Minacce Cyber nel settore sanitario: Sfide attuali e nuove frontiere per il futuro

Mario Garofano, CISO (Chief Information Security Officer) presso la Fondazione Policlinico Universitario Campus Bio-Medico

Luca Faramondi, Coordinatore Scientifico Master di I livello in Cybersecurity Management presso l'Università Campus Bio-Medico di Roma

Ministero delle Imprese e del Made in Italy
Dipartimento per il digitale, la connettività e le nuove tecnologie
Direzione Generale per il digitale e le telecomunicazioni - ISCTI

CYBER 4.0 CYBERSECURITY COMPETENCE CENTER

CYBER SHOT Lab
Cybersecurity laboratory for Systems, Health, and Operational Technologies

UNIVERSITÀ CAMPUS BIO-MEDICO DI ROMA

SSSTLC
Scuola Superiore di Specializzazione in Telecomunicazioni

Dall'analisi e classificazione dei **45 eventi cyber** rilevati nel periodo in esame (2022-2023) sono emerse le principali tipologie di minacce, dove si evince una sensibile predominanza del **ransomware**.

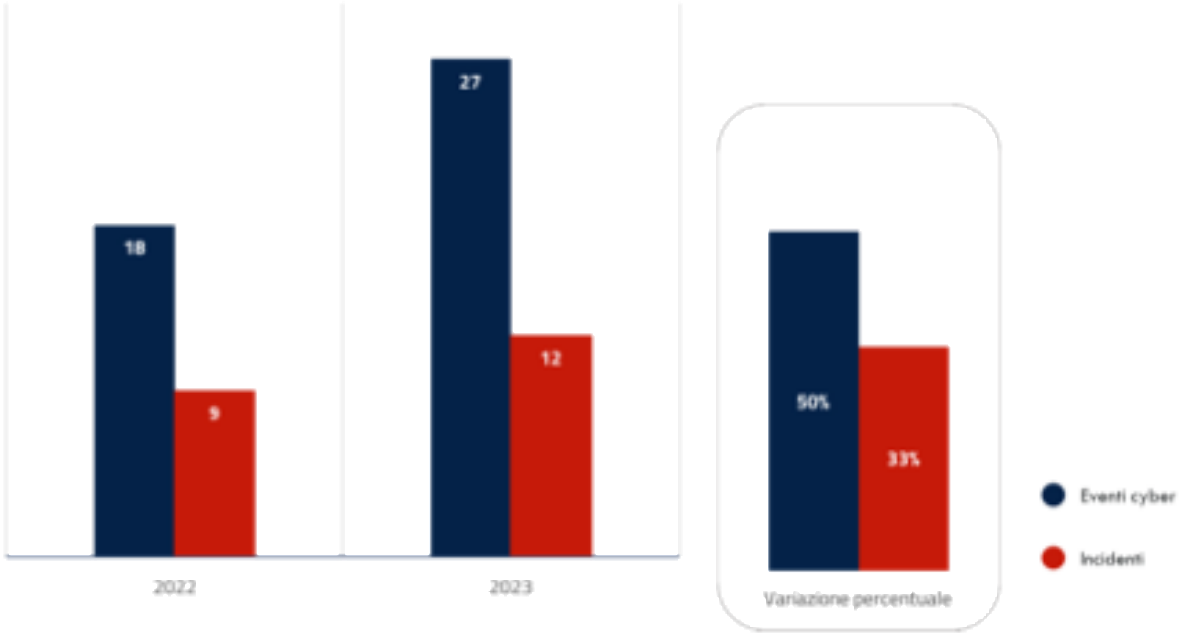
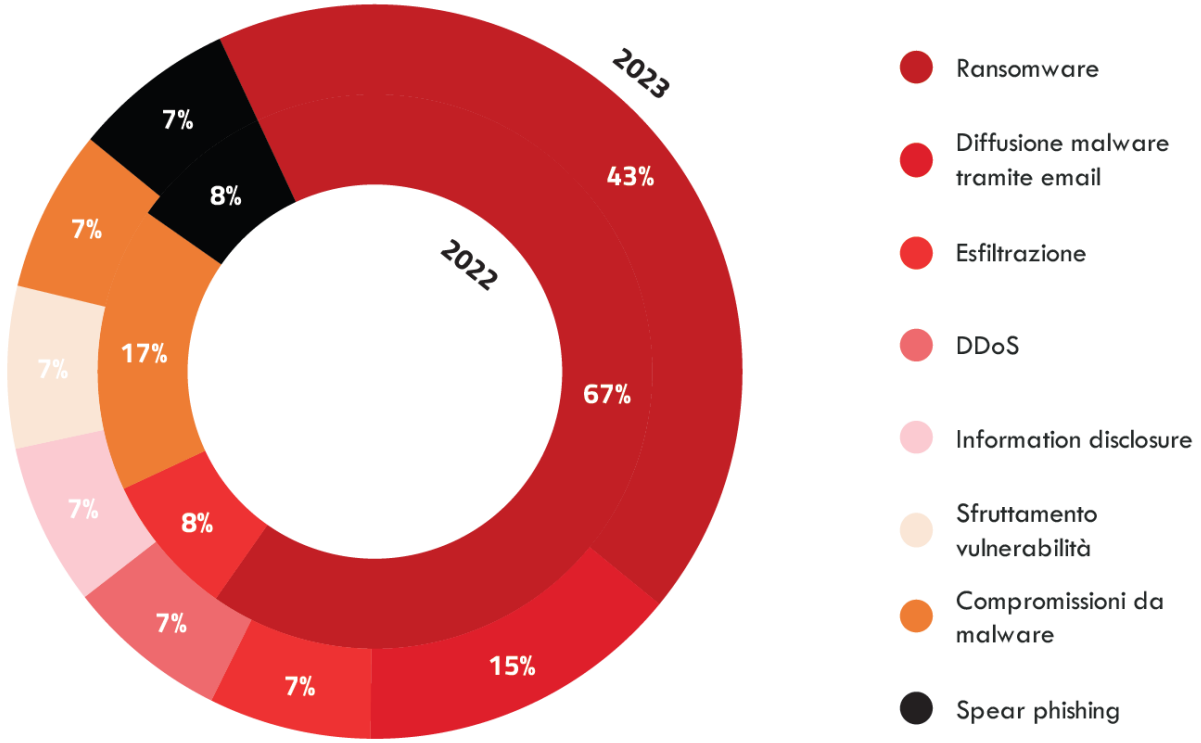


Figura 2: numero di eventi cyber e incidenti nel periodo 2022-2023 e loro variazione percentuale annua

- Gli attacchi **ransomware** risultano essere la minaccia cibernetica più diffusa per il settore, con il **35% degli eventi** nel 2023 e il **60% degli eventi** nel 2022;
- L'attività di **information disclosure** è stata rilevata nel **14% degli eventi** nel 2023;
- La **diffusione di malware tramite e-mail** è stata rilevata nell'**10% degli eventi** del 2023;
- Lo **sfruttamento di vulnerabilità** ha caratterizzato il **10% degli eventi** nel 2023 e il **13% degli eventi** nel 2022.

