In aumento i cyberattacchi dall’Iran: l’allarme delle agenzie di sicurezza americane

Maria Cattini | 03/07/2025 | Sicurezza digitale

□□ Nuova ondata di attacchi informatici dall’Iran: il pericolo si avvicina

Un documento congiunto rilasciato da quattro importanti agenzie statunitensi – CISA, NSA, FBI e DC3 – mette nero su bianco un timore crescente: i cyberattacchi provenienti dall’Iran sono in aumento e potrebbero intensificarsi nelle prossime settimane. Una dichiarazione che suona come un vero e proprio campanello d’allarme.

“Negli ultimi mesi – si legge nell’avviso – abbiamo registrato un incremento delle attività da parte di gruppi affiliati al governo iraniano e a collettivi hacktivisti, che potrebbero proseguire e aggravarsi in conseguenza degli eventi geopolitici recenti”.

□□ Chi è nel mirino degli attacchi iraniani?

Secondo le analisi delle agenzie statunitensi, i bersagli più esposti sono:

• Enti e aziende con legami economici o tecnologici con Israele
• Infrastrutture critiche (energia, sanità, trasporti)
• Settori pubblici e privati con sistemi di sicurezza obsoleti

Ma l’elemento più preoccupante è che, sebbene non ci siano ancora prove di attacchi diretti agli Stati Uniti, le agenzie ritengono “molto probabile” che ciò accada a breve.

□□ Le tattiche già in atto: defacement, leak e DDoS

I gruppi legati all’Iran hanno intensificato le azioni di:

• Defacement: modifiche fraudolente delle homepage di siti web
• Furto e diffusione di dati sensibili (leak mirati)
• Attacchi DDoS, per bloccare l’accesso a portali strategici

La dinamica è semplice quanto efficace: si penetra in siti poco protetti, si sottraggono dati o si oscurano contenuti, e si pubblicizza l’azione per ottenere visibilità e fare pressione politica o ideologica.

> □□**Curiosità**: il “defacement” è spesso accompagnato da messaggi propagandistici o simbolici – un attacco non solo digitale, ma anche comunicativo.

□□ Collaborazioni pericolose: rischio ransomware in aumento

Non finisce qui. Le agenzie temono una nuova fase degli attacchi: la **collaborazione con gruppi cybercriminali non statali**, al fine di lanciare campagne di **ransomware**. In pratica: infettare sistemi, bloccarli e chiedere riscatti.

Un'alleanza tattica, tra ideologia e criminalità, che potrebbe moltiplicare l'efficacia degli attacchi e confondere le attribuzioni.

□□ Il precedente del 2023: PLC israeliani nel mirino

Il rapporto congiunto richiama un episodio emblematico del 2023: l'attacco condotto dal Corpo delle Guardie della Rivoluzione Islamica, che ha compromesso PLC israeliani (controller logici programmabili) usati da organizzazioni statunitensi. L'obiettivo? Colpire infrastrutture critiche. Un'operazione sofisticata e, soprattutto, riuscita.

In parallelo, numerose operazioni "hack-and-leak" hanno preso di mira aziende e istituzioni israeliane, con la pubblicazione di documenti sensibili per danneggiarne l'immagine o il business.

□□ Le contromisure consigliate dalle agenzie USA

Le raccomandazioni contenute nel report sono chiare e operative. Nessun tecnicismo inutile: solo ciò che serve davvero per prevenire un disastro informatico.

□□ 1. Aggiorna subito tutto

Molti attacchi sfruttano **vulnerabilità note** in software non aggiornati. Il consiglio è semplice: installare **sempre l'ultima versione** disponibile di ogni applicazione.

□□ 2. Disconnetti i sistemi di automazione dalla rete pubblica

I sistemi industriali non dovrebbero essere esposti su internet. Il rischio è che un accesso remoto consenta il controllo diretto di macchinari o impianti critici.

□□ 3. Dì addio alle password di default

Un errore ancora troppo diffuso: lasciare le **password predefinite**. I criminali le conoscono, le testano in automatico e penetrano facilmente nei sistemi. Serve:

• Cambiarle subito
• Renderle robuste
• Attivare l'autenticazione a più fattori

□□ Quali sono i settori più a rischio?

