
netskope
Report Cloud + Threat:
tendenze globali del malware cloud e web
REPORT ELABORATO DA:
netskope
THREAT LABS

EXECUTIVE SUMMARY

In questa edizione del Report Cloud + Threat esaminiamo le tendenze del malware scaricato da web e cloud negli ultimi dodici mesi. I trojan rappresentano l'assoluta maggioranza del download di malware e gli hacker ne hanno utilizzati diversi tipi, insieme a tecniche di ingegneria sociale, per colpire le loro vittime. La maggior parte del malware scaricato è costituita da file Windows EXE/DLL o documenti di Microsoft Office, dal momento che Microsoft Windows, tuttora il sistema operativo desktop più diffuso a livello aziendale, resta l'obiettivo preferito dagli hacker.

Per quanto riguarda le fonti del malware scaricato, il 53% proviene da siti web tradizionali, mentre il 47% da applicazioni cloud. Il malware scaricato dal web ha origine in siti di molte categorie diverse, a partire da siti di tecnologia e server di contenuti. Il malware scaricato dal cloud ha origine in centinaia di applicazioni diverse, con in testa le più diffuse applicazioni cloud di archiviazione. Sia il malware scaricato dal web che quello scaricato dal cloud in genere proviene da server ubicati nelle stesse regioni geografiche delle vittime.

Abbiamo ottenuto una migliore comprensione di alcune delle tecniche utilizzate dagli hacker per diffondere il malware analizzando i più comuni referrer del malware scaricato. I principali referrer includono i motori di ricerca, poiché gli hacker sfruttano diffuse tecniche SEO per assicurarsi buoni posizionamenti sui motori di ricerca. I siti web compromessi e i siti web malevoli ideati per simulare siti legittimi sono altri referrer comuni di malware.

RISULTATI PRINCIPALI

- **Il 77% di tutto il malware scaricato da web e cloud è rappresentato dai trojan,** utilizzati per conquistarsi un punto d'appoggio da cui poi diffondere una serie di payload di livello successivo tra cui backdoor, infostealer e ransomware.
- **Il 47% del malware scaricato ha origine da applicazioni cloud,** mentre il 53% proviene da siti web tradizionali, il che dimostra che gli hacker continuano a utilizzare un mix di web e cloud per raggiungere le loro vittime.
- **Il phishing tramite download è in aumento, poiché gli hacker utilizzano tecniche SEO** per posizionare file PDF malevoli tra i principali risultati dei motori di ricerca più utilizzati, tra cui Google e Bing.
- **I file EXE e DLL costituiscono circa la metà di tutto il malware scaricato:** gli hacker continuano infatti a bersagliare Microsoft Windows, mentre i file malevoli di Microsoft Office sono in calo, essendo tornati ai livelli pre Emotet.
- **La maggior parte del malware parte da server ubicati nelle stesse regioni geografiche delle vittime,** perché gli hacker posizionano il loro malware in ogni parte del mondo proprio per evitare il geofencing.

INFORMAZIONI SU QUESTO REPORT

Netskope fornisce protezione dei dati e dalle minacce a milioni di utenti nel mondo. Le informazioni presentate in questo report si basano su dati di utilizzo anonimi raccolti previo consenso dalla piattaforma Security Cloud di Netskope relativi a una sottocategoria di clienti Netskope. Il report contiene informazioni sulle minacce rilevate dal Next Generation Secure Web Gateway (Next Gen SWG) di Netskope, a prescindere dal significato dell'impatto di ogni singola minaccia. Le statistiche del report sono elaborate sulla base di dati raccolti in un periodo di dodici mesi tra il 1° aprile 2021 e il 31 marzo 2022.

Netskope Threat Labs

Grazie ai principali ricercatori esperti in malware e minacce cloud, i Netskope Threat Labs scoprono e analizzano le più recenti minacce relative a dati e cloud elaborando le difese più adatte per le aziende. I nostri ricercatori partecipano regolarmente come volontari e relatori alle più importanti conferenze sulla sicurezza informatica, tra cui DefCon, BlackHat e RSA.

