Attacchi informatici

Massimo Battaglioni

Università Politecnica delle Marche

Dipartimento di Ingegneria dell'Informazione

m.battaglioni@univpm.it

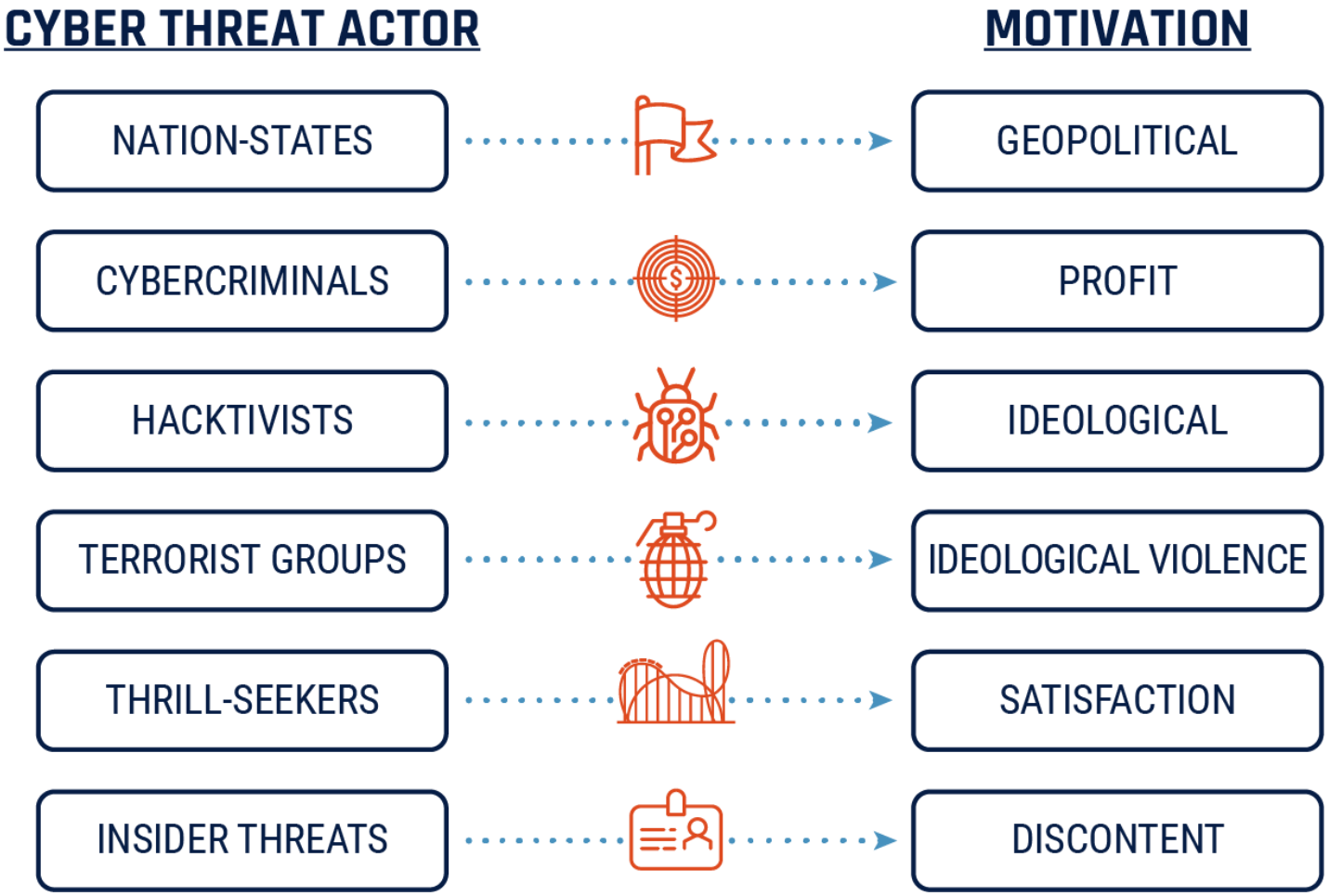
A.A. 2023/2024

Definizione di attacco informatico

Nella ISO/IEC 27000:2018 un **attacco cyber** viene definito come «*un tentativo di distruggere, esporre, alterare, disabilitare, rubare o ottenere l'accesso non autorizzato o fare un uso non autorizzato di un asset*», dove con asset si intende qualsiasi cosa materiale o immateriale che abbia un valore

Il tentativo è *malevolo* e *intenzionale* da parte di un *individuo* o di *un'organizzazione* che intende violare il sistema informativo di un altro individuo o azienda, solitamente con lo scopo di ottenere qualche tipo di **vantaggio**

Chi sono i cyber attaccanti?



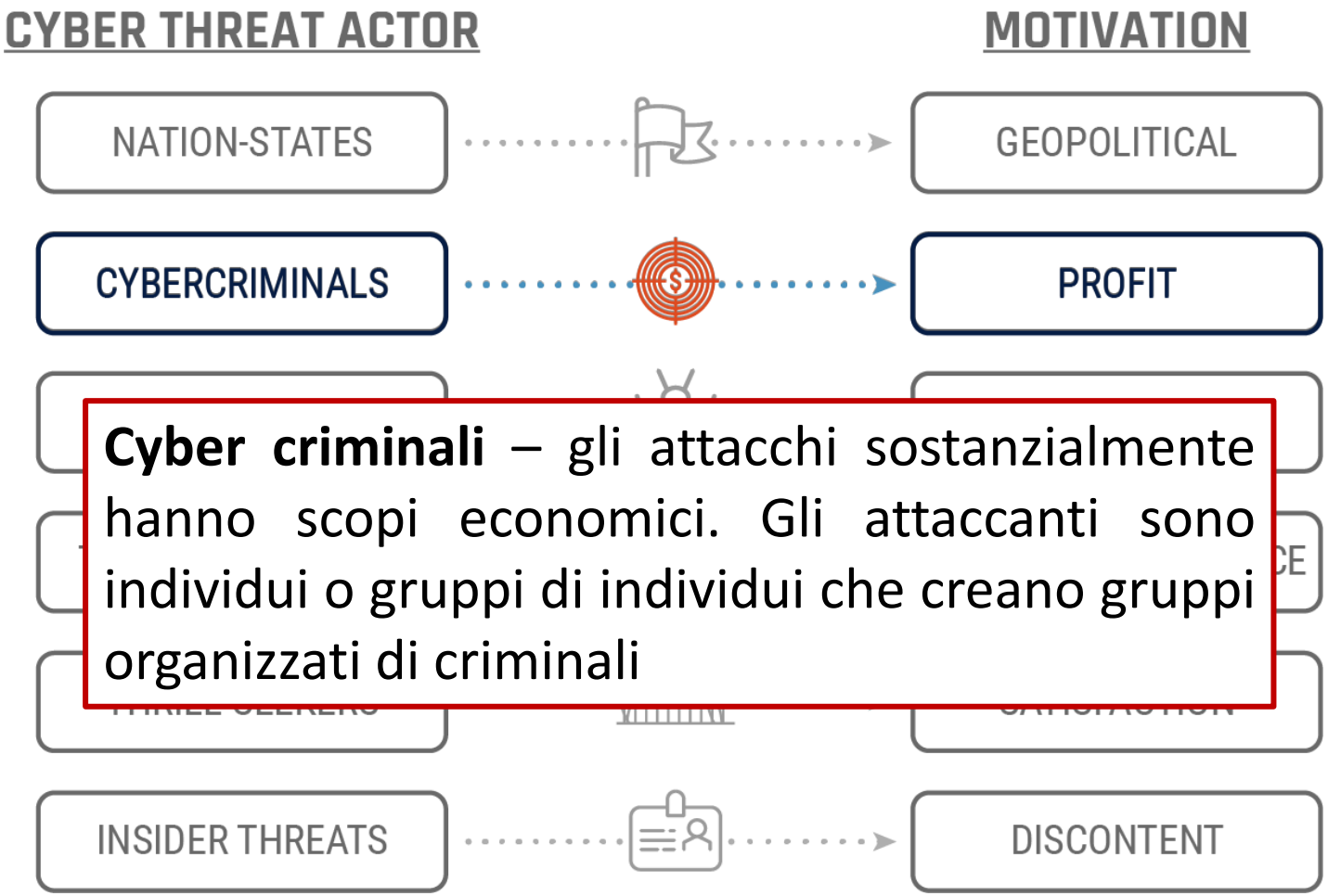
Fonte: https://cyber.gc.ca/en/guidance/introduction-cyber-threat-environment

Chi sono i cyber attaccanti?

Governativi – gli attacchi sono rivolti ad interessi di tipo militare, economico, politico. Le risorse a disposizione per gli attacchi sono enormi. Mirano a colpire infrastrutture critiche

Fonte: https://cyber.gc.ca/en/guidance/introduction-cyber-threat-environment

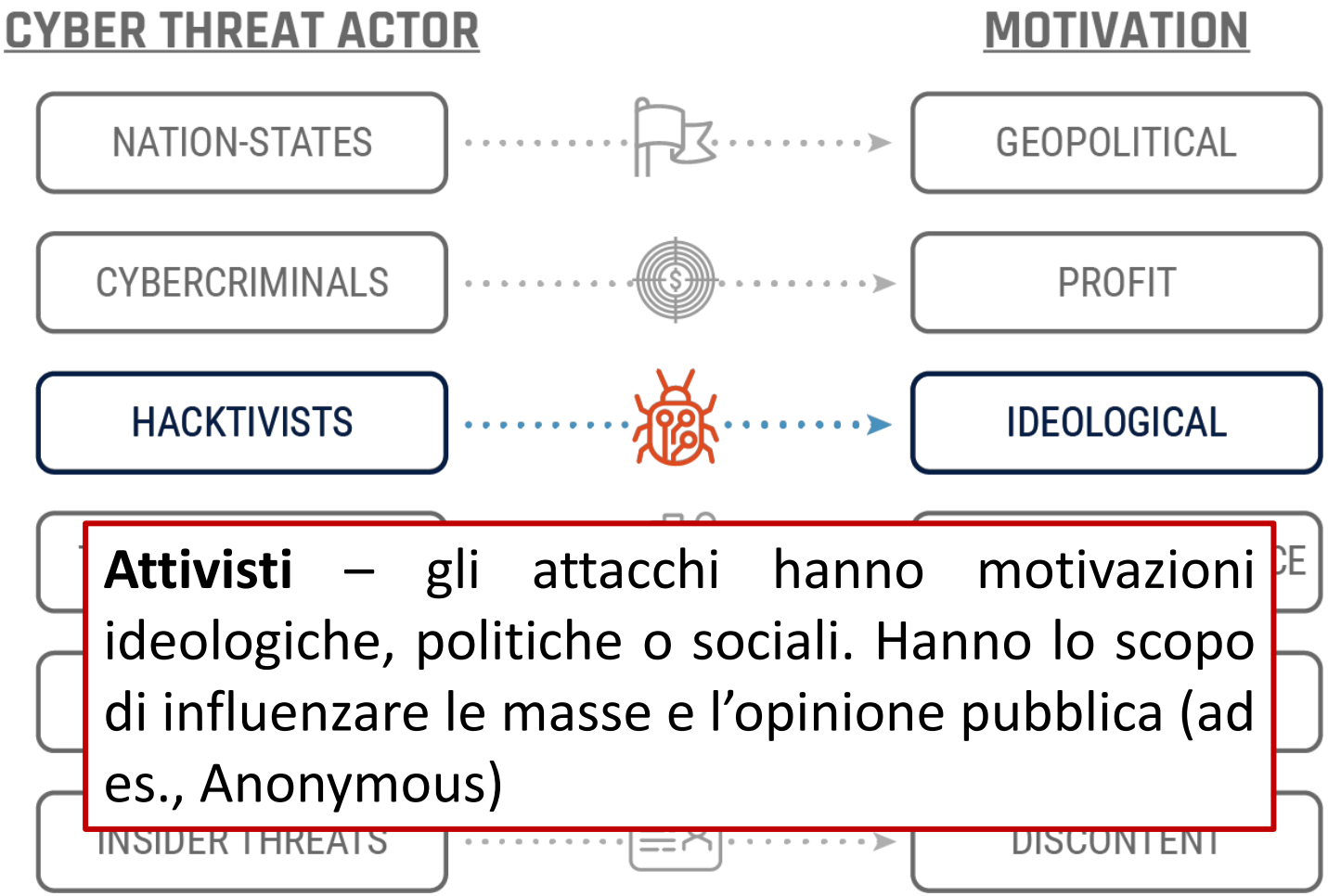
Chi sono i cyber attaccanti?



Cyber criminali – gli attacchi sostanzialmente hanno scopi economici. Gli attaccanti sono individui o gruppi di individui che creano gruppi organizzati di criminali

Fonte: https://cyber.gc.ca/en/guidance/introduction-cyber-threat-environment

Chi sono i cyber attaccanti?



