Polizia di Stato

LEGALITÀ, CI PIACE!
CONFCOMMERCIO

20 Aprile

Polizia di Stato

POLIZIA POSTALE E DELLE COMUNICAZIONI

Dai reati Postali a quelli legati al mondo ICT

Servizio Centrale
CNAIPIC e CNCPO

20 *Compartimenti regionali*

80 *Sezioni provinciali*

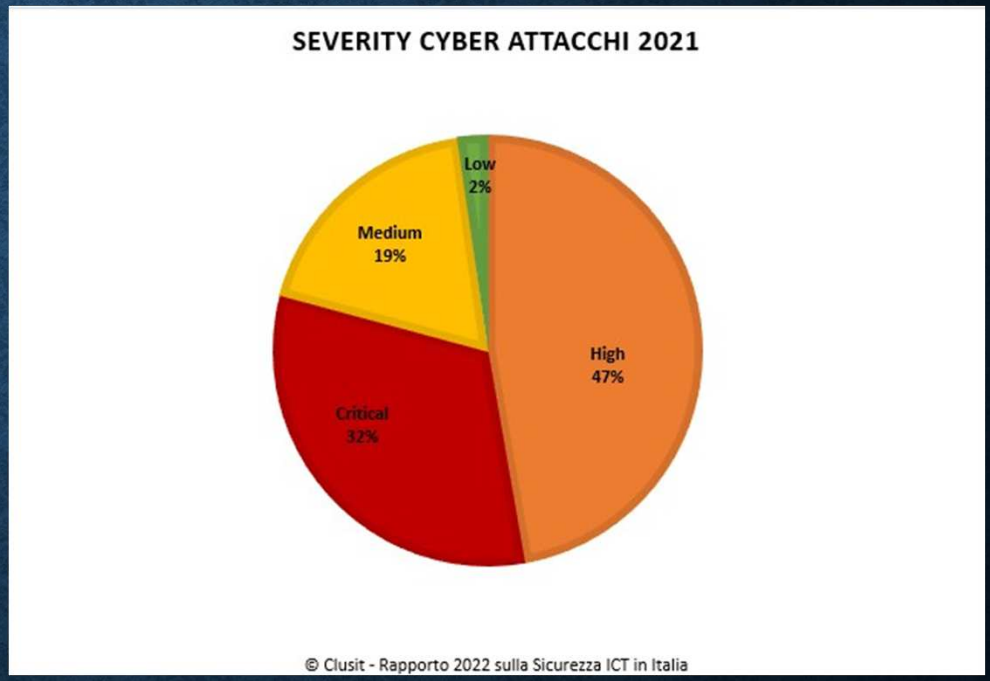
Competenze (DM 15 agosto 2017):

- Pedopornografia online
- Cyberterrorismo
- Financial cybercrime
- Protezione infrastrutture critiche
- Intrusioni informatiche

Polizia di Stato

DATI STATISTICI

- Nel 2021 sono stati registrati 2049 cyberattacchi gravi.
- Aumento del 10% rispetto all'anno precedente, per una media mensile di 171 attacchi.
- Gli attacchi crescono in frequenza e in gravità con ripercussioni di immagine, economiche, sociali e geopolitiche.
- Nel 2021 il 79% degli attacchi rilevati ha avuto un impatto elevato, contro il 50% dell'anno scorso.
- Stimati danni per il 2021 in sei trilioni di dollari, contro un trilione di dollari per il 2020.
- Situazione effettiva reale ben peggiore data la tendenza delle vittime a mantenere riservati gli attacchi cyber subiti nonostante il Regolamento GDPR e la Direttiva NIS.

