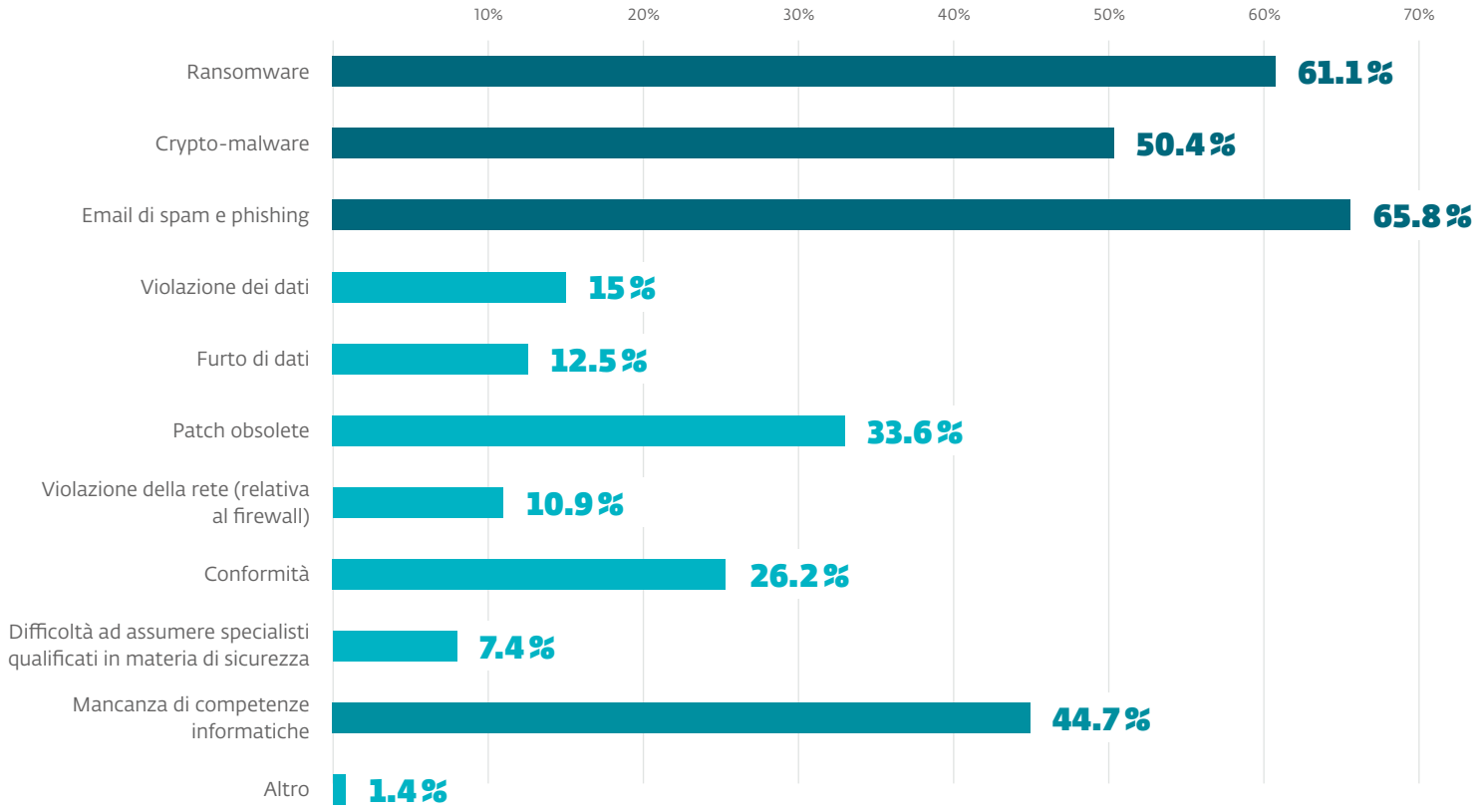
ESET MSP PROGRAM

LE PRINCIPALI SFIDE PER LE PMI

1. RANSOMWARE
2. INGEGNERIA SOCIALE
3. CRYPTOMINING ILLECITO
4. SICUREZZA DELLA PASSWORD

Come affrontare le principali sfide in termini di sicurezza delle PMI identificate dagli MSP

Abbiamo chiesto ai nostri partner MSP quali sono le principali sfide che si trovano ad affrontare nel garantire protezione ai propri clienti. Quasi 500 MSP hanno risposto, dicendoci che gli attacchi di ransomware, crypto-malware e social engineering, tramite e-mail di spam e phishing, sono le principali preoccupazioni, così come la mancanza di competenze informatiche. Ecco quindi una lista di utili consigli su come affrontare questi problemi.

