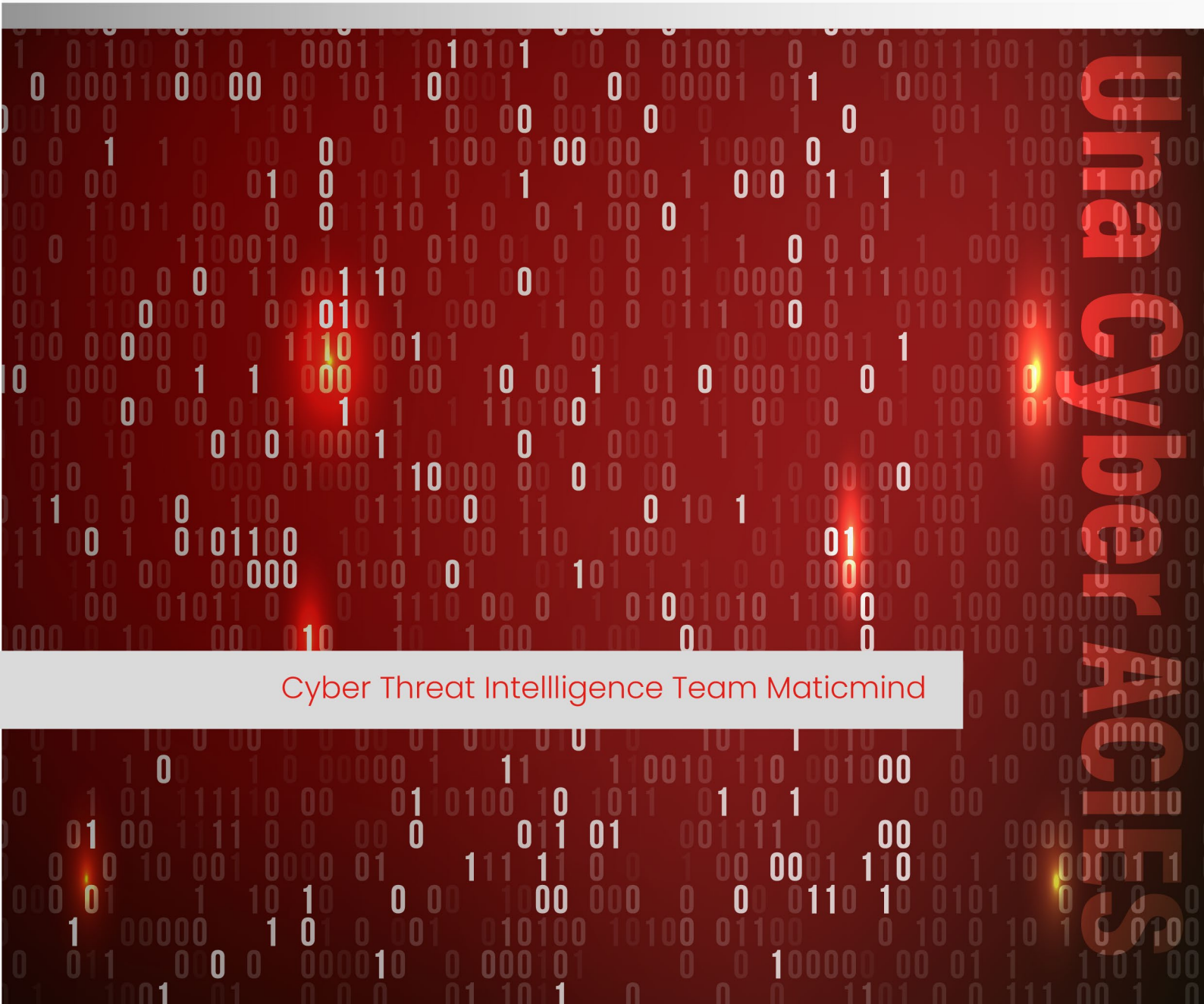
MATICMIND®
MAKES IT EASY

SCHEDA THREAT ACTOR

PREDATORY SPARROW

www.maticmind.it



Cyber Threat Intellligence Team Maticmind

Sommario

INTRODUZIONE

Il 17 giugno 2025 un attacco informatico ha paralizzato **Bank Sepah**, una delle principali istituzioni finanziarie dell'Iran.

L'attacco è stato rivendicato dal gruppo **Predatory Sparrow**, già noto per le sue operazioni distruttive contro infrastrutture critiche iraniane.

