CYBER-SECURITY:

COSA FARE E COSA NON FARE QUANDO SI SUBISCE UN ATTACCO

6.07.2023

FPI FONDAZIONE PIEMONTE INNOVA

Fondazione Piemonte Innova - già Torino Wireless -
è un partenariato pubblico privato
che abilita l'innovazione e la digitalizzazione
delle imprese e delle organizzazioni non profit
e che affianca le pubbliche amministrazioni
per lo sviluppo di progetti di innovazione sostenibili e replicabili

Modello di supporto Area Compliance

NORMATIVA

Adeguamento GDPR

Servizio DPO

Certificazioni

ORGANIZZATIVA

Revisione processi interni

Revisione modelli organizzativi

Definizione/revisione policy IT

TECNOLOGICA

Prevenzione e gestione attacchi

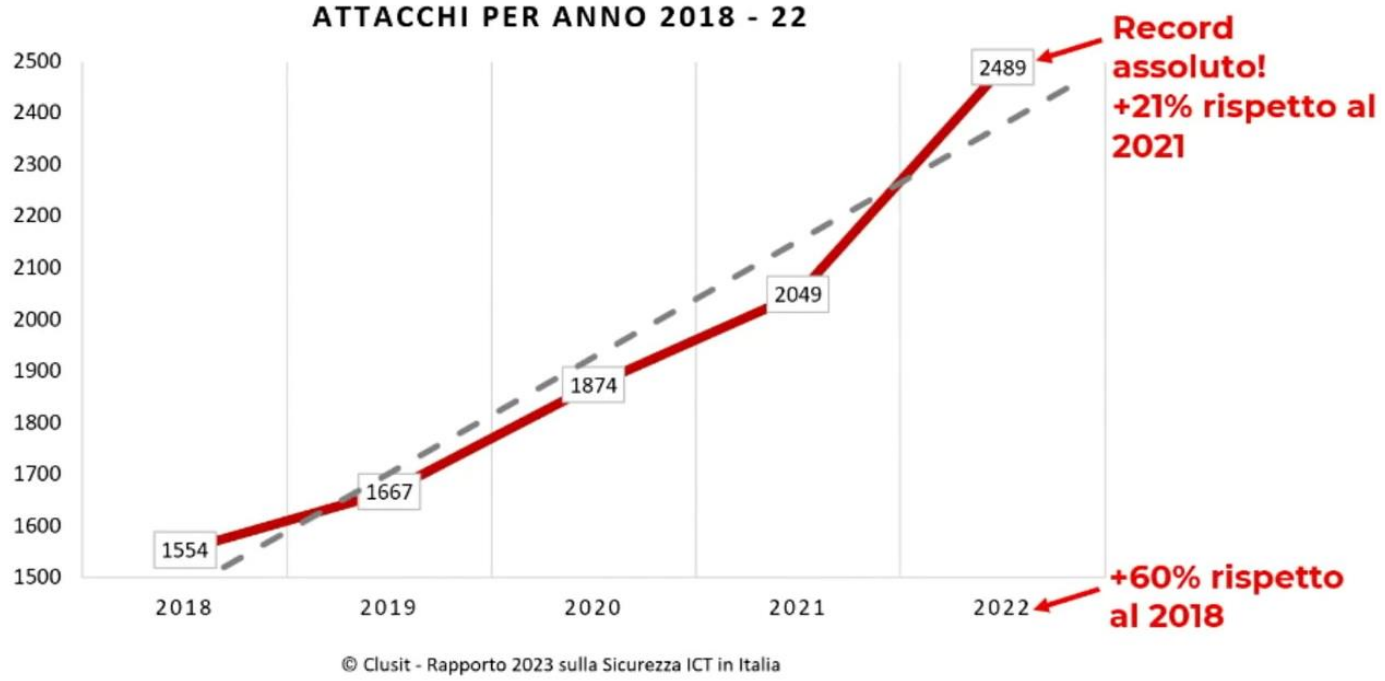
Mitigazione rischi

FONDAZIONE PIEMONTE INNOVA

Agenda

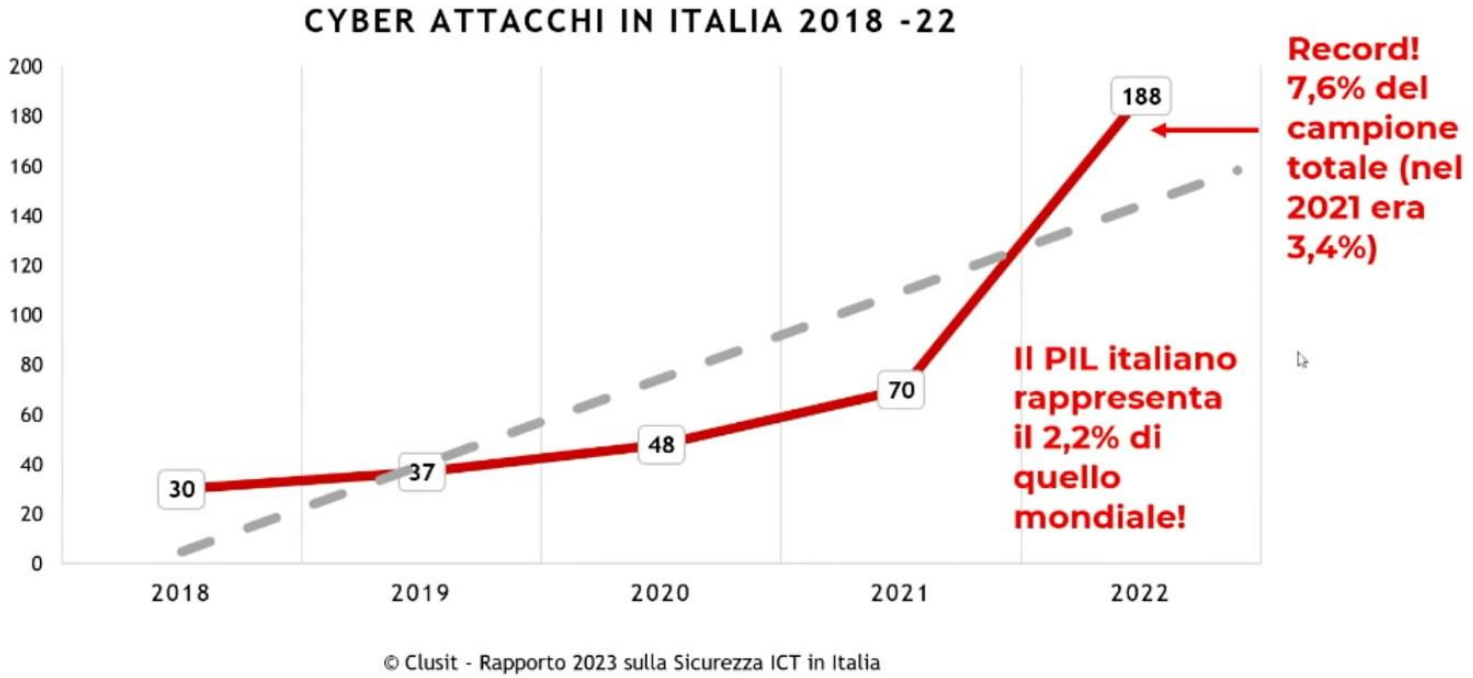
- Attacchi Cyber: scenario
- Tipologie di attacco e come reagire
- La notifica delle violazioni: quando farla e come