Attivisti – gli attacchi hanno motivazioni ideologiche, politiche o sociali. Hanno lo scopo di influenzare le masse e l'opinione pubblica (ad es., Anonymous)

Fonte: https://cyber.gc.ca/en/guidance/introduction-cyber-threat-environment

Chi sono i cyber attaccanti?

Gruppi terroristici – gli attacchi sono motivati dalla violenza ideologica. Le abilità tecniche sono spesso poche e quindi gli attacchi poco sofisticati

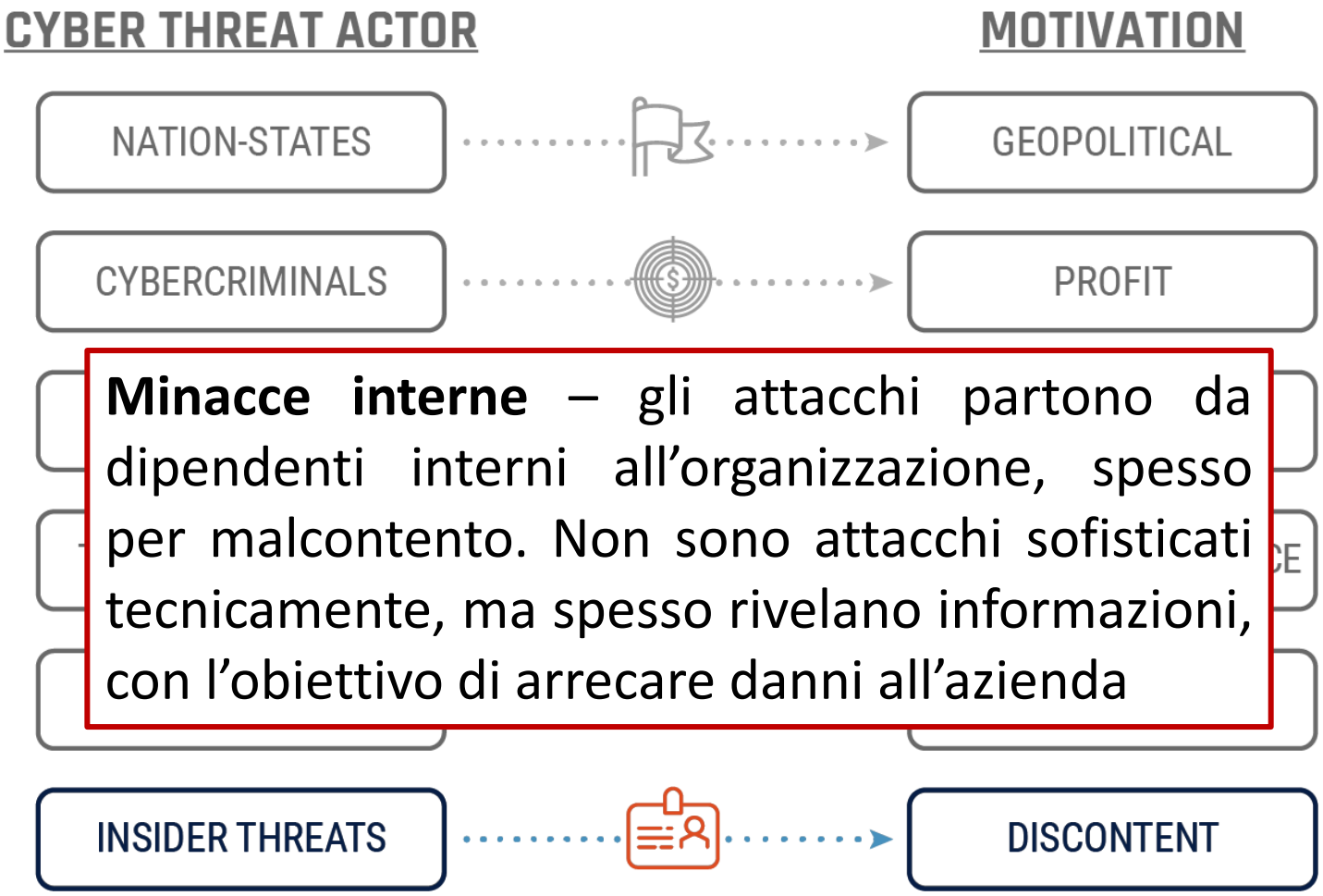
Fonte: https://cyber.gc.ca/en/guidance/introduction-cyber-threat-environment

Chi sono i cyber attaccanti?

«Amanti del brivido» – gli attacchi sono lanciati da hacker poco esperti che utilizzano software esistenti per sperimentare il mondo cyber. Attaccano essenzialmente per divertimento

Fonte: https://cyber.gc.ca/en/guidance/introduction-cyber-threat-environment

Chi sono i cyber attaccanti?



Minacce interne – gli attacchi partono da dipendenti interni all'organizzazione, spesso per malcontento. Non sono attacchi sofisticati tecnicamente, ma spesso rivelano informazioni, con l'obiettivo di arrecare danni all'azienda

Fonte: https://cyber.gc.ca/en/guidance/introduction-cyber-threat-environment

Chi sono le vittime?

Le **vittime** di attacchi informatici possono essere:

- *specifiche* o *casuali* (target mirato, o multi-target)
- sistemi informatici con *vulnerabilità* (data breach)
- utenti *non consapevoli* e non preparati (phishing, ransomware)

Chi sono le vittime?

Le **conseguenze** degli attacchi informatici possono essere molteplici:

- *danni materiali* ai sistemi informatici
- *interruzione* dell'attività con una conseguente perdita economica;
- *danno reputazionale* e richieste di risarcimento danni
- costi legati ai servizi professionali necessari a *contenere la crisi* causata dall'attacco informatico

