

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



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**.

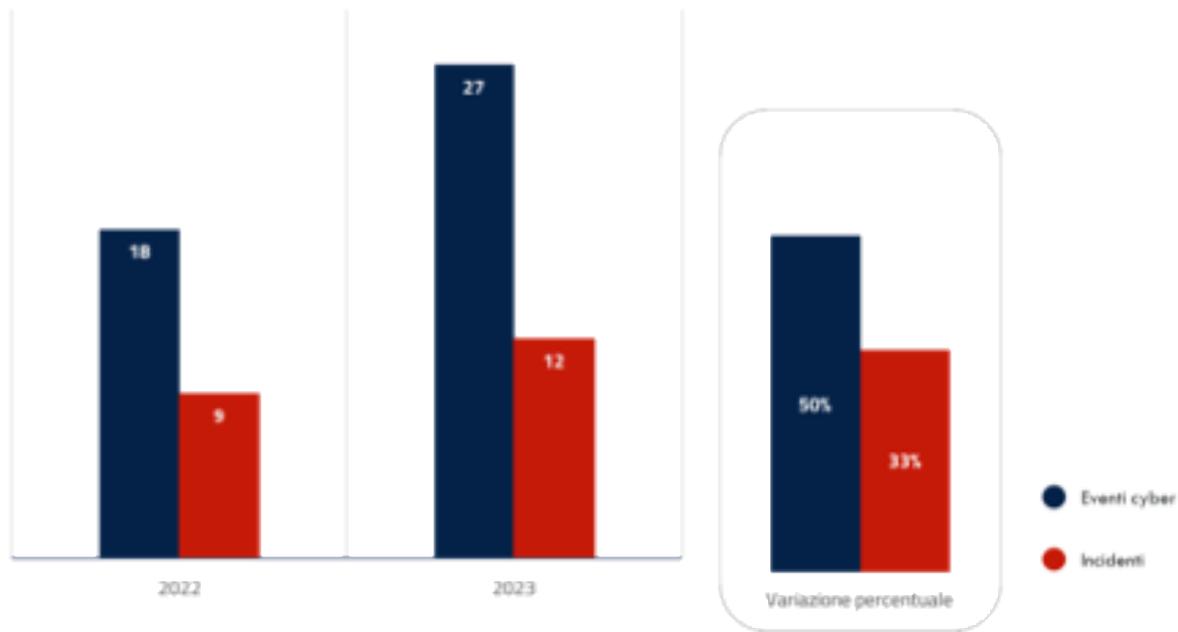


Figura 2: numero di eventi cyber e incidenti nel periodo 2022-2023 e loro variazione percentuale annua

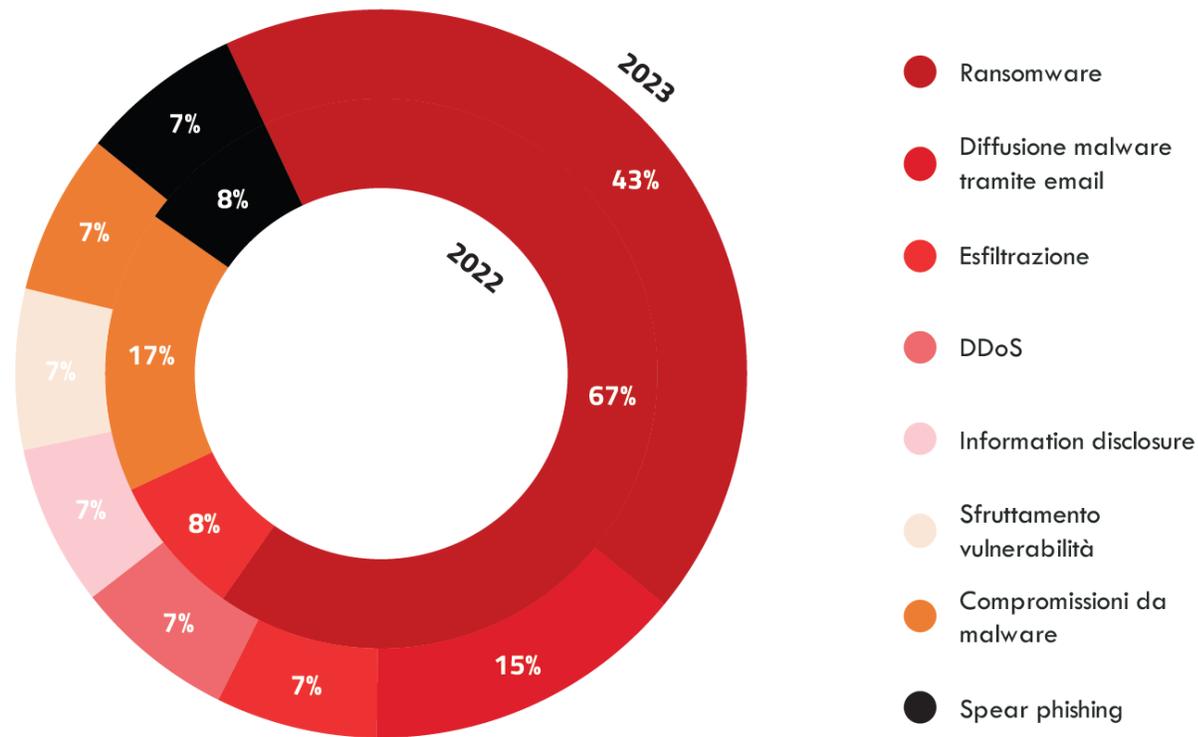
- Gli attacchi **ransomware** risultano essere la minaccia cibernetica più diffusa per il settore, con il **35% degli eventi** nel 2023 e il **60% degli eventi** nel 2022;
- L'attività di **information disclosure** è stata rilevata nel **14% degli eventi** nel 2023;
- La **diffusione di malware tramite 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»