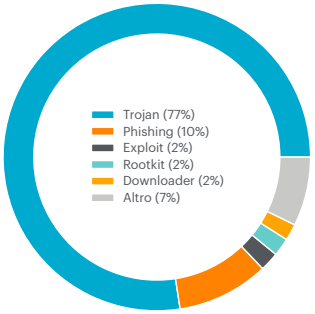
DOWNLOAD DI MALWARE

Categorie e famiglie di malware

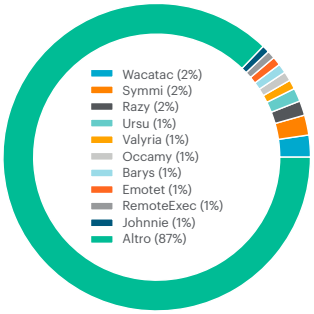
La stragrande maggioranza (77%) di tutto il malware scaricato da web e cloud è rappresentata da trojan. I trojan sono utilizzati comunemente nella prima fase di un attacco informatico con l'obiettivo di ingannare la vittima inducendola a scaricare ed eseguire un software, che fornirà agli hacker un punto d'appoggio iniziale. Spesso questo tipo di malware appare come software legittimo ed è utilizzato per sfruttare eventi importanti. Per fare un esempio, durante la pandemia da COVID-19 è circolata una grande varietà di trojan. Gli hacker li usano per diffondere una serie di payload di livello successivo, come backdoor, infostealer e ransomware. Mentre i trojan costituiscono la grande maggioranza del malware scaricato, non esiste un'unica famiglia di trojan che prevalga sulle altre a livello globale. Le prime dieci famiglie di trojan costituiscono solamente il 13% di tutti i trojan scaricati, mentre il rimanente 87% proviene da una lunga serie di tipi meno comuni.

I trojan sono stati il tipo principale di malware scaricato in ogni regione, con l'eccezione del Medio Oriente, che ha registrato un'incidenza maggiore di exploit rispetto alle altre regioni. Con exploit qui ci riferiamo a file di malware che sfruttano un bug o una vulnerabilità quando vengono aperti o eseguiti dalla vittima. Il phishing tramite download, sopra la media ancora in Medio Oriente, ha raggiunto il suo apice in Africa. Il phishing tramite download è diverso rispetto ai tradizionali siti web di phishing. Si tratta, in genere, di file PDF che assumono la forma di falsi CAPTCHA, false richieste di condivisione di file o false fatture, e fanno parte di una più ampia campagna di phishing. Il phishing tramite download è aumentato nel novembre 2021, quando gli hacker sono riusciti a posizionarli nei risultati dei principali motori di ricerca attraverso comuni tecniche SEO, aumentandone la diffusione.

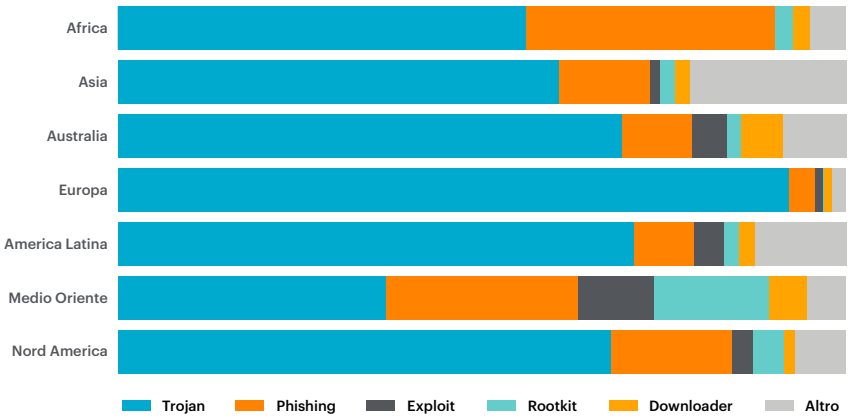
Categorie principali di malware negli ultimi 12 mesi



