Rapporto sugli attacchi e sulle criticità attuali nella cybersecurity

Paolo Passeri
ppasseri@netskope.com
@paulsparrows
https://www.linkedin.com/in/paulsparrows/

ANICA
Associazione Nazionale Industrie Cinematografiche Audiovisive e Digitali

WHOAMI

Paolo Passeri, (ex) Alfista e Cyber Intelligence Principal di Netskope, è un professionista di sicurezza informatica con oltre 20 anni di esperienza

I campi di interesse includono la sicurezza delle applicazioni cloud, ed il rilevamento del malware avanzato.

Paolo è anche un blogger: nel suo tempo libero, oltre alla corsa e alla bicicletta, gestisce il suo blog personale, hackmageddon.com, considerato una fonte primaria di dati e tendenze nel panorama delle minacce informatiche

ANICA
Associazione Nazionale Industrie Cinematografiche Audiovisive e Digitali


THE
INTERVIEW

IL PANORAMA ATTUALE

- Il 60% dei dati risiede nel cloud[1]
- Una organizzazione media utilizza 2,415 servizi cloud[2]
- Oltre il 60% dei dipendenti lavora da remoto[3]
- Il concetto di *Digital Trust* degli utenti è cambiato[4]

ANICA
Associazione Nazionale Industrie Cinematografiche Audiovisive e Digitali

[1] https://www.statista.com/statistics/1062879/worldwide-cloud-storage-of-corporate-data/
[2] https://www.netskope.com/resources/reports-guides/cloud-and-threat-report-february-2020-edition
[3] https://www.netskope.com/resources/reports-guides/cloud-and-threat-report-2022-year-in-review

IL CLOUD ACCELERA LA TRASFORMAZIONE DIGITALE

Cloud has a multitude of implications for corporate strategy, risk, and the broader business.

Category	Example impact	
Improved speed and agility	~90%	improvement in time to market
Easier innovation	~95%	time reduction for adding digital features
Efficient scalability	~10–15%	savings from capacity utilization
Reduced risk	~90%	outage reduction

Source: Based on externally available information on the internet and team analysis

