100 (Talos), Yttrium (Microsoft), Iron Hemlock (SecureWorks), Minidionis (Palo Alto), CloudLook (Kaspersky), ATK 7 (Thales), ITG11 (IBM)

Grizzly Steppe (US Government), UNC2452 (FireEye), Dark Halo (Volexity), SolarStorm (Palo Alto), StellarParticle (CrowdStrike), SilverFish (Prodaft), Nobelium (Microsoft), Iron Ritual (SecureWorks), Cloaked Ursa (Palo Alto)

BlueBravo (Recorded Future), Midnight Blizzard (Microsoft), e rappresenta un gruppo di cyberspionaggio altamente organizzato e sponsorizzato dallo stato, presumibilmente collegato alla Federazione Russa dal 2008.

Cozy Bear ha dimostrato di avere un obiettivo principale che riguarda i governi occidentali, in particolar modo ministeri e agenzie governative, think tank politici e subappaltatori governativi. Tuttavia, le vittime non si limitano solo all'Occidente; hanno preso di mira anche i governi di membri della Comunità degli Stati Indipendenti, governi asiatici, africani e mediorientali, organizzazioni legate all'estremismo ceceno e individui russi coinvolti nel commercio illecito di sostanze illecite.

Settori Osservati:

Aerospaziale, Difesa, Istruzione, Energia, Finanza, Governo, Sanità, Forze dell'Ordine, Media, Organizzazioni Non Governative (ONG), Farmaceutico, Telecomunicazioni, Trasporti, Think Tank e Settore delle Immagini.

Paesi Coinvolti:

Una vasta gamma di paesi tra cui Australia, Stati Uniti, Russia, Regno Unito, Germania, Giappone, Francia, India, Cina, e molti altri.

La particolarità risiede nella loro ampia gamma di strumenti malware personalizzati, tra cui MiniDuke, CosmicDuke, OnionDuke, CozyDuke, CloudDuke, SeaDuke, HammerDuke, PinchDuke e GeminiDuke.

Negli ultimi anni, hanno condotto campagne di spear-phishing su larga scala, con una frequenza apparentemente semestrale, mirando a centinaia o migliaia di destinatari associati a istituzioni governative e organizzazioni affiliate. Queste campagne adottano un approccio "smash-and-grab," caratterizzato da un'entrata rapida, seguita dalla raccolta e dall'estrazione veloce di dati.

Cozy Bear e il gruppo russo APT28 (Fancy Bear), sono stati responsabili dell'infiltrazione nella rete del Comitato Nazionale Democratico (DNC) negli Stati Uniti, che ha portato a una significativa violazione dei dati.

L'attacco alla catena di approvvigionamento software SolarWinds, condotto dall'APT29, è stato uno dei più sofisticati attacchi di questo tipo, coinvolgendo 18.000 aziende in tutto il mondo che avevano scaricato versioni manipolate della piattaforma di gestione IT SolarWinds Orion.

Nel 2022, è stato scoperto un documento ingannevole che si presume appartenesse all'APT29, contenente uno script dannoso e che sembrava provenire dall'Ambasciata di Israele.

Wizard spider

Wizard Spider, anche conosciuto come Grim Spider (CrowdStrike), TEMP.MixMaster (FireEye), Gold Blackburn (SecureWorks), Gold Ulrick (SecureWorks), ITG23 (IBM)

DEV-0193 (Microsoft), Periwinkle Tempest (Microsoft), è un gruppo di minacce che sembrerebbe essere associato a Lunar Spider.

Il gruppo, con base in Russia, è noto per la creazione e la gestione del malware bancario TrickBot; originariamente orientato verso frodi finanziarie nel 2016, ha successivamente ampliato il proprio raggio d'azione, diventando un'entità altamente avanzata con un vasto e potente arsenale, gestendo diverse famiglie di ransomware con modalità operative differenziate. Utilizzando TrickBot e BazarLoader per infiltrarsi negli ambienti delle vittime, il gruppo ha mostrato una capacità reattiva di fronteggiare e aggirare i tentativi di contrasto.

Questo gruppo rappresenta un'impresa criminale in espansione, di cui Grim Spider sembra essere una suddivisione. D'altra parte, il gruppo di minacce Lunar Spider, con sede nell'Europa orientale, opera e sviluppa un malware bancario di base chiamato BokBot (conosciuto anche come IcedID), che è stato individuato per la prima volta nell'aprile del 2017. Il malware BokBot fornisce ai membri affiliati di Lunar Spider varie funzionalità per il furto di credenziali e frode bancaria, attraverso l'uso di webinject e una funzione di distribuzione del malware.

Diversi settori, tra cui Difesa, Finanza, Governo, Sanità e Telecomunicazioni, sono stati colpiti dagli attacchi di WIZARD SPIDER, con attività osservate in varie parti del mondo.

Dal settembre 2018, il ransomware Ryuk, utilizzato dal gruppo, ha rappresentato un'importante fonte di guadagno attraverso richieste di riscatto. Si stima che le vittime abbiano pagato oltre 61 milioni di dollari per ripristinare i file crittografati da Ryuk, secondo quanto riportato dal Federal Bureau of Investigation (FBI) degli Stati Uniti. Nel marzo 2020, WIZARD SPIDER ha temporaneamente interrotto la distribuzione di Ryuk fino a metà settembre.

Nonostante l'interruzione di Ryuk, tra marzo e settembre 2020, il gruppo è passato al ransomware Conti, rilevato per la prima volta nel giugno 2020. WIZARD SPIDER ha dimostrato un approccio variegato nella selezione dei bersagli, caratteristica delle sue operazioni su vasta scala nel campo del ransomware. Durante le campagne, Conti è stato soggetto a un continuo sviluppo da parte dell'APT, integrando regolarmente nuove funzionalità, tecniche di offuscamento e modifiche al codice, con aggiornamenti quasi settimanali.

Il 7 settembre 2023, gli Stati Uniti, in collaborazione con il Regno Unito, hanno imposto sanzioni a undici individui appartenenti al gruppo di criminali informatici collegati a Trickbot, con sede in Russia.

