UNIMORE – FIM
Corso di Algoritmi di Crittografia

Il crimine Informatico

Antonio Apruzzese

lII^ Edizione

a.a. 2023/2024

Obiettivi del corso

Ampliare la dotazione della cassetta degli strumenti

Facilitare l’inserimento nei vari contesti di attività professionale

Prospetto analitico

I) Sicurezza e Criminalità Informatica

Lo stato dell’arte aggiornato

Analisi dei principali attacchi cyber noti a livello globale dal 2018 al 2022

Fonte rapporto CLUSIT 2023 sulla sicurezza ICT in Italia

Attacchi per anno 2018 - 22

II) Crimini informatici e reati informatici

Un approccio preliminare.

L’evoluzione del fenomeno. Casi storici.

Il ruolo dell’ingegneria sociale.

Il phishing : analisi introduttiva e prime esperienze operative.

La catena di difesa – anelli forti e anelli deboli

I

III) Fattore umano e Ingegneria sociale

Tipologie criminali «di primo livello» :

BEC (Business Email Compromise) e

MITM (Man in the Middle)

Analisi di casi concreti

Frodi finanziarie tecnologicamente avanzate :

MITB (Man in The Browser)

IV) **Fattore umano e ingegneria sociale**

Tipologie criminali più complesse

Dal Phishing allo Smishing al Vishing

Analisi di casi concreti

V) **La “crittografia criminale”**

Il Ransomware e il il Cryptolocker.

Il quadro e le dimensioni del fenomeno

sulla scorta di casi concreti.

Le problematiche e le strategie di difesa.

Il ruolo del fattore umano e dell’ingegneria

sociale.

VI) Il rischio Informatico nei contesti aziendali

Il Cloud

Il problema della identità. Gli Access Broker

Infrastrutture Critiche Italiane

La Cyber resilienza

Attacchi alla identità e Sistemi Zero Trust

Supply Chain

Enterprise Architecture e Information Security

VII) Sicurezza nei servizi bancari on line

Strategia di difesa margine dei tecnicismi più avanzati

OF2CEN – Un esempio concreto di cyber security «fatto in casa»

I) La Sicurezza e la Criminalità Informatica

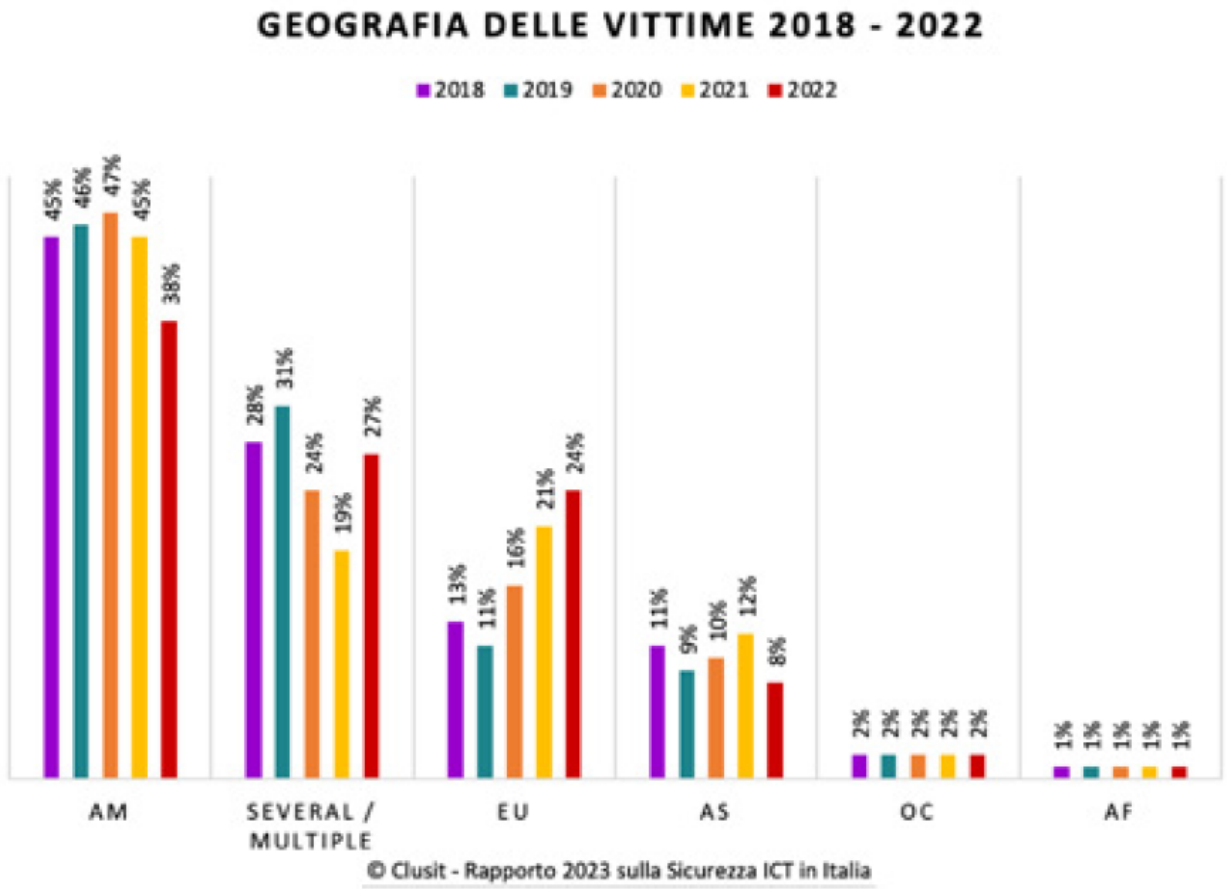
Lo stato dell’arte aggiornato

Analisi dei principali attacchi cyber noti a livello globale dal 2018 al 2022

Fonte rapporto CLUSIT 2023 sulla sicurezza ICT in Italia

Andamento dei cyber attacchi nel periodo 2018 - 22

Fig.1 pag. 11



Distribuzione geografica percentuale della tipologia delle vittime nel periodo 2018-2022

