ARGO
CYBER

Argo**menti**
Cyber

Gennaio 2025

Contenuti

01 News dall'Italia

NONAME, ANCORA ATTACCHI ALLE ISTITUZIONI ITALIANE

Analogamente allo scorso dicembre, il gruppo di hacker filorussi **Noname057(16)** ha condotto attacchi DDoS (Distributed Denial of Service) contro siti web di ministeri e istituzioni italiane, tra cui i Ministeri degli Esteri, delle Infrastrutture e dei Trasporti, la Consob, i Carabinieri, la Marina e l'Aeronautica.

Anche aziende di trasporto pubblico locale, come l'Atac di Roma, l'Amat di Palermo e l'Amt di Genova, sono state colpite[1] .

GRAPHITE, UNA VIOLAZIONE DELLA PRIVACY IN TUTTO IL MONDO

Altrettanto rilevante è lo scandalo di spionaggio che ha coinvolto almeno 90 giornalisti e attivisti per i diritti umani in diversi paesi, inclusa l'Italia.

Il software israeliano **Graphite**, sviluppato da Paragon, è stato utilizzato per infiltrarsi nei telefoni cellulari tramite messaggi o chiamate WhatsApp, consentendo il furto di informazioni senza necessità di interazione da parte dell'utente.
In Italia, almeno sette persone sono state colpite, tra cui Francesco Cancellato, direttore del quotidiano digitale Fanpage, e l'attivista

Luca Casarini dell'ONG Mediterranea.

A inizio febbraio, Paragon ha sospeso il contratto con l'Italia, affermando che non erano state rispettate le condizioni etiche dell'accordo[2] .

01 News dall'Italia

[1] https://www.unidprofessional.com/noname057-nuova-ondata-attacchi-hacker-in-italia/

[2] https://www.milanofinanza.it/news/meta-100-giornalisti-e-decine-di-utenti-su-whatsapp-dall-israeliana-paragon-solutions-202501311920542854 e https://www.ilsole24ore.com/art/spiato-software-militare-israeliano-fondatore-ong-mediterranea-AGim5PjC

02 News dal mondo

FURTO DI CRYPTO SU PHEMEX

La piattaforma di criptovalute **Phemex** ha subito un sofisticato attacco informatico che ha portato al furto di oltre **85 milioni di dollari** in criptovaluta. L'incidente ha interessato esclusivamente i **portafogli hot**, mentre i **portafogli cold** sono rimasti intatti. A seguito dell'attacco, Phemex ha sospeso temporaneamente le operazioni di deposito e prelievo, implementando misure di sicurezza aggiuntive e collaborando con aziende di sicurezza informatica e autorità competenti per indagare sull'accaduto[3].

[3]https://phemex.com/announcements/phemex-hot-wallet-security-incident-update-and-timeline e https://www.bleepingcomputer.com/news/security/hackers-steal-85-million-worth-of-cryptocurrency-from-phemex/

840.000 DOLLARI SOTTRATTI: LE VULNERABILITÀ DI ORANGE FINANCE

La piattaforma **Orange Finance** è stata vittima di un attacco che ha sfruttato vulnerabilità nei suoi ***smart contract***, causando una perdita di circa **840.000 dollari** in criptovaluta. Gli aggressori hanno approfittato di falle nei protocolli dei contratti intelligenti, eseguendo transazioni fraudolente e distribuendo rapidamente i fondi sottratti su diversi indirizzi per eludere il tracciamento. In risposta, gli esperti di sicurezza hanno consigliato agli utenti di interrompere immediatamente qualsiasi interazione con la piattaforma e di revocare le autorizzazioni concesse ai relativi *smart contract* per prevenire ulteriori perdite[4] .

[4]https://crypto.news/arbitrums-largest-liquidity-manager-orange-finance-loses-840k-in-hacker-attack/

03 Attacchi informatici e vulnerabilità

Nel mese di **gennaio 2025**, sono state segnalate e/o aggiornate vulnerabilità cyber significative che hanno evidenziato lacune nei software aziendali, nelle piattaforme di sicurezza e nelle infrastrutture critiche, con attacchi mirati ai settori della **Pubblica Amministrazione**, della **Tecnologia e Reti Aziendali**, e delle **Infrastrutture Critiche**.

