2cents on Security
Pillole di Cyber Sicurezza

EUROPEAN CYBER SECURITY MONTH

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

#11 ENISA THREAT LANDSCAPE 2025 | 4 TREND CHIAVE SULLA CYBERSECURITY

I 4 TREND CHIAVE DA CONOSCERE PER L'EUROPEAN CYBERSECURITY MONTH (ECSM)

IL REPORT:

- L'Agenzia dell'Unione Europea per la Cybersecurity (ENISA) ha analizzato circa 4.900 incidenti nel periodo Luglio 2024 - Giugno 2025.
- Il panorama delle minacce è sempre più maturo e caratterizzato da rapidità di sfruttamento delle vulnerabilità.

TREND #1:
IL PHISHING È UNA PRATICA SEMPRE PIÙ DIFFUSA

KEY HIGHLIGHTS:

- Il Phishing rimane il vettore di intrusione primario degli attacchi, responsabile del 60% circa dei casi osservati.
- Nuove forme di attacco sempre più credibili: casi di phishing attraverso il QR Code (Quishing);
- Cresce il fenomeno del Phishing-as-a-Service (PhaaS), con piattaforme progettate per automatizzare la generazione di kit di phishing che abbassano la soglia di accesso per i criminali.

COME DIFENDERSI:

Non fidarti di email, messaggi o richieste urgenti. Verifica sempre il mittente e non cliccare su link o allegati sospetti.

TREND #2:
L'AI POTENZIA GLI ATTACCHI

KEY HIGHLIGHTS:

- L'Intelligenza Artificiale non è solo uno strumento per il social engineering, ma per l'intera catena di attacco.
- L'AI viene sfruttata per automatizzare la scansione delle reti, identificare le vulnerabilità e creare codici malevoli ad alta efficacia.
- Impatto Strategico: L'AI contribuisce a campagne più continue, diversificate e convergenti che, collettivamente, erodono la resilienza del sistema.

COME DIFENDERSI:

Adottare un approccio proattivo alla difesa, integrando l'automazione dei processi di rilevamento e risposta per contrastare la velocità della minaccia AI.

TREND #3:
LA SUPPLY CHAIN COME "ANELLO DEBOLE"

KEY HIGHLIGHTS:

- L'abuso delle dipendenze cibernetiche (fornitori, partner esterni) si è intensificato.
- Il rischio legato alla Supply Chain (catena di fornitura) rappresenta il 10,6% delle categorie di minaccia totali.
- Gli aggressori prendono di mira i fornitori di servizi, compromettono repository open-source o sfruttano estensioni malevole per browser per amplificare il danno attraverso ecosistemi digitali interconnessi.

COME DIFENDERSI:

Valuta la sicurezza dei tuoi fornitori. Verifica sempre la fonte dei software che scarichi e utilizzi.

TREND #4:
MINACCE AI DISPOSITIVI MOBILI (42,4%)

KEY HIGHLIGHTS:

- Le minacce rivolte ai dispositivi mobili costituiscono la quota maggiore di tutte le categorie di minaccia, raggiungendo il 42,4%.
- I cybercriminali sfruttano i dispositivi mobili, spesso meno protetti, per accedere a dati sensibili, credenziali e reti aziendali.

COME DIFENDERSI:

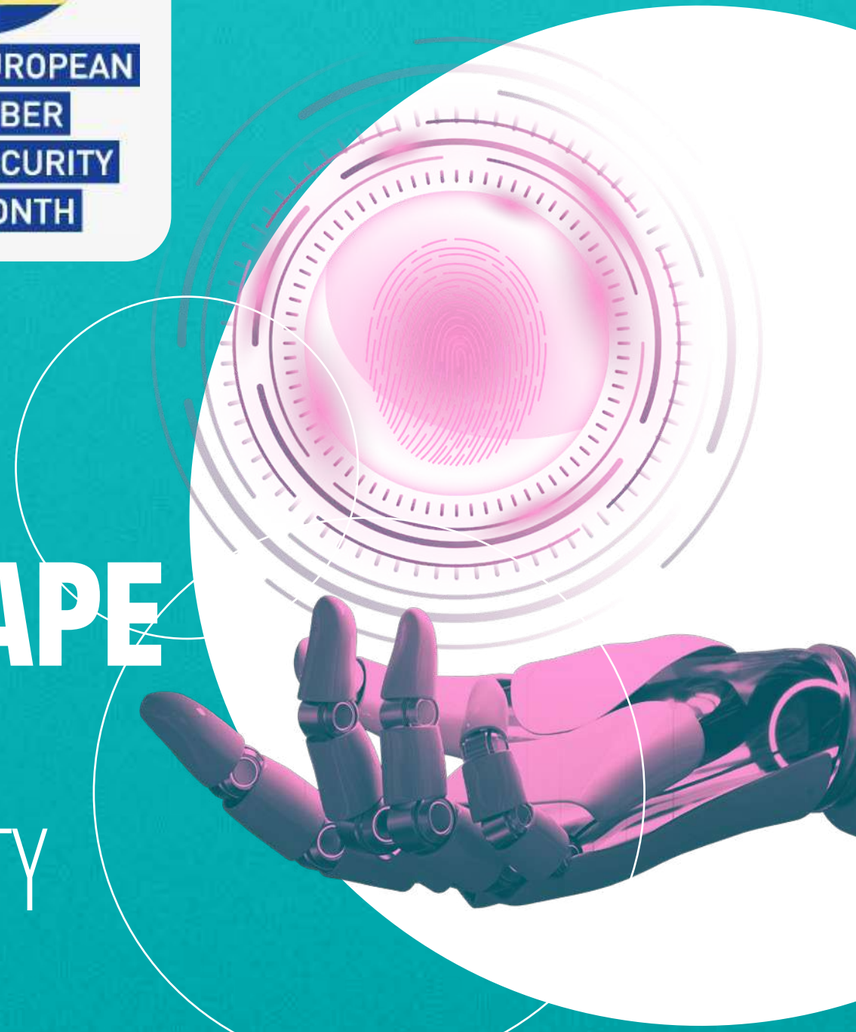
Non eseguire il jailbreak o il root del tuo dispositivo. Utilizza soluzioni di sicurezza mobile e mantieni sempre aggiornati il sistema operativo e le app per correggere le vulnerabilità.