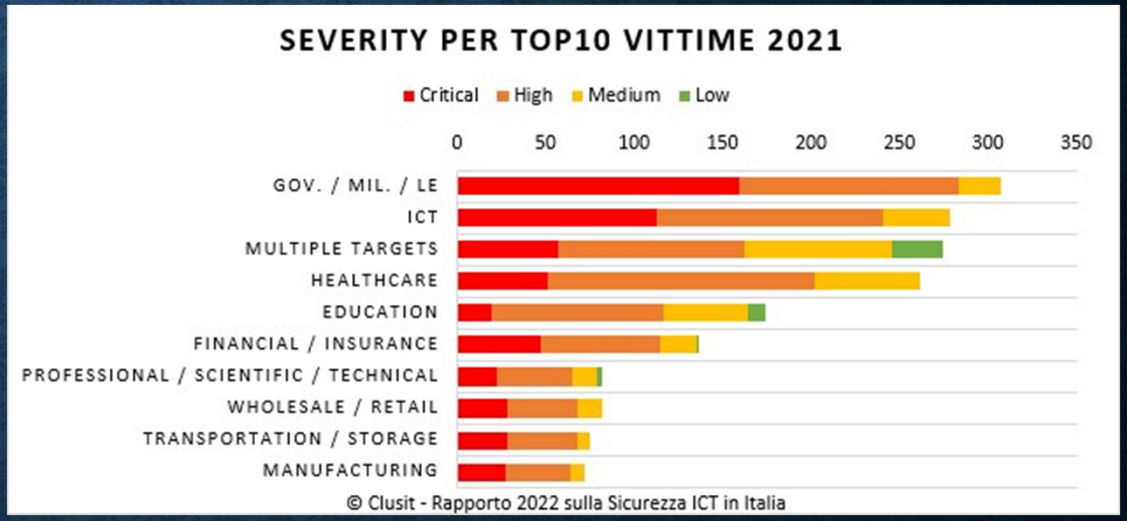


(Clusit – rapporto 2022 sulla Sicurezza ICT in Italia)

Polizia di Stato

DATI STATISTICI

- Cybercrime si conferma la motivazione dell' 86% dei cyber attacchi.
- 11% riferibile ad attività di espionage.
- 2% campagne di information warfare.
- I cybercriminali non colpiscono più in modo indifferenziato obiettivi molteplici, ma mirano a colpire bersagli ben precisi.



(Clusit – rapporto 2022 sulla Sicurezza ICT in Italia)

Polizia di Stato

GLI ATTORI: ATTACCANTI, OBIETTIVI E VITTIME

Hacker provenienti da scuole dell'est europeo, bulgare,rumene, ucraine, giorgiane o asiatiche; organizzazioni criminali e/o governative

- denaro, contratti, dati, reputazione, segreti industriali .
- Istituzioni, aziende, categorie di professionisti, privati cittadini.