Nel presente documento vi è un'analisi approfondita del Threat Actor Predatory Sparrow, delle sue capacità tecniche e degli obiettivi dichiarati, con particolare attenzione al contesto geopolitico e all'uso di malware proprietari.

SCHEDA THREAT ACTOR: PREDATORY SPARROW

INFORMAZIONI GENERALI

Nome Principale: Predatory Sparrow

Nomi Alternativi: - Gonjeshke Darande (گنجشک درنده - traduzione in farsi) – Indra (overlap parziale, similitudini nel codice dei malware utilizzati)

Classificazione: Gruppo hacktivist pro-israeliano
Primo Avvistamento: 2021

Stato Attuale: Attivo (ultima attività documentata: giugno 2025)

IDENTITÀ E AFFILIAZIONI

Natura del Gruppo

Predatory Sparrow si presenta come un gruppo di hacktivisti autoproclamato, ma la sua sofisticazione tecnica e le capacità operative suggeriscono un probabile coinvolgimento governativo o militare. Secondo un articolo di WIRED, fonti della difesa statunitense hanno riferito al New York Times che il gruppo era collegato a Israele.

Il gruppo, nato nel 2021, è entrato in stato di quiescenza tra il 2022 e l'ottobre 2023, tornando operativo all'avvio delle ostilità nella striscia di Gaza.

Diamond Model

Avversario	Predatory Sparrow/Gonjeshke Darande
Vittima	Entità affiliate al regime iraniano degli Ayatollah
Infrastruttura	N/A
Capacità	Wiper e malware avanzati atti a compromettere sistemi industriali, distruzione fisica di apparati industriali, cancellazione massiva di dati, blocco delle operazioni di infrastrutture e telecomunicazioni

Motivazioni e Obiettivi

- **Obiettivo Primario:** Condurre attacchi distruttivi contro l'Iran, allo scopo di infliggere danni paragonabili a quelli di attacchi convenzionali, con effetti nella sfera psicologica, per indebolire la fiducia della popolazione nel regime degli Ayatollah e la tenuta di questo, in un quadro di operazioni PSYOPS, campagne di disinformazione e azioni di sabotaggio, causando al contempo conseguenze economiche significative alle aziende iraniane connesse con il governo o con l'esercito.
- **Motivazione Geopolitica:** Si inserisce all'interno del confronto tra Israele, Iran e i proxy di quest'ultimo, allo scopo di rispondere agli attacchi condotti dalla Repubblica islamica direttamente o tramite proxy.

- **Valenza strategica:** affermare la capacità offensiva dell'attore nel colpire asset industriali e digitali critici in territorio iraniano, con l'obiettivo di esercitare pressione e destabilizzazione mirata.
- **Tattiche di rivendicazione e propaganda:**
  - Utilizza canali X e Telegram per rivendicare gli attacchi
  - Pubblica video come prova degli attacchi riusciti, come nel caso del video dell'attacco distruttivo all'acciaieria iraniana
  - Include messaggi provocatori con riferimenti al Leader Supremo Iraniano
  - Si presenta talvolta come gruppo hacktivisti Iraniano per confondere l'attribuzione
  - Apparentemente, il gruppo conduce attacchi con il criterio dichiarato di non mettere a repentaglio vite innocenti (come riportato sul canale Telegram del TA e riportato da BBC)

CAPACITÀ TECNICHE

Livello di Sofisticazione

Il gruppo dimostra capacità tecniche avanzate che lasciano intendere l'accesso a risorse significative, una conoscenza approfondita dei sistemi industriali iraniani, nonché la capacità di sviluppare malware su misura per obiettivi specifici. Inoltre, evidenzia competenze rilevanti nei sistemi SCADA e ICS (Industrial Control Systems), utilizzati nel controllo di infrastrutture critiche. Rispetto alla maggior parte degli hacktivisti che intervengono su tematiche geopolitiche o di attualità, Predatory Sparrow si distingue per un know-how tecnico notevolmente superiore, che risulta tipico di attori collegati ad apparati statuali.

Settori di Specializzazione

1. **Sistemi di Controllo Industriale (ICS/SCADA)**
    - Capacità di manipolare equipaggiamento industriale
    - Accesso a sistemi di controllo di acciaierie e pompe di benzina
    - Interferenza con sistemi ferroviari
2. **Sistemi di Pagamento**
    - Compromissione di reti point-of-sale
    - Attacchi a sistemi di carte di sussidio carburante
    - Compromissione di Crypto Exchange
    - Compromissione di enti finanziari
3. **Infrastrutture Critiche**
    - Sistemi ferroviari nazionali
    - Reti di distribuzione carburante
    - Impianti siderurgici

TOOLSET E MALWARE

Sulla base delle informazioni attualmente disponibili, si ritiene che il gruppo sia in possesso di varianti del wiper “Meteor”, comparso per la prima volta nel 2021 e utilizzato da un threat actor denominato “Indra” contro infrastrutture siriane. Questo fattore potrebbe indicare una parziale sovrapposizione tra i due threat actor.

