Falle PaperCut sfruttate contro scuole e atenei: dal server di stampa al dominio Active Directory

Due vulnerabilità concatenate di PaperCut NG/MF sono state usate per rubare credenziali a scuole e atenei in Europa e negli Stati Uniti. Il caso mostra perché un server di stampa integrato con la directory va trattato come sistema critico, anche ai fini NIS2.

Un server di gestione delle stampe compare raramente negli inventari delle risorse critiche. Eppure, tra fine agosto e i primi di settembre 2026, attaccanti non identificati lo hanno usato per raccogliere credenziali di scuole e università in Europa e negli Stati Uniti. Lo documenta l'analisi dell'Adversary Research Team di Arctic Wolf, datata 4 settembre e ripresa dalla stampa specializzata il giorno seguente. La catena di sfruttamento parte da due vulnerabilità di PaperCut NG/MF. In pochi passaggi arriva agli *hive* del registro di Windows e ai file di configurazione che custodiscono le credenziali verso Active Directory e LDAP.

Le vulnerabilità erano già note. La novità del rapporto è il quadro completo: chi viene colpito, con quali strumenti e che cosa cercano gli attaccanti una volta dentro.

La campagna secondo Arctic Wolf

Il rapporto, firmato dagli analisti Jens Pose e Ross Phillips, documenta lo sfruttamento di server PaperCut vulnerabili a CVE-2026-81578 e CVE-2026-82078. Le attività osservate comprendono esecuzione di comandi, ricognizione e tentativi di creare account privilegiati. Arctic Wolf ha precisato a The

Hacker News che le vittime appartengono al settore dell'istruzione in senso ampio: dalle scuole primarie e secondarie (il segmento statunitense K-12) alle grandi università, negli Stati Uniti e in Europa. Nessuna istituzione è stata nominata e il rapporto non propone alcuna attribuzione.

La cronologia mostra quanto rapidamente si è aperta la finestra di esposizione. Le date, indicate di seguito, sono tratte dall'avviso di sicurezza di PaperCut, dall'avviso CISA e dal rapporto Arctic Wolf; dove la fonte è un'azienda di sicurezza:

- **26 agosto 2026**: Huntress dichiara di aver rilevato la prima attività di attacco nota e di aver riprodotto una catena completa di esecuzione di codice remoto senza autenticazione contro un'installazione standard di PaperCut NG.
- **27 agosto**: PaperCut pubblica l'avviso urgente e conferma incidenti presso i clienti. La prima patch di emergenza per le versioni 25 e 26 esce alle 02:10 del 28 agosto, ora australiana, cioè la sera del 27 in Europa.
- **28 agosto**: vengono assegnate le due CVE. In serata PaperCut pubblica la Emergency Patch Release 2, con misure di irrobustimento sviluppate con Huntress e watchTowr, perché la prima patch era aggirabile; poche ore dopo la estende alla versione 24.
- **29 agosto**: la società Defused riferisce di attività di sfruttamento nei propri honeypot, con un attore che usa l'aggiramento dell'autenticazione per estrarre tabelle dal database interno Derby anziché eseguire codice.
- **31 agosto**: CISA inserisce entrambe le CVE nel catalogo Known Exploited Vulnerabilities con un unico avviso, richiamando la Binding Operational Directive 26-04 sulla correzione prioritaria delle vulnerabilità sfruttate. Lo stesso giorno il CSIRT Italia pubblica l'alert AL04/260831/CSIRT-ITA. Rapid7 rende disponibile un

modulo Metasploit.

- **1 settembre**: PaperCut pubblica la Emergency Patch Release 3 per le versioni 24, 25 e 26. È cumulativa, corregge due regressioni (accesso SAML e driver Microsoft SQL Server legacy per la ricerca esterna dei numeri di tessera) e, secondo il produttore, chiude ulteriori vettori osservati in rete.
- **2 settembre**: il produttore segnala una seconda ondata di attacchi contro i server esposti e non completamente aggiornati, con comportamento post compromissione più sofisticato.
- **4 settembre**: Arctic Wolf pubblica l'analisi della campagna contro il settore dell'istruzione.

Sul piano tecnico, PaperCut classifica CVE-2026-81578 come difetto di controllo degli accessi nell'interfaccia web di amministrazione (CWE-306, CVSS 4.0 pari a 8.8). In determinate condizioni, richieste remote non autenticate dirette a funzioni amministrative attivano azioni prima che la verifica degli accessi sia completata. L'effetto è la modifica di alcune configurazioni di sistema. CVE-2026-82078 (CWE-470, CVSS 4.0 pari a 9.4) riguarda invece il caricamento dinamico non sicuro di classi Java nelle utilità di connessione al database. L'applicazione istanzia i driver in base a nomi configurabili, senza confrontarli con una lista di driver approvati. Concatenate, le due falle permettono di eseguire bytecode Java arbitrario nel contesto del processo del server PaperCut, senza credenziali e senza interazione dell'utente. John Hammond di Huntress ha sintetizzato così a Cybersecurity Dive: all'attaccante basta l'indirizzo IP o il nome host del bersaglio.

Il produttore considera potenzialmente interessate tutte le versioni di PaperCut NG e MF. Le patch di emergenza coprono le versioni 24, 25 e 26; per le precedenti l'indicazione è aggiornare alla versione corrente.

Perché un server di stampa è un bersaglio di valore

Guardato dalla funzione, PaperCut conta pagine, applica quote e rilascia le stampe in modo sicuro. Guardato dalla posizione in rete, il quadro cambia. L'Application Server sincronizza utenti e gruppi da Active Directory, LDAP, Microsoft Entra ID o Google Workspace, come documenta il manuale del prodotto. Conserva quindi credenziali di collegamento (*bind*) verso la directory, spesso associate ad account di servizio con privilegi più ampi del necessario. Deve essere raggiungibile da tutte le postazioni e da tutte le multifunzione dell'organizzazione; questo lo colloca spesso in segmenti di rete poco filtrati. In molte realtà educative è inoltre pubblicato su internet per consentire la stampa via web e il rilascio da dispositivi mobili.

Si aggiunge un fattore organizzativo. Il sistema di stampa è spesso gestito da un fornitore esterno o rientra nel contratto di noleggio delle multifunzione. Gli aggiornamenti seguono i tempi del fornitore, non quelli del rischio. Il risultato è una risorsa con accesso alla directory, esposta verso l'esterno, con un ciclo di patch lento e spesso senza un responsabile interno.

Non è la prima volta che PaperCut finisce al centro di una campagna simile. Nella primavera 2023 le vulnerabilità CVE-2023-27350 e CVE-2023-27351 furono sfruttate, secondo le ricostruzioni dell'epoca, per distribuire i ransomware LockBit e Clop; anche allora il CSIRT Italia diffuse un alert sullo sfruttamento attivo. Lo schema si ripete: un componente considerato accessorio diventa la porta d'ingresso verso il dominio.

Le tecniche post sfruttamento e cosa cercare nei log

La parte più utile del rapporto di Arctic Wolf descrive che cosa fanno gli attaccanti dopo aver ottenuto l'esecuzione di codice. La sequenza è coerente su più vittime.

1. **Ricognizione**: comandi lanciati tramite cmd.exe con pc-app.exe, il processo del server PaperCut, come processo padre. Le forme registrate sono cmd.exe /d /s /c "ver || uname -a" e cmd /c "whoami & ver & tasklist"; la prima è costruita per funzionare sia su Windows sia su Linux.
2. **Account privilegiati**: creazione, o tentativo di creazione, di un account amministrativo con il nome ricorrente Administrator17.
3. **Raccolta dei risultati**: gli output dei comandi e i dati raccolti vengono scritti in file /custom/pcp_<10 caratteri>.txt o /custom/web/pcp_<10 caratteri>.txt nelle directory di PaperCut. Vengono poi recuperati con richieste GET dall'indirizzo 45.142.193[.]132, con *User-Agent* python-requests/2.32.5.
4. **Strumenti di raccolta credenziali**: tramite certutil.exe vengono scaricati dallo stesso indirizzo, sulla porta 8000, gli eseguibili lsa_collect.exe, lsa_collect_small.exe e save_hives.exe. In sandbox, Arctic Wolf ha osservato lsa_collect.exe estrarre chiavi di registro per ricostruire il BootKey di sistema, che dà accesso al database SAM e quindi agli *hash* delle password locali.
5. **Accesso remoto**: *payload* Java di Meterpreter scaricati da 194.180.48[.]134, con sessioni stabilite verso lo stesso host.
6. **Ricerca di segreti nella configurazione**: findstr /s /i /n /c:"password" /c:"secret" /c:"bind" /c:"ldap" /c:"token" sui file *.config di PaperCut.

L'ultimo passaggio è quello che, a nostro avviso, collega il

server di stampa al dominio: le stringhe cercate sono quelle che identificano le credenziali di *bind* verso LDAP e Active Directory e i token di integrazione.

Gli indicatori pubblicati dal produttore sono concreti. Nel server.log vanno cercate stringhe come jdbc:derby:memory:pwn;create=true, ERROR DatabaseUtils - Database error looking up cardID: VALUES CAST, ERROR No suitable driver found for jdbc:no:x e VALUES CAST(X'cafebabe, dove cafebabe è la firma esadecimale di un file .class Java. Sono sospetti anche log mancanti, troncati o cancellati. Nel file system vanno cercati file .class in server\lib e file .cmd e .out in server\data\content, tutti con nomi casuali di cinque caratteri; il produttore avverte che gli attaccanti li rimuovono man mano che l'attività procede. Sui dispositivi, la regola di rilevamento più efficace è la più semplice: pc-app.exe che genera cmd.exe, powershell.exe o altri interpreti, con revisione della riga di comando e del traffico di rete associato. Sul fronte delle identità, occorre esaminare gli eventi di gestione degli account alla ricerca di Administrator17 e di qualsiasi utenza privilegiata creata a ridosso di attività anomale sul server di stampa.

