MATERIALE WEBINAR **16 SETTEMBRE** 2025

IL NUOVO VOLTO DELLA CYBERSECURITY:

Dati, attaccanti e risposte efficaci per le aziende.

L'evoluzione delle minacce informatiche: modelli, dinamiche e impatti

Gianluca Dini

Dipartimento di Ingegneria dell'Informazione, Università di Pisa

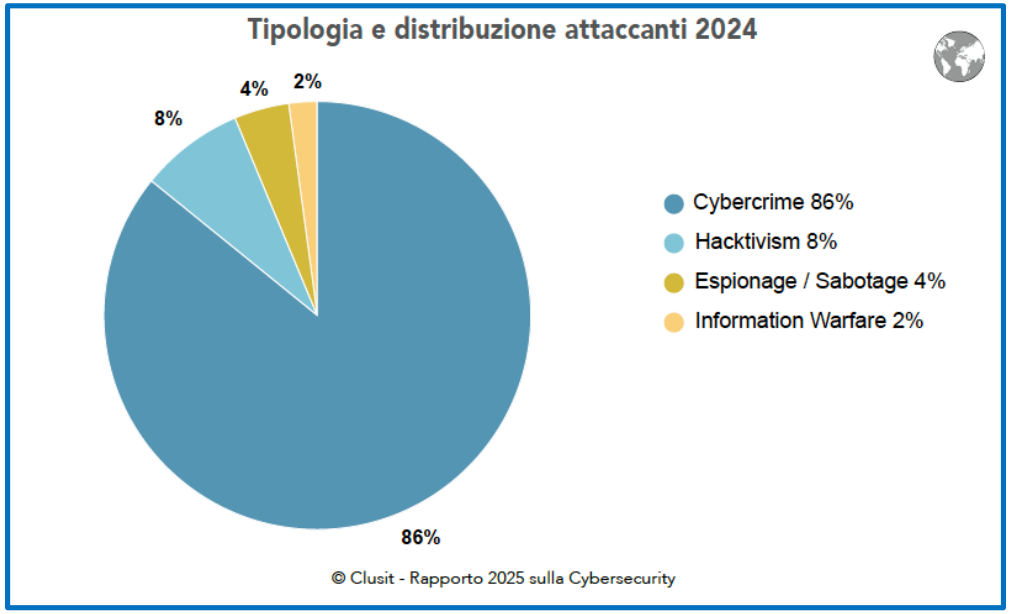
Email: gianluca.dini@unipi.it

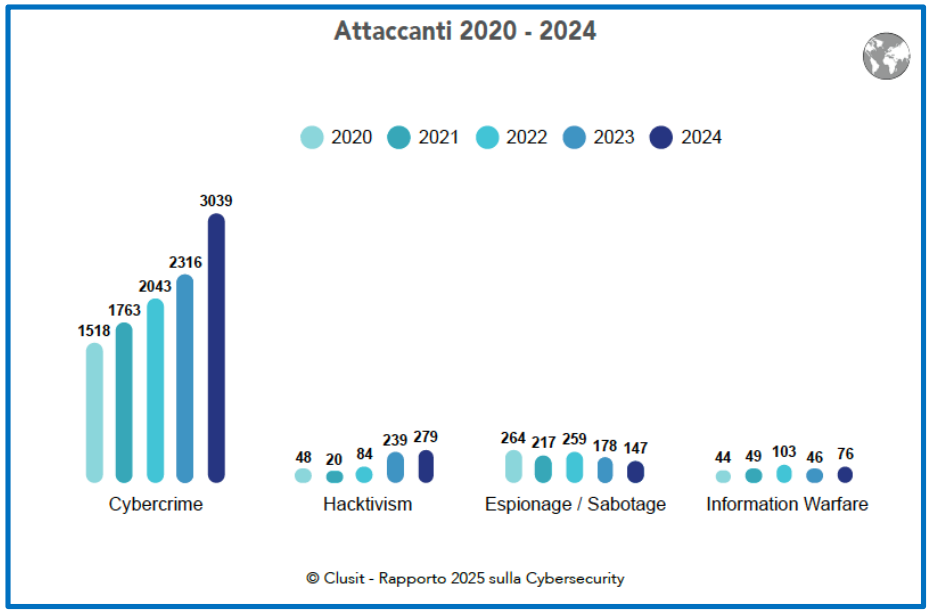
DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

Il rapporto Clusit

Incidenti per anno

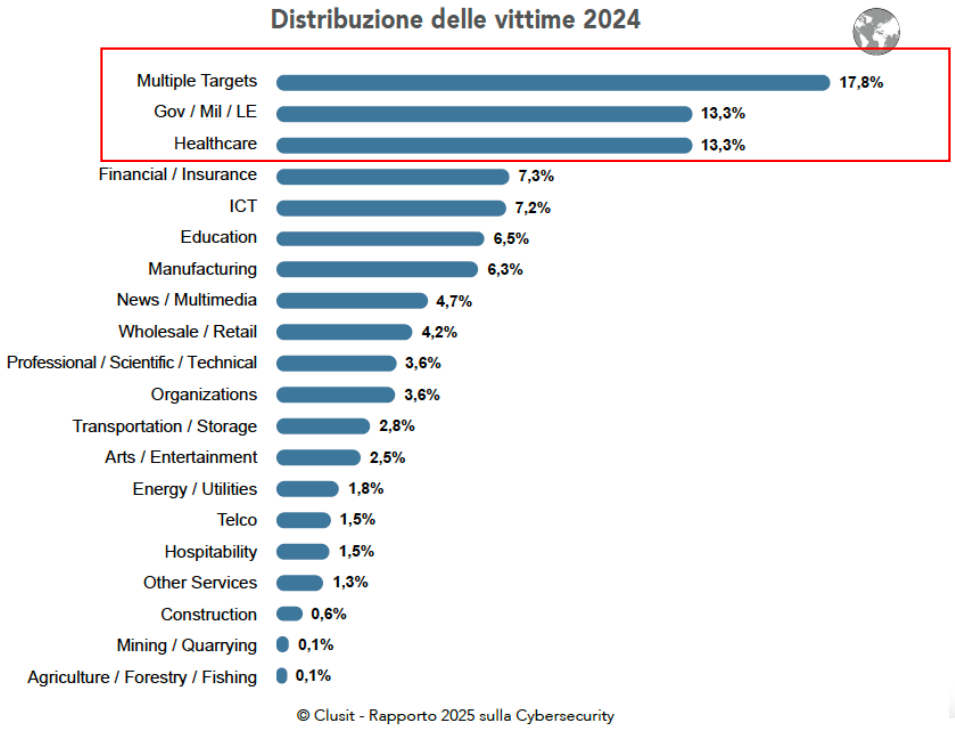
Chi sono gli attaccanti?

