https://www.wired.it
16.03.2026

# Handala, chi sono i cybercriminali diventati il simbolo della rappresaglia digitale dell’Iran

ANDY GREENBERG - MATT BURGESS and LILY HAY NEWMAN

## Chi sono i cybercriminali iraniani di Handala
## Il gruppo è il principale attore responsabile degli attacchi informatici riconducibili alla Repubblica islamica. E dall'inizio della guerra sta decisamente alzando i giri

Da quando gli Stati Uniti e Israele hanno avviato la loro guerra contro l'Iran alla fine di febbraio, gli esperti di sicurezza informatica avvertono che la campagna di ritorsioni della Repubblica islamica avrebbe incluso pericolosi cyberattacchi contro obiettivi occidentali. Nella tarda serata del 10 marzo, la prima di queste offensive ha colpito proprio gli Stati Uniti: stando alle ricostruzioni, una violazione devastante subita dall'azienda di tecnologie mediche Stryker ha messo fuori uso decine di migliaia di computer e paralizzato

gran parte delle attività della società nel mondo. A sferrare l'attacco è stato un gruppo di criminali informatici iraniani, che si fa chiamare Handala.

"Annunciamo al mondo che, come rappresaglia per il brutale attacco alla scuola di Minab e in risposta agli assalti informatici in corso contro le infrastrutture dell'Asse della resistenza, la nostra grande operazione informatica è stata eseguita con pieno successo", si legge in una dichiarazione pubblicata sul sito web di Handala, che fa riferimento sia al missile americano Tomahawk che ha ucciso almeno 165 civili in una scuola femminile in Iran, sia alle numerose operazioni informatiche che Stati Uniti e Israele hanno portato avanti contro l'Iran. "Questo è solo l'inizio di una nuova era di guerra informatica".

# Da dove arriva e cosa vuole Handala

Finora Handala – che prende il suo nome da un noto protagonista delle vignette politiche dell'artista palestinese Naji al-Ali – non ha raccolto grande notorietà. Ma chi ne ha seguito l'evoluzione, in particolare nel settore della sicurezza informatica israeliana, sottolinea che l'opinione diffusa è che dietro il collettivo si celi il ministero dell'Intelligence iraniano, o Mois. L'organizzazione è diventata l'attore di maggior rilievo in una costellazione di operatori informatici controllati dal regime iraniano, che si presentano come hacktivisti ma cercano di colpire gli avversari in modo rumoroso e spesso per motivi politici. Negli anni, Handala, che in passato si è presentato anche con nomi diversi, ha lanciato operazioni contro bersagli che vanno dal governo albanese a imprese e funzionari politici israeliani, con l'obiettivo di distruggere dati oppure violare i sistemi delle vittime per poi pubblicarne il contenuto.

Ora che si trova ad affrontare una minaccia esistenziale, è probabile che il regime di Teheran abbia incaricato i suoi cybercriminali – e in particolare Handala – di ricorrere a ogni strumento nel proprio arsenale e a ogni punto d'appoggio all'interno delle reti occidentali per contrastare gli Stati Uniti e Israele, afferma Sergey Shykevich, responsabile dell'intelligence delle minacce

presso la società di cybersicurezza israeliana Check Point. "Hanno fatto all-in", dice. "Stanno cercando di fare tutto il possibile per portare avanti operazioni rovinose".

Nel contesto delle organizzazioni finanziate dall'Iran che hanno il compito di punire i nemici del regime con cyberattacchi d'impatto e ben visibili, Handala è cresciuta fino a diventare "probabilmente il gruppo più dominante", dice Shykevich. "Ora sono loro il volto principale".

Pur tenendo presente che i gruppi di criminali informatici sono notoriamente inclini a esagerare o “infiocchettare” i loro successi e l'impatto delle proprie azioni, Handala ha rivendicato pubblicamente di aver colpito oltre una dozzina di vittime, per lo più israeliane, dall'inizio della guerra. Il gruppo ha "combinato il rumoroso e caotico manuale d'azione di un gruppo di hacktivisti con le capacità distruttive di uno stato nazionale", afferma Justin Moore, ricercatore che si occupa di intelligence delle minacce per il gruppo Unit 42 della società di sicurezza Palo Alto Networks, e che definisce Handala il "braccio principale della cyber-ritorsione del regime iraniano".

# Strategie, obiettivi e configurazioni

Nonostante il caos che è riuscita a scatenare, le capacità strategiche di Handala non vanno sopravvalutate, afferma Rafe Pilling, direttore dell'intelligence sulle minacce di un'unità che fa parte della società di sicurezza informatica Sophos. L'impressione è che il gruppo stia cercando di guadagnare rapidamente l'accesso alle organizzazioni bersaglio e infliggere quanti più danni possibili nel bel mezzo degli attacchi aerei statunitensi e israeliani (che avrebbero colpito anche le operazioni informatiche dell'Iran). "Non ci sono i tratti distintivi di un piano", osserva Pilling a proposito della campagna avviata da Handala. "È probabile che attualmente stiano cercando obiettivi casuali da colpire in Israele o negli Stati Uniti".

I ricercatori di sicurezza hanno individuato per la prima volta Handala verso la fine del 2023, dopo gli attacchi del 7 ottobre di Hamas in Israele e i successivi bombardamenti di Gaza. Alexander Leslie, analista della società di sicurezza Recorded Future, ricorda che, quando è comparso per la prima volta, il gruppo si presentava come un collettivo “hacktivista pro-palestinese”. Il suo operato però è allineato con gli interessi del regime iraniano. Pubblicamente, Handala ha puntato molto sulla promozione delle sue attività su Telegram e X, ma gestisce anche siti web dove pubblica aggiornamenti sugli attacchi. Per aggirare i blackout di internet in Iran, ha fatto affidamento su Starlink, la connessione internet satellitare di Elon Musk, come riportato recentemente da Forbes.