Al Qassam

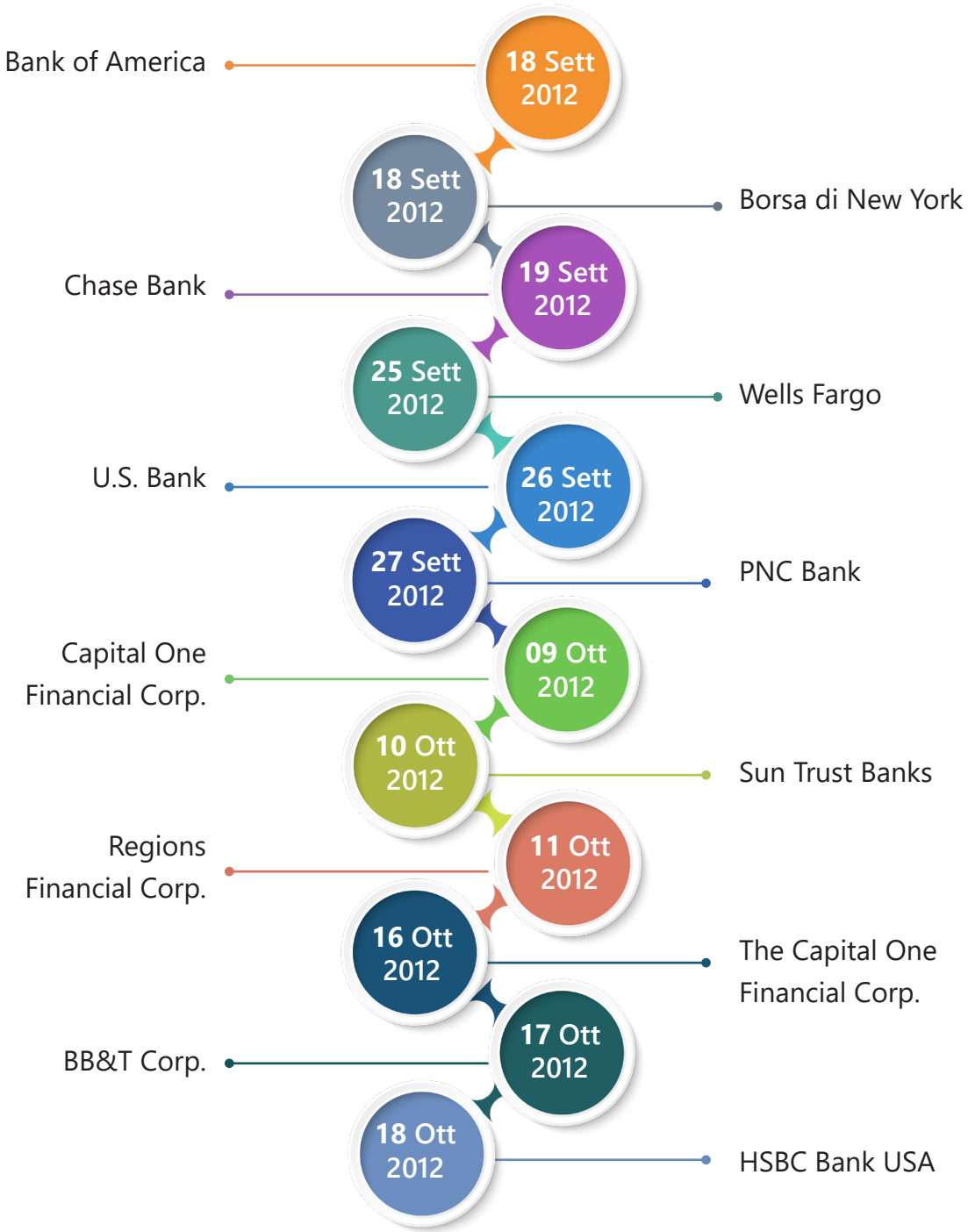
gruppo conosciuto anche con il nome di Cyber fighters of Izz Ad-Din Al Qassam (self given), Qassam Cyber Fighters (self given), QCF (self given), Fraternal Jackal (CrowdStrike).

La comparsa di Qassam Cyber Fighters (QCF) nel panorama delle minacce informatiche ha suscitato preoccupazione **da settembre 2012,** quando il gruppo ha annunciato il proprio obiettivo di condurre attacchi informatici contro istituzioni finanziarie statunitensi. Il messaggio pubblicato su Pastebin, redatto sia in inglese che in arabo, ha chiarito l'intenzione del gruppo di attaccare le banche statunitensi come risposta al video anti-musulmano "Innocence of Muslims".

Il gruppo ha rivendicato attacchi contro numerose istituzioni finanziarie, tra cui Bank of America, la Borsa di New York e altre banche di rilievo negli Stati Uniti. La vastità dei bersagli indica l'entità e la portata degli attacchi perpetrati dal gruppo, creando preoccupazione per la sicurezza delle istituzioni finanziarie e sollevando interrogativi sulle implicazioni geopolitiche di tali azioni.

L'operazione Ababil, nome con cui vennero denominati questi attacchi, rappresentò una diretta reazione alle nuove sanzioni economiche imposte dagli Stati Uniti all'Iran. La complessità dell'operazione ha portato l'amministrazione statunitense a sospettare che gli aggressori fossero affiliati al governo iraniano.

Le banche che sono state oggetto di attacco durante l'Operazione Ababil includono:



Nonostante il rapido ripristino dei servizi, l'operazione ha provocato danni stimati in decine di milioni di dollari e ha scosso il settore finanziario statunitense, evidenziando la vulnerabilità delle istituzioni bancarie rispetto agli attacchi informatici di questo tipo.

Desert Falcon

L'APT Desert Falcon è noto con vari nomi come APT-C-23 (Qihoo 360), Two-tailed Scorpion (Qihoo 360), Arid Viper (Palo Alto), ATK 66 (Thales), TAG-CT1 (Recorded Future), Mantis (Symantec). Osservato per la prima volta **nel 2011**, si ritiene che operi dalla regione di Gaza ed è sponsorizzato da Hamas.

Le loro attività si estendono a una vasta gamma di paesi in tutto il mondo:

- **Europa:** Albania, Belgio, Bosnia ed Erzegovina, Danimarca, Francia, Germania, Grecia, Italia, Paesi Bassi, Norvegia, Portogallo, Romania, Russia, Svezia, Ucraina.
- **Medio Oriente e Africa del Nord:** Algeria, Egitto, Iran, Iraq, Israele, Giordania, Kuwait, Libano, Libia, Mali, Mauritania, Marocco, Palestina, Qatar, Arabia Saudita, Sudan, Siria, Turchia, Emirati Arabi Uniti, Yemen.
- **Asia:** Cina, India, Giappone, Pakistan, Taiwan.
- **Nord America:** Canada, Stati Uniti.
- **Sud America:** Messico.
- **Africa:** Zimbabwe.