Rapporto CLUSIT

Rapporto CLUSIT 2023

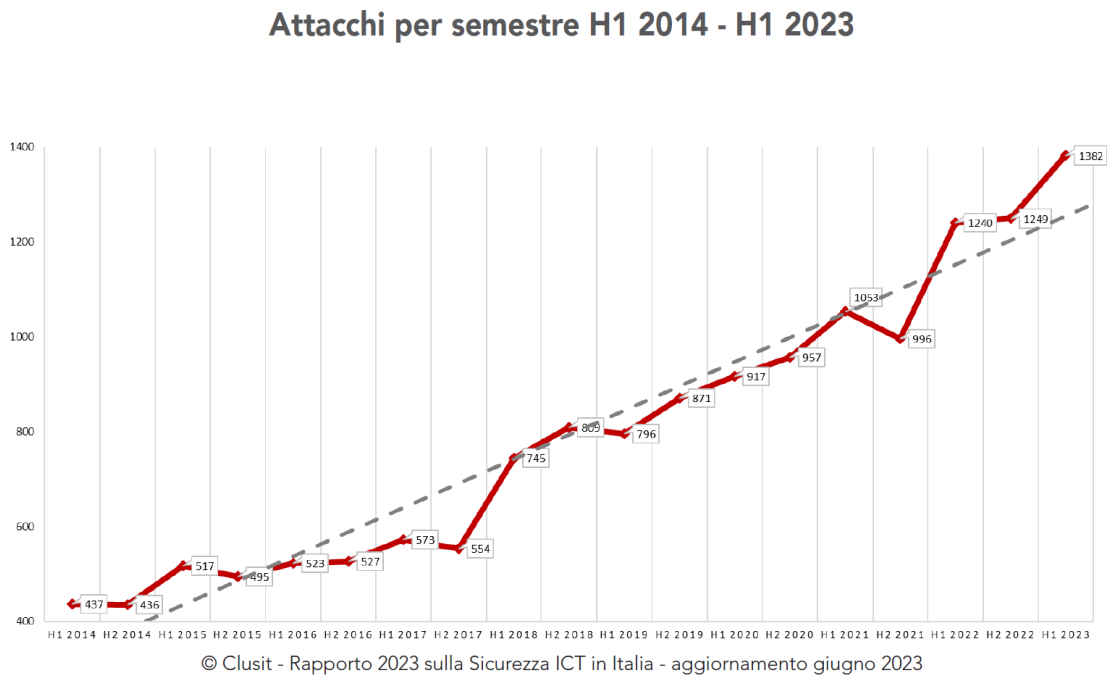


Fig. 1: *Andamento dei cyber attacchi per semestre da H1 2014 a H1 2023*

- Numero di attacchi noti <u>di particolare gravità</u>

Rapporto CLUSIT 2023

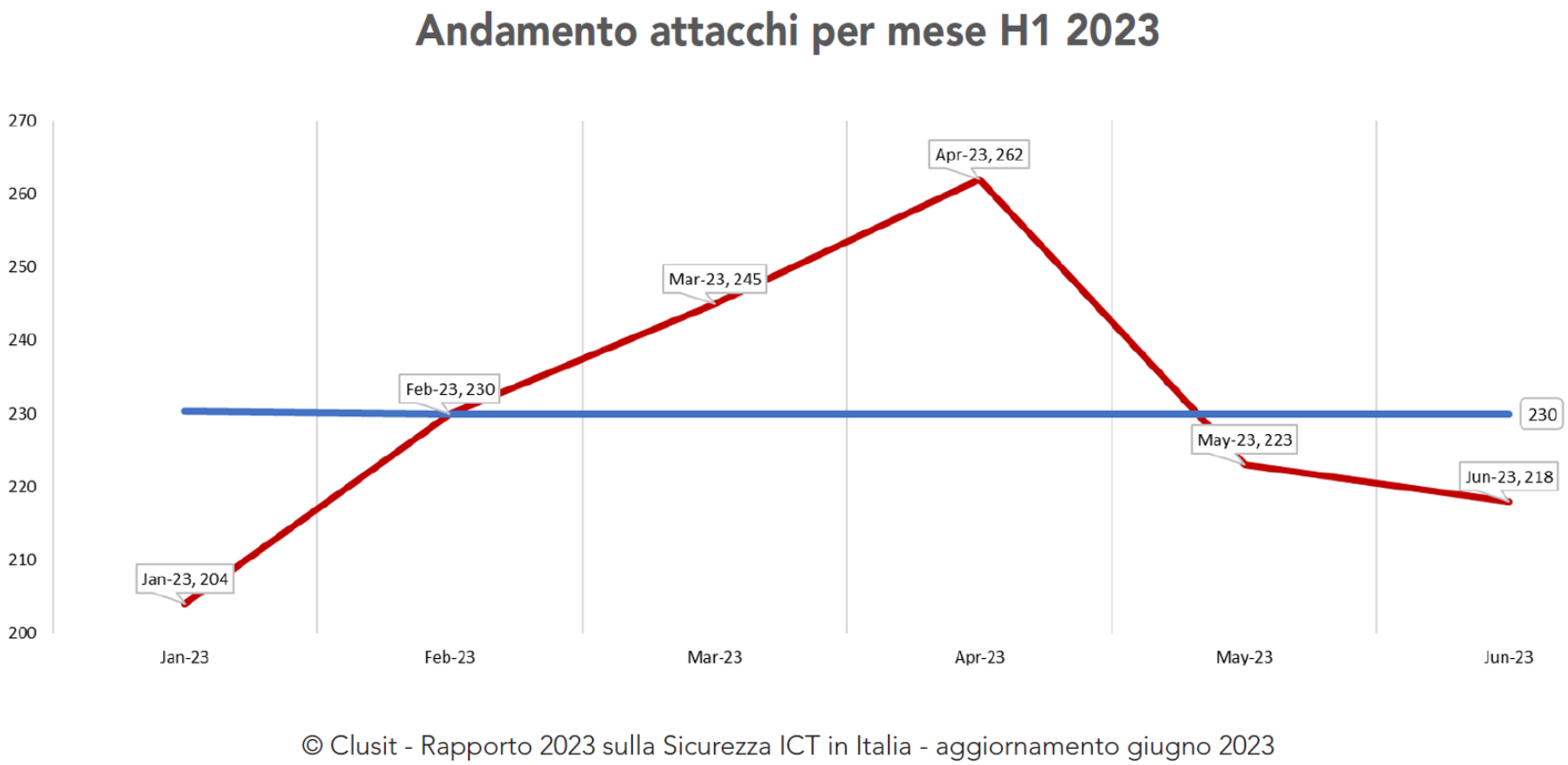


Fig. 3: *Numero di attacchi per mese nel primo semestre 2023*

Rapporto CLUSIT 2023

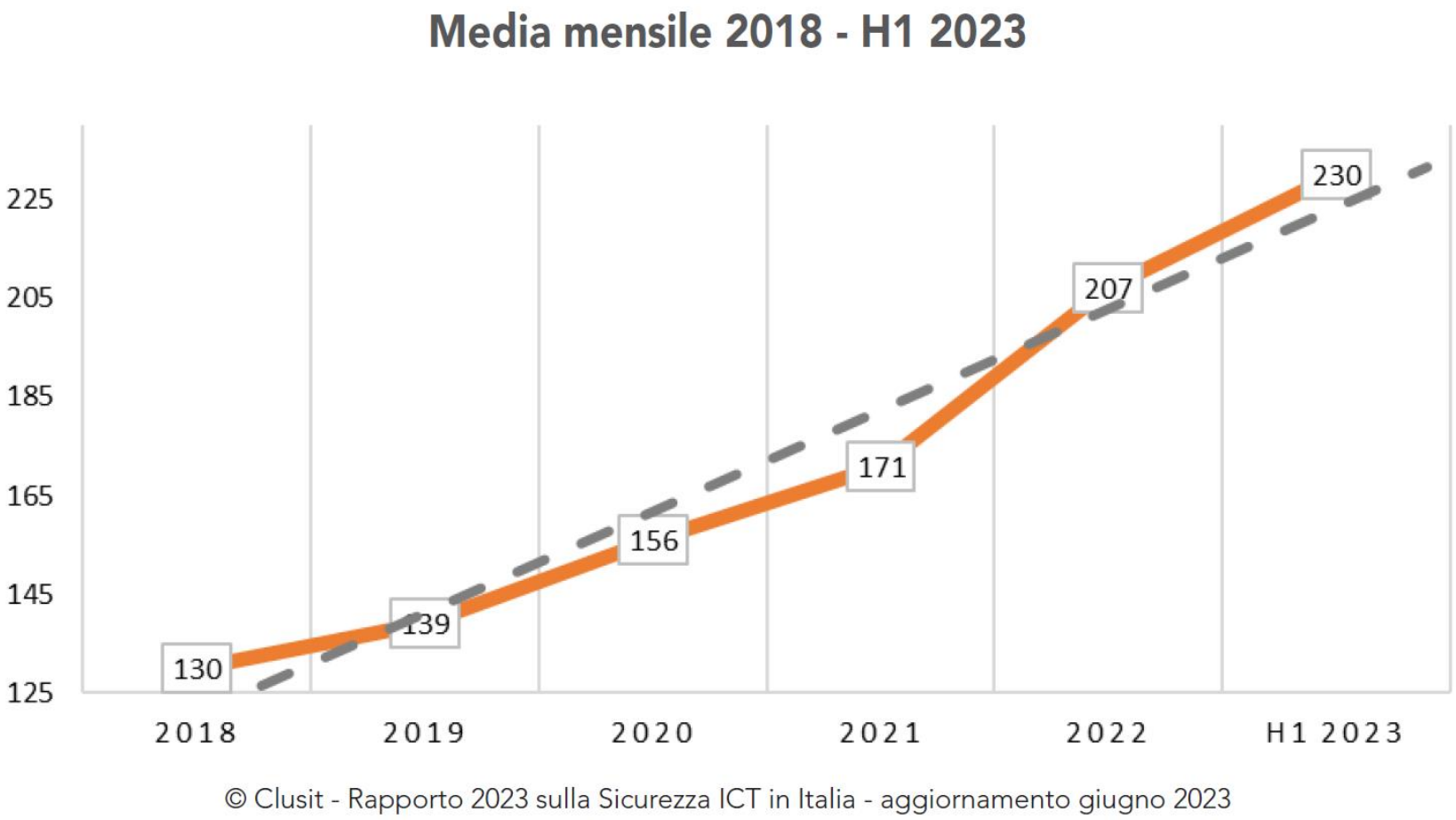


Fig. 4: *Andamento delle medie mensili nel periodo 2018-H1 2023*

Rapporto CLUSIT 2023

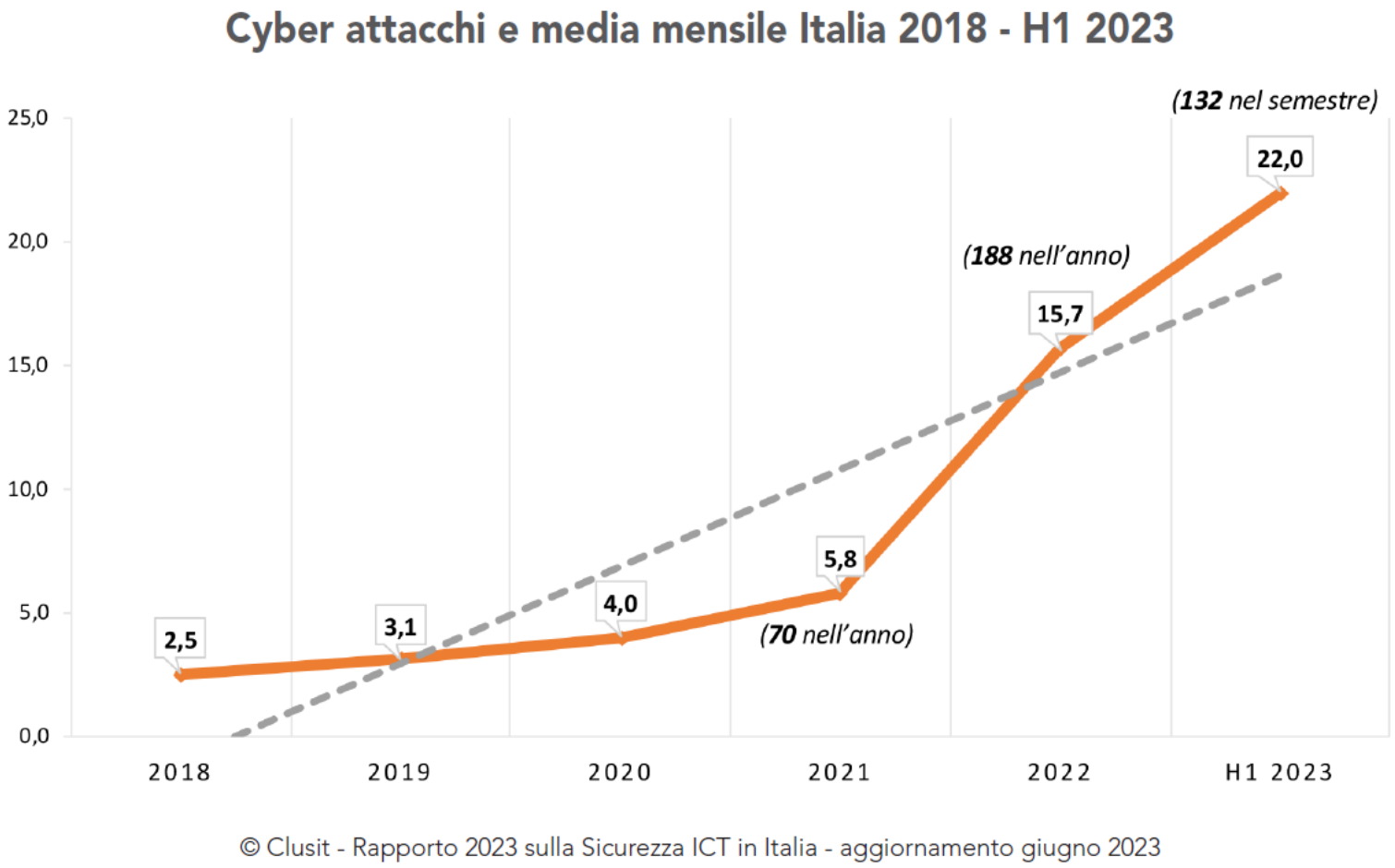


Fig. 21: *Distribuzione dei cyber attacchi e media mensile in Italia nel periodo 2018-H1 2023*

Hacker

- **Definizione originale:** Qualcuno con una conoscenza approfondita del mondo dei computer e dell'informatica – e di conseguenza in grado di entrare nelle profondità del sistema

Hacker

- **Black hat hacker (Cracker):** hacker attivamente impegnato in qualsiasi tipo di operazione criminale informatica. Il suo obiettivo è ottenere un guadagno economico tramite azioni di cyberspionaggio o altri scopi dannosi per le organizzazioni

Hacker

- **Black hat hacker (Cracker):** hacker attivamente impegnato in qualsiasi tipo di operazione criminale informatica. Il suo obiettivo è ottenere un guadagno economico tramite azioni di cyberspionaggio o altri scopi dannosi per le organizzazioni
- **White hat hacker (Ethical hacker):** conduce test e attacchi a siti Web e ai software per identificare possibili falle. Una volta rilevate le criticità, il white hat invia le notifiche direttamente al fornitore (o a un CERT), in modo che questo possa rilasciare una patch per correggere il difetto

Hacker

- **Black hat hacker (Cracker):** hacker attivamente impegnato in qualsiasi tipo di operazione criminale informatica. Il suo obiettivo è ottenere un guadagno economico tramite azioni di cyberspionaggio o altri scopi dannosi per le organizzazioni
- **White hat hacker (Hetical hacker):** conduce test e attacchi a siti Web e ai software per identificare possibili falle. Una volta rilevate le criticità, il white hat invia le notifiche direttamente al fornitore (o a un CERT), in modo che questo possa rilasciare una patch per correggere il difetto
- **Grey hat hacker:** opera in un regime di ambiguità etica. In sintesi, non compromette i sistemi con l'obiettivo malevolo di rubare dati ma è disposto a usare anche metodi illegali per trovare difetti o per rendere pubbliche le vulnerabilità o, ancora, vendere exploit zero-day ai governi o alle agenzie di intelligence

Tipologie di attaccanti

Cybercrime

Crimine commesso via computer, reti o dispositivi hardware

Cyber espionage

Attività volta ad ottenere informazioni industriali e commerciali da aziende competitor in maniera illecita

Hacktivism

Hacking per scopi politici o sociali

Information warfare

Uso di tecnologie informatiche per assumere posizioni di vantaggio nell'ambito di un conflitto (dichiarato o sommerso)

