Microsoft

Identity Is the New Battleground

Cyber Signals

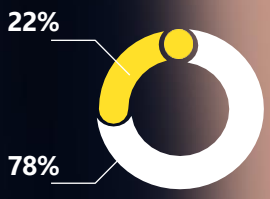
Gennaio-Decembre 2021

Gestione delle identità:
Un nuovo campo di battaglia

83

milioni di attacchi

11/26 to 12/31 commercial/ enterprise customers



- **22%** di utenti Azure Active Directory dotato di un sistema di autenticazione efficiente
- **78%** di utenti Azure Active Directory non dotato di un sistema di autenticazione efficiente

Introduzione

Non ti limitare a reagire alle minacce: anticipale

Quando si parla di identità digitale, sebbene questa possa assumere varie forme, si fa banalmente riferimento agli indirizzi email e password che ogni giorno utilizziamo per accedere ad app e servizi online. Ed in realtà, sono proprio questi gli strumenti utilizzati dagli aggressori informatici per accedere alle reti, rubare le credenziali o fingersi consumatori del mondo digitale.

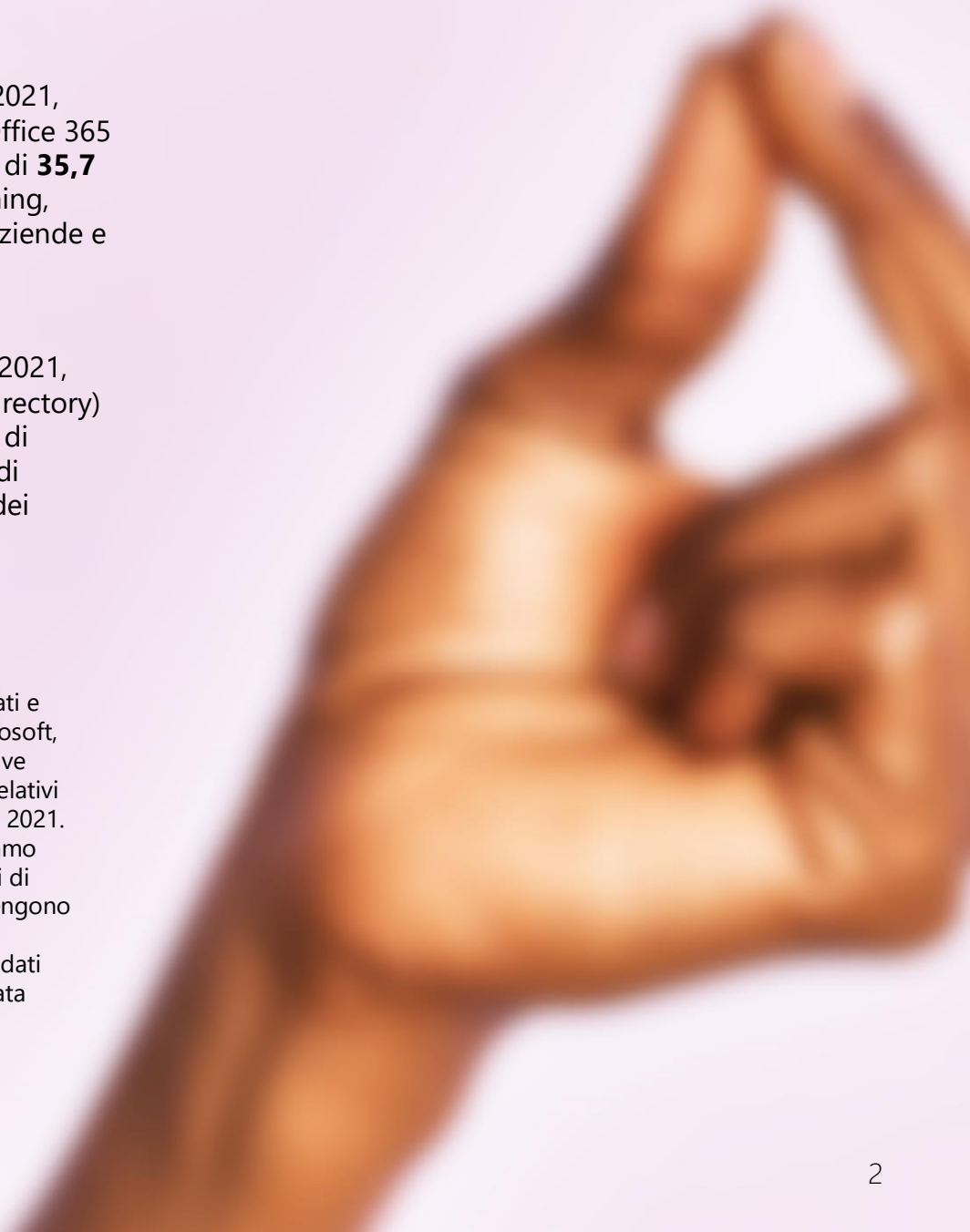
We are all Cybersecurity Defenders

Security Snapshot

Minacce agli endpoint:
Tra Gennaio e Dicembre 2021, Microsoft Defender per Endpoint ha rilevato e bloccato più di **9,6 miliardi** di minacce malware indirizzate alle aziende.

Minacce alle email:
Tra Gennaio e Dicembre 2021, Microsoft Defender per Office 365 ha rilevato e bloccato più di **35,7 miliardi** di email di phishing, che prendevano di mira aziende e consumatori.

Minacce alle identità:
Tra Gennaio e Decembre 2021, Microsoft (Azure Active Directory) ha rilevato e bloccato più di **25,6 miliardi** di tentativi di violazione degli account dei clienti aziendali.