Lo strain di “Meteor” comprende diverse versioni, note come “Stardust” e “Comet”, sempre con funzionalità di wiper. “Chaplin” risulta invece essere il malware utilizzato nell’attacco alle acciaierie iraniane, non dotato di capacità di cancellazione dei dati ma di compromissione e controllo dei sistemi industriali.

Meteor Express (2021)

Descrizione tecnica

Meteor Express è un malware di tipo wiper a tre stadi, sviluppato tramite una combinazione di componenti open source e software legacy. Il codice è altamente modulare e progettato per operazioni distruttive mirate a infrastrutture strategiche.

Funzionalità principali

1. Sovrascrittura e cancellazione di file di sistema.
2. Blocco dell’accesso utente e terminazione dei processi.
3. Cancellazione del Master Boot Record (MBR).
4. Disabilitazione delle interfacce di rete.
5. Cambio delle password per tutti gli utenti
6. Log off delle sessioni attive
7. Disabilitazione della recovery mode

Kill Chain

Reconnaissance: Presunta fase iniziale di raccolta informazioni tramite accessi precedenti alla rete target.

Weaponization: Uso di componenti dropper e script batch per il rilascio dei payload.

Delivery: Infezione attraverso accesso fisico/logico alle macchine o vulnerabilità RDP.

Installation: Scrittura su disco di tool e script batch eseguiti in sequenza.

- **Command and Control:** Non presente in quanto malware *non persistente* e *senza C2 attivo*.
- **Actions on Objectives**: Distruzione dei dati, blocco degli account, sabotaggio del sistema operativo.

Tecniche MITRE ATT&CK correlate

- T1490 – Inhibit System Recovery
- T1485 – Data Destruction
- T1562.001 – Impair Defenses: Disable or Modify Tools
- T1489 – Service Stop
- T1491.001 – Defacement: Internal Defacement
- T.1531 – Account Access Removal

Contesto operativo

Attacco lanciato nel luglio 2021 contro la rete ferroviaria iraniana. L'obiettivo apparente era la destabilizzazione dell'infrastruttura pubblica e la generazione di caos operativo su larga scala.

Attribuzione

Malware attribuito al gruppo Indra.

Valutazione di impatto

- **Tecnico:** Paralisi totale del sistema informatico ferroviario, con disservizi prolungati e blocchi operativi.
- **Psicologico:** Tentativo di disorientare l'opinione pubblica iraniana attraverso il sabotaggio simbolico.
- **Obiettivo operativo:** Operazione PSYOPS volta a delegittimare il governo iraniano e dimostrare la vulnerabilità delle infrastrutture pubbliche strategiche.

Indicatori di Compromissione (IoCs)

Directory di staging: %temp%\Meteor\

Comet (2021)

Descrizione tecnica:

Malware *wiper* simile a Meteor ma privo di payload provocatori. Architettura a tre stadi, con codice misto tra componenti open e legacy.

Funzionalità principali

- Cancellazione file.
- Blocco utente e sistema.
- Disattivazione strumenti di logging.

Kill Chain

- **Delivery:** Script locali o remotizzati.
- **Execution:** Blocco e visualizzazione contenuti.
- **Impact**: Interruzione della normale operatività utente.

Tecniche MITRE ATT&CK correlate

- T1490 – Inhibit System Recovery
- T1485 – Data Destruction
- T1562.001 – Impair Defenses: Disable or Modify Tools
- T1489 – Service Stop
- T1491.001 – Defacement: Internal Defacement
- T.1531 – Account Access Removal

Contesto operativo

Uso in attacchi silenziosi contro infrastrutture critiche.

Attribuzione

Malware attribuito al gruppo Indra.

Valutazione di impatto

- **Tecnico:** Elevato.
- **Psicologico:** Consistente, in quanto crea disservizio e mina la fiducia nelle infrastrutture statali
- **Obiettivo operativo:** Sabotaggio silenzioso e persistente.