Lo scenario globale dei cyber attacchi



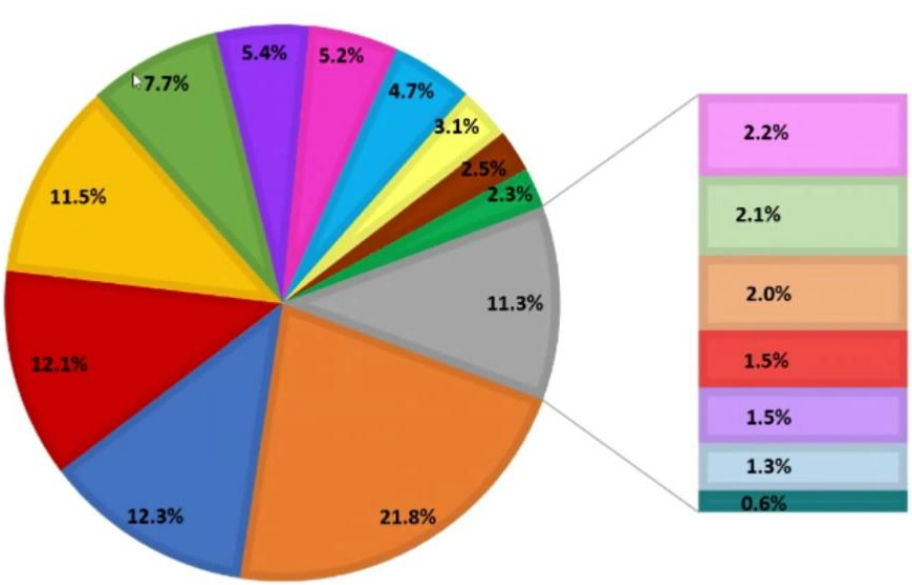
FONDAZIONE PIEMONTE INNOVA

Lo scenario dei cyber attacchi in Italia



FONDAZIONE PIEMONTE INNOVA

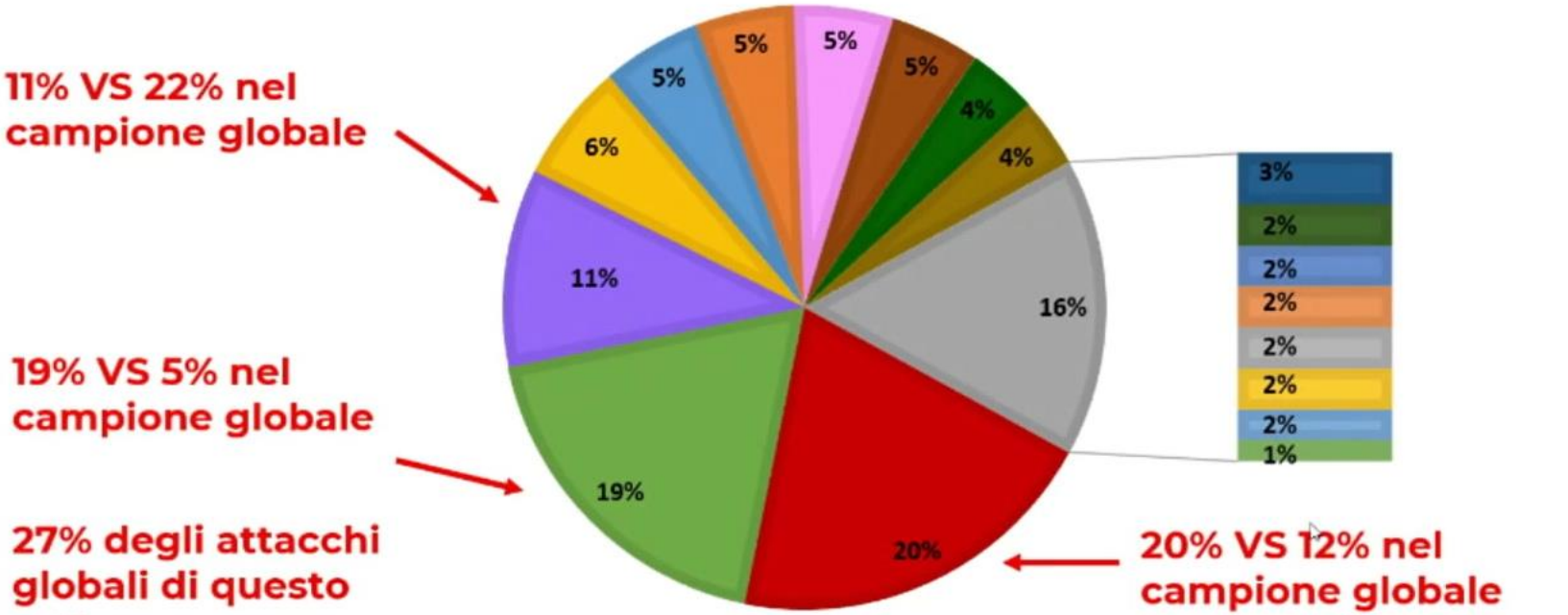
Le vittime nel 2022



- Multiple Targets
- Healthcare
- Gov / Mil / LE
- ICT
- Financial / Insurance
- Education
- Manufacturing
- News / Multimedia
- Professional / Scientific / Technical
- Wholesale / Retail
- Transportation / Storage
- Organizations
- Energy / Utilities
- Arts / Entertainment
- Telecommunications
- Other Services
- Hospitability
- Construction