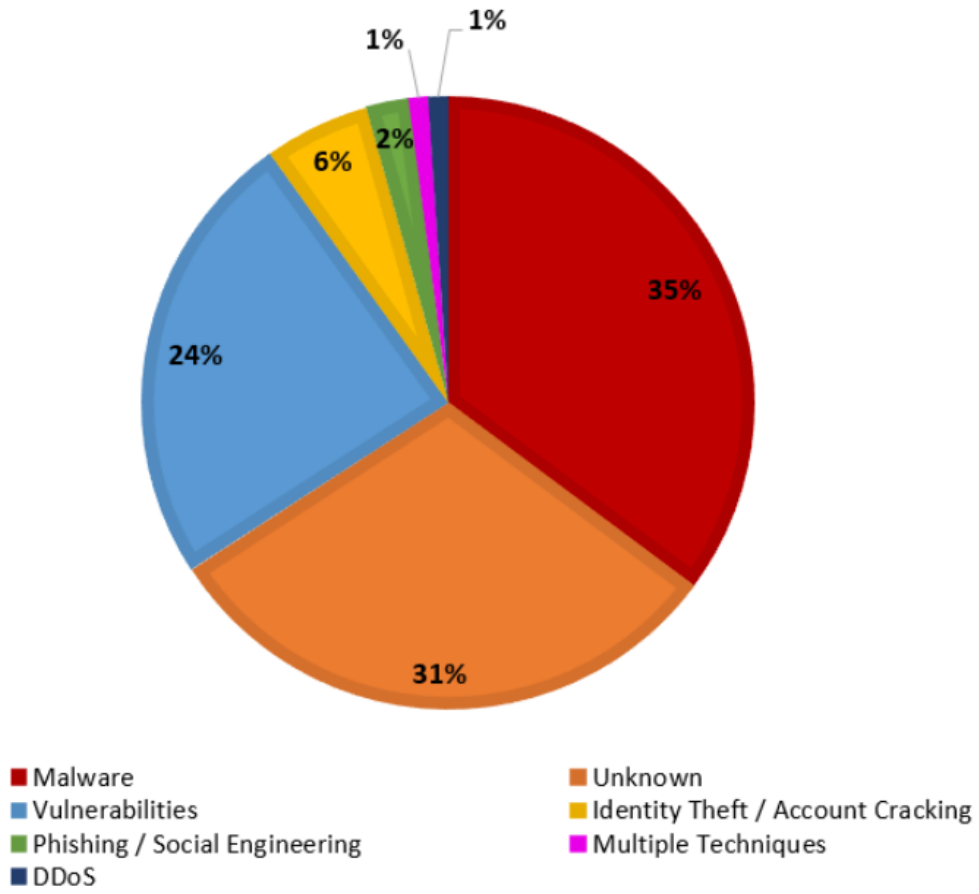
Fonte: «LA MINACCIA CIBERNETICA AL SETTORE SANITARIO Analisi e raccomandazioni Gennaio 2022 – Settembre 2022»



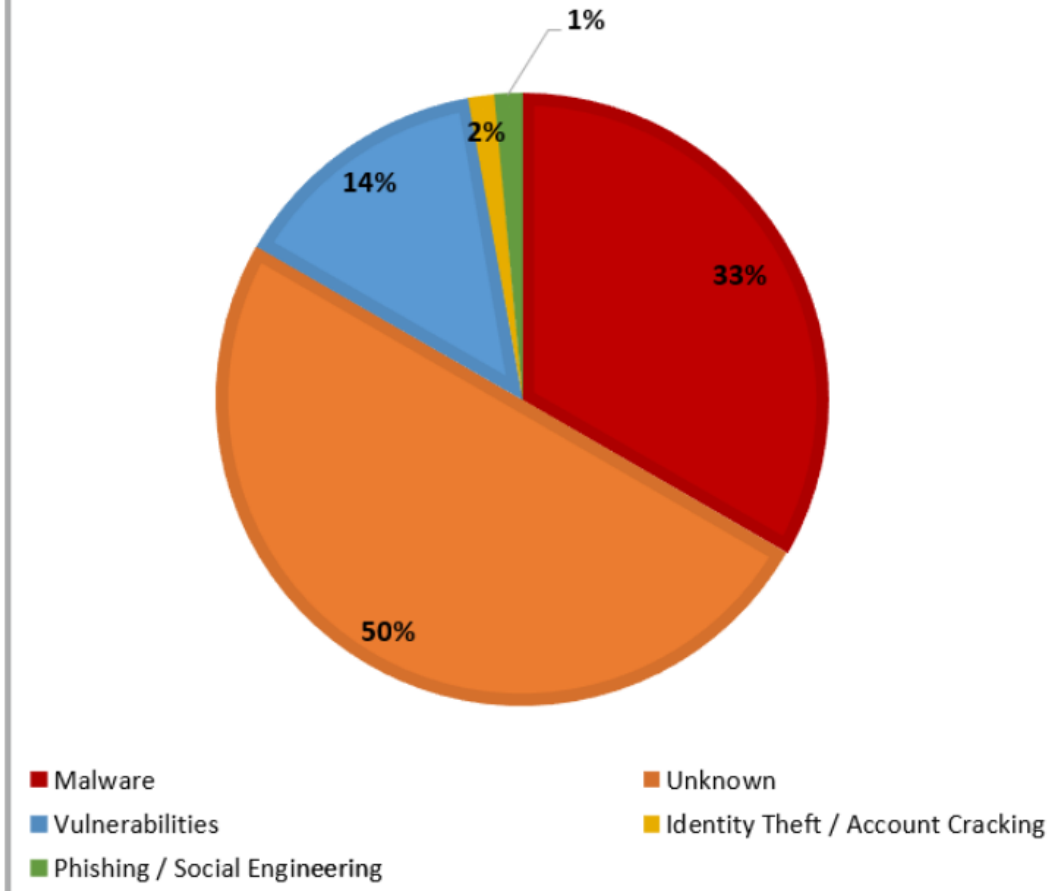
Queste tipologie di incidenti possono non solo interrompere i servizi e compromettere la **privacy dei pazienti**, ma anche mettere a rischio la sicurezza delle **informazioni mediche sensibili**. Inoltre, il potenziale danneggiamento della **reputazione** dell'istituzione sanitaria può avere ripercussioni a lungo termine sull'affidabilità e la fiducia da parte dei pazienti e degli stakeholder del settore sanitario.

Fonte: «LA MINACCIA CIBERNETICA AL SETTORE SANITARIO Analisi e raccomandazioni Gennaio 2022 – Settembre 2022»