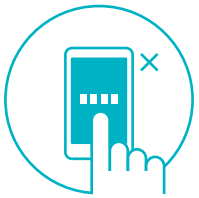


 Fonte: * ESET ha eseguito un sondaggio su 488 partner MSP in 14 paesi, nel luglio 2019, tramite un questionario online.

1 Ransomware: come funziona?

Ci sono molteplici tecniche di ransomware utilizzate dai cyber-criminali, tra cui:

Ransomware Screen locker
impedisce l'accesso alla schermata di un dispositivo, che resta bloccata sull'interfaccia utente del malware.



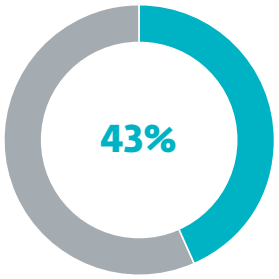
Ransomware PIN locker
modifica il codice PIN del dispositivo, rendendone inaccessibili il contenuto e le funzionalità.

Ransomware Disk coding
codifica l'MBR (Master Boot Record) e/o le strutture critiche del file system, impedendo così all'utente di accedere al sistema operativo.

Crypto-ransomware
cripta i file utente memorizzati su disco

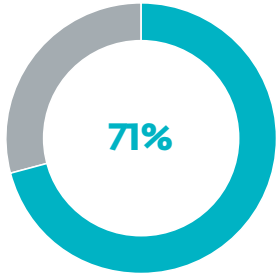
Perché dovrebbe interessare le PMI?

Le piccole e medie imprese sono oggi sempre più spesso un bersaglio interessante per i cyber-criminali. Sono obiettivi più appetibili rispetto ai semplici consumatori, e più vulnerabili delle grandi imprese.



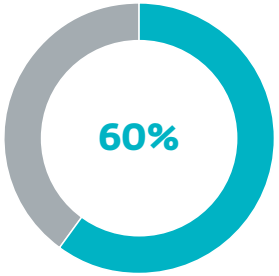
Il 43% delle vittime di violazioni di dati sono PMI.

Fonte: Verizon 2019 Data Breach Investigations Report, 10th Edition



Il 71% delle violazioni sono di natura finanziaria

Fonte: Verizon 2019 Data Breach Investigations Report, 10th Edition



Il 60% delle vittime ha pagato il riscatto richiesto.

Fonte: Indagine Ponemon 2017 State of Cybersecurity in Small & Medium-Sized Businesses (SMB)

Gli MSP riferiscono che il **riscatto medio richiesto alle PMI è di ~$4.300**, mentre il costo medio dei tempi di inattività legati a un attacco di ransomware è di ~$46.800.

Fonte: Datto 2018 State of the Channel Ransomware Report

NON PAGARE!

Non c'è assolutamente alcuna garanzia che i criminali informatici rispettino la loro parte dell'accordo (a volte non sono in grado di farlo, intenzionalmente o a causa di una codifica sbagliata). ESET **raccomanda di non pagare** la somma richiesta, almeno non prima di aver contattato il supporto tecnico del vostro fornitore di sicurezza per verificare le possibilità di decrittazione.

Come mantenere i vostri sistemi protetti

Raccomandazioni di base

Ci sono alcune cose che potete fare per evitare che la richiesta di riscatto vi rovini la giornata. Cominciamo con quello che si può fare in anticipo per evitare che il malware entri nel vostro sistema e come minimizzare i danni se dovesse accadere.