Metodologia: I dati qui riportati e fornitici dalle piattaforme Microsoft, incluse Defender ed Azure Active Directory, sono dati anonimi, relativi al periodo -Gennaio-Dicembre 2021. Maggiori informazioni le abbiamo anche grazie ai milioni di avvisi di sicurezza che ogni giorno ci vengono segnalati dal cloud, dai sistemi endpoint e *l'intelligent edge*. I dati dotati di autenticazione avanzata combinano i sistemi MFA (autenticazione a più fattori) e quelli passwordless.

Le minacce degli "Stati-nazione"

Gli attacchi informatici perpetrati dagli attori degli "Stati-nazione" sono in aumento. Spesso gli autori di tali minacce, sebbene dotati di ampie risorse, si servono di semplici tattiche per entrare in possesso delle password degli utenti. Nel caso di attacchi alle reti aziendali, gli attori degli Stati-nazione si servono di appigli per muoversi sia "in verticale", cioè tra utenti e risorse simili tra loro, che "in orizzontale", ottenendo cioè accesso a credenziali e risorse di maggior valore. Lo *spear-phishing*, gli attacchi di *social engineering*, e *password sprays* rientrano in questo contesto, sono cioè tutte tattiche tese al furto delle password. Microsoft, tuttavia, è in grado di monitorare le attività degli aggressori studiandone le tecniche di attacco: se un account è gestito in maniera poco efficiente, ad esempio senza misure di sicurezza come i sistemi MFA e passwordless, gli Stati-nazione continuano a servirsi delle stesse, semplici, tattiche.

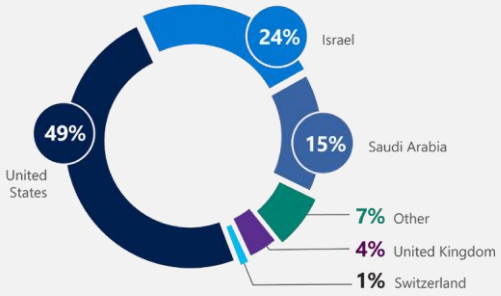
Threat briefing

La necessità di imporre l'adozione della MFA (Autenticazione a più fattori) o di dotarsi di sistemi passwordless, non può essere sottovalutata. La semplicità ed i costi relativamente bassi di tali attacchi li rende sempre più convenienti ed efficaci.