Famiglie principali di trojan negli ultimi 12 mesi

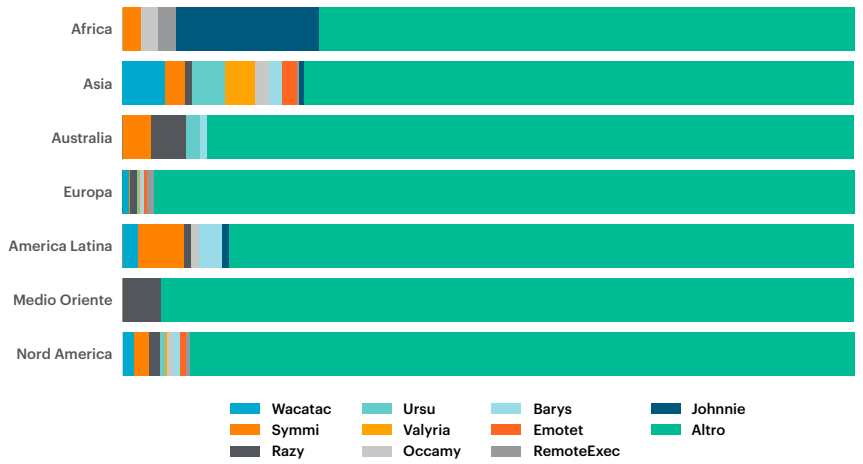


Categorie principali di malware per regione



I principali tipi di trojan variano a seconda della regione, dal momento che le campagne trojan sono in genere mirate nello specifico a utenti che parlano una certa lingua o che vivono in un determinato paese, oppure riguardano eventi importanti a livello locale. Alcune famiglie di trojan sono risultate più dominanti in alcune regioni, come Johnnie in Africa e Razy in Medio Oriente. In altre regioni, come Nord America e Asia, abbiamo rilevato quasi tutte le famiglie principali. A differenza delle altre regioni, in Europa le famiglie principali hanno rappresentato una percentuale più contenuta rispetto al totale dei trojan scaricati.

Principali famiglie di malware per regione

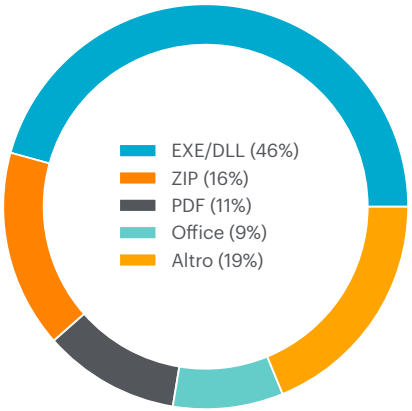


Tipi di file di malware

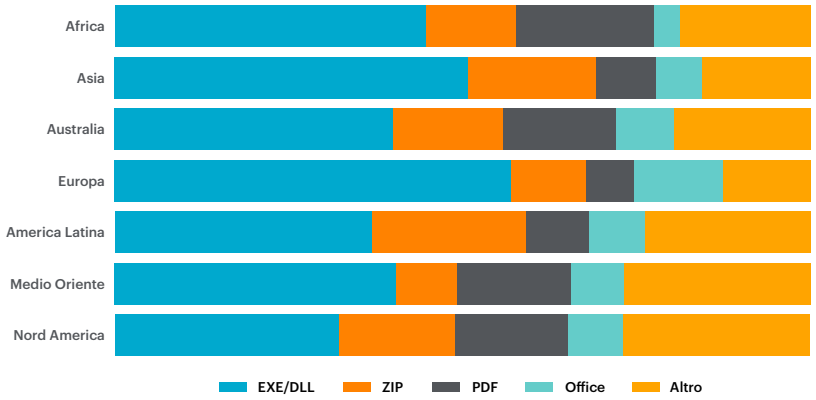
File Portable Executable (EXE/DLL), file di Microsoft Office, file PDF e file ZIP rappresentano l'81% di tutto il malware scaricato negli ultimi dodici mesi. Documenti di Office malevoli, che nel 2020 e all'inizio del 2021 erano molto più comuni a seguito dell'attività di Emotet e Dridex, sono tornati ai livelli pre Emotet. Due modifiche recenti apportate da Microsoft, e cioè il blocco delle macro di Excel 4.0 e il blocco delle macro VBA per i file scaricati da internet, farà probabilmente diminuire ancora di più questa percentuale, obbligando gli hacker a cercare strategie alternative. Oltre ai file PDF di phishing appena menzionati, gli hacker hanno utilizzato PDF malevoli anche per reindirizzare gli utenti verso siti di distribuzione di spam, scam e malware.

A livello regionale, c'è una variazione minima rispetto alla frequenza di ciascun tipo di file. I file EXE/DLL costituiscono sempre la maggioranza del malware scaricato, seguiti da file PDF, ZIP o Office. L'Africa ha registrato non solo la percentuale più elevata di download di file di phishing, ma anche di PDF scaricati, poiché la maggioranza del malware scaricato di tipo phishing in Africa è stata di file PDF.