Il produttore ha inoltre documentato una sequenza post compromissione diversa da quella di Arctic Wolf, osservata dove la protezione dei dispositivi non ha bloccato l'esecuzione. Dopo whoami & ver e tasklist, l'attaccante enumera i controller di dominio con nltest /dclist: ed elenca sessioni e cartelle utente con quser e dir c:\users. Poi scarica con PowerShell un eseguibile (ace.exe) da un servizio di condivisione file e lo installa in modalità silenziosa. Il risultato è un servizio Windows chiamato "Remote Access Service", che esegue l'agente SimpleHelp come LocalSystem con avvio automatico; circa mezz'ora dopo viene scaricato AnyDesk. L'intera sequenza dura meno di trenta minuti dal primo comando. Il comando nltest /dclist: conferma l'interesse per i controller di dominio prima ancora del consolidamento

dell’accesso remoto. PaperCut raccomanda di cercare quel servizio e installazioni impreviste di AnyDesk.

Un punto va sottolineato: un server aggiornato oggi può essere stato compromesso ieri. La patch chiude la porta, non espelle chi è già entrato; la stessa BOD 26-04 di CISA fissa aspettative su quando le agenzie devono verificare una compromissione precedente alla patch. In caso di sospetta compromissione, il produttore raccomanda di mettere in sicurezza i backup, ricostruire da zero l’Application Server e ripristinare un backup precedente all’attività sospetta. A questo va aggiunta, per prudenza, la rotazione di tutte le credenziali che il server conosceva: account di servizio della directory, credenziali del database esterno, chiavi API e token di integrazione.

Lo stato dell’esposizione e come segregare l’istanza

Secondo quanto riportato da BleepingComputer, Shadowserver rileva oltre 800 server PaperCut NG/MF raggiungibili da internet; il dato, che non abbiamo verificato direttamente sulla piattaforma Shadowserver, non distingue tra sistemi già protetti, honeypot e istanze vulnerabili. Per un ateneo o un istituto scolastico la verifica è semplice. Basta interrogare i servizi di scansione passiva (Shodan, Censys, la stessa Shadowserver per gli enti abilitati) sulle porte predefinite dell’Application Server, 9191 e 9192. Vanno aggiunte le porte 80 e 443 quando l’interfaccia è pubblicata dietro un *reverse proxy*. Il risultato va confrontato con l’inventario degli indirizzi pubblici. Se l’interfaccia di amministrazione risponde da fuori, l’istanza va trattata come potenzialmente toccata.

Le indicazioni del produttore sono lineari: limitare subito l’accesso web a indirizzi fidati, con regole firewall, liste di controllo o restrizioni sul *reverse proxy*; applicare la

Emergency Patch Release 3 anche se si è già installata la prima o la seconda; aggiornare anche Site Server e server di stampa secondari, non solo l'Application Server principale. Mobility Print, Print Deploy, i client utente e i prodotti cloud Hive e Pocket non sono interessati. Chi usa la ricerca dei numeri di tessera su un database esterno deve riattivare esplicitamente la funzione nel file security.properties, perché dopo la patch è disabilitata per impostazione predefinita. Nelle scuole senza personale tecnico interno, il primo passo è chiedere al fornitore delle multifunzione se il server PaperCut è raggiungibile da internet e quale versione è installata: due domande a cui si risponde in pochi minuti.

Il quadro italiano: scuole, atenei ed enti di ricerca tra NIS2 e inventario delle risorse

Il CSIRT Italia ha pubblicato il 31 agosto l'alert AL04/260831/CSIRT-ITA sullo sfruttamento attivo delle due CVE, con impatto sistemico "critico" (78,71). L'alert indica come vulnerabili le versioni precedenti alla 24.1.9, alla 25.0.12 e alla 26.0.4 Emergency Patch Release 2; è uscito prima della Release 3 dell'1 settembre, che resta la versione di riferimento. PaperCut è un prodotto seguito con continuità dal CSIRT: a giugno 2026 un alert aveva segnalato una vulnerabilità di gravità alta nel client Print Deploy per Windows (CVE-2026-6645), e nel 2023 lo sfruttamento delle CVE-2023-27350 e 27351. Per il lettore italiano, però, la questione non è solo di gestione delle patch.

Il D.Lgs. 4 settembre 2024, n. 138, che recepisce la direttiva NIS2, colloca il mondo della ricerca nel perimetro per due vie. L'Allegato II, tra gli altri settori critici, elenca al punto 7 le organizzazioni di ricerca. L'Allegato III, che individua le pubbliche amministrazioni soggette al decreto ai sensi dell'articolo 3, comma 6, comprende tra gli altri

soggetti pubblici gli enti e le istituzioni di ricerca. Le università non rientrano automaticamente in nessuna delle due categorie. La direttiva, all'articolo 6, punto 41, definisce organizzazione di ricerca il soggetto che svolge in via principale ricerca applicata o sviluppo sperimentale a fini commerciali, ed esclude espressamente gli istituti di istruzione. L'articolo 2, paragrafo 5, lettera b), lascia però agli Stati membri la facoltà di includere gli istituti di istruzione, in particolare quando svolgono attività di ricerca critiche.

Il legislatore italiano ha esercitato questa facoltà. L'Allegato IV del decreto elenca al punto 2 gli "istituti di istruzione che svolgono attività di ricerca". Accanto figurano il trasporto pubblico locale, i soggetti di interesse culturale e le società in house o a controllo pubblico. Per questi soggetti il decreto si applica indipendentemente dalle dimensioni, ma solo dopo l'individuazione da parte dell'Autorità nazionale competente NIS su proposta delle Autorità di settore (articolo 3, commi 8 e 13). Un ateneo non è nel perimetro per il solo fatto di esistere: lo è quando ACN glielo notifica. L'articolo 3, comma 9, lettera f), prevede inoltre che vi possa essere attratto chi è critico come elemento sistemico della catena di approvvigionamento, anche digitale, di un soggetto essenziale o importante. È una clausola che riguarda da vicino i fornitori che gestiscono servizi come la stampa per conto di atenei ed enti.

Per i soggetti nel perimetro, gli obblighi di notifica sono operativi dal gennaio 2026, come ricorda ACN nel rapporto sul primo semestre. L'articolo 25 del decreto fissa la sequenza. Pre-notifica al CSIRT Italia senza ingiustificato ritardo, e comunque entro 24 ore dalla conoscenza dell'incidente significativo, indicando ove possibile se derivi da atti malevoli. Notifica entro 72 ore, con una valutazione iniziale di gravità e impatto e, se disponibili, gli indicatori di compromissione. Relazione finale entro un mese, con

descrizione dell’incidente, causa originaria e misure di attenuazione. Lo stesso articolo definisce significativo l’incidente che ha causato, o è in grado di causare, una grave perturbazione operativa o perdite finanziarie, oppure ripercussioni considerevoli su terzi. A nostro giudizio un furto di credenziali della directory da un server di stampa può rientrare in questa definizione: l’impatto potenziale riguarda l’intera identità digitale dell’ente, e la norma chiede di valutare l’idoneità a causare il danno, non solo il danno già prodotto.

Le misure di gestione del rischio dell’articolo 24, comma 2, del decreto (che riprende l’articolo 21 della direttiva) contengono tre elementi che questa vicenda mette alla prova. La lettera i) affianca le politiche di controllo dell’accesso alla “gestione dei beni e degli assetti”: un inventario che non comprende il server PaperCut, o lo classifica come periferica, non permette di valutare il rischio. La lettera d) impone la sicurezza della catena di approvvigionamento, compresi i rapporti con i diretti fornitori e fornitori di servizi, e il comma 3 chiede di considerare le vulnerabilità specifiche di ciascun fornitore: se il sistema è gestito da terzi, il contratto deve prevedere tempi per le patch di emergenza, accesso ai log e obblighi di comunicazione in caso di incidente. Le stesse politiche di controllo dell’accesso implicano che l’account di servizio usato da PaperCut verso la directory abbia privilegi di sola lettura sugli attributi necessari, e non sia un account amministrativo riutilizzato.

Le scuole del primo e del secondo ciclo, che di norma non svolgono attività di ricerca, restano in gran parte fuori dal perimetro NIS2. Non restano fuori dal problema. PaperCut è diffuso negli istituti scolastici perché gestisce quote di stampa per studenti e docenti, e gli istituti operano con risorse di sicurezza minime, spesso senza un referente tecnico interno. In questi contesti la responsabilità di fatto ricade sul fornitore delle multifunzione e sull’ufficio tecnico della

scuola, che raramente ha visibilità sulla configurazione del server. È qui che le indicazioni operative contano più delle norme.

Raccomandazioni operative e domande da porre al fornitore

Per chi gestisce direttamente il sistema:

- Applicare la Emergency Patch Release 3 (o la versione corrente, per le versioni precedenti alla 24) e non considerare risolutive le patch precedenti.
- Rimuovere l'esposizione diretta a internet dell'Application Server. Se la stampa via web dall'esterno è necessaria, pubblicarla attraverso un *reverse proxy* con restrizioni e autenticazione a monte.
- Cercare nei log e sui dispositivi gli indicatori descritti sopra, con priorità a pc-app.exe come processo padre di interpreti di comandi e ai file pcp_*.txt.
- Trattare ogni istanza esposta come potenzialmente compromessa fino a prova contraria. In presenza di evidenze, ricostruire il server e ruotare tutte le credenziali note al sistema.
- Ridurre i privilegi dell'account di servizio verso Active Directory o LDAP e verificare che non sia condiviso con altri sistemi.
- Inserire il server di stampa nell'inventario delle risorse con la classificazione corretta: sistema con accesso alla directory, non periferica.

Per chi si affida a un fornitore esterno, le domande da porre per iscritto sono cinque:

1. Il server PaperCut è raggiungibile da internet? Su quali porte e indirizzi?
2. Quale versione e quale patch di emergenza sono installate, e in che data sono state applicate?

3. I log del server e le directory di PaperCut sono stati verificati rispetto agli indicatori pubblicati dal produttore e da Arctic Wolf? Con quale esito?
4. Con quale account il server si collega alla directory dell'istituto, e quali privilegi ha quell'account?
5. In caso di compromissione, quali tempi e modalità di comunicazione prevede il contratto?

Le risposte a queste domande dicono più di qualsiasi certificazione. E ricordano che il percorso più breve verso il dominio raramente passa dai sistemi che tutti considerano critici; passa da quelli che nessuno pensa di guardare.

https://www.ictsecuritymagazine.com/notizie/vulnerabilita-papercut-attacchi-scuole-universita/

Speciale Adnkronos dal Forum Teha di Cernobbio – Diretta 5

(Adnkronos) – Speciale Adnkronos dal Forum Teha di Cernobbio – Diretta 5, domenica 6 settembre ore 11.