Sebbene l'MFA non rappresenti l'unico strumento di protezione delle identità per le organizzazioni, può comunque essere considerato un ottimo deterrente contro attacchi di questo tipo. L'abuso delle credenziali è cosa nota a NOBELIUM, uno Stato-nazione avversario legato alla Russia. Anche altri avversari come Iran-linked DEV 0343 si servono di attacchi del tipo *password spray*. Attività da DEV-0343 sono state osservate da aziende del settore difesa volte alla produzione di radar militari, sistemi satellitari e sistemi di comunicazione in risposta alle emergenze. Altre attività hanno invece preso di mira i porti del golfo Persico e diverse compagnie di trasporto marittime (o cargo) con un focus di business nel Medio Oriente.

Iran: paesi più colpiti

(Luglio 2020-Giugno 2021)



Per vedere l'intero diagramma

Clicca qui

Raccomandazioni

Le organizzazioni dovrebbero:

Configurare l'autenticazione a più fattori: Facendo così, si riduce il rischio che le password finiscano nelle mani sbagliate. Sarebbe ancora meglio utilizzare il *passwordless MFA* (che non prevede appunto l'utilizzo di password).

Controllare gli account privilegiati: Gli account dotati di accesso privilegiato, se "dirottati", diventano una potente arma per gli autori delle minacce, che possono servirsi di questi per avere ampio accesso a reti e risorse. Il team di sicurezza dovrebbe controllare di frequente gli account ad accesso privilegiato, adottando il principio di *least-privilege*.

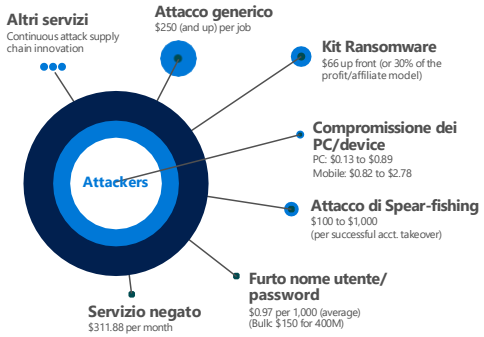
Controllare e monitorare tutti gli account tenant administrator: Il team di sicurezza dovrebbe controllare a fondo tutti gli user/account tenant administrator legati ai privilegi di amministratore, delegati per verificare l'identità e le attività degli utenti. Dovrebbe inoltre disattivare o rimuovere qualsiasi privilegio amministrativo delegato.

Stabilire delle *security-baseline* per mitigare il rischio: Gli Stati-nazione si servono di strategie di lungo termine e dispongono dei fondi e della volontà necessari allo sviluppo di tecniche e strategie di attacco. Qualsiasi iniziativa di *network hardening* ritardata, dovuta a larghezza di banda o alla troppa burocrazia, gioca a loro favore. Il team di sicurezza dovrebbe implementare pratiche zero-trust, come MFA e passwordless upgrades.

Ransomware: solo alcune varianti riescono ad avere la meglio

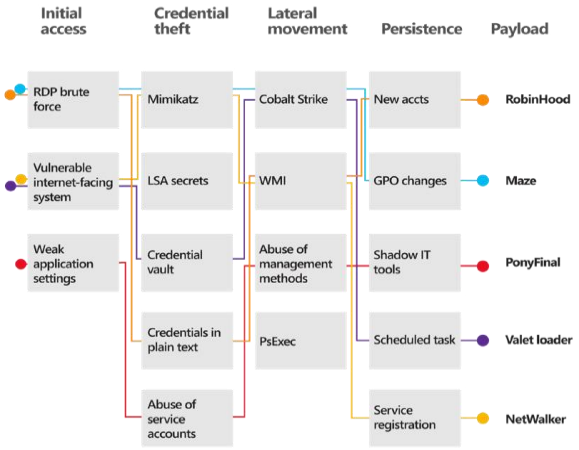
La narrazione prevalente sembra suggerirci l'esistenza di diversi tipi di minacce ransomware, tutte all'avanguardia ed in grado di superare le nostre capacità di difesa. Tuttavia, l'analisi condotta da Microsoft ci dice che si tratta di una percezione errata. C'è infatti spesso l'idea che i gruppi di ransomware siano rappresentati da un'unica entità. La verità è che ci troviamo di fronte a un'economia criminale i cui molteplici attori operano mediante catene di attacco standardizzate. Di seguito, mostriamo come i vari gruppi traggono vantaggio dalle molteplici strategie applicate.

