ARGO CYBER

Argo**menti** Cyber

Dicembre 2024

Contenuti

01 News dall'Italia

LINATE E MALPENSA: ATTACCO DDoS

Tra le notizie di maggior peso, va menzionato l'attacco informatico rivendicato dal gruppo filorusso **Noname057(16)**, che ha preso di mira diverse infrastrutture critiche italiane, tra cui il sito web del **Ministero degli Esteri** e gli aeroporti di **Linate** e **Malpensa.**

L'azione, condotta attraverso un attacco **Distributed Denial of Service (DDoS)**, è stata motivata da presunte politiche "russofobe" adottate dall'Italia.
Sebbene i siti colpiti siano stati temporaneamente disabilitati, l'**Agenzia per la Cybersicurezza Nazionale (ACN)** è intervenuta tempestivamente, ripristinando i servizi entro due ore e limitando l'impatto, che non ha influenzato le operazioni aeroportuali.

INFOCERT DATABREACH

Altrettanto rilevante è l'attacco informatico avvenuto ai danni di **InfoCert**, uno dei principali fornitori di SPID – o identità digitale.

Questa compromissione ha portato all'esfiltrazione di circa **5,5 milioni di dati personali**; tra questi, sono stati sottratti **1,1 milioni di numeri di telefono** e **2,5 milioni di indirizzi e-mail.**

Gli aggressori hanno successivamente messo in vendita queste informazioni sul portale BreachForums, ospitato sul dark web al prezzo di **1.500 dollari.**

InfoCert ha comunque comunicato che "*nessuna credenziale di accesso ai servizi InfoCert e/o password di accesso agli stessi è stata compromessa in tale attacco*" [1] .

Stante questo furto, è estremamente probabile che nei mesi seguenti si noterà un sensibile aumento nelle campagne di phishing.

01

News dall'Italia

[1] https://www.lastampa.it/cronaca/2024/12/30/news/infocert_spid_attacco_hacker-14912113/

02 News dal mondo

ATTACCO INFORMATICO DA TRADERTRAITOR: BITCOIN.DMM.COM CHIUDE

La piattaforma giapponese Bitcoin.DMM.com è stata colpita da un attacco informatico perpetrato dal gruppo nordcoreano **TraderTraitor**, che ha sottratto 308 milioni di dollari in criptovalute. Per mettere a segno il colpo, gli hacker si sono serviti di tecniche di ingegneria sociale (e.g. phishing) attraverso cui hanno indotto un dipendente della società Ginco, che sviluppa software per portafogli aziendali, a eseguire un malware mascherato da test per un colloquio di lavoro.

Tale software maligno ha quindi compromesso il sistema, permettendo agli hacker di deviare una transazione autorizzata dal valore di 4502,9 bitcoin su portafogli controllati dal gruppo.

Le autorità giapponesi e internazionali stanno indagando, mentre la piattaforma Bitcoin.DMM.com ha annunciato la chiusura delle sue operazioni nel 2025.

NUOVA BOTNET: TP-LINK, DIGIEVER E TELTONIKA

È stata scoperta una nuova botnet, basata sul codice Mirai (progettato per sfruttare vulnerabilità in dispositivi **TP-Link**, **DigiEver** e **Teltonika RUT9XX**). In questo caso, gli hacker utilizzano una combinazione di exploit per compromissione remota (RCE) per eseguire comandi malevoli. Dopo la compromissione, i dispositivi infetti entrano a far parte della botnet per condurre attacchi **DDoS** e reclutare ulteriori macchine.