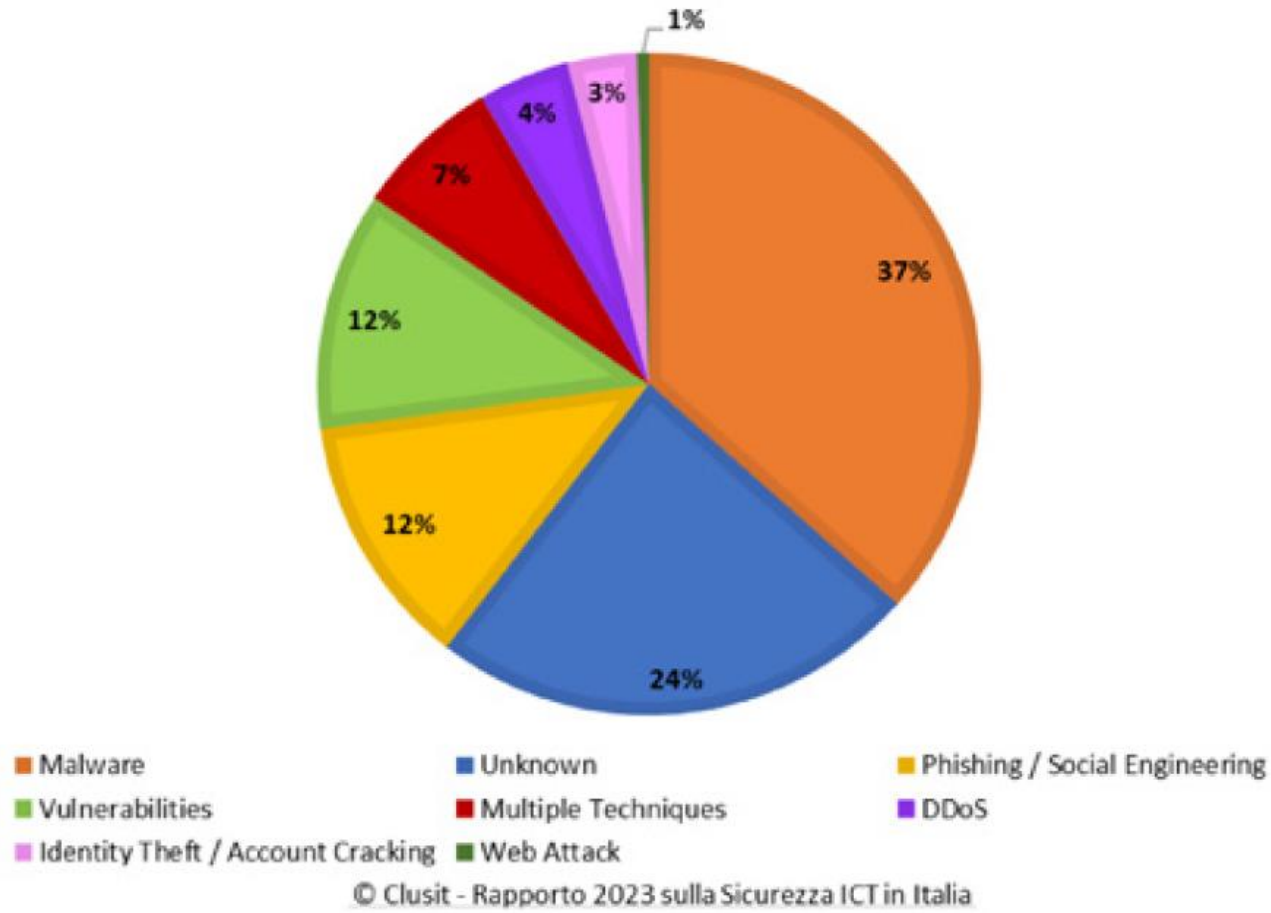
Fig.11 pag. 19

- L’America scende dal 45 al 38%
- L’EU aumenta dal 18 (2018) al 21 (2021) fino al 24% del 2022 (quasi raddoppia!)

- Le ragioni :

  maggior digitalizzazione

  maggiore sensibilizzazione al fenomeno



Distribuzione delle tecniche di attacco anno 2022

Fig.13 pag. 21

- Distribuzione delle tecniche di attacco

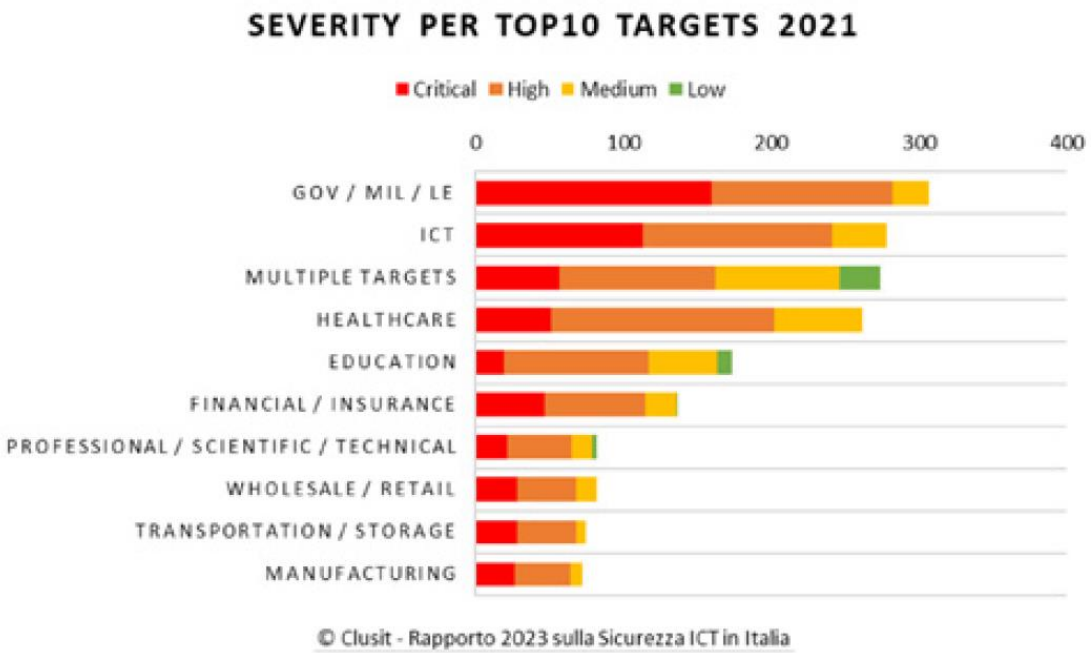
prevalgono ancora Malware-Vulnerabilità (ad esclusione della componente di attacchi basati sui cd «0-day»)- Phishing e Account Cracking tutte tecniche semplici e a basso costo per l'attaccante

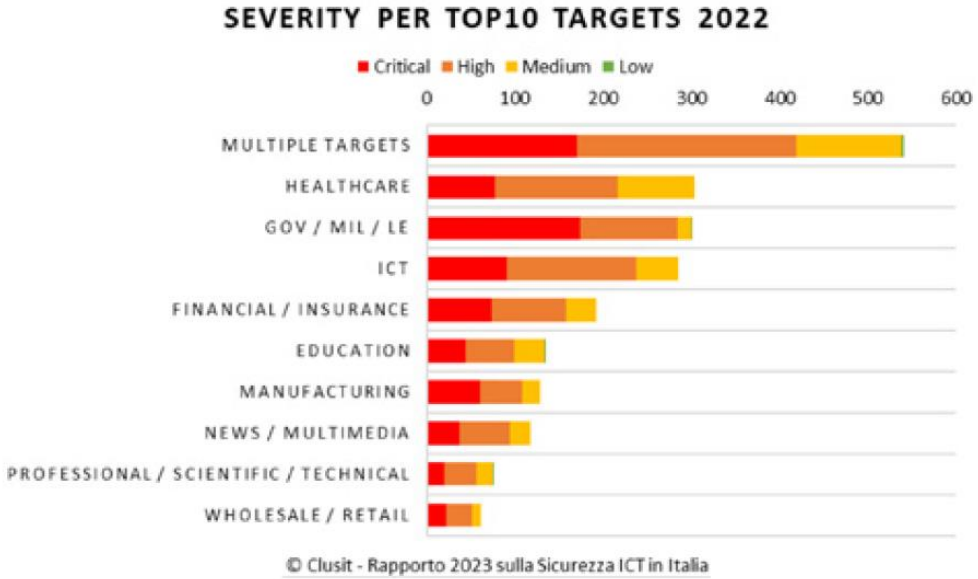
Sfruttano l'incapacità di gestire i nostri account, di tenere aggiornati i nostri dispositivi cliccando incautamente «cose» sbagliate nelle mail

…..basta un piccolo errore della vittima perché l’attaccante possa sferrare un attacco devastante per quanto a basso costo

Il Cybercrime conferma di operare con logiche economiche delle aziende tradizionali :

massimo risultato con minimo sforzo, investimento e rischio





Distribuzione della Severity
prime 10 vittime
Anno 2021 - 2022

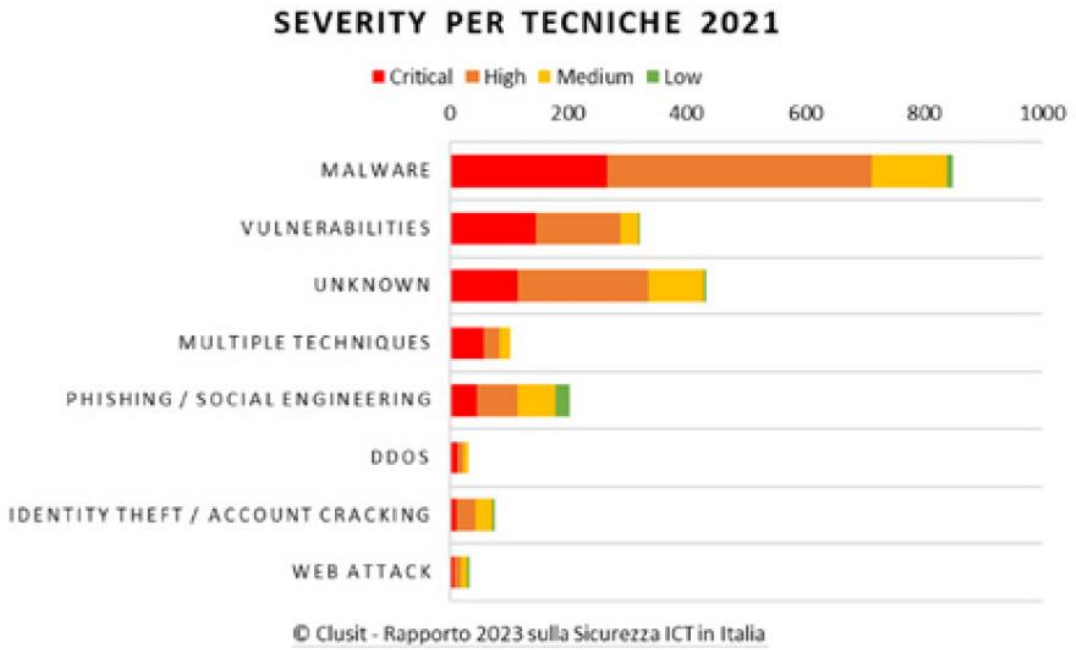
Fig.19 e fig 20 pag. 26-27
differenze fra gli anni 2021-2022