Principali tipi di file di malware negli ultimi 12 mesi



Principali tipi di file di malware per regione



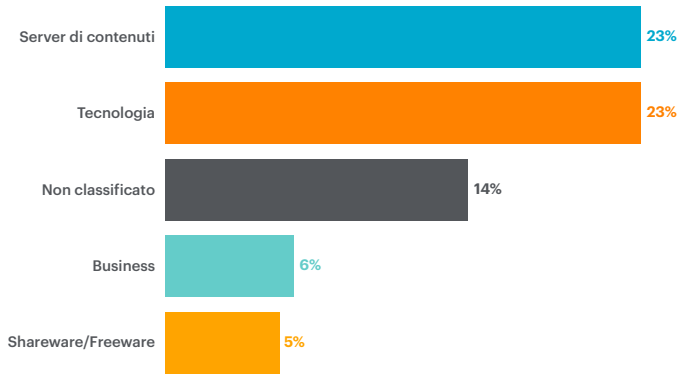
FONTI DI MALWARE

Download di malware dal web

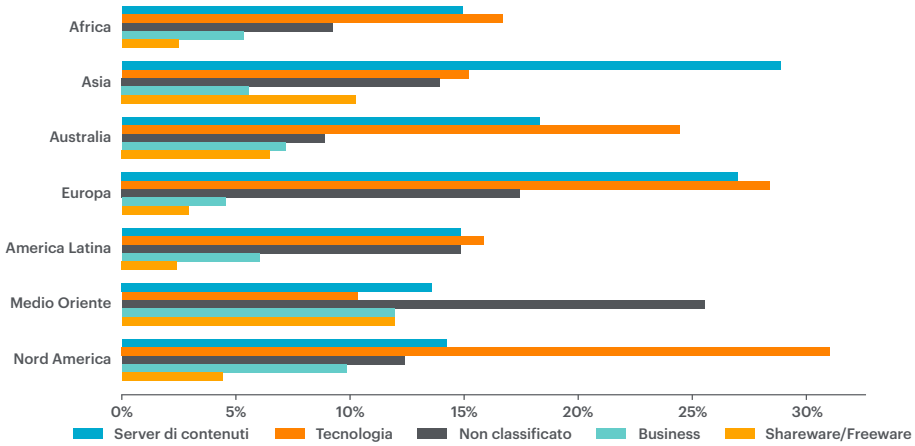
Il 53% di tutto il malware scaricato dal web negli ultimi dodici mesi proveniva da siti web tradizionali anziché da applicazioni cloud. Del malware scaricato dal web, una parte ha avuto origine da siti tradizionalmente associati al malware. Ad esempio, i siti "non classificati", cioè quelli non abbastanza diffusi da essere assegnati a una particolare categoria, sono stati responsabili del 14% dei download di malware dal web. Analogamente, i siti "shareware/freeware", che a volte distribuiscono software accompagnato da spyware e altri software malevoli, rappresentano il 5% del malware scaricato dal web. Le altre categorie principali, "tecnologia", "server di contenuti" e "business", rappresentano una larga parte del web non malevolo e non possono essere filtrati altrettanto facilmente.

A livello regionale, abbiamo notato alcune variazioni nelle categorie di siti web più comuni per i download di malware. Mentre i siti web appartenenti alla categoria "tecnologia" sono in pole position nella maggior parte delle regioni, i siti appartenenti alla categoria "server di contenuti" sono al primo posto in Asia e quelli "non classificati" in Medio Oriente. In America Latina non c'è una categoria dominante: le prime tre categorie rappresentano ciascuna circa il 15% di tutti i download di malware.