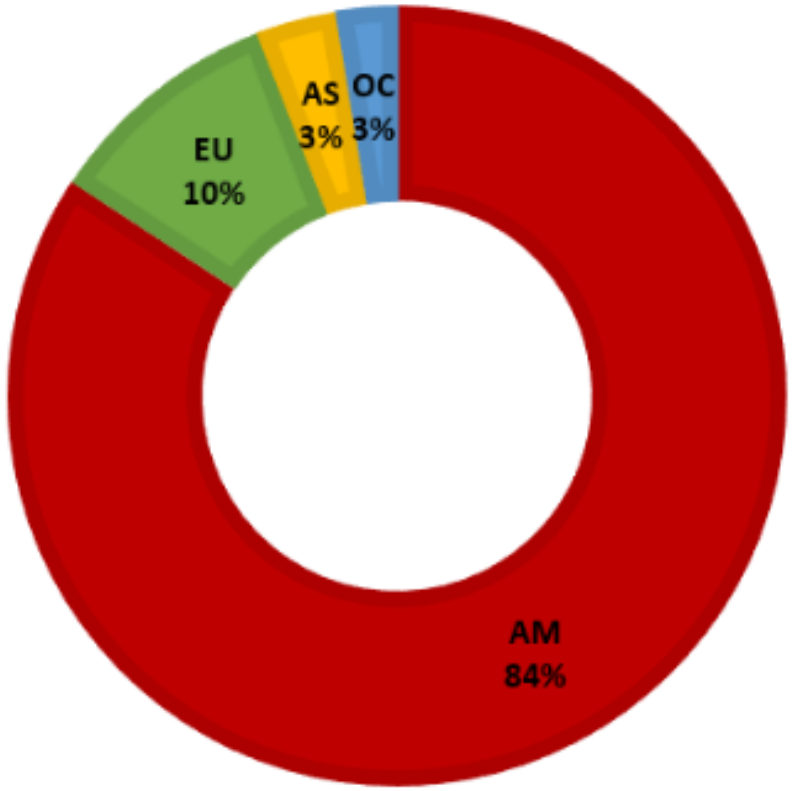
TECNICHE HEALTHCARE 2023



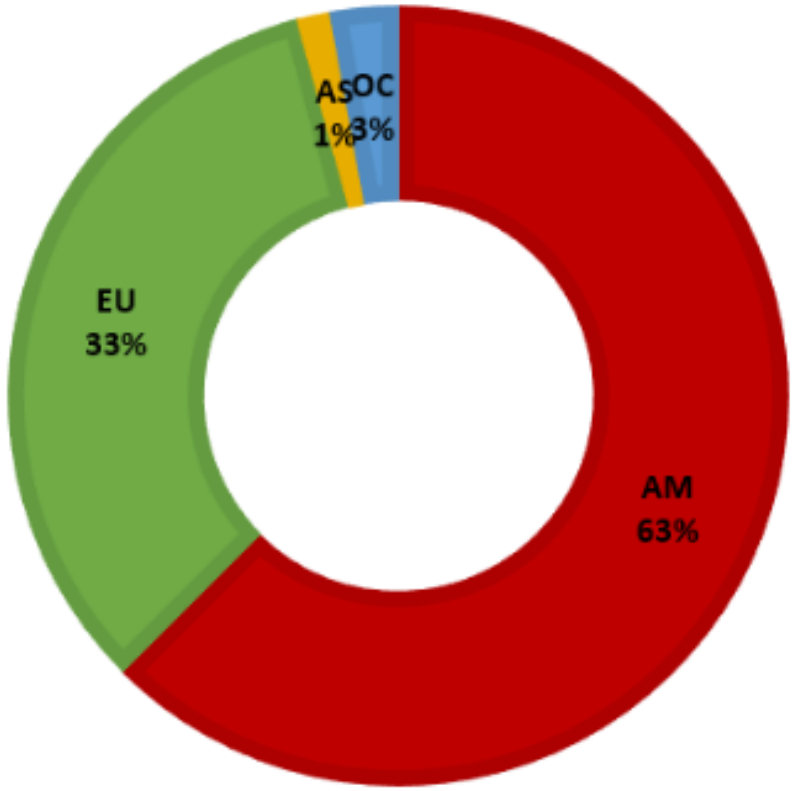
TECNICHE HEALTHCARE 1Q24



GEOGRAFIE VITTIME HEALTHCARE 2023



GEOGRAFIE VITTIME HEALTHCARE 1Q24



Data lookup

Web client
BETA

Desktop client

Store

Subscriptions

Referral program

Settings

source
- Collection 1

email [redacted]

password [redacted]
source
- Stealer Logs

email [redacted]

password [redacted]
source
- Zoosk.com

email [redacted]

password [redacted]
source
- MyHeritage.com

email [redacted]

password [redacted]
email [redacted]

password [redacted]
email [redacted]

password | Evidenzia | Maiuscole/minuscole | Segni diacritici | Parole intere | Corrispondenza 313 di 724

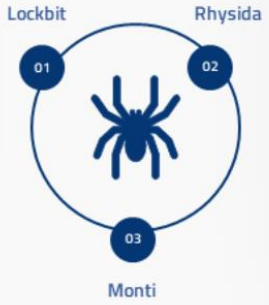
RANSOMWARE

Tipologia di minaccia che ha lo scopo di cifrare i dati del bene informatico target in modo da comprometterne la disponibilità e l'integrità. Inoltre, in questa tipologia di minaccia spesso l'attaccante crea dei file, detti ransom notes, tramite i quali viene richiesto alla vittima un riscatto in cambio dell'accesso ai propri dati.

PREDOMINANZA DEI CASI

42%
DEGLI EVENTI NEL BIENNIO 2022-23 SONO RANSOMWARE

TOP 3 RANSOMWARE GANGS



INFORMATION DISCLOSURE

Tipologia di minaccia cyber in cui è occorsa una violazione di sicurezza dei dati/informazioni personali o proprietarie. L'information disclousure, la cui natura può essere sia intenzionale sia accidentale, può avvenire mediante la divulgazione non autorizzata, la perdita, la modifica o la distruzione dei dati.

PREDOMINANZA DEI CASI

14%
DEGLI EVENTI HA CAUSATO UN INFORMATION DISCLOSURE

TOP 3 IMPACT

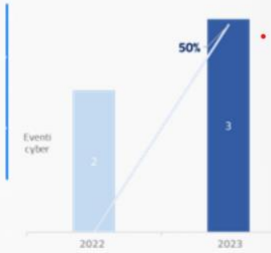
SFRUTTAMENTO VULNERABILITÀ

Gli attacchi attuati attraverso l'utilizzo degli errori e difetti involontariamente presenti nel software, ovvero le c.d. vulnerabilità. I cyber criminali possono sfruttare vulnerabilità già note nella comunità ma non ancora "sanate" dalle vittime, oppure vulnerabilità di tipo "0-day", tipicamente scoperte dagli attaccanti e non ancora note al produttore del software, per le quali quindi non esiste ancora un rimedio.

PREDOMINANZA DEI CASI

11%
DEGLI EVENTI SONO AVVENUTI A CAUSA DELLO SFRUTTAMENTO DI VULNERABILITÀ

TREND DELLA MINACCIA



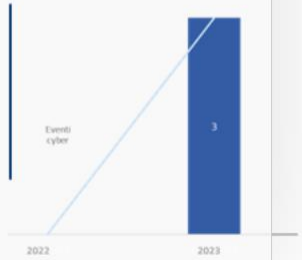
TENTATIVI DI INTRUSIONE TRAMITE CREDENZIALI

Tipologia di eventi cyber che utilizzano come vettore d'attacco un account valido. L'attaccante può sfruttare a proprio vantaggio e illecitamente le autorizzazioni dell'utenza interessata per effettuare attività malevole come ad esempio ottenere privilegi superiori, attivare persistenza, sottrarre illecitamente informazioni o eseguire codice non autorizzato. Questo tipo di evento può coinvolgere sia utenze privilegiate sia non.

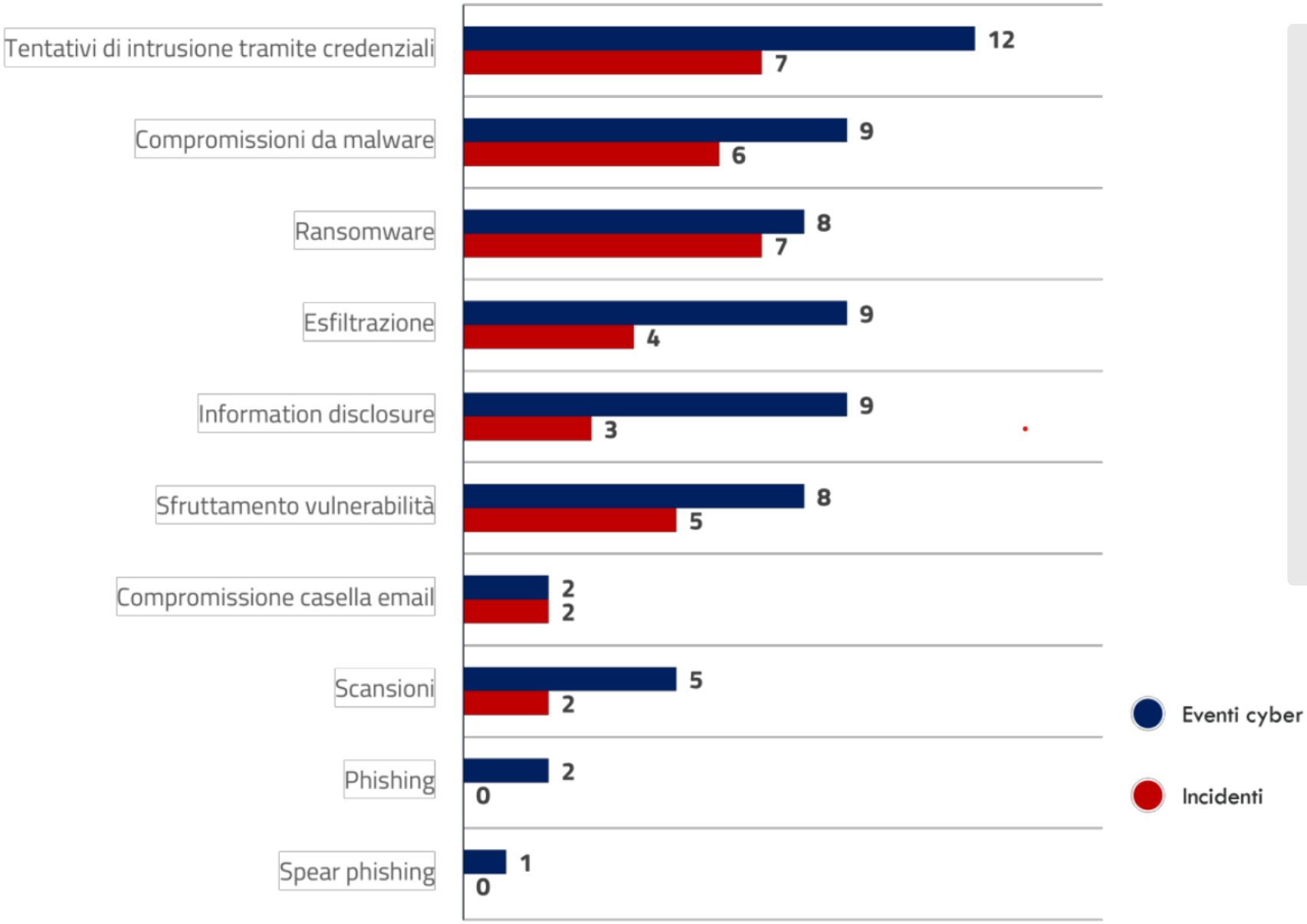
PREDOMINANZA DEI CASI

10%
NEL 2023 GLI EVENTI CON TENTATIVI DI INTRUSIONE

TREND DELLA MINACCIA



Fonte: «LA MINACCIA CIBERNETICA AL SETTORE SANITARIO Analisi e raccomandazioni Gennaio 2022 – Settembre 2022»