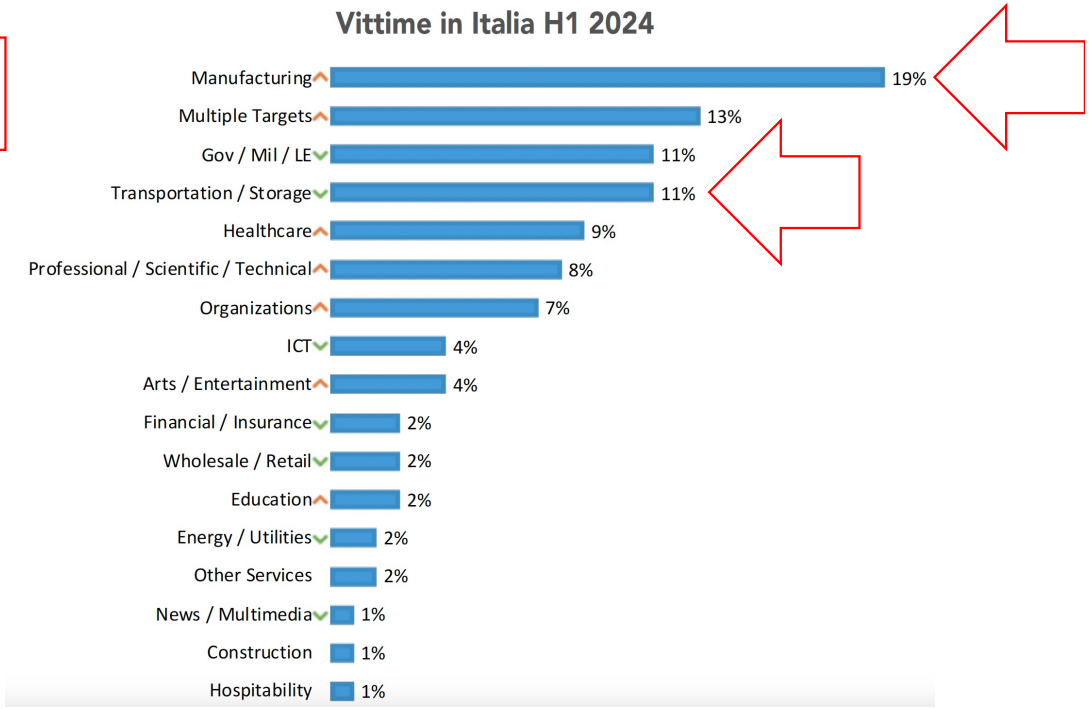




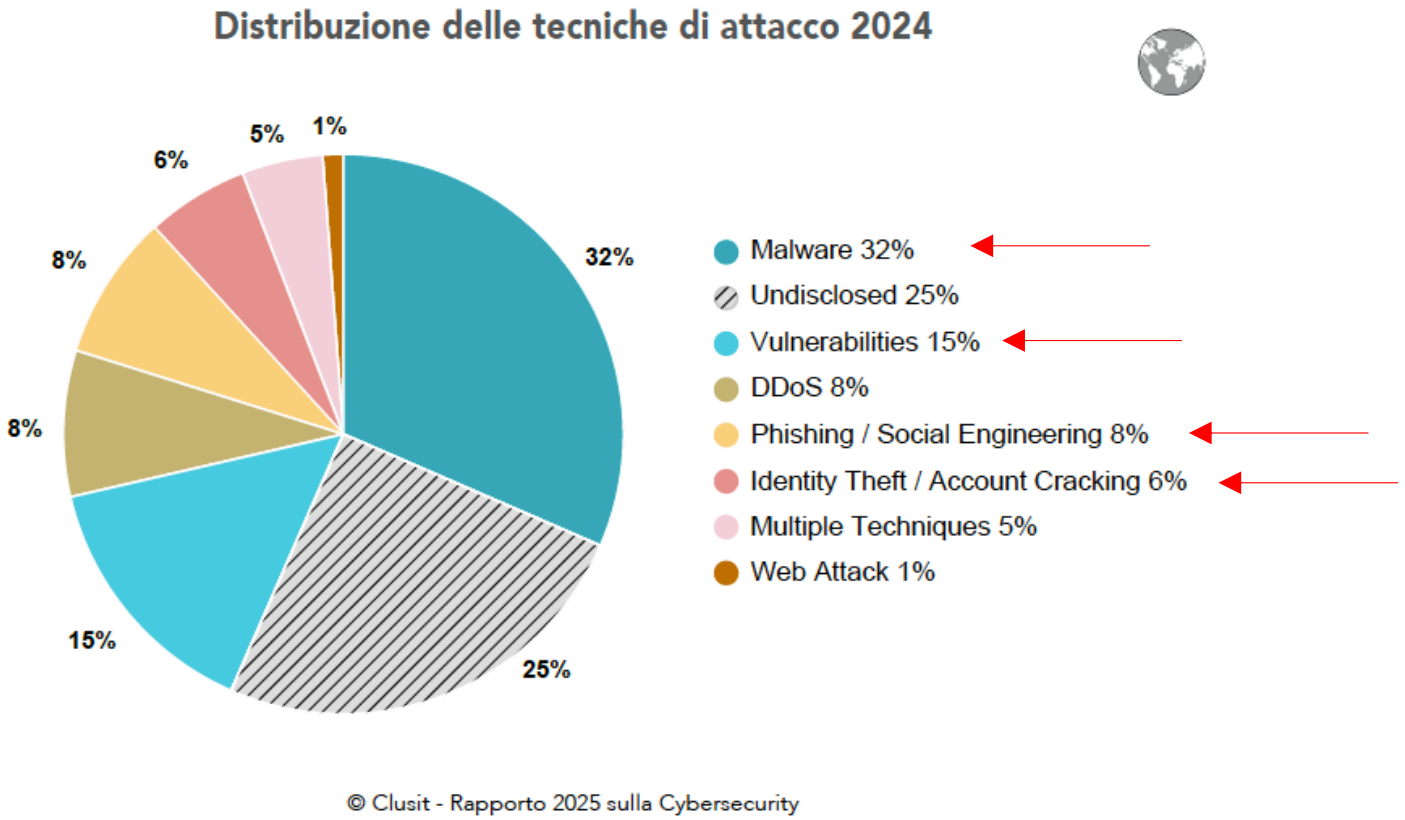
Si sta affermando il modello Attack-as-a-Service

Chi sono le vittime





Le tecniche di attacco [1/2]



Le tecniche di attacco [2/2]

- **60+%** degli attacchi sono riconducibili ad **azioni** “**maldestre**” degli utenti
  - Non sappiamo gestire le password
  - Non aggiorniamo i software
  - Clicchiamo incautamente sulle «cose» sbagliate

Una vulnerabilità ineliminabile: Dave!