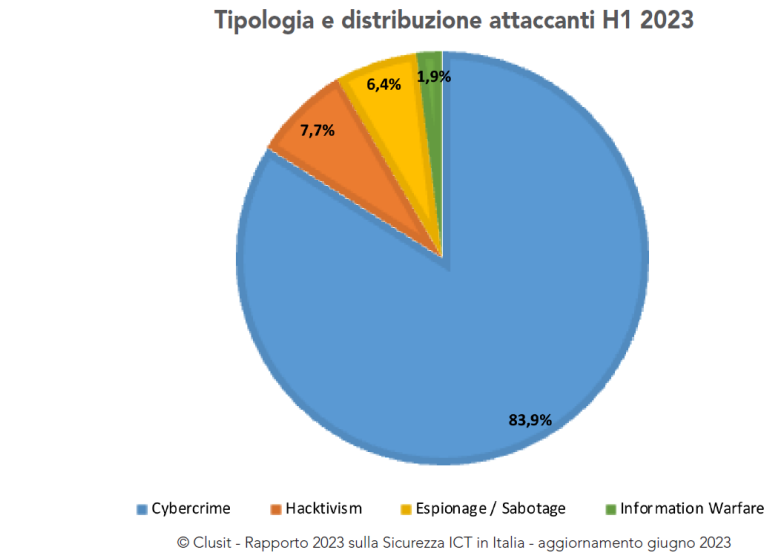


Fig. 6: *Andamento percentuale della tipologia di attaccanti nel H1-2023*

Tipologie di attaccanti

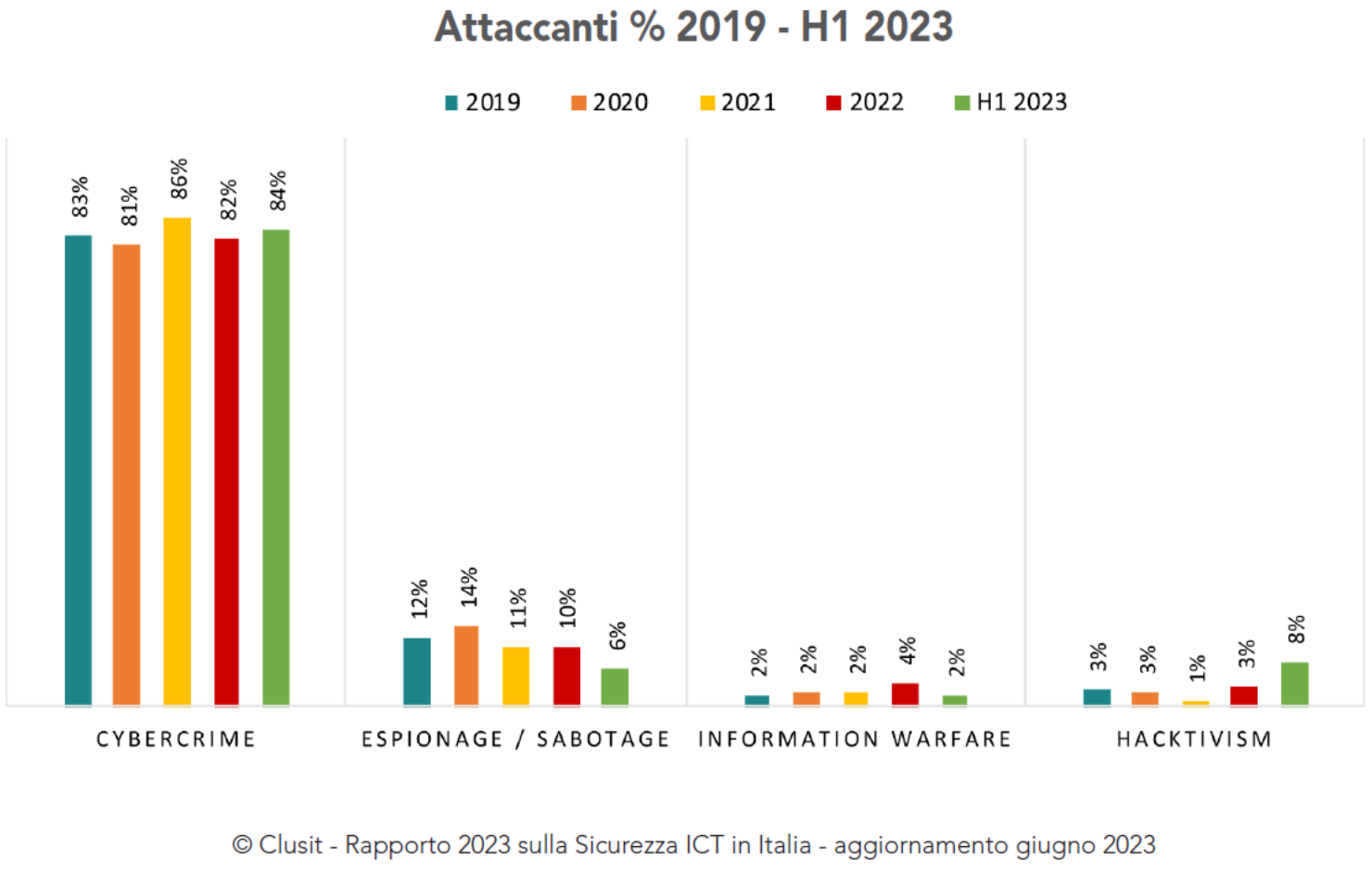


Fig. 5: *La distribuzione percentuale degli attaccanti tra il 2019 -H1 2023*

Vittime

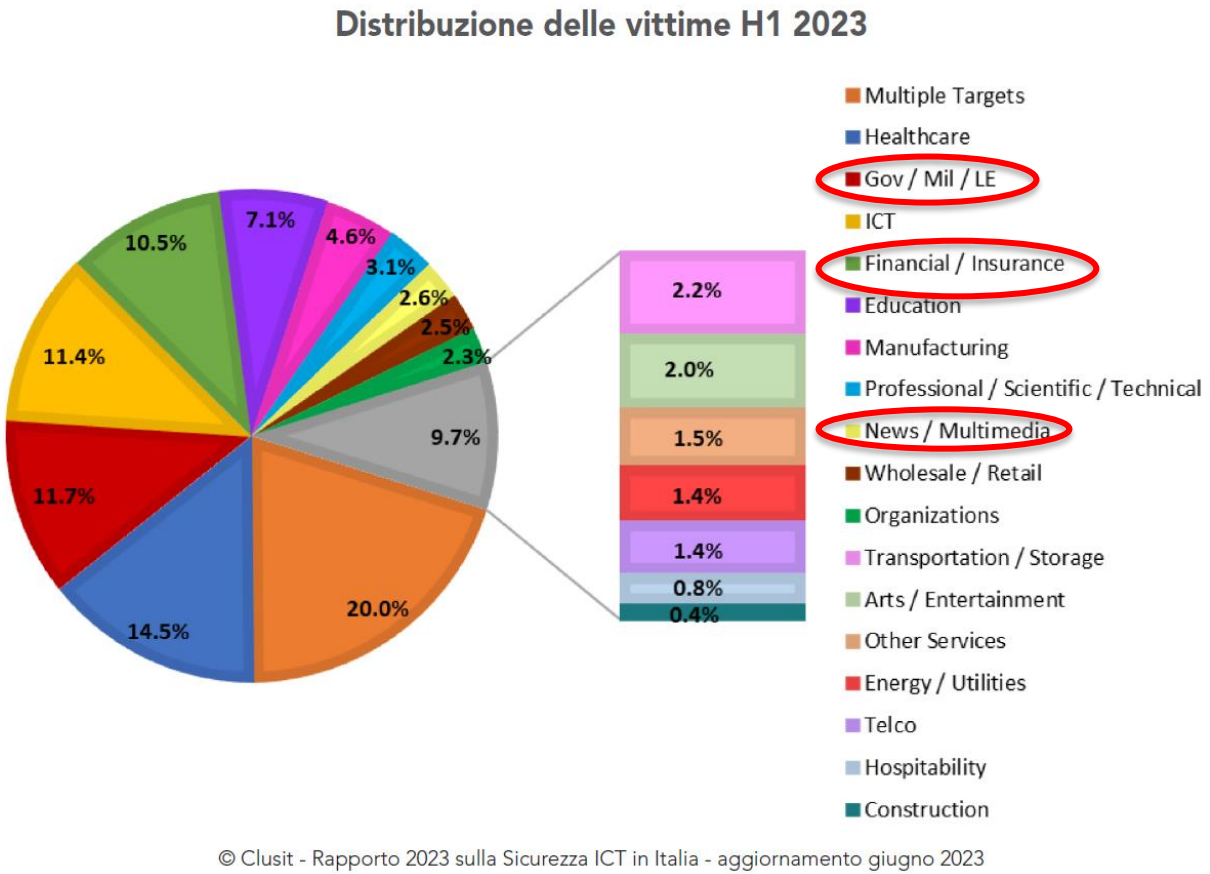


Fig. 7: *Andamento percentuale della tipologia di vittime nel primo semestre 2023*

Distribuzione delle vittime

1. Multiple targets
2. Healthcare
3. Government/Military
4. ICT
5. Financial/Insurance
6. Education
7. Manufacturing
8. News/Multimedia
9. …

Distribuzione geografica delle vittime

- Nel 2023H si confermano le vittime preponderanti in America
- Quasi un quarto degli attacchi ha come bersaglio posti in paesi diversi

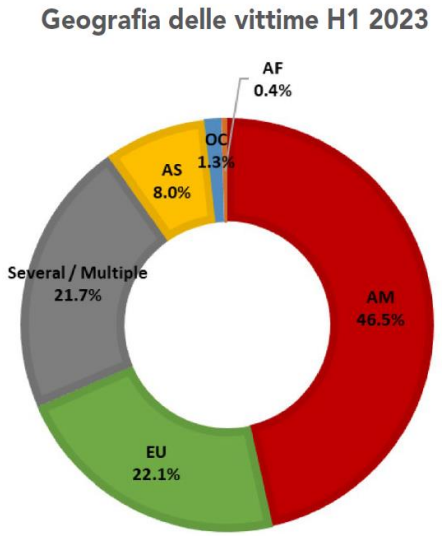


Fig. 10: *Distribuzione geografica delle vittime nel primo semestre 2023*

Distribuzione delle tecniche di attacco

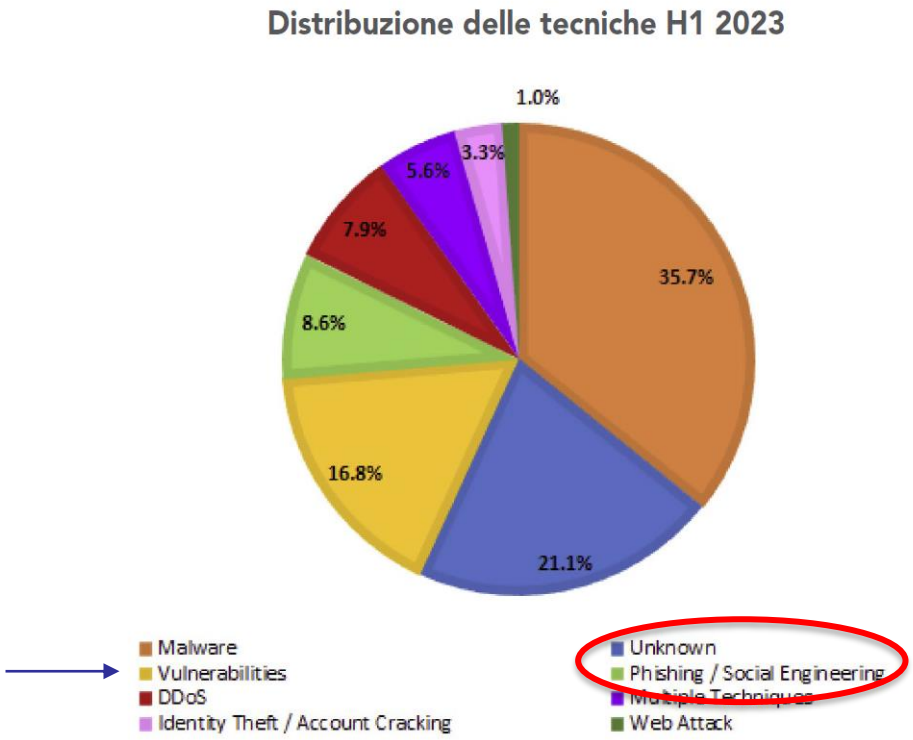


Fig. 11: *Distribuzione delle tecniche di attacco nel primo semestre 2023*

- Più del 60% degli attacchi ha come causa azioni «maldestre». Evidentemente, la nostra maturità e la postura delle nostre organizzazioni è a livelli ancora troppo bassi

Distribuzione delle tecniche di attacco

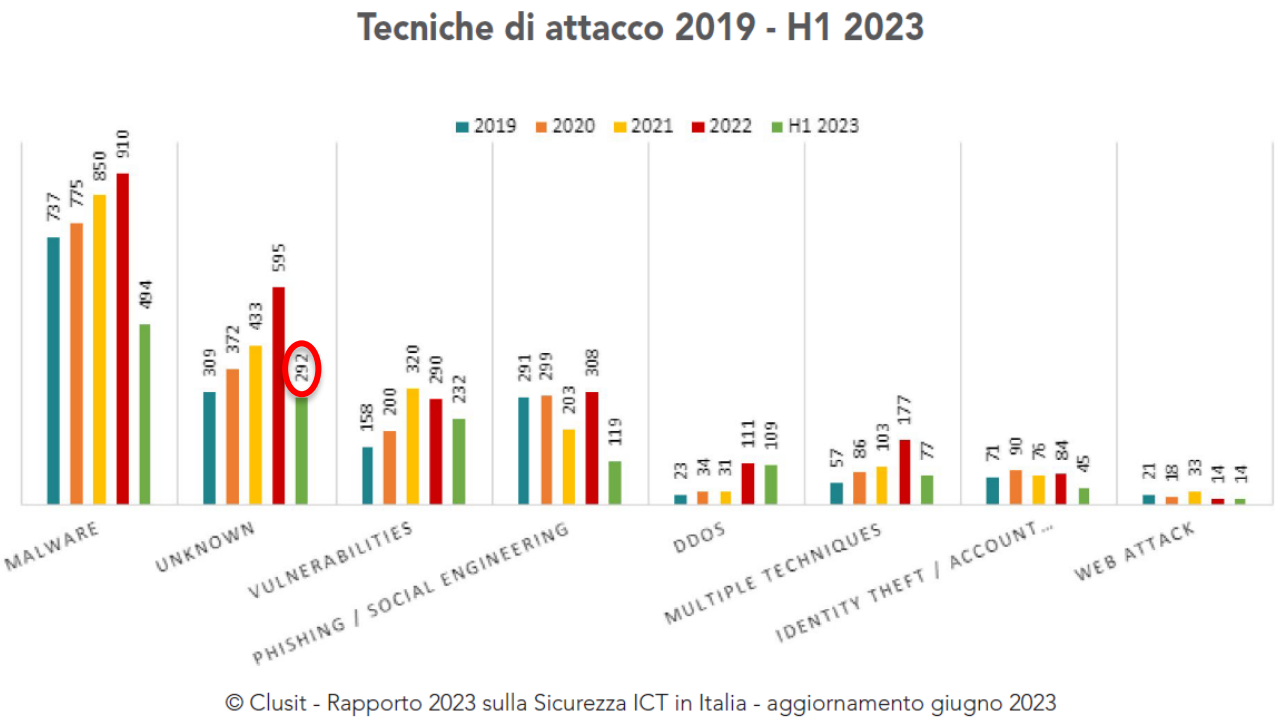


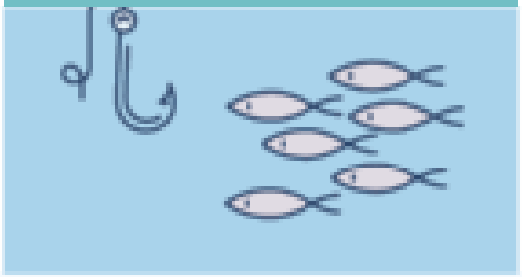
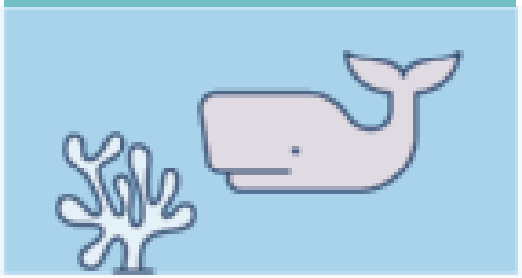
Fig. 12: *Distribuzione delle tecniche di attacco nel periodo 2019 - primo semestre 2023*