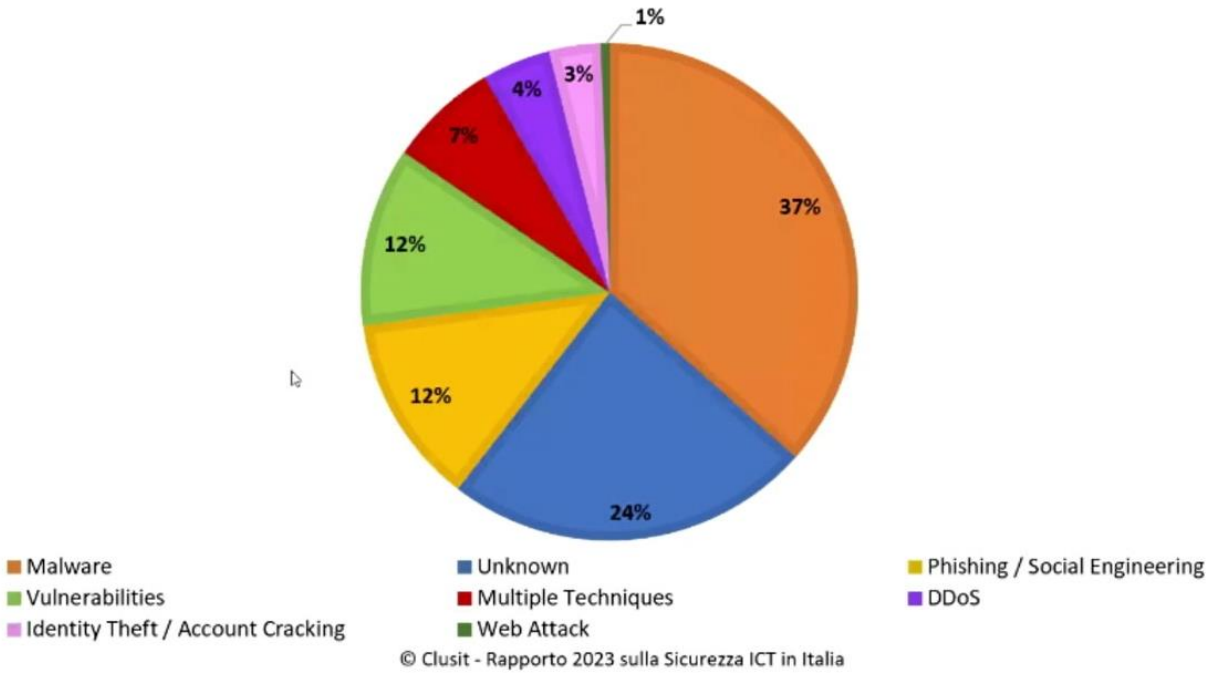
© Clusit - Rapporto 2023 sulla Sicurezza ICT in Italia

Le vittime in Italia nel 2022



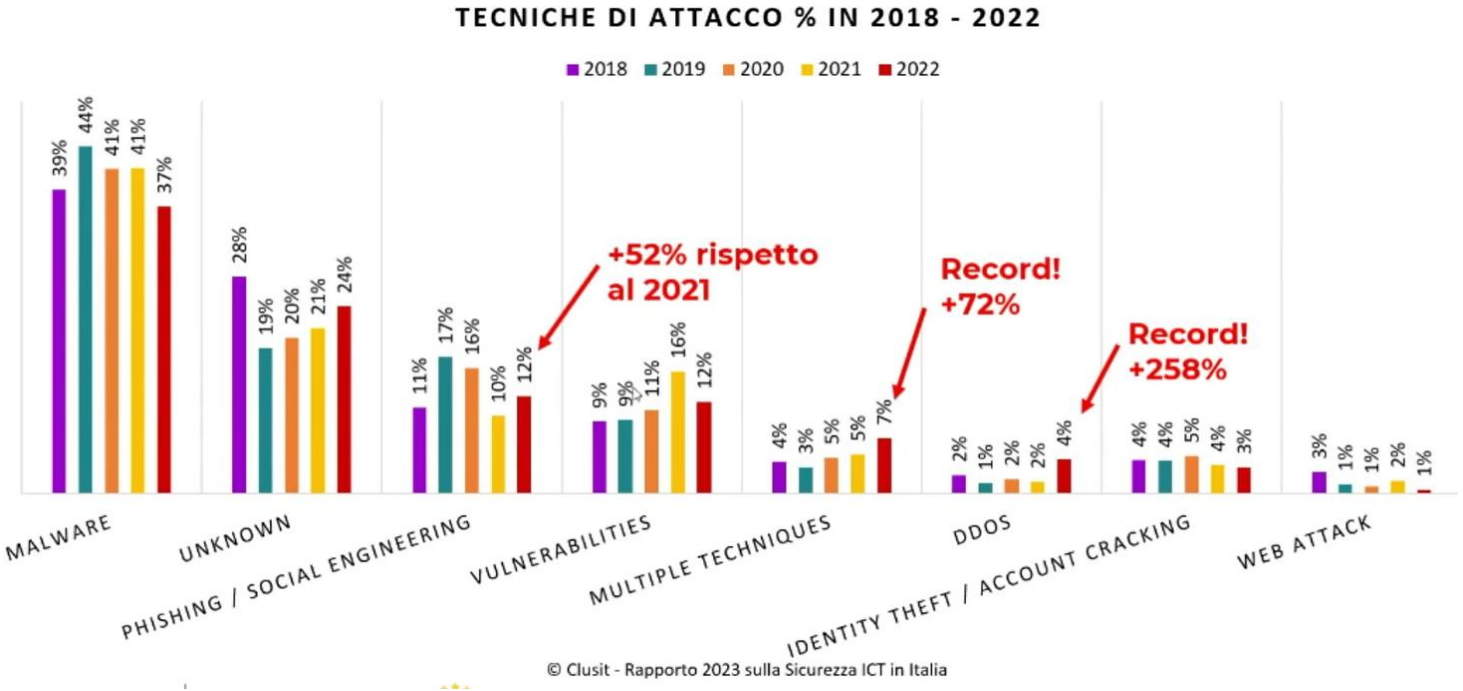
© Clusit - Rapporto 2023 sulla Sicurezza ICT in Italia