- **Informazione e formazione del personale**
- **Policy aziendali chiare e formalizzate**

"Companies spend millions of dollars on firewalls, encryption, and secure access devices and it is money wasted because none of

***weakest link in the security chain**: **the people** who use, administer,*

information…"

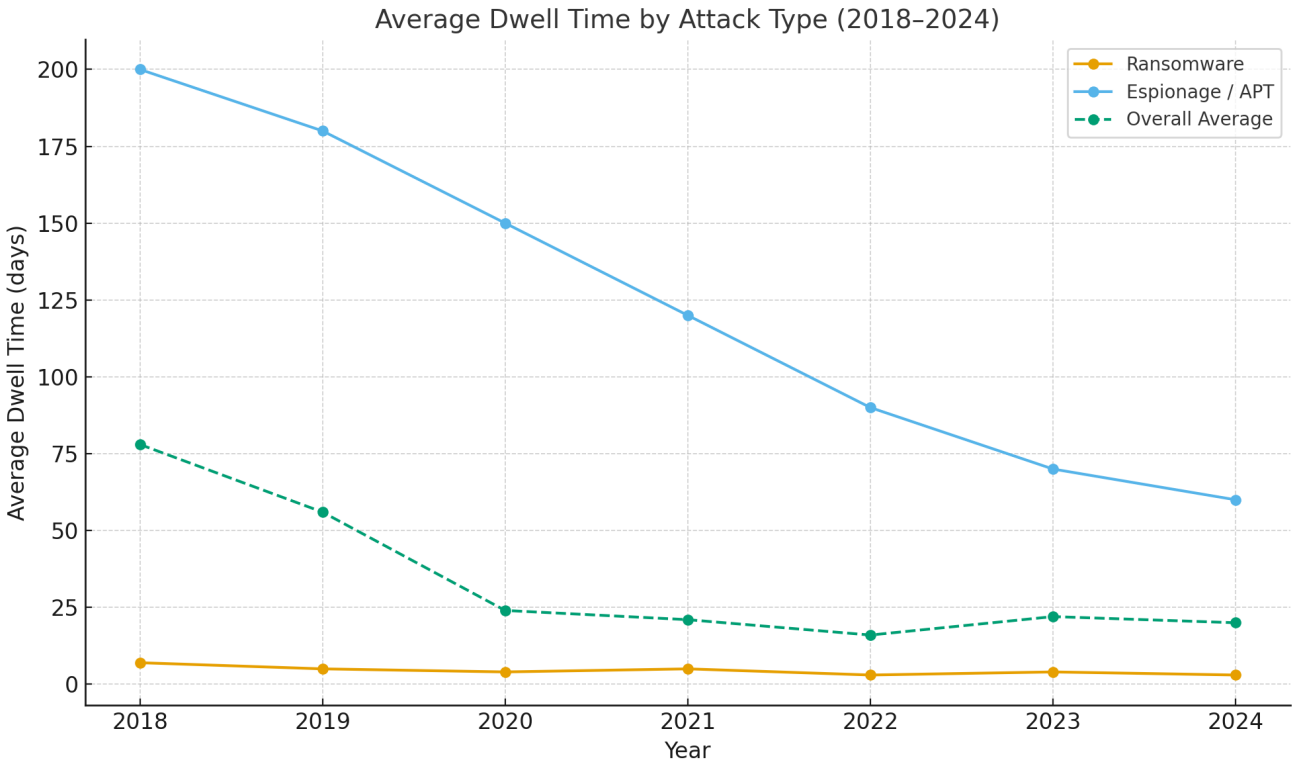
- Kevin Mitnick, March 2, 2000, U.S. Senate Committee on Governmental Affairs

Una vulnerabilità ineliminabile : il software

Una vulnerabilità: il software

Crescita record dell'exploitation	• 768 vulnerabilità note sfruttate attivamente nel 2024 (rispetto alle 639 del 2023).
Patching lento	• Oltre il 60% delle vulnerabilità sfruttate rimane senza patch oltre le scadenze di correzione.
Obiettivi critici	• La maggior parte dei CVE sfruttati ha 2 anni o meno; molti di quelli più sfruttati sono stati sfruttati per la prima volta come zero-day.
Impatto elevato	• Le vulnerabilità sfruttate sono la principale causa di ransomware e intrusioni, alimentate da ritardi nell'applicazione delle patch.

Dwell time (aka Mean Time to Detect, MTTD)



…e le PMI?

Se le Pmi sottovalutano i rischi connessi alla cyber security

La strada che porta le nostre Pmi verso la *cyber security* non è lunga, ma lunghissima, non difficile, ma difficilissima. I numeri non lasciano dubbi

di Alessandro Curioni

3 gennaio 2024

*"In buona sostanza **quello che si pensava fosse un problema di risorse è invece diventato culturale**: e purtroppo, in quanto tale, ha il difetto di appartenere alla categoria di quelli più difficili da risolvere."*

*"Lo scenario che si apre per il sistema delle Pmi italiane non è più soltanto quello di subire un attacco che le metta in ginocchio, ma anche la **concreta possibilità di trovarsi a scalare rapidamente e verso il basso le classifiche dei fornitori di grandi aziende e pubbliche amministrazioni di tutta Europa** che progressivamente dovranno introdurre proprio la cyber security come elemento qualificante dei propri partner."*

Linee guida di ACN per le PMI

- Integrazione della sicurezza digitale nella strategia d’impresa
- Importanza della formazione continua dei dipendenti
- La gestione degli incidenti e la business continuity
- Adozione di strumenti come autenticazione a più fattori (MFA), cifratura dei dati
- Backup sicuri e monitoraggio delle minacce
- Selezione di fornitori qualificati e l’utilizzo consapevole di servizi cloud SaaS
- Limitare i privilegi utente e adottare approcci come lo Zero Trust
- Nomina di un responsabile per la cybersicurezza

E la IA?

- Utilizzata per assistere o sostituire i lavoratori della conoscenza
  - Come i professionisti della sicurezza informatica ... o gli hacker
- Usata dai difensori
  - Anomaly detection, identificazione vettori di attacco, risposta ad un attacco
- Usata dagli attaccanti
  - Esposizione di dati sensibili, AI/data poisoning, Spear Phishing, Deep fakes
- IA introduce molti grandi vantaggi nelle organizzazioni ma
  - IA può essere attaccata
  - IA può essere usata per creare attacchi
  - IA può essere utilizzata per aiutare a difendere la tua organizzazione.
- Bisogna essere preparati a ciò che deve ancora venire...