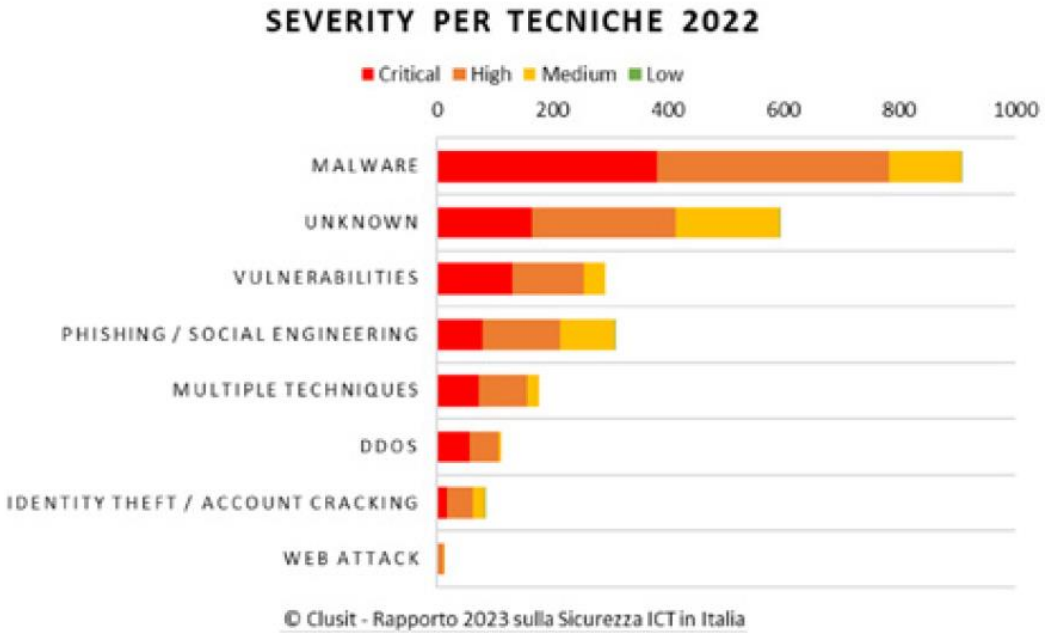
- Severity per tipologia di vittima

Al primo posto in assoluto i Multiple Targets

(tra cui spiccano Gov – Mil – FFOO) per evidenti connessioni con l'invasione dell'Ucraina ad opera della Russia

Un considerevole salto in avanti è quello del comparto Healtcare





Distribuzione della Severity per tecniche di attacco Anno 2021 - 2022

Fig.21 e fig 22 pag. 28
differenze fra gli anni 2021-2022

Severity per tecniche di attacco

- Il quadro viene definito «sconsolante»
- A parte la categoria degli attacchi unknown, le tecniche più ricorrenti sono le stesse di 30 anni fa, spesso banali e obsolete
- Si evidenziano infatti forti limiti nelle capacità di difesa delle vittime
- Si rende impellente un nuovo modello di approccio alla cybersecurity con cambio di passo che ponga la dovuta attenzione alla governance dei fornitori

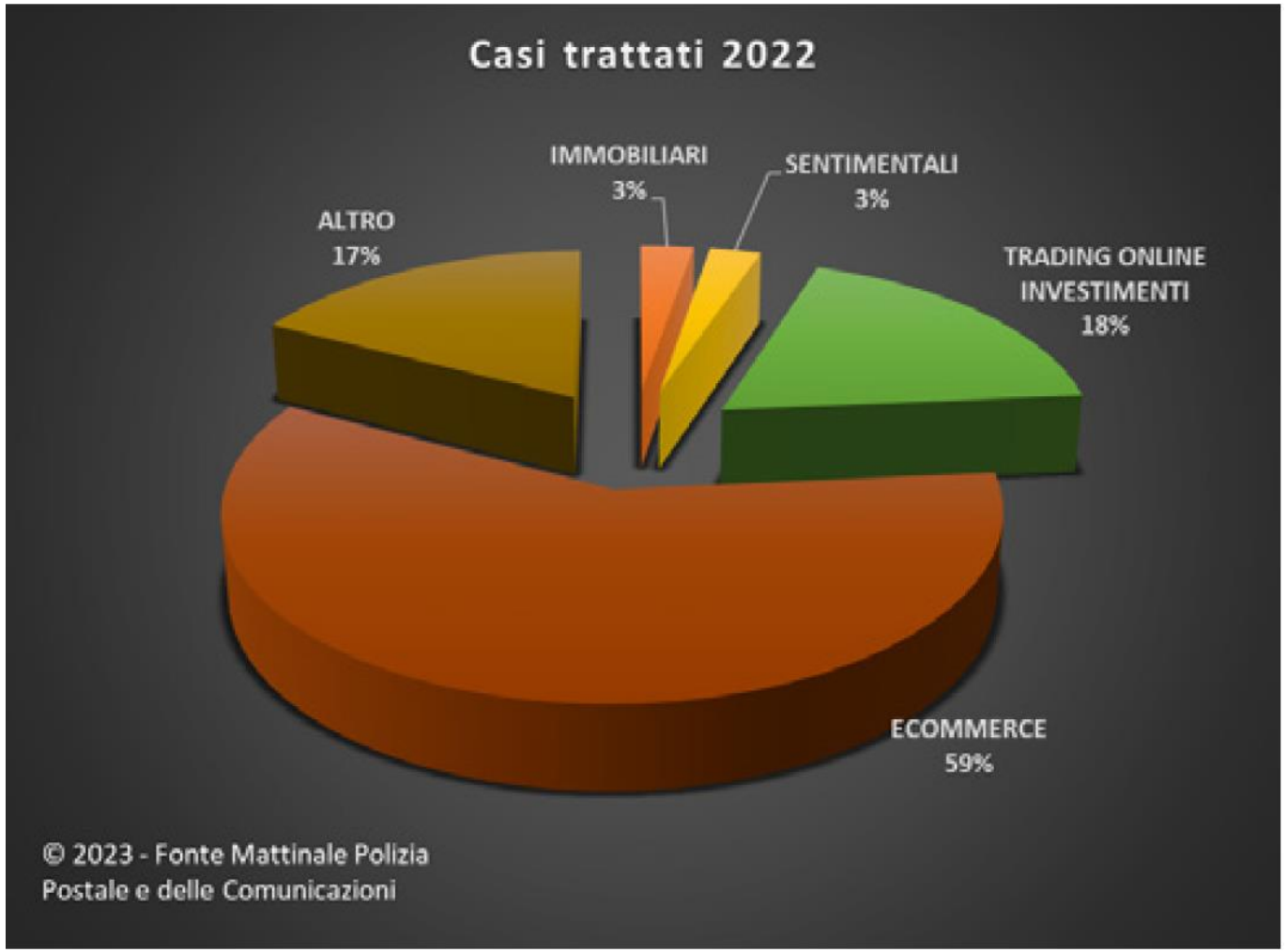
Dall’analisi alla sintesi: dai trend alla strategia