Le tecniche di attacco nel 2022



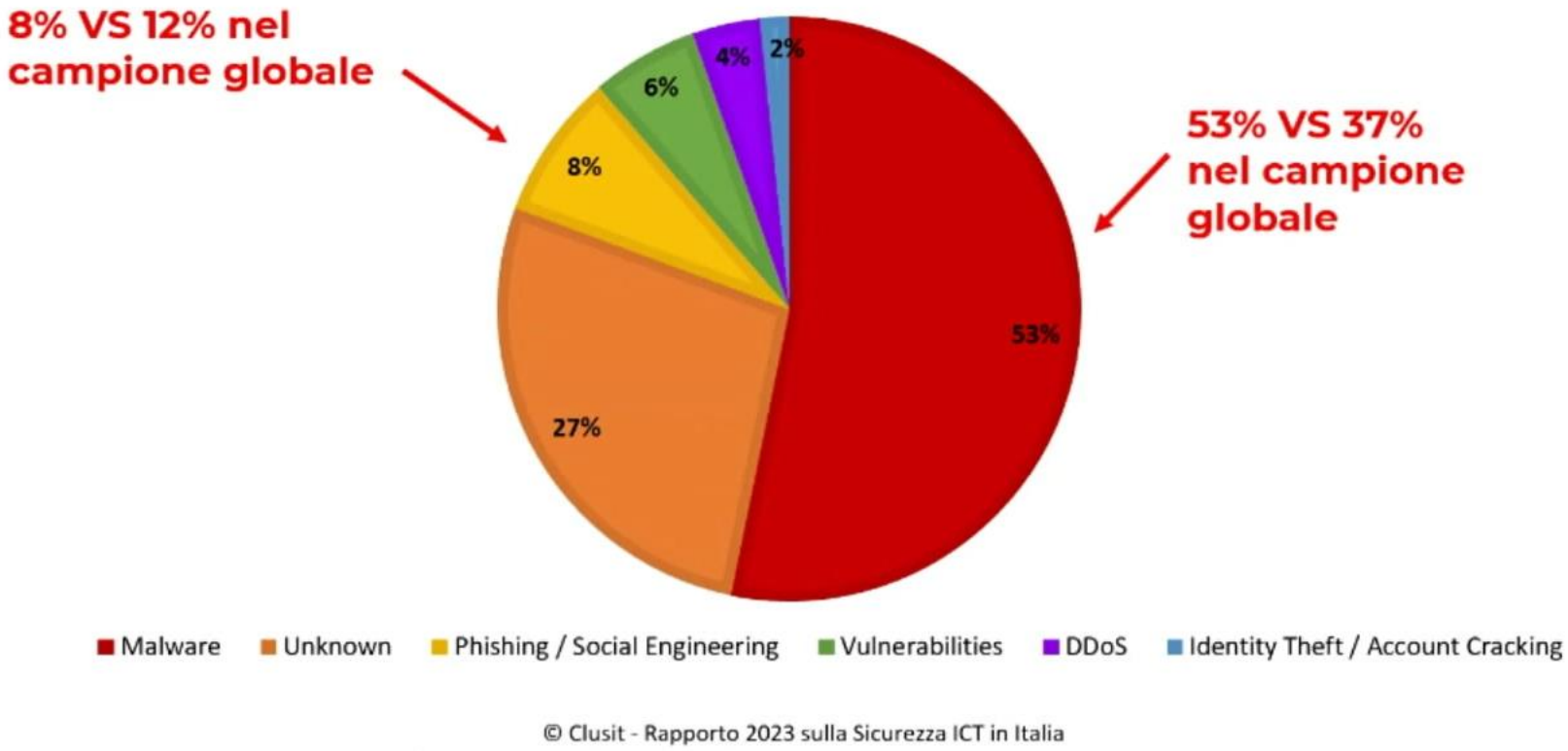
FONDAZIONE PIEMONTE INNOVA

Le tecniche di attacco nel periodo 2018 - 2022



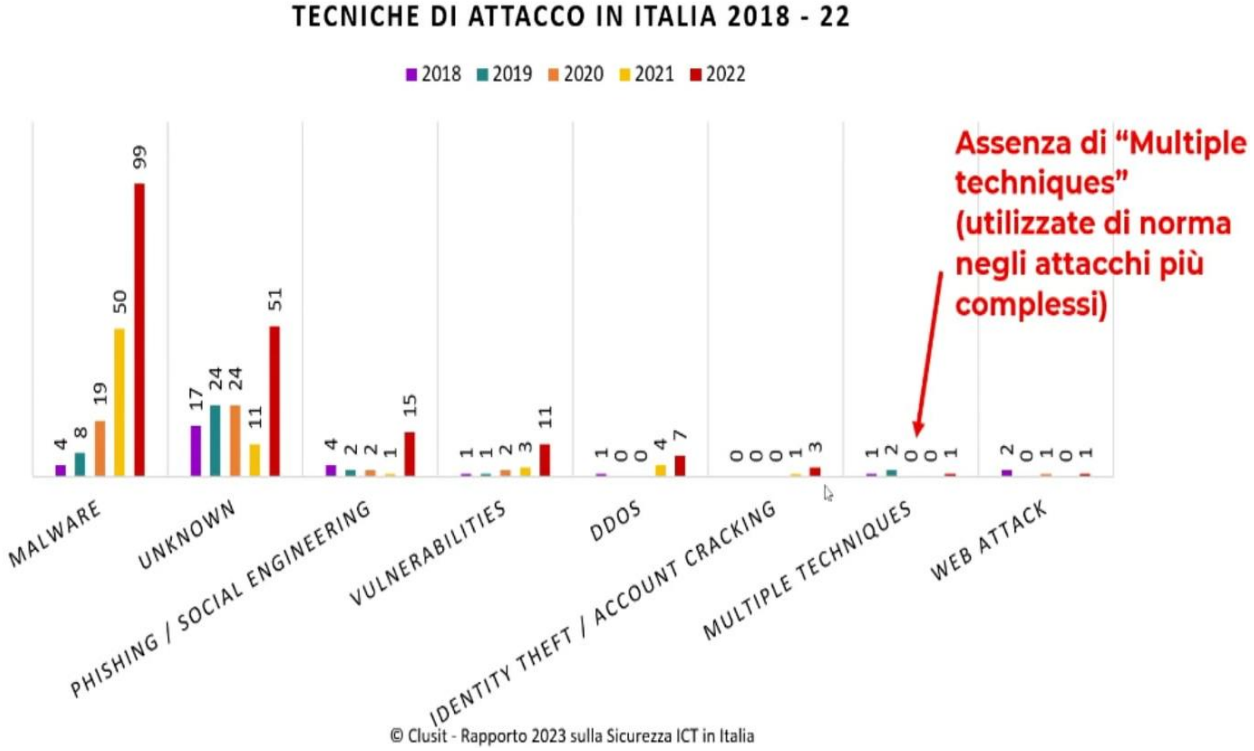
FONDAZIONE PIEMONTE INNOVA

Le tecniche di attacco in Italia nel 2022



© Clusit - Rapporto 2023 sulla Sicurezza ICT in Italia

Le tecniche di attacco in Italia nel periodo 2018 -2022



FONDAZIONE PIEMONTE INNOVA

Ransomware: più livelli di estorsione

1. Crittografia dei dati
2. Esfiltrazione dei dati (Double Extortion)
3. Minaccia di attacco DDoS con interruzione dei servizi
4. Minaccia di informare e/o ricattare anche i clienti