Tanto per iniziare

- Controlli Essenziali di Cybersecurity, Laboratorio Nazionale di Cybersecurity
- Misure minime di sicurezza ICT per le pubbliche amministrazioni, AgID
- Guida pratica pr supportare le PMI nella protezione dai rischi informatici, ACN

Come vi possiamo aiutare

- Consulenza tecnica
- Trasferimento tecnologico
- Master di I livello in Cybersecurity
- Formazione ad-hoc

Gianluca Dini

- Professore Ordinario di Sistemi di Elaborazione
  - Dipartimento di Ingegneria dell'Informazione, Università di Pisa
- Contatti
  - Email: gianluca.dini@unipi.it
  - Linkedin: www.linkedin.com/in/gianlucadini
  - Tel.: +39 050 2217 549

Ercole Plez
Senior Sales Engineer @Sophos
September 2025

Panorama attuale delle minacce

SOPHOS

Categorie di Threat Actor

E-Crime Organizzato

Motivati dal profitto, cercano di monetizzare l'accesso e/o le informazioni rubate

Sponsorizzati da Stati

Spionaggio tradizionale che si è spostato nel dominio cyber, campagne di disinformazione, attacchi distruttivi

Hacktivist

Motivati da problemi, con l'obiettivo di distrarre, esporre, mettere in imbarazzo o infliggere danni pubblici

Minacce interne

Implica il furto di IP / segreti commerciali, analisi della concorrenza e/o informazioni su potenziali clienti, clienti o mercati

Categorie di Threat Actor

MIRATO

Sponsorizzati da Stati

Spionaggio tradizionale che si è spostato nel dominio cyber, campagne di disinformazione, attacchi distruttivi

Hacktivist

Motivati da problemi, con l'obiettivo di distrarre, esporre, mettere in imbarazzo o infliggere danni pubblici

Risultati e impatto

- Spesso nascosto o non evidente all'inizio
- Impatto strategico a lungo termine sulla sicurezza
- Furto di proprietà intellettuale
- Implicazioni internazionali e politiche
- Acquisiscono informazioni e capacità per azioni distruttive e dirompenti
- DDoS – Negano accesso a servizi
- Futuro economico/finanziario – i clienti perdono fiducia

Categorie di Threat Actor

OPPORTUNISTICO

E-Crime Organizzato

Motivati dal profitto, che cercano di monetizzare l'accesso e/o le informazioni rubate

Risultati e impatto

- Ransomware
- Estorsione
- Compromissione della posta elettronica
- Frode del CEO

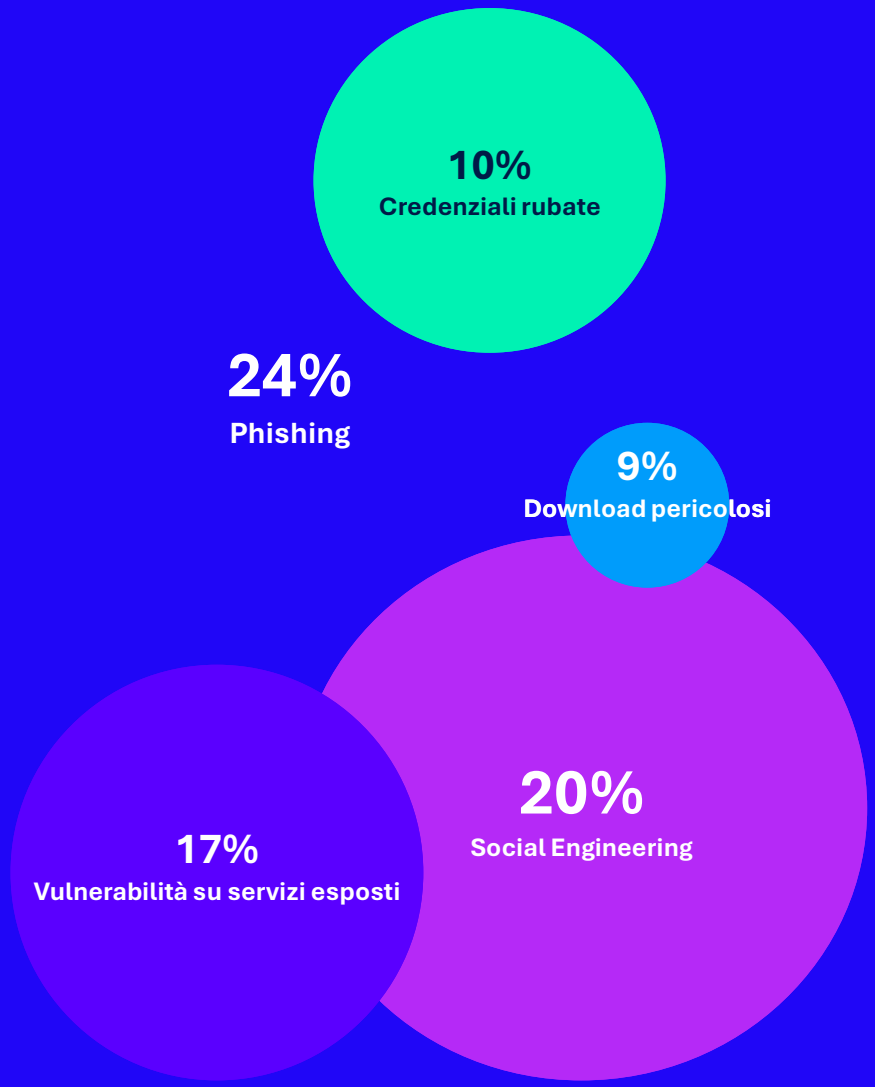
Porta a:

- Perdita finanziaria
- Interruzione operativa
- Futuro economico/finanziario – i clienti perdono fiducia

GLI ATTACCHI HANNO CONSEGUENZE ANCHE SE NON HANNO SUCCESSO AL 100%

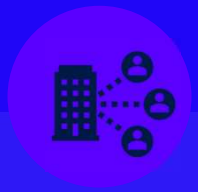
Opportunity

In che modo gli attori delle minacce entrano in gioco?



SOPHOS

Principali metodi di accesso per ransomware

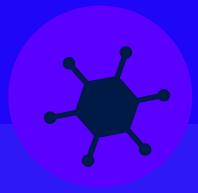


Abuso di credenziali

- VPN senza MFA
- Credenziali rubate (da dump di dati/violazioni precedenti/phishing/infostealer) o indovinate (tramite attacchi di forza bruta)
- Ingegneria sociale

Exploitation di Servizi Remoti

- Gli exploit usati contro firewall/VPN, Exchange, SharePoint sono molto popolari
- Qualsiasi vulnerabilità di connessione Internet che consenta l'esecuzione di codice in modalità remota sarà probabilmente altrettanto diffusa



