ARGO
CYBER

Argo**menti**
Cyber

Febbraio 2025

Contenuti

01 News dall'Italia

NONAME057(16) ATTACCA ANCORA L'ITALIA

Continuano gli attacchi perpetrati dal gruppo russo **NoName057(16)**, che ha condotto operazioni di **DDoS (Distributed Denial of Service)** contro infrastrutture critiche e siti istituzionali. Tra gli obiettivi figurano le banche **Intesa Sanpaolo**, gli aeroporti di **Milano Malpensa** e **Linate**, i porti di **Trieste e Taranto**, nonché il **Ministero delle Imprese e del Made in Italy**, la **Guardia di Finanza**, il **Consiglio Superiore della Magistratura (CSM)** e la **Regione Lombardia**. Gli attacchi sono stati motivati da dichiarazioni del Presidente della Repubblica **Sergio Mattarella**, che aveva paragonato l'invasione russa dell'Ucraina alle guerre di conquista del Terzo Reich.
Sebbene gli attacchi abbiano causato interruzioni temporanee ai servizi, l'**Agenzia per la Cybersicurezza Nazionale (ACN)** e la **Polizia Postale** hanno implementato misure di difesa efficaci, limitando i danni.

Questo episodio conferma la crescente esposizione dell'Italia alle minacce cyber, con il Paese che nel 2024 ha subito circa il 10% degli attacchi informatici mondiali, colpendo in particolare i settori dei media, della manifattura e dei trasporti[1] .

[1] https://www.fanpage.it/innovazione/tecnologia/nuovo-attacco-hacker-allitalia-questa-volta-gli-obiettivi-sono-parecchio-strani/ e https://www.cybersecurity360.it/cybersecurity-nazionale/attacchi-ddos-russi-ai-siti-italiani-la-minaccia-noname05716-e-le-contromisure/

MALWARE SU GITHUB RUBA CRIPTOVALUTE E DATI SENSIBILI

Una campagna malevola denominata **GitVenom**, in cui cybercriminali hanno sfruttato la piattaforma GitHub per distribuire malware mascherato da progetti open-source legittimi, è stata recentemente scoperta.

Questi falsi strumenti, che promettevano funzionalità come l'automazione di Instagram, bot per la gestione di wallet Bitcoin tramite Telegram e hack per il gioco Valorant, infettavano i dispositivi degli utenti, rubando dati personali e finanziari.
Il malware era in grado di sostituire gli indirizzi dei wallet di criptovalute copiati negli appunti con quelli degli attaccanti, portando al furto di almeno 5 Bitcoin (circa 456.600 dollari al momento della scoperta).

Le principali vittime sono state individuate in Russia, Brasile e Turchia. Il codice malevolo, scritto in vari linguaggi tra cui Python, JavaScript, C e C++, scaricava ed eseguiva ulteriori payload da repository GitHub controllati dagli attaccanti, inclusi infostealer basati su Node.js e strumenti di amministrazione remota come AsyncRAT e Quasar RAT[2] .

[2] https://exploit.in/2025/17720/ e https://www.securitylab.ru/news/556774.php?ref=123

02

News dal mondo

ATTACCO XSS SU KRPANO COLPISCE SITI GOVERNATIVI E AZIENDE FORTUNE 500

Una vulnerabilità di tipo **Cross-Site Scripting (XSS)** nel framework Krpano, utilizzato per creare tour virtuali a 360°, è stata sfruttata per iniettare script malevoli in centinaia di siti web, inclusi portali governativi, università, hotel, concessionari d'auto e grandi aziende della lista Fortune 500.

Denominata **360XSS**, questa campagna mirava a manipolare i risultati dei motori di ricerca e a promuovere spam pubblicitari.

Gli attaccanti utilizzavano un parametro XML per caricare configurazioni esterne contenenti codice malevolo codificato in Base64, che reindirizzava gli utenti verso pagine pubblicitarie. Nonostante una patch rilasciata nel 2020 per la vulnerabilità CVE-2020-24901, gli aggressori sono riusciti a sfruttare nuovamente la falla attraverso l'inclusione esplicita del parametro XML nella lista delle eccezioni.

In risposta, gli sviluppatori di Krpano hanno rilasciato l'aggiornamento 1.22.4, disabilitando completamente il supporto per le configurazioni XML esterne e consigliando agli amministratori di aggiornare il framework e disabilitare la funzione passQueryParameters[3] .