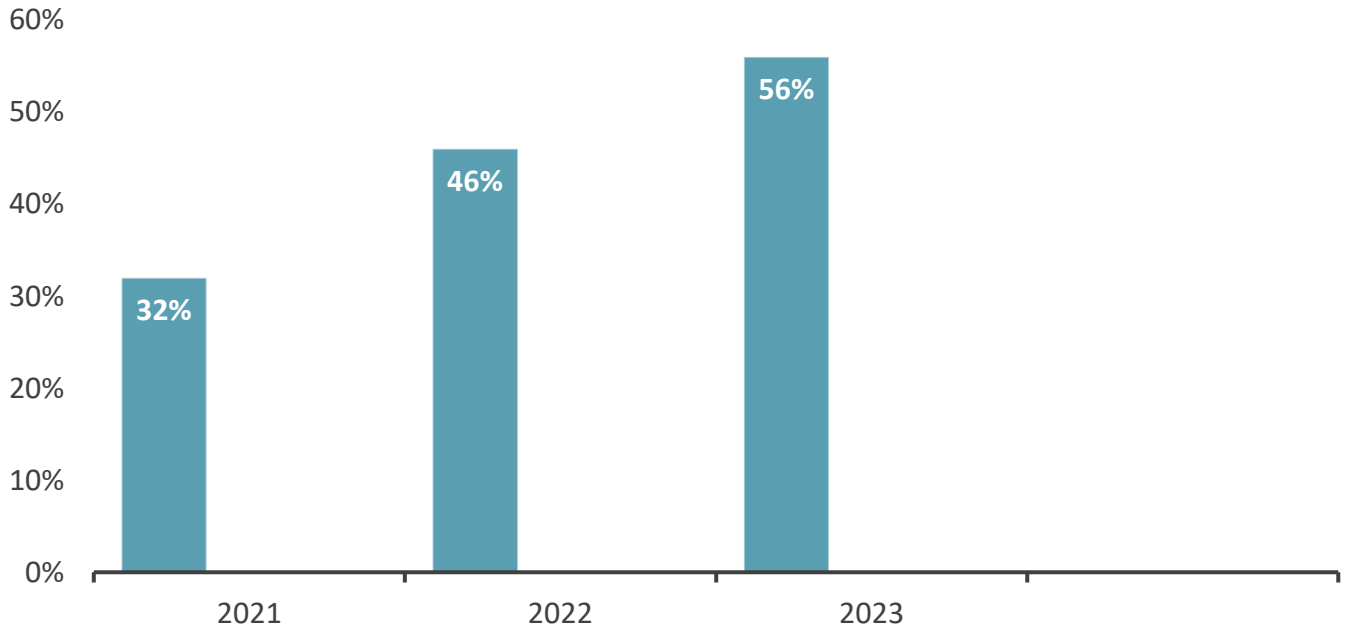
FONDAZIONE PIEMONTE INNOVA

Attacco Ransomware: se decidessi di pagare il riscatto?

→ **pagare il riscatto è illegale**, sia per l'organizzazione che ha subito l'attacco sia per i consulenti di quell'organizzazione

- ✓ Se l'attacco è subito da un ente pubblico, l'ente ha l'obbligo di denunciare l'accaduto ex art. 615-ter
- ✓ Se a subire l'attacco è un'azienda, si potrebbero configurare i reati di **false comunicazioni sociali, ostacolo all'esercizio delle funzioni dell'autorità di vigilanza e impedito controllo**
- ✓ Solo se chi subisce un attacco è un privato, la vittima è da ritenersi in ogni caso parte offesa

Aziende che dichiarano di aver pagato il riscatto



Fonte: Sophos "The State of Ransomware 2023"

Fonte: Sophos "The State of Ransomware 2023"

Ransomware: quali danni si rischiano?

Non si tratta solo del riscatto:

- Fermo attività durante le operazioni di ripristino
- Costi di ripristino dell'infrastruttura
- Costo per l'indagine forense
- Pubblicazione di dati critici e riservati
- Eventuali spese legali per perdita dati sensibili utenti/clienti
- Danno reputazionale

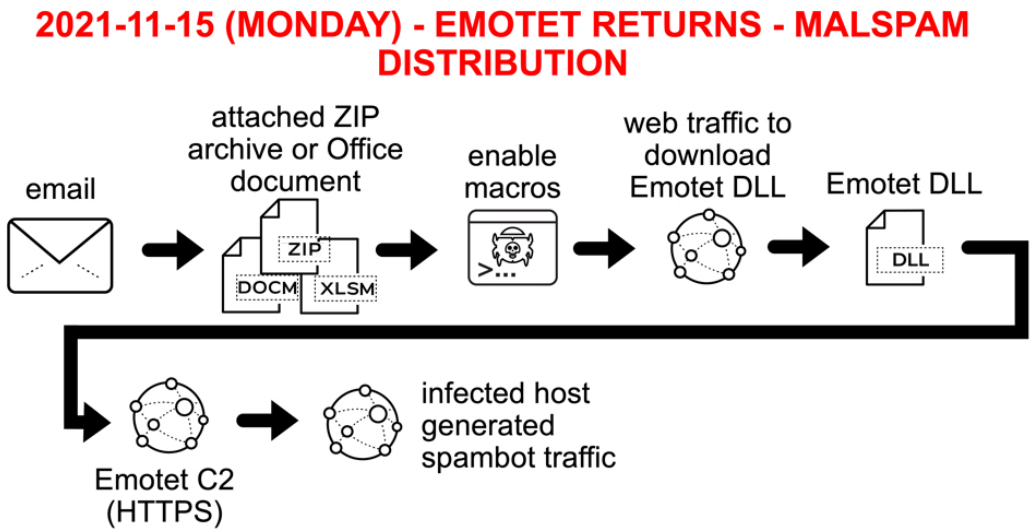
I Vettori d’infezione

Il fattore umano

- Email di phishing
- Navigazione su siti compromessi
- Chiavetta USB armata con SW malevolo
- all’interno di altri software

- **Errori tecnici**
  - Attacchi brute force su desktop remoto
  - Vulnerabilità dei sistemi
  - Supply Chain Attack (caso solar Wind 2020; Kaseya 2021)

Attacco progressivo



FONDAZIONE PIEMONTE INNOVA

Ransomware As a Service (RaaS)