–

economia

webinfo@adnkronos.com (Web Info)

The post Speciale Adnkronos dal Forum Teha di Cernobbio – Diretta 5 appeared first on Key4biz.

https://www.key4biz.it/speciale-adnkronos-dal-forum-teha-di-cernobbio-diretta-5/586349/

Cernobbio, Vannacci: “Con Salvini stretta di mano tra gentiluomini”

(Adnkronos) – “C’è stata una stretta di mano con Salvini, con Pichetto Fratin, tra gentiluomini, come è giusto che sia”, lo ha detto Roberto Vannacci andando via dal Forum di Cernobbio insieme alla moglie.

–

economia

webinfo@adnkronos.com (Web Info)

The post Cernobbio, Vannacci: “Con Salvini stretta di mano tra gentiluomini” appeared first on Key4biz.

https://www.key4biz.it/cernobbio-vannacci-con-salvini-stretta-di-mano-tra-gentiluomini/586351/

Come informarsi su politica e attualità in modo efficiente senza perdersi nelle notizie

Quando il tempo è limitato, il problema non è trovare altre notizie, ma decidere quali meritano attenzione per prime.

Aggiornarsi, comprendere un avvenimento e verificarne i dettagli sono attività diverse: trattarle come un unico compito porta facilmente a passare da un titolo all'altro senza arrivare a una conclusione solida.

Una routine efficiente separa quindi tre momenti: una rassegna iniziale per individuare i fatti rilevanti, un approfondimento riservato a pochi temi e un controllo delle fonti proporzionato all'importanza della notizia. Il punto di partenza non è il flusso disponibile, ma il tempo che si può dedicare e il risultato che si vuole ottenere.

Prima il tempo, poi il flusso delle notizie

La frequenza con cui informarsi dipende dalle proprie esigenze. Chi segue la politica per orientarsi come cittadino può programmare consultazioni regolari; chi deve monitorare un settore per lavoro avrà bisogno di passaggi più frequenti. Non esiste una durata standard valida per tutti, perché una rassegna generale e la verifica di un caso controverso richiedono impegni differenti.

Prima di aprire siti e applicazioni conviene definire tre elementi:

- il tempo disponibile per la rassegna e quello eventualmente riservato all'approfondimento;
- i temi prioritari, distinguendo quelli da seguire con continuità da quelli occasionali;
- la condizione che giustifica una verifica ulteriore, come una decisione pubblica importante, un dato sorprendente o versioni tra loro discordanti.

Questi confini impediscono che ogni aggiornamento riceva lo stesso peso. Una dichiarazione del giorno può essere registrata rapidamente; un provvedimento che incide su un tema

rilevante richiede invece di individuare il testo originario, l’istituzione competente e i passaggi necessari perché produca effetti.

Costruire una rassegna di base

La rassegna iniziale serve a sapere che cosa è accaduto, non a esaurire ogni argomento. Per questa fase è utile scegliere in anticipo un insieme limitato di fonti con funzioni diverse: una fonte per la panoramica generale, testate capaci di offrire ricostruzioni autonome e, quando si parla di decisioni pubbliche, i documenti diffusi dagli organismi coinvolti.

Consultare più pagine non equivale necessariamente a confrontare più versioni. Se diversi articoli riprendono la stessa origine, il numero di pagine cresce ma la base informativa rimane sostanzialmente una. Il confronto diventa utile quando permette di distinguere i fatti condivisi, i dettagli ancora incerti e le interpretazioni redazionali.

Per le notizie politiche occorre inoltre capire chi abbia il potere di compiere l’azione descritta. Una distinzione introduttiva richiamata da Politica Semplice riguarda Parlamento e Governo: il primo esercita il potere legislativo, mentre il secondo esercita quello esecutivo. Il Governo non viene eletto direttamente e opera con il sostegno della maggioranza parlamentare. Questa base consente di leggere con maggiore precisione formule come proposta, approvazione, voto, decreto o attuazione, senza attribuire a un organo decisioni che competono a un altro.

Il contesto storico va aggiunto quando chiarisce il fatto corrente. Una controversia può dipendere da una decisione precedente, da un iter già avviato o da un impegno rimasto incompiuto. In questi casi fermarsi al titolo del giorno non basta; per un aggiornamento ordinario, invece, non è necessario ricostruire ogni precedente remoto.

Scegliere che cosa approfondire

Dopo la rassegna, la selezione può basarsi su tre domande: quanto è rilevante il fatto, quanto sono solide le informazioni disponibili e che conseguenze avrebbe accettare o condividere una versione inesatta. Una notizia marginale e facilmente correggibile non richiede lo stesso investimento di tempo di un'affermazione destinata a influenzare un'opinione o una decisione.

Per effettuare questo vaglio si può ricorrere al test CRAAP, presentato da Agenda Digitale come una checklist orientativa. I cinque criteri sono attualità, rilevanza, autorevolezza, accuratezza e scopo. In pratica, bisogna chiedersi se il contenuto sia abbastanza recente per la questione trattata, se risponda davvero alla domanda, se provenga da un soggetto competente e identificabile, se offra elementi controllabili e quale obiettivo persegua.

Il test non certifica la verità di una notizia. Serve piuttosto a decidere se il contenuto possa essere usato come primo riferimento, se debba essere confrontato con altre fonti o se presenti problemi tali da sconsigliarne l'impiego.

Verificare prima di formarsi un'opinione

Il primo controllo riguarda quattro elementi distinti: il sito che pubblica la notizia, l'autore, le fonti citate e la data di diffusione. Agenda Digitale li indica come criteri di base per ridurre il rischio di disinformazione. Nessuno di essi, considerato da solo, prova che il contenuto sia corretto: insieme permettono però di individuare rapidamente lacune e incongruenze.

Il nome del sito chiarisce chi si assume la responsabilità della pubblicazione. L'autore permette di valutarne ruolo e

competenza. Le fonti citate mostrano se le affermazioni possano essere ricondotte a documenti, dati o dichiarazioni identificabili. La data, infine, evita di trattare come attuale un contenuto superato o riproposto fuori contesto.

Quando la notizia si fonda su un atto, un rapporto o un intervento pubblico, il passaggio successivo consiste nel cercare il materiale originale. Il documento primario attesta che cosa è stato pubblicato o dichiarato, ma non risolve automaticamente ogni interpretazione. Per questo conviene confrontarlo con ricostruzioni competenti e separare quattro piani:

1. il fatto documentato;
2. la dichiarazione di una parte coinvolta;
3. l’interpretazione proposta dall’articolo;
4. le previsioni sulle possibili conseguenze.

Formarsi un’opinione diventa più semplice quando questi livelli non vengono confusi. Se due ricostruzioni divergono, la domanda utile non è soltanto quale sembri più convincente, ma su quale documento si basi ciascuna, quali passaggi selezioni e quali aspetti lasci irrisolti.

Quando la notizia è un’immagine o un video

I contenuti visivi richiedono controlli specifici. È utile verificare se l’immagine o il filmato siano originali, se siano già apparsi in precedenza e se luogo e periodo dichiarati risultino compatibili con gli elementi disponibili. La ricerca degli utilizzi precedenti può far emergere materiale riciclato; geolocalizzazione e cronolocalizzazione possono aiutare a controllare dove e quando sia stato realizzato.

Queste tecniche riducono l’incertezza, ma non garantiscono da

sole autenticità e significato. Un contenuto reale può comunque essere accompagnato da una descrizione fuorviante, tagliato in modo da omettere il contesto o attribuito a un evento diverso.

Occorre anche proporzionare l'impegno. Nei casi complessi, un'indagine su foto, video o post può richiedere persino mesi. Il controllo quotidiano di un lettore non deve imitare un'indagine specialistica: quando gli elementi non bastano, la scelta più corretta è sospendere il giudizio, non condividere il contenuto come certo e cercare verifiche professionali già disponibili.

Una routine sostenibile in tre passaggi

La procedura può essere adattata al tempo disponibile senza modificarne la logica. Nel primo passaggio si effettua una rassegna delle fonti di base e si annotano soltanto gli avvenimenti pertinenti ai temi scelti. Nel secondo si selezionano una o poche notizie in base a rilevanza, incertezza e conseguenze. Nel terzo si controllano origine, autore, data, documenti e versioni alternative prima di arrivare a un giudizio.

Se il tempo termina dopo la rassegna, è sufficiente conservare la notizia come aggiornamento provvisorio. Se emerge un dubbio importante, l'approfondimento può essere rimandato a un momento dedicato. Questa distinzione evita di trasformare ogni sessione informativa in una ricerca senza fine e, nello stesso tempo, impedisce di scambiare una lettura rapida per una comprensione completa.

La routine va corretta quando una fonte produce ripetizioni, commenti non distinguibili dai fatti o contenuti che richiedono controlli sproporzionati rispetto al loro valore. Può invece essere mantenuta quando consente di risalire

facilmente alle informazioni originali e di riconoscere ciò che rimane incerto.

La qualità si misura dalla comprensione raggiunta

Al termine di una sessione informativa, il risultato non dipende dal numero di titoli letti. Conta poter spiegare che cosa è successo, quale soggetto ha agito, su quali elementi si basa la ricostruzione, che cosa non è ancora verificato e perché il fatto è rilevante.

Se queste risposte mancano, aggiungere altre notizie al flusso difficilmente colmerà il vuoto. È più utile tornare sulla priorità iniziale, scegliere una sola domanda e seguirla fino a una fonte controllabile. Una routine efficiente non punta a sapere tutto in tempo reale, ma a uscire dall'informazione quotidiana con meno incertezza e una comprensione utilizzabile.

L'articolo Come informarsi su politica e attualità in modo efficiente senza perdersi nelle notizie proviene da Il Kim Magazine.

https://www.ilkim.it/come-informarsi-su-politica-e-attualita-in-modo-efficiente-senza-perdersi-nelle-notizie/

Vicenzaoro, Trenti (Intesa Sanpaolo): "Export italiano

regge nonostante contesto internazionale complesso”

(Adnkronos) – “Il settore orafo italiano, dopo la fase molto positiva culminata con il 2024, sta attraversando un momento di normalizzazione. Il contesto internazionale è estremamente complesso e lo possiamo vedere attraverso il forte calo che si è verificato nella domanda di gioielli in oro a livello internazionale. Nonostante questo contesto, però, le esportazioni italiane sono state in grado di reggere bene questa situazione”. Lo afferma Stefania Trenti, Responsabile dell’Ufficio Industry della Direzione Studi e Ricerche di Intesa Sanpaolo, in merito all’indagine presentata con Federorafi in occasione della seconda giornata di lavori di Vicenzaoro September 2026, il salone internazionale dell’oreficeria e della gioielleria firmato IEG – Italian Exhibition Group, in programma fino all’8 settembre nel quartiere fieristico di Vicenza.