[3] https://exploit.in/2025/17721/ e https://www.securitylab.ru/news/556865.php?ref=123

03 Attacchi informatici e vulnerabilità

Nel mese di **febbraio 2025**, sono state rilevate vulnerabilità cyber significative che hanno evidenziato criticità nei software aziendali, nelle infrastrutture IT e nei dispositivi di rete, con attacchi mirati ai settori della **Pubblica Amministrazione, delle Infrastrutture Critiche e della Sicurezza Informatica.**

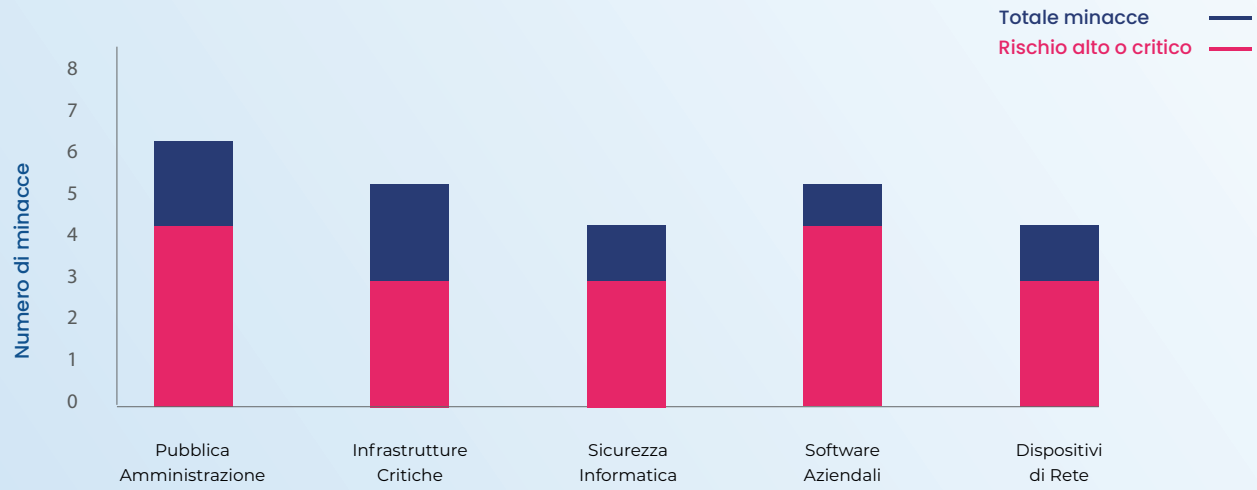
Sono state segnalate **24 vulnerabilità**, di cui **16 classificate come ad alto o critico rischio**. In particolare, Microsoft ha confermato **attività di exploit attivo** contro una falla in **.NET** e una vulnerabilità critica in **Power Pages**, mentre Zyxel ha subito uno **sfruttamento attivo della CVE-2024-40891**, mettendo a rischio la sicurezza delle reti aziendali. Parallelamente, vulnerabilità critiche sono state rilevate e successivamente corrette in **MongoDB, OpenSSL e Cisco Nexus**, con possibili implicazioni su sistemi IT e infrastrutture digitali.

Anche il settore della sicurezza dei dispositivi ha riscontrato problematiche, con aggiornamenti rilasciati per **Mozilla Firefox e Thunderbird, Juniper Networks e SonicWall**, al fine di mitigare possibili exploit.

Infine, si segnala un incremento delle campagne di **smishing**, con un'ondata di attacchi mirati agli utenti della piattaforma **Hype**, mirati alla sottrazione di credenziali bancarie. Il mese di febbraio ha quindi mostrato un **aumento delle vulnerabilità sfruttate attivamente**, sottolineando la necessità di interventi tempestivi per la protezione dei sistemi informatici.

La situazione è riassunta nel seguente grafico:

Vulnerabilità cyber di febbraio: distribuzione per settore



Il panorama delle vulnerabilità informatiche ha evidenziato una combinazione di sfruttamento attivo di falle critiche, attacchi mirati a infrastrutture IT e campagne di ingegneria sociale sofisticate. Le vulnerabilità riscontrate possono essere suddivise in due macro-categorie: (1) falle nei software e nei dispositivi di rete e (2) attacchi informatici mirati.

Tra le prime, si segnalano criticità rilevanti in **Zyxel, MongoDB, OpenSSL, SonicWall** e **Cisco Nexus**, che hanno richiesto patch urgenti per mitigare possibili attacchi basati su escalation dei privilegi, esecuzione di codice remoto e compromissione delle reti aziendali. Particolarmente rilevante è stato lo sfruttamento attivo della **CVE-2024-40891**, **CPE**, che ha esposto numerose infrastrutture a possibili accessi non autorizzati.

Anche **Microsoft** ha segnalato attacchi attivi contro falle in .NET e Power Pages, mentre software open-source come **Moodle**, **Apache OFBiz** e **Apache Fineract** sono stati oggetto di aggiornamenti di sicurezza per sanare vulnerabilità classificate ad alto rischio.

Parallelamente, il settore dei sistemi di autenticazione e gestione IT ha registrato aggiornamenti urgenti per **IBM Security Verify Directory Server**, **Mozilla Firefox** e **Thunderbird**, oltre a patch critiche per **Oracle** e **Ivanti**, evidenziando un'attenzione crescente verso la protezione dei dati aziendali e delle identità digitali.