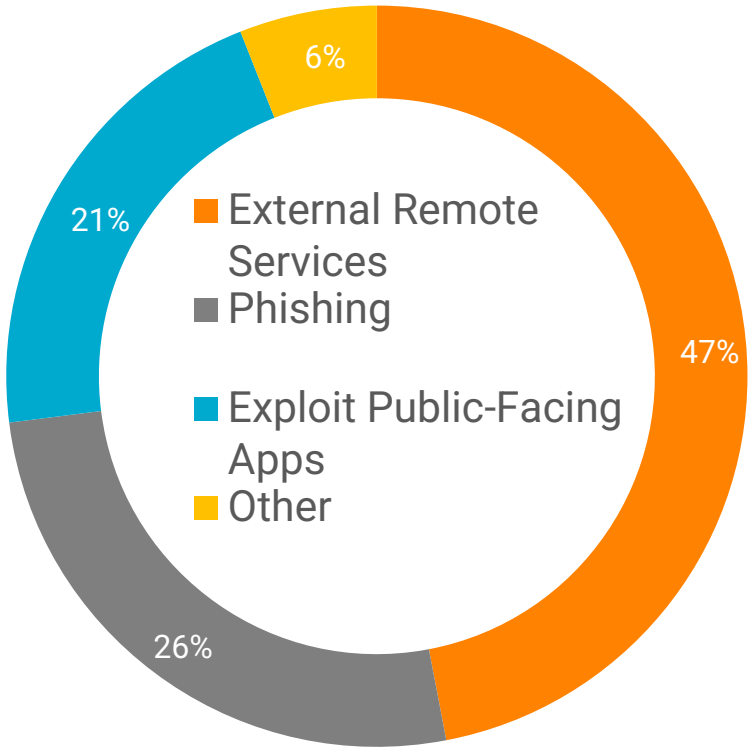
McKinsey & Company

Ma introduce anche nuovi rischi…

ANICA
Associazione Nazionale Industrie Cinematografiche Audiovisive e Digitali

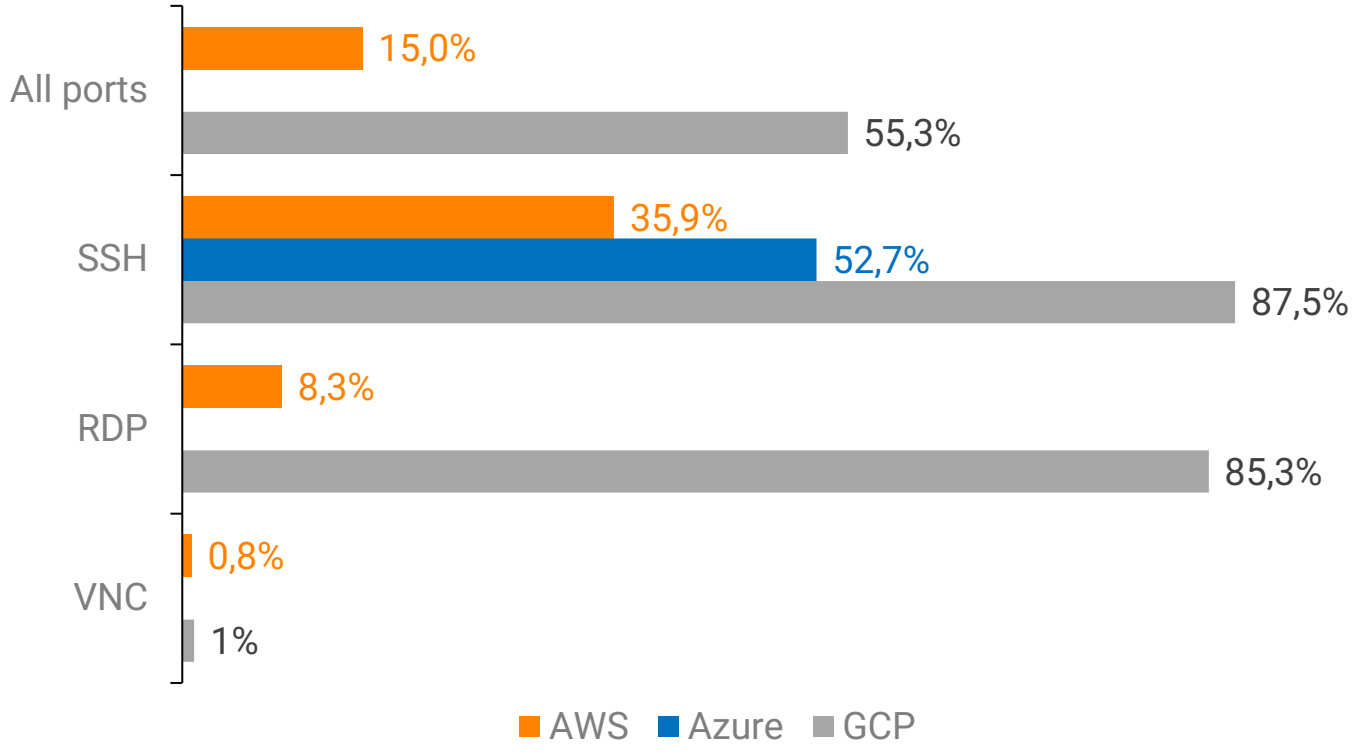
SERVIZI ESPOSTI: IL CLOUD COME OBBIETTIVO

VETTORI PRINCIPALI DI ACCESSO INIZIALE PER IL RANSOMWARE



Group-IB: Ransomware Uncovered 2021-2022

WORKLOAD ESPOSTI IN CLOUD



Netskope: Remote Access Statistics for Public Cloud Workloads

ANICA
Associazione Nazionale Industrie Cinematografiche Audiovisive e Digitali

PRINICIPALI MINACCE AL CLOUD

Posizione 2022		Posizione 2019
1	Insufficient Identity, Credentials, Access, and Key Management	4 ↑
2	Insecure Interfaces and APIs	7 ↑
3	Misconfiguration and Inadequate Change Control	2 ↓
4	Lack of Cloud Security Architecture and Strategy	3 ↑
5	Insecure Software Development	
6	Unsecured Third-Party Resources	
7	System Vulnerabilities	
8	Accidental Cloud Data Disclosure	
9	Misconfiguration and Exploitation of Serverless and Container Workloads	
10	Organized Crime/Hackers/APT	11 ↑
11	Cloud Storage Data Exfiltration	

ANICA
Associazione Nazionale Industrie Cinematografiche Audiovisive e Digitali


Nothing to see here.
Please disperse.