Questo ampio raggio di nazioni suggerisce che questo gruppo di minacce è coinvolto in attività di spionaggio su scala internazionale. Essi mirano a vari settori chiave, inclusi settori governativi e difensivi, nonché infrastrutture critiche, media e trasporti.

Le vittime degli attacchi finora sono state selezionate con cura; sono attive e influenti nelle rispettive culture, ma sono anche attraenti per i cybercriminali come fonti di informazioni e obiettivi per l'estorsione.

Desert Falcon è sospettato di operare per conto di Hamas: le Forze di Difesa Israeliane (IDF) hanno segnalato una campagna mirata ai soldati vicino al confine con Gaza, attribuita all'APT in questione sulla base della vittimologia e delle somiglianze con attività precedenti. Questo gruppo ha dimostrato di prendere di mira individui di alto profilo palestinesi e israeliani, oltre a gruppi più ampi, in particolare nel settore della difesa, delle organizzazioni governative, delle forze dell'ordine e dei partiti o movimenti politici. Utilizza spesso attacchi di phishing e social engineering per infettare i bersagli,

e social media come Facebook e Instagram per instaurare rapporti con le vittime.

Le vittime delle loro operazioni suggeriscono dunque che il target demografico è costituito da individui associati a gruppi pro-Fatah, organizzazioni governative palestinesi, personale militare e di sicurezza e gruppi di studenti in Palestina.

A fine novembre 2019, Arid Viper ha registrato il dominio enti5abat[.]pw ("enti5abat" ricorda la parola "aintikhabat", che si traduce in arabo con "elezioni") e hanno creato un sito web che imiti la Commissione Elettorale Centrale (CEC) palestinese, il cui vero dominio è elections[.]ps, per ingannare gli utenti ad inserire le loro credenziali.

Si tratta di un evento significativo perché la Palestina non ha avuto elezioni presidenziali dal 2005, anche se si era parlato di elezioni sia nel 2014 che nel 2018. All'inizio dell'autunno 2019, Mahmoud Abbas, presidente dell'Autorità nazionale palestinese, ha annunciato all'Assemblea generale delle Nazioni Unite l'intenzione di fissare una data all'inizio del 2020 per lo svolgimento di elezioni generali.

Sebbene vi siano prove di attacchi opportunistici al di fuori della Palestina, tali casi appaiono politicamente motivati e coerenti con gli obiettivi di questo attore della minaccia. I bersagli includono individui legati all'Autorità Nazionale Palestinese, al movimento Fatah, nonché ad altre organizzazioni governative di opposizione, ai servizi di sicurezza e a gruppi studenteschi:

- Autorità Nazionale Palestinese
- Ministero dell'Istruzione
- Ministero dell'Economia Nazionale
- Servizio di Sicurezza Preventiva Palestinese
- Organizzazione per la Liberazione della Palestina
- Movimento di Liberazione Nazionale Palestinese Fatah
- Polizia Speciale Palestinese
- Movimenti studenteschi affiliati a Fatah
- Ministero degli Interni
- Altri enti governativi

Polonium

Polonium è un gruppo APT (Advanced Persistent Threat) con sede in Libano e affiliato ad Hezbollah, noto anche con il nome Plaid Rain, che si dedica a campagne di ciberspionaggio contro Israele.

A partire da febbraio **2022**, il gruppo APT Polonium ha concentrato le sue attività principalmente su organizzazioni situate in Israele, con una particolare enfasi sui settori della produzione, dell'IT e dell'industria della difesa israeliana. In almeno un caso documentato, Polonium ha compromesso un'azienda nel settore dell'informatica e ha utilizzato questa violazione per condurre un attacco alle catene di approvvigionamento. Questo attacco ha sfruttato le credenziali dei fornitori di servizi per ottenere accesso alle reti delle organizzazioni vittime, colpendo successivamente un'azienda aeronautica e uno studio legale.

Le organizzazioni vittime di Polonium appartengono dunque a diversi settori, tra cui produzione, IT, sistemi di trasporto, difesa, agenzie e servizi governativi, prodotti alimentari e agricoltura, servizi finanziari, sanità e salute pubblica e i paesi principali coinvolti sono Israele e il Libano.Questa diversificazione dei settori obiettivo suggerisce un ampio spettro di interessi per Polonium nell'ambito delle sue operazioni di cyberspionaggio.

Esiste una probabile collaborazione con i servizi di intelligence iraniani, in particolare con il Ministero dell'Intelligence e della Sicurezza dell'Iran (MOIS), come suggerito dalla sovrapposizione delle vittime e dalla similitudine di strumenti e tecniche. Questa possibile connessione con Teheran è in linea con le tendenze emerse dal 2020, secondo le quali l'Iran utilizza terze parti per condurre operazioni cibernetiche in modo da aumentare la sua plausibile negabilità.

Polonium dispone di un insieme di sette backdoor personalizzate nel proprio arsenale:

- ***CreepyDrive***, che sfrutta i servizi cloud di OneDrive e Dropbox per il comando e il controllo (C&C);
- ***CreepySnail,*** responsabile dell'esecuzione dei comandi ricevuti dall'infrastruttura degli attaccanti;
- ***DeepCreep e MegaCreep,*** che fanno uso dei servizi di archiviazione file di Dropbox e Mega;
- ***FlipCreep,*** TechnoCreep e PapaCreep, che ricevono i comandi dai server degli attaccanti.

Parallelamente, il gruppo ha adottato diversi moduli personalizzati per condurre operazioni di spionaggio sui propri obiettivi.

Nel 2022, Polonium ha preso di mira più di 20 organizzazioni con sede in Israele e un'organizzazione intergovernativa con operazioni in Libano. In particolare, ha creato e utilizzato account legittimi di OneDrive come parte delle sue operazioni di attacco.

Volatile Cedar

Il gruppo è stato osservato per la prima volta **nel 2012** e, in modo simile a Plaid Rain, viene associato al gruppo militante sciita libanese Hezbollah e alla possibile coordinazione con attori legati all'Iran, affiliati con il Ministero dell'Intelligence e della Sicurezza (MOIS).

I metodi di accesso iniziale osservati con maggiore frequenza si concentrano sulla compromissione dei server web delle vittime attraverso vulnerabilità zero-day per l'installazione di webshells, tra cui ASPXSpy, devilzshell e Caterpillar.