- Emerge la necessità di
- rafforzare la governance dei processi di patch e vulnerabilities management
- introdurre logiche di security by design che comprendano la gestione dei processi di sourcing e delle terze parti

Dai trend alla strategia

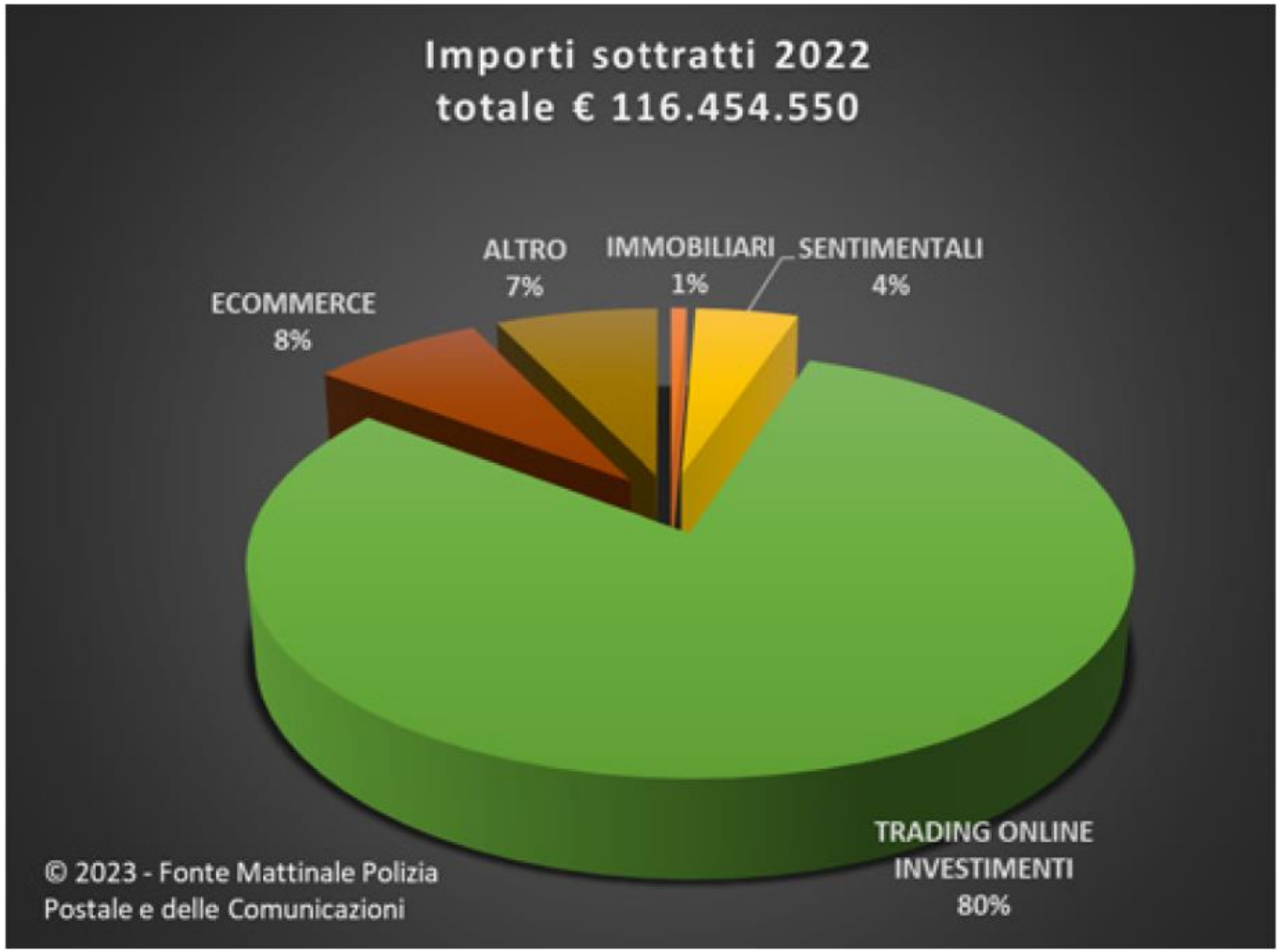
- Indispensabile un cambio di passo nell'approccio alla cybersecurity non più esclusivamente indotto da driver normativi ma di valutazione e gestione del rischio per il business
- I settori più colpiti infatti sono quelli meno «impattati» dalle normative generali e particolari con prescrizioni di cybersecurity