E COME VETTORE DI ATTACCO…

48%

DEL MALWARE PROVIENE DA APPLICAZIONI CLOUD

401

DIFFERENTI APPLICAZIONI CLOUD UTILIZZATE PER DISTRIBUIRE MALWARE

94.4%

PERCENTUALE DI MALWARE PROVENIENTE DA SITI COMPROMESSI, SITI FAKE O SERVIZI DI HOSTING

30%

DEL MALWARE PROVIENE DA ONEDRIVE

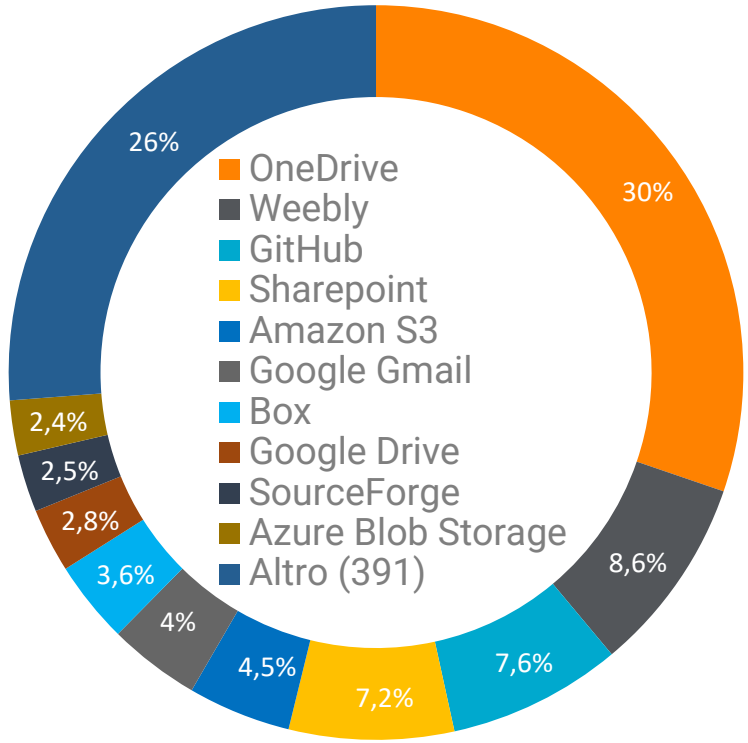
40%

UTENTI CHE USANO ONEDRIVE OGNI GIORNO

25%

UTENTI CHE CARICANO FILE SU ONEDRIVE OGNI GIORNO

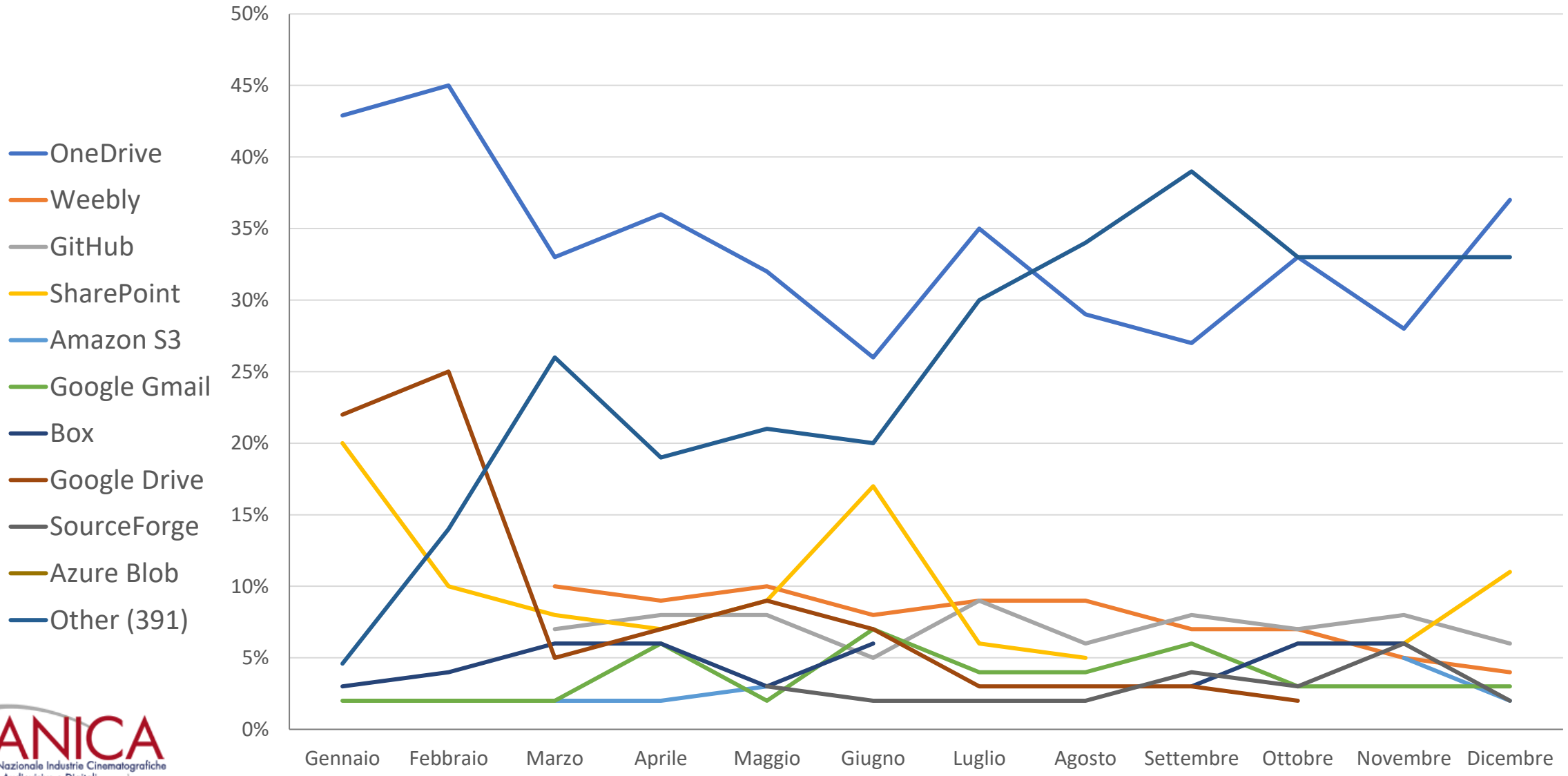
TOP EXPLOITED APPS



ANICA
Associazione Nazionale Industrie Cinematografiche Audiovisive e Digitali