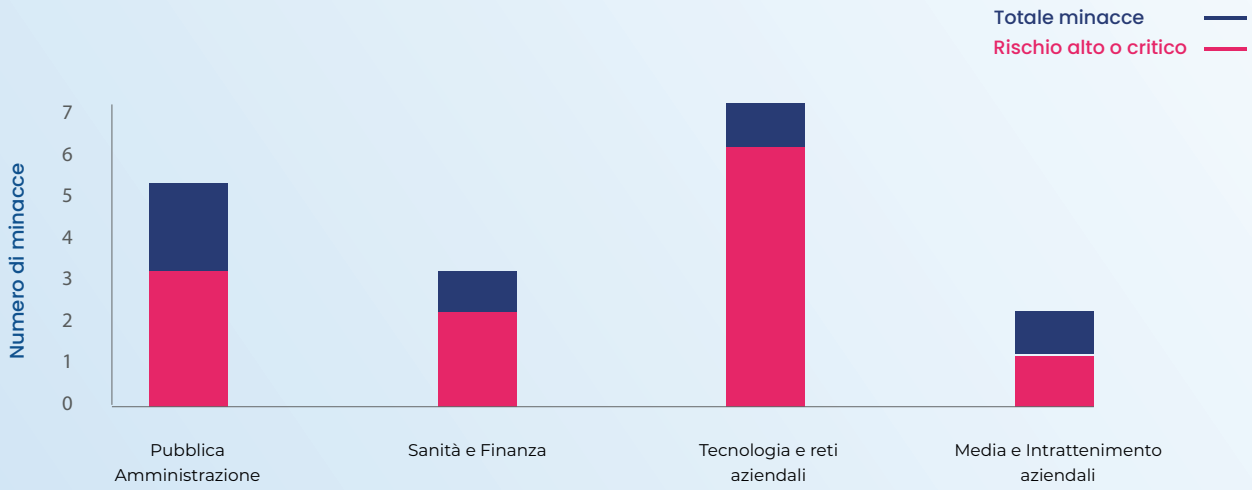
Una particolarità di questa campagna è l'uso di tecniche avanzate di offuscamento, come la crittografia XOR e ChaCha20, che rendono la botnet resistente al rilevamento, ma anche tecniche che consentono di mantenere il controllo persistente sui dispositivi infettati. La campagna sarebbe attiva da ottobre 2024, e avrebbe infettato dispositivi con architetture **x86**, **ARM** e **MIPS**, dimostrando una capacità di adattamento notevole.

Nel mese di **dicembre 2024**, sono state rilevate vulnerabilità cyber significative che hanno evidenziato lacune nei software aziendali e di sicurezza, con attacchi mirati ai settori della Pubblica Amministrazione, Tecnologia, e, per l'appunto, reti e infrastrutture aziendali.

Evidenziamo il numero ridotto di minacce, pari a **17**; tuttavia, alla maggior parte di queste (12) è stato assegnato un rischio alto o critico. Il settore **pubblico** è stato attaccato mediante campagne malevole di smishing e phishing sfruttando temi legati a Poste Italiane e al Ministero della Difesa, i settori sanitario e aziendale hanno visto vulnerabilità rilevanti nei sistemi e software di gestione.

Ultimo settore interessato, è quello legato a media e intrattenimento (2 vulnerabilità, di cui una a rischio elevato).
La situazione è riassunta nel seguente grafico:

Vulnerabilità cyber di dicembre: distribuzione per settore



Le vulnerabilità rilevate hanno riguardato sia software aziendali, che soluzioni di sicurezza, evidenziando lacune nelle infrastrutture digitali che potevano essere sfruttate per attacchi di diversa natura.
Tra i software colpiti si segnalano prodotti come Solarwinds e GitLab CE/EE, fondamentali per la gestione e il monitoraggio delle infrastrutture aziendali, nonché firewall Zyxel e applicazioni come VMware Spring, Adobe ColdFusion e Sophos. I punti deboli rilevati, quando sfruttati, potevano consentire accessi non autorizzati, esfiltrazione di dati sensibili o interruzioni di servizio. Molte di queste vulnerabilità sono, infatti, state sfruttate attivamente da attori malevoli.

Parallelamente, si sono anche verificati attacchi mirati, sotto forma di smishing (una forma evoluta di phishing) che hanno preso di mira utenti di Poste Italiane, cercando di ingannarli con messaggi apparentemente autentici legati alla corrispondenza.