I dati della Polizia Postale e delle Comunicazioni



Truffe sul web – casi trattati Polizia delle Comunicazioni Anno 2022

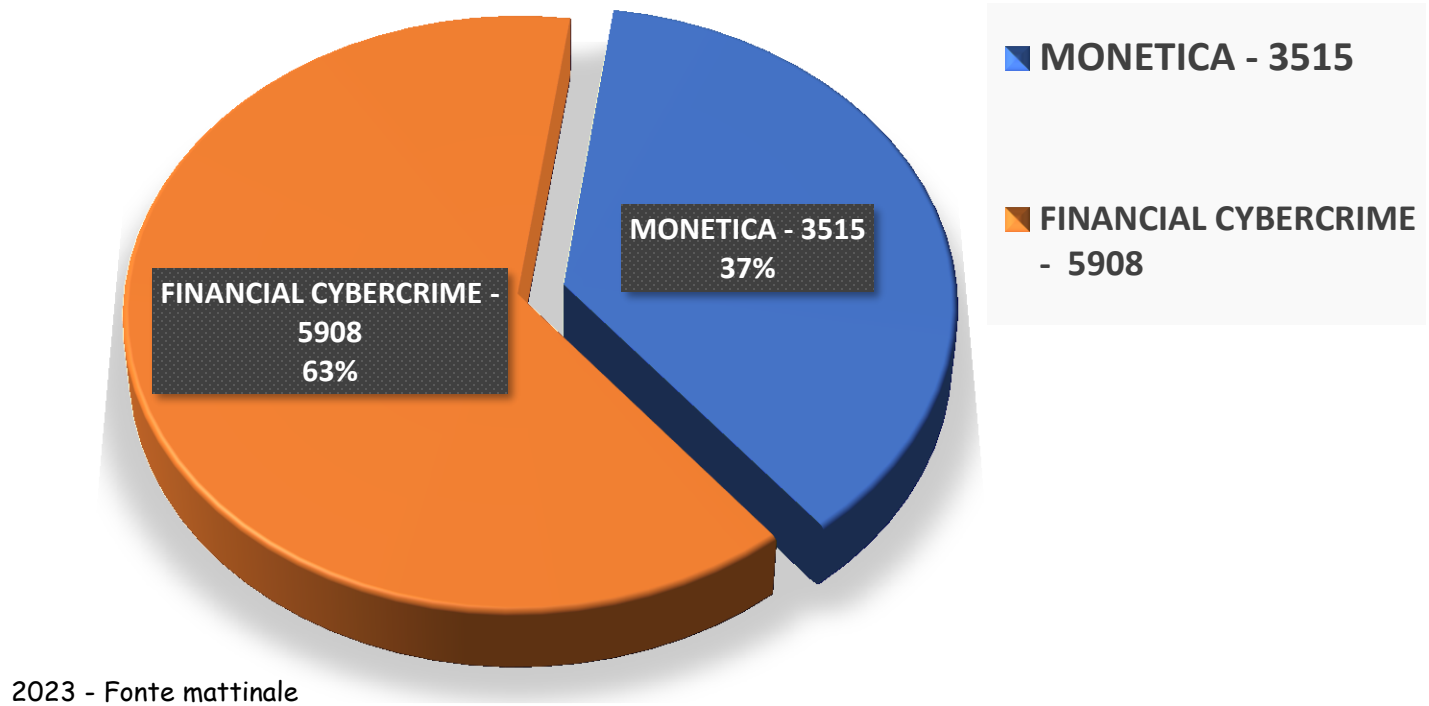
Pag. 83 – Fig. Casi trattati



Truffe sul web – importi sottratti Anno 2022

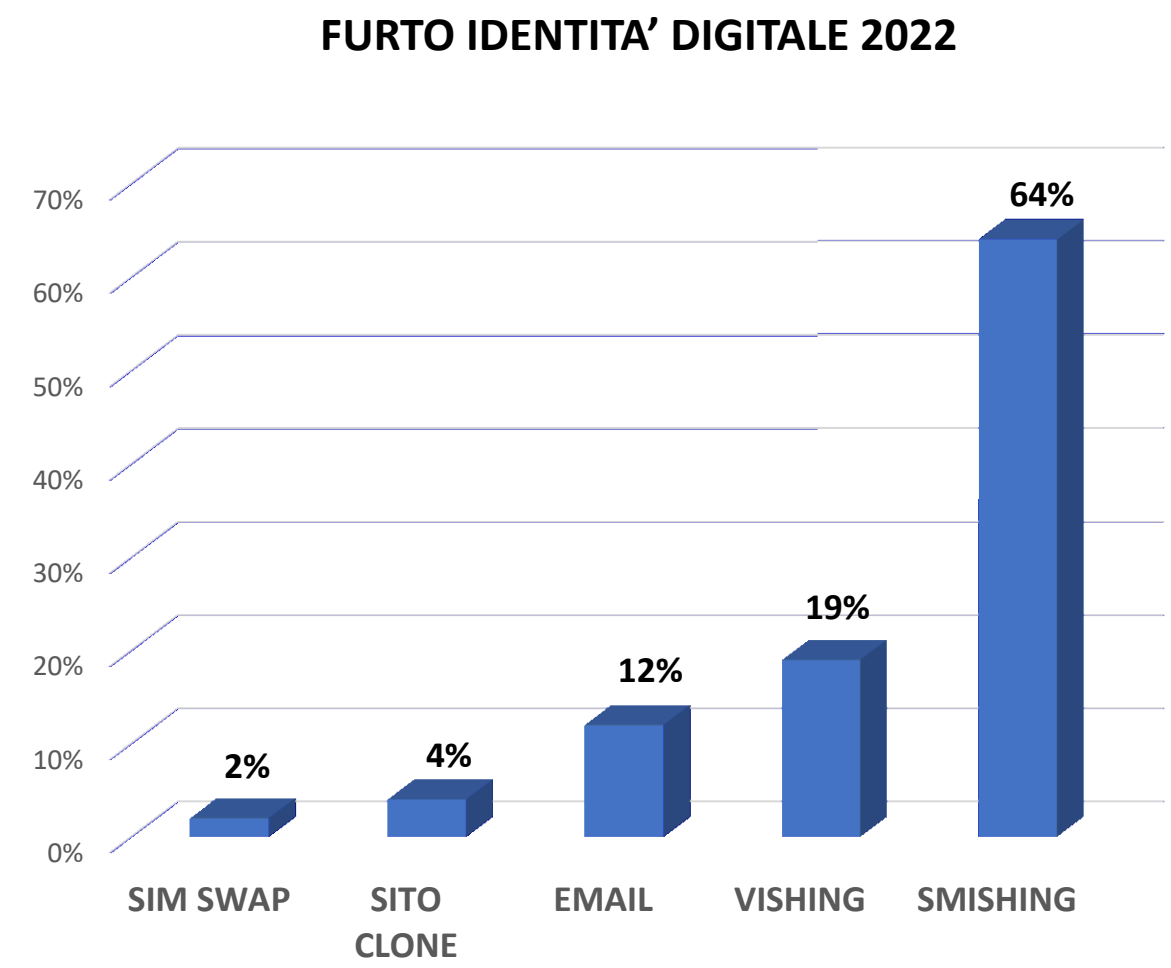
Pag. 84 – Fig. importi sottratti

FINANCIAL CYBERCRYME E MONETICA 2022



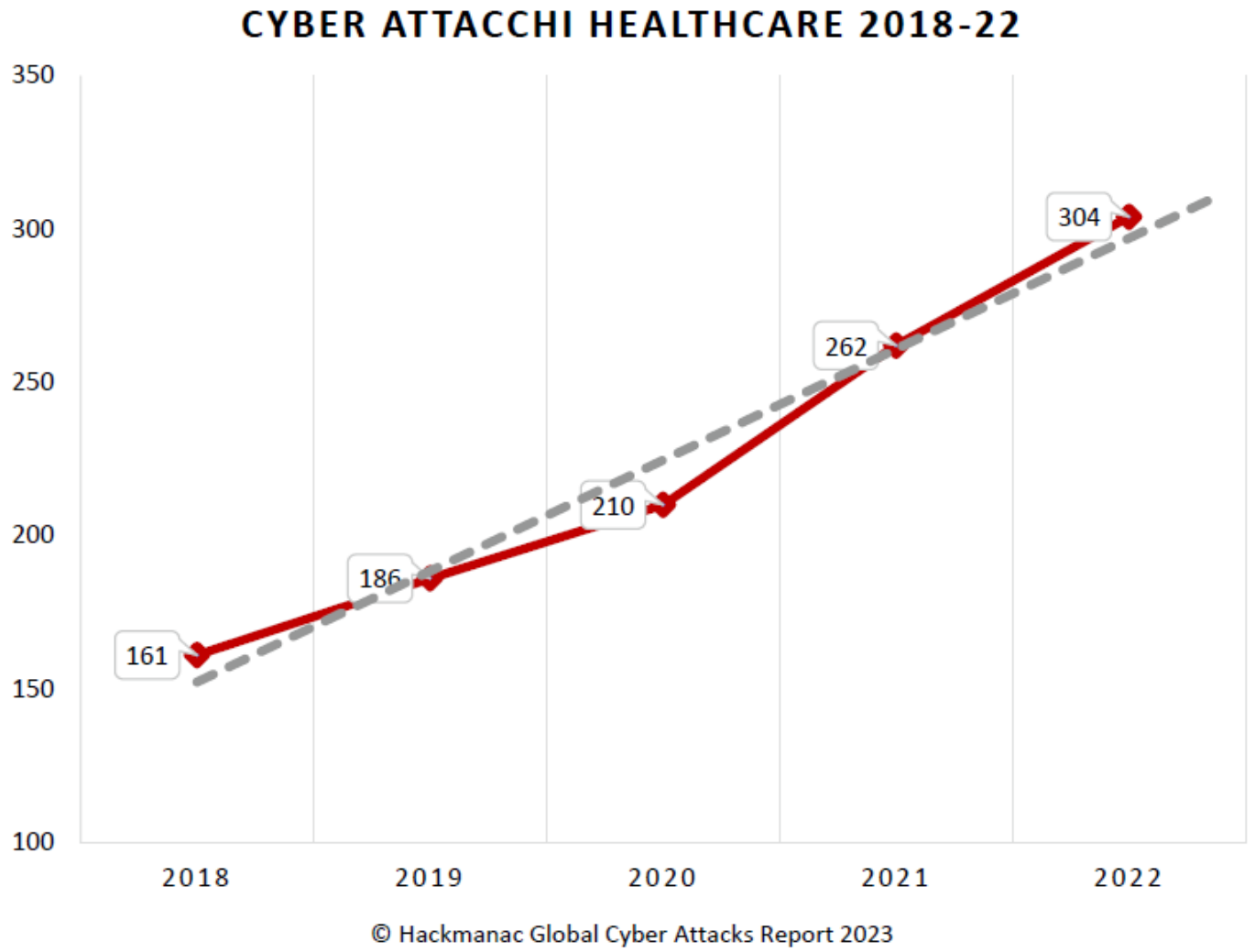
2023 - Fonte mattinale
Polizia Postale e delle comunicazioni