Prezzi medi dei servizi di Cybercrime



Per vedere l'intero diagramma **Clicca qui**

Proteggiti dagli attacchi



Per vedere l'intero diagramma **Clicca qui**

In ogni caso, indipendentemente dal numero di ransomware in circolazione o dalle varianti coinvolte, tutto si riduce a tre principali vettori d'ingresso: il tentativo di forzare il protocollo desktop da remoto (RDP), i sistemi vulnerabili esposti su Internet, e le attività di phishing. Ognuno di questi vettori può essere mitigato mediante l'implementazione di pratiche di protezione delle password, gestione delle identità e aggiornamenti del software. Ricorda infatti che qualsiasi tipologia di ransomware diventa dannosa, ma solo quando riesce ad ottenere l'accesso alle tue credenziali.

Raccomandazioni

I team di sicurezza dovrebbero:

Sapere che il ransomware si sviluppa sfruttando credenziali predefinite o compromesse: Pertanto, è fondamentale che intesifichino i controlli, implementino l'autenticazione senza password ed MFA, con particolare attenzione agli account di dirigenti, amministratori o altri ruoli di rilievo.

Individuare segnali sospetti in tempo utile ed intervenire tempestivamente: Le prime fasi di login ed il trasferimento di file, ad esempio, possono sembrare delle procedure insignificanti, ma vanno comunque monitorate attentamente.

Disporre di un piano di risposta al ransomware e condurre esercitazioni di ripristino: Le copie di dati sono diverse per ciascun sistema IT e database. I team dovrebbero sempre disporre di un piano di risposta al ransomware.

Agire tempestivamente per mitigare il rischio: Sebbene gli attacchi ransomware siano temuti da tutti, la priorità del team di sicurezza dovrebbe essere il rafforzamento delle configurazioni deboli di sicurezza che, alla fine, determinano il successo di tali attacchi.

The cybersecurity bell curve: Basic security hygiene still protects against 98% of attacks.

Per vedere l'intero diagramma **Clicca qui**

Expert Profile

Christopher Glyer:

Principal Threat Intelligence Lead at MSTIC

Christopher Glyer ricopre il ruolo di Principal Threat Intelligence Lead (Responsabile intelligence sulle minacce) con una particolare attenzione ai ransomware presso il Microsoft Threat Intelligence Center (MSTIC). Fa parte del team incaricato di indagare su come gli attori delle minacce informatiche più avanzate riescano ad accedere e sfruttare i sistemi. In questa prima edizione di Cyber Signals, condivide le sue riflessioni sull'importanza dell'identità e della sicurezza.

Infatti, il passaggio al cloud, pone l'identità come uno dei pilastri fondamentali che le organizzazioni devono considerare quando implementano misure di sicurezza proattiva. Glyer spiega:

"Quando un aggressore riesce a ottenere l'accesso all'identità di qualcuno, le organizzazioni devono essere in grado di comprendere come tale identità sia stata compromessa, quali applicazioni sono state coinvolte e quali azioni sono state intraprese. La massima priorità consiste nel prevenire il furto o l'uso improprio di un'identità. La prevenzione iniziale riveste un'importnaza cruciale"

L'adozione dell'autenticazione multi-fattore (MFA), l'implementazione di soluzioni passwordless e l'istituzione di politiche di accesso condizionale per tutti gli utenti, rafforza notevolmente la protezione dei dispositivi, specialmente in un contesto di lavoro ibrido. Soluzioni di questo tipo aiutano le organizzazioni a controllare meglio l'accesso alle informazioni critiche e ad individuare attività potenzialmente anomale.

L'obiettivo principale è quello di conferire una maggiore rilevanza alla sicurezza delle identità, il che consentirebbe di stringere le autorizzazioni di accesso associate ad autenticazioni più "robuste", riducendo il rischio di accessi non autorizzati.