Commodity Malware

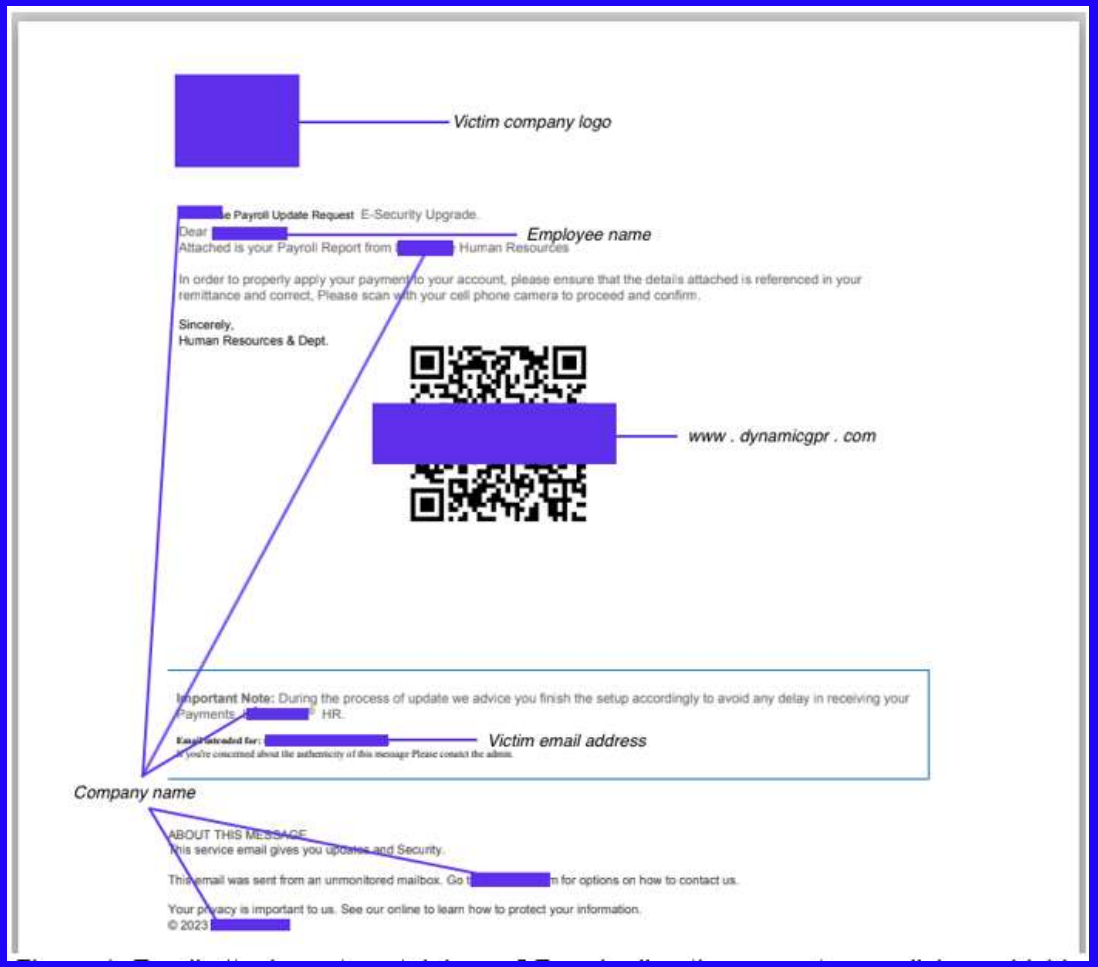
- Gli operatori di botnet ottengono e vendono l'accesso
- Loaders consegnati con campagne di phishing
- Download drive-by tramite avvelenamento SEO/Google Ads

Manipolazione dei comportamenti appresi

SOPHOS

QR Code Phishing

- Aumento dei volumi
- Ignora il filtro della posta
- Il phishing avviene sul dispositivo dell'utente, al di fuori dei controlli aziendali
- Può acquisire token MFA
- Può portare all'accesso all'account Azure e a frodi in stile BEC

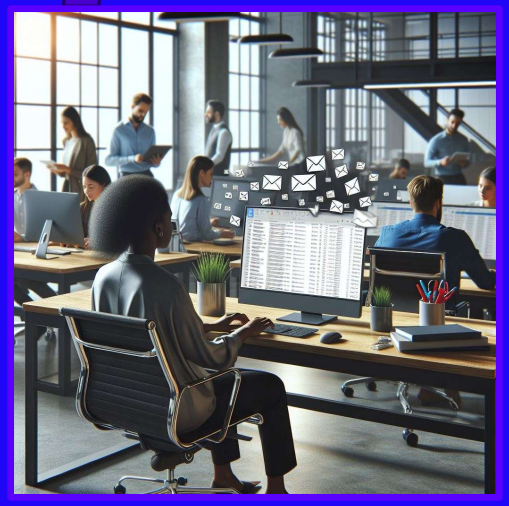


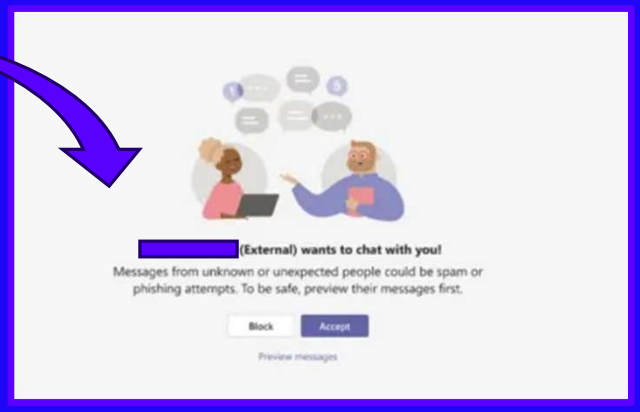
Spamming + Teams chat social engineering

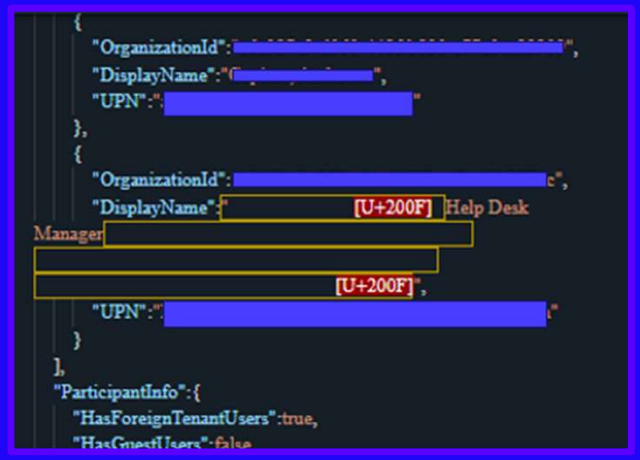
GOLD REBELLION invia spam alle organizzazioni tramite e-mail.

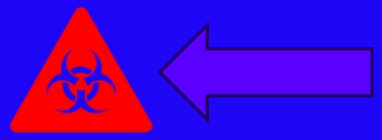
Quindi fingendosi operatori dell'help desk IT installano strumenti di accesso remoto sui computer delle vittime.

Questo rappresenta un'altra tecnica innovativa utilizzata da GOLD REBELLION nei suoi attacchi ransomware Black Basta.