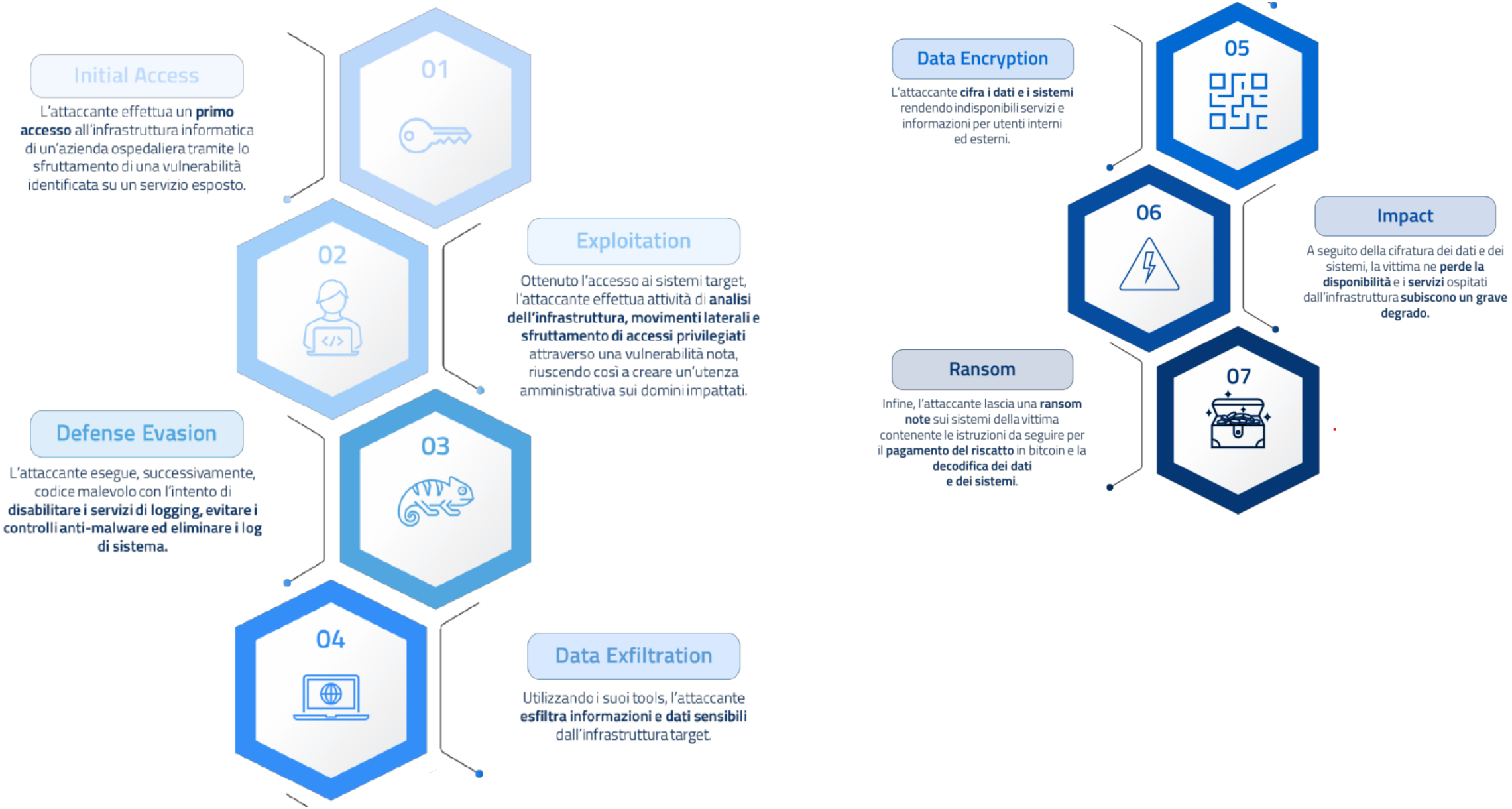
In figura sono riportate le **principali tipologie** di minacce rilevate negli eventi cyber e negli incidenti nei primi nove mesi del 2024, da cui emerge che gli attacchi **ransomware** continuano ad essere la minaccia cibernetica più diffusa per il settore, insieme ai **tentativi di intrusione tramite credenziali** e le **compromissioni da malware**. Questi ultimi in aumento rispetto al 2022 e 2023.

Fonte: «LA MINACCIA CIBERNETICA AL SETTORE SANITARIO Analisi e raccomandazioni Gennaio 2022 – Settembre 2022»

La predominanza degli attacchi di tipo ransomware potrebbe far pensare ad impatti esclusivamente sulla disponibilità dei servizi. In realtà le evidenze riscontrate nelle attività del CSIRT Italia sono più complesse. Se è vero, infatti, che negli **ospedali** gli impatti maggiori si sono registrati principalmente sulla **disponibilità** dei servizi, a causa della cifratura dei file, è altresì vero che sono stati rilevati anche altri impatti sulle infrastrutture IT: esfiltrazioni di dati (**riservatezza**), non sempre ai fini di riscatto, modifiche ai dati (e quindi perdita dell'**integrità**, con conseguente impossibilità per gli operatori sanitari di utilizzare alcuni macchinari) e cancellazioni di file (**disponibilità**). In particolare, gli impatti rilevati sono stati i seguenti:

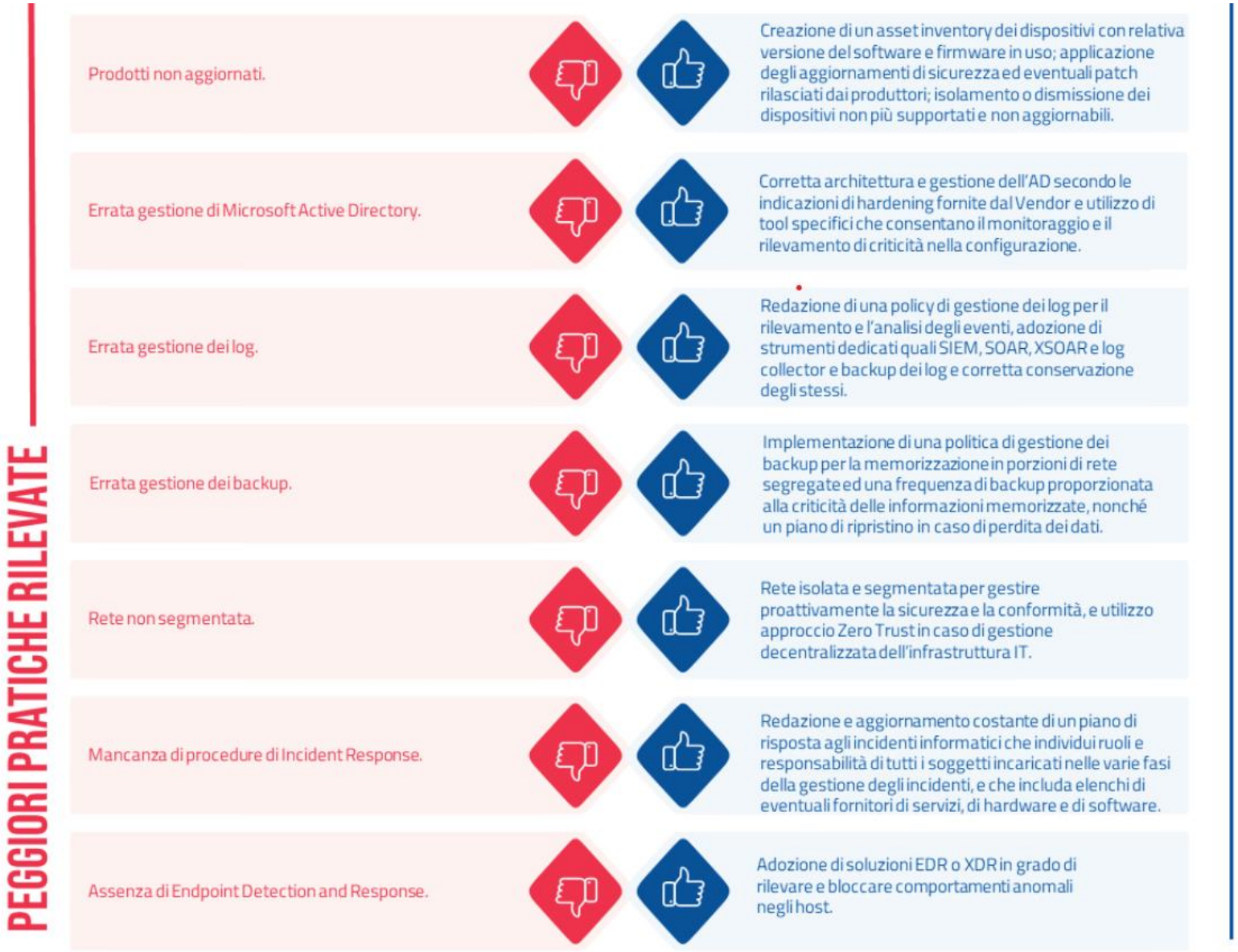
- **Blocco temporaneo** dell'erogazione di almeno un servizio nella maggioranza dei casi, con variazioni nella distribuzione che includono: o blocco di tutti i servizi IT; o blocco di tutti i servizi tranne uno; o blocco di almeno due servizi;
- **Esfiltrazione di dati** con e senza cifratura;
  Modifiche all'integrità dei dati.