2cents on Security

Pillole di Cyber Sicurezza

EUROPEAN CYBER SECURITY MONTH

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER



#11 ENISA THREAT LANDSCAPE 2025

I 4 TREND CHIAVE SULLA CYBERSECURITY

I 4 TREND CHIAVE DA CONOSCERE PER L'EUROPEAN CYBERSECURITY MONTH (ECSM)

IL REPORT:

- **L'Agenzia dell'Unione Europea per la Cybersecurity (ENISA) ha analizzato circa 4.900 incidenti nel periodo Luglio 2024 - Giugno 2025.**

- **Il panorama delle minacce è sempre più maturo e caratterizzato da rapidità di sfruttamento delle vulnerabilità.**

TREND #1:

IL PHISHING È UNA PRATICA SEMPRE PIÙ DIFFUSA

KEY HIGHLIGHTS:

- **Il Phishing rimane il vettore di intrusione primario degli attacchi, responsabile del 60% circa dei casi osservati.**
- **Nuove forme di attacco sempre più credibili: casi di phishing attraverso il QR Code (Quishing);**
- **Cresce il fenomeno del Phishing-as-a-Service (PhaaS), con piattaforme progettate per automatizzare la generazione di kit di phishing che abbassano la soglia di accesso per i criminali.**

COME DIFENDERSI:

Non fidarti di email, messaggi o richieste urgenti. Verifica sempre il mittente e non cliccare su link o allegati sospetti.

TREND #2:

L'AI POTENZIA GLI ATTACCHI

KEY HIGHLIGHTS:

- **L'Intelligenza Artificiale non è solo uno strumento per il social engineering, ma per l'intera catena di attacco.**
- **L'AI viene sfruttata per automatizzare la scansione delle reti, identificare le vulnerabilità e creare codici malevoli ad alta efficacia.**
- **Impatto Strategico: L'AI contribuisce a campagne più continue, diversificate e convergenti che, collettivamente, erodono la resilienza del sistema.**

COME DIFENDERSI:

Adottare un approccio proattivo alla difesa, integrando l'automazione dei processi di rilevamento e risposta per contrastare la velocità della minaccia AI.

TREND #3:

LA SUPPLY CHAIN COME "ANELLO DEBOLE"

KEY HIGHLIGHTS:

- **L'abuso delle dipendenze cibernetiche (fornitori, partner esterni) si è intensificato.**
- **Il rischio legato alla Supply Chain (catena di fornitura) rappresenta il 10,6% delle categorie di minaccia totali.**
- **Gli aggressori prendono di mira i fornitori di servizi, compromettono repository open-source o sfruttano estensioni malevole per browser per amplificare il danno attraverso ecosistemi digitali interconnessi.**

COME DIFENDERSI:

Valuta la sicurezza dei tuoi fornitori. Verifica sempre la fonte dei software che scarichi e utilizzi.

TREND #4:
MINACCE AI DISPOSITIVI MOBILI (42,4%)

KEY HIGHLIGHTS:

- **Le minacce rivolte ai dispositivi mobili costituiscono la quota maggiore di tutte le categorie di minaccia, raggiungendo il 42,4%.**
- **I cybercriminali sfruttano i dispositivi mobili, spesso meno protetti, per accedere a dati sensibili, credenziali e reti aziendali.**

COME DIFENDERSI:

Non eseguire il jailbreak o il root del tuo dispositivo. Utilizza soluzioni di sicurezza mobile e mantieni sempre aggiornati il sistema operativo e le app per correggere le vulnerabilità.