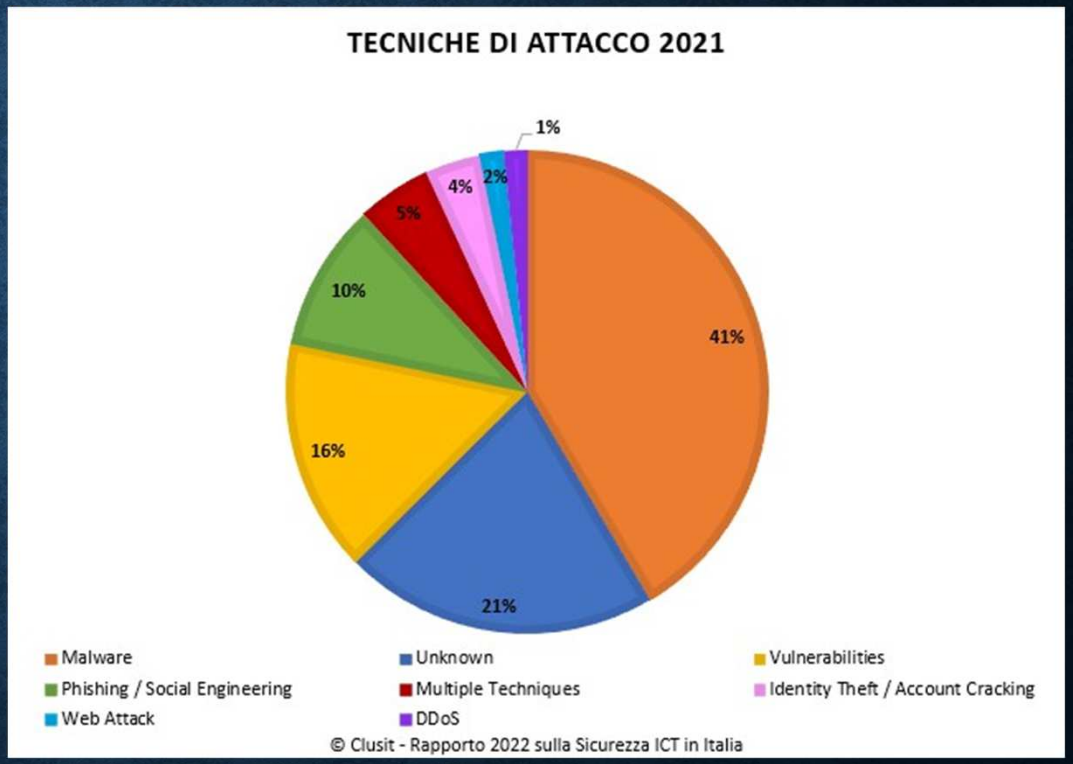
Perché così poca sicurezza

- Diffusione capillare e massiccia di dispositivi elettronici nuovi interessi criminali
- Vulnerabilità tecniche
  - bug nelle applicazioni / S.O.
- Fattore umano
  - evoluzione tecnologica esponenziale *(storage – banda - miniaturizzazione)*
  - scarsa consapevolezza del rischio *(sicurezza ≠ cybersecurity)*

Polizia di Stato

TIPOLOGIE DI ATTACCHI PIÙ UTILIZZATE NELL'ANNO 2021

- Malware (41% Ransomware)
- Unknown (21% Data breach)
- Vulnerabilities
- Phishing/ Social Engineering (ceo fraud, man in the middle)
- Multiple Techniques
- Identity Theft / Account Cracking
- Web attack
- Attacchi DDOS
- Oggi i criminali collaborano attivamente tra loro, si sono consolidati dei cartelli di servizi criminali identificabili come «Ransomware as a Service».



Polizia di Stato

RANSOMWARE: LA RICHIESTA È AUMENTATA DEL 144%

- La richiesta media di riscatto ha raggiunto quota 2,2 milioni di dollari, mentre il pagamento medio è salito del 78%, a 541.010 dollari.

- Il cybercrime dilaga. Nel 2021, i pagamenti estorti alle aziende tramite attacchi ransomware hanno raggiunto nuovi record, con i criminali informatici che si sono rivolti sempre più spesso ai siti del Dark Web minacciando di rilasciare dati sensibili, facendo così pressione sulle vittime.

- I settori più colpiti sono stati i servizi professionali e legali, costruzioni, commercio all'ingrosso e retail, sanitario e manifatturiero.

- Ransomware: tra i gruppi criminali più pericolosi spiccano Conti (15% 1 su 5)e Revil noto anche come Sodinokibi (7,1%)
- seguito da Hello Kitty (4,8%), Phobos (4,8%) e SunCrypt (4,8%). Conti ha anche pubblicato i nomi di 511 organizzazioni sul suo sito Dark Web, confermandosi il più "attivo" tra tutti i gruppi individuati.

- Nel 2021,sono emerse 35 nuove gang ransomware, le imprese criminali hanno investito gli elevati profitti nella creazione di strumenti più semplici da utilizzare, che sfruttano sempre più spesso vulnerabilità zero-day.

- Nel 2021 è aumentato anche dell'85% il numero di vittime i cui dati sono stati pubblicati su siti di leak, raggiungendo quota 2.566 organizzazioni. Di queste, il 60% appartiene al continente americano, 31% all'area EMEA e 9% a quella Asia-Pacifico.