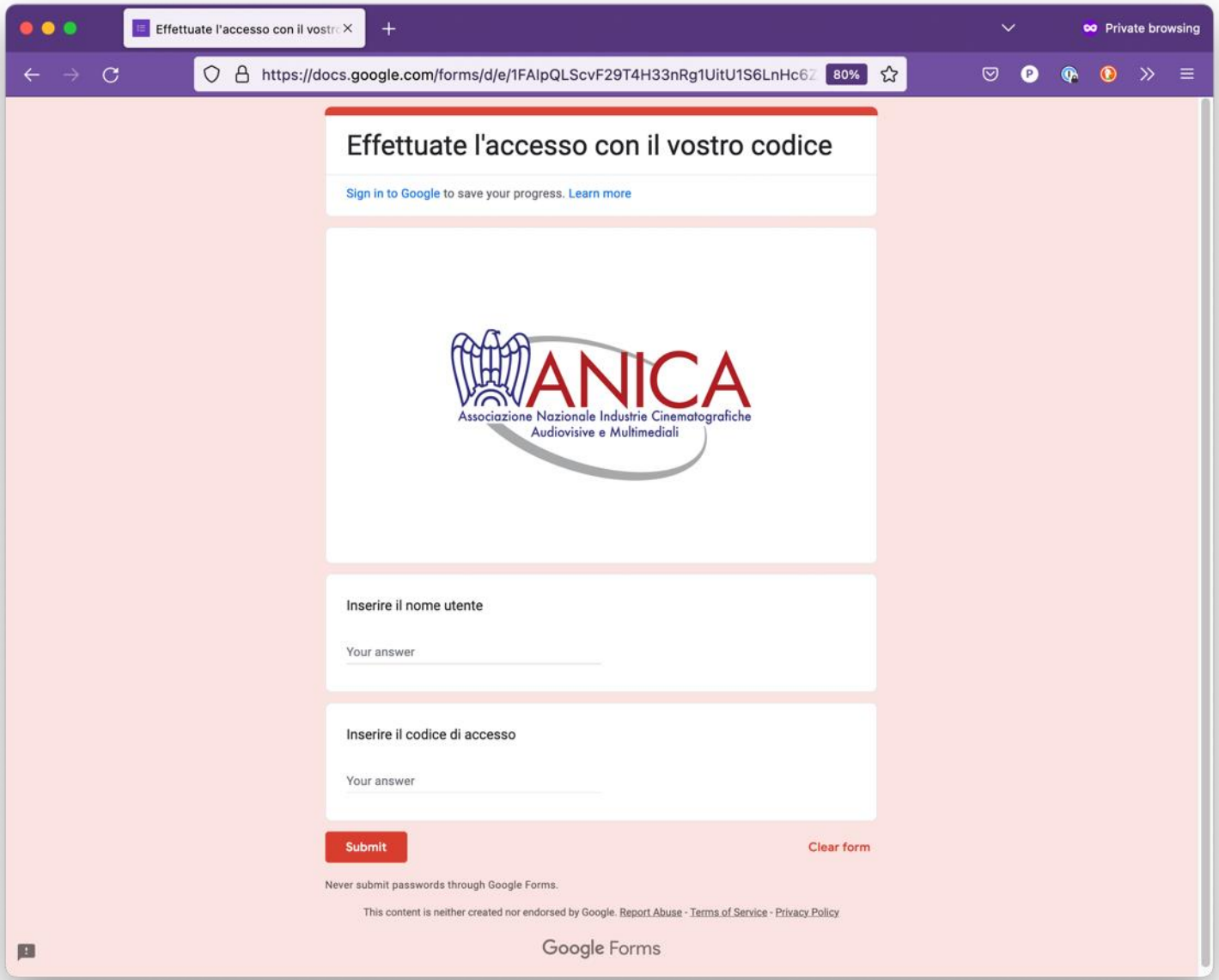
Netskope Cloud and Threat Report: 2022 Year In Review

PRINCIPALI APP PER DISTRIBUIRE MALWARE



ANICA
Associazione Nazionale Industrie Cinematografiche Audiovisive e Digitali

PAGINA DI PHISHING SU UN SERVIZIO CLOUD



- Tempo necessario per creare la pagina: **5 minuti** (ascoltando la musica e parlando al telefono)
- Costo: **0 EURO**
- **BONUS POINT:** Gmail può essere utilizzata per inviare la mail di phishing

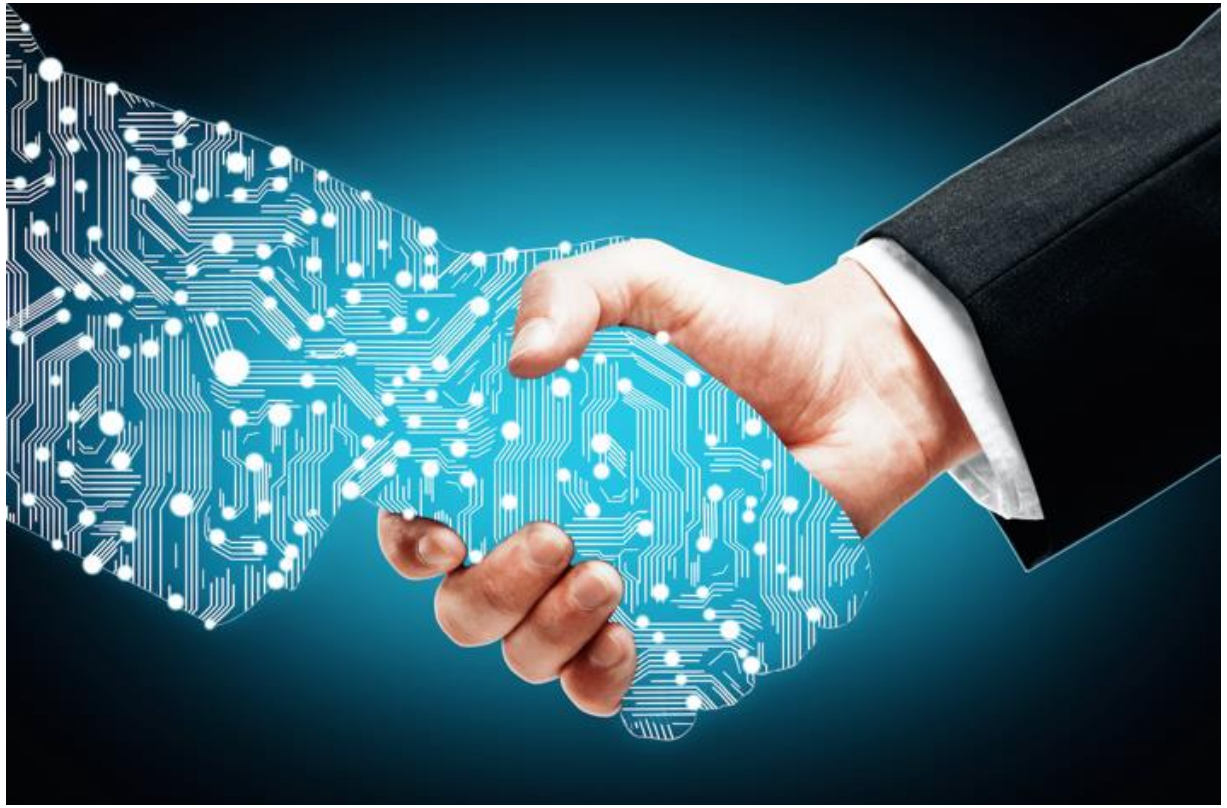
ANICA
Associazione Nazionale Industrie Cinematografiche Audiovisive e Digitali

