

Cybersecurity Italia 2025: Minacce APT, Ransomware e Attacchi Statali in aumento secondo la Relazione sulla Sicurezza Nazionale



In un contesto geopolitico caratterizzato da crescenti tensioni internazionali e da un moltiplicarsi delle crisi in vari quadranti del globo, la dimensione cibernetica emerge come uno dei domini più contesi e vulnerabili. La Relazione Annuale sulla Politica dell'Informazione per la Sicurezza 2025 offre un'analisi dettagliata dello stato della cybersecurity italiana, rivelando tendenze preoccupanti e l'evoluzione di minacce sempre più sofisticate.

Cybersecurity Italia 2025: il panorama della minaccia cibernetica in Italia

Secondo i dati forniti dalla Relazione, il 2024 ha visto un significativo aumento delle offensive cyber perpetrate da attori riconducibili ad apparati governativi stranieri contro obiettivi italiani. Questi attacchi, classificati come Advanced Persistent Threats (APT), sono caratterizzati da operazioni *“particolarmente mirate e persistenti”* e rappresentano oggi il **50% degli attacchi** rilevati, con un incremento di 12 punti percentuali rispetto al 2023.

La distribuzione degli attacchi rivela un interesse quasi equamente distribuito tra **target pubblici (50%) e privati (49%)**, con un particolare focus sulle amministrazioni centrali

dello Stato, che costituiscono il 75% degli obiettivi pubblici, in aumento di 10 punti percentuali rispetto all'anno precedente. Per quanto riguarda il settore privato, gli attacchi si sono concentrati principalmente su infrastrutture digitali e servizi IT (14%), trasporti (11%), energia (12%) e telecomunicazioni (5%).

Tecniche e tattiche in evoluzione

Particolarmente significativa è l'evoluzione delle tecniche, tattiche e procedure (TTP) impiegate dagli attori ostili. La Relazione evidenzia tre tendenze principali:

1. L'abuso di strumenti legittimi

Un elemento distintivo del 2024 è stato "il crescente abuso, da parte di attori ostili, di strumenti software legittimamente presenti all'interno dei dispositivi attaccati". Questa tecnica, nota come "living off the land", offre ai criminali informatici tre vantaggi significativi:

- Limita il traffico malevolo tra l'attaccante e la vittima, rendendo più difficile l'individuazione dell'attacco;
- Complica l'analisi forense e l'attribuzione tecnica, data l'assenza di elementi malevoli direttamente riconducibili all'attore ostile;
- Permette l'esecuzione di attività cibernetiche ostili anche a personale con limitata esperienza tecnica

2. L'impiego di Covert Relay Network

La Relazione evidenzia il maggior impiego di infrastrutture di rete particolarmente complesse, denominate "*Covert Relay Network*". Queste reti sono costituite da numerosi nodi proxy (server virtuali privati, router, firewall, dispositivi IoT e NAS compromessi) gestiti da attori strutturati per garantire l'anonimato e nascondere l'origine del traffico di rete

generato durante gli attacchi.

Queste reti, altamente dinamiche e resilienti, vengono impiegate da “quei Paesi che si pongono l’obiettivo di facilitare la propria raccolta intelligence” e possono servire sia per operazioni di spionaggio cibernetico che come piattaforma per future campagne offensive.

3. L’uso duale del ransomware

Un dato particolarmente allarmante riguarda l’evoluzione nell’uso del ransomware. Se tradizionalmente questi strumenti venivano impiegati principalmente a scopo di estorsione economica, la Relazione evidenzia come oggi vengano “ampiamente impiegati per finalità di spionaggio, influenza, disturbo e sabotaggio digitale”, tipicamente perseguite da attori di matrice statale.

Questa tendenza rappresenta un rischio considerevole, in quanto i ransomware possono generare “impatti di natura sistemica sulle infrastrutture, i servizi e sulle catene del valore del sistema Paese”, oltre a offrire opportunità di mascheramento (“operazioni sotto falsa bandiera”) e di negazione della responsabilità (“*plausible deniability*”).

Gli obiettivi degli attacchi

L’analisi delle finalità degli attacchi mostra che, sebbene il vantaggio economico rimanga l’obiettivo principale (57% del totale, in riduzione di 28 punti percentuali rispetto al 2023), **le offensive a scopo di spionaggio hanno registrato un notevole incremento, passando dal 9% al 25%.**

Questo dato riflette l’evoluzione del panorama geopolitico globale, caratterizzato da molteplici teatri di crisi, e conferma come il dominio cibernetico venga sempre più utilizzato dagli attori statuali per il raggiungimento dei propri obiettivi strategici.

Per quanto riguarda gli esiti degli attacchi, la Relazione evidenzia:

- Furto di identità digitali o credenziali (41%, in diminuzione di 41 punti percentuali);
- Esfiltrazione di informazioni sensibili (28%, in aumento di 24 punti percentuali);
- Compromissione attraverso APT (19%)

Le campagne di pre-posizionamento

Un elemento di particolare preoccupazione evidenziato dalla Relazione riguarda le *“campagne cibernetiche ostili potenzialmente orientate al pre-posizionamento all'interno delle reti telematiche di realtà pubbliche e private nazionali”*.