–

economia

webinfo@adnkronos.com (Web Info)

The post Vicenzaoro, Trenti (Intesa Sanpaolo): “Export italiano regge nonostante contesto internazionale complesso” appeared first on Key4biz.

https://www.key4biz.it/vicenzaoro-trenti-intesa-sanpaolo-export-italiano-regge-nonostante-contesto-internazionale-complesso/586345/

Fiere, Vicenzaoro: Squarcialupi (Federorafi): “export Stati Uniti segna +22%”

(Adnkronos) – “Temevamo molto i dazi di Trump. Nel 2025 hanno influito molto sul nostro export, però nel 2026 vediamo un segnale positivo, con gli Stati Uniti che crescono al 22%. Un mercato che sembrava ormai chiuso ha riaperto le porte alla manifattura italiana”. Sono le parole di Maria Cristina Squarcialupi, presidente di Confindustria Federorafi, a Vicenzaoro September 2026, il salone internazionale dell’oreficeria e della gioielleria firmato IEG – Italian Exhibition Group, in programma fino all’8 settembre nel quartiere fieristico di Vicenza.

–

economia

webinfo@adnkronos.com (Web Info)

The post Fiere, Vicenzaoro: Squarcialupi (Federorafi): “export Stati Uniti segna +22%” appeared first on Key4biz.

https://www.key4biz.it/fiere-vicenzaoro-squarcialupi-federorafi-export-stati-uniti-segna-22/586343/

Zero-day Magento e Adobe Commerce: StyleSmuggler sfruttato attivamente, Adobe non ha ancora rilasciato la patch

Dal 4 settembre 2026 un attacco senza correzione ufficiale colpisce i negozi Magento Open Source aggiornati. Le mitigazioni disponibili sono di terze parti. Per gli e-commerce italiani si aprono due questioni giuridiche: la notifica al Garante e la responsabilità dell'agenzia.

Dal 4 settembre 2026 gli e-commerce basati su Magento Open Source e Adobe Commerce sono esposti a un attacco attivo. Il produttore non ha ancora pubblicato una correzione. La vulnerabilità, chiamata **StyleSmuggler** dalla società olandese Sansec che l'ha scoperta, permette a un attaccante non autenticato di eseguire codice sul server del negozio e di installare una backdoor persistente.

Al 6 settembre Adobe non ha pubblicato avvisi, identificativi CVE, patch o soluzioni temporanee. L'indice dei bollettini di sicurezza di Adobe Commerce si ferma all'aggiornamento dell'11 agosto (APSB26-92). Quel bollettino correggeva sette CVE, tra cui un'escalation di privilegi non autenticata con punteggio CVSS 9.1 (CVE-2026-71362), e dichiarava che Adobe non era a conoscenza di exploit in circolazione. Secondo Sansec, la prossima release di sicurezza è prevista per l'8 settembre, ma non è noto se coprirà questo difetto.

Questo articolo non ripercorre la cronaca. Si concentra sul vuoto tra la scoperta e la patch. Cosa può fare oggi un esercente italiano che tratta dati di pagamento? Quali limiti

hanno le mitigazioni non ufficiali? Quali obblighi giuridici scattano quando la compromissione è probabile ma non accertata?

Cosa è StyleSmuggler

La cronologia dell'avviso di Sansec fissa la prima esecuzione confermata dell'exploit alle 22:20 UTC del 4 settembre. Alle 22:40 Sansec ha individuato la campagna; alle 23:10 il suo scanner eComscan ha segnalato l'impianto su negozi non collegati tra loro. Nelle ore successive Sansec ha riprodotto l'intera catena su installazioni pulite di Magento Open Source 2.4.7, 2.4.8 e 2.4.9. Le regole di blocco del suo prodotto Shield sono entrate in funzione il 5 settembre alle 07:15 UTC. L'avviso è uscito lo stesso giorno, prima del completamento dell'analisi, perché i negozi venivano compromessi in quel momento.

L'attacco abusa del sistema di template di Magento, in particolare delle proprietà styles, per aggirare le protezioni esistenti. Si svolge in due fasi:

1. **Iniezione.** L'attaccante fa scrivere codice PHP in un file che Magento stesso genera. Sansec cita i rapporti di errore in var/report/. Disrex Group, società olandese di hosting e sviluppo Magento, ha gestito la risposta a due negozi compromessi. In entrambi i casi ha osservato l'avvelenamento di var/log/system.log: l'attaccante invia un codice negozio non valido e Magento lo registra così com'è. Secondo Disrex questa fase non è filtrabile a livello di server web, perché è indistinguibile da un'integrazione malfunzionante.
2. **Esecuzione.** L'attaccante provoca l'invio dell'email standard "Payment Transaction Failed Reminder". Il codice iniettato viene eseguito mentre Magento prepara il messaggio. Nessuno deve aprire l'email; l'attacco riesce anche se la consegna fallisce. L'assenza di

messaggi in casella non è quindi una prova di sicurezza.

La ricostruzione del meccanismo, pubblicata da Disrex in un documento dedicato, è un'interpretazione indipendente. Secondo questa lettura, una direttiva {{block}} nel testo iniettato conduce, attraverso una catena di classi native di Magento, fino a codice pensato per il solo compilatore di dependency injection da riga di comando. Quel codice termina con un include su un percorso scelto dall'attaccante: il log avvelenato un istante prima. Disrex ha corretto una prima versione che identificava un punto di ingresso sbagliato. Sansec non ha confermato la ricostruzione né pubblicato la catena completa; Disrex non ha diffuso la richiesta assemblata. Per le stesse ragioni questo articolo non riporta dettagli riproducibili.

Una volta ottenuta l'esecuzione, un dropper PHP prova in ordine sei funzioni di avvio processo (shell_exec, exec, system, passthru, proc_open, popen) e usa la prima disponibile. Poi scarica e avvia l'impianto: un binario Rust statico e privo di simboli di circa 1,9 MB, per x86-64 e arm64. Il file viene installato in ~/.local/share/.gvfsd/gvfsd-user, nella home dell'utente del sito e non nella cartella web. Il processo si maschera con il nome [kworker/u:8:0], tipico di un thread del kernel Linux. Una voce cron lo riavvia ogni cinque minuti; è scritta direttamente nel file di spool, così il registro di sistema non mostra alcuna sostituzione del crontab.

Il perimetro reale: perché le patch di agosto non proteggono

Il dato che più dovrebbe preoccupare i responsabili IT è il profilo della prima vittima documentata da Sansec. Girava su Magento 2.4.6-p15, con le patch di luglio e agosto 2026 applicate e security:patch-status pulito. È il livello più alto che Adobe distribuisce per la linea 2.4.6, quello che il

bollettino di agosto etichetta 2.4.6-2026-aug. Secondo la cronologia delle versioni, il supporto ordinario di quella linea è terminato l'11 agosto 2026, con supporto esteso fino ad agosto 2027. Essere aggiornati non ha protetto.

Il secondo caso documentato è l'opposto. Il negozio 2.4.7-p2 gestito da Disrex girava su un livello del 13 agosto 2024, otto livelli indietro rispetto al 2.4.7-p10 del 12 maggio 2026. L'esito è stato lo stesso. Come scrive Disrex, il livello di patch non dice nulla sull'esposizione.

Il perimetro noto al 6 settembre è il seguente:

- **Vulnerabile per riproduzione diretta:** Magento Open Source 2.4.7, 2.4.8, 2.4.9 (Sansec).
- **Compromesso in attacchi reali:** 2.4.6-p15 (Sansec), 2.4.7-p2 (Disrex).
- **Non verificato:** Adobe Commerce e Adobe Commerce on Cloud. L'avviso Sansec li dichiara interessati, ma riporta riproduzioni solo su Magento Open Source. Adobe non ha confermato quali versioni siano coinvolte. Vanno trattate come esposizione sconosciuta, non come sicure.
- **Fuori perimetro:** Magento 1, fuori supporto dal 2020. Non esistono dati e le mitigazioni descritte più avanti non sono state provate.

La cronologia di Disrex aggiunge un elemento che va oltre il caso specifico. Il suo primo negozio è stato colpito alle 23:10 UTC del 4 settembre, cinquanta minuti dopo la prima esecuzione confermata a livello mondiale e otto ore prima che esistesse qualsiasi regola di blocco. Nessun livello di patch e nessuna firma avrebbero coperto quella finestra. È l'argomento più forte a favore delle misure di sistema indipendenti dalla vulnerabilità, descritte più avanti.

Non esistono statistiche ufficiali sulla diffusione di Magento in Italia. Chi voglia stimare l'esposizione nazionale può usare servizi di rilevamento tecnologico come BuiltWith o

W3Techs con filtro geografico. Questi strumenti contano i domini, non le installazioni, e non distinguono in modo affidabile Open Source da Adobe Commerce. La domanda pratica è un'altra: il mio sito espone l'endpoint /graphql e quale vetrina lo usa? Vale anche ricordare che StyleSmuggler non è un caso isolato. A giugno una falla nel modulo di terze parti Mirasvit Full Page Cache Warmer (CVE-2026-45247), segnalata in questa rassegna, apriva anch'essa a esecuzione di codice remota non autenticata sui negozi Magento e Adobe Commerce, ed è stata inserita da CISA nel catalogo delle vulnerabilità sfruttate. La differenza è che StyleSmuggler colpisce il core della piattaforma, non un'estensione, e non ha una patch.

Indicatori di compromissione e verifica

Il primo passo, prima di qualsiasi mitigazione, è verificare se il negozio è già compromesso. Applicare regole di blocco su un server infetto non serve: l'impianto è dentro e si riavvia da solo.