Oltre alle collaborazioni con Israele, risultano particolarmente vulnerabili:

Settore	Rischio Stimato	Tipologia di Attacco
Energia	Alto	Ransomware, sabotage PLC
Sanità	Alto	Furto dati sensibili, DDoS
Logistica e trasporti	Medio-Alto	DDoS, blocco sistemi operativi
Pubblica amministrazione	Medio	Defacement, attacchi simbolici

□□ Perché l'Iran? Perché adesso?

Le tensioni geopolitiche in Medio Oriente, sommate al supporto occidentale a Israele, hanno spinto

Teheran a investire maggiormente in strumenti di cyberwarfare. Rispetto agli attacchi cinetici, quelli digitali:

• Costano meno
• Sono difficilmente attribuibili
• Possono causare danni reali (economici, sociali, reputazionali)

Ecco perché il rischio è destinato ad aumentare, non solo per gli USA, ma per tutti gli Stati percepiti come “alleati” israeliani.

□□ Cosa fare adesso? Le 5 mosse immediate

1. Mappare le vulnerabilità: verifica se i tuoi sistemi sono esposti su internet.
2. Formare il personale: chi clicca su un link malevolo apre la porta all’attacco.
3. Implementare backup off-line: per recuperare dati anche in caso di ransomware.
4. Monitorare i log di sistema: segui le anomalie e segnala comportamenti sospetti.
5. Usare VPN e MFA: cifrare le connessioni e proteggere gli accessi è oggi essenziale.

□□ Una minaccia silenziosa, ma concreta

Il cyberconflitto tra Iran, Israele e Stati Uniti non è un’ipotesi, ma una realtà in evoluzione. Le aziende – anche quelle piccole – non possono più permettersi di ignorare questo scenario.

Le agenzie di sicurezza americane non lanciano allarmi a vuoto: chi si muove in tempo può evitare i danni peggiori. Chi resta indietro, rischia di finire nel mirino.

□□Hai aggiornato i tuoi sistemi?

□□ Nuova ondata di attacchi informatici dall’Iran: il pericolo si avvicina

Un documento congiunto rilasciato da quattro importanti agenzie statunitensi – CISA, NSA, FBI e DC3 – mette nero su bianco un timore crescente: i cyberattacchi provenienti dall’Iran sono in aumento e potrebbero intensificarsi nelle prossime settimane. Una dichiarazione che suona come un vero e proprio campanello d’allarme.

“Negli ultimi mesi – si legge nell’avviso – abbiamo registrato un incremento delle attività da parte di gruppi affiliati al governo iraniano e a collettivi hacktivisti, che potrebbero proseguire e aggravarsi in conseguenza degli eventi geopolitici recenti”.

□□ Chi è nel mirino degli attacchi iraniani?

Secondo le analisi delle agenzie statunitensi, i bersagli più esposti sono:

• Enti e aziende con legami economici o tecnologici con Israele
• Infrastrutture critiche (energia, sanità, trasporti)
• Settori pubblici e privati con sistemi di sicurezza obsoleti

Ma l’elemento più preoccupante è che, sebbene non ci siano ancora prove di attacchi diretti agli Stati Uniti, le agenzie ritengono “molto probabile” che ciò accada a breve.

□□ Le tattiche già in atto: defacement, leak e DDoS

I gruppi legati all’Iran hanno intensificato le azioni di:

• Defacement: modifiche fraudolente delle homepage di siti web

• Furto e diffusione di dati sensibili (leak mirati)
• Attacchi DDoS, per bloccare l’accesso a portali strategici

La dinamica è semplice quanto efficace: si penetra in siti poco protetti, si sottraggono dati o si oscurano contenuti, e si pubblicizza l’azione per ottenere visibilità e fare pressione politica o ideologica.

> **Curiosità**: il “defacement” è spesso accompagnato da messaggi propagandistici o simbolici – un attacco non solo digitale, ma anche comunicativo.