SOPHOS

Attacchi Fake Verification

Profilo di attacco

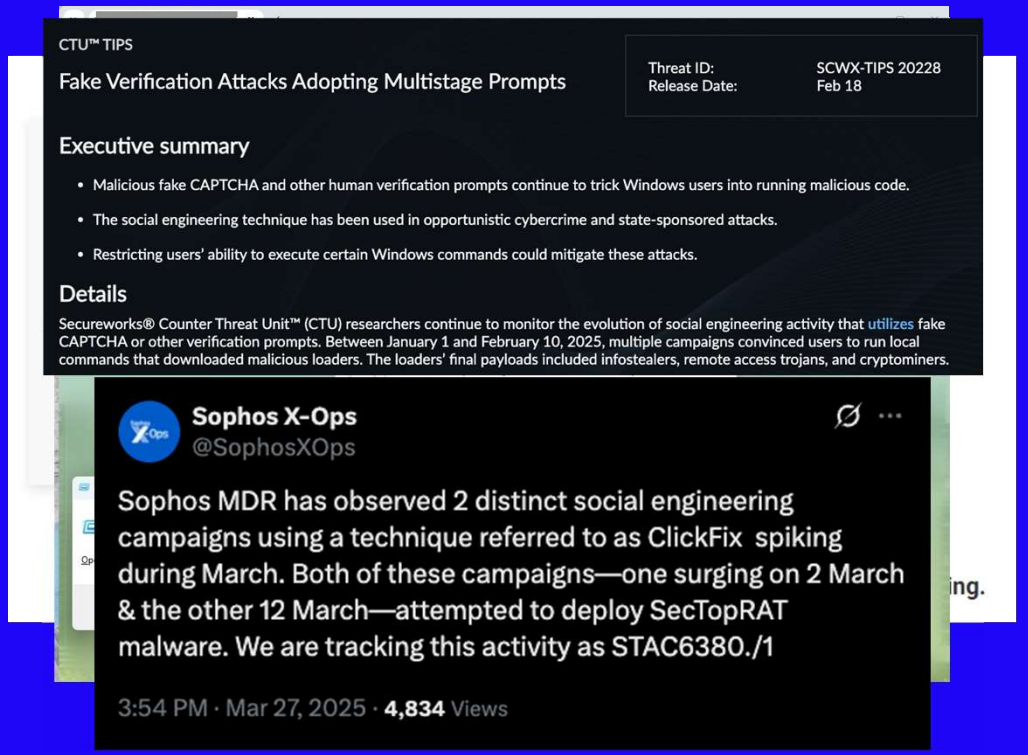
L'utente visita i siti WordPress infetti

Fa clic su Fix/Prompt "Non sono un robot"; Più fasi possibil*

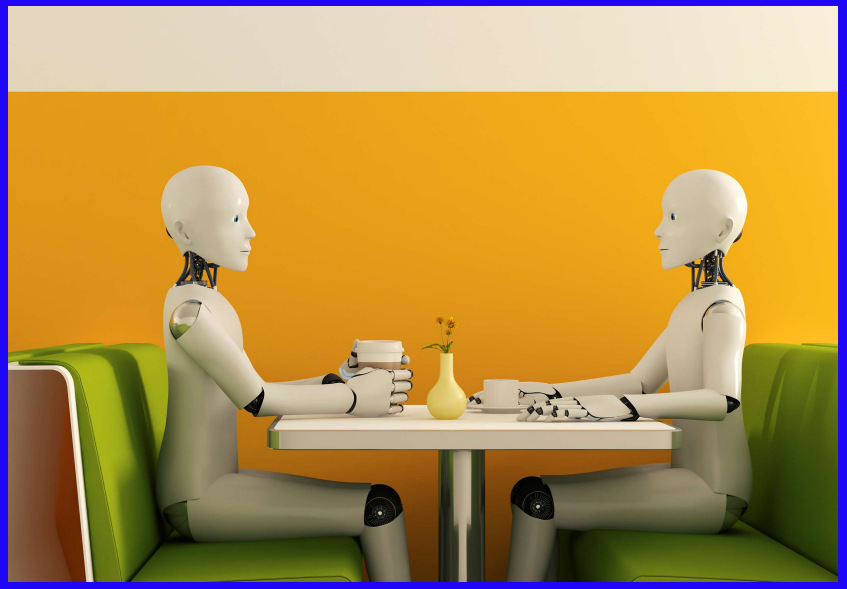
La vittima apre l'utility «Esegui», incolla gli appunti, esegue il comando avviando l'infezione

Seguono infostealer o altri malware

Impiegato da Threat Actor del e-Crime Organizzato o sponsorizzati da stati



Schemi fraudolenti per i lavoratori IT nordcoreani: dalle minacce interne all'estorsione



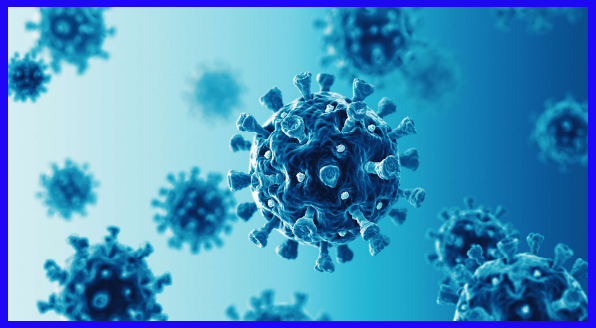
I criminali prendono di mira le persone perché **le organizzazioni sono incentrate sulle persone**

"Nella sicurezza informatica, **le persone** sono la linea di difesa più intelligente"

Il reclutamento di talenti è un obiettivo facile

Tre campagne rivolte alle risorse umane e alle persone in cerca di lavoro: sfumail confine tra APT e criminalità informatica

Lavoratori remoti fraudolenti



Interviste contagiose

Assunzioni di Trojan

Intelligenza incorporata....

Sophos X-Ops

Task force congiunta per la risposta avanzata alle minacce

Un approccio multidimensionale per contrastare le moderne minacce informatiche

SOPHOS

Perché Sophos Threat Intelligence è essenziale

X-Ops è un elemento di differenziazione

Forniamo l'intero ciclo di intelligence sulle minacce in tutto il portafoglio Sophos. La nostra intelligence fruibile alimenta un processo continuo di protezione, rilevamento, analisi e risposta, aiutandoti a rafforzare ed evolvere la tua posizione di sicurezza ogni giorno.