Stardust (2020)

Descrizione tecnica:

Wiper distruttivo impiegato in attacchi mirati contro obiettivi siriani. Simile a Comet, ma specificamente orientato alla distruzione sistematica dei dati sensibili.

Funzionalità principali

- Sovrascrittura file sensibili.
- Interruzione del sistema.
- Blocco del boot.

Kill Chain

- **Delivery:** Tramite accesso ai sistemi vulnerabili.
- **Execution:** Esecuzione del wiper su endpoint.
- **Impact:** Eliminazione dei dati sensibili e blocco operativo.

Tecniche MITRE ATT&CK correlate

- T1485 – Data Destruction
- T1490 – System Recovery Inhibition
- T1499 – DoS

Contesto operativo

Attacchi contro aziende siriane strategiche, senza elementi rivendicativi.

Attribuzione

Malware attribuito al gruppo Indra.

Valutazione di impatto

- **Tecnico:** Critico, distruzione completa dei dati.
- **Psicologico:** Contenuto, in quanto assente la componente narrativa.
- **Obiettivo operativo:** Danneggiamento economico e operativo.

Chaplin (2022)

Descrizione tecnica

Evoluzione del malware Meteor, classificabile come *disruptive malware*. Manca la componente *wiper*, ma introduce azioni visivamente provocatorie.

Funzionalità principali

1. Disconnessione dalla rete.
2. Logout forzato dell'utente.
3. Blocco dello schermo.
4. Visualizzazione messaggi provocatori.4

Kill Chain

- **Delivery:** Script locali o remoti.
- **Execution:** Blocco e visualizzazione contenuti.
- **Impact:** Interruzione della normale operatività utente. Comandi inviati ai sistemi industriali che ne causano il malfunzionamento

Tecniche MITRE ATT&CK correlate

- T1531 – Account Access Removal
- T1499 – Endpoint Denial of Service
- T1551 – Input Capture (blocco schermo)

Contesto operativo

Probabilmente impiegato in attacchi dimostrativi o a basso impatto distruttivo.

Attribution

Non nota, ma verosimilmente collegata agli stessi attori di Meteor.

Valutazione di impatto

- **Tecnico:** Limitato ma visibile.
- **Psicologico:** Elevato, per via dei messaggi diretti (es. invito a chiamare l'ufficio del Leader Supremo iraniano).
- **Obiettivo operativo:** Guerra psicologica, dimostrazione di capacità.

Timeline degli Attacchi Principali

Attacco alle Stazioni di Servizio

Data: Ottobre 2021

Obiettivo: Oltre 4.000 stazioni di servizio in Iran (sistema di distribuzione carburante)

Metodo d'attacco: Compromissione dei sistemi point-of-sale

Impatto:

- Disattivazione del sistema di pagamento con carte sovvenzionate
- Paralisi temporanea della distribuzione di carburante su scala nazionale

MITRE ATT&CK TTPs:

- T1190 (Exploit Public-Facing Application)
- T1486 (Data Encrypted for Impact)

Malware/Toolset: Non noto

Attribution: Predatory Sparrow

Impatto Strategico: Interruzione dei servizi essenziali per aumentare la pressione interna

Attacco alle Acciaierie Iraniane

Data: Giugno 2022

Obiettivo: Tre principali acciaierie iraniane (Khouzestan, Mobarakeh, HOSCO)

Metodo d'attacco: Malware Chaplin + manipolazione dei sistemi di controllo industriale (ICS)

Impatto:

- Fuoriuscita di acciaio fuso (oltre 1.300°C)
- Incendio nell'impianto
- Interruzione delle operazioni produttive

MITRE ATT&CK TTPs:

- T0859 (Manipulation of Control)
- T0882 (Loss of Safety)
- T0814 (Alarm Suppression)

Malware/Toolset: Chaplin

Attribution: Predatory Sparrow

Impatto Strategico: Danneggiamento delle capacità industriali critiche e dimostrazione di capacità offensive contro ICS

Figura 1 - Telecamera sorveglianza

Riattivazione - Conflitto Gaza-Israele

Data: Ottobre 2023

Contesto: Conflitto israelo-palestinese

Messaggio: "Pensate che questo faccia paura? Siamo tornati."