Fonte: «LA MINACCIA CIBERNETICA AL SETTORE SANITARIO Analisi e raccomandazioni Gennaio 2022 – Settembre 2022»

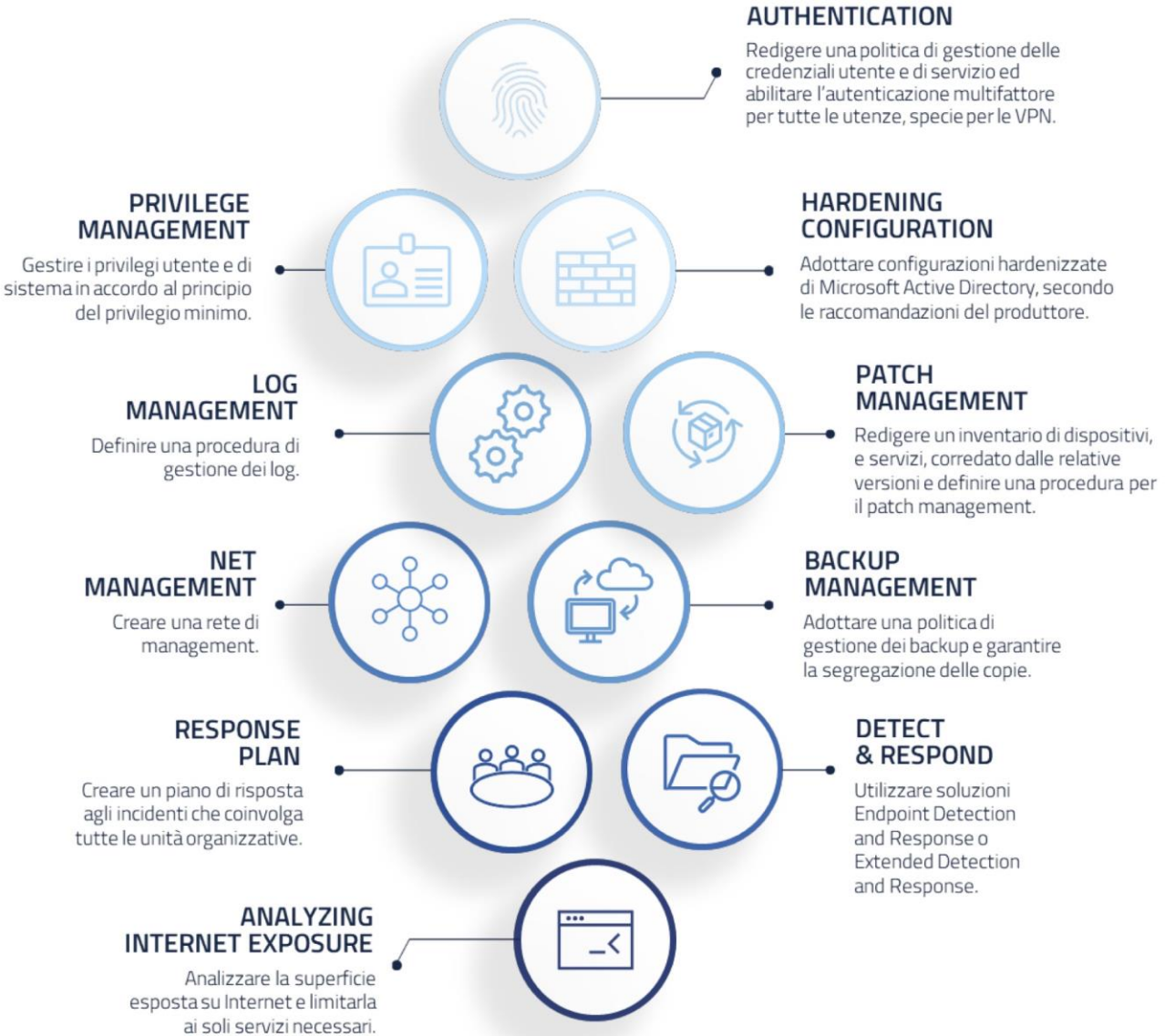


Fonte: «LA MINACCIA CIBERNETICA AL SETTORE SANITARIO Analisi e raccomandazioni Gennaio 2022 – Settembre 2022»

Fonte: «LA MINACCIA CIBERNETICA AL SETTORE SANITARIO Analisi e raccomandazioni Gennaio 2022 – Settembre 2022»



Fonte: «LA MINACCIA CIBERNETICA AL SETTORE SANITARIO Analisi e raccomandazioni Gennaio 2022 – Settembre 2022»



Fonte: «LA MINACCIA CIBERNETICA AL SETTORE SANITARIO Analisi e raccomandazioni Gennaio 2022 – Settembre 2022»

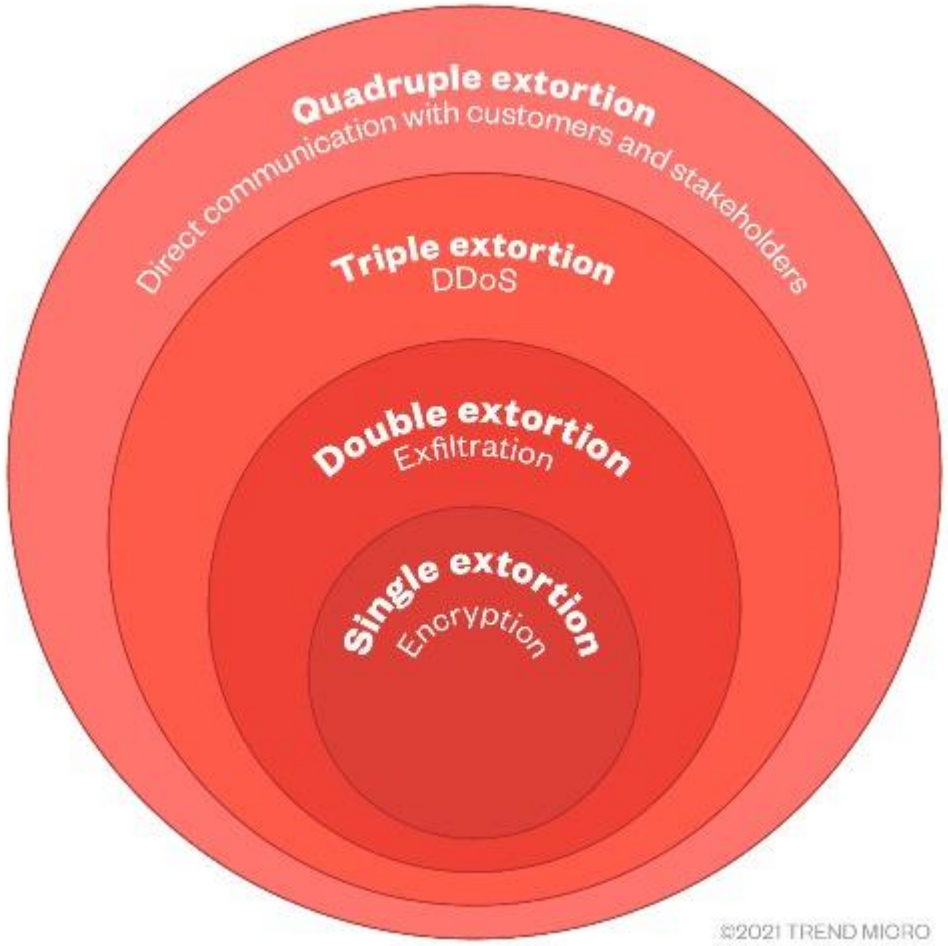
Figura 11: le 10 raccomandazioni più rilevanti per il settore

Estorsione Singola
Il ransomware con estorsione singola (la prima fase del ransomware multi-estorsione) implica la crittografia. Gli attaccanti criptano interi sistemi o selezionano file ritenuti altamente importanti. L'estorsione singola è l'unico metodo di attacco per alcuni tipi di ransomware, come WannaCry e CryptoLocker.