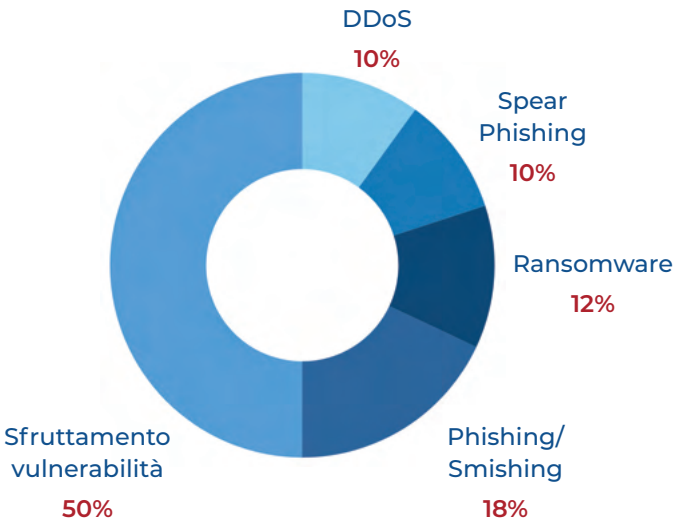
Sul fronte degli attacchi, il mese di febbraio ha mostrato un incremento delle minacce sfruttando **vulnerabilità zero-day**, ovvero falle sconosciute agli sviluppatori al momento dello sfruttamento, rendendo difficile l'implementazione di misure di mitigazione tempestive. Tra gli attacchi più significativi, si segnala un'ondata di campagne di *smishing*, con un attacco mirato contro gli utenti della piattaforma **Hype**, finalizzato alla sottrazione di credenziali bancarie. Parallelamente, attacchi APT (*Advanced Persistent Threats*) hanno continuato a colpire infrastrutture critiche, sfruttando falle note in 7-Zip, Rsync e sistemi Linux, con l'obiettivo di mantenere una presenza persistente nelle reti aziendali e governative per attività di spionaggio o sabotaggio. Anche i dispositivi mobili sono stati al centro dell'attenzione, con vulnerabilità critiche risolte nei sistemi Android e Google Pixel, mentre le stampanti multifunzione **Xerox Versalink** hanno rivelato falle di sicurezza che potrebbero consentire accessi non autorizzati a dati sensibili.

Ancora, si è registrata un'evoluzione nelle tecniche di attacco ransomware, con nuovi metodi per aggirare le difese aziendali e criptare dati sensibili in modo più rapido ed efficace. L'uso di botnet avanzate ha facilitato attacchi su larga scala, con dispositivi compromessi che hanno agito come vettori per ulteriori intrusioni. Gli attacchi DDoS, invece, hanno preso di mira aziende e servizi essenziali, causando interruzioni temporanee e mettendo sotto pressione le infrastrutture di rete. Infine, si è osservata una crescita degli attacchi di *spear phishing*, con messaggi mirati verso dirigenti aziendali e responsabili IT, sfruttando tematiche legate alla sicurezza informatica e alla conformità normativa per ottenere credenziali di accesso privilegiato.

Tra i metodi di attacco descritti, lo **sfruttamento di vulnerabilità zero-day** è senza dubbio il più pericoloso. Gli attaccanti possono sfruttare queste vulnerabilità per ottenere **accesso non autorizzato ai sistemi**, eseguire **codice arbitrario** e **muoversi lateralmente** all'interno di reti aziendali o governative senza essere rilevati dai tradizionali sistemi di sicurezza.

Di seguito un grafico riassumente quanto scritto circa la tipologia di attacchi osservati:

Tipi di attachi rilevati - Febbraio 2025



03.1 CVE Monitoring – Le nuove vulnerabilità

Presentiamo in forma tabellare alcuni esempi di vulnerabilità di rischio alto e critico rilevate recentemente:

03

Attacchi informatici e vulnerabilità

RISCHIO ALTO

Nome in codice	Descrizione
CVE-2025-27364	La vulnerabilità risiede nella funzionalità di compilazione dinamica degli agenti (noti come "implant") del server Caldera. Un attaccante può inviare una richiesta web appositamente predisposta all'API del server Caldera, utilizzata per la compilazione e il download degli agenti Sandcat o Manx. Questa richiesta può sfruttare il flag del linker con sottocomandi, permettendo l'esecuzione di codice arbitrario sul server. Fortunatamente è stata patchata.
Fonte	https://www.cve.org/CVERecord?id=CVE-2025-27364

RISCHIO CRITICO

Nome in codice	Descrizione
CVE-2025-24989	La vulnerabilità deriva da un controllo degli accessi inadeguato in **Power Pages**, consentendo a malintenzionati di bypassare i meccanismi di registrazione e ottenere privilegi elevati senza autorizzazione. Questo potrebbe portare all'accesso non autorizzato a dati sensibili e a funzionalità amministrative del sito. Microsoft ha già mitigato la situazione.
Fonte	https://www.cve.org/CVERecord?id=CVE-2025-24989

ARGO
CYBER

www.argocyber.it