Pag 97– Fig. Financial Cyber Crime e Monetica



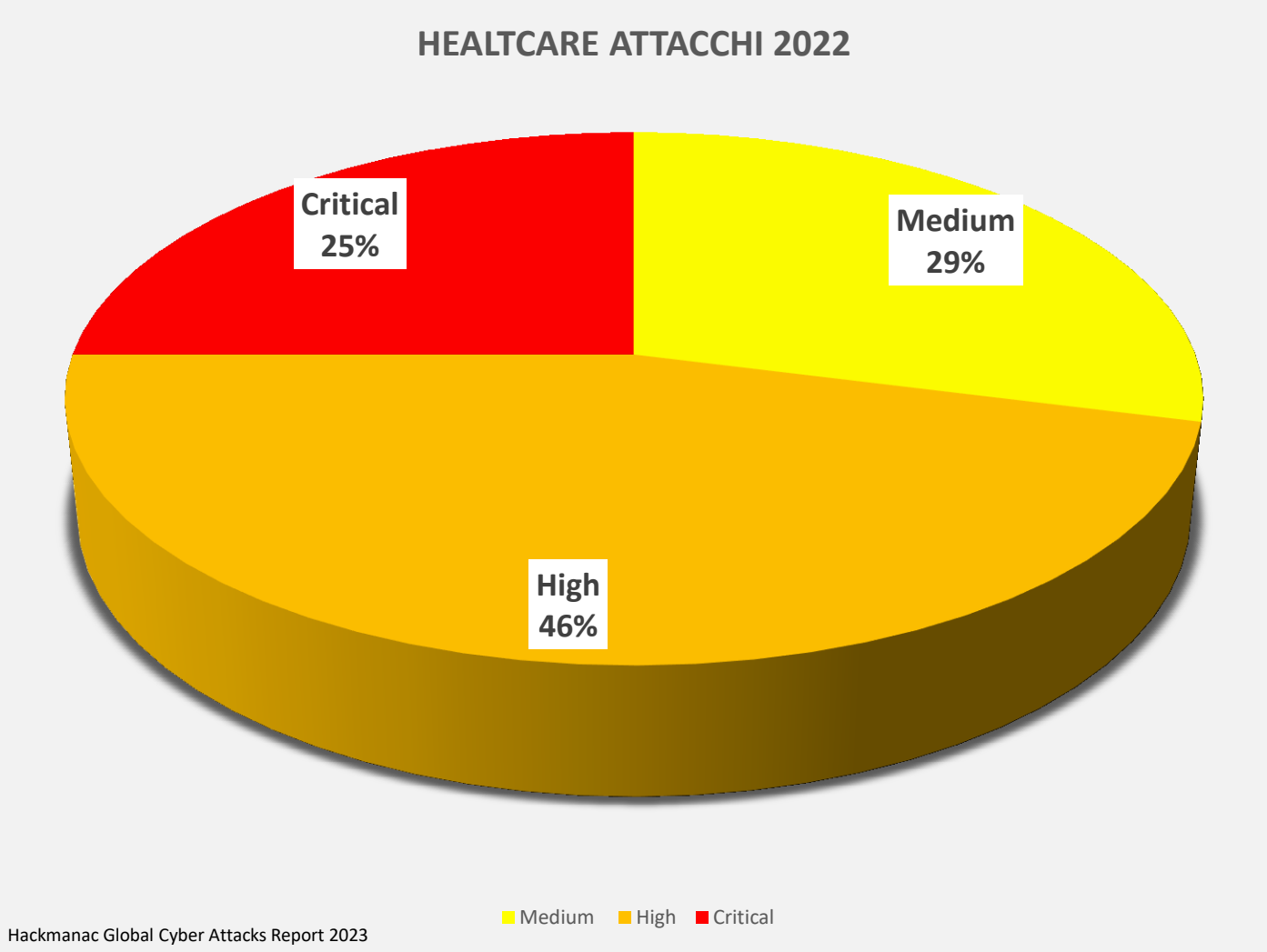
2023 - Fonte mattinale
Polizia Postale e delle comunicazioni

Pag 97– Fig. Furto identità



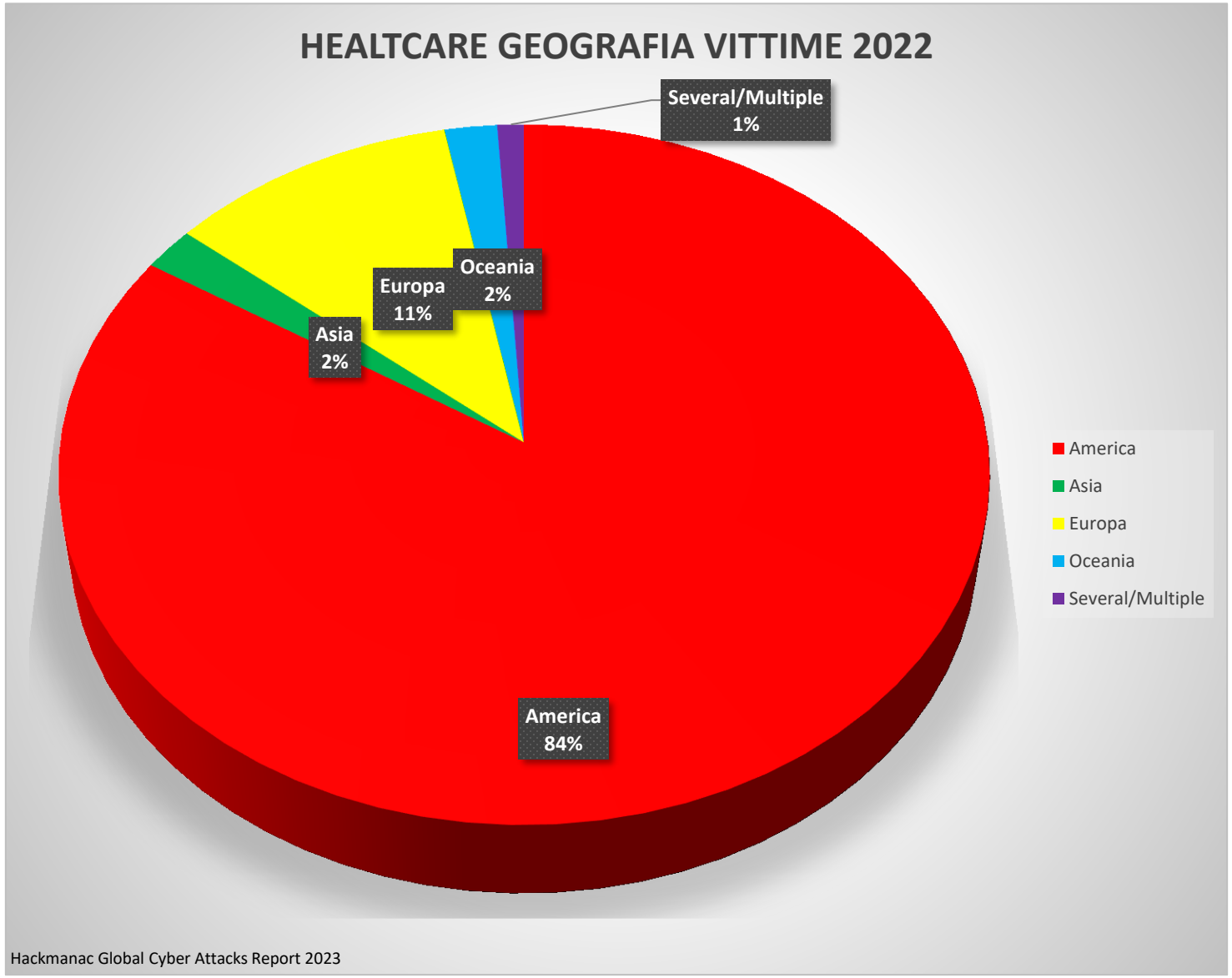
Trend dei cyber attacchi nel settore sanitario periodo 2018-2022