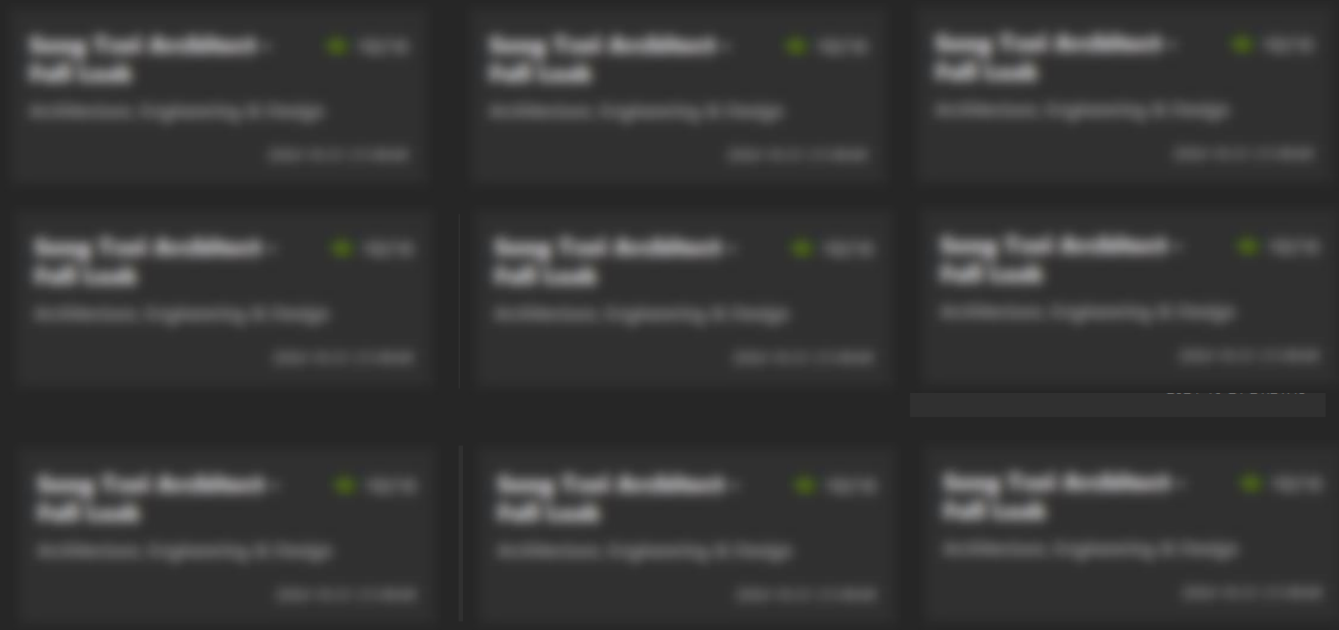
Doppia Estorsione
Molte organizzazioni riescono a superare la minaccia della crittografia dei file grazie a un sistema di backup semplice e aggiornato. Per contrastare questa tendenza, gli operatori di malware hanno aggiunto un'altra fase di estorsione, che prevede l'esfiltrazione di dati, una tattica resa popolare da malware come Maze e DoppelPaymer. Gli attaccanti rubano dati sensibili e minacciano di divulgarli al pubblico (spesso tramite siti di leak nel dark web) o di venderli sul mercato nero.

Tripla Estorsione
Un attacco di tripla estorsione può assumere forme diverse, ma in genere espande ulteriormente il campo d'azione degli attaccanti. Ad esempio, se la vittima rifiuta di pagare il riscatto anche dopo la minaccia di divulgazione delle informazioni, il cyberattaccante potrebbe eseguire un attacco di interruzione del servizio per esercitare una pressione aggiuntiva. AvosLocker è un tipo di ransomware che utilizza attacchi DDoS come parte del suo strumento di tripla estorsione.

Quadrupla Estorsione
Gli attori delle minacce possono ampliare ulteriormente i loro guadagni con ransomware di quadrupla estorsione che aggiunge un ulteriore livello, spesso coinvolgendo terze parti.



Wall of Shame



MONTI

Data Breach Report 522 GB CORP DATA

views: 502933

We did not leave any ransom requests, the media invented the amount, today we publish all the data, and we promise you tough attacks

"We did not leave any ransom requests, the media invented the amount, today we publish all the data, and we promise you tough attacks"

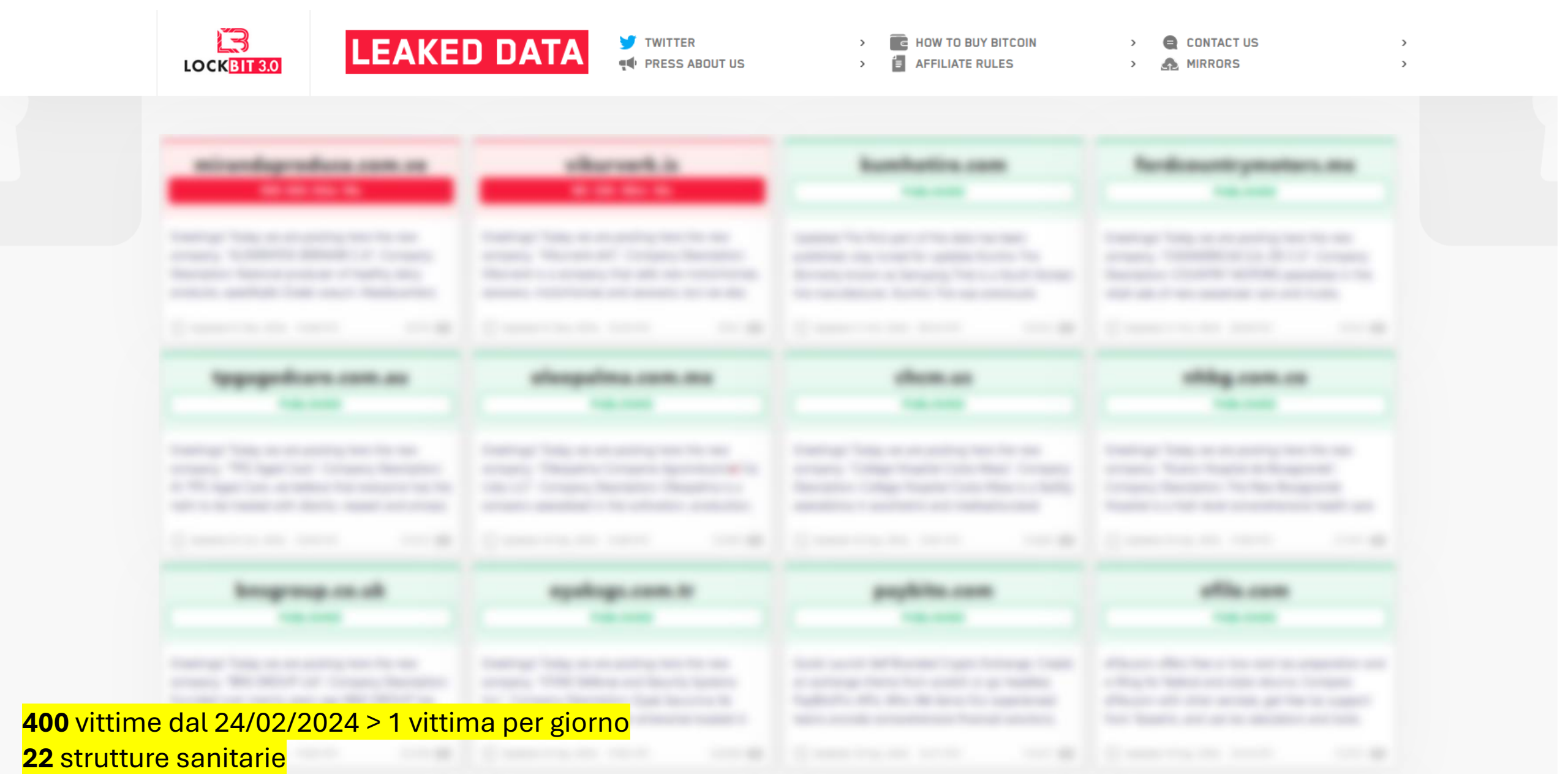
Ministero delle Imprese e del Made in Italy