Ministero delle Imprese
e del Made in Italy





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.

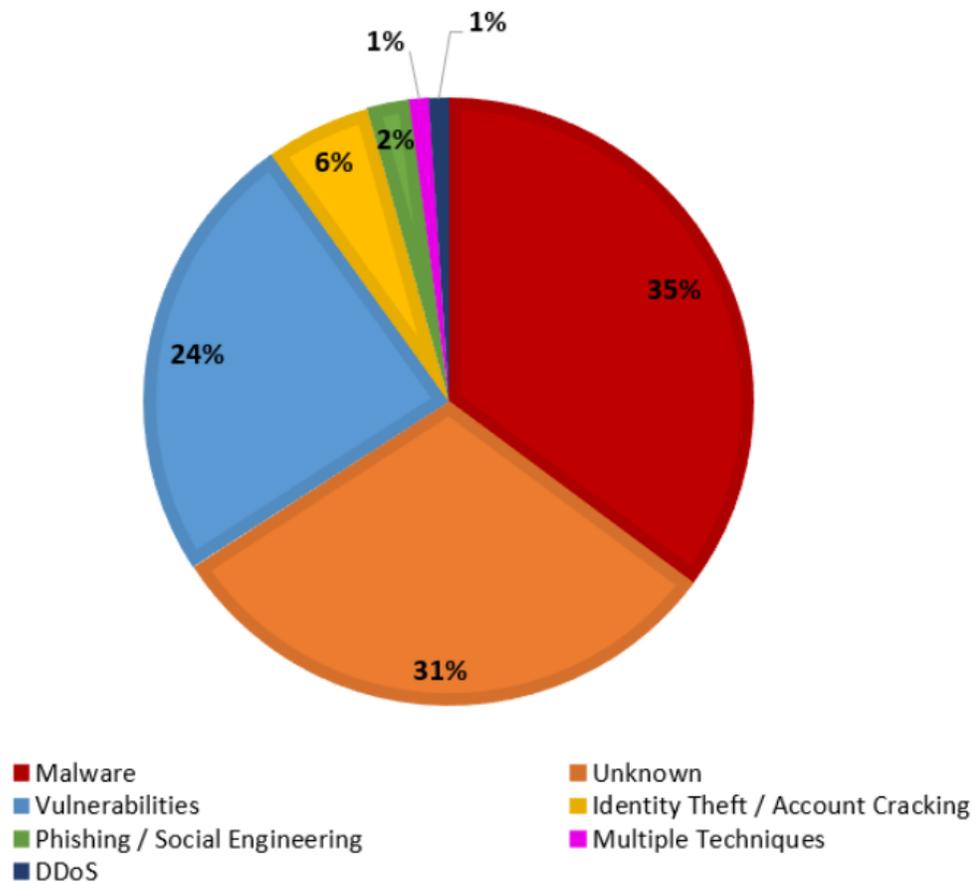
Fonte: «LA MINACCIA CIBERNETICA AL SETTORE SANITARIO Analisi e raccomandazioni Gennaio 2022 – Settembre 2022»