UNA TECNOLOGIA
TRADIZIONALE ALLE PRESE
CON IL TRAFFICO CLOUD

IL DIGITAL TRUST

Digital Trust is a necessity in a global economy reliant on ever-increasing connectivity, data use, and new innovative technologies.

In order to be trustworthy, technology must be secure (ensuring connected systems' confidentiality, integrity, and availability) as well as responsibly used.



COME CI VEDIAMO NOI…

COME CI VEDONO GLI ATTACCANTI

ANICA
Associazione Nazionale Industrie Cinematografiche Audiovisive e Digitali

GLI ATTACCANTI SFRUTTANO CONTINUAMENTE IL DIGITAL TRUST

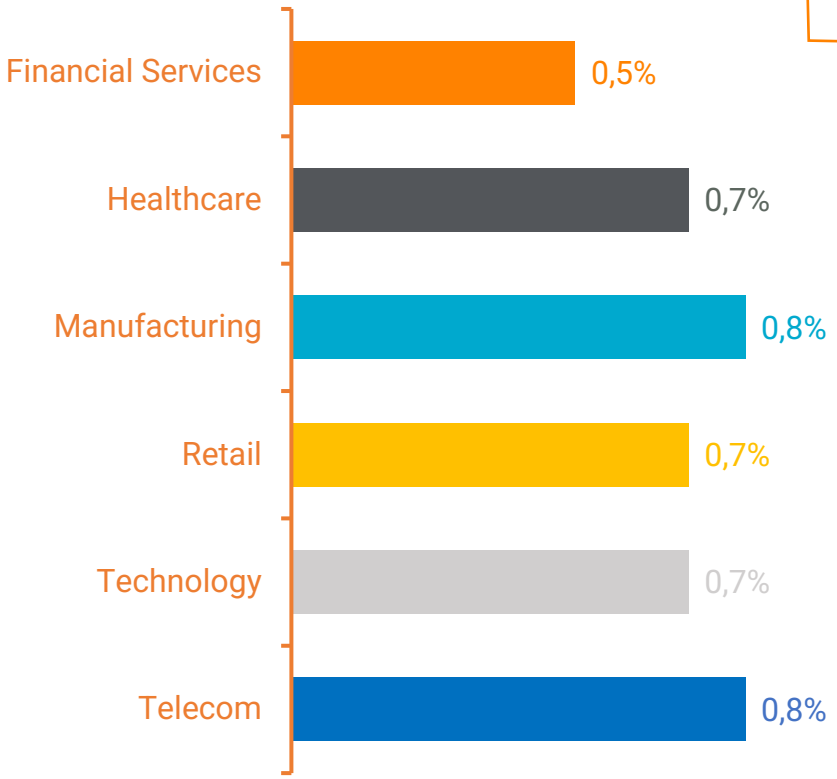
L’intento è quello di far presa sulle nostre emozioni e farci premere il famigerato bottone rosso (un link malevolo, aprire un allegato, etc..)