SSSTLC Scuola Superiore di Specializzazione in Telecomunicazioni

CYBER 4.0 CYBERSECURITY COMPETENCE

CYBER SHOT Lab Cybersecurity laboratory for Systems, Health,

UNIVERSITÀ CAMPUS BIO-MEDICO



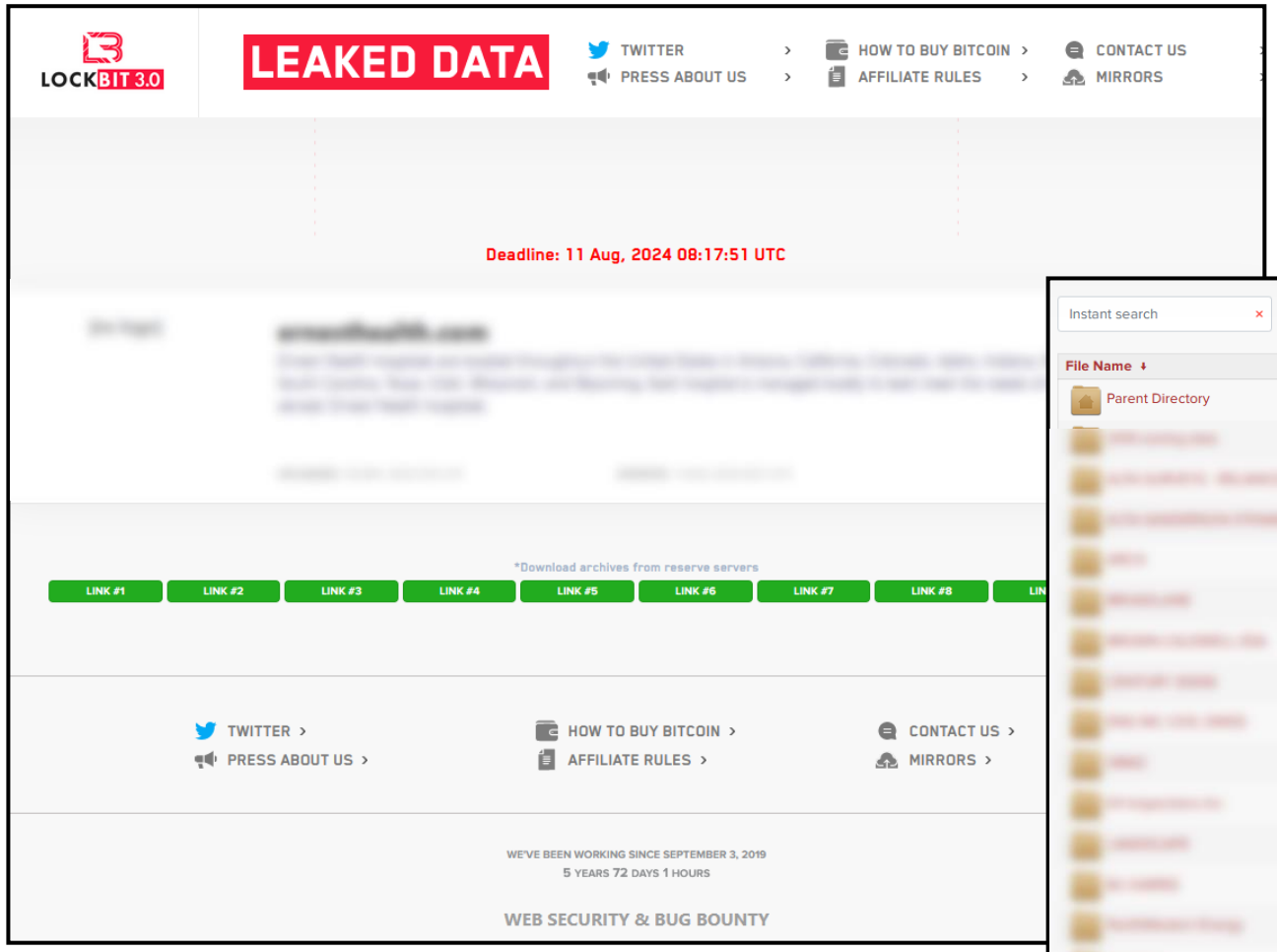
400 vittime dal 24/02/2024 > 1 vittima per giorno
22 strutture sanitarie

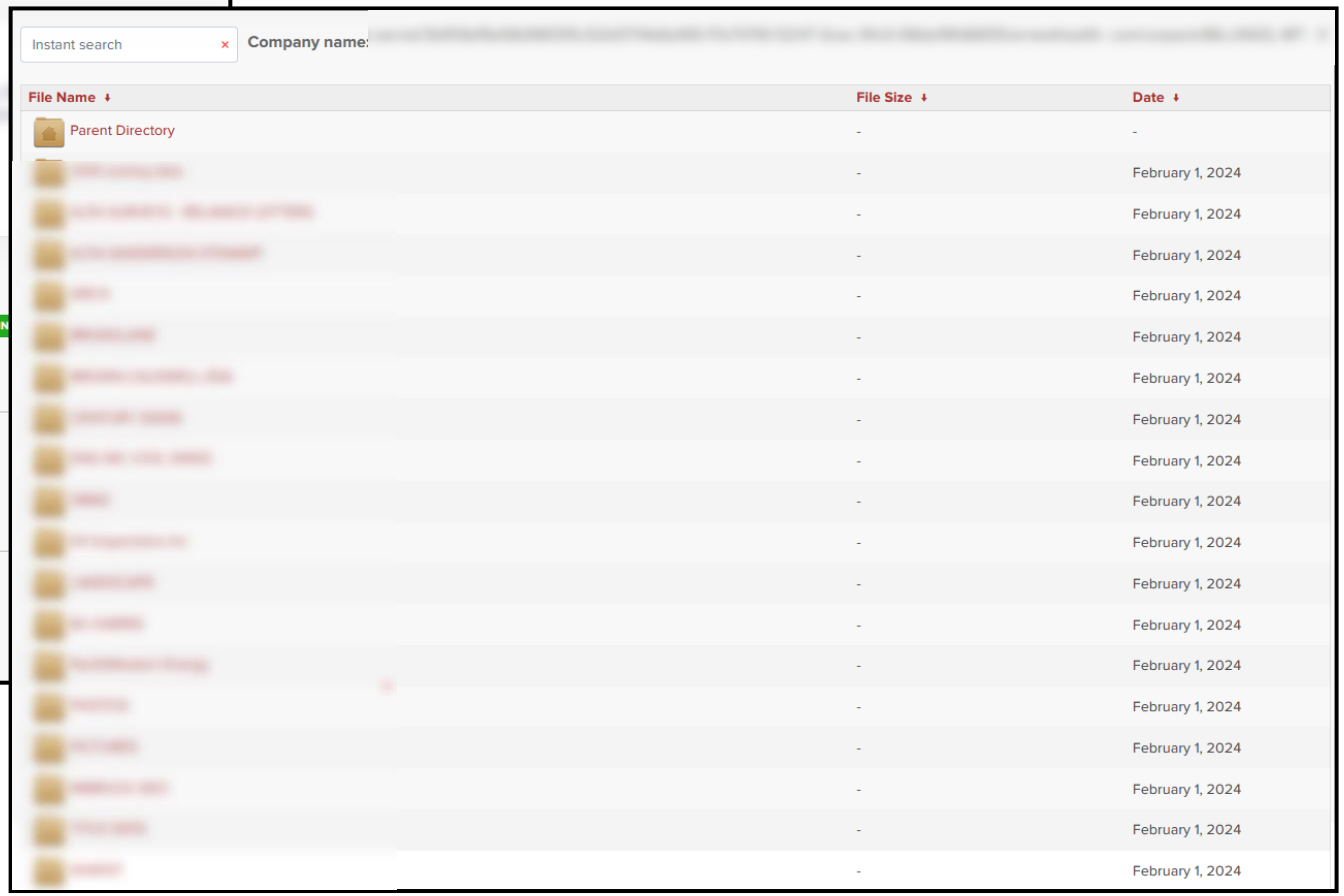
Ministero delle Imprese e del Made in Italy