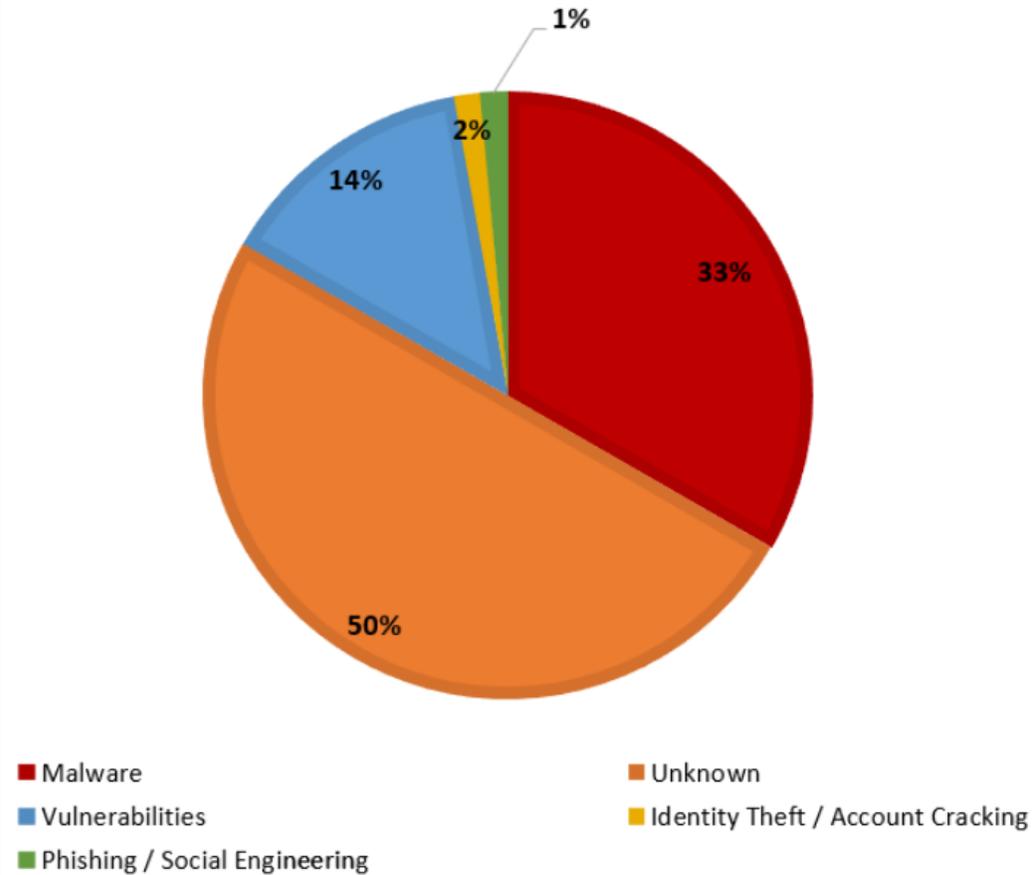
Ministero delle Imprese
e del Made in Italy



TECNICHE HEALTHCARE 2023



TECNICHE HEALTHCARE 1Q24



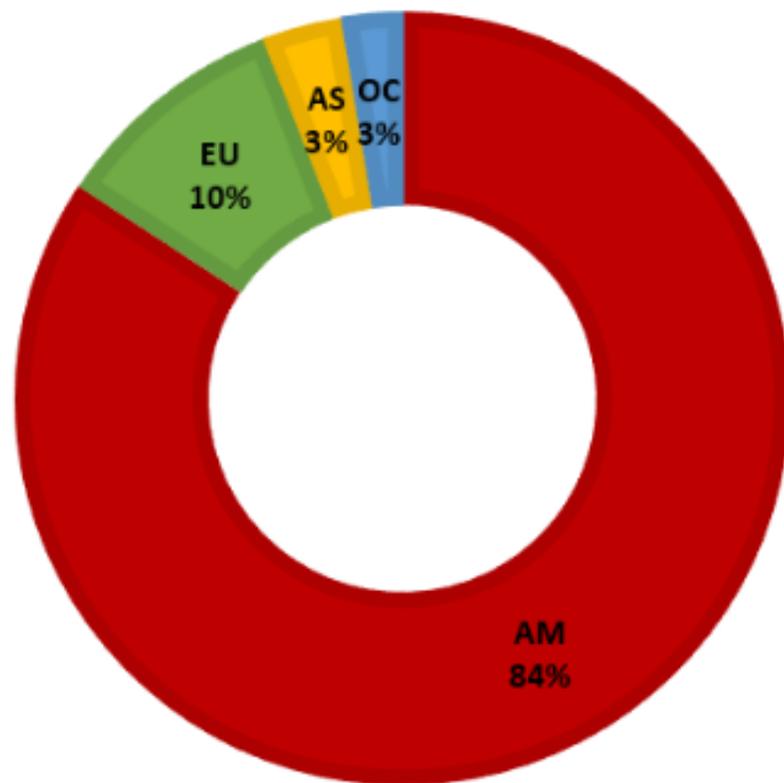
© Clusit - Rapporto 2024 sulla Sicurezza ICT in Italia