Collaborazioni pericolose: rischio ransomware in aumento

Non finisce qui. Le agenzie temono una nuova fase degli attacchi: la **collaborazione con gruppi cybercriminali non statali**, al fine di lanciare campagne di **ransomware**. In pratica: infettare sistemi, bloccarli e chiedere riscatti.

Un’alleanza tattica, tra ideologia e criminalità, che potrebbe moltiplicare l’efficacia degli attacchi e confondere le attribuzioni.

Il precedente del 2023: PLC israeliani nel mirino

Il rapporto congiunto richiama un episodio emblematico del 2023: l’attacco condotto dal Corpo delle Guardie della Rivoluzione Islamica, che ha compromesso PLC israeliani (controller logici programmabili) usati da organizzazioni statunitensi. L’obiettivo? Colpire infrastrutture critiche. Un’operazione sofisticata e, soprattutto, riuscita.

In parallelo, numerose operazioni “hack-and-leak” hanno preso di mira aziende e istituzioni israeliane, con la pubblicazione di documenti sensibili per danneggiarne l’immagine o il business.

Le contromisure consigliate dalle agenzie USA

Le raccomandazioni contenute nel report sono chiare e operative. Nessun tecnicismo inutile: solo ciò che serve davvero per prevenire un disastro informatico.

1. Aggiorna subito tutto

Molti attacchi sfruttano **vulnerabilità note** in software non aggiornati. Il consiglio è semplice: installare **sempre l’ultima versione** disponibile di ogni applicazione.

2. Disconnetti i sistemi di automazione dalla rete pubblica

I sistemi industriali non dovrebbero essere esposti su internet. Il rischio è che un accesso remoto consenta il controllo diretto di macchinari o impianti critici.

3. Dì addio alle password di default

Un errore ancora troppo diffuso: lasciare le **password predefinite**. I criminali le conoscono, le testano in automatico e penetrano facilmente nei sistemi. Serve:

• Cambiarle subito
• Renderle robuste
• Attivare l’autenticazione a più fattori

Quali sono i settori più a rischio?

Oltre alle collaborazioni con Israele, risultano particolarmente vulnerabili:

Settore	Rischio Stimato	Tipologia di Attacco
Energia	Alto	Ransomware, sabotage PLC
Sanità	Alto	Furto dati sensibili, DDoS
Logistica e trasporti	Medio-Alto	DDoS, blocco sistemi operativi
Pubblica amministrazione	Medio	Defacement, attacchi simbolici

Perché l’Iran? Perché adesso?

Le tensioni geopolitiche in Medio Oriente, sommate al supporto occidentale a Israele, hanno spinto Teheran a investire maggiormente in strumenti di cyberwarfare. Rispetto agli attacchi cinetici, quelli digitali:

• Costano meno
• Sono difficilmente attribuibili
• Possono causare danni reali (economici, sociali, reputazionali)

Ecco perché il rischio è destinato ad aumentare, non solo per gli USA, ma per tutti gli Stati percepiti come “alleati” israeliani.

Cosa fare adesso? Le 5 mosse immediate

1. Mappare le vulnerabilità: verifica se i tuoi sistemi sono esposti su internet.
2. Formare il personale: chi clicca su un link malevolo apre la porta all’attacco.
3. Implementare backup off-line: per recuperare dati anche in caso di ransomware.
4. Monitorare i log di sistema: segui le anomalie e segnala comportamenti sospetti.
5. Usare VPN e MFA: cifrare le connessioni e proteggere gli accessi è oggi essenziale.

Una minaccia silenziosa, ma concreta

Il cyberconflitto tra Iran, Israele e Stati Uniti non è un’ipotesi, ma una realtà in evoluzione. Le aziende – anche quelle piccole – non possono più permettersi di ignorare questo scenario.

Le agenzie di sicurezza americane non lanciano allarmi a vuoto: chi si muove in tempo può evitare i danni peggiori. Chi resta indietro, rischia di finire nel mirino.

Hai aggiornato i tuoi sistemi?