- Le “tecniche sconosciute” sono dovute al fatto che molti attacchi (un quinto del totale) diventano di dominio pubblico a seguito di un “data breach”, nel qual caso le normative impongono una notifica agli interessati, ma non di fornire una descrizione precisa delle modalità dell’attacco (che normalmente quindi non viene fornita)

Phishing

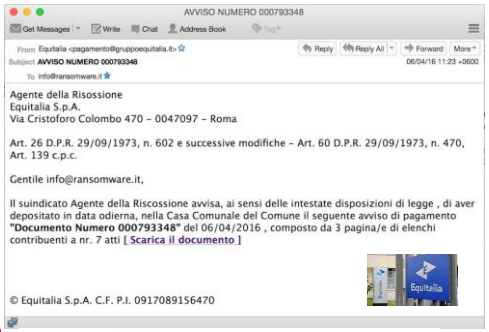
- Il phishing sfrutta la psicologia umana e fa uso dell'inganno per ottenere dalla vittima dati riservati o confidenziali (password, codici, pin, dati della carta di credito, informazioni finanziarie, ecc.), estorcere denaro o addirittura rubarne l'identità
- Email contraffatte, SMS, chat e social media
- I messaggi di phishing invitano a fornire direttamente i propri dati personali, oppure a cliccare un link che rimanda ad una pagina web dove è presente un form da compilare

Phishing

PHISHING	SPEAR-PHISHING	WHALING
		
prendono di mira chiunque abbia una casella di posta elettronica	prende di mira un gruppo specifico di individui per ottenere l'accesso all'obiettivo	prendono di mira una persona, in genere un dirigente di alto livello , al fine di ottenere informazioni riservate.

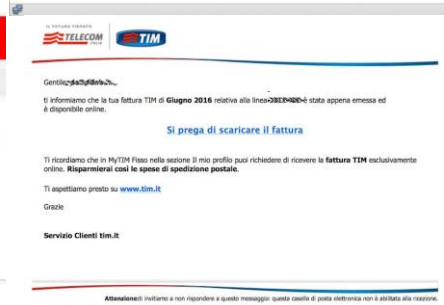
Phishing

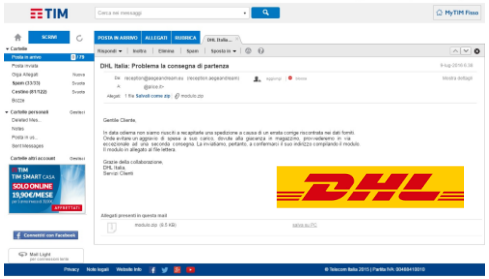

Enel
ENEL SERVIZIO ELETTRICO - Servizio di Maggior Tutela
DATI CLIENTE
Numero cliente: 566 880 539
Codice Fiscale: ZDRW6414UHQ
BOLLETTA PER LA FORNITURA DI ENERGIA ELETTRICA
N. fattura 19591426 del 6/07/2016 Bimestre giugno-luglio 2016
Totale da pagare entro il 31/05/2016: euro 497,32
DATI FORNITURA
RIEPILOGO IMPORTI FATTURATI

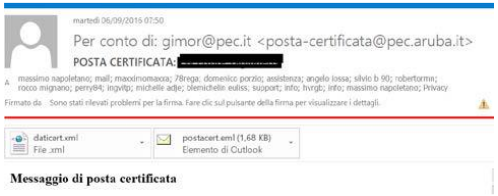

AVVISO NUMERO 000793348
Agente della Risossione
Equitalia S.p.A.
Via Cristoforo Colombo 470 – 0047097 – Roma
Art. 26 D.P.R. 29/09/1973, n. 602 e successive modifiche – Art. 60 D.P.R. 29/09/1973, n. 470, Art. 139 c.p.c.
Gentile info@ransomware.it,
Il suindicato Agente della Riscossione avvisa, ai sensi delle intestate disposizioni di legge , di aver depositato in data odierna, nella Casa Comunale del Comune il seguente avviso di pagamento "Documento Numero 000793348" del 06/04/2016 , composto da 3 pagina/e di elenchi contribuenti a nr. 7 atti [Scarica il documento]
© Equitalia S.p.A. C.F. P.I. 0917089156470


aruba.it


Recapito Elettronico Fattura
Il inviamo in allegato il Conto Telefonico Completo all'interno del quale puoi trovare la Fattura nr.
dell'importo di 146,16euro.
Ti ricordiamo che puoi scaricare il tuo Conto Telefonico Completo nella sezione "190 Fai da te" del sito www.vodafone.it (scopri come).
Per maggiori informazioni sulle voci del tuo Conto Telefonico visita la sezione dedicata su www.vodafone.it.
Cordiali Saluti.
Servizio Clienti Vodafone


TELECOM
TIM
ti informiamo che la tua fattura TIM di Giugno 2016 relativa alla linea
è disponibile online.
Si prega di scaricare il fattura
Ti ricordiamo che in MyTIM Fisso nella sezione Il mio profilo puoi richiedere di ricevere la fattura TIM esclusivamente online. Risparmierai così le spese di spedizione postale.
Ti aspettiamo presto su www.tim.it
Grazie
Servizio Clienti tim.it


TIM
DHL Italia: Problema la consegna di partenza
DHL


martedì 06/09/2016 07:50
Per conto di: gimor@pec.it <posta-certificata@pec.aruba.it>
POSTA CERTIFICATA:
daticert.xml
File .xml
postacert.eml (1,68 KB)
Elemento di Outlook
Messaggio di posta certificata

Come si svolge un attacco di phishing

Un tipico attacco di phishing si articola in diverse fasi:

1. Alle potenziali vittime, vengono inviate delle email contenenti informazioni il più possibile veritiere, familiari e/o allettanti. Un tipico messaggio di phishing potrebbe riguardare:
    - la scadenza di una determinata password di un servizio on-line;
    - l'accettazione dei cambiamenti delle condizioni contrattuali;
    - il rinnovo della carta di credito;
    - dei problemi inerenti accrediti, addebiti o trasferimenti di denaro su determinati conti online;
    - la mancata o incompleta presenza di informazioni, che riguardano determinati servizi on-line;
    - la presenza di offerte particolarmente invitanti, che magari invitano ad inserire informazioni personali per far sì di esser tra i primi a beneficiarne.

Come si svolge un attacco di phishing

2. Una volta catturata l'attenzione della vittima, l'email può contenere:
   - un file allegato che può diffondere malware (o minacce simili) all'interno del dispositivo e inviare dati personali della vittima al truffatore
   - un link che una volta cliccato riporta a un sito web fittizio controllato dal truffatore. La vittima viene invitata ad inserire i propri dati (come nome, password, numero di carta di credito, codice PIN e altro ancora), senza rendersi conto che li sta regalando al criminale

3. A questo punto il truffatore potrà disporre e utilizzare a suo piacimento i dati ottenuti con tutte le spiacevoli conseguenze del caso

Esempio di Phishing

Oggetto: Rimborso canone RAI
Mittente: Assistenza servizi telematici <no-reply@servizitelematici.it>
Data:
A:

Agenzia Entrate

Gentile cliente,

Le è stato riconosciuto il diritto al parziale rimborso del canone **RAI**, per un ammontare di euro **37,00**, A causa di un errore nel calcolo automatico, Lei ha versato una cifra in eccesso rispetto al dovuto e ha quindi diritto al rimborso della somma.

Importo : 37 euro
Riferimento : RAI-A8005W

Una volta inviata la richiesta, l'importo accreditato sarà visualizzato sul suo estratto conto secondo i tempi previsti dalla sua banca.

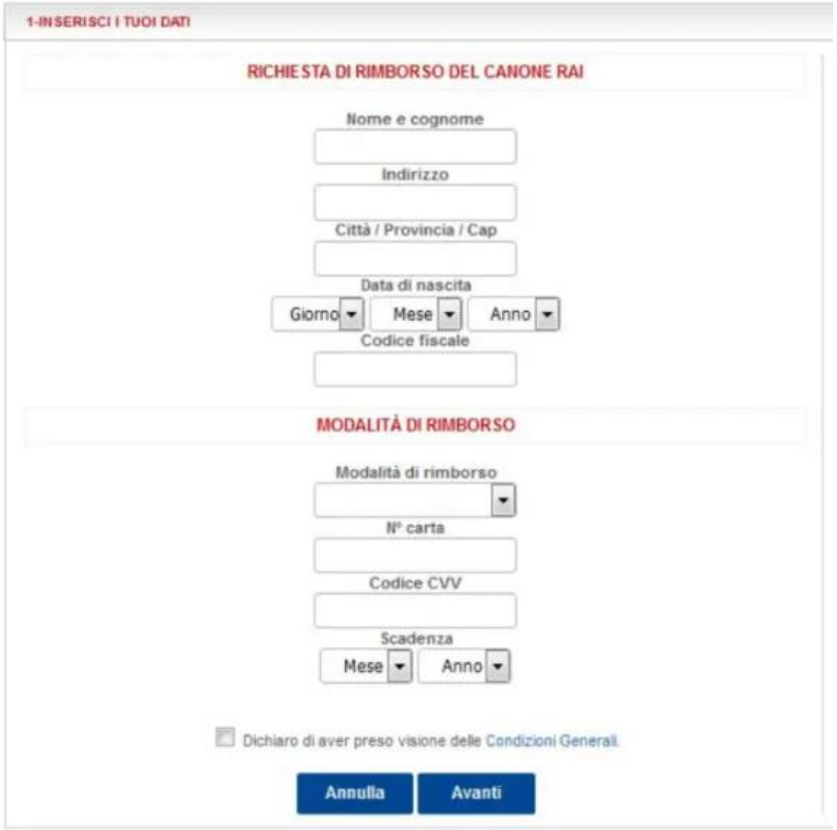
Nel caso lei non lo riuscisse a visualizzare, provi a contattare il servizio assistenza della sua carta in modo da ricevere informazioni riguardanti le tempistiche del suo circuito carta.

Per procedere con la richiesta segui il link : **https://www.rimborso.rai.it**

Cordiali saluti

Assistenza servizi telematici

RIMBORSO CANONE RAI
Riferimento: RAI-A8005W



Come difendersi dal phishing

Mettere in pratica queste semplici regole di sicurezza informatica suggerite dal CERT-PA:

- non condividere mai i propri dati sensibili con una terza parte. Le compagnie ufficiali non chiedono mai informazioni sensibili via e-mail;
- non aprire allegati del messaggio se non si è sicuri dell'identità del mittente;
- non cliccare su alcun link presente nel corpo del messaggio se non si è sicuri dell'identità del mittente;
- se si ricevono mail che chiedono di inserire dati personali (login e password o numero di carta di credito), è opportuno verificare sempre la veridicità del messaggio con una semplice telefonata all'istituto

Come difendersi dal phishing

Mettere in pratica queste semplici regole di sicurezza informatica suggerite dal CERT-PA:

- controllare che la connessione sia HTTPS e verificare che, all'apertura della pagina, il dominio sia effettivamente quello "ufficiale";
- installare nel computer un antivirus che protegga anche dal phishing e mantenerlo costantemente aggiornato;
- fidarsi dei filtri antispam del proprio provider di posta;
- utilizzare password robuste e cambiarle con frequenza;
- non utilizzare mai la stessa password per i vari servizi on-line.