Obiettivo: Nuovi attacchi a stazioni di servizio in Iran

Metodo d'attacco: Continuazione della strategia disruption verso infrastrutture civili

Impatto: Non specificato nel dettaglio ma coerente con attacchi precedenti

MITRE ATT&CK TTPs: presumibilmente analoghi all'evento di Ottobre 2021

Attribution: Predatory Sparrow

Impatto Strategico: Segnale politico e ritorsione cibernetica in chiave geopolitica

Attacco Bank Sepah

Data: 17 giugno 2025

Obiettivo: Bank Sepah – uno degli istituti finanziari pubblici più antichi dell'Iran

Metodo d'attacco: Attacchi informatici distruttivi con probabile uso di wiper (es. Comet/Stardust)

Impatto:

- Interruzione delle operazioni bancarie
- Impossibilità per i cittadini di prelevare denaro dagli sportelli ATM
- Diffusione di CVE pubblici da parte dell'attore (es. cve_poc_codes_export_works.csv)

MITRE ATT&CK TTPs:

- T1485 (Data Destruction)
- T1499 (Endpoint Denial of Service)
- T1588.006 (Vulnerability Disclosure)

Malware/Toolset: Presunta variante wiper simile a Meteor / Comet / Stardust

Attribution: Predatory Sparrow (evidenza su Telegram + X)

Impatto Strategico: Destabilizzazione del sistema bancario nazionale e perdita di fiducia nella capacità del governo iraniano di proteggere dati finanziari

Al momento non si conoscono dettagli sulle tecniche, tattiche e procedure (TTP) utilizzate dal threat actor, benché la cancellazione dei dati con conseguente paralisi delle operazioni faccia propendere per l'ipotesi dell'impiego di una versione dei wiper "proprietari" del gruppo, come Meteor, Stardust o Comet. Nella giornata del 16/06, sul proprio canale Telegram il gruppo aveva diffuso una lista di cve ancora funzionati, dal titolo "cve_poc_codes_export_works".

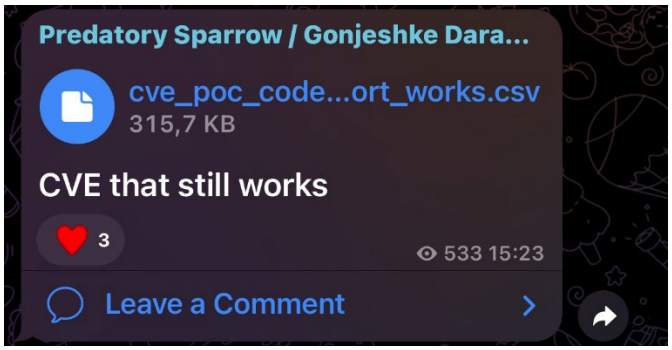


Figura 2 - Cve diffusa su canale Telegram del TA

Secondo fonti presenti su X, i cittadini iraniani erano impossibilitati a prelevare denaro contante dagli ATM del Paese.

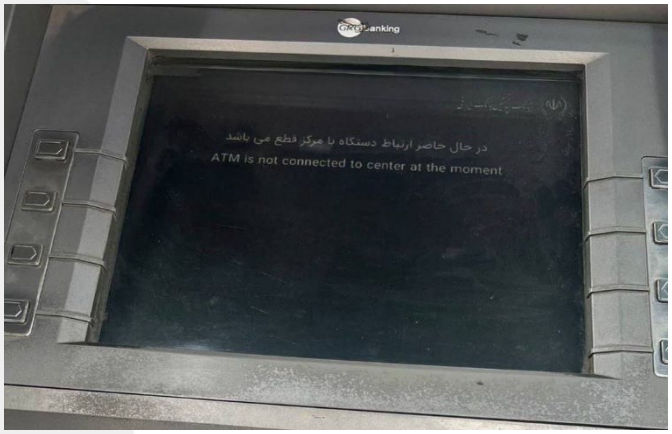


Figura 3 - Sportello banca in disservizio

Tale fattore, unito ai timori relativi al furto di dati sensibili dalle banche colpite, contribuisce all'aggravamento dello scenario e sottolinea le capacità da cyberwar in possesso del Threat Actor.

Figura 4 - Documentazione Bank Sepah

A differenza di molti hacktivisti, infatti, Predatory Sparrow non si è limitato ad un Denial of Service (DoS), ma ha mostrato capacità tecnologiche avanzate e determinazione nel procurare danni su vasta scala.

Al momento non si hanno informazioni ulteriori sullo stato dei servizi erogati dalle banche colpite ma, nel caso in cui tali disservizi dovessero protrarsi, ciò rappresenterebbe un danno considerevole alla capacità dell'Iran di rispondere alle minacce cibernetiche e potrebbe contribuire a generare malcontento e tensioni tra la popolazione colpita.