Gli indicatori pubblicati da Sansec e nell'elenco di Disrex, aggiornato nel corso del 5 settembre, convergono su questi elementi:

- **Processo:** [kworker/u:8:0] di proprietà di un utente non root. Un vero thread del kernel appartiene sempre a root e non ha memoria residente. Un nome tra parentesi quadre sull'utente del sito, con memoria reale, è l'impianto. L'impianto imposta la riga di comando alla stringa letterale, quindi un controllo sul campo comm del processo non trova nulla; va letto args.
- **File:** ~/.local/share/.gvfsd/gvfsd-user, ~/.local/share/.gvfsd/.gvfsd_<8hex>.lock, /tmp/.gvfsd_<8hex>.lock, /tmp/.kw_<random>.
- **Cron:** */5 * * * * exec <home>/.local/share/.gvfsd/gvfsd-user, con una variante che punta a /tmp/.kw_. Su un

negozio la stessa riga compariva 1.728 volte e tornava entro un secondo dalla rimozione.

- **Hash SHA-256:** Sansec pubblica due campioni (e315687a...a26a7 e b79dfdc1...51420). Disrex ne aggiunge uno trovato su disco in entrambi i negozi (8334b434...d06ef) e uno diverso in esecuzione in memoria su uno di essi (251fabd5...bf220). L'operatore aggiorna l'impianto in memoria: va calcolato l'hash anche di /proc/<pid>/exe.
- **Rete:** 247.cdnflare[.]xyz (host di scaricamento), 99.84.67[.]186:443 (comando e controllo via WebSocket su TLS), windwsecurity[.]run:443 (shell remota). Tre domini imitano server NTP con traffico UDP sulla porta 123: ntp.timesysnc[.]net, time.microsft[.]run, pool.microsft[.]studio. Le imitazioni di Microsoft sono evidenti e vanno cercate nei log DNS.
- **Sorgenti:** 88.216.72[.]181 (Sansec, vista su più vittime), 5.181.86[.]133 e 91.238.181[.]19 (Disrex, traffico in massa). La seconda è la sorgente quasi esclusiva della seconda ondata, nel pomeriggio del 5 settembre.
- **Firme di richiesta:** POST /graphql?styles[...]= con codifica percentuale; POST /paypal/transparent/response/ con codice PHP nella stringa di query. C'è poi la richiesta ordinaria GET /customer/section/load/, che nella variante osservata da Disrex portava il payload nell'intestazione User-Agent. Le richieste di exploit arrivano con user agent python-requests (2.15.0 nella prima ondata, 2.32.4 nella seconda), mai con un browser.
- **Prova di esecuzione:** secondo Disrex il payload racchiude il proprio output in un delimitatore MG<20 hex>::...::/MG<20 hex>. La sua presenza nei log prova che il codice è stato eseguito, non solo inviato. Un secondo segnale è un TypeError di array_merge() con argomento intero in system.log, subito dopo l'include: indica che l'exploit è riuscito. La variante più silenziosa restituisce un array vuoto e non lascia

traccia.

Tre avvertenze emerse sul campo meritano attenzione. Primo: il controllo pubblicato da Sansec cerca X_TRACE_ in var/report/. Entrambe le infezioni gestite da Disrex passavano da var/log/system.log e sarebbero sfuggite; vanno ispezionate entrambe le cartelle. Secondo: l’intestazione di innesco è cambiata nella stessa giornata, da X-TRACE-<10 hex> al mattino a X-<12 hex> al pomeriggio, con valore rigenerato a ogni richiesta. Una rilevazione ancorata alla stringa letterale è diventata cieca in un giorno: la ricerca deve intercettare la forma. Terzo: su uno dei due negozi l’impianto non ha aperto alcuna connessione in uscita. Ha letto le sessioni Magento dall’istanza Redis locale con 28 connessioni a 127.0.0.1:6379. Due catture di traffico di oltre 200 MB ciascuna non contenevano un solo pacchetto verso gli indirizzi noti. L’assenza di traffico sospetto non prova nulla.

Sugli scanner c’è un dato discordante, da riportare come tale. Sansec raccomanda il proprio eComscan e ha rilasciato la versione 1.9.7, che termina i processi per i clienti Shield. Disrex riferisce invece che su uno dei negozi infetti lo scanner, con i controlli su processi in background e attività pianificate attivi, ha dato esito pulito con 1.728 righe cron malevole presenti. Disrex non indica versione e orario dell’esecuzione. In ogni caso gli scanner puntati sulla sola cartella web non vedono un impianto installato un livello sopra.

Un segnale indiretto: raffiche inattese di email “Payment Transaction Failed Reminder” sono un motivo per indagare, anche se pagamenti rifiutati legittimamente generano la stessa notifica.

Mitigazioni disponibili ora

In assenza di una correzione del produttore, le opzioni si dispongono su tre livelli. L’ordine riflette la robustezza. La

ragione sta nella struttura della catena come la descrive Disrex. Il punto di ingresso non può essere protetto in modo pulito, perché il codice che elabora il testo iniettato prepara anche ogni email transazionale. Un controllo lì romperebbe le conferme d'ordine. Restano il blocco del punto di uscita e le misure che non dipendono dalla conoscenza della vulnerabilità.

Livello 1: misure di sistema indipendenti dalla catena. Sono le due misure che Disrex mette davanti a ogni altra regola del proprio repository. Su uno dei negozi compromessi le prime quattro delle sei funzioni tentate dal dropper erano disabilitate, ma proc_open no. È stata quella ad avviare l'impianto, e open_basedir non ha contenuto il processo figlio, che una volta avviato gira fuori da PHP. Una lista disable_functions che ferma cinque funzioni su sei non ferma nulla. Le misure sono quindi due: aggiungere proc_open e le altre cinque funzioni a disable_functions in PHP; montare /tmp, /var/tmp e /dev/shm con opzione noexec, così che un binario scaricato non possa essere eseguito. Entrambe vanno provate in staging, perché alcune estensioni legittime dipendono da proc_open.

Livello 2: disattivazione temporanea di GraphQL. È il consiglio interinale di Sansec per i negozi che non usano Shield. Le vetrine headless e PWA richiedono GraphQL; la maggior parte delle vetrine classiche e Hyvä non lo usa. Un conteggio delle richieste POST /graphql nei log di accesso dice se la disattivazione è praticabile. È la strada scelta anche da alcuni fornitori di hosting. Nexcess, marchio di Liquid Web, ha comunicato la sera del 5 settembre un blocco completo delle richieste GraphQL su tutti gli ambienti Magento e Adobe Commerce gestiti. Ha avvertito che le vetrine headless e PWA possono risentirne. Un esercente italiano su hosting gestito potrebbe quindi trovarsi con GraphQL bloccato senza averlo deciso: va verificato con il fornitore.

Livello 3: patch e regole non ufficiali. Tre soggetti hanno

pubblicato mitigazioni il 5 settembre:

- **Disrex Group** ha rilasciato regole nginx e Apache che bloccano le richieste con i parametri dell'exploit nella stringa di query. Ha pubblicato inoltre un guard per tre metodi degli scanner di dependency injection di Magento (ArrayScanner, ClassesScanner, XmlInterceptorScanner), che impedisce loro di girare fuori dalla riga di comando. Il guard è disponibile anche come patch composer che si riapplica a ogni deploy. Secondo Disrex, la patch è stata verificata in prova a secco sui tag 2.4.6, 2.4.7, 2.4.8 e 2.4.9. È stata poi applicata su installazioni attive 2.4.7-p2 e 2.4.8-p4, con setup:di:compile e vetrina funzionanti. Il repository dichiara i propri limiti. È stato scritto con assistenza di intelligenza artificiale durante un incidente e non è stato revisionato. Le regole Apache non sono mai state eseguite su un server Apache reale; nulla è stato provato su hosting condiviso, Docker o pannelli di controllo. Una prova su un negozio attivo ha mostrato che le regole per il server web si aggirano spostando gli stessi parametri nel corpo di una POST. Fermano la campagna come è condotta oggi, non la vulnerabilità. Disrex avverte che il guard non è una correzione completa, perché in Magento esistono altri punti di include non proteggibili allo stesso modo.
- **ProxiBlue** ha pubblicato su GitHub tre patch con lo stesso guard sugli stessi tre metodi, in modo indipendente. Disrex le cita come conferma incrociata e raccomanda di applicare una sola delle due soluzioni.
- **Graycore LLC** ha pubblicato un modulo Magento su GitHub e Packagist che irrobustisce tre punti della catena. La direttiva {{block}} dei template email rifiuta i blocchi di backend. Il generatore di URL delle righe di griglia valida la classe prima di costruirla. I tag di apertura PHP nei rapporti di errore delle Web API vengono spezzati. L'ultima release (2.0.0) aggiunge il rifiuto

di template caricati da stream wrapper o percorsi con byte nullo e rimuove un override di un resolver PayPal presente nella prima versione. L’autore avverte che il pacchetto cambierà mentre prova nuovi livelli di mitigazione e che va letto il changelog prima di ogni aggiornamento. Precisa che si tratta di irrobustimento e non di correzione: la vulnerabilità resta aperta.

Va detto con chiarezza: né Sansec né Adobe hanno confermato che gli scanner DI siano il punto in cui la catena termina. Chi applica queste patch lo fa a proprio rischio, sulla base di una ricostruzione indipendente non convalidata dal produttore.

Se il negozio è già compromesso. La guida di pulizia di Disrex fissa un ordine. Prima confermare e preservare le prove; poi contenere, cercare altre persistenze e ruotare i segreti; quindi decidere se pulire o ricostruire. Le mitigazioni si applicano solo alla fine. Tre regole contano più delle altre. Rimuovere la voce cron prima di terminare il processo, perché il processo la ripristina. Non riavviare la macchina, perché la copia in /proc può essere l’unico binario superstite. Non eseguire composer install come pulizia, perché sovrascrive le date di modifica che documentano cosa è stato toccato.

La ricerca va estesa oltre il crontab: timer systemd anche per utente, at, auto_prepend_file, file PHP in pub/media, chiavi SSH sconosciute. Dentro Magento: account amministrativi non riconosciuti, integrazioni e token API, script iniettati in core_config_data, blocchi CMS modificati. Segue lo svuotamento delle sessioni, che l’impianto leggeva. Vanno poi ruotate la crypt/key in app/etc/env.php, la password del database, tutte le password amministrative, le chiavi API dei fornitori di pagamento e ogni altra credenziale in quel file. Disrex indica anche quando la ricostruzione è preferibile alla pulizia. I casi sono quattro: negozio non sotto controllo di versione; file modificati non spiegabili in vendor/ o app/code/; impianto attivo per giorni; impossibilità di datare l’inizio

della compromissione.