Attacchi: i malware

- Il termine *malware* (abbreviazione di «malicious software») indica in maniera generica, un qualunque software che agisca contro l'interesse dell'utente. Oltre al computer o al dispositivo infetto, il malware può colpire anche tutti i dispositivi con cui questo comunica
- Esistono diverse tipologie di malware (trojan, worm, keylogger, ransomware, infostealer, rootkit, virus, cryptominer, ecc)
- In generale, lo scopo principale dei malware è di rubare dati personali e/o aziendali, spiare le vittime e danneggiare i sistemi infetti

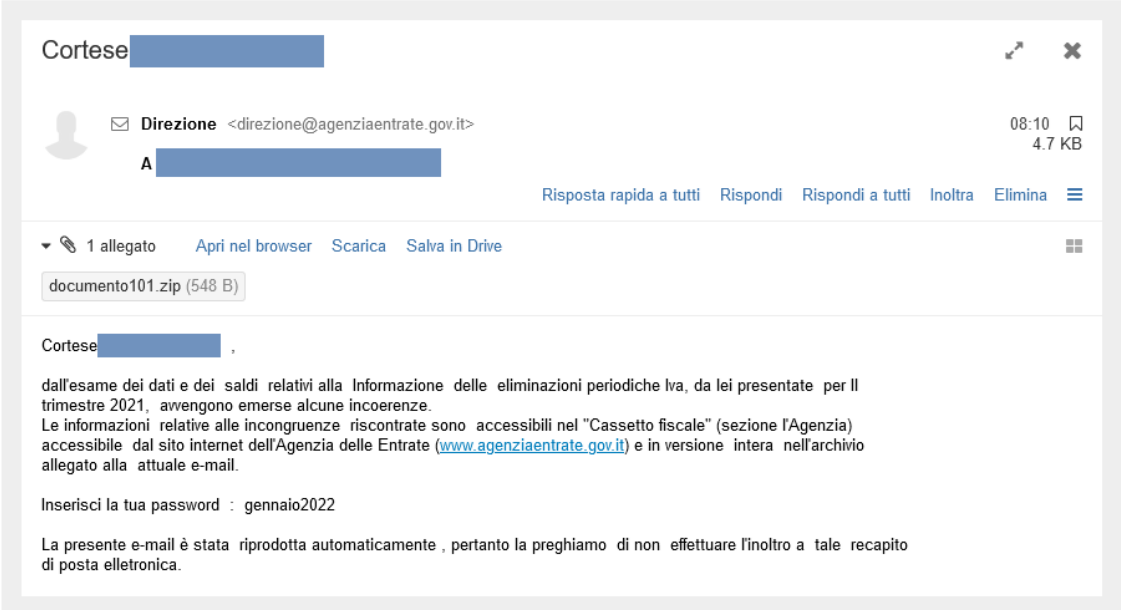
Esempio di campagna malevola

In atto campagna massiva Gozi/Urnsif veicolata come una comunicazione della Agenzia delle Entrate

12/01/2022

Ursnif

È iniziata ieri ed è attualmente in corso una campagna mirata verso utenze italiane volta a veicolare il malware Ursnif tramite una email che chiede di prendere visione di un documento allegato dell'Agenzia delle Entrate contenente informazioni riguardanti presunte "incoerenze" emerse nel trimestre 2021.



Cortese [redacted]

Direzione <direzione@agenziaentrate.gov.it> 08:10 4.7 KB

A [redacted]

Risposta rapida a tutti | Rispondi | Rispondi a tutti | Inoltra | Elimina

1 allegato | Apri nel browser | Scarica | Salva in Drive

documento101.zip (548 B)

Cortese [redacted] ,

dall'esame dei dati e dei saldi relativi alla Informazione delle eliminazioni periodiche Iva, da lei presentate per Il trimestre 2021, avvengono emerse alcune incoerenze.
Le informazioni relative alle incongruenze riscontrate sono accessibili nel "Cassetto fiscale" (sezione l'Agenzia) accessibile dal sito internet dell'Agenzia delle Entrate (www.agenziaentrate.gov.it) e in versione intera nell'archivio allegato alla attuale e-mail.

Inserisci la tua password : gennaio2022

La presente e-mail è stata riprodotta automaticamente , pertanto la preghiamo di non effettuare l'inoltro a tale recapito di posta elletronica.

Attacchi: i ransomware

- Il ransomware è un tipo di malware in grado di "infettare" un dispositivo bloccando l'accesso a tutti o ad alcuni dei suoi contenuti per poi chiedere un riscatto (in inglese, "ransom").
- Un attacco ransomware potrebbe causare danni devastanti a qualsiasi organizzazione in quanto viene compromessa:
  - l'integrità dei dati che vengono cifrati dal ransomware;
  - la disponibilità di dati/servizi;
  - la riservatezza dei dati se oltre alla cifratura c'è stata una esfiltrazione degli stessi.
- All'organizzazione colpita viene comunicato che ha poco tempo per effettuare il versamento del riscatto, altrimenti il blocco dei contenuti diventerà definitivo e i dati trafugati verranno messi in vendita.

Ransomware

- Alcuni ransomware bloccano il sistema e intimano l'utente a pagare per sbloccare il sistema

- Altri cifrano i file dell'utente chiedendo di pagare per riportare i file cifrati in chiaro

Ransomware

- Generalmente l'operazione prevede che prima di procedere con la cifratura dei dati presenti nel sistema possa essere effettuata un'esfiltrazione di tutte le informazioni.

- Fino allo scorso anno gli attacchi ransomware prevedevano quasi esclusivamente la crittografia dei dati che venivano resi indisponibili a tempo indeterminato.

- Nell'ultimo anno si è aggiunta la divulgazione dei dati nel dark web.

Double extortion

Ransomware

- Oltre a richiedere il riscatto all'azienda e a farne trapelare i dati, ora le richieste di riscatto vengono recapitate anche ai clienti dell'azienda stessa.

- Questo è, ad esempio, avvenuto per l'azienda finlandese Vastaamo, specializzata in supporto psicoterapeutico.

- Molti pazienti hanno riferito di aver ricevuto e-mail con una richiesta di 200 euro in Bitcoin per evitare che il contenuto delle loro discussioni con gli psicologi fosse reso pubblico.

Triple extortion

Ransomware

C’è il denaro e non l’ideologia all’origine di quello che è stato definito “un attacco senza precedenti”. Si tratta di un ransomware e l’attacco è partito dal PC di un dipendente di LazioCrea in smartworking. Salvi i backup, la Regione sta man mano rendendo nuovamente disponibili i servizi

05 Ago 2021

di Patrizia Fabbri

Ransomware

Utilizza il modello commerciale "**Ransomware as a Service**", che consente a gruppi di criminali informatici di utilizzare il malware in "franchising". Gli affiliati dispongono di un'interfaccia web per generare autonomamente nuove varianti di ransomware, gestire le vittime, elaborare i riscatti, ottenere statistiche, decriptare i file e altro ancora

Ransomware

L'ANALISI TECNICA

ESXiArgs, il ransomware dell'attacco ai server VMware ESXi: cosa sappiamo e come difendersi

Home > Attacchi hacker e Malware: le ultime news in tempo reale > Ransomware

169 condivisioni

Nei recenti attacchi su scala globale in cui sono stati presi di mira i server VMware ESXi non aggiornati gli attori della minaccia hanno utilizzato il nuovo ransomware ESXiArgs. Ecco tutti i dettagli e i consigli per mitigare la minaccia

Pubblicato il 06 Feb 2023

https://www.cybersecurity360.it/nuove-minacce/ransomware/esxiargs-il-ransomware-dellattacco-ai-server-vmware-esxi-cosa-sappiamo-e-come-difendersi/

Ransomware

- Nuova figura: **Negoziatore**.
- Persone che hanno fatto questo mestiere nei Carabinieri o in Polizia.
- Oltre a tenere dal punto di vista psicologico, mentre chiedono dilazioni del pagamento o una riduzione della cifra, devono essere consapevoli del fatto che gli attaccanti conoscono benissimo la situazione dell'azienda, sia dal punto di vista economico sia da quello infrastrutturale.
- Occorre anche avere una conoscenza capillare delle tattiche e dell'affidabilità dei gruppi ransomware coinvolti.

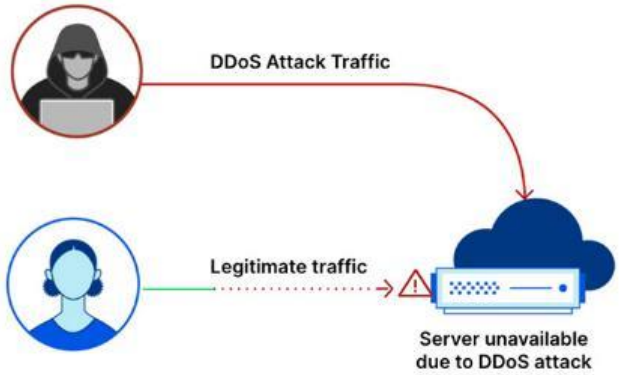
https://www.fortuneita.com/2021/08/03/come-si-negozia-con-un-hacker/

Ransomware


Figure 1 //
TOP 10
ACTIVE
RANSOMWARE
GROUPS IN Q4
Lockbit3
243
Play
109
Alphv
109
8Base
71
Noescape
58
Akira
48
Medusa
46
Incransom
46
Bianlian
28
Blackbasta
28

Attacchi DDoS

- Nuova tendenza: esecuzione di attacchi DDoS accompagnata da richieste monetarie in cambio dell'annullamento dell'attacco.



- Più di un attacco DDoS su cinque è accompagnato da una richiesta di riscatto.
- Gli attaccanti si avvalgono spesso di botnet a noleggio.

Attacchi alle applicazioni web

Allegato 1: Linee Guida per l'adozione di un ciclo di sviluppo di software sicuro

- Secondo la fonte Gartner, negli ultimi anni oltre il 75% degli attacchi sono stati indirizzati verso le applicazioni web;
- Gli obiettivi degli attacchi sono le vulnerabilità che si celano all'interno delle applicazioni software che forniscono un facile percorso d'ingresso per compromettere i sistemi o lanciare ulteriori attacchi e malware.

2021
A01:2021-Broken Access Control
A02:2021-Cryptographic Failures
A03:2021-Injection
A04:2021-Insecure Design
A05:2021-Security Misconfiguration
A06:2021-Vulnerable and Outdated Components
A07:2021-Identification and Authentication Failures
A08:2021-Software and Data Integrity Failures
A09:2021-Security Logging and Monitoring Failures*
A10:2021-Server-Side Request Forgery (SSRF)*

L'OWASP traccia periodicamente la lista delle 10 vulnerabilità più critiche delle applicazioni web.

Attacco 0-day

Che cos'è?

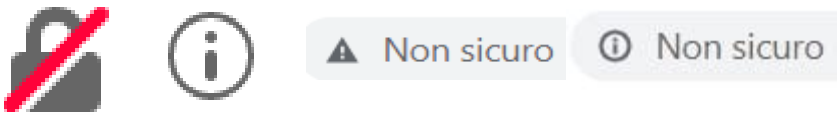
- Lo 0-day (o zero-day) è una qualsiasi vulnerabilità di sicurezza informatica non pubblicamente nota.
- Vengono chiamati 0-day proprio perché lo sviluppatore del software vulnerabile ha "zero giorni" per riparare la falla nel programma prima che qualcuno la possa sfruttare.

Perché è rilevante?

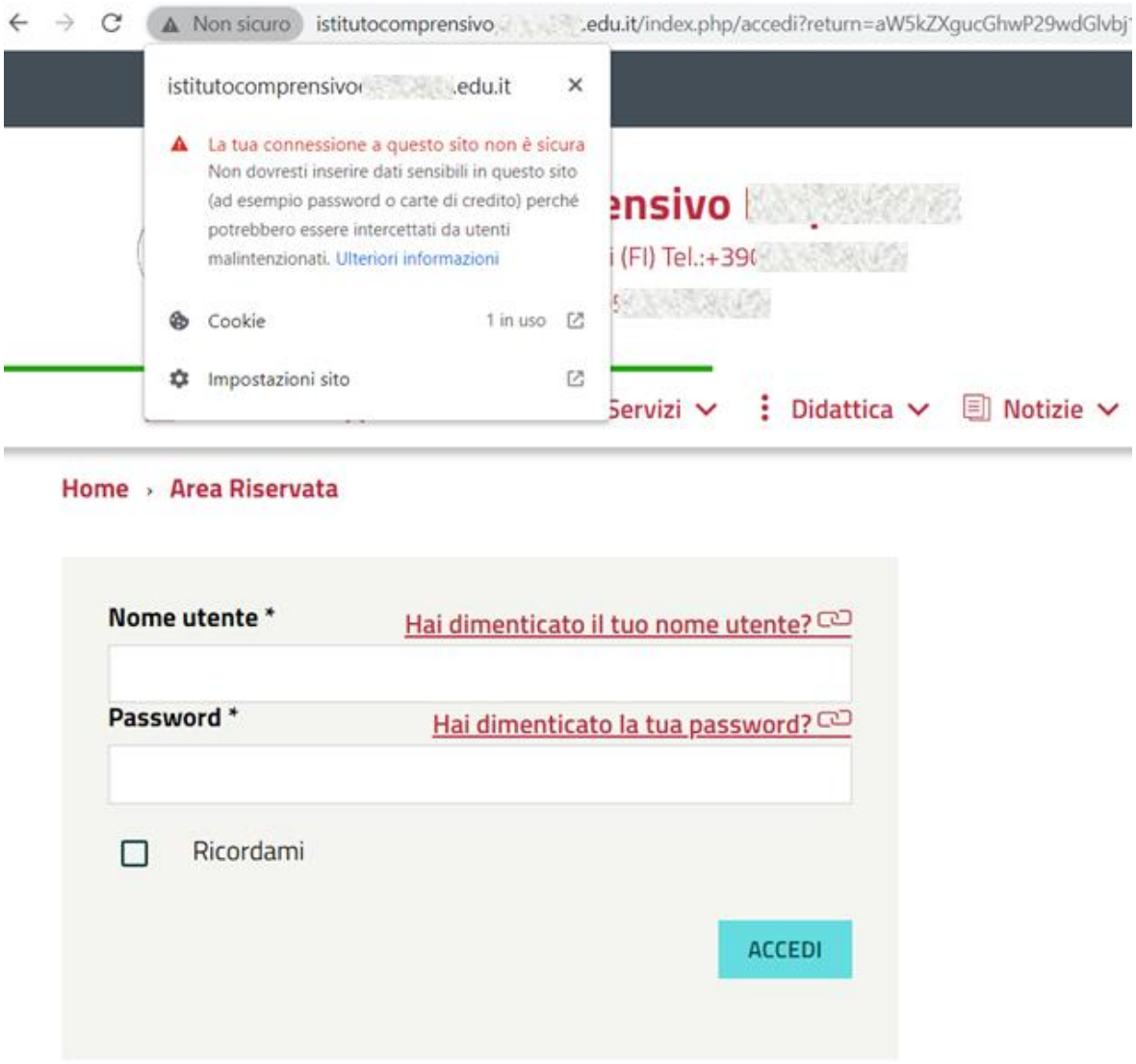
- Lo zero-day è molto rilevante perché è una vulnerabilità ancora sconosciuta. Di conseguenza può essere molto pericolosa e sfruttata dai cyber criminali per portare avanti le loro azioni indisturbati.