Categorie principali dei download
di malware dal web negli ultimi 12 mesi

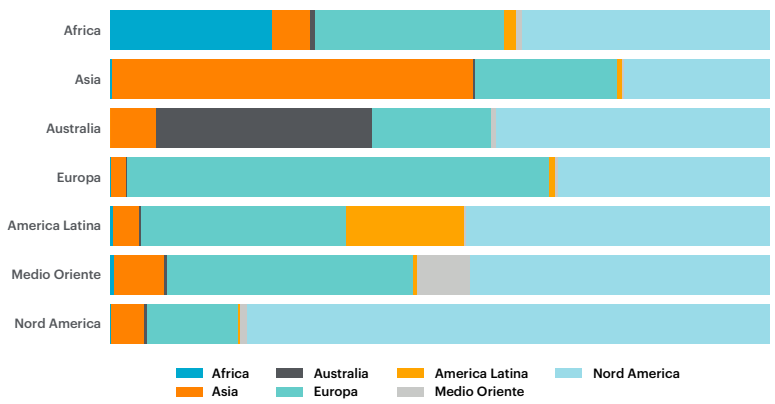


Categorie principali dei download di malware dal web per regione



Inoltre, gli hacker prendono di mira gli utenti di una specifica regione con malware ubicato su server della stessa regione. Nella maggior parte delle regioni, la maggioranza dei download di malware ha avuto origine nella stessa regione delle vittime. Ciò è particolarmente vero per il Nord America, dove l'84% del malware scaricato dagli utenti di questa regione proveniva da siti web ospitati in Nord America. All'altra estremità dello spettro c'è il Medio Oriente, dove solo il 7% del malware scaricato proveniva dall'interno della regione, mentre molti download hanno invece avuto origine nelle regioni confinanti dell'Europa e dell'Asia. In media, l'Europa è stata la fonte del 30% e il Nord America del 42% di tutti i download di malware a livello globale.

Regione d'origine del malware scaricato

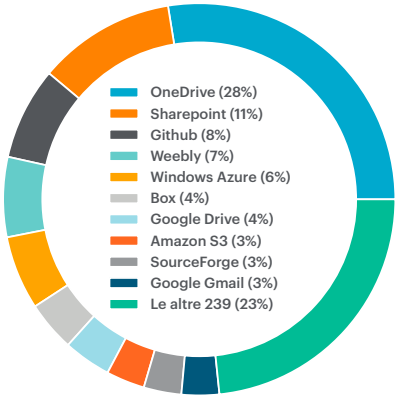


Download di malware dal cloud

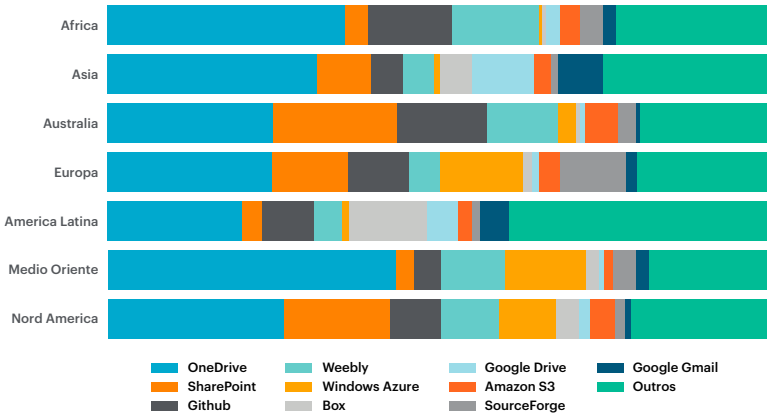
Il 47% di tutto il malware scaricato ha avuto origine da applicazioni cloud invece che da siti web. In totale, è stato scaricato malware da 257 applicazioni diverse, con il 75% di tutti i download di malware dal cloud proveniente dalle prime dieci applicazioni. Questi dati riflettono sia l'attività degli hacker che il comportamento degli utenti: gli hacker tendono a sfruttare le applicazioni più popolari per raggiungere più vittime, mentre è più probabile che gli utenti scarichino malware dalle applicazioni più diffuse e che utilizzano di più.

Nell'ambito di ciascuna regione, le prime dieci applicazioni sono responsabili per la maggioranza dei download di malware dal cloud. Microsoft OneDrive è stata l'applicazione più diffusa in ogni regione, a vari livelli. Alcune applicazioni sono risultate più comuni in alcune regioni rispetto ad altre: Box in America Latina, Google Drive in Asia e Windows Azure Blob Storage in Medio Oriente. Questi dati riflettono sia le tattiche degli hacker che il comportamento degli utenti in ciascuna regione.