Queste operazioni, che prevedono *“l'installazione silente di malware non orientata a produrre effetti palesi nell'immediato”*, consentono agli attaccanti di mantenere l'accesso alle reti compromesse e di attivare in un secondo momento, *“in relazione al cambiamento dello scenario o in attuazione di una specifica strategia dello Stato mandante”*, effetti dannosi come l'interruzione di servizi o la distruzione di dati.

A incrementare il rischio contribuisce il fenomeno dell'esfiltrazione di credenziali di accesso a risorse ICT strategiche, che vengono poi messe in vendita su forum e black market nel dark web, facilitando così l'accesso illecito alle infrastrutture critiche da parte di attori ostili.

Le misure di contrasto

La Relazione evidenzia l'impegno dell'Intelligence italiana nel monitoraggio e nel contrasto alle minacce cibernetiche, attraverso:

- Il supporto alle attività del “Gruppo di coordinamento

per l'esercizio dei poteri speciali" (Golden Power), con 660 notifiche pervenute alla Presidenza del Consiglio dei Ministri nel 2024, in aumento del 14% rispetto all'anno precedente;

- La collaborazione con le Forze di Polizia e altri attori istituzionali nell'ambito del Comitato di Analisi Strategica Antiterrorismo (CASA);
- Il monitoraggio delle attività nel dark web, per individuare la vendita di credenziali e dati sensibili relativi a infrastrutture critiche nazionali

Il ruolo dell'Intelligenza Artificiale

La Relazione dedica particolare attenzione al ruolo dell'Intelligenza Artificiale (IA) nel panorama della cybersecurity. Se da un lato questa tecnologia offre nuove opportunità per la difesa, dall'altro rappresenta una risorsa significativa per gli attori ostili.

Gli Organismi Informativi evidenziano come l'IA stia contribuendo a trasformare il modo in cui le organizzazioni estremiste e terroristiche operano, facilitando:

- La creazione di contenuti persuasivi personalizzati per la propaganda;
- La micro-profilazione per il reclutamento in rete;
- L'analisi di dati per la pianificazione di attacchi;
- Il potenziamento di operazioni cyber offensive.

Particolarmente preoccupante è la capacità dell'IA di rendere più efficaci gli attacchi di social engineering, creando messaggi phishing altamente personalizzati e credibili, e di automatizzare la ricerca di vulnerabilità nei sistemi target.

La dimensione economica della

sicurezza cibernetica

La cybersecurity si conferma come un elemento fondamentale della sicurezza economico-finanziaria nazionale. La Relazione sottolinea come il settore bancario italiano, grazie agli sforzi di patrimonializzazione compiuti negli anni, rappresenti oggi un target appetibile per competitor esteri interessati ad allargare la propria presenza sul mercato nazionale.

Allo stesso tempo, si registra un *“inedito attivismo sul piano aggregativo”* nel segmento dei pagamenti, con manovre finalizzate alla creazione di *“poli”* specializzati. L'attenzione dell'Intelligence è diretta a *“monitorare gli assetti delle infrastrutture dei pagamenti, considerate strategiche per la loro cruciale funzione nelle attività economiche”*.

Prospettive e raccomandazioni

La crescente complessità delle minacce cibernetiche richiede un approccio integrato alla sicurezza, che coinvolga non solo gli organismi di intelligence e le forze dell'ordine, ma anche il settore privato e il mondo accademico.

Diventa fondamentale:

- Investire nello sviluppo di competenze specialistiche nel campo della cybersecurity;
- Potenziare la cooperazione internazionale per contrastare minacce che non conoscono confini;
- Adottare un approccio proattivo alla sicurezza, basato sull'intelligence e sull'analisi predittiva delle minacce;
- Sensibilizzare aziende e cittadini sull'importanza della sicurezza informatica.

Conclusioni

Il quadro delineato dalla Relazione 2025 evidenzia come la cybersecurity rappresenti oggi una componente imprescindibile della sicurezza nazionale. In un contesto caratterizzato da crescenti tensioni geopolitiche e dalla digitalizzazione di settori sempre più ampi dell'economia e della società, la protezione del cyberspazio diventa una priorità strategica.

Le minacce stanno evolvendo a un ritmo incessante, diventando sempre più sofisticate e difficili da individuare. Gli attori ostili, siano essi stati nazionali o gruppi criminali, stanno adottando tecniche avanzate di mascheramento e sfruttando le nuove tecnologie per rendere più efficaci i loro attacchi.

In questo scenario, l'attività di intelligence nel dominio cibernetico assume un ruolo cruciale per anticipare le minacce e proteggere le infrastrutture critiche nazionali, garantendo così non solo la sicurezza informatica, ma la stabilità stessa del sistema Paese.

Condividi sui Social Network:

<https://www.ictsecuritymagazine.com/notizie/cybersecurity-italia-2025/>