HTTP

- HTTP e HTTPS sono due varianti dello stesso protocollo che permettono la comunicazione tra il browser dell'utente e i web server che ospitano i siti web che l'utente visita durante la navigazione su Internet.
- **HTTP** (Hyphertext Transfer Protocol) è un protocollo estremamente funzionale, tanto che viene utilizzato per gestire queste comunicazioni da quando esiste il web ma presenta una grossa limitazione: non garantisce la riservatezza dei dati in quanto essi vengono trasmessi in chiaro e sono quindi potenzialmente intercettabili durante la comunicazione.
    - Gli aggressori possono, in sostanza, leggere o modificare qualsiasi traffico HTTP, senza che l'utente ne sia a conoscenza.
    - Il protocollo HTTP è quindi considerato un protocollo non sicuro.



Esempio di sito web non sicuro

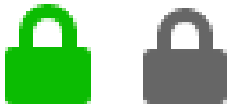


HTTPS

HTTPS (Hyphertext Transfer Protocol Secure) invece, è un protocollo che fornisce alcuni livelli fondamentali di protezione delle informazioni che viaggiano sulla rete Internet:

- Crittografia: tutti i dati scambiati tra il browser dell'utente e il server vengono cifrati per proteggerli dalle intercettazioni, migliorando la sicurezza dell'utente e impedendo agli aggressori di leggere o alterare i dati in transito.
- Integrità dei dati: i dati coinvolti nella comunicazione non possono essere modificati o alterati durante il trasferimento, anche in maniera non intenzionale, senza che questo evento venga rilevato. Questa funzionalità non solo mette al riparo da attacchi intenzionali ma anche da errori di comunicazione che potrebbero bloccare o alterare la visualizzazione delle pagine.
- Autenticazione**:** il browser ha sempre la certezza di stare dialogando con il sito web desiderato.

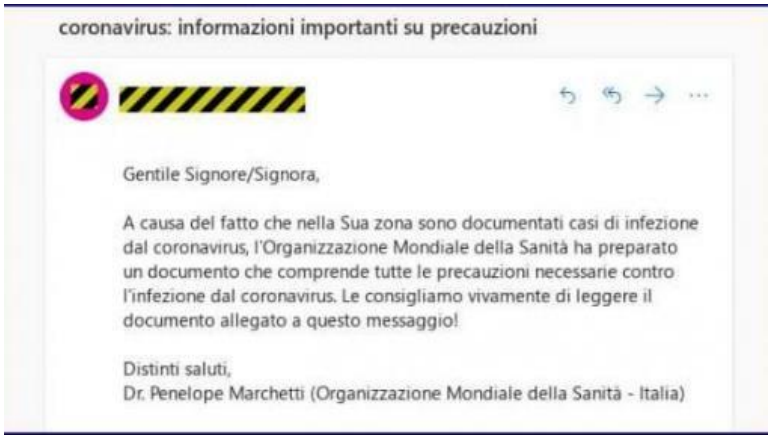
L'HyperText Transfer Protocol over Secure Socket Layer rispetta dunque i principi di autenticazione (del sito web visitato), riservatezza del dato e integrità del dato.



Cybersecurity e Covid-19

- Eventi come lo tsunami nell'Oceano Indiano del 2004 e l'epidemia di virus Zika sono stati utilizzati come esche per attacchi cyber.

- L’emergenza Covid-19 ha fornito un’ulteriore opportunità di questo tipo, sfruttando la psicosi:
  - tentativi di **ingegneria sociale** a tema virale
  - vendita di **prodotti sanitari** contraffatti
  - diffusione di **disinformazione**



Cybersecurity e Covid-19

- Inoltre, un numero senza precedenti di persone **lavora da remoto**, spesso per la prima volta.

- Le aziende si affrettano a fornire terminali ai dipendenti, distribuire software ed implementare piattaforme di collaborazione.

- Spesso l'accesso avviene da **macchine private** poco sicure ed attaccabili.

- Ma anche in assenza di attacchi, un dipendente in **smart working** potrebbe ad esempio inviare documenti aziendali sulla propria posta elettronica personale per lavorarci da casa.

- Se tali documenti contengono dati personali (ad es. di clienti o altri dipendenti), ciò già si inquadra come **data breach** (GDPR).

Cyber2Physical

Cyber2Physical

Doctors disabled wireless in Dick Cheney's pacemaker to thwart hacking

22 OCT 2013 2

Celebrities, Data loss, Denial of Service, Malware, Security threats, Vulnerability

Cyber2Physical

- 21 Luglio 2015: (White Hat) Hacker controllano Jeep Cherokee via internet a 110 km/h e la portano fuori strada.

- Gli ″hacker″, ad una distanza di circa 20 km, hanno utilizzato un comune laptop, sfruttando la vulnerabilità del servizio Uconnect.

https://www.youtube.com/watch?v=MK0SrxBC1xs&ab_channel=WIRED

Cyber2Physical

Attacco hacker provoca un black-out in Ucraina

Dic 22, 2016 Marco Schiaffino Attacchi, Hacking, News, RSS 0

Vittima del sabotaggio una compagnia che fornisce energia elettrica. L'Ucraina protagonista di un incidente simile lo scorso anno. I sospetti si concentrano su hacker russi.

Ci sarebbe un attacco hacker dietro al **black out di 1 ora** che ha interessato il territorio Ucraino. La fornitura di energia ha subito uno stop prolungato lo scorso 17 dicembre e, stando a quanto dichiarato da **Vsevolod Kovalchuk**, direttore della società elettrica **Ukrenergo**, la causa sarebbe un attacco informatico.

In un post su Facebook, Vsevolod Kovalchuk ha attribuito il black out di 75 minuti a una "interferenza esterna proveniente dalla rete informatica". Tradotto: un attacco hacker.

Non è la prima volta che le centrali elettriche finiscono vittima di attacchi del genere. I sistemi SCADA che gestiscono le infrastrutture di questo tipo di impianti sono trai bersagli più "gettonati" dai gruppi hacker che collaborano con servizi segreti e agenzie governative.

Cyber2Physical

Usa, hacker tenta di avvelenare le acque di una città della Florida con la soda caustica

Fbi e Cia sono alla ricerca del colpevole. Non è chiaro se americano o straniero. È successo a 27 chilometri da Tampa

09 FEBBRAIO 2021

1 MINUTI DI LETTURA

WASHINGTON - Un hacker ha tentato di inquinare le riserve di acqua della cittadina di Oldsmar in Florida, alzando i livelli di un additivo chimico potenzialmente pericoloso mettendo a rischio la vita di migliaia di persone. Le autorità sono riuscite a impedire il peggio mettendo al sicuro tutti i cittadini.

Cyber Warfare

Rai News Cronaca Esteri Politica Televideo Rai Sport | TG Regionali | Rai News 24 • LIVE

Roma 10° 3°

Rai

Temi Caldi → Covid Quirinale Diario dall'Afghanistan

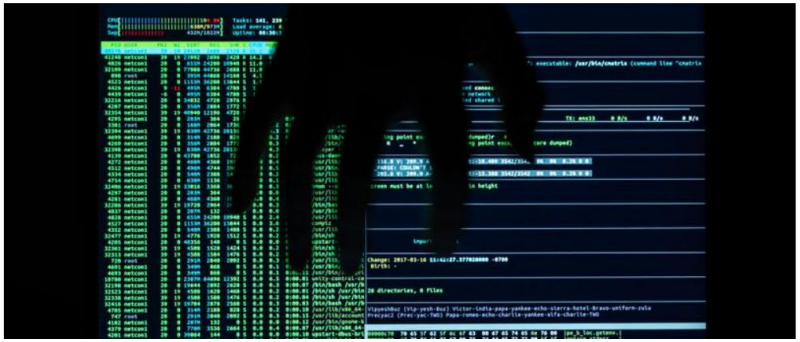
— ESTERI

14 Gennaio 2022

Allarme lanciato via Facebook

Attacco informatico contro siti governativi ucraini

Nato: sostegno pratico all'Ucraina



LEGGI ANCHE:

Fifa 2022, attacco hacker contro la piattaforma EA Sport. Colpiti anche profili italiani

Vulnerabilità

Come ci rubano le credenziali?

- Ingegneria sociale (social engineering): con email o messaggi di *phishing* si convince l'utente a comunicare la propria password. In pratica siamo noi che ci lasciamo ingannare dalle tecniche di social engineering e diamo le password a chi ce le chiede, attraverso per esempio messaggi, e-mail, siti fake (falsi) che dissimulano un sito a noi noto;

- La password viene indovinata: molto spesso utilizziamo informazioni personali quali nomi, date di nascita o altri riferimenti che sono facilmente indovinabili;

- Password reuse: si sfrutta la cattiva abitudine degli utenti di riutilizzare la stessa password su servizi web diversi. Questo errore rende possibile un tipo di attacco noto come "Credential Stuffing" nel quale le credenziali rubate da portali web, vengono usate per ottenere l'accesso ad altri servizi web dove gli utenti hanno riutilizzato le stesse password;

Come ci rubano le credenziali?

- Attacco a forza bruta ("brute force"): consiste nel provare in modo automatico tutte le possibili combinazioni di lettere, caratteri speciali e numeri che formano le possibili password, finché non si individua quella giusta. A seconda della lunghezza e complessità della password, la sua individuazione può richiedere da pochi secondi a molti anni.

- Attacco a dizionario: tecnica di brute force verso un cifrario o sistema di autenticazione, in cui l'attaccante impiega un "dizionario", ossia un insieme predefinito di stringhe aventi un'alta probabilità di successo. Solitamente i dizionari sono composti da un elenco di parole o stringhe di uso comune.

Gestione delle credenziali – Lato utente

Una buona password:

- deve essere abbastanza lunga: almeno 8 caratteri; più aumenta il numero dei caratteri più la password diventa “robusta”;

- deve contenere caratteri di almeno 4 diverse tipologie, da scegliere tra: lettere maiuscole, lettere minuscole, numeri, caratteri speciali;

- non deve contenere riferimenti personali facili da indovinare (nome, cognome, data di nascita, ecc.). Non deve nemmeno contenere riferimenti al nome utente (detto anche user account, alias, user id, user name);

Gestione delle credenziali – Lato utente

Una buona password:

- meglio evitare che contenga parole “da dizionario”, cioè parole intere di uso comune: è meglio usare parole di fantasia oppure parole “camuffate” per renderle meno comuni, magari interrompendole con caratteri speciali (ad esempio: caffè può diventare caf-f3);

- andrebbe periodicamente cambiata, soprattutto per i profili più importanti o quelli che usi più spesso (e-mail, e-banking, social network, ecc.).

Gestione delle credenziali – Lato utente

- Utilizzare password diverse per account diversi (e-mail, social network, servizi digitali di varia natura, ecc.).
- NON utilizzare password già utilizzate in passato;
- Eventuali password temporanee rilasciate da un sistema o da un servizio informatico vanno sempre immediatamente cambiate, scegliendone una personale;
- Utilizzare (laddove disponibili) meccanismi di autenticazione multi fattore (es. codici OTP one-time-password), che rafforzano la protezione offerta dalla password;

Gestione delle credenziali – Lato utente

- Non scrivere mai le password su biglietti che possono essere distrattamente lasciati in giro, oppure in file non protetti su dispositivi personali (computer, smartphone o tablet).

- Evitare sempre di condividere le password via e-mail, sms, social network, instant messaging, ecc.;

- Se si usano pc, smartphone e altri dispositivi che non ci appartengono, evitare sempre che possano conservare in memoria le password da voi utilizzate.