1. **Eseguire un backup dei dati** su base regolare e mantenere almeno un backup off-line completo dei dati più importanti
2. Mantenere tutti i software e le applicazioni - compresi i sistemi operativi - **patchati e aggiornati**
3. **Utilizzate una soluzione di sicurezza** affidabile e multistrato e assicuratevi che sia patchata e aggiornata

Ulteriori misure di protezione

- **Ridurre la possibilità di attacco** disabilitando o disinstallando eventuali servizi e software non necessari
- **Scansionare le reti** alla ricerca di account a rischio che utilizzano password deboli e assicurarsi che vengano modificate
- **Limitare o vietare l'uso del Remote Desktop Protocol (RDP)** dall'esterno della rete o abilitare la Network Level Authentication
- **Utilizzare una rete privata virtuale (VPN)** per l'accesso remoto
- **Rivedere le impostazioni** del firewall e chiudere tutte le porte non essenziali che potrebbero portare a un'infezione
- **Riesaminare le regole e le politiche per il traffico** tra i sistemi interni dell'azienda e la rete o le reti esterne
- Proteggere con password le configurazioni delle soluzioni di sicurezza
- Segmentare la LAN aziendale in sottoreti e collegarle ai firewall per limitare i movimenti laterali
- Proteggere i backup con l'autenticazione a più fattori
- Istruire regolarmente i dipendenti a riconoscere le minacce cibernetiche ed evitare gli attacchi di social engineering
- Limitare l'accesso ai file e alle cartelle condivise solo a chi ne ha bisogno
- Attivare il rilevamento di applicazioni potenzialmente non sicure/non desiderate (PUSA/PUA) al fine di bloccare gli strumenti che possono essere sfruttati dagli aggressori per disattivare la soluzione di sicurezza

2

Social engineering - Una definizione del problema

Il social engineering è una categoria di strategie di attacco non tecniche utilizzate dai criminali informatici per manipolare gli utenti e indurli a violare i protocolli di sicurezza o altri protocolli aziendali, a compiere azioni dannose o a fornire informazioni sensibili.

- **Gli attacchi di social engineering in genere non richiedono molte abilità tecniche** da parte dell'aggressore, il che permette a tutti i tipi di criminali informatici, dai piccoli ladri agli hacker avanzati, di cimentarcisi.
- Il danno è reale ed esteso, il che è ben illustrato dal rapporto annuale dell'Internet Crime Complaint Center (IC3) dell'FBI, che stima che solo nel 2018 le aziende statunitensi abbiano **perso più di 2,7 miliardi di dollari a causa degli attacchi informatici**. Di questi, 1,2 miliardi di dollari sono stati attribuiti a business email compromise (BEC)/email account compromise (EAC), dove i truffatori hanno preso il controllo degli account di posta elettronica legittimi della dirigenza e ne hanno fatto un uso improprio per ordinare/eseguire trasferimenti di fondi non autorizzati.
- Anche alcuni dei più sofisticati cyberattack della storia, come Black Energy, GreyEnergy o Industroyer, hanno utilizzato il phishing e altre forme di ingegneria sociale come vettori iniziali per l'attacco, **dimostrando l'efficacia di queste tecniche** e la loro popolarità tra i criminali informatici.

Aumento del 100% delle perdite globali dovute a truffe mirate BEC/EAC tra maggio 2018 e luglio 2019

Fonte: FBI Public Service Announcement, 10 settembre 2019. https://www.ic3.gov/media/2019/190910.aspx#fn1

Le tecniche usate dai cyber-criminali per ingannarci

Ci sono molte tecniche che rientrano nell'ambito del social engineering Queste sono le più frequenti:

Spam

è qualsiasi forma di comunicazione non richiesta inviata in massa. Il più delle volte lo spam è un'e-mail commerciale inviata al maggior numero possibile di utenti, ma può anche essere recapitata tramite messaggi istantanei, SMS e social media. Lo spam non è di per sé social engeeniring, ma alcune campagne utilizzano tecniche come il phishing, lo spearphishing, il vishing, il phishing SMS o la diffusione di allegati o link dannosi.

Impersonificazione

da parte dei criminali informatici che agiscono in nome di una persona di fiducia per ingannare le vittime e indurle a intraprendere azioni che danneggiano loro o le loro organizzazioni. Un esempio tipico è un criminale che si spaccia per l'amministratore delegato di un'azienda che richiede e approva transazioni fraudolente.

Phishing

è una forma di cyberattack in cui il criminale si spaccia per un'entità affidabile per richiedere informazioni sensibili alla vittima, di solito via e-mail. I sottotipi specifici del vettore includono il **vishing (**voice phishing), che impiega chiamate telefoniche fraudolente, e lo **smishing (**SMS phishing), che utilizza messaggi di testo SMS contenenti link o contenuti dannosi. Questi tipi di frode di solito cercano di creare un senso di urgenza o di usare tattiche di paura per costringere la vittima a soddisfare le richieste dell'aggressore. Le campagne di phishing possono rivolgersi a un gran numero di utenti anonimi, o a una vittima specifica o a un piccolo gruppo di vittime associate.