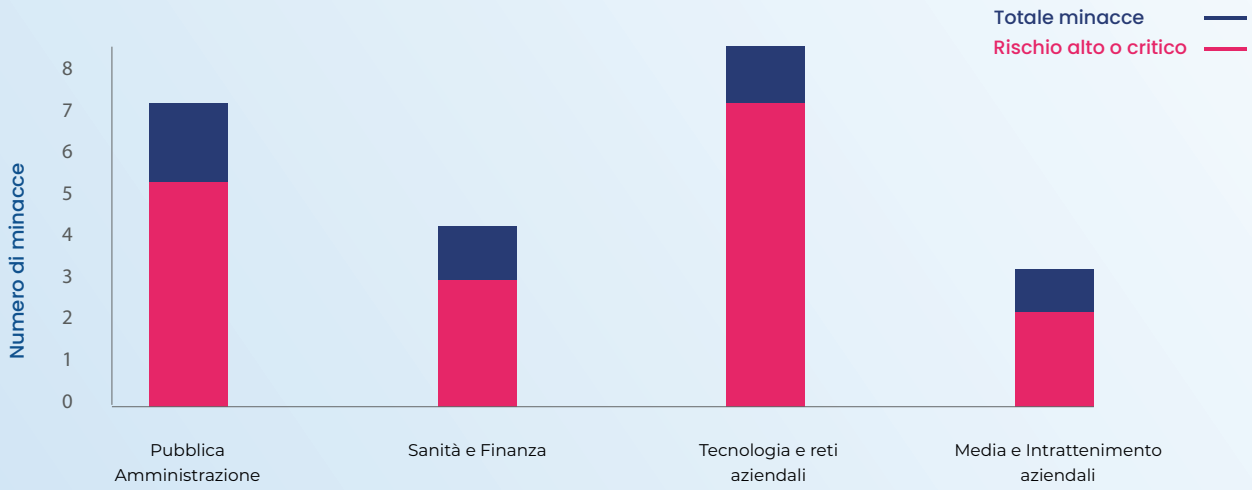
Si registra un numero complessivo di 30 vulnerabilità, di cui **20 classificate a rischio alto o critico.**

La Pubblica Amministrazione è stata vittima di campagne di **phishing e smishing**, che hanno preso di mira utenti e dipendenti di enti pubblici, mentre il settore sanitario ha subito attacchi dovuti a falle nei software di gestione e nei dispositivi di rete.

Le infrastrutture critiche e le reti aziendali, con **8 vulnerabilità segnalate**, hanno subito le conseguenze di exploit attivi e botnet che hanno compromesso firewall e dispositivi di sicurezza. Infine, il settore finanziario ha visto un numero minore di vulnerabilità, ma con implicazioni significative per l'integrità dei dati.

La situazione è riassunta nel seguente grafico.

Vulnerabilità cyber di gennaio: distribuzione per settore



Il panorama delle minacce informatiche ha mostrato un aumento significativo di segnalazioni e/o aggiornamenti circa le vulnerabilità critiche che hanno colpito diversi settori, con particolare attenzione ai dispositivi mobili, alle infrastrutture aziendali e alle piattaforme di sicurezza.

Le vulnerabilità riscontrate si suddividono principalmente in due categorie: (1) falle nei software e (2) attacchi mirati.

Le prime riguardano bug di sicurezza identificati in prodotti di largo utilizzo come Google Android, Google Pixel, Node.js, Oracle WebLogic e SAP NetWeaver, che avrebbero potuto consentire l'esecuzione di codice da remoto o l'accesso non autorizzato a dati sensibili. In ambito corporate, sono state segnalate criticità nei sistemi di sicurezza come Palo Alto Networks, Juniper Networks e SonicWall, con exploit che hanno permesso agli attaccanti di aggirare le protezioni e compromettere i sistemi aziendali. Parallelamente, attacchi di ingegneria sociale come phishing e smishing hanno continuato a prendere di mira utenti individuali e dipendenti di enti pubblici e aziende, con campagne mirate che hanno sfruttato tematiche legate a **Poste Italiane**, **iCloud** e altre piattaforme di uso comune.