Settori osservati: **Educazione, Governo** e **Hosting.**

Paesi colpiti:

Canada, Egitto, Israele, Giordania, Libano, Russia, Arabia Saudita, Emirati Arabi Uniti, Regno Unito, Stati Uniti e Autorità Palestinese.

Molerats

Molerats (noto con vari nomi tra cui *Extreme Jackal (CrowdStrike), Gaza Cybergang (Kaspersky), Gaza Hackers Team (Kaspersky), TA402 (Proofpoint), Aluminum Saratoga (SecureWorks), ATK 89 (Thales), TAG-CT5 (Recorded Future)*, è un gruppo attivo almeno **dal 2012** che mira principalmente al Medio Oriente, compresi Israele e la Palestina, osservato in misura minore anche nell'UE e negli Stati Uniti e sembrerebbero essere affiliati ad Hamas. I bersagli del gruppo includono entità governative, della difesa, dell'energia, finanziarie, dei media, della tecnologia, delle telecomunicazioni. Il gruppo ha storicamente mostrato una preferenza notevole per il phishing mirato come metodo di accesso iniziale. Gli strumenti includono Molerat Loader, XtremeRAT, SharpStage, DropBook, Spark, Pierogi, PoisonIvy e molti altri osservati nel corso degli anni.

Alcuni dei maggiori attacchi osservati sono:

Gennaio 2012: Defacement del sito web del servizio antincendio di Israele da parte di criminal hacker che dichiarano di essere dalla Striscia di Gaza, con un messaggio che recita "Morte a Israele."

Ottobre 2012: Attacchi di malware contro obiettivi governativi israeliani.

Giugno 2013-2014 Attacchi contro obiettivi nel Medio Oriente e negli Stati Uniti.

2014 Operazione "Moonlight" con attacchi mirati contro entità del Medio Oriente che coinvolgono oltre 200 malware generati dal gruppo negli ultimi due anni. Questi attacchi erano incentrati su questioni politiche del Medio Oriente.

2016 Durante l'operazione "DustySky" sono stati condotti attacchi contro vari obiettivi nel Medio Oriente.

Novembre 2016 Gli analisti di PwC hanno rilevato la continuazione di una campagna malware iniziata nell'aprile 2016, che ha preso di mira siti web di notizie in lingua araba, figure politiche e altri obiettivi influenti nei territori palestinesi e nei paesi arabi limitrofi.

Gennaio 2019 Con la campagna "Spark" il gruppo ha usato la tecnica del social engineering per infettare vittime principalmente nei territori palestinesi. Questa campagna si è concentrata su eventi geopolitici recenti, inclusi il conflitto israelo-palestinese, l'assassinio di Qasem Soleimani e il conflitto in corso tra Hamas e il movimento Fatah palestinese.

Moses Staff

Da settembre **2021**, si è assistito all'inizio di una serie di attacchi informatici mirati alle organizzazioni israeliane da parte del gruppo conosciuto come Moses Staff. Questa azione si è aggiunta a una sequenza di attacchi avviati circa un anno prima da altri gruppi quali Parisite, Fox Kitten, Pioneer Kitten e Agrius. Le azioni di questi attori erano prevalentemente motivate da scopi politici, cercando di generare un impatto mediatico e danneggiare l'immagine del Paese.

Tuttavia, Moses Staff si è distinto per il proprio comportamento differente rispetto agli altri gruppi: il gruppo ha dichiarato esplicitamente che il suo obiettivo nel prendere di mira le aziende israeliane è causare danni mediante la divulgazione di dati sensibili rubati e crittografando le reti delle vittime, senza formulare alcuna richiesta di riscatto. Nella terminologia utilizzata dagli aggressori, il loro scopo si basa su "combattere la resistenza e denunciare i crimini dei sionisti nei territori occupati".

Questa variazione di approccio evidenzia un cambiamento nelle motivazioni e negli obiettivi degli attacchi informatici, passando da richieste finanziarie a un intento più marcatamente politico. Moses Staff si propone quindi di agire come un ente che mira a danneggiare attivamente la reputazione e la sicurezza delle organizzazioni israeliane, proponendo una motivazione di resistenza politica piuttosto che perseguire guadagni finanziari attraverso estorsioni.

Inoltre, l'analisi condotta dalla Counter Threat Unit™ (CTU) di Secureworks ha rivelato interessanti somiglianze tra due gruppi di hacktivisti: Moses Staff, emerso nel settembre 2021, e Abraham's Ax, comparso nel novembre 2022. Questa indagine evidenzia punti in comune nell'iconografia, videografia e nei siti web utilizzati dai due gruppi, suggerendo una possibile connessione o gestione da parte di un'unica entità.

Entrambi i gruppi utilizzano figure bibliche come punto di partenza per la propria identità, incorporando citazioni religiose all'interno dei loro siti. Tuttavia, mentre Moses Staff si focalizza sull'attacco diretto alle organizzazioni israeliane, Abraham's Ax adotta una posizione diversa: afferma di operare a nome dell'Hezbollah Ummah, associando il suo intento a un partito politico islamico sciita libanese e a un gruppo militante sostenuto dall'Iran, pur senza prove concrete di un legame diretto con tale entità.

Abraham's Ax, anziché attaccare direttamente Israele, concentra i propri sforzi sui ministeri del governo dell'Arabia Saudita. Il gruppo ha reso pubblici dati presumibilmente ottenuti da attacchi al Ministero dell'Interno, insieme a un video contenente conversazioni telefoniche presumibilmente intercettate tra ministri del governo saudita. Questo potrebbe riflettere una risposta al ruolo di lea-

dership dell'Arabia Saudita nel tentativo di migliorare le relazioni tra Israele e le nazioni arabe, vista come una minaccia agli interessi dell'Iran nella regione. In particolare, le discussioni riguardanti la potenziale collaborazione nella difesa aerea tra Arabia Saudita e altri Paesi potrebbero aver spinto l'Iran a percepire tali relazioni come una minaccia.

Entrambi i gruppi hanno prodotto video come parte delle loro operazioni. Questi video, in stile cinematografico hollywoodiano, mostrano azioni di hacking coinvolgenti satelliti, telecamere di sorveglianza, modelli tridimensionali di edifici.