Spearphishing

è una forma mirata di phishing in cui l'aggressore invia messaggi altamente personalizzati a un gruppo limitato di persone, o anche solo a un singolo individuo, allo scopo di raccogliere i loro dati o di manipolarli per compiere azioni dannose.

Technical Support Scams

sono di solito telefonate fasulle o annunci sul web in cui gli aggressori offrono alla vittima servizi di assistenza tecnica non richiesti. In realtà, i cyber-criminali cercano di fare soldi vendendo servizi falsi e risolvendo problemi inesistenti.

Scareware

è un software che utilizza varie tecniche che inducono l'ansia per manipolare le vittime affinché installino un ulteriore codice dannoso sui loro dispositivi, spesso richiedendo al contempo il pagamento per un software non funzionale o assolutamente dannoso. Un esempio tipico è un falso prodotto antivirus progettato per indurre gli utenti a pensare che i loro dispositivi siano stati compromessi e che debbano pagare per la versione completa che include la funzionalità di pulizia (questo può a sua volta fornire un vettore per ulteriori infezioni).

Come riconoscere un attacco di social engeeniring

Senso di urgenza

I criminali dietro le campagne di social engineering spesso cercano di spaventare le vittime utilizzando frasi che inducono all'ansia come "inviaci subito i tuoi dati, o il tuo ordine verrà rifiutato" o "se non aggiorni subito il tuo profilo, chiuderemo il tuo account". Le banche, le società di spedizione pacchi, le istituzioni pubbliche e persino i dipartimenti interni comunicano di solito in modo neutrale e oggettivo. Pertanto, se il messaggio cerca di spingere il destinatario ad agire rapidamente, è probabilmente una truffa malevola e potenzialmente pericolosa.

Scarse competenze linguistiche

Di solito gli aggressori non prestano troppa attenzione ai dettagli, inviando messaggi pieni di errori di battitura, parole mancanti e scarsa grammatica. Un altro elemento linguistico che può segnalare un tentativo di attacco sono saluti e formulazioni generiche. Quindi se un'e-mail inizia con "Caro destinatario" o "Caro utente", siate prudenti.

Strano indirizzo del mittente

La maggior parte degli spammer non si prende il tempo di falsificare il nome o il dominio del mittente per farli sembrare affidabili. Quindi, se un'e-mail proviene da un indirizzo che è un mix di numeri e caratteri casuali o è sconosciuto al destinatario, deve andare direttamente nella cartella spam ed essere segnalata al reparto IT.

Richieste di informazioni sensibili

Le istituzioni e anche altri reparti della vostra azienda non richiedono normalmente informazioni sensibili via e-mail o telefono, a meno che il contatto non sia stato avviato dal dipendente.

Se qualcosa suona troppo bello per essere vero, probabilmente è così

Questo vale tanto per gli omaggi non richiesti sui social media quanto per quella "eccellente opportunità di business in scadenza a breve" che è appena arrivata nella vostra casella di posta.

Come può la vostra azienda proteggersi dagli attacchi?

Ci sono diverse cose che voi e il vostro MSP potete fare per proteggervi dal social engineering:

- **Formazione regolare sulla sicurezza informatica per TUTTI i dipendenti**, compreso il top management e il personale IT. Ricordate che tale formazione dovrebbe mostrare o simulare scenari di vita reale. I punti di apprendimento devono essere attuabili e, soprattutto, testati attivamente al di fuori dell'aula di formazione: le tecniche di social engeeniring si basano sulla scarsa consapevolezza della sicurezza informatica dei loro obiettivi.

- **Scansionate le password deboli** che potrebbero potenzialmente diventare una porta aperta nella rete della vostra organizzazione per gli aggressori. Inoltre, proteggete le password con un alto livello di sicurezza implementando l'autenticazione a più fattori.

- **Implementate soluzioni per gestire le comunicazioni truffa** in modo che i messaggi di spam e phishing vengano rilevati, messi in quarantena, neutralizzati e cancellati. Le soluzioni di sicurezza, comprese molte di quelle fornite da ESET, hanno alcune o tutte queste capacità.