SOPHOS


SOPHOS
DEFEAT CYBERATTACKS

hi solution
better ICT for every business

Misurare il rischio, guidare l'azione con l'AI

Luca Salvatori
Product Manager, HiSolution

LUCART SHARING THE FUTURE · PORTOBELLO · Club del Sole FULL LIFE HOLIDAYS · SAPIENZA UNIVERSITÀ DI ROMA · hiop MILANO · AZIMUT | BENETTI · Sant'Anna Scuola Universitaria Superiore Pisa

I dati in Italia

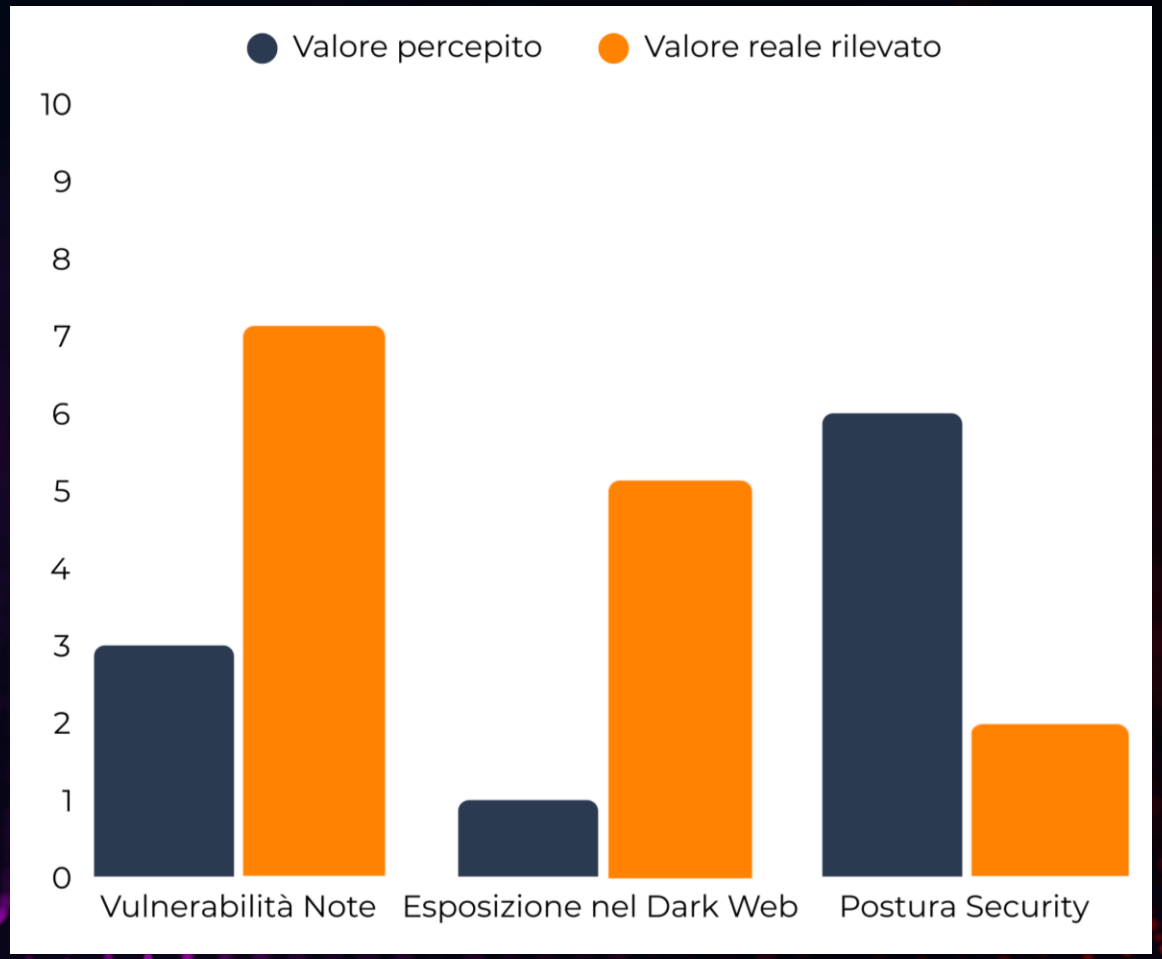
- L’Italia è il terzo paese al mondo per attacchi malware
- È il paese più colpito in Europa
- Il 91% degli attacchi malware avviene al di fuori dell’orario di lavoro

Fonte Clusit

HISOLUTION

Perché misurare il rischio

Per passare dalla percezione soggettiva a una valutazione oggettiva.



HISOLUTION

Dal rischio all’azione concreta

Per avere un indice accurato e dinamico che offra la fotografia della situazione: superfici esposte, vulnerabilità note, dati compromessi, postura di sicurezza.

HISOLUTION

Dal dato al piano di remediation

Il valore non è solo misurare, ma indicare la strada per ridurre il rischio.

- I piani di remediation danno al management: **priorità definite**, **ownership chiara**, **visione** dell'impatto delle azioni.
- **Vantaggi:** **maggiore resilienza** + possibilità di dimostrare **solidità** anche in ottica finanziaria e di compliance.
- **Output:** un **indice chiaro e confrontabile**, report e piani di remediation concreti.

Conformità NIS2 • Gestione Cyber Risk • Monitoraggio 24/7

HiCompliance:
Piattaforma integrata di Cyber Risk Management

HiCompliance offre una soluzione completa per la gestione del rischio cyber, la conformità alle direttive e alle best practices di settore e il monitoraggio continuo della sicurezza aziendale.

Inizia Ora →

Scopri di Più

500+
Conformità NIST/NIS2/ISO

100%
Conformità NIST/NIS2/ISO

99.9%
Conformità NIST/NIS2/ISO

63%
Conformità NIST/NIS2/ISO

HISOLUTION

-65% del rischio in 3 mesi senza stravolgimenti tecnologici!

"*Con HiCompliance® abbiamo ridotto il nostro rischio cyber del 65% in soli 3 mesi. Un investimento che si è ripagato immediatamente.*"
- CIO, Azienda Manifatturiera

"*Finalmente possiamo dimostrare al CdA l'efficacia dei nostri investimenti in sicurezza con metriche oggettive.*"
- CISO, Società di Servizi