SSSTLC Scuola Superiore di Specializzazione in Telecomunicazioni

CYBER 4.0 CYBERSECURITY COMPETENCE CENTER

UNIVERSITÀ CAMPUS BIO-MEDICO DI ROMA





Ministero delle Imprese e del Made in Italy

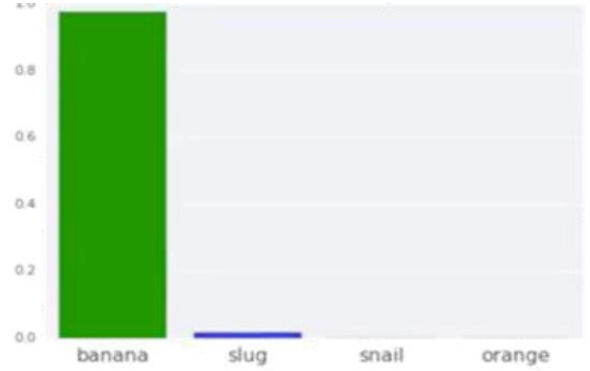
SSSTLC Scuola Superiore di Specializzazione in Telecomunicazioni

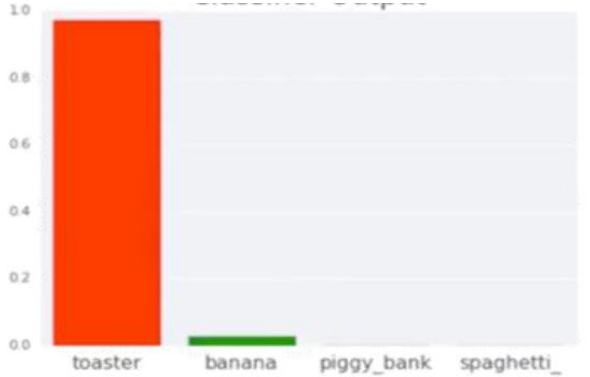
CYBER 4.0 CYBERSECURITY COMPETENCE CENTER

CYBER SHOT Lab Cybersecurity laboratory for Systems, Health, and Operational Technologies

UNIVERSITÀ CAMPUS BIO-MEDICO DI ROMA

ADVERSARIAL MACHINE LEARNING





ADVERSARIAL MACHINE LEARNING

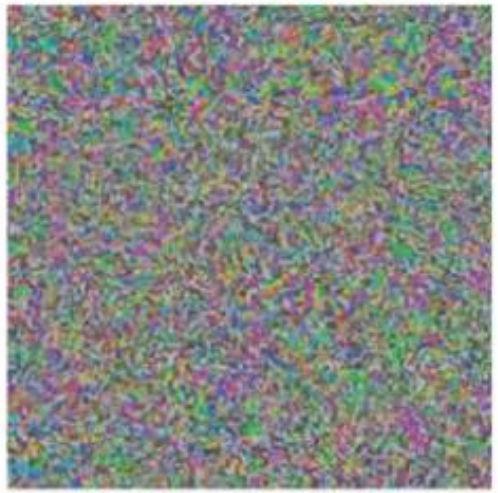
CYBER SHOT Lab
Cybersecurity laboratory
for Systems, Health,
and Operational Technologies

Original image

Dermatoscopic image of a benign melanocytic nevus, along with the diagnostic probability computed by a deep neural network.

+ 0.04 ×

Adversarial noise



Perturbation computed by a common adversarial attack technique. See (*7*) for details.

=

Adversarial example

Combined image of nevus and attack perturbation and the diagnostic probabilities from the same deep neural network.

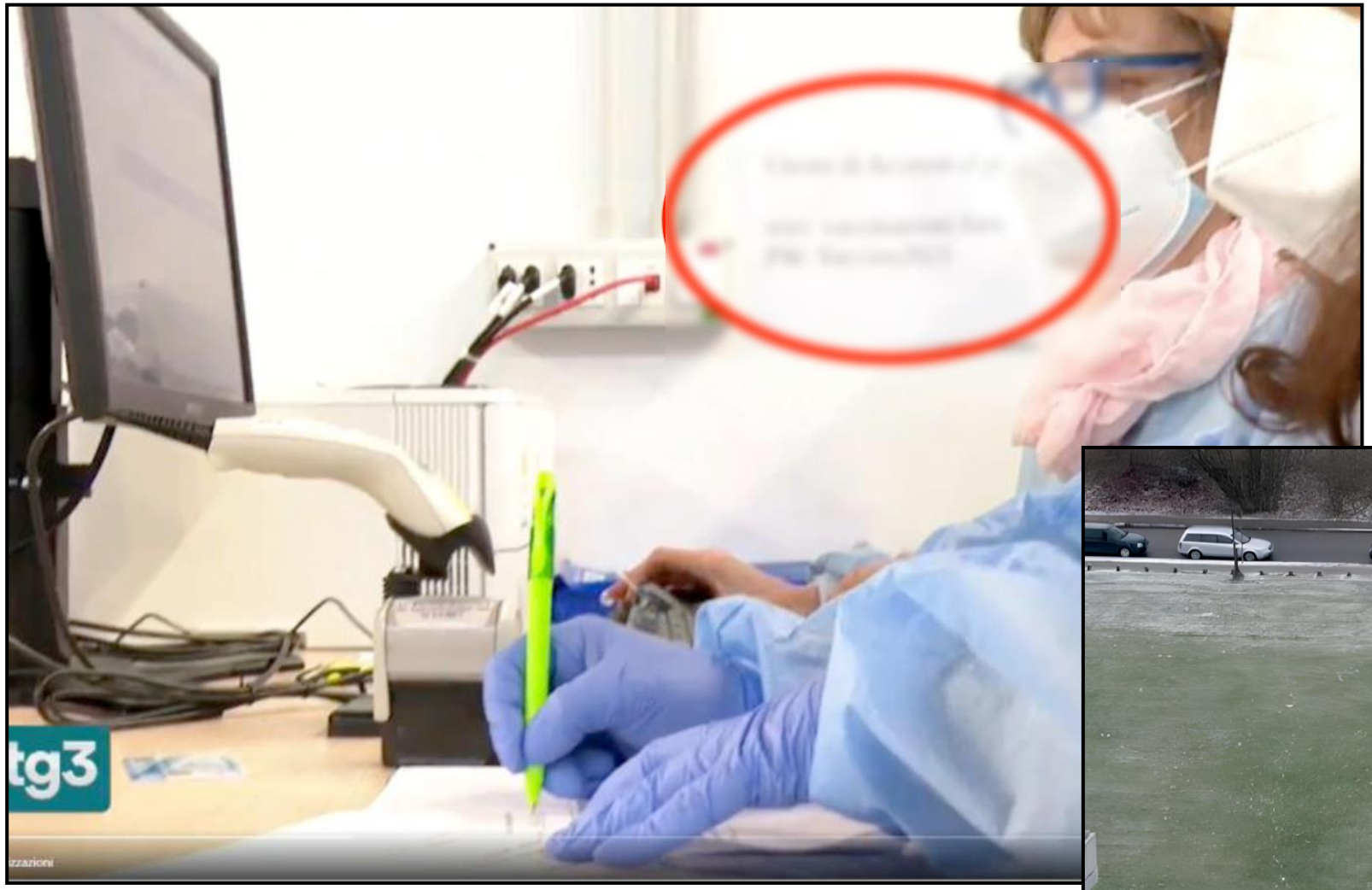
Ministero delle Imprese e del Made in Italy

SSSTLC Scuola Superiore di Specializzazione in Telecomunicazioni

CYBER 4.0 CYBERSECURITY COMPETENCE CENTER

CYBER SHOT Lab
Cybersecurity laboratory
for Systems, Health,
and Operational Technologies

UNIVERSITÀ CAMPUS BIO-MEDICO DI ROMA


tg3