- Industrializzazione del Cybercrime
- Chiunque può acquistare il servizio e chiedere un riscatto
- Dashboard di configurazione
- Gli autori del codice trattengono una quota del ricavato dal riscatti (30-40%)

Cosa fare prima di un attacco

Avere un piano

Identificare le risorse necessarie

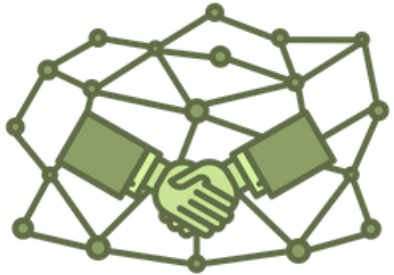
Implementare una tecnologia appropriata per proteggere gli asset fondamentali

Formare i dipendenti e i collaboratori

FONDAZIONE PIEMONTE INNOVA

Cosa fare durante un attacco

Valutare la situazione



Circoscrivere il danno

Raccogliere informazioni per una documentazione legale

FONDAZIONE PIEMONTE INNOVA

Cosa NON fare durante un attacco

Spegnere tutto

Avere fretta

Affidarsi a chiunque

Sottovalutare la comunicazione

FONDAZIONE PIEMONTE INNOVA

Cosa fare dopo l’attacco

Continuare a monitorare i sistemi colpiti

Individuare le misure per prevenire futuri attacchi

FONDAZIONE PIEMONTE INNOVA

A chi notificare?

CSIRT

Istituito con Decreto Legge n. 82/2021, ha tra i compiti principali:

- monitoraggio degli incidenti a livello nazionale;
- emissione di preallarmi, allerte, annunci e divulgazione di informazioni alle parti interessate in merito a rischi e incidenti;
- intervento in caso di incidente;
- analisi dinamica dei rischi e degli incidenti;
- sensibilizzazione situazionale;

A chi notificare?

Istituita nel 1999, ha tra i compiti principali:

- tutelare la sicurezza e la regolarità dei servizi delle telecomunicazioni.;
- prevenzione, controllo e repressione degli illeciti penali ed amministrativi del crimine informatico
- Combatte reati quali:
  - Pedopornografia
  - Cyberterrorismo
  - download illegale
  - truffe sui conti on line
  - Giochi e scommesse on line
  - Tutela del diritto d'autore

A chi notificare?

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Istituito dalla cosiddetta legge sulla privacy (legge 31 dicembre 1996, n. 675) ha tra i suoi compiti:

- controllare che i trattamenti di dati personali siano conformi al Regolamento;
- tenere registri interni delle violazioni più rilevanti e imporre sanzioni pecuniarie ove previsto dal Regolamento e dalla normativa nazionale;
- partecipare alle attività dell'Unione europea ed internazionali di settore

Il Data breach

L’articolo 4 del Regolamento definisce il Data Breach come "violazione dei dati personali”, ossia la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l’accesso ai dati personali trasmessi, conservati o comunque trattati

In tale ambito la responsabilità del titolare è duplice:

1. **evitare che avvenga** una violazione predisponendo e aggiornando le misure di sicurezza e
2. in caso di violazione, **adempiere tempestivamente** a quanto prescritto dal Regolamento.

Quali violazioni vanno notificate al Garante?

- Unicamente le violazioni di dati personali che possono avere **effetti avversi significativi** sugli individui, causando danni fisici, materiali o immateriali.

- Sono inclusi, ad esempio, la perdita del controllo sui propri dati personali, la limitazione di alcuni diritti, la discriminazione, il furto d'identità o il rischio di frode

Cosa fare in caso di violazione dei dati personali?

- Il titolare del trattamento **senza ingiustificato ritardo** e, ove possibile, **entro 72 ore dal momento in cui ne è venuto a conoscenza**, deve notificare la violazione al Garante per la protezione dei dati personali a meno che sia **improbabile** che la violazione dei dati personali comporti un rischio per i diritti e le libertà delle persone fisiche.

- Il responsabile del trattamento che viene a conoscenza di una eventuale violazione è tenuto a informare tempestivamente il titolare in modo che possa attivarsi.

La notifica all’interessato

- La necessità dell’invio della comunicazione dipende dalla valutazione del rischio per gli interessati
- La notifica va fatta anche all’interessato con “linguaggio semplice e chiaro”
- quando tale comunicazione richiederebbe sforzi sproporzionati, per cui può essere sostituita da una comunicazione pubblica.

Come fare la notifica al Garante?

- A partire dal 1° luglio 2021, la notifica di una violazione di dati personali deve essere inviata al Garante tramite un'apposita procedura telematica *https://servizi.gpdp.it/databreach/s/*

GRAZIE.

Seguiteci sui nostri canali

www.piemonteinnova.it

FONDAZIONE PIEMONTE INNOVA