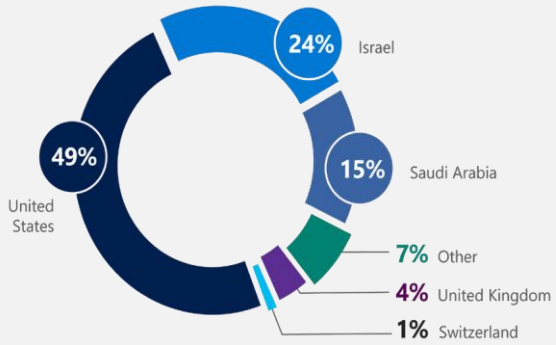
"Gli aggressori cercano costantemente di alzare l'asticella. Fortunatamente, le organizzazioni dispongono di numerose risorse che possono sfruttare, grazie ad esercitazioni pratiche o test di penetrazione, finalizzati a scoprire eventuali punti deboli o limitazioni nelle misure di sicurezza delle identità."

Glyer evidenzia che il focus sulla ricerca di debolezze dei sistemi di identità rappresenta una tattica comune condivisa da numerosi aggressori, criminali informatici e attori statali: "analizzando una tendenza di più ampio raggio nel tempo, notiamo che gli Stati-nazione sfruttano sempre più spesso gli attacchi informatici per scopi di spionaggio. Credo che assisteremo a un aumento degli aggressori che si servono di tali tattiche, poichè i vantaggi in termini di acquisizione di informazioni, rispetto ai costi di esecuzione, possono essere potenzialmente molto elevati. Garantire una protezione sicura delle identità riduce quest'opportunità e rende più complesso alzare il livello di attacco per gli aggressori".

> **"Il primo passo da compiere è quello di prevenire il furto, l'abuso o l'uso improprio delle identità. La prevenzione inziale riveste un'importanza vitale."**
>
> Principal Threat Intelligence Lead at MSTIC
>
> **Christopher Glyer**

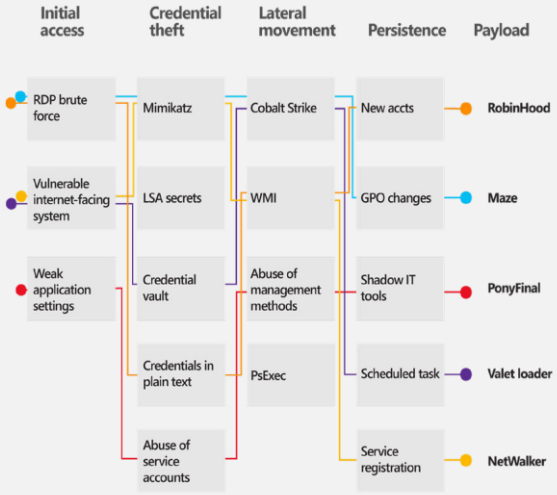
Appendix

Iran: paesi più colpiti
(Luglio 2020-Giugno 2021)



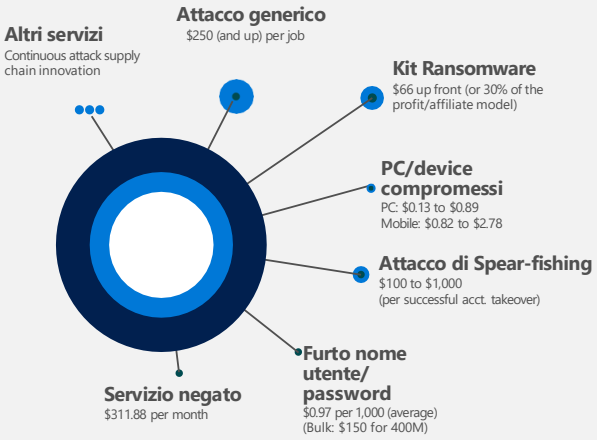
Clicca qui per tornare alla pagina 3

Playload di ransomware gestiti dall'uomo



Clicca qui per tornare alla pagina 4

Prezzi medi dei servizi di Cybercrime



Clicca qui per tornare alla pagina 4

La curva a campana della Cybersecurity: la *basic-security* continua a proteggere dal 98% degli attacchi

Clicca qui per tornare alla pagina 4

Microsoft