Un altro elemento chiave delle minacce di gennaio è stato lo sfruttamento attivo di vulnerabilità critiche da parte di botnet avanzate, come la variante di **Aquabot**, che ha preso di mira dispositivi **Mitel** per condurre attacchi DDoS e compromettere

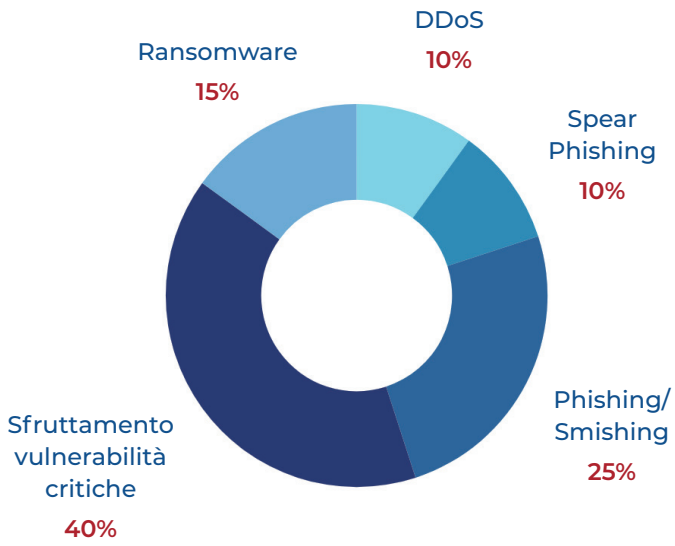
infrastrutture aziendali. Inoltre, le infrastrutture IT sono state messe sotto pressione da minacce persistenti avanzate (APT), con gruppi di cybercriminali che hanno sfruttato vulnerabilità note in Microsoft Patch-Tuesday, 7-Zip e Rsync, strumenti largamente diffusi in ambienti di sviluppo e gestione IT. Tra le vulnerabilità di maggiore impatto figurano anche quelle legate a dispositivi di rete, come quelle nei firewall Fortinet, che hanno permesso l'accesso remoto non autorizzato a reti aziendali e infrastrutture critiche.

Sul fronte degli attacchi, si osserva un utilizzo sempre più diffuso di **exploit zero-day,** ovvero vulnerabilità sconosciute agli sviluppatori e quindi prive di patch disponibili al momento dello sfruttamento.
Questo tipo di minaccia è particolarmente pericoloso perché consente agli attaccanti di infiltrarsi nei sistemi senza essere rilevati dai tradizionali sistemi di sicurezza. Parallelamente, si è assistito a un'evoluzione nelle tecniche di attacco basate su ransomware, con nuovi metodi per eludere le difese aziendali e criptare dati sensibili in modo più efficace.

Le campagne di *spear phishing* hanno invece puntato su attacchi altamente personalizzati, ingannando i destinatari con messaggi mirati che simulavano comunicazioni aziendali affidabili per ottenere credenziali e accessi riservati.

Lo sfruttamento di vulnerabilità critiche rappresenta il metodo di attacco più pericoloso, poiché consente agli aggressori di infiltrarsi nei sistemi senza necessità di interazione umana, colpendo su larga scala e con un elevato livello di automazione (**CVE-2024-55591 - Fortinet FortiOS e FortiProxy**).
A differenza del phishing o del ransomware, che richiedono il coinvolgimento della vittima, le vulnerabilità nei firewall, nei software aziendali e nei sistemi di sicurezza possono essere sfruttate per ottenere accesso non autorizzato, compromettere intere infrastrutture e lanciare attacchi combinati, come esfiltrazione di dati o movimenti laterali nelle reti.
Di seguito un grafico riassumente quanto scritto circa la tipologia di attacchi osservati:

Distribuzione delle vulnerabilità - Gennaio 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-2024-11128	Si tratta di una falla nel file eseguibile *BitdefenderVirusScanner* utilizzato da **Bitdefender Virus Scanner** per macOS. Un attaccante con privilegi limitati potrebbe sfruttare questa vulnerabilità per eseguire codice arbitrario con privilegi elevati sul sistema macOS interessato, compromettendo la riservatezza e l'integrità del sistema. Fortunatamente, è stata patchata.
Fonte	https://www.cve.org/CVERecord?id=CVE-2024-11128

RISCHIO CRITICO

Nome in codice	Descrizione
CVE-2025-0282	Si tratta di un **overflow del buffer basato sullo stack** che consente a un attaccante remoto non autenticato di eseguire codice arbitrario. **Ivanti** ha rilasciato aggiornamenti per risolvere questa vulnerabilità che, tuttavia, **risulta essere sfruttata attivamente in rete.**
Fonte	https://www.cve.org/CVERecord?id=CVE-2025-0282 e https://www.acn.gov.it/portale/w/ivanti-rilasciati-aggiornamenti-di-sicurezza

ARGO
CYBER

www.argocyber.it