Ancora, una seconda campagna di phishing, anch'essa sofisticata, ha invece sfruttato l'immagine dell'Arma dei Carabinieri e del Ministero della Difesa per attirare l'attenzione degli utenti e indurli a fornire informazioni personali o finanziarie.

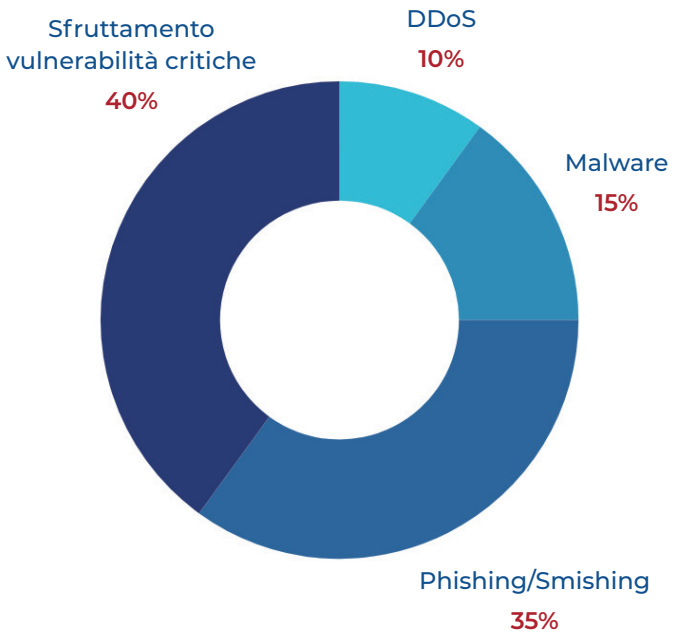
Anche i settori della tecnologia e delle reti aziendali sono stati oggetto di particolare attenzione, con vulnerabilità anche in grado

di compromettere l'integrità delle reti e la sicurezza dei dati aziendali.
La sanità e il settore finanziario, seppur meno colpiti in termini quantitativi, sono rimasti bersagli chiave a causa della loro elevata esposizione a rischi legati all'accesso non autorizzato ai dati sensibili.
Infine, il settore dei media e dell'intrattenimento ha affrontato criticità nei software di produzione come Adobe ColdFusion e Premiere Pro.

Tra i metodi di attacco esaminati, lo sfruttamento di vulnerabilità come quelle nei firewall Zyxel (CVE-2024-11667) o in Apache Struts (CVE-2024-53677) rappresentano una minaccia significativa per le infrastrutture. Infatti, questi exploit consentono agli attaccanti di ottenere accessi non autorizzati, eseguire codice malevolo o persino compromettere interi sistemi.

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

Distribuzione dei tipi di attacchi in Italia - Dicembre 2024



03

Attacchi informatici e vulnerabilità

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-2024-53677	Questa vulnerabilità, associata a un exploit Proof of Concept (PoC) pubblico, consente agli attaccanti di sfruttare il sistema in modo malevolo per eseguire codice arbitrario. La sua pericolosità risiede nella possibilità per gli attaccanti di ottenere il controllo completo del server che ospita l'applicazione web vulnerabile, aprendo la strada al furto di dati, all'interruzione di servizi o all'uso del server per scopi illeciti, come la distribuzione di malware. Fortunatamente, è stata patchata.
Fonte	https://www.cve.org/CVERecord?id=CVE-2024-53677

RISCHIO CRITICO

Nome in codice	Descrizione
CVE-2024-8785	Falla critica identificata nelle versioni di **WhatsUp Gold** precedenti alla 24.0.1, un software di monitoraggio di rete sviluppato da Progress Software Corporation. Questa vulnerabilità consente a un attaccante remoto non autenticato di sfruttare il componente **NmAPI.exe** per creare o modificare valori nel registro di sistema di Windows. Ciò può portare all'esecuzione di codice arbitrario sul sistema target, permettendo potenzialmente all'attaccante di ottenere il controllo completo del sistema compromesso. Anche questa è stata risolta.
Fonte	https://www.cve.org/CVERecord?id=CVE-2024-8785

ARGO
CYBER

www.argocyber.it