REGIONE PIEMONTE

CSI your digital partner

WEBINAR
SICURI di essere SICURI?

La gestione degli incidenti cyber: casi reali

Cybercrime: tecniche investigative e strategie di prevenzione

Relatore Comm. Capo Francesco Saverio Bacco
COSC – Polizia Postale Torino

La gestione degli incidenti cyber: casi reali

Azienda vittima – settore automotive

DINAMICA ATTACCO

1. Social engineering a danno di soggetti neo-assunti (screening social network, LinkedIn, c.v);
2. Campagna di phishing su utenze con dominio aziendale; (falso dominio di servizio supporto);
3. Compromissione account aziendali VPN;
4. Movimento laterale verso account con privilegi elevati;
5. Compromissione mediante cifratura dei NAS;
6. Data breach: lista file trafugati – lista account compromessi;

La gestione degli incidenti cyber: casi reali

CYBER KILL CHAIN / 1
Struttura tipo di un cyber attack

- ✓ OSINT / Social Engineering / spear phishing;
- ✓ Scelta strategica del giorno e della fascia oraria dell'attacco (ad es. giorni festivi, pausa pranzo);
- ✓ Attività di port scanning, penetretion testing;
- ✓ Individuazione hardware in rete;
- ✓ Mappatura di rete, enumerazione, movimenti laterali;
- ✓ Riconoscimento vulnerabilità / EXPLOIT

La gestione degli incidenti cyber: casi reali

CYBER KILL CHAIN / 2

- ✓ Privilege escalation;
- ✓ Impostazione regole di re-inoltro di mail/condivisione dati/ attenuazione policy di controllo;
- ✓ Inoculazione di script malevoli;
- ✓ Creazione di persistenze nella struttura di rete;
- ✓ Attivazione payload;
- ✓ Interlocuzione con Comando e Controllo – «call home» del malware.

La gestione degli incidenti cyber: casi reali

INDAGINI

1. OSINT sul data breach;
2. Analisi del falso dominio;
3. Analisi degli IP log sulla VPN aziendale;
4. Analisi dei dischi alterati;
5. Preservation request;
6. Richieste di cooperazione internazionale;
7. Emissione di richieste rogatoriali.

REGIONE PIEMONTE

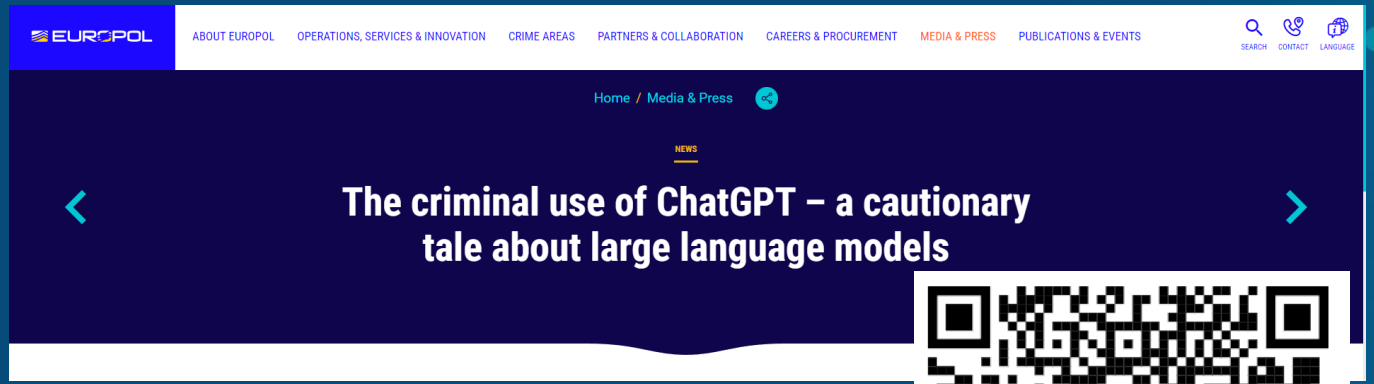
CSI your digital partner

WEBINAR

SICURI di essere SICURI?

La gestione degli incidenti cyber: casi reali

AI E CYBERCRIME



La gestione degli incidenti cyber: casi reali

Regolamento Europeo sull' Intelligenza Artificiale

Approvazione in Parlamento Europeo il 13 Marzo 24

Applicazioni vietate:

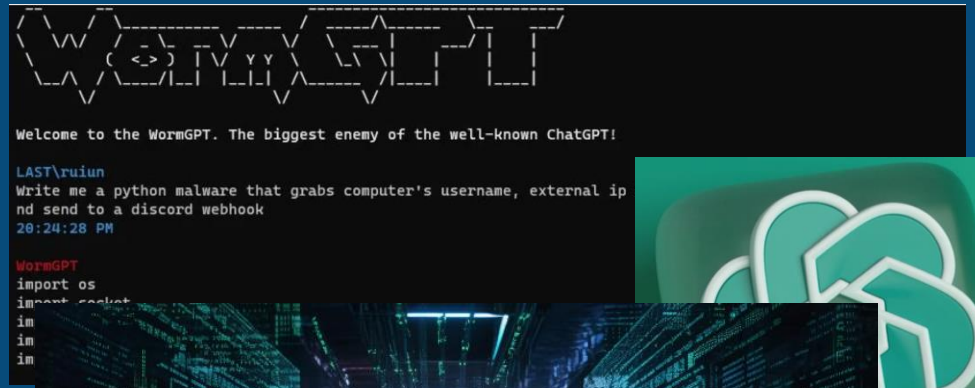
- ✓ Analisi biometrica su caratteri sensibili;
- ✓ Estrapolazione indiscriminata di immagini;
- ✓ Analisi emozionale;
- ✓ Sistemi di credito sociale;
- ✓ Predictive Policing

Sistemi ad alto rischio:

- ✓ Incidenza su settori critici (giustizia, sanità educazione);
- ✓ Valutazione e riduzione rischi;
- ✓ Mantenimento registri d'uso;
- ✓ Sorveglianza umana;
- ✓ Possibilità di formulare reclami;
- ✓ Argomentazione delle decisioni.

La gestione degli incidenti cyber: casi reali

AI E CYBERCRIME



La gestione degli incidenti cyber: casi reali

Cyber attacchi, Polizia Postale:

"1.008 casi solo a gennaio scorso, 66 critici contro PA e aziende"

Gennaio 2024: **1008** casi di sicurezza cibernetica

Rilevati attacchi:
Ransomware, DDoS, diffusione di Malware e altre tecniche di hacking (come Advanced Persistent Threat (APT), Databreach, Infostealer, ecc...)

Gennaio 2024: **66** cyber attacchi critici contro **Infrastrutture Critiche, Operatori di Servizi Essenziali** e **Pubbliche Amministrazioni Locali**

Fonte:
Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche

La gestione degli incidenti cyber: casi reali

RILEVAZIONE STATISTICA CNAIPIC
Attacchi gestiti

ANNO 2023	
Attacchi rilevati	12.101
Alert diramati	77.012
Indagini avviate dal C.N.A.I.P.I.C.	96
Persone indagate	224
Richiesta di cooperazione internazionale in ambito Rete 24/7 High Tech Crime G8 (Convenzione Budapest)	79
Attacchi Ransomware	269

La gestione degli incidenti cyber: casi reali

Previsioni sui costi della criminalità informatica

$ 10,5

Il costo globale della criminalità informatica raggiungerà i **10.5 trilioni di dollari** entro il 2025

INTERPOL

Interpol Secretary General Jurgen Stock
Interpol's 90th General Assembly