Un ultimo elemento sulla campagna. L’elenco di Disrex, nella revisione più recente, conta 27 indirizzi sorgente distinti su tre negozi e due ondate. La cifra era 26 nella prima versione ed è stata corretta; il README dello stesso repository riporta 28. Tre indirizzi appartengono a infrastrutture di hosting che inviavano in massa; il resto è un insieme di proxy residenziali con due-sei richieste ciascuno. Disrex raccomanda di non bloccare in blocco gli indirizzi residenziali: sono connessioni di consumatori affittate o compromesse, e il blocco costerebbe clienti reali. Bloccare il solo indirizzo citato nell’avviso Sansec avrebbe fermato meno di un quarto del traffico osservato. È un dato di una sola fonte, ma è coerente con l’infrastruttura distribuita tipica delle campagne di web skimming degli ultimi anni.

Riquadro giuridico: cosa scatta quando la compromissione è probabile ma non accertata

Questa sezione ha finalità informativa e non sostituisce il parere di un legale.

Notifica al Garante. L’articolo 33 del GDPR impone al titolare di notificare la violazione all’autorità di controllo senza ingiustificato ritardo e, ove possibile, entro 72 ore da quando ne è venuto a conoscenza. L’obbligo cade se è improbabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche. Il nodo, in una situazione come questa, è il momento della “conoscenza”. Le Linee guida 9/2022 dell’EDPB (versione 2.0, adottata il 28 marzo 2023) lo definiscono al paragrafo 31. Il titolare è a conoscenza quando ha un ragionevole grado di certezza che un incidente di sicurezza abbia compromesso dati personali. Il paragrafo 34 ammette un breve periodo di indagine iniziale,

durante il quale il titolare non è ancora “a conoscenza”. Il paragrafo 36 precisa però che le verifiche preliminari vanno completate poco dopo il primo allarme, e possono richiedere più tempo solo in casi eccezionali. Il paragrafo 40 aggiunge che chi non agisce tempestivamente e poi scopre la violazione rischia la contestazione di mancata notifica. L’esempio 3 del paragrafo 33 descrive il caso di specie: un titolare rileva una possibile intrusione, controlla i sistemi, conferma la compromissione dei dati e da quel momento è a conoscenza.

Tradotto in pratica. Un esercente che rileva gli indicatori sopra descritti ha superato la soglia, perché l’impianto leggeva le sessioni e aveva accesso a credenziali e chiavi di pagamento; le 72 ore partono da lì. Un esercente che non rileva indicatori, ma non può escludere l’esposizione tra il 4 settembre e l’applicazione delle mitigazioni, si trova nella fase di indagine. Deve avviarla subito, documentarla con date e attività svolte e chiuderla in fretta. L’articolo 33, paragrafo 5, impone di registrare ogni violazione; il paragrafo 125 delle Linee guida chiede di motivare per iscritto anche la decisione di non notificare. L’articolo 33, paragrafo 4, consente la notifica per fasi. Il paragrafo 57 delle Linee guida indica proprio gli incidenti informatici che richiedono analisi forense come il caso tipico in cui il quadro completo manca nelle 72 ore. Il paragrafo 60 ricorda infine che non c’è sanzione per aver notificato un incidente che poi si rivela non essere una violazione.

Comunicazione agli interessati. L’articolo 34 richiede la comunicazione agli interessati quando la violazione è suscettibile di presentare un rischio elevato. La compromissione di un server che gestisce pagamenti rientra quasi sempre in questa categoria. L’esempio ii dell’allegato B delle Linee guida (attacco a un servizio online con esfiltrazione di dati) prevede la notifica all’autorità e, a seconda della gravità, agli interessati. L’esenzione per dati cifrati (paragrafi 76-78) vale solo se la chiave non è stata

compromessa. È da escludere quando la crypt/key di Magento era leggibile dall'utente del sito con cui girava l'impianto. Le stesse Linee guida avvertono che, se la chiave risulta compromessa in un secondo momento, l'obbligo di notifica si riattiva.

Ripartizione delle responsabilità. Nella filiera tipica di un e-commerce italiano l'esercente è titolare del trattamento. L'agenzia che gestisce l'installazione e il fornitore di hosting sono di regola responsabili ai sensi dell'articolo 28. Due conseguenze pratiche. La prima: l'articolo 33, paragrafo 2, obbliga il responsabile a informare il titolare senza ingiustificato ritardo. Il paragrafo 44 delle Linee guida chiarisce che il responsabile non deve prima valutare il rischio; deve solo accertare che la violazione c'è stata e avvisare. Da quel momento il titolare è considerato a conoscenza. Un'agenzia che ha visto gli indicatori sui server dei clienti e non lo ha comunicato ha quindi una responsabilità autonoma. L'esempio vii dell'allegato B (fornitore di hosting che scopre un difetto nel proprio codice) mostra che l'obbligo scatta anche prima di aver accertato lo sfruttamento effettivo.

La seconda: il contratto di servizio è il luogo in cui si decide chi doveva applicare le mitigazioni e in quanto tempo. Molti contratti prevedono l'applicazione delle patch ufficiali entro un certo termine, ma tacciono sul caso in cui una patch ufficiale non esista. Chi decide se applicare una patch di terze parti non revisionata? Chi risponde se quella patch rompe il negozio, o se la mancata applicazione lo espone? Sono domande che i contratti in essere raramente affrontano e che questa vicenda rende urgenti. L'articolo 82, sul diritto al risarcimento, ripartisce la responsabilità civile tra titolare e responsabile in base al rispettivo contributo al danno.

PCI DSS. Per chi è soggetto allo standard, la versione 4.0.1 richiede al requisito 6.3.3 che le patch per le vulnerabilità critiche siano installate entro un mese dal rilascio. Il

requisito presuppone una patch. In sua assenza operano il requisito 6.3.1 (identificazione delle vulnerabilità tramite fonti riconosciute, compresi gli avvisi dei CERT, e loro classificazione per rischio) e i controlli compensativi. I requisiti 6.4.3 e 11.6.1 sono qualificati dallo standard come buone pratiche fino al 31 marzo 2025 e obbligatori da quella data. Il primo impone autorizzazione, integrità e inventario di tutti gli script caricati nelle pagine di pagamento. Il secondo richiede un meccanismo che rilevi le modifiche non autorizzate alle intestazioni HTTP e agli script così come li riceve il browser del cliente, eseguito almeno ogni settimana. Sono esattamente i controlli che intercetterebbero uno skimmer inserito dopo una compromissione via StyleSmuggler. Il requisito 12.10.1 impone infine un piano di risposta agli incidenti, da attivare al primo indicatore.

NIS2. Il singolo negozio online non rientra tra i soggetti del D.Lgs. 138/2024. L'allegato II del decreto include invece i fornitori di mercati online tra i fornitori di servizi digitali. Un fornitore di hosting che gestisce molti e-commerce può rientrare nel perimetro come fornitore di servizi cloud o di data center (allegato I, settore 8, infrastrutture digitali). Un'agenzia che amministra le installazioni Magento dei clienti può rientrarvi come fornitore di servizi gestiti o di servizi di sicurezza gestiti (allegato I, settore 9, gestione dei servizi TIC business-to-business). Restano fermi i criteri dimensionali e la registrazione presso l'ACN. In quel caso l'articolo 25 prevede tre adempimenti per gli incidenti significativi. Una pre-notifica al CSIRT Italia entro 24 ore dalla conoscenza; una notifica entro 72 ore con valutazione iniziale e indicatori di compromissione; una relazione finale entro un mese. Il comma 3 precisa che la notifica non espone chi la effettua a una responsabilità maggiore di quella derivante dall'incidente. I commi 9 e 10 prevedono la comunicazione ai destinatari dei servizi sia degli incidenti sia delle minacce significative, con le misure di mitigazione adottabili. Per un fornitore in perimetro,

StyleSmuggler è una minaccia significativa da comunicare ai clienti anche prima di qualsiasi compromissione accertata.

Cosa aspettarsi dall’8 settembre

La release di sicurezza di Adobe dell’8 settembre è il primo momento in cui il quadro può cambiare. Tre scenari sono possibili. La release include una correzione con relativo CVE. Oppure non la include, e Adobe pubblica un bollettino fuori ciclo nei giorni successivi. Oppure Adobe pubblica prima una soluzione temporanea ufficiale e poi la patch. In ogni caso la finestra successiva va preparata ora.

Chi ha applicato patch non ufficiali deve pianificarne la rimozione prima di installare quella del produttore. La sovrapposizione di modifiche agli stessi file può produrre conflitti o, peggio, l’illusione di aver aggiornato; la patch composer di Disrex prevede un percorso di ritorno esplicito. Chi ha disattivato GraphQL deve avere pronto il piano di riattivazione, con prove funzionali sul pagamento. Chi ha pulito un negozio compromesso deve ricordare che la patch non rimuove una backdoor già installata né invalida credenziali già sottratte. La rotazione dei segreti resta necessaria anche dopo l’aggiornamento.

Resta il punto più scomodo. Un e-commerce compromesso tra il 4 settembre e l’applicazione delle mitigazioni può aver perso dati di pagamento senza che nulla lo segnali, perché l’impianto può operare senza traffico verso indirizzi noti. Per quegli esercenti l’8 settembre non chiude l’incidente. Apre la fase in cui bisogna decidere, con i log alla mano e con un legale al fianco, se e cosa notificare.

https://www.ictsecuritymagazine.com/notizie/zero-day-magento-stylesmuggler-adobe-commerce/

MikroTik RouterOS: la catena “MikroTrick” è sfruttata attivamente, patch urgente

Bastano un servizio SSH esposto su Internet e nessuna credenziale. Con questi soli requisiti, almeno dal 2 settembre, alcuni attaccanti prendono il controllo completo di dispositivi MikroTik RouterOS e lasciano come firma un account amministrativo chiamato ops. Lo ha confermato il 5 settembre 2026 CERT Polska, il team che ha scoperto le vulnerabilità e ha chiamato la catena “MikroTrick”. MikroTik ha pubblicato le versioni corrette su tutti i canali e raccomanda di aggiornare subito.