Social engineering e phishing

Tecniche di attacco	2018	2019	2020	2021	2021 su 2020	TREND
Malware	601	737	775	850	9.7%	↗
Unknown	429	309	372	433	16.4%	↗
Vulnerabilities	143	158	200	320	60.0%	↑
Phishing / Social Engineering	170	291	299	203	-32.1%	↓
Multiple Techniques	64	57	86	103	19.8%	↗
Identity Theft / Account Cracking	67	71	90	76	-15.6%	↘
Web Attack	43	21	18	33	83.3%	↑
DDoS	37	23	34	31	-8.8%	↘
TOTALE	1.554	1.667	1.874	2.049		

Social engineering

- Il social engineering (o ingegneria sociale) è una tecnica di attacco basata sullo studio del comportamento delle persone col fine di manipolarle e carpire informazioni confidenziali

- Il procedimento si basa sulla psicologia umana e sfrutta la fiducia, la mancanza di conoscenza e, in generale, le vulnerabilità della vittima per ottenere dati confidenziali (password, informazioni su conti correnti, informazioni finanziarie), estorcere denaro o persino rubarne l'identità

Social engineering

- Il cuore di un attacco di ingegneria sociale presuppone che nella truffa entri in gioco l'abilità del singolo hacker di manipolare la vittima facendo leva su questi elementi:
  - Paura
  - Compassione
  - Senso di colpa
  - Autorevolezza
  - Ignoranza
  - Avidità

Social engineering: vettori di attacco

20 password più comuni in Italia (2023)

1	admin
2	123456
3	password
4	Password
5	12345678
6	123456789
7	password99
8	qwerty
9	UNKNOWN
10	12345
11	ciaociao
12	francesco
13	1234567890
14	Windows1
15	Windows10
16	riccardo
17	corrado
18	francesca
19	andrea
20	juventus

fonte: *NordPass*

La scelta della password

“The only secure password is the one you can’t remember”
(Troy Hunt – 2011)

Chi può essere al sicuro?

Chi può essere al sicuro?

Cos’è una vulnerabilità informatica?

VULNERABILITÀ

secondo la terminologia elaborata dal MITRE

«Un difetto in un software, firmware, hardware o componente di servizio derivante da una debolezza che può essere sfruttata da un attaccante, causando un impatto negativo sulla riservatezza, integrità o disponibilità di uno o più componenti interessati.»

MITRE Corporation: associazione americana a supporto di diverse Agenzie governative, tra cui quello della sicurezza informatica

Cos’è una vulnerabilità informatica?

Una vulnerabilità è la somma di tre fattori:

- una debolezza esistente;
- l’accessibilità dell’attaccante alla debolezza;
- la capacità dell’attaccante di “sfruttare” la debolezza per conseguirne un vantaggio

Cos’è una vulnerabilità informatica?

- Se gli errori del software mettono a rischio la sicurezza dei dati si parla di vulnerabilità informatica del software.
- In assenza di strumenti di attacco e di valore per l’hacker attaccante siamo in presenza di un “normale” bug.
- Vi sono molteplici vulnerabilità software che possono essere sfruttate dagli attaccanti per compromettere confidenzialità, integrità e disponibilità di dati/servizi.

Cos’è una vulnerabilità informatica?

- Le vulnerabilità possono riscontrarsi ovunque intervenga il software:
  - Sistemi operativi
  - Applicazioni
  - Programmi
  - Librerie
  - Protocolli
  - Ecc.

Come si misura la gravità di una vulnerabilità?

- Il CVSS (Common Vulnerability Scoring System) è un framework (arrivato alla versione 3.1) utilizzato per classificare le caratteristiche e la gravità dei punti deboli sfruttabili, creando un sistema di punteggio che valuta la «Severity» (gravità) di ogni singola vulnerabilità.

- Il punteggio di base opera utilizzando una scala da 0 a 10 attribuita a vulnerabilità intrinseche del software:

  0 = Nessuna minaccia;
  1 - 3,9 = Basso;
  4 - 6.8 = Medio;
  7 - 8.9 = Alto;
  9 - 10 = Critico.

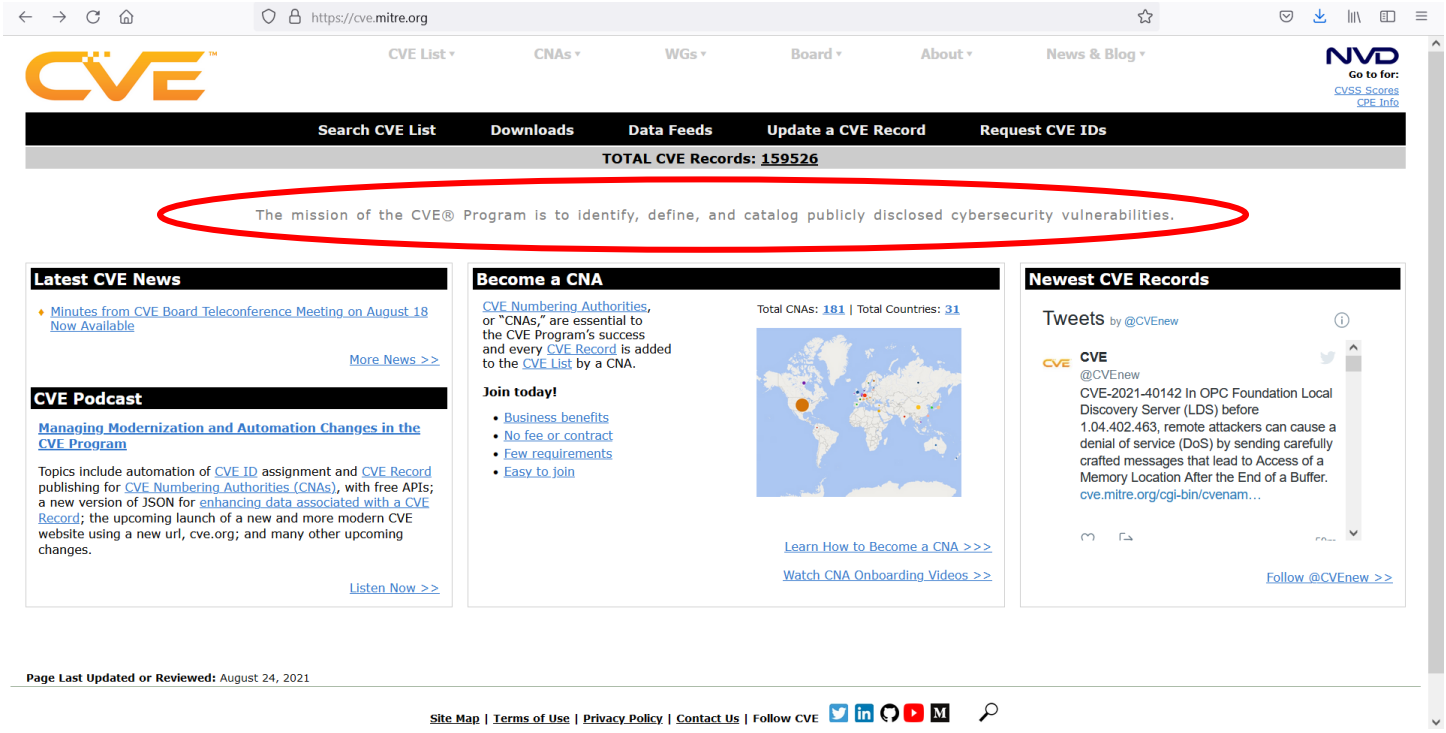
Rating	CVSS Score
None	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

Come si misura la gravità di una vulnerabilità?

- Il punteggio di base CVSS è composto da due gruppi di metriche:
  - Exploitability (sfruttabilità): riflette la facilità e i mezzi tecnici con cui la vulnerabilità può essere sfruttata (Da dove si riesce a sfruttare? Quanto è semplice metterla in atto?)
  - Impact (impatto): riflette le conseguenze di uno sfruttamento riuscito dell'exploit (Cosa permette di ottenere?).

CVE - Common Vulnerabilities and Exposures

- In ambito IT, il rischio deriva dalle potenziali perdite o danni causati dalle minacce che sfruttano le vulnerabilità dell'hardware o del software.



In sintesi…

Tutte le organizzazioni devono affrontare tre sfide principali:

- la *comprensione delle minacce* alla sicurezza;
- la promozione della *cultura* cyber;
- la *gestione dei rischi* per la sicurezza informatica, lavorando anche sul **fattore umano**.

In sintesi…

Di seguito, qualche buona pratica tratta dalle raccomandazioni e linee guida

- Fare sempre dei backup **sicuri** dei dati
- Non cliccare *link* o scaricare *allegati* sospetti
- Disabilitare le *macro* di Office e non usare versioni vecchie di Office
- Aggiornare gli antivirus e i sistemi operativi ogni giorno
- Utilizzare password **complesse** e ogni volta **diverse**
- Evitare reti *WiFi non protette*
- Essere sempre **sospettosi** e ricordarsi che ci sono istituzioni per il supporto nella prevenzione e in caso di incidente

GDPR

Il Regolamento Europeo UE 2016/679 in materia di protezione dei dati personali (GDPR, General Data Protection Regulation) ha come oggetto la «tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati» (art. 1, par. 1) e disciplina i trattamenti di dati personali, sia nel settore privato che nel **settore pubblico**

Il GDPR, tra le altre cose, mira ad adeguare il livello di protezione dei dati all'evoluzione degli strumenti utilizzati in una PA digitale

GDPR

Il GDPR pone l'accento sulla responsabilizzazione (*accountability*) dei titolari e dei responsabili dei trattamenti. Questi devono adottare comportamenti proattivi e dimostrare di implementare misure per assicurare l'attuazione del regolamento

Uno dei concetti fondamentali introdotto con il GDPR è quello della cosiddetta data protection by default and by design, e cioè del mettere in atto tutte le misure necessarie per soddisfare i requisiti del regolamento e tutelare i diritti degli interessati fin dall'inizio della configurazione del trattamento

Questo richiede che i titolari del trattamento facciano un'analisi preventiva e si impegnino a portare avanti una serie di attività specifiche e dimostrabili

GDPR – Articolo 25

Articolo 25 – Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita

«Tenendo conto dello **stato dell'arte** e dei **costi di attuazione**, nonché della **natura**, **dell'ambito di applicazione, del contesto e delle finalità del trattamento**, come anche dei **rischi** aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto **misure tecniche e organizzative adeguate**, quali la *pseudonimizzazione*, volte ad attuare in modo efficace i principi di protezione dei dati, quali la *minimizzazione*, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati. […]»

GDPR – Articolo 32

Articolo 32 - Sicurezza del trattamento

«1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un **livello di sicurezza adeguato al rischio**, che comprendono, tra le altre, se del caso: a) la *pseudonimizzazione* e la *cifratura* dei dati personali; b) la capacità di assicurare su base permanente la *riservatezza, l'integrità, la disponibilità e la resilienza* dei sistemi e dei servizi di trattamento; c) la capacità di *ripristinare tempestivamente la disponibilità e l'accesso dei dati* personali in caso di incidente fisico o tecnico; d) una procedura per *testare, verificare e valutare regolarmente l'efficacia* delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati. […]”

Analisi del rischio

Il GDPR richiede quindi che tutte le organizzazioni performino una valutazione e un'analisi dei rischi

Il GDPR, infatti, ha un approccio basato sulla valutazione del rischio. Quindi, al fine di implementare misure di sicurezza adeguate, le organizzazioni devono implementare una *corretta analisi dei rischi* del trattamento dei dati. Per ogni rischio occorre individuare la *probabilità* di accadimento dell'evento, e la *gravità* conseguente all'accadimento dello stesso, in modo da stabilire le misure di sicurezza adeguate per mitigare il rischio.

Best practices per il trattamento dei dati personali

È difficile però capire quali misure di sicurezza siano **adeguate** al contesto in esame

Nell'allegato 4 delle «*Linee guida per lo sviluppo del software sicuro*», l'AgID fornisce delle «*Linee guida per la modellazione delle minacce ed individuazione delle azioni di mitigazione conformi ai principi del secure/privacy by design*»

In particolare, nella sezione 4.5.2 dell'allegato sono presenti una serie di «Best practices per il trattamento dei dati personali»

Best practices per il trattamento dei dati personali

1. Ridurre al minimo i dati personali utilizzati - Ridurre l'impatto dei rischi limitando la gestione di dati personali a ciò che è strettamente necessario per raggiungere lo scopo definito.
2. Gestire i periodi di conservazione dei dati personali - Ridurre l'impatto dei rischi assicurando che i dati personali non vengano mantenuti per più di quanto necessario.
3. Informare i soggetti e ottenere il consenso - Consentire ai soggetti interessati di effettuare una scelta libera, specifica e informata.
4. Partizionare i dati personali - Ridurre la possibilità che i dati personali possano essere correlati e che possa verificarsi una violazione di tutti i dati personali.
5. Cifrare i dati personali - Rendere incomprensibili i dati personali a chiunque senza autorizzazione di accesso.
6. Anonimizzare i dati personali - Eliminare le caratteristiche che identificano i dati personali.