In merito alla guerra, Moses Staff ha avvertito Israele: "Subirete danni irreparabili in campo informatico e infrastrutturale. D'ora in poi dovrete pagare per ogni sangue versato. Aspettatevi grandi attacchi combinati. Il nostro obiettivo è chiaro, specifico e preciso". Il gruppo ha pubblicato un filmato della base del Mossad e della unit-8200 del regime criminale sionista.

Oltre all'obiettivo principale rappresentato da Israele, il gruppo Moses Staff ha preso di mira organizzazioni in diverse altre nazioni, tra cui Italia, India, Germania, Cile, Turchia, Emirati Arabi Uniti e Stati Uniti e ha puntato diversi settori, tra cui quelli governativi, finanziari, energetici, manifatturieri e dei servizi pubblici.

Agrius

Agonizing Serpens, conosciuto anche come Agrius, è un gruppo APT emerso **nel 2020** che si presume abbia legami con l'Iran e concentri principalmente le sue azioni nel Medio Oriente. Questo gruppo è principalmente riconosciuto per la sua pericolosa attività, che comprende attacchi distruttivi mediante wiper e falsi ransomware, mirati principalmente a organizzazioni israeliane in vari settori e paesi.

Anche se non è del tutto chiara la sua connessione all'interno dell'Iran, recenti rapporti lo hanno associato al Ministero dell'Intelligence e della Sicurezza iraniano (MOIS).

Gli attacchi condotti si concentrano principalmente su due obiettivi fondamentali: il primo riguarda il furto di informazioni sensibili, inclusi dati personali e proprietà intellettuale. Queste informazioni vengono successivamente pubblicate dagli attori minacciosi su piattaforme di social media o canali come Telegram. Sembrerebbe che il loro intento nel pubblicare tali dati sia quello di seminare paura o danneggiare la reputazione delle vittime. Il secondo obiettivo è quello di generare caos e infliggere danni significativi. Nei più recenti attacchi condotti, gli aggressori non hanno richiesto un riscatto, ma il risultato potenziale è stato comunque la significativa perdita di dati e la compromissione delle attività aziendali.

Da quando è emerso, il gruppo ha continuamente sviluppato nuovi strumenti personalizzati e ha sfruttato strumenti e tecniche di hacking consolidati al fine di portare avanti le proprie operazioni aggressive. La loro presenza e la continua evoluzione dei loro metodi rappresentano una minaccia significativa per le organizzazioni coinvolte e richiedono un'attenta vigilanza e sicurezza informatica per mitigare tali rischi.

Il gruppo ha adottato una tattica ingannevole, facendo apparire gli attacchi come ransomware per mascherare i loro obiettivi reali, tracciando un percorso diversivo per eludere la rilevazione da parte dei team di sicurezza.

Oltre all'uso di MultiLayer, il gruppo ha introdotto due nuovi strumenti distruttivi denominati BFG Agonizer e Partial Washer. Parallelamente, i criminal hacker hanno sviluppato un'applicazione personalizzata, Sqlextractor, progettata per estrarre i record dai database dei server compromessi.

Il ransomware di recente individuazione, denominato Moneybird e utilizzato da questo gruppo, è stato impiegato per attaccare organizzazioni in Israele. Questo è collegato alle precedenti azioni di Agrius contro altre istituzioni in Israele, in particolare Shirbit e l'Università Bar Ilan.

In particolar modo, i settori dell'istruzione e tecnologici israeliani sono stati presi di mira come parte di una serie di attacchi informatici distruttivi iniziati a gennaio 2023, verificatesi fino a ottobre.

Comment Crew

Emerso **nel 2006**, Comment Crew, noto spesso anche come APT1, è un gruppo APT con forti legami con l'esercito cinese. Attivi fino al 2010, gli attori di questa minaccia hanno colpito oltre 140 aziende statunitensi, mirando a dati aziendali sensibili e proprietà intellettuale. Il gruppo di minacce cinese è stato associato al 2° Ufficio del Dipartimento di Stato Maggiore Generale (GSD) del 3° Dipartimento dell'Esercito di Liberazione del Popolo Cinese (PLA), comunemente noto come Unità 61398.

Altri nomi con cui è noto il gruppo sono Comment Panda (CrowdStrike), TG-8223 (SecureWorks)

APT 1 (Mandiant), BrownFox (Symantec), Group 3 (Talos), Byzantine Hades (US State Department), Byzantine Candor (US State Department), Shanghai Group (SecureWorks), GIF89a (Kaspersky).

Il loro modus operandi principale prevedeva campagne di spear-phishing, inviando e-mail con documenti dal titolo personalizzato per le potenziali vittime, come "ArmyPlansConferenceOnNewGCV-Solicitation.pdf" o "Chinese Oil Executive Learning From Experience.doc".

Le tattiche sofisticate utilizzate da Comment Crew hanno dimostrato una certa maestria nel nascondere le proprie attività, rendendo la rilevazione più complessa per le difese informatiche tradizionali. Questo gruppo è stato particolarmente abile nel penetrare le reti aziendali e rubare dati sensibili, un'azione che ha sollevato preoccupazioni significative sulla sicurezza delle informazioni aziendali negli Stati Uniti.

Il gruppo ha preso di mira un'ampia varietà di settori, dimostrando una grande versatilità e interessi diversificati. Tra i settori colpiti ci sono: Aerospaziale, Chimico, Costruzioni, Difesa, Educazione, Energia, Ingegneria, Intrattenimento, Finanza, Alimentare e Agricolo, Governo, Sanità, High-Tech, IT, Manifatturiero, Media, Organizzazioni non-profit, Telecomunicazioni, Trasporti.

Inoltre, l'attività dell'APT ha avuto impatto su diversi paesi in tutto il mondo:

Belgio, Canada, Francia, India, Israele, Giappone, Lussemburgo, Norvegia, Singapore, Sudafrica, Corea del Sud, Svizzera, Taiwan, Emirati Arabi Uniti, Regno Unito, Stati Uniti d'America, Vietnam.

Per quanto riguarda l'Israele, nel corso del 2011 e del 2012, tre importanti subappaltatori del programma di difesa israeliano, coinvolti nella costruzione dello scudo missilistico "Iron Dome", sono stati compromessi da attacchi informatici che hanno portato al furto di una vasta quantità di documenti altamente sensibili riguardanti la tecnologia alla base del famoso scudo.