Cosa è successo

Il team polacco ha individuato sei vulnerabilità in RouterOS, due delle quali critiche, e ne ha coordinato la divulgazione. Combinandone due, un attaccante ottiene privilegi amministrativi completi senza autenticarsi, purché il dispositivo esponga SSH su rete pubblica. Le falle riguardano il server e il client SSH, il servizio bandwidth-test, la gestione dei certificati X.509 e l’interfaccia WebFig.

Secondo i record NVD, sono interessate tutte le release RouterOS 6.x precedenti alla 6.49.21, le 7.x precedenti alla 7.23.4 e la 7.24 precedente alla 7.24.2. I punteggi che seguono sono i CVSS 4.0 assegnati da CERT Polska, ente assegnatario delle CVE; NVD non ha ancora pubblicato una propria valutazione.

Le tre vulnerabilità principali sono:

- **CVE-2026-67276** (CVSS 9.2): elusione dell’autenticazione SSH. RouterOS non confrontava per intero la chiave pubblica RSA associata a un utente. Chi conosceva il nome utente e il modulo pubblico della chiave poteva costruire una chiave diversa e autenticarsi senza la chiave privata, con i privilegi dell’account bersaglio.
- **CVE-2026-86060** (CVSS 9.2): elevazione dei privilegi di sessione tramite un nome utente costruito ad arte. Il meccanismo di login SSH gestiva male i nomi utente che iniziano con un carattere non ammesso; l’attaccante poteva così modificare la maschera dei permessi e ottenere una sessione con pieni diritti amministrativi.
- **CVE-2026-67277** (CVSS 8.8): il servizio bandwidth-test permetteva a una connessione non autenticata di raggiungere uno stato riservato agli utenti autenticati. Insieme a due ulteriori difetti (esposizione di dati non inizializzati e integer underflow nella verifica delle dimensioni), consentiva di leggere memoria del kernel o di provocare un riavvio remoto del sistema.

L’elenco completo delle sei CVE è disponibile su una pagina dedicata di CERT Polska. Il team spiega di aver anticipato la pubblicazione per una ragione precisa: i pacchetti corretti erano già pubblici e il confronto tra le versioni aveva permesso alla comunità di ricostruire alcune correzioni. Non ha diffuso codice di exploit né dettagli utili ad automatizzare gli attacchi.

Gli attacchi osservati e gli indicatori di compromissione

CERT Polska dichiara di aver ricevuto conferma che la catena MikroTrick viene usata per assumere il controllo di dispositivi con SSH esposto e che le patch bloccano gli attacchi osservati. Gli attacchi riusciti, compresa la creazione dell’account ops, provengono dall’indirizzo IP

82.192.72.4 e risalgono almeno al 2 settembre. Un secondo indirizzo, 103.102.31.18, è stato usato in tentativi di sfruttamento della stessa catena.

Nei log di RouterOS l'attacco lascia due tracce riconoscibili: un accesso fallito per l'utente -2 via SSH, seguito dalla creazione di un nuovo utente da parte di ssh:-2@<ip>. La presenza di uno qualsiasi di questi elementi va indagata subito. La loro assenza, avverte il team, non esclude un'attività non autorizzata.

La risposta del vendor

Il bollettino di sicurezza MikroTik, datato 3 settembre 2026, definisce l'aggiornamento importante e afferma che la maggior parte delle configurazioni non è a rischio. Conferma che la correzione è inclusa in RouterOS 7.25beta3, 7.24.2, 7.23.4 e 6.49.21. Il 4 settembre è uscita anche la 7.23.5 per il ramo long-term: non aggiunge correzioni di sicurezza, ma risolve una regressione del DHCP IPv6 introdotta dalla 7.23.4, ed è quindi la versione a cui puntare. Il vendor non ha ancora pubblicato dettagli tecnici, per dare tempo agli amministratori di aggiornare. Per gli utenti domestici, scrive, il rischio non è immediato, ma consiglia comunque a tutti di aggiornare. CERT Polska riferisce inoltre che MikroTik, per la prima volta, ha inviato una notifica push agli utenti dell'app mobile ufficiale.

Le release corrette utilizzano anche il meccanismo Flagged, presente da tempo nel device-mode di RouterOS. All'avvio il sistema analizza la configurazione alla ricerca di segni noti di modifiche non autorizzate; disabilita le voci sospette, scrive un messaggio critico nel log e imposta lo stato "Flagged", descritto nella pagina dedicata del manuale. CERT Polska precisa però tre cose: il meccanismo rileva solo alcune tracce; l'assenza del marcatore non prova che il dispositivo sia integro; non si può escludere che il vendor abbia corretto

anche vulnerabilità ignote al team e non descritte nelle note di rilascio.

Perché conta per l’Italia

RouterOS è usato, in Italia come altrove, da operatori ISP e WISP, in reti aziendali e di PMI e in contesti edge. La catena colpisce esattamente i dispositivi che espongono SSH su Internet. Un dato di contesto, datato ma indicativo, viene dal rapporto Eclypsium del dicembre 2021: su oltre due milioni di dispositivi MikroTik con interfacce di gestione raggiungibili dalla rete, circa 300.000 risultavano vulnerabili a falle note. L’Italia figurava tra i cinque Paesi più interessati, con Cina, Brasile, Russia e Indonesia.

Al momento non risultano vittime italiane confermate pubblicamente e CSIRT Italia non ha pubblicato un avviso su questa catena. Lo stesso CSIRT era però già intervenuto sull’ecosistema MikroTik nell’ultimo anno. Il 29 ottobre 2025 ha pubblicato un alert sul componente WebFig di RouterOS e SwitchOS; il 17 gennaio 2025 un bollettino su una botnet di dispositivi MikroTik compromessi.

Un router o gateway compromesso offre all’attaccante persistenza a livello di rete, intercettazione o deviazione del traffico, tunnel verso l’esterno e movimento laterale verso i sistemi interni. È il modello, ormai documentato, dei dispositivi di rete usati come infrastruttura offensiva. Va aggiunta una considerazione normativa: gli obblighi di notifica NIS2 al CSIRT Italia sono operativi dal 15 gennaio 2026, quindi un dispositivo di frontiera compromesso può diventare rapidamente un incidente da segnalare per i soggetti in perimetro.

Cosa fare subito

1. **Aggiornare senza attendere** a RouterOS 7.24.2 (stable),

7.23.5 (long-term; la 7.23.4 contiene la stessa correzione ma soffre della regressione DHCP IPv6), 6.49.21 (long-term v6) o 7.25beta3, o a versioni successive.
2. **Dopo l’aggiornamento**, controllare nel log l’eventuale messaggio di compromissione e il valore del marcatore Flagged con /system/device-mode/print. Verificare la presenza di utenti sconosciuti (in particolare ops), script, attività dello scheduler, proxy e tunnel non riconosciuti.
3. **Se la patch non è applicabile subito**, disattivare i servizi esposti o limitarne l’accesso alle sole reti di gestione fidate, in particolare SSH, WWW/WWW-SSL e il server bandwidth-test. Evitare di avviare connessioni TLS dal dispositivo non aggiornato e di usare i client SSH integrati (/system ssh e /system ssh-exec) verso host o reti non fidati. Sono misure temporanee che non sostituiscono la patch.
4. **In caso di compromissione sospetta o confermata**, isolare il dispositivo e mettere al sicuro log e configurazione prima di qualsiasi ripristino. Segnalare l’evento al CSIRT competente. Ripristinare le impostazioni di fabbrica, riconfigurare da una configurazione verificata e cambiare password, chiavi e altri segreti. Non ripristinare alla cieca una copia di sicurezza completa proveniente da un dispositivo potenzialmente compromesso; non cancellare lo stato Flagged prima di aver completato l’analisi.

Vulnerabilità trovate con l’aiuto degli LLM

Un dettaglio di metodo merita attenzione. CERT Polska riferisce di aver individuato le vulnerabilità con il supporto dei modelli GPT-5.5-cyber e GPT-5.6-sol, disponibili al team nell’ambito del programma OpenAI Government and Trust Agency

Collaboration. I modelli hanno lavorato in un ambiente di ricerca agentico su un laboratorio isolato. Hanno automatizzato la creazione delle macchine di prova, il confronto tra versioni e l'analisi di RFC e codice binario. Particolarmente efficace, secondo il team, è stata la modellazione dei protocolli come macchine a stati, per verificare cosa accade quando una fase viene saltata, ripetuta o eseguita nell'ordine sbagliato.

Ogni ipotesi ha però richiesto conferma su sistemi RouterOS reali, test di controllo negativi e valutazione d'impatto da parte dei ricercatori. I modelli, conclude CERT Polska, hanno accelerato l'analisi senza sostituire la verifica umana. È una lezione coerente con quella portata al Forum ICT Security 2025 dal Politecnico di Torino sugli agenti AI applicati all'individuazione delle CVE: l'architettura dell'agente e il controllo umano pesano più del modello.

https://www.ictsecuritymagazine.com/notizie/mikrotik-mikrotrick/

Panzer, il nuovo ransomware-as-a-service che ha già colpito due aziende italiane

Emerso ad agosto 2026, Panzer unisce un programma di affiliazione già maturo, payload per Windows, Linux, ESXi e FreeBSD e doppia estorsione. Tra le prime vittime rivendicate figurano Doimo Cucine e NTE Italia.

Un esordio rapido e strutturato

Nel panorama ransomware la comparsa di una nuova sigla non è, di per sé, una notizia: il ricambio è continuo e molti operatori scompaiono nel giro di poche settimane. Panzer merita attenzione per un motivo diverso: la rapidità con cui ha messo in piedi una piattaforma completa. Secondo il profilo pubblicato il 4 settembre 2026 dalla società di threat intelligence CyberXtron, il leak site del gruppo sulla rete Tor è attivo dal 5 agosto, data della prima osservazione, e in un mese ha pubblicato 16 vittime in almeno 11 Paesi.

La distribuzione geografica non ha un baricentro: tre vittime in Thailandia, due in Italia, due in Indonesia, due in Serbia e una sola in ognuno degli altri Paesi colpiti, cioè Curaçao, Corea del Sud, Spagna, Repubblica Ceca, Germania, Nigeria e Svizzera. Anche i settori sono eterogenei: la tecnologia è in testa con quattro casi, seguita dalla manifattura con tre; poi governo e difesa, agroalimentare, energia e utility, istruzione e retail. È il profilo tipico di una campagna opportunistica, guidata dagli accessi che gli affiliati riescono a procurarsi e non da una scelta mirata di Paesi o settori.