- **Create politiche di sicurezza comprensibili** che i dipendenti possano utilizzare e che li aiutino a identificare i passi da compiere quando devono affrontare episodi di social engeeniring

- **Utilizzate una soluzione di sicurezza e strumenti amministrativi,** come ESET Security Management Center, per proteggere gli endpoint e le reti della vostra organizzazione, dando agli amministratori la piena visibilità e la capacità di rilevare e mitigare le potenziali minacce nella rete.

3

Cryptomining illecito
Una minaccia nascosta

Un cryptominer illecito è un codice potenzialmente indesiderato o maligno progettato per dirottare la potenza di elaborazione inutilizzata di un dispositivo e usarlo in modo improprio per estrarre la criptovaluta. La minaccia è di solito nascosta o si svolge in background.

Ci sono due tipi principali di cryptominer:

Binary-based cryptominers
sono applicazioni dannose scaricate e installate sul dispositivo mirato con l'obiettivo di estrarre la crittovaluta. Le soluzioni di sicurezza ESET classificano la maggior parte di queste applicazioni come Trojan.

Browser-based cryptominers
utilizza un JavaScript dannoso incorporato in una pagina web o in alcune delle sue parti/oggetti per estrarre la crittovaluta attraverso i browser dei visitatori del sito. Questo metodo è soprannominato **criptojacking** ed è diventato sempre più popolare tra i cyber-criminali a partire dalla metà del 2017. ESET rileva la maggior parte degli script di criptojacking come applicazioni potenzialmente indesiderate (PUA).

Lo sapevi?

La maggior parte degli attacchi cryptominer tenta di estrarre Monero o Ethereum poiché offrono diversi vantaggi rispetto al più noto Bitcoin: hanno un livello più elevato di anonimato delle transazioni e, cosa più importante, possono essere estratti con normali CPU e GPU invece di costosi hardware specializzati.

I possibili danni causati dal cryptomining

Grazie alle loro prestazioni più elevate, l'hardware e le reti di livello aziendale sono obiettivi più preziosi rispetto ai dispositivi di consumo, offrendo agli aggressori guadagni più elevati in un periodo di tempo più breve.

Nonostante il criptaggio illecito sembri rappresentare una minaccia meno grave degli attacchi più invasivi, le organizzazioni non dovrebbero sottovalutare il rischio che rappresenta. Questi attacchi di solito dirottano gran parte della potenza di elaborazione hardware.

Il risultato è:

1. **prestazioni ridotte**
2. **minore produttività**
3. **danni ai dispositivi colpiti,** poiché il processo di estrazione di energia pone un ulteriore stress ai componenti hardware, ne accorciano la durata di utilizzo.
4. **I Cryptominer espongono le vulnerabilità della sicurezza informatica di un'organizzazione** che possono portare nel futuro a gravi danni e interruzioni.

Il 50% degli MSP identifica il cripto-malware come una delle maggiori sfide di sicurezza che incontrano con i loro clienti.

Fonte: * ESET ha eseguito un sondaggio su 488 partner MSP in 14 paesi, nel luglio 2019, tramite un questionario online.

Di seguito le cause del carico computazionale aggiuntivo sui dispositivi Android:

- Durata inferiore della batteria
- Notevole aumento della temperatura del dispositivo
- Minore produttività del dispositivo
- Nei casi peggiori, danni fisici alla batteria dovuti al "gonfiore"

Mantenete la vostra infrastruttura IT libera dai rischi del cryptomining

- Proteggere endpoint, server e altri dispositivi implementando **soluzioni di sicurezza affidabili e multistrato** in grado di rilevare script di cryptomining potenzialmente indesiderati (PUA) e Trojan di cryptomining

- Implementare un **software di Intrusion Detection (IDS)** che aiuta a identificare i modelli di rete sospetti e le comunicazioni potenzialmente legate a cryptomining illecito (ad es. domini infetti, connessioni in uscita su tipiche porte di mining come 3333, 4444 o 8333, segni di persistenza, ecc.)