Negli ultimi anni, continua Leslie, Handala ha portato a termine diversi leak, pubblicando informazioni relative a molte delle sue vittime israeliane come forma di "arma psicologica". Ma il gruppo ha anche adottato tecniche più sofisticate, come nel caso di un malware di tipo wiper usato per cancellare i file dei bersagli. Le operazioni sono state "coerenti con la più ampia preferenza di Teheran per le architetture […] che combinano la possibilità di negare ogni responsabilità e un impatto psicologico", commenta l'analista.

Check Point sostiene che in realtà Handala sia solo una delle varie manifestazioni di un unico gruppo di criminali informatici sovvenzionato dall'Iran, chiamato Void manticore. La società di sicurezza informatica è riuscita a trovare tracce del collettivo legato al Mois – che come detto è conosciuto anche con altri nomi nel settore, tra cui Red sandstorm e Cobalt mystique – già nel 2022. All'epoca, Microsoft ha attribuito all'organizzazione, che in quel periodo si faceva chiamare Homeland justice, diversi attacchi informatici che hanno preso di mira le agenzie governative albanesi con un wiper in grado di distruggerne i dati. L'offensiva era probabilmente un tentativo di intimidire il governo di Tirana, per convincerlo a non ospitare più nel paese la base dei Mojahedin del popolo iraniano, un gruppo d'opposizione.

Void manticore sembra aver creato Handala dopo gli attacchi di Hamas del 7 ottobre e la guerra di Israele a Gaza, come sottogruppo incaricato di attaccare obiettivi israeliani con il pretesto della causa pro-palestinese.

"Finché i proiettili e lo spargimento di sangue nella mia terra non si stancheranno e la ferita sarà ancora viva sulla gamba, resisteremo. #FreePalestine", si legge in una dichiarazione pubblicata sul sito dell'organizzazione.

Sempre sul proprio sito, Handala ha pubblicato anche annunci di quelle che sembravano essere operazioni di estorsione in stile ransomware e violazioni finalizzate ai leak, anche se la reale portata delle intrusioni si è spesso rivelata difficile da verificare. In alcuni casi, i cybercriminali hanno sfruttato malware modificati, mentre in altri hanno utilizzato strumenti per cancellare quanti più dati possibili dalle reti di vittime all'interno del governo israeliano e in settori della finanza, utilizzando email di phishing e falsi aggiornamenti di sicurezza per distribuire data wiper come Coolwipe, Chillwipe e Bibiwiper (dal nome del primo ministro israeliano Benjamin Netanyahu). "La combinazione formata da un fronte ransomware, un brand da hacktivisti e tattiche sponsorizzate dallo stato li rende unici", afferma Ian Gray, ricercatore della società di sicurezza Flashpoint.

Nell'ultima operazione di alto profilo prima della guerra in Iran, Handala ha violato e divulgato i tabulati telefonici privati di funzionari israeliani. Il gruppo ha dichiarato di aver bucato gli iPhone del capo dello staff di Netanyahu, Tzachi Braverman, e dell'ex primo ministro Naftali Bennett, anche se alcune analisi hanno suggerito che in realtà avessero solo preso possesso dei loro account Telegram.

Con lo scoppio della guerra, i membri di Handala potrebbero essere stati parzialmente riassegnati a un lavoro di ricognizione: Check Point ha rilevato che il gruppo è uno dei tre collettivi di cybercriminali iraniani che ha provato a sfruttare le vulnerabilità delle telecamere di sicurezza civili connesse a internet in tutto il Medio Oriente. Questi tentativi sono avvenuti in concomitanza dei bombardamenti statunitensi e israeliani nel paese e coincidono geograficamente con i contrattacchi del regime in paesi come il Bahrein, gli Emirati Arabi Uniti, Israele e Cipro. Quest'ultimo aspetto suggerisce che le telecamere manomesse fossero destinate a un'attività di sorveglianza prima delle operazioni militari e, forse, all'individuazione degli obiettivi di attacchi con missili e droni.

Ma quella contro Stryker potrebbe comunque rappresentare l'azione di maggiore impatto messa a segno fin qui dal gruppo, anche a fronte delle attuali difficoltà dell'azienda nel tornare alla normale attività. Handala ha affermato di aver attaccato la società medica per via dei suoi legami con attori “sionisti” (nel 2019 Stryker ha acquisito l'azienda israeliana Orthospace e l'anno scorso ha siglato un contratto militare da 450 milioni di dollari con gli Stati Uniti, come riportato da Bloomberg). Stryker non ha risposto immediatamente a una richiesta di commento di Wired.

Mentre la guerra in Iran sembra destinata a prolungarsi, sembra che Handala stia cercando di sfruttare ogni opportunità per seminare il maggior caos possibile. I

suoi messaggi pubblici spesso contengono un “severo avvertimento”, o preannunciano notizie che "scuoteranno il mondo cyber".

Per quanto affermazioni di questo tipo si siano talvolta rivelate esagerate, la natura un po' casuale degli attacchi di Handala non è di grande conforto per vittime come Stryker. Come si legge in uno dei post del gruppo: "Il gioco è nelle nostre mani".

Questo articolo è apparso originariamente su Wired US.