ANICA
Associazione Nazionale Industrie Cinematografiche Audiovisive e Digitali

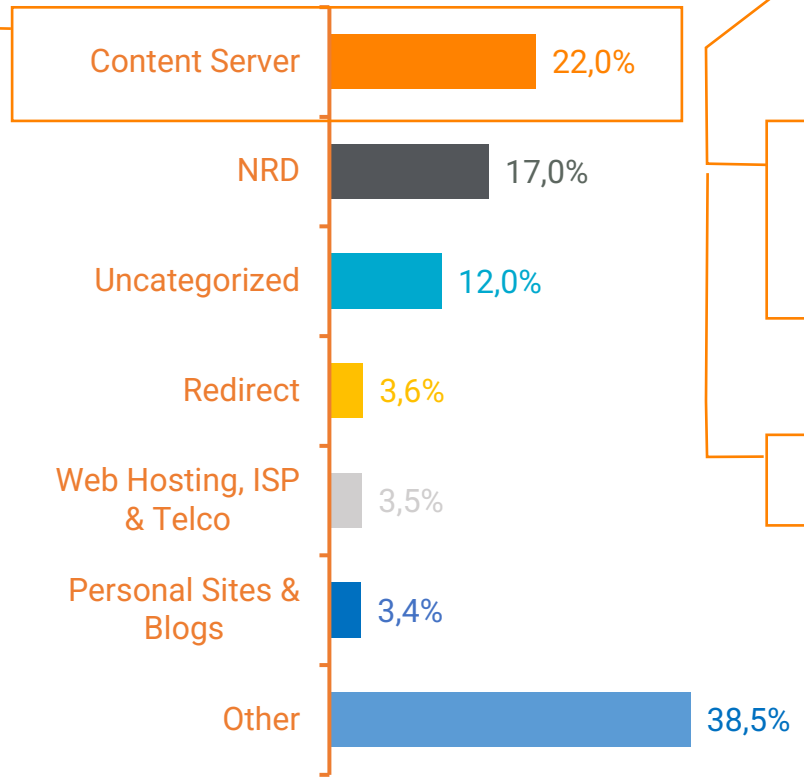
PHISHING: Q3 2022

Sfruttamento del Digital Trust

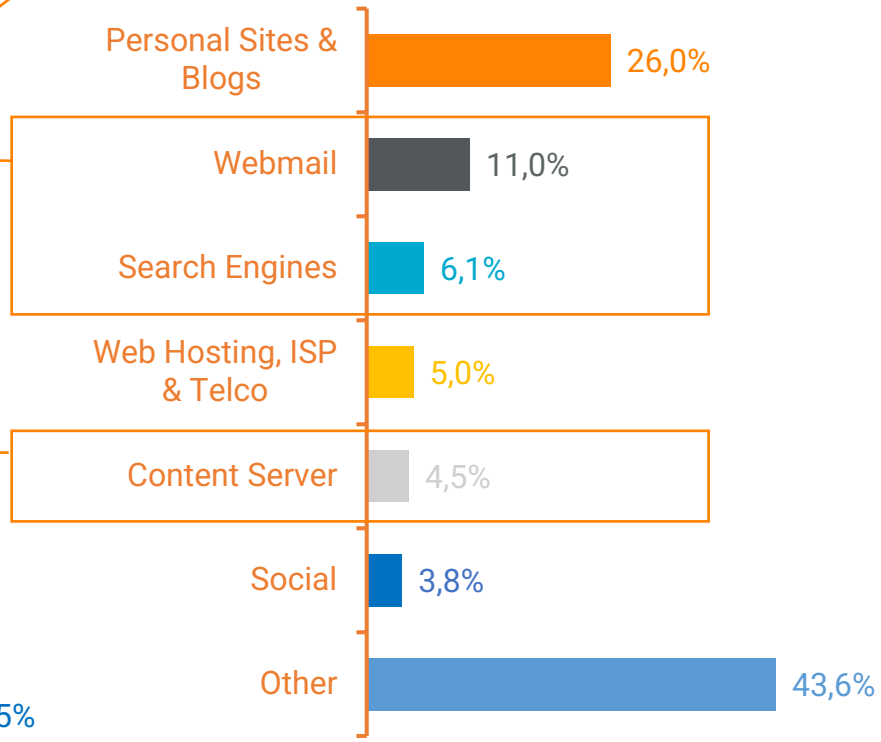
PHISHING BY INDUSTRY (CLICK EVERY 1000 USERS)