- **Aumentare la visibilità della rete** utilizzando una console di gestione remota per applicare le politiche di sicurezza, monitorare lo stato del sistema e proteggere gli endpoint e i server aziendali

- **Istruire tutti i dipendenti** (compresi i dirigenti e gli amministratori di rete) su come mantenere una buona igiene informatica e creare e utilizzare password forti, rafforzate con l'autenticazione a più fattori, aumentando così la protezione dei sistemi aziendali in caso di fuga di notizie o di attacchi di brute-force delle password

- Seguire il **principio del privilegio minimo**. Tutti gli utenti devono avere un account utente con i permessi minimi necessari per poter completare le loro mansioni attuali. Questo approccio riduce significativamente il rischio che utenti e amministratori siano manipolati per aprire o installare cryptominer o altri software dannosi in un dispositivo collegato alla rete aziendale

- Utilizzare **controlli di applicazione** che riducono al minimo l'utilizzo del software in esecuzione, impedendo l'installazione di malware di cryptomining

- Implementare una **buona** politica di aggiornamento e patch per ridurre significativamente la possibilità che un'organizzazione sia compromessa da vulnerabilità precedentemente note; molti cryptominer avanzati utilizzano exploit noti, come EternalBlue, per la loro distribuzione primaria

- **Monitorare** i sistemi aziendali per rilevare un **eccessivo consumo di energia** o altre anomalie di consumo energetico che potrebbero indicare un'attività di cryptomining non richiesta.

4 Sicurezza della password, cosa c'è in gioco?

Le password sono una misura di sicurezza di base, ma il loro numero e la loro complessità crescenti le rendono difficili da gestire e da utilizzare in sicurezza. Ecco perché sono necessarie ulteriori soluzioni di protezione, come l'autenticazione a più fattori (MFA), per rafforzare l'accesso con password.

Le PMI sono un punto molto appetibili per i criminali informatici, in quanto dispongono di dati e beni più preziosi rispetto ai semplici consumatori, e sono più vulnerabili rispetto alle imprese, che hanno budget per la sicurezza più elevati. Questo problema è amplificato dal numero crescente di aziende che incorporano dispositivi "intelligenti" nella loro infrastruttura IT. Mentre l'Internet delle cose (Internet of Things - IoT) li aiuta a rendere le operazioni commerciali più veloci e più fluide, questi dispositivi sono spesso vulnerabili e funzionano con nomi utente e password di amministrazione di default disponibili al pubblico, rappresentando un rischio che può portare a conseguenze dannose.

Secondo il Verizon 2017 Data Breach Investigations Report, ben l'**81% delle** violazioni di dati **sono state causate da password deboli o rubate.** Dato che oltre 5 miliardi di password sono trapelate online, la protezione offerta dalle password di base è stata resa inefficace.

Implicazioni dovute a una scarsa sicurezza delle password

Il regolamento generale dell'UE sulla protezione dei dati (GDPR) stabilisce che **le organizzazioni di tutte le dimensioni devono garantire la sicurezza dei dati in loro possesso** attuando "adeguate misure tecniche e organizzative". Quindi, se si verifica una violazione e sono presenti solo password semplici e statiche, è possibile incorrere in una grossa multa.

Modi per migliorare la protezione della password

Implementare politiche efficaci in materia di password. I dipendenti devono essere formati su come creare password forti

8 passi per creare password forti

Il vostro dipartimento IT dovrebbe implementare delle regole quando si stabilisce e si applica la politica aziendale in materia di password

6 regole fondamentali per una corretta gestione delle password

Per proteggere meglio i dati, utilizzare l'autenticazione a più fattori (MFA)

ESET Secure Authentication (Autenticazione sicura ESET)

Protezione ancora più forte

Poiché gli SMS e i dispositivi mobili sono spesso soggetti ad attacchi di malware, le moderne soluzioni MFA tendono a utilizzare notifiche push, più sicure e di facile utilizzo, piuttosto che la verifica via SMS. Per aumentare ulteriormente la sicurezza del processo di autenticazione, le organizzazioni possono aggiungere una protezione **biometrica,-** *qualcosa che fa parte dell'utente, per* aumentare la protezione dell'accesso.

AFFRONTARE
LE PRINCIPALI SFIDE PER LA SICUREZZA DELLE PMI

Affrontare i ransomware, combattere la social engeeniring, fermare la cryptomining illecita e rafforzare la sicurezza delle password.

COME PUÒ AIUTARTI ESET

ESET Italia Srl

Via Campo Lodigiano, 3
20122 - Milano
Tel.: +39 02 3032 8208
esetitaly@eset.com

https://www.eset.com/it/

CYBERSECURITY EXPERTS ON YOUR SIDE