Gli attacchi hanno coinvolto tre aziende chiave israeliane nel campo della difesa: Elisra Group, Israel Aerospace Industries e Rafael Advanced Defense System: tra il 10 ottobre 2011 e il 13 agosto 2012,

si ritiene che criminal hacker provenienti dalla Cina abbiano violato le reti aziendali di queste tre aziende, estraendo una considerevole quantità di dati sensibili. Gran parte di queste informazioni riguardava la proprietà intellettuale associata ai missili Arrow III, ai veicoli aerei a pilotaggio remoto, ai razzi balistici e ad altri documenti tecnici correlati.

L'Israel Aerospace Industries (IAI) è stata inizialmente compromessa il 16 aprile 2012 attraverso una serie mirata di attacchi di phishing via e-mail. Questi attacchi avevano somiglianze con le tattiche attribuite alla "Comment Crew". Dopo aver ottenuto accesso alla rete dell'IAI, i membri della Comment Crew hanno trascorso circa quattro mesi del 2012 installando software dannosi e sfruttando credenziali, compiendo attività di raccolta di informazioni sensibili.

CopyKittens

CopyKittens è un gruppo di cyber-spionaggio emerso per la prima volta **nel 2013**, operante con presunta affiliazione iraniana. La portata delle sue attività ha coinvolto diversi paesi chiave come Israele, Arabia Saudita, Turchia, Stati Uniti, Giordania e Germania. Questo gruppo è stato collegato alla campagna nota come "Operazione Wilted Tulip".

Gli hacker hanno violato l'account e-mail di un dipendente del Ministero degli Esteri nella Repubblica Turca di Cipro del Nord. L'account compromesso è stato utilizzato per inviare un documento a ministeri degli esteri di vari paesi in tutto il mondo.

I settori bersaglio delle sue operazioni comprendono: **Difesa**, **Istruzione**, **Governo**, **IT** e **Media**.

Nel 2014, si ritiene abbiano tentato di infiltrarsi nel Ministero degli Affari Esteri di Tel Aviv, cercando anche di accedere ai sistemi di rinomati accademici israeliani specializzati negli studi del Medio Oriente. Alcuni degli attacchi mirati alle entità israeliane hanno sfruttato anche profili social fasulli, spesso appartenenti a donne attraenti.

Il gruppo ha condotto una serie di attacchi, con particolare rilevanza nell'anno 2015. Similarmente ad altri attori di minacce, fa affidamento su tecniche di social engineering per ingannare i potenziali obiettivi prima dell'infezione.

Ciò che distingue questo gruppo è la sua abitudine a mantenere un basso profilo: non ci sono evidenze dell'utilizzo da parte del gruppo di strumenti altamente sofisticati o sfruttamento di vulnerabilità zero-day.

Madi

L'Advanced Persistent Threat Madi, noto anche come "Mahdi", ha fatto la sua comparsa **nel 2011**. Il gruppo ha effettuato una campagna che ha coinvolto 800 vittime in Iran, Israele e in diverse nazioni in un arco temporale di otto mesi: le vittime erano prevalentemente uomini d'affari coinvolti in progetti critici per l'infrastruttura in Iran e Israele, istituti finanziari israeliani, studenti di ingegneria nel Medio Oriente e diverse agenzie governative attive nella regione.

I settori sotto osservazione includono **istruzione**, **ingegneria**, **finanza**, **governo**, **petrolio** e **gas**, e **think tank**.

Questo gruppo ha dimostrato una presenza diffusa in una varietà di paesi, tra cui Australia, Ecuador, Grecia, Iran, Iraq, Israele, Mozambico, Nuova Zelanda, Pakistan, Arabia Saudita, Svizzera, Stati Uniti e Vietnam.

Magic Hound

Magic Hound è un gruppo sponsorizzato dall'Iran noto per attività di furto di informazioni e spionaggio principalmente nel Medio Oriente. Attivo **dal 2012**, il gruppo ha come bersaglio organizzazioni nei settori dell'energia, del governo e della tecnologia, specialmente quelle con interessi o basi in Arabia Saudita.

Conosciuto anche come:

APT 35 (Mandiant), Cobalt Illusion (SecureWorks), Cobalt Mirage (SecureWorks), Charming Kitten (CrowdStrike), TEMP.Beanie (FireEye), Timberworm (Symantec), Tarh Andishan (Cylance), TA453 (Proofpoint), Phosphorus (Microsoft), TunnelVision (SentinelOne), UNC788 (FireEye), Yellow Garuda (PWC), Educated Manticore (Check Point), Mint Sandstorm (Microsoft), Ballistic Bobcat (ESET).

Inoltre, presenta un sottogruppo denominato DEV-0270, noto come Nemesis Kitten, che sembra derivare dall'evoluzione di Cutting Kitten, precedentemente identificato come TG-2889.

Esistono intersezioni infrastrutturali con altri gruppi di minacce, tra cui Rocket Kitten, Newscaster, NewsBeef, ITG18 e APT 42. Magic Hound opera in diversi settori chiave come difesa, energia, finanza,

governo, sanità, informatica, produzione, petrolio e gas, tecnologia e telecomunicazioni, concentrandosi sulle organizzazioni collegate all'Arabia Saudita e agli attivisti per i diritti civili e umani. Le attività del gruppo sono state rilevate in varie nazioni, tra cui Afghanistan, Brasile, Canada, Egitto, Iran, Iraq, Israele, Giordania, Kuwait, Marocco, Pakistan, Arabia Saudita, Spagna, Siria, Turchia, Emirati Arabi Uniti, Regno Unito, Stati Uniti, Venezuela e Yemen.

Nel 2018, il gruppo ha assunto il falso nome della società di sicurezza informatica che ha esposto le sue operazioni e campagne. La società israeliana ClearSky Security ha dichiarato che il gruppo è riuscito a replicare il suo sito web ufficiale su un dominio dal nome simile - clearskysecurity[.]net. Il sito web reale di ClearSky è Clearskysec.com.

"Hanno copiato pagine dal nostro sito web pubblico e ne hanno modificata una per includere un'opzione 'accedi' con diversi servizi. Queste opzioni di accesso sono tutte pagine di phishing che avrebbero inviato le credenziali della vittima agli aggressori."

Il sito web ufficiale di ClearSky non presenta opzioni di accesso. Poiché il sito era ancora in costruzione, ClearSky non ritiene che gli hacker siano riusciti a effettuare phishing su alcuno, aggiungendo che i suoi dipendenti, sistemi e clienti non sono stati influenzati dall'incidente.