PHISHING HOSTING



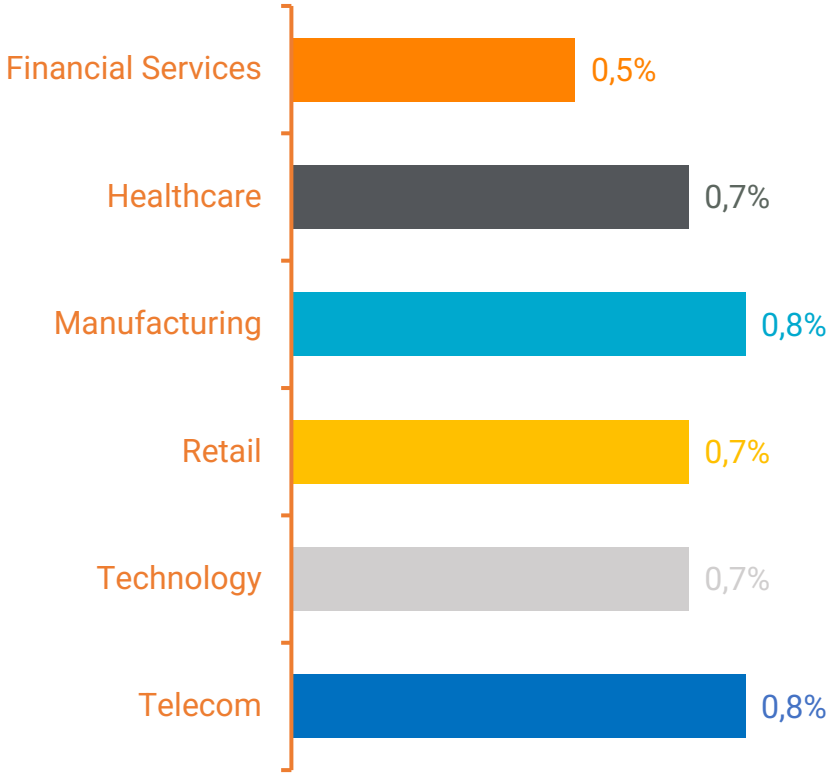
PHISHING REFERERS



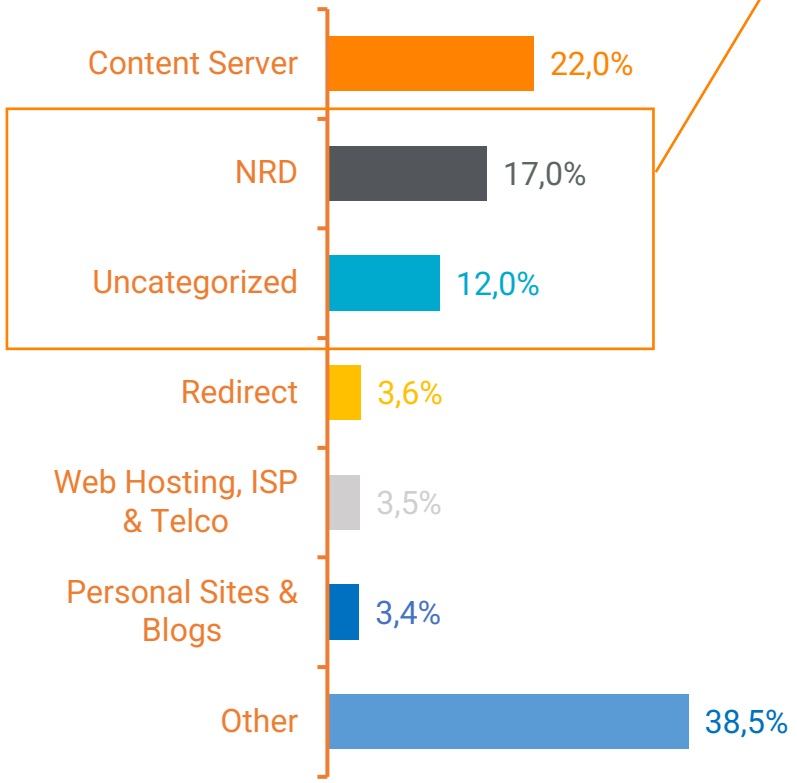
Netskope Cloud and Threat Report: Phishing
Data from July 1, 2022 through September 30, 2022.

PHISHING: Q3 2022

PHISHING BY INDUSTRY (CLICK EVERY 1000 USERS)