Principali applicazioni per il download di malware negli ultimi 12 mesi



Principali applicazioni per il download di malware per regione



Origine del malware scaricato

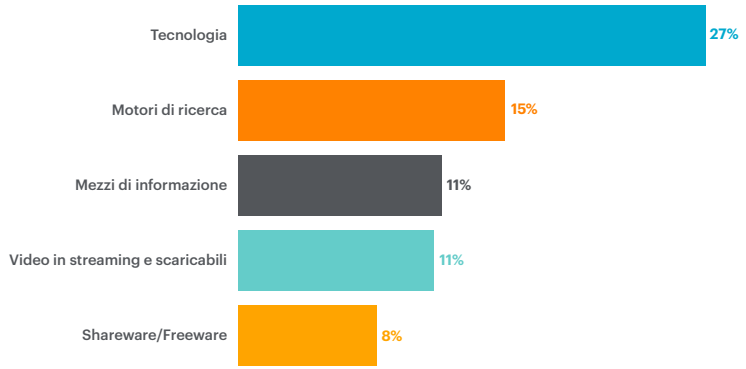
Il download del malware dal cloud o dal web non si verifica spontaneamente. Insieme ai trojan, gli hacker usano l'ingegneria sociale per ingannare le vittime e indurle a scaricare il malware. Le tecniche più comuni consistono nell'attirare gli utenti per sfruttare grandi avvenimenti (ad es. la pandemia da COVID-19), generare un senso di urgenza (magari una fattura che deve essere saldata) o dissimulare un'applicazione come legittima (si pensi alla versione gratuita di un videogame famoso). Gli hacker sfruttano anche aspetti tecnici come exploit nei software, download drive-by e attacchi smuggling HTML per scaricare malware.

L'intestazione della richiesta HTTP del referrer consente di comprendere meglio le tecniche di ingegneria sociale utilizzate dagli hacker per ingannare gli utenti e indurli a scaricare il malware. Il 14% dei referrer proveniva da applicazioni cloud, mentre l'86% da siti web tradizionali. I principali referrer delle applicazioni cloud includevano note applicazioni di archiviazione, collaborazione e webmail (applicazioni che consentono agli hacker di inviare messaggi direttamente alle vittime sotto molte forme diverse, tra cui email, messaggi diretti, commenti e condivisione di documenti).

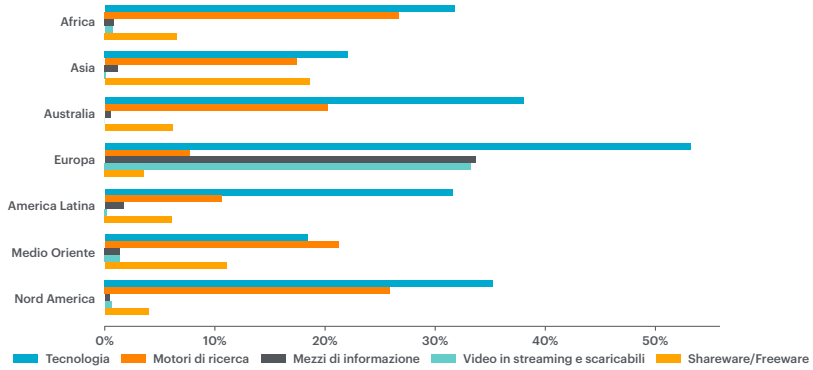
Le categorie principali di referrer web includevano alcune delle categorie tradizionalmente associate al malware, soprattutto "shareware/freeware," ma erano dominate da categorie solitamente non associate al malware. Quella dei "motori di ricerca" è una new entry di particolare interesse, perché rivela quanto alcuni hacker siano diventati bravi nelle tecniche SEO. Il download di malware che si può far risalire ai motori di ricerca riguarda soprattutto file PDF malevoli, compresi molti falsi CAPTCHA malevoli che reindirizzavano gli utenti verso siti web di phishing, spam, scam e malware.

I siti della categoria "tecnologia" sono in cima alla lista dei referrer di malware in tutte le regioni, mentre nelle altre categorie ci sono differenze significative. L'Europa ha fatto registrare la maggior percentuale di referrer delle categorie "mezzi di informazione" e "video in streaming e scaricabili", mentre in Africa la percentuale più alta è riferita alla categoria "motori di ricerca" e in Asia a quella "shareware/freeware". Queste differenze regionali riflettono sia le tecniche di ingegneria sociale utilizzate dagli hacker che il comportamento degli utenti.