Pag 123– Fig. 1



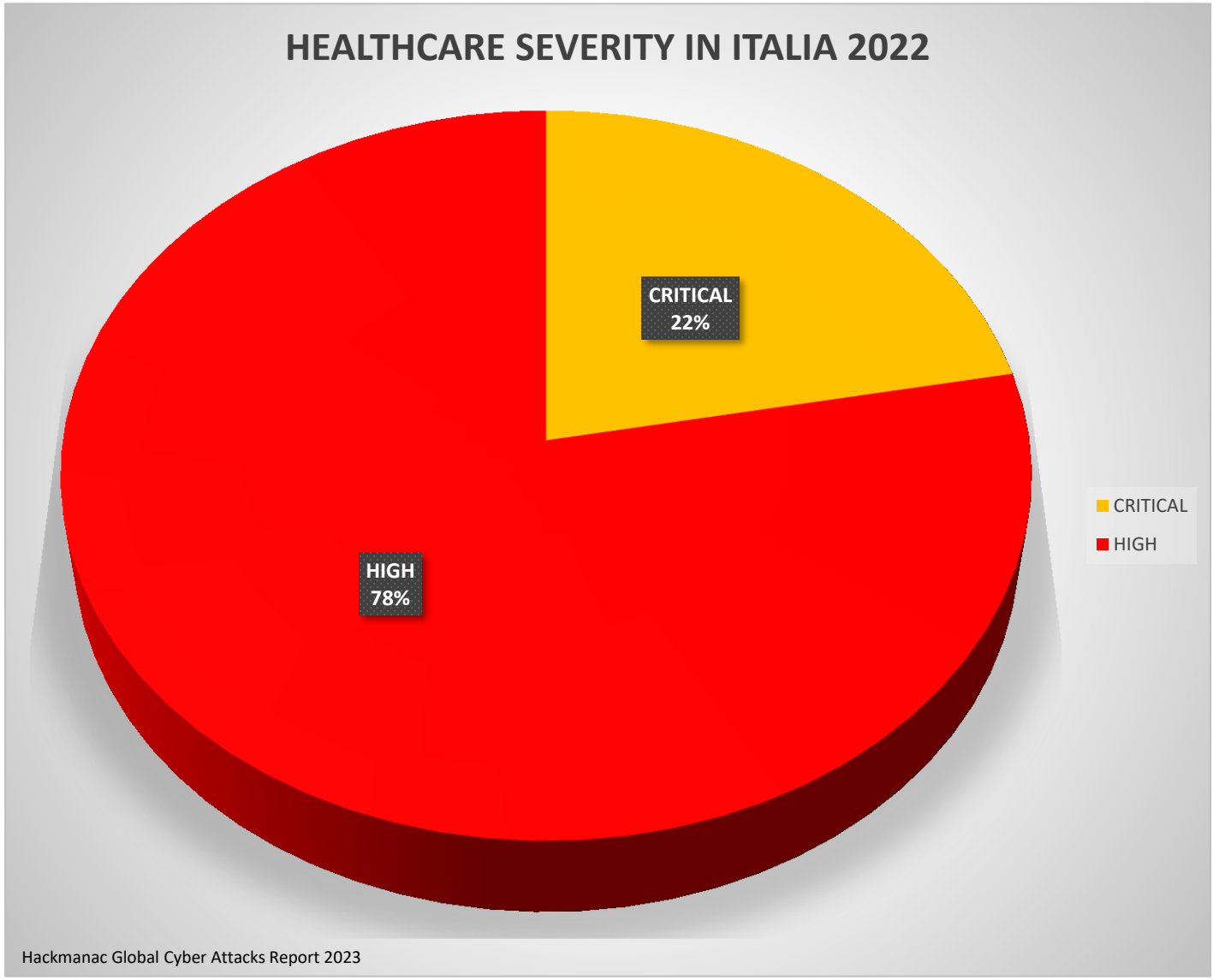
Severity dei cyber attacchi in ambito sanitario nel 2022

Pag 124– Fig. 2



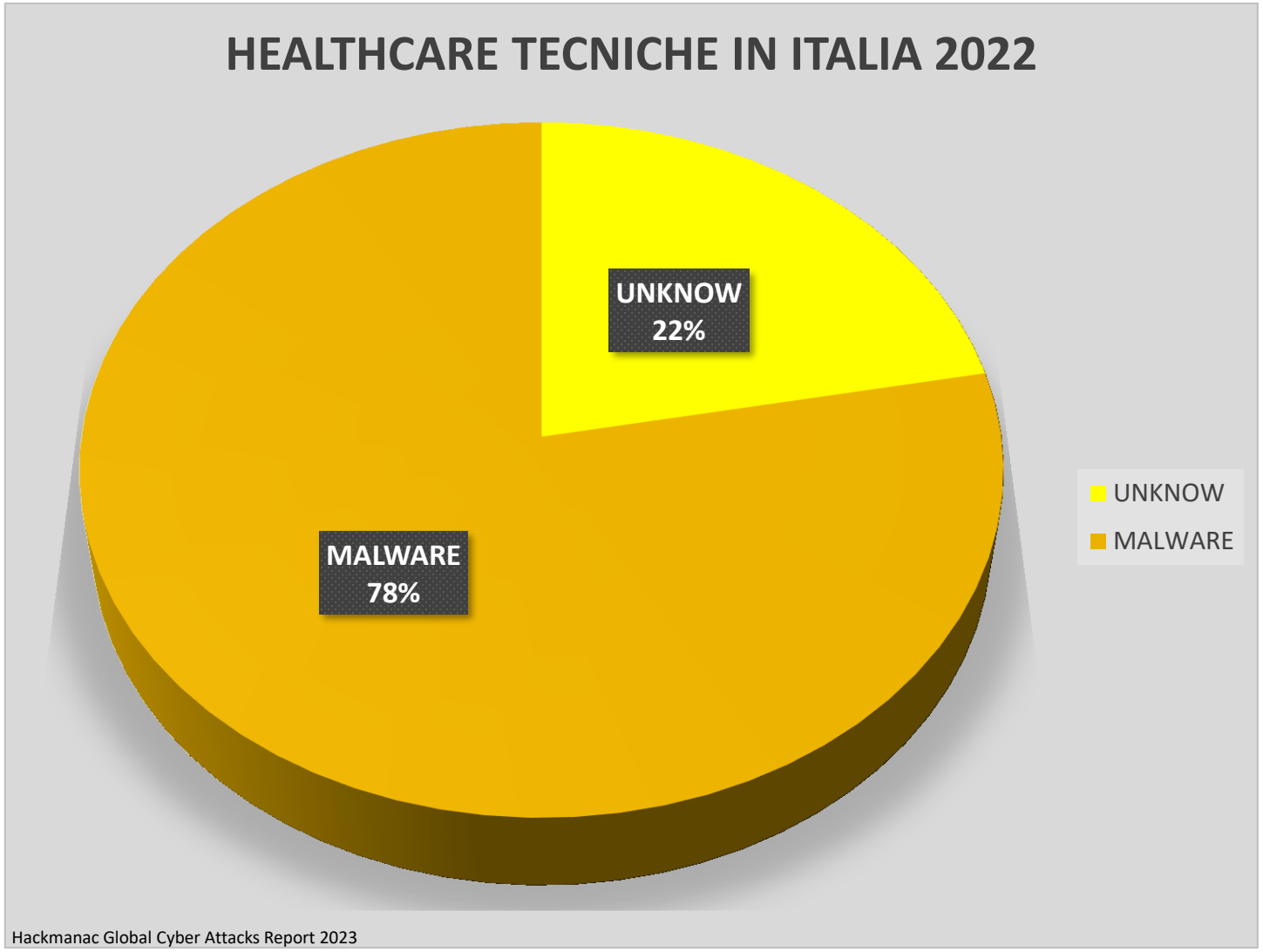
Geografia delle vittime dei cyber attacchi in ambito sanitario nel 2022

Pag 125 – Fig. 3



Severity dei cyber attacchi verso il settore sanitario in Italia nel 2022

Pag 127– Fig. 6



Tecniche dei cyber attacchi verso il settore sanitario in Italia nel 2022

Pag 127– Fig. 7

II) Crimini informatici e reati informatici

Un approccio preliminare.

L’evoluzione del fenomeno.

Casi storici. Il ruolo dell’ingegneria sociale.

Il phishing : analisi introduttiva

Prime esperienze operative.

La catena di difesa – anelli forti e anelli deboli

Crimini informatici e reati informatici

differenze concettuali

I delitti tradizionali assumono connotati digitali

Violazione di domicilio
Art. 614 c.p.

Accesso abusivo a sistema informatico o telematico
Art. 615 *ter* c.p.

Truffa
Art. 640 c.p.

Frode informatica
Art. 640 *ter* c.p.

Danneggiamento
Art. 635 c.p.

Danneggiamento di informazioni, dati e programmi informatici
Art. 635 *quater* c.p.