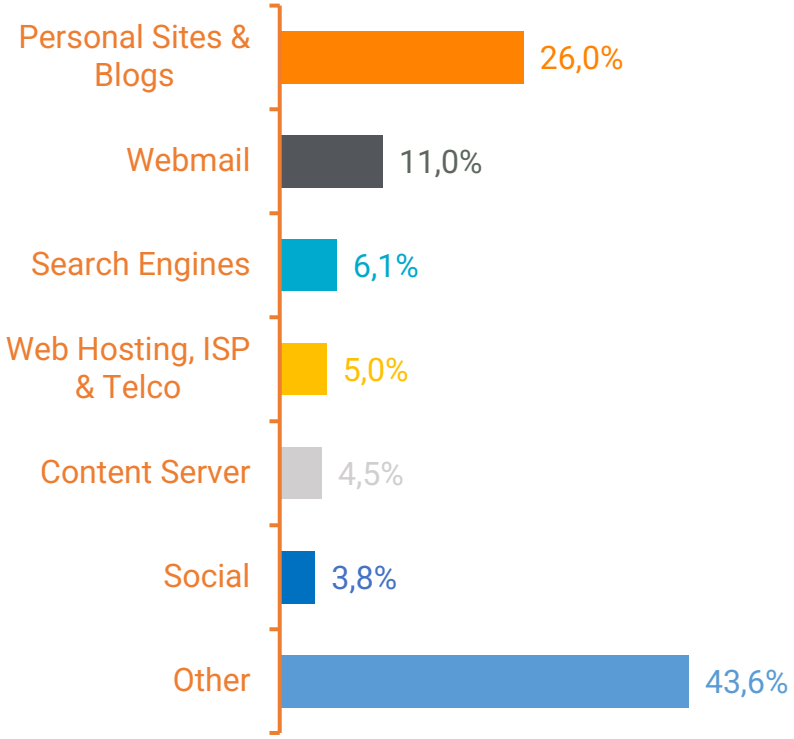


PHISHING HOSTING



Mancanza di educazione di sicurezza

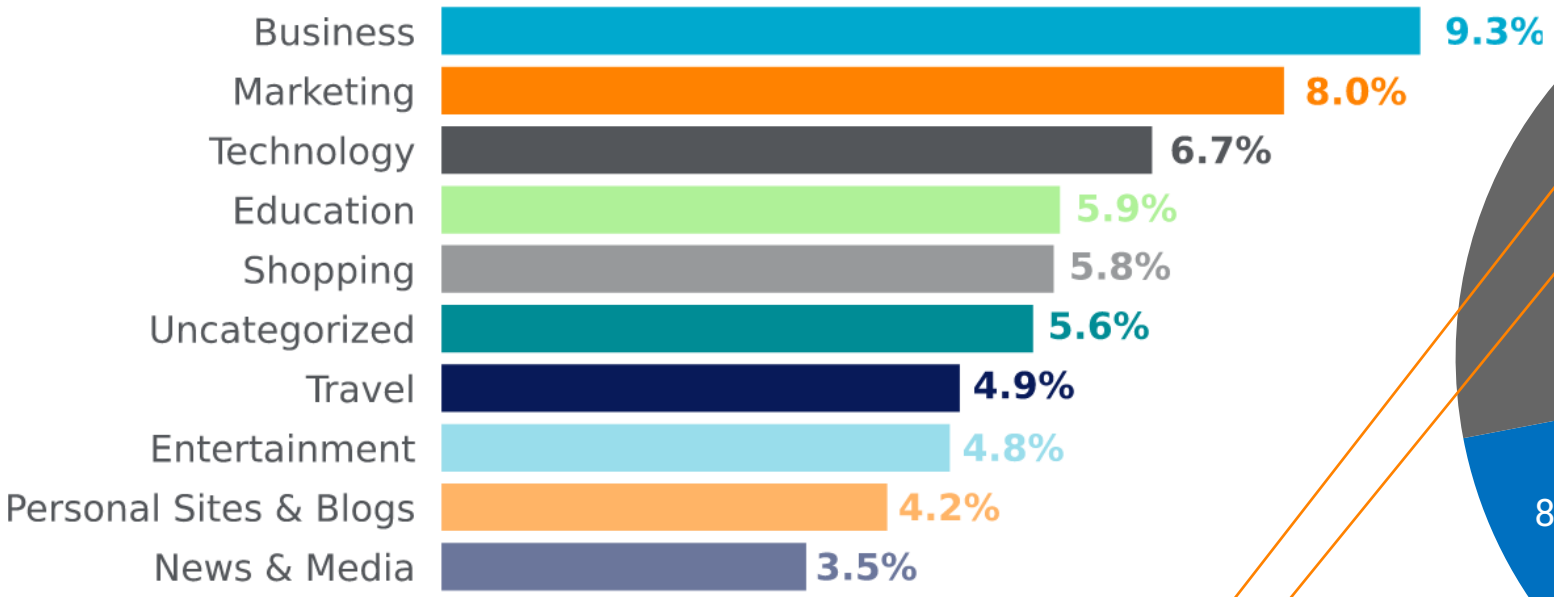
PHISHING REFERERS



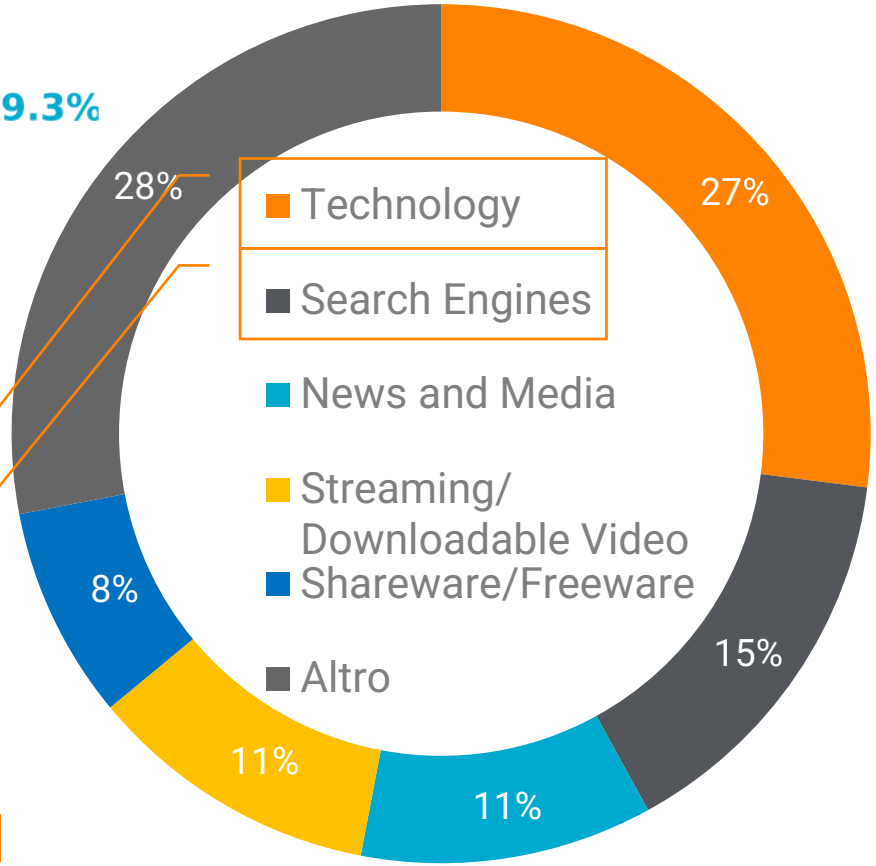
Netskope Cloud and Threat Report: Phishing
Data from July 1, 2022 through September 30, 2022.

PHISHING: Q3 2022

PRINCIPALI CATEGORIE DI DISTRIBUZIONE DEL MALWARE



LINK DI PROVENIENZA



Sfruttamento del Digital Trust


ONE DOES NOT SIMPLY...
GIVES AWAY WINDOWS 11 UPGRADES FOR FREE

STRATEGIE DI MITIGAZIONE

- Il cloud è un fattore abilitante per la trasformazione digitale, ma anche un fattore di ampliamento della superifice di attacco.
- Gli attaccanti stanno sfruttando il digital trust, utilizzando servizi leciti per distribuire malware o per redirigere a contenuto malevolo.
- Le organizzazioni devono incoraggiare una cultura di sicurezza
- Questi aspetti sono critici dal momento che la forza lavoro è distribuita e gli utilizzano i dispositivi aziendali per uso personale
- I controlli di sicurezza debbono ora essere applicati al punto di accesso per proteggere gli utenti da ovunque essi si colleghino, indipendentemente dal dispositivo.

ANICA
Associazione Nazionale Industrie Cinematografiche Audiovisive e Digitali