Attacco Nobitex

Data: 18 giugno 2025

Obiettivo: Nobitex – sito iraniano di crypto exchange

Metodo d'attacco: Al momento non si hanno informazioni inerenti alla metodologia di attacco utilizzata

Impatto:

- Distruzione asset crypto per un totale di 90 milioni di dollari
- Sito nobitex[.].ir ancora offline a 24h dall'attacco

MITRE ATT&CK TTPs:

- T1485 (Data Destruction)
- T1499 (Endpoint Denial of Service)
- T1588.006 (Vulnerability Disclosure)

Malware/Toolset: Presunta variante wiper simile a Meteor / Comet / Stardust

Attribution: Predatory Sparrow

Impatto Strategico: Destabilizzazione del sistema valutario di crypto exchange iraniano. Recisione di una linea di finanziamento che permetteva all'Iran di aggirare, parzialmente, le sanzioni occidentali. Effetti psicologici come la diffusione di panico e incertezza riguardo la resilienza degli asset iraniani nel cyberspazio.

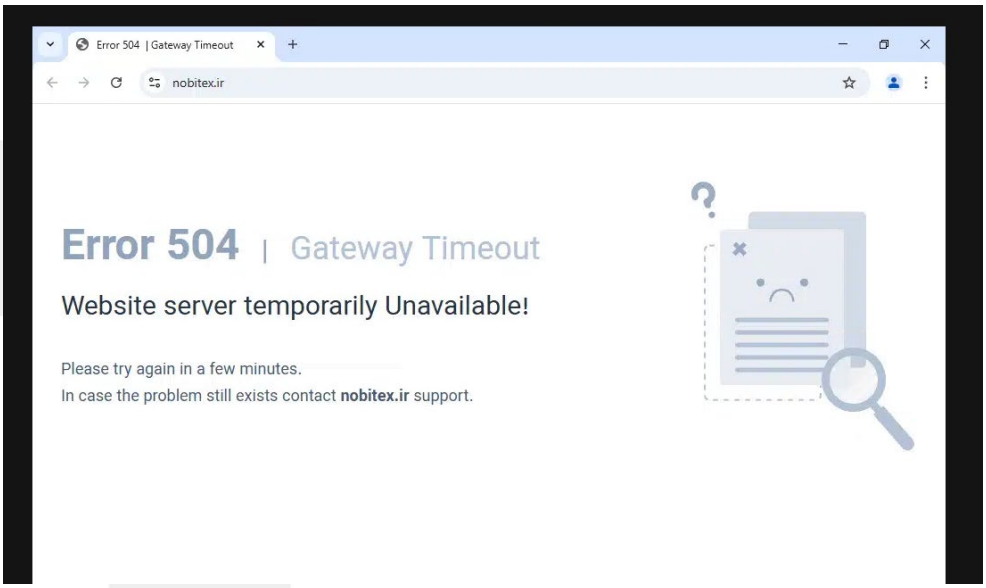


Figura 5 - Nobitex[.]ir ancora irraggiungibile nella giornata del 19/06, a un giorno dall'attacco

Predatory Sparrow ha attaccato il sito di exchange di criptovalute iraniano "Nobitex" nella giornata del 18 giugno, soltanto un giorno dopo l'attacco a Sepah Bank. La motivazione dichiarata è la medesima, ovvero l'evasione delle sanzioni imposte all'Iran e il finanziamento del terrorismo. Su X, Predatory Sparrow ha anche sottolineato il nesso tra le attività del regime e quelle di Nobitex, dichiarando che, per il governo iraniano, il servizio presso l'exchange di criptovalute è considerato alla stregua del servizio militare.

Il Threat Actor non ha sottratto le criptovalute, ma ne ha di fatto bruciato un ammontare pari a 90 milioni di dollari, inviandole verso indirizzi inutilizzabili ("burn addresses"), da cui non possono essere recuperate. La tecnica adoperata sottolinea l'obiettivo di Predatory Sparrow di arrecare danno senza alcuna finalità di monetizzazione o finanziamento, come sotteso anche dal ricorso ai wiper.

In data 20/06/2025 threat actor ha inoltre reso pubblico il source code di Nobitex, mettendo a rischio gli asset ancora presenti sul sito e rendendo più facile l'accesso e l'exploit da parte di ulteriori attori malevoli. Questa divulgazione del codice sorgente amplifica la vulnerabilità del sistema, consentendo agli aggressori di identificare rapidamente punti deboli e sviluppare exploit mirati.