Il conteggio, peraltro, è già superato. Tre tracker indipendenti, SOCRadar, Ransomware.live e l'italiano Ransomfeed, concordano su 19 vittime al 6 settembre. Le ultime due rivendicazioni, del 3 e del 4 settembre, riguardano un ente pubblico indonesiano e un'università tedesca; dopo le 17 rivendicazioni di agosto il ritmo è rallentato, ma il gruppo resta attivo.

Sul numero di Paesi colpiti, invece, i tracker divergono: Ransomware.live ne conta 11, SOCRadar 16, e negli elenchi compaiono Portogallo, Francia e Cipro, assenti dal censimento di CyberXtron. Le differenze dipendono dai criteri di attribuzione geografica, e una stessa vittima può essere

attribuita a Paesi diversi a seconda della piattaforma: il gruppo orologiero Festina, per esempio, è registrato in Spagna da Ransomfeed e in Svizzera da SOCRadar. È un’avvertenza da tenere presente ogni volta che si citano questi numeri. SOCRadar indica inoltre la Russia come Paese di origine del gruppo: un’attribuzione coerente con il divieto di colpire i Paesi della CSI, ma non confermata da altre fonti.

Le vittime italiane

Le due organizzazioni italiane sono censite, con dati coincidenti, sia da Ransomware.live sia da Ransomfeed. La prima è Doimo Cucine, produttore di cucine di design con sede a Nervesa della Battaglia, in provincia di Treviso: la rivendicazione è stata rilevata il 17 agosto e, secondo la scheda di Ransomware.live, il gruppo dichiara di aver esfiltrato 30 GB di dati. La seconda è NTE Italia, società di servizi tecnici e di ingegneria per le telecomunicazioni e la sicurezza dei cantieri, con sede a Catanzaro e uffici a Roma e Catania: è comparsa sul leak site il 21 agosto e il gruppo afferma di aver sottratto 16 GB di dati, descritti come migliaia di documenti sensibili.

Una pubblicazione su un leak site resta una rivendicazione dell’attaccante, non una prova. Nessuna delle due aziende ha confermato pubblicamente l’incidente, e le rivendicazioni di un gruppo appena emerso, privo di uno storico verificabile, vanno trattate con particolare cautela fino a verifica indipendente. La comparsa di due vittime italiane in pochi giorni richiama una dinamica ricorrente nei RaaS di recente formazione: concentrare più bersagli in un breve intervallo per costruire credibilità presso i potenziali affiliati.

Come funziona il programma di

affiliazione

Il tratto più interessante di Panzer non è il malware, di cui si sa ancora poco, ma l'infrastruttura commerciale. L'operazione si presenta come un RaaS semi-aperto: gli aspiranti affiliati presentano domanda tramite un canale Tox e ottengono l'accesso al pannello di controllo solo dopo una selezione. La ripartizione dei proventi è 80/20 a favore dell'affiliato, con la quota della piattaforma trattenuta automaticamente su ogni pagamento. Le regole vietano di colpire organizzazioni nei Paesi della CSI e soggetti coinvolti in abusi su minori; gli account inattivi per più di una settimana vengono disattivati.

Il pannello di controllo descritto da CyberXtron è quello di un servizio già rodato. Comprende il monitoraggio del saldo e delle transazioni, la gestione delle build per le diverse piattaforme, con una chat di negoziazione dedicata a ogni vittima e un generatore integrato di fatture in Bitcoin, un sistema di ticket di assistenza e sotto-account per i team. La pubblicazione dei leak segue un flusso con approvazione preventiva degli operatori, conto alla rovescia e possibilità di mettere in evidenza i casi ritenuti più redditizi. Gli operatori dichiarano inoltre di sottoporre i nuovi affiliati a un monitoraggio automatico durante il primo mese, per individuare ricercatori o forze dell'ordine infiltrati.

Un investimento di questo tipo in strumenti per il reclutamento, i pagamenti e l'autotutela indica un progetto pensato per crescere attraverso operatori esterni, non un gruppo chiuso che conduce in proprio le intrusioni. È la logica del ransomware human-operated portata alle estreme conseguenze: la piattaforma fornisce strumenti e infrastruttura, gli affiliati eseguono le intrusioni. Alcuni osservatori accostano il modello a quello di VanHelsing e di altri RaaS emersi negli ultimi anni.

Cosa si sa, e cosa non si sa, delle tecniche

Sul piano tecnico il quadro è frammentario e il vettore di accesso iniziale non è stato verificato in modo indipendente. Le attività che CyberXtron associa al gruppo, con confidenza medio-bassa, comprendono il dumping delle credenziali del sistema operativo, attacchi di forza bruta, la ricognizione dei servizi di rete, il movimento laterale tramite servizi remoti e account validi, la raccolta di dati dal sistema locale, l'esfiltrazione su protocolli alternativi e la disabilitazione o manomissione degli strumenti di sicurezza. La mappatura di SOCRadar, in parte diversa, aggiunge l'esecuzione tramite interprete di comandi, la persistenza all'avvio e l'inibizione del ripristino di sistema, tecnica che prende di mira le copie shadow e i meccanismi di recupero.

Non esistono al momento indicatori di compromissione confermati, siano essi hash, indirizzi IP, domini o campioni di malware: gli unici indicatori pubblici riguardano l'infrastruttura del leak site e il canale di reclutamento. Ciò che invece dichiarano gli stessi operatori è la copertura dei payload: build per Windows, Linux, VMware ESXi e FreeBSD, con oltre quindici comandi personalizzabili, funzioni anti-rilevamento e un pannello di avvio con monitoraggio in tempo reale dell'operazione. Lo schema è quello della doppia estorsione: i dati vengono esfiltrati prima della cifratura e alcuni campioni finiscono sul leak site come prova.

Perché è rilevante per le organizzazioni italiane

Due caratteristiche rendono Panzer una minaccia concreta per il tessuto produttivo nazionale, al di là dei due casi già noti.

La prima è il supporto a ESXi. Gran parte delle medie e grandi imprese italiane concentra i propri carichi di lavoro su infrastrutture virtualizzate: compromettere un hypervisor significa cifrare in un'unica operazione decine di macchine virtuali e i servizi che vi girano, con tempi di ripristino ben più lunghi rispetto a un attacco limitato agli endpoint Windows. Le build per Linux e FreeBSD allargano ulteriormente la superficie esposta negli ambienti con parchi server misti. Non è un rischio teorico: il CSIRT Italia, nel bollettino dedicato a Qilin, ha già segnalato l'uso di tecniche mirate agli ambienti VMware ESXi da parte di un gruppo il cui impatto sistemico sul Paese è classificato come critico.

La seconda è la doppia estorsione. Backup solidi e testati restano indispensabili per la continuità operativa, ma non neutralizzano il rischio legato alla pubblicazione dei dati sottratti, con le conseguenze reputazionali, contrattuali e regolamentari che ne derivano, comprese le notifiche previste dal GDPR e, per i soggetti che rientrano nel suo ambito di applicazione, dalla NIS2.

Il contesto aggrava il quadro. Secondo Ransomfeed, al 6 settembre le rivendicazioni contro organizzazioni italiane nel 2026 sono già 212, contro le 169 dell'intero 2025, su un totale storico di 850. Nella sola settimana tra il 6 e il 13 agosto, secondo una ricostruzione ripresa anche da Bismark.it, otto gruppi diversi hanno rivendicato 15 vittime italiane. Panzer si inserisce in una fase in cui gli attaccanti puntano soprattutto sulla manifattura, già segnalata dall'ACN come bersaglio privilegiato nei distretti industriali del Nord, e sui fornitori di servizi tecnologici e di telecomunicazione: ne sono esempi NTE Italia e Retelit, quest'ultima colpita da Qilin a fine luglio.

Le priorità difensive

Le raccomandazioni pubblicate da CyberXtron coincidono con le

buone pratiche già consolidate contro il ransomware, ma alcune assumono un peso particolare alla luce delle caratteristiche di Panzer.

Sul fronte delle identità, la priorità è l'autenticazione a più fattori resistente al phishing su tutti gli accessi remoti, le VPN e gli account privilegiati, unita al principio del minimo privilegio e a una revisione periodica degli account amministrativi: le tecniche associate al gruppo ruotano intorno al furto e all'abuso di credenziali valide. Sul fronte architetturale, la segmentazione deve isolare dalle reti utente i controller di dominio, i sistemi di backup e, soprattutto, l'interfaccia di gestione degli hypervisor, confinando i protocolli di amministrazione remota in segmenti dedicati e monitorati.

Contro la doppia estorsione servono controlli sul traffico in uscita e il rilevamento dei trasferimenti anomali di dati: l'esfiltrazione precede la cifratura ed è la finestra più utile per intercettare l'attacco. I backup devono essere immutabili, con almeno una copia offline, isolata dalla rete, e test di ripristino regolari che verifichino l'integrità dei punti di ripristino. Il piano di risposta agli incidenti, infine, dovrebbe prevedere esplicitamente lo scenario di esposizione dei dati, con i flussi legali, regolamentari e di comunicazione pronti prima che una rivendicazione compaia online.

Panzer è ancora in fase di espansione e il suo profilo tecnico potrebbe cambiare rapidamente man mano che nuovi affiliati introducono metodi propri. Proprio per questo va trattato come una minaccia credibile e trasversale, non come un fenomeno di nicchia.

https://www.ictsecuritymagazine.com/notizie/panzer-ransomware-vittime-italiane/

Pagamenti digitali in Italia continuano a crescere in Italia, i dati di Bankitalia

(Adnkronos) – Continuano a crescere in Italia i pagamenti alternativi al contante. Secondo i dati di Bankitalia, le transazioni digitali e senza contante segnano un incremento del 13%. L'88% dei pagamenti al POS è avvenuto avvicinando la carta, senza inserirla nel lettore. Il 24% dei pagamenti nei negozi fisici è stato avviato tramite dispositivi mobili. Le carte restano il principale strumento digitale e coprono circa tre quarti delle transazioni non in contanti.

–

multimedia/news-to-go

webinfo@adnkronos.com (Web Info)

The post Pagamenti digitali in Italia continuano a crescere in Italia, i dati di Bankitalia appeared first on Key4biz.

https://www.key4biz.it/pagamenti-digitali-in-italia-continuano-a-crescere-in-italia-i-dati-di-bankitalia/586322/