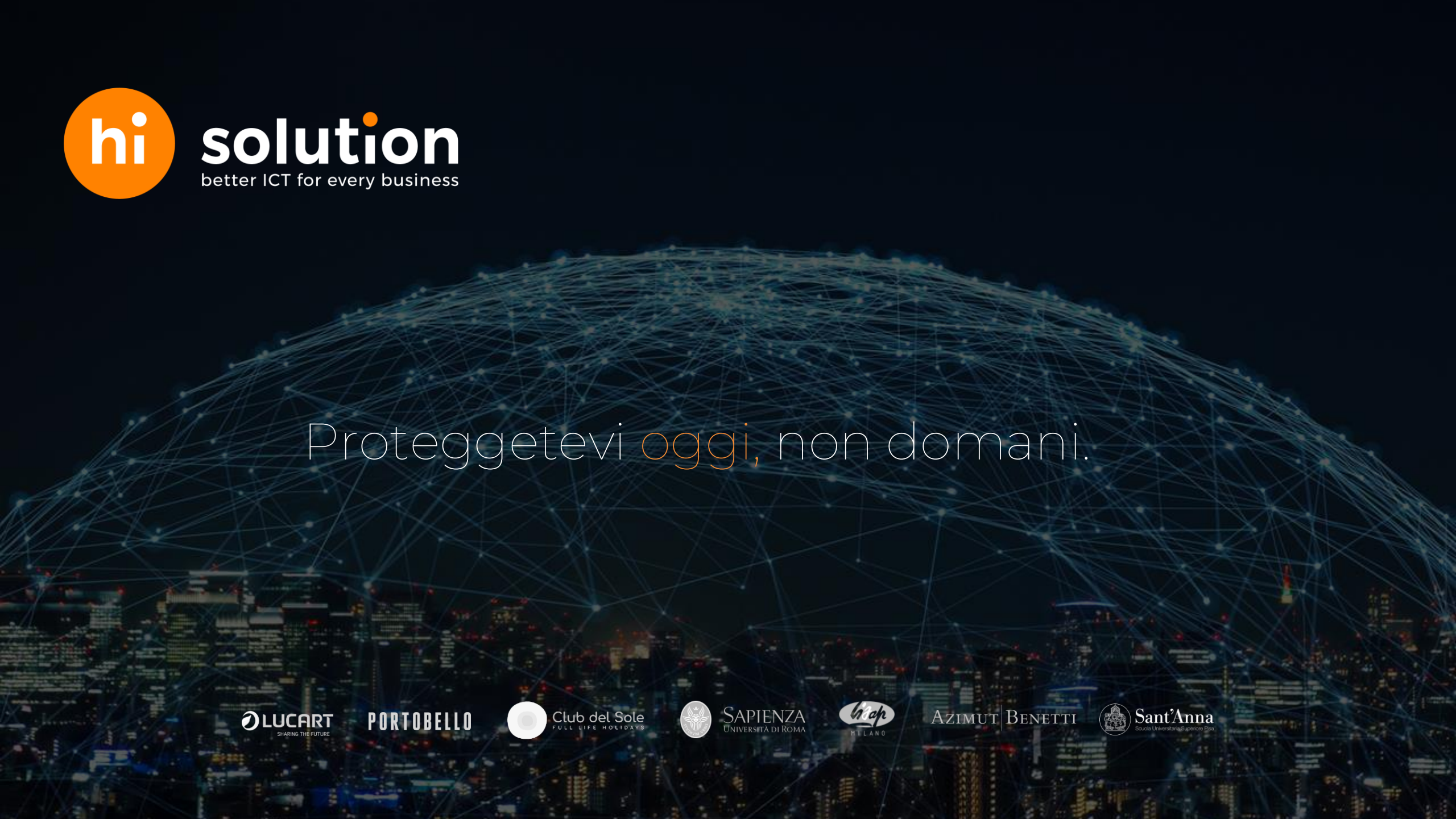
"*Il report HiCompliance® ha convinto il nostro CFO ad approvare un budget per la sicurezza che chiedevamo da anni.*"
- IT MANAGER, Azienda Food&Beverage

HISOLUTION

Oltre l’assessment, dentro l’azienda.

- Non è un tool, ma un servizio gestito.
- Pronto in 72h.
- Pensato per realtà complesse e multisede.
- Scalabile su ogni settore.

	Assessment singolo	HiCompliance
Approccio	Statico	Continuativo
Personalizzazione	Limitata	Alta (per BU, per dominio)
Remediation supportata	No	Si, con Security Manager
Risultati	Report generico (tante pagine da leggere)	Dashboard (+piano operativo)


hi solution
better ICT for every business
Proteggetevi oggi, non domani.
LUCART
SHARING THE FUTURE
PORTOBELLO
Club del Sole
FULL LIFE HOLIDAYS
SAPIENZA
UNIVERSITÀ DI ROMA
hiap
MILANO
AZIMUT | BENETTI
Sant'Anna
Scuola Universitaria Superiore Pisa

HISOLUTION

HiCompliance e Incident Response Plan (IRP)

Che cos'è un IRP?
Guida operativa che definisce **procedure, ruoli e responsabilità** per la gestione degli incidenti di sicurezza.

Perché serve?

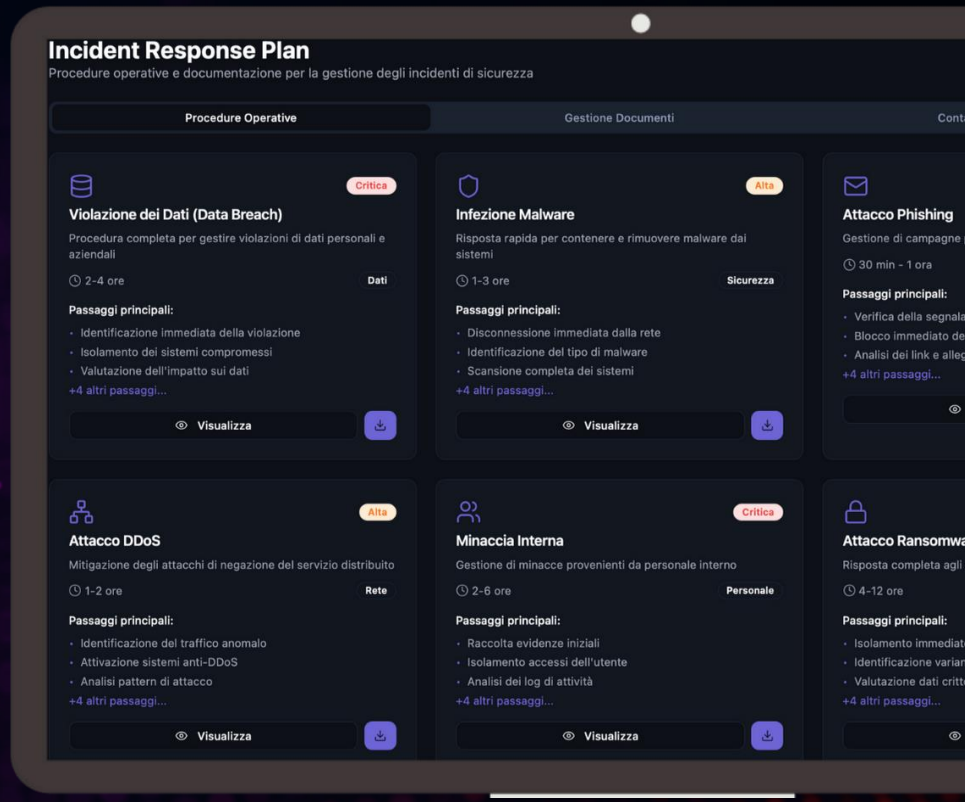
- Preparare l'organizzazione a gestire eventi critici
- Standardizzare azioni e responsabilità
- Ridurre impatto economico, operativo e reputazionale
- Garantire tracciabilità e compliance (NIS2, GDPR, ISO 27001)

HISOLUTION

HiCompliance e Incident Response Plan (IRP)

Per coloro che attivano HiCompliance, **regaliamo un Incident Response Plan** strutturato: uno strumento pronto all'uso per reagire rapidamente ad un attacco.

- Obiettivi e ambito del piano
- Ruoli e contatti
- Classificazione della gravità degli incidenti
- Flusso di gestione
- Linee guida per reporting e analisi post-incidente



Q&A

Grazie per l’attenzione!

Per domande, approfondimenti o qualsiasi necessità:
marketing@hisolution.it