Polizia di Stato

RANSOMWARE: MECCANISMO DELL'ATTACCO

1. L'incursore:
- Conosce i tuoi punti deboli
- Agisce di notte/prima di un giorno festivo

2. I sistemi difensivi vengono bypassati entra nei server paralizza il sistema informatico e preleva :

dati

contratti

accordi

Informazioni riservate

3. Sullo schermo del pc compare un messaggio: *« paga o i tuoi dati saranno diffusi e non più recuperabili»*

4. Il ricatto è sempre di più in criptovalute (Bitcoin e Monero)

Lunedi 15 febbraio 2021 Corriere della Sera – Sezione data room

Polizia di Stato

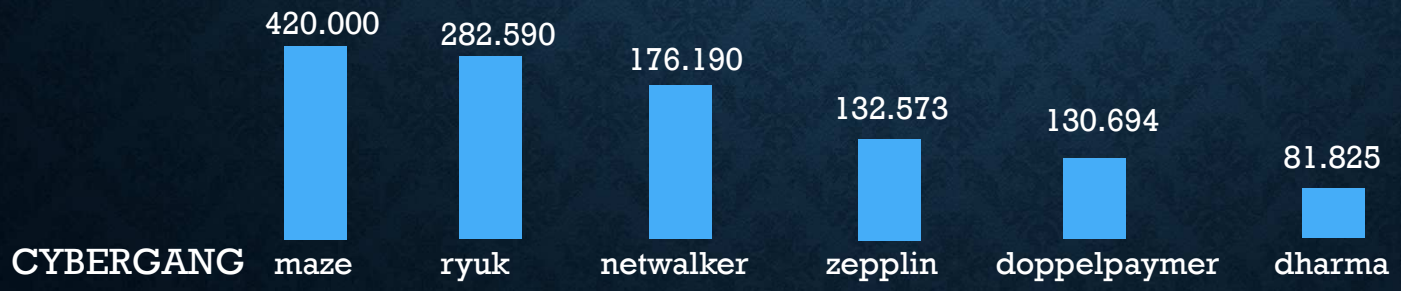
RANSOMWARE

Chi ha sporto denuncia ?? 1 su 4 paga!

le somme più rilevanti richieste in bitcoin

CAMPARI	ENEL	BONFIGLIOLI SPA	COMUNE DI RIETI
16 MILIONI	14 MILIONI	2,4 MILIONI	500 MILA

RICHIESTA MEDIA DELL'ESTORSIONE anno 2020:
(in dollari)



Polizia di Stato

ATTACCO DDOS

- Distribuited denial of service: pratica criminale che consiste nel tempestare di richieste un sito fino a metterlo fuori servizio e renderlo irraggiungibile;
- Si suggerisce di prevedere un servizio di monitoraggio del traffico di rete che permetta di allertare subito l azienda dell'attacco in corso o della sua preparazione.
- Allertare prontamente ISP per valutare azioni di contrasto

Polizia di Stato

ELEMENTI DA INSERIRE NELLA DENUNCIA

Conoscere quando possibile il veicolo di infezione:
(allegato email, intrusione, vulnerabilità di eventuali software, Vulnerabilità VPN specie su sistemi Fortinet non aggiornati, Utenza VPN con credenziali valide etc etc)

Fornire una ricostruzione tecnica di come il virus sia entrato nel sistema.
Un elenco di eventuali servizi esposti alla rete internet
(siti web, teleassistenza, remote desktop, team viewer etc etc)

Elencare la tipologia ed entità di dati cifrati
(database clienti, documenti vari, documenti contabili, documenti personali , dati sensibili etc etc)
Fornire una valutazione economica dei costi sostenuti, sia in termini di intervento tecnico che di mancato guadagno per l'azienda.