Altra azienda legittima impersonata dal gruppo di hacker è la United Technologies (UTC). All'inizio del 2017, gli aggressori hanno creato un falso sito web di UTC che affermava di offrire "Programmi e Corsi Speciali Gratuiti per Dipendenti di Aziende Aerospaziali" progettati per ingannare i visitatori nello scaricare un falso documento che era in realtà il malware DownPaper del gruppo.

Il 21 novembre 2017, il Dipartimento di Giustizia degli Stati Uniti ha reso pubblico un atto di accusa contro Behzad Mesri (alias "Skote Vahshat") per il suo coinvolgimento nell'hacking e nell'estorsione a danno di HBO, nonché per aver successivamente diffuso i contenuti rubati su Internet. I dati trapelati includevano informazioni riservate su episodi imminenti della popolare serie televisiva "Game of Thrones" e file video contenenti episodi inediti di altre serie televisive create da HBO.

Secondo l'atto d'accusa, "Mesri è un hacker informatico con base in Iran che in passato aveva lavorato per conto dell'esercito iraniano per condurre attacchi informatici mirati a sistemi militari, sistemi software nucleari e infrastrutture israeliane. Inoltre, Mesri è stato membro di un gruppo di criminal hacker con sede in Iran chiamato "Turk Black Hat". Un'analisi condotta da ClearSky ha identificato connessioni tra l'attività di questo gruppo con Magic Hound.

Alla fine del 2020, il gruppo ha lanciato una campagna di phishing che ha preso di mira professionisti medici specializzati in genetica, neurologia e ricerca oncologica negli Stati Uniti e in Israele. Quest'ultima campagna, denominata BadBlood, si discosta dalle attività abituali del gruppo. Se da

un lato questa campagna può rappresentare un cambiamento nel target generale, è anche possibile che sia il risultato di una specifica esigenza di raccolta di intelligence a breve termine. BadBlood è in linea con la tendenza crescente della ricerca medica, sempre più bersaglio degli attori delle minacce.

Nel 2021 il gruppo ha condotto un'operazione di spear-phishing che mirava a dirigenti di alto profilo in Israele e negli Stati Uniti. Gli aggressori hanno preso il controllo delle e-mail di persone di spicco in Israele e successivamente le hanno utilizzate per mirare ad altri funzionari di alto livello al fine di rubare informazioni personali. Tra i bersagli ci sono stati l'ex Ministro degli Esteri israeliano, Tzipi Livni, l'ex Ambasciatore degli Stati Uniti in Israele, un ex Maggiore Generale dell'IDF e altre tre persone.

A novembre 2021, l'Agenzia per la Sicurezza delle Infrastrutture e dei Servizi (CISA) degli Stati Uniti ha sollevato l'allarme riguardo a un gruppo di hacker iraniani sponsorizzati dallo stato che sfruttava vulnerabilità critiche ben note in Fortinet FortiOS, FortiGate e Microsoft Exchange.

In un caso particolare, datato ad agosto, gli esperti di sicurezza di ESET hanno documentato un attacco condotto da Charming Kitten contro un'organizzazione israeliana. Il gruppo ha sfruttato la vulnerabilità CVE-2021-34473, una vulnerabilità di esecuzione remota di codice (RCE) valutata 9.8 secondo il sistema di valutazione CVSS, presente in Microsoft Exchange. Nel corso dei mesi successivi, Charming Kitten ha sfruttato l'accesso ottenuto attraverso la CVE-2021-34473 per rilasciare una serie di payload in evoluzione, giungendo infine, nel dicembre successivo, al suo ultimo backdoor denominato "Sponsor".

Nel corso degli ultimi due anni, dopo l'avvertimento di CISA, Charming Kitten ha ripetutamente sfruttato la stessa vulnerabilità, sfruttando i server MS Exchange esposti per rilasciare il malware Sponsor. Inoltre, il gruppo ha impiegato diverse altri tool open source, come Mimikatz e Plink (Putty Link), nelle reti israeliane non aggiornate.

Subgroup: DEV-0270, Nemesis Kitten

Comparso **nel 2022**, DEV-0270, noto anche come Nemesis Kitten, emerge come un sottogruppo all'interno della più ampia minaccia Magic Hound, mostrando connessioni con altre organizzazioni come APT 35, Cobalt Illusion e Charming Kitten.

Le informazioni di intelligence fornite da Microsoft identificano DEV-0270 come un sottogruppo dell'attore iraniano PHOSPHORUS, noto per le sue attività sponsorizzate dallo stato. Le campagne ransomware associate a DEV-0270 sono state collegate a operazioni dannose di rete presumibilmente condotte per conto del governo iraniano.

OilRig, APT 34, Helix Kitten, Chrysene

Il gruppo di minacce noto come OilRig con presunte origini iraniane ha iniziato le sue operazioni almeno dal 2014 ed è conosciuto con vari nomi, quali APT 34 (FireEye), Helix Kitten (CrowdStrike). Twisted Kitten (CrowdStrike), Crambus (Symantec), Chrysene (Dragos), Cobalt Gypsy (SecureWorks), TA452 (Proofpoint), IRN2 (Area 1)

ATK 40 (Thales), ITG13 (IBM), EUROPIUM (Microsoft), Hazel Sandstorm (Microsoft).

Il gruppo ha focalizzato la sua attenzione su vittime nel Medio Oriente, mostrando un particolare interesse per settori chiave quali finanza, governo, energia, settore chimico e telecomunicazioni.

OilRig presenta un sottogruppo noto come Greenbug, Volatile Kitten. Inoltre, il gruppo mostra chiare sovrapposizioni con altri attori di minacce come APT 33, Elfin, Magnallium, e possibilmente anche con DNSpionage e Hexane.

Si distingue per la mirata attenzione alle infrastrutture e agli interessi del Medio Oriente, con in particolare attacchi alla supply chain.

Una delle caratteristiche salienti di questi attacchi recenti è l'adozione di tattiche avanzate di social engineering: i threat actor si sono spostati da offerte di lavoro fasulle a un nuovo approccio, presentandosi come fornitori di servizi legittimi. Questa tattica mira a sfruttare la fiducia delle vittime,

inducendole ad interagire con contenuti dannosi sotto il falso pretesto di assistenza tecnica o risoluzione di problemi.