Figura 6 - Post con cui Predatory Sparrow rende pubblico il codice sorgente di Nobitex, https://x.com/GonjeshkeDarand/status/1935593397156270534

Al momento non si hanno ulteriori dettagli sulle tecniche, tattiche e procedure (TTP) utilizzate dal threat actor in questa operazione.

VALUTAZIONE DEL RISCHIO

Livello di Minaccia: ALTO

Determinanti di minaccia: Capacità dimostrate di causare danni fisici - Accesso persistente a infrastrutture critiche - Sofisticazione tecnica in crescita - Motivazione geopolitica forte

Settori a Rischio: Infrastrutture energetiche - Sistemi di trasporto - Industria pesante - Sistemi di pagamento - Settore bancario e finanziario

Indicatori di Compromissione (IoC)

- Presenza di file denominati “Chaplin”
- Messaggi di sistema con riferimenti al numero 64411
- Disconnessioni anomale dalla rete
- Malfunzionamenti di sistemi industriali coordinati
- Indirizzi wallet crypto recanti messaggi diretti contro le Guardie della repubblica islamica (Islamic Republic Guard Corps IRGC) del tipo "F*ckIRGCterrorists”

CONTROMISURE RACCOMANDATE

Sulla base delle evidenze presentate all’interno del report, si formulano alcune raccomandazioni e contromisure utili a minimizzare o contenere danni provenienti dall’attore qui descritto o da eventuali gruppi emulatori.

Considerata la mancanza di informazioni dettagliate sulle compromissioni, a fronte della mancata disclosure da parte degli enti iraniani colpiti, si presentano qui alcune considerazioni generali atte a ridurre l’impatto dei malware tipo “wiper” come Meteor e di altri tool utilizzati in contesti di cyber warfare e cyber-espionage come InfoStealer e SpyWare. Inoltre, considerando la presenza di un elenco di CVE con i relativi link alle Proof of Concept pubblicate direttamente dal Threat Actor sul proprio canale Telegram, dove viene evidenziato che si tratta di exploit ancora funzionanti, si può ipotizzare che Predatory Sparrow utilizzi anche applicazioni esposte e vulnerabili come vettore di accesso iniziale, verranno pertanto suggerite delle raccomandazioni per proteggere la superficie di attacco esposta.

Al fine di contenere la propagazione di un wiper all’interno della rete, è opportuno adattare una segmentazione rigida, che separi reti OT da IT, anche attraverso il ricorso ad architetture Zero Trust e stretto controllo degli accessi.

Al tempo stesso, il backup separato, air-gapped, associato a piani di ripristino e disaster recovery, consente il recupero della normale operatività in caso di compromissione.

Il patching, la chiusura delle porte superflue esposte su internet e la disabilitazione dei servizi non necessari sono altresì misure utili a ridurre la superficie di attacco e a minimizzare il rischio derivante dalle applicazioni esposte.

Honeypot ICS/SCADA consentono inoltre di rilevare anomalie e intrusioni prima che attori malevoli raggiungano le aree critiche per l'operatività industriale.

Minaccia o vettore	Contromisura chiave	Impatto atteso
Meteor malware (strain)	Isolamento delle reti OT, presenza di EDR, backup immutabili conservati offline	Riduzione rischio sabotaggio, contenimento dell'infezione, ripristino in caso di attacco
C2 communication	Firewalling e deep packet inspection	Interruzione delle comunicazioni col C2
Social Engineering	Formazione del personale, cultura di awareness e cyber hygiene	Riduzione del rischio connesso al phishing
Exploit Public-Facing Application	Patch management, configurazione sicura, least privilege policy, implementazione WAF, disabilitazione servizi non necessari,	Riduzione della superficie d'attacco, riduzione delle vulnerabilità sfruttabili, riduzione del rischio di accessi non autorizzati.
InfoStealer, SpyWare, cyber espionage tools	EDR, Segmentazione della rete, Patching delle vulnerabilità, Politiche di controllo accessi, crittografia dei dati, DLP, Deployment di honeypot di deception	Riduzione del rischio di esfiltrazione di dati sensibili

Autori:

Cyber Defence Center Maticmind

Cyber Competence Center Maticmind

Andrea Mariucci - *Head of Cyber Defence Center Maticmind*

Riccardo Michetti - *Cyber Threat Intelligence Manager Maticmind*

Federico Savastano - *Cyber Threat Intelligence Analyst Maticmind*

Ada Spinelli - *Cyber Threat Intelligence Analyst Maticmind*

Ultimo Aggiornamento: 20 giugno 2025

Referenze

Fonti Primarie e Database

Malpedia Threat Actor Database: https://malpedia.caad.fkie.fraunhofer.de/actor/predatory_sparrow