Principali categorie di referrer per download di malware negli ultimi 12 mesi



Principali categorie di referrer dei download di malware per regione



RACCOMANDAZIONI

L'attuale panorama del malware è dominato dai trojan, che vengono veicolati tramite le più diffuse categorie di siti web e applicazioni cloud, solitamente all'interno della stessa regione in cui si trovano le vittime. Per mitigare i rischi derivanti dal malware diffuso tramite web e cloud, Netskope raccomanda alle aziende di adottare le seguenti misure:

1. Ispezionare tutto, comprese le corsie di traffico degli utenti per web, SaaS gestiti e non gestiti, shadow IT, IaaS e istanze aziendali e personali. Evitare di bypassare le suite di applicazioni con archiviazione nel cloud dove il download di malware è più comune. Evitare bypass o blocchi basati su categorie, preferendo un approccio più chirurgico.

2. Implentare una protezione dalle minacce inline e multilivello per tutto il traffico web e cloud, compresa l'analisi inline basata sull'apprendimento automatico di file PE (rispetto al sandboxing in background) per rilevare e bloccare il malware prima che arrivi agli endpoint, e per bloccare le comunicazioni contenenti malware rivolte all'esterno.

3. Eseguire la rilevazione di malware in background tramite analisi pre-esecuzione, sandboxing, analisi basate sull'apprendimento automatico, emissione di avvisi "paziente zero" per nuove minacce, analisi retrospettiva mediante indicatori di compromissione (IOC) e analisi MITRE ATT&CK per una migliore mitigazione della risposta.

4. Sfruttare il Cloud Threat Exchange (CTE) di Netskope per automatizzare gli aggiornamenti bidirezionali IOC in base alle informazioni sulle minacce nei sistemi di difesa, gestire il decadimento degli IOC e integrare il proprio stack di sicurezza con SSE, endpoint, email security, SIEM, XDR e SOAR.

5. Rilevare e ostacolare le minacce bloccando siti web rischiosi, e utilizzare RBI per siti non classificati, domini appena registrati e domini parcheggiati. Utilizzare firewall cloud (FWaaS) per filtrare il traffico in uscita su tutte le porte e in tutti i protocolli.

6. Ridurre i rischi nell'ambito delle proprie applicazioni raccomandando applicazioni alternative più sicure, oltre a monitorare e formare gli utenti per evitare l'utilizzo di applicazioni con classificazione mediocre e bassa.

7. Attuare la federazione di Single Sign-On e autenticazione a più fattori tra tutte le tue applicazioni e servizi cloud, e sfruttare Zero Trust Network Access (ZTNA) per applicazioni e risorse private. Utilizzare l'autenticazione step-up nell'ambito di policy adattive in base a rischio dell'applicazione, rischio dell'utente, rischio del dispositivo e sensibilità dei dati per promuovere principi zero trust.

8. Utilizzare l'analisi comportamentale per rilevare minacce interne, esfiltrazione di dati, dispositivi e credenziali compromessi tra tutte le corsie di traffico utente, verso applicazioni private e verso applicazioni gestite tramite introspezione API.

9. Automatizzare i flussi di lavoro di risposta relativi ad avvisi selezionati mediante Cloud Ticket Orchestrator di Netskope per indagini e risposte, e utilizzare Cloud Log Shipper di Netskope per inviare log web, cloud e firewall a XDR, SIEM e data lake.

10. Analizzare e monitorare continuamente movimenti di dati sconosciuti, comportamenti anomali, rischi e duplicazione delle applicazioni, profili di insider, utenti a rischio e fare attenzione alle dashboard comuni, includendo anche la valutazione del rischio cloud.

SCOPRI DI PIÙ

Per maggiori informazioni sulle minacce veicolate dal cloud e gli ultimi risultati delle ricerche dei Netskope Threat Lab, visita:
NETSKOPE.COM/NETSKOPE-THREAT-LABS

Per maggiori informazioni su come ridurre i rischi, contattaci oggi stesso:
WWW.NETSKOPE.COM/REQUEST-DEMO

REPORT ELABORATO DA:

netskope
THREAT LABS

2022 © Netskope, Inc. Tutti i diritti riservati. Netskope è un marchio registrato e Netskope Active, Netskope Discovery, Cloud Confidence Index e SkopeSights sono marchi commerciali di Netskope, Inc. Tutti gli altri marchi sono marchi commerciali dei rispettivi proprietari. 04/22 RR-533-1