OilRig ha concentrato le sue operazioni su diverse organizzazioni in Israele e in altri paesi del Medio Oriente sin dalla fine del 2015. In attacchi recenti, gli attaccanti hanno istituito un falso Portale Web VPN, prendendo di mira almeno cinque fornitori IT israeliani, diverse istituzioni finanziarie e l'Ufficio Postale Israeliano.

Successivamente, gli aggressori hanno creato due siti web fake che si fingevano una pagina di registrazione a una conferenza presso l'Università di Oxford e un sito di candidature per lavoro.

Nel 2023, il gruppo ha effettuato un'intrusione prolungata di otto mesi contro un governo del Medio Oriente, estendendosi da febbraio a settembre 2023. Durante questa compromissione, gli attaccanti hanno rubato file e password e, in un caso, hanno installato una backdoor PowerShell.

Oltre al deployment di malware, gli aggressori hanno fatto ampio uso di Plink per configurare regole di port-forwarding su macchine compromesse, consentendo l'accesso remoto tramite Remote Desktop Protocol (RDP).

Operation viceleaker

Nel maggio del 2018, è emersa un'operazione di spionaggio mobile denominata "ViceLeaker" che ha preso di mira dispositivi mobili Android appartenenti a cittadini israeliani. Questo malware introduce funzionalità dannose, tra cui la registrazione delle chiamate e l'eliminazione di file senza il consenso degli utenti. Attraverso una backdoor gli attaccanti hanno la possibilità di controllare la fotocamera, registrare l'audio ambiente, effettuare chiamate o inviare messaggi a numeri specifici, e gestire l'upload e il download di file.

Un aspetto rilevante è che il principale metodo di diffusione di ViceLeaker è attraverso la distribuzione diretta di applicazioni compromesse inviate direttamente alle vittime designate tramite messaggi su Telegram o WhatsApp.

Sphinx

Conosciuta anche come APT-C-15 (Qihoo 360), riscontrata per la prima volta nel 2014, l'operazione Sphinx è un'attività di cyberspionaggio concentrata principalmente nel Medio Oriente. Le sue vittime principali includono organizzazioni politiche e militari in Paesi come Egitto e Israele. Gli aggressori dietro Sphinx mirano al furto di dati sensibili, con il periodo di massima attività compreso tra giugno 2014 e novembre 2015, sebbene alcuni timestamp dei campioni risalgano al dicembre 2011, suggerendo un possibile inizio dell'attacco prima di quanto precedentemente identificato.

Pat Bear

Dal 2015 è emerso il gruppo denominato "Pat Bear Organization", conosciuto anche come APT-C-37 (Qihoo 360) e Racquet Bear (CrowdStrike), una sottoorganizzazione dell'Syrian Electronic Army (SEA), nota anche come Deadeye Jackal. La motivazione principale di questo gruppo è il furto di informazioni e l'attività di spionaggio.

Nel corso degli anni, ha ampliato i suoi bersagli, includendo agenzie governative, forze armate, organizzazioni mediatiche, attivisti politici e diplomatici. L'attenzione principale del gruppo è contro l'Egitto, Israele e stato islamico, con l'intenzione di compromettere i loro siti web e account social, lasciando una traccia pubblica dopo aver violato la vittima.

Nel giugno 2019, APT-C-37 ha rilasciato un'app fake di WhatsApp utilizzata come strumento di spionaggio per monitorare le forze di opposizione siriane per estrarre informazioni private dai dispositivi.

Sono state notate somiglianze tra i gruppi di minacce Molerats e APT-C-37. Entrambi i gruppi si concentrano sulla regione del Medio Oriente e del Nord Africa, con particolare attenzione. La tattica di avvicinarsi alle vittime attraverso il phishing, utilizzando documenti esca in arabo legati alla situazione politica della zona, è comune a entrambi.

SCENARI FUTURI

Come oramai chiaro, dall'inizio delle ostilità, si è assistito a un'intensa attività da parte di gruppi pro-Hamas, che hanno lanciato attacchi informatici contro Israele e alcuni Paesi occidentali. Tuttavia, con l'inizio dei negoziati tra le due parti, nel periodo compreso tra la metà e la fine di novembre 2023, queste attività sembrano essere notevolmente affievolite.

Ciò suggerisce che tali gruppi agiscano in stretta sintonia con le direttive dei governi di riferimento. Inoltre, la supremazia digitale israeliana ha probabilmente contribuito a contrastare gli attacchi informatici. Prendendo in considerazione, però, quanto osservato in questo studio, possiamo notare che c'è una differenza significativa tra gli hacktivisti della prima ora - attivi soprattutto a ridosso delle stragi del 7 ottobre - e le APT qui analizzate, che potremmo paragonare alla differenza tra coscritti e forze speciali. In futuro, soprattutto con il sopraggiungere della fine della tregua tra le due parti. potremmo assistere a una maggiore presenza dei gruppi APT sul campo con un maggiore utilizzo delle loro abilità altamente specializzate.

Non è da escludere che questi gruppi, da attività di intelligence gathering, potrebbero passare a attività distruttive, come abbiamo visto nel luglio 2022, quando gruppi APT iraniani hanno agito in rappresaglia contro l'Albania di Edi Rama, andando a causare profondi danni all'infrastruttura IT di tutto il Paese. Questo conflitto tra Hamas e Israele si è combattuto e si sta tuttora combattendo anche nella quinta dimensione del cyberspazio, ingresso di player come i gruppi APT potrebbe segnalare un'altra significativa svolta

ABOUT US

Swascan è una Cyber Security Company nata da un'idea di Pierguido Iezzi e Raoul Chiesa.

La prima azienda di Cyber Security Italiana proprietaria di una piattaforma di **Cyber Security Testing e Threat Intelligence,** oltre ad un **Cyber Competence Center** premiato con numerosi riconoscimenti nazionali e internazionali dai più importanti player del mercato IT e non solo.

Da ottobre 2020, **Swascan** è parte integrante del Gruppo **Tinexta S.P.A.** azienda quotata sul segmento STAR di Borsa Italiana.

Swascan è diventata protagonista attiva del **primo polo nazionale di cyber security**: non solo una azienda, ma un gruppo italiano, un nuovo hub nazionale specializzato nei servizi di identità digitale e sicurezza digitale.

Technical Contributors:

Soc Team Swascan

Editing & Graphics:

Federico Giberti
Melissa Keysomi

Contact Info

Milano
+39 0278620700
www.swascan.com
info@swascan.com
Via Fabio Filzi, 2b, 20063, Cernusco sul Naviglio, MI