Elencare la tipologia di pagamento presente nella richiesta di riscatto
(bitcoin,monero, ucash,paypal. etc etc.) specificando qualora vi sia abbia dato seguito ogni informazione disponibile (ricevute,comunicazioni, email etc etc) – fornire copia della "Ransom note"

Polizia di Stato

IN DENUNCIA

Fornire i log degli apparati di rete relativi al traffico telematico in ingresso/uscita dall'azienda per il periodo antecedente l'infezione al fine di individuare il primo collegamento al server di comando e controllo.

Individuare il software utilizzato per i "lateral movement" all'interno della rete
(Power shell, empire, Cobalt Strike)
le modalità di attacco utilizzate per la privilege escalation
(zero logon- printnightmare etc etc.)

Fornire copia dei dati cifrati e del trojan/beacon/crypter individuato.

Fornire un elenco degli IOC e POC individuati.

Polizia di Stato

COME PROTEGGERSI

Dal punto di vista tecnico :sistemi di monitoraggio del traffico di rete interna(aggiornamento dei sistemi, backup off line/protetto, firewall(FW,)intrusion detector sistem(IDS), intrusion prevent sistem(IPS), etc)

Dal punto di vista umano comportamentale

Evita l'apertura degli allegati delle mail (ebbene sì, ancora questo consiglio!)

Verifica del reale mittente di una mail (punto di partenza di truffe ben organizzate)

Gestione delle password (diverse per ogni sito/servizio – livelli di robustezza diversa)

Rendere la sicurezza «comoda» (pin – sequenza sblocco – impronta digitale)

Consapevolezza dei possibili rischi

Polizia di Stato

BEST PRACTICE

COME MINIMIZZARE I RISCHI DI UN ATTACCO

- PRIMA

- ASSESSMENT : Valutazione del rischio, attivazione dei SOC (Security Operation Center struttura dove vengono centralizzate le informazioni sullo stato di sicurezza IT di una azienda)
- Documentazione e procedure (prove di simulazione di attacco./cosa fare, come agire, prima che accada l incidente)
- « Data panic room « l organizzazione in caso di emergenza, designazione delle persone che dovranno prendere le decisioni durante l attacco

- DAY BY DAY

- Offensive team (es di attacchi buoni x verificare se ci sono delle debolezze/test sui dipendenti/difesa attiva ciò che accade fuori dall azienda. es scansione del web /sentimental analisys/
- CSDC (Monitor & Response) Cyber Security Defense Center/analisti specializzati nell' analisi del traffico di rete, il livello di lavoro dei server, quantità di ram se c'è qualcosa di anomalo nel funzionamento delle macchine etc..

- DURANTE INCIDENTE

- Cert (Computer Emergency Response Team)personale tecnico in grado di fronteggiare l'attacco in corso e/o minimizzare i danni;
- Recovery team (recupero e ripartenza delle macchine dopo l attacco)
- Comunicazione interna che esterna

Polizia di Stato

COLLABORAZIONE CON IL MONDO PRIVATO

La Polizia postale e delle Comunicazioni ha stipulato in Lombardia protocolli di intesa con Assolombarda, Confindustria e Confcommercio al fine di tutelare la sicurezza informatica non solo delle aziende ritenute «infrastrutture critiche» ma anche di alcune aziende con rilevanza strategica per il paese.

Polizia di Stato

CONCLUSIONI

Let me use the title of a famous book, "No place to hide". I mean that both nation-state actors and cybercriminal organizations are spending a growing effort to increase their hacking capabilities and evasion techniques.

Unfortunately, today most of the organizations still consider cybersecurity a cost to cut and this approach gives the attackers an immense advantage.

We need a cultural change and we must consider that a security by design approach is the unique way to make the Internet a safe place.

We also need globally recognized norms of responsible state behavior in cyberspace.

Pierluigi Paganini member of ENISA

Polizia di Stato

Grazie per l'attenzione

VQ Lisa Di Berardino