Reati informatici

- **Art. 615 ter C.P. Accesso abusivo ad un sistema informatico o telematico** *Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.*
- **Art. 640 ter C.P. Frode Informatica** *…chiunque intervenendo senza diritto con qualsiasi modalità sui dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno… reclusione da sei mesi a tre anni e multa. La pena è da 2 a 6 anni… se il fatto è commesso con furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti.*
- **Art. 617 sexies C.P. Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche** *Chiunque, al fine di procurare a sé o ad altri un vantaggio o di arrecare ad altri un danno, forma falsamente ovvero altera o sopprime, in tutto o in parte, il contenuto, anche occasionalmente intercettato, di taluna delle comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, è punito, qualora ne faccia uso, con la reclusione da uno a quattro anni.*

Reati informatici

Art. 617 sexies C.P. Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche

Chiunque, al fine di procurare a sé o ad altri un vantaggio o di arrecare ad altri un danno, forma falsamente ovvero altera o sopprime, in tutto o in parte, il contenuto, anche occasionalmente intercettato, di taluna delle comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, è punito, qualora ne faccia uso, con la reclusione da uno a quattro anni.

Reati comuni richiamati in crimini informatici

- **Art. 640 C.P. Truffa** C*hiunque, con artifizi o raggiri, inducendo taluno in errore, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da 51 euro a 1.032 euro*

- **Art. 694 C.P. Sostituzione di persona** C*hiunque, al fine di procurare a se o ad altriun vantaggio o di di recare ad altri un danno, induce taluno in errore, sostituendo illegittimamente la propèria all'altrui persona o attribuendo a sé o ad altri un falso nome o un falso stato, ovvero una qualità a cui la legge atttribuisce effetti giuridici, è punito, se il fatto non costituisce un altro delitto contro la fede pubblica, con la reclusione fino a un anno.*
- **Art 648 bis C.P. Riciclaggio …** *fuori dai casi di concorso nel reato, chiunque sostituisce o trasferisce denaro, beni o altre utilità provenienti da delitto non colposo, ovvero compie in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa è punito con la reclusione da quattro a dodici anni e con la multa da 1.032 a 15.493 euro*

.

L’accesso abusivo a sistema informatico

La particolarità dell’accesso abusivo
ad un sistema informatico
ipotizzabile non solo attraverso artifizi tecnici
ma anche tramite *social engineering*
o per carenza di legittimazione all’accesso

Crimini informatici e loro evoluzione

Un esempio storico : il caso Joker

(anni 2008/2009)

Contesto criminale di frodi su carte di credito (not present card fraud) quando ancora non introdotti gli ulteriori fattori di autenticazione

Caso Jocker

Un gruppo di truffatori di provincia di basso livello che si sviluppa fino a proiettarsi in ambito internazionale in contesti di articolate organizzazioni cybercriminali dedite al grande traffico di enormi quantità di dati rubati

La prima sfida

… le più avanzate tecniche di cyber security…

…I più complessi e blindati algoritmi di crittografia

alla prova delle debolezze del fattore umano

e della ingegneria sociale

Il *phishing* e l'ingegneria sociale

"…..ma se già imparassimo a difenderci dal malware e dal phishing…. probabilmente avremmo risolto l'80% dei nostri problemi"

….come ci ricorda il Clusit

Conoscere bene il *phishing*

Il phishing è il più subdolo degli attacchi, perché è esclusivamente basato sul fattore umano.

La tecnologia aiuta, ma senza l'errore umano il phishing non avrebbe scampo.

Sbaglieremmo però a semplificare il problema limitandoci ad etichettare come superficiali e poco attente le vittime del phishing. Non è così.

L'attaccante gioca sulla debolezza delle persone, sulla stanchezza, sullo stress, sulla minima impercettibile distrazione.

… *phishing*

Ci sono diversi livelli di phishing da quelli banali a quelli più sofisticati

“*Ricorrendo a una analogia ittica, si passa dalla pesca a strascico indiscriminata, brutale e ignorante, alla pesca mirata, dove il pescatore è un professionista che sceglie con cura la canna giusta, l’esca giusta per il tipo di pesce che vuole pescare, e la zona giusta del lago*”

… *phishing*

Il phishing ”B2B”, ovvero il business di chi crea il “kit di phishing” completo per poi venderlo ai criminali che ne fanno uso.

Un kit completo dal motore necessario per poter spedire migliaia di email (senza essere bloccato dai sempre più sofisticati sistemi di filtering) ai siti clone, prevalentemente di istituti bancari, accuratamente predisposti per ingannare la vittima :

… verso lo *spear phishing* …

Il marchingegno criminale si evolve

Con i dati rubati, ad esempio dai milioni di profili facebook, le campagne di phishing diventano sempre più personalizzate e prendono il nome di *spear phishing.*

Consentono di sapere se le vittime hanno figli o no, se sono sposate, dove vivono, etc. Le campagne di spear phishing useranno questi dati rubati e venduti nel dark web, per far arrivare l'email giusta alla persona giusta.

Quando, invece dell'email, si usano gli sms si parla di *smishing*, quando si usano i messaggi vocali *vishing*, ma il concetto è sempre lo stesso.

… *phishing*

In sintesi il phishing come una delle più tipiche tecniche di *social engineering,*

ovvero

l’arte di manipolare e raggirare le persone per estorcere informazioni da usare per scopi illeciti

Ingegneria sociale e vecchi maestri

Non si può parlare di *social engineering* senza citare uno dei suoi più grandi maestri nella storia contemporanea : Kevin Mitnick, detto Condor

Leggendario "cracker", ricercatissimo dall'FBI riuscì ad entrare nei server delle grandi multinazionali anche grazie a sofisticate tecniche di ingegneria sociale come espressamentte spiegato nel suo best seller "*L'arte dell'inganno*".

Il *phishing* e le esperienze dirette…

Lo schema classico della tonnara per carpire i dati sensibili

Dalla mail trappola ai *money mules*

I furti massivi di identità digitali

La scarsa cooperazione internazionale

Il difficile contrasto : no a guerre “ad alta quota” - unica forma di di contrasto il ricorso alle tradizionali tecniche investigative “da strada”

Anelli forti e anelli deboli della catena di difesa
«la forza di una catena dipende dal suo anello più debole»

- Gli attacchi mirano a individuare l'anello più debole della catena.
- Le comunicazioni in generale sono considerate sicure, protette da algoritmi di crittografia che, se implementati in modo corretto, impediscono di intercettare e alterare i flussi comunicativi.

I criminali prendono di mira le tecnologie e le loro implementazioni,

o fanno leva sulla debolezza rappresentata dagli utilizzatori dei sistemi (fattore umano).

Attacchi indiretti

In molti casi i criminali invece di attaccare direttamente i loro bersagli (in particolare aziende) attaccano i loro fornitori ad esempio installando un software malevolo nei loro prodotti che vengono poi utilizzati dalle aziende bersaglio.

(Attacchi alla *supply chain)*

Un esempio

2011 - Attacco alla RSA, colosso USA della sicurezza informatica, per sottrarre i semi per la generazione dei Token, fondamentali nei processi di autenticazione.

La connessa breccia nei sistemi di difesa della Lockheed Martin fornitore delle Forze Armate degli Stati Uniti

•

Attacco alla RSA

L’attacco a RSA è stato realizzato attraverso una coalizione tra un primo gruppo di criminali che hanno “penetrato” un livello del network di RSA a bassa priorità mediante una campagna di *phishing* a mezzo posta elettronica.

In seguito altri cyber criminali sono risaliti nel network fino a compromettere la tecnologia di cifratura impiegata sui diffusissimi token di autenticazione SecureID

Anelli forti e anelli deboli
Attacco alla RSA

Nonostante la gravità dell'incidente, RSA ha tenuto a precisare che il database dei clienti non era stato compromesso perché l'attacco era stato individuato in tempo.

"I dati dei contractor della Difesa USA, presunto obiettivo finale degli hacker probabilmente riconducibili a Stati ostili – secondo RSA – sono al sicuro".

Stranamente però il colosso aerospaziale della Difesa Lockheed Martin poco dopo la compromissione dei token Secure ID aveva denunciato di aver subito un attacco.