Articoli di Analisi e Reportage

- **Jason Institute** https://jasoninstitute.com/predatory-sparrow-when-angry-birds-attack/
- **Wired Magazine** (2024-01-25): “How a Group of Israel-Linked Hackers Has Pushed the Limits of Cyberwar” - https://www.wired.com/story/predatory-sparrow-cyberattack-timeline/
- **Heimdal Security** (2021): “MeteorExpress Wiper Responsible for the Iranian Railway Attack” https://heimdalsecurity.com/blog/meteorexpress-wiper-responsible-for-the-iranian-railway-attack/
- **Dark Reading** (2023-10-10): “Pro-Israeli Hacktivist Group ‘Predatory Sparrow’ Reappears” - https://www.darkreading.com/threat-intelligence/pro-israeli-hacktivist-group-predatory-sparrow-reappears
- **BBC Technology** (2022-07-11): “Predatory Sparrow: Who are the hackers who say they started a fire in Iran?” - https://www.bbc.com/news/technology-62072480
- **Risky Biz News** (2022-06-29): “Hackers hit Iranian steel industry” - https://riskybiznews.substack.com/p/risky-biz-news-hackers-hit-iranian
- **Reuters:** https://www.reuters.com/business/finance/exclusive-crypto-exchange-binance-helped-iranian-firms-trade-8-billion-despite-2022-11-04/
- **Binding Hook** (2024-12-09): https://bindinghook.com/articles-binding-edge/predatory-sparrow-cyber-sabotage-with-a-conscience/
- **IranInternational:** https://www.iranintl.com/en/202506176243
- **Check Point Research**: https://research.checkpoint.com/2021/indra-hackers-behind-recent-attacks-on-iran/
- **CyberScoop** (2023-10-10): “Savvy Israel-linked hacking group reemerges amid Gaza” - https://cyberscoop.com/predatory-sparrow-israel-gaza-cyber/
- **SecureWorld** (2022-06-29): “Cyberattack on Iranian Steel Industry Disrupts Operations” - https://www.secureworld.io/industry-news/cyberattack-iran-steel-industry
- **ANSA** (2025-06-17): “Banca pubblica iraniana paralizzata da cyber attacco” - https://www.ansa.it/canale_tecnologia/notizie/cybersecurity/2025/06/17/banca-pubblica-iraniana-paralizzata-da-cyber-attacco_55c8b39d-27d0-4cc2-86d9-4f88b6c7e601.html
- **The Record** (2025): “Pro-Israel hackers claim breach of Iranian bank amid…” - https://therecord.media/pro-israel-hackers-claim-attack-on-iranian-bank

- **Security Affairs** (2024): “Pro-Israel Predatory Sparrow hacker group disrupted…” - https://securityaffairs.com/156065/hacktivism/pro-israel-predatory-sparrow-iran-fuel-stations.html
- https://www.bleepingcomputer.com/news/security/pro-israel-hackers-hit-irans-nobitex-exchange-burn-90m-in-crypto/
- **El País** (2024-02-14): “Predatory Sparrow and other weapons of hybrid warfare” - https://english.elpais.com/technology/2024-02-14/predatory-sparrow-and-other-weapons-of-hybrid-warfare-cheap-fast-undetectable-and-effective.html
- **Haaretz** (2023-12-26): “When Predatory Sparrow Strikes: Israel-Iran Shadow War…” - https://www.haaretz.com/israel-news/security-aviation/2023-12-26/ty-article-magazine/.premium/when-predatory-sparrow-strikes-israel-iran-shadow-war-awakens/0000018c-a524-df1f-a7bf-b7e59ba00000
- **The Independent** (19/06/25) “Pro-Israel hackers ‘burn’ $100m from Iran’s biggest crypto exchange” https://www.independent.co.uk/tech/iran-crypto-exchange-hack-nobitex-israel-b2773027.html

Fonti Accademiche e Istituzionali

- **NATO CCD COE Cyber Law (2022):** “Predatory Sparrow operation against Iranian steel maker” - https://cyberlaw.ccdcoe.org/wiki/Predatory_Sparrow_operation_against_Iranian_steel_maker_(2022)

Social media e app di messaggistica

- **Telegram e X:** canali del Threat Actor
  X: https://x.com/GonjeshkeDarand
  Telegram: https://t.me/gonjeshkdarand