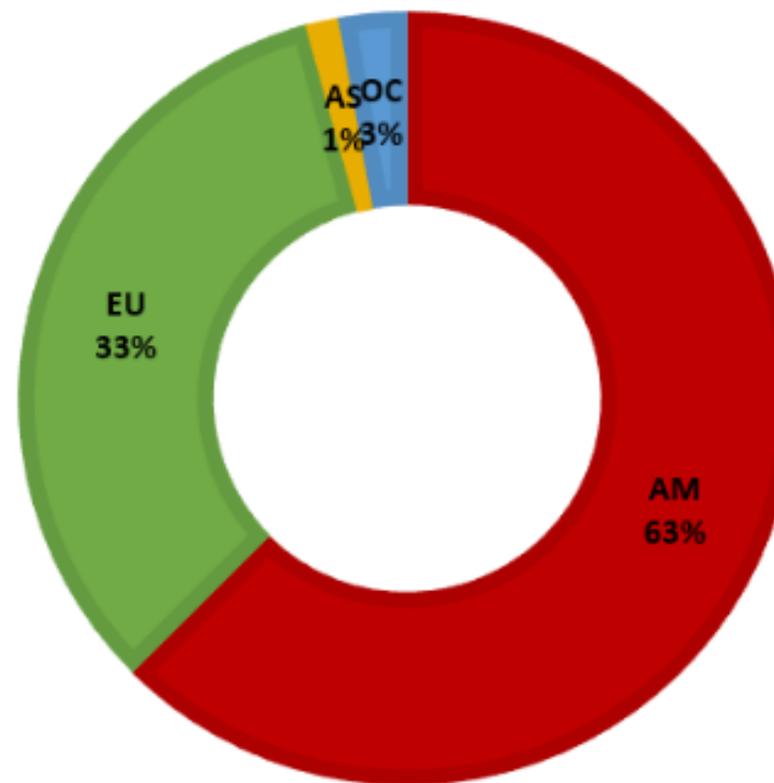
Ministero delle Imprese
e del Made in Italy



GEOGRAFIE VITTIME HEALTHCARE 2023



GEOGRAFIE VITTIME HEALTHCARE 1Q24



© Clusit - Rapporto 2024 sulla Sicurezza ICT in Italia



Ministero delle Imprese
e del Made in Italy





RANSOMWARE

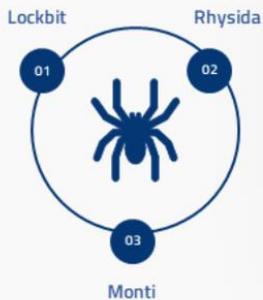
Tipologia di minaccia che ha lo scopo di cifrare i dati del bene informatico target in modo da comprometterne la disponibilità e l'integrità. Inoltre, in questa tipologia di minaccia spesso l'attaccante crea dei file, detti ransom notes, tramite i quali viene richiesto alla vittima un riscatto in cambio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

PREDOMINANZA DEI CASI

TOP 3 RANSOMWARE GANGS

42%

DEGLI EVENTI NEL BIENNIO 2022-23 SONO RANSOMWARE



INFORMATION DISCLOSURE

Tipologia di minaccia cyber in cui è occorsa una violazione di sicurezza dei dati/informazioni personali o proprietarie. L'information disclosure, 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

TOP 3 IMPACT

14%

DEGLI EVENTI HA CAUSATO UN INFORMATION DISCLOSURE



SFRUTTAMENTO VULNERABILITÀ

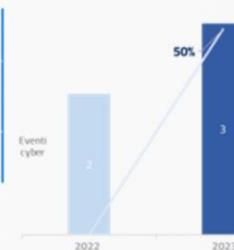
Gli attacchi attuati attraverso l'utilizzo degli errori e difetti involontariamente presenti nel software, ovvero le c.d. vulnerabilità. I cyber criminali possono sfruttare vulnerabilità già note nella comunità ma non ancora "sanate" dalle vittime, oppure vulnerabilità di tipo "0-day", tipicamente scoperte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

PREDOMINANZA DEI CASI

TREND DELLA MINACCIA

11%

DEGLI EVENTI SONO AVVENUTI A CAUSA DELLO SFRUTTAMENTO DI VULNERABILITÀ



TENTATIVI DI INTRUSIONE TRAMITE CREDENZIALI

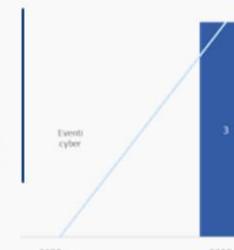
Tipologia di eventi cyber che utilizzano come vettore d'attacco un account valido. L'attaccante può sfruttare a proprio vantaggio e illecitamente le autorizzazioni dell'utente interessata per effettuare attività malevole come ad esempio ottenere privilegi superiori, attivare persistenza, sottrarre illecitamente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

PREDOMINANZA DEI CASI

TREND DELLA MINACCIA

10%

NEL 2023 GLI EVENTI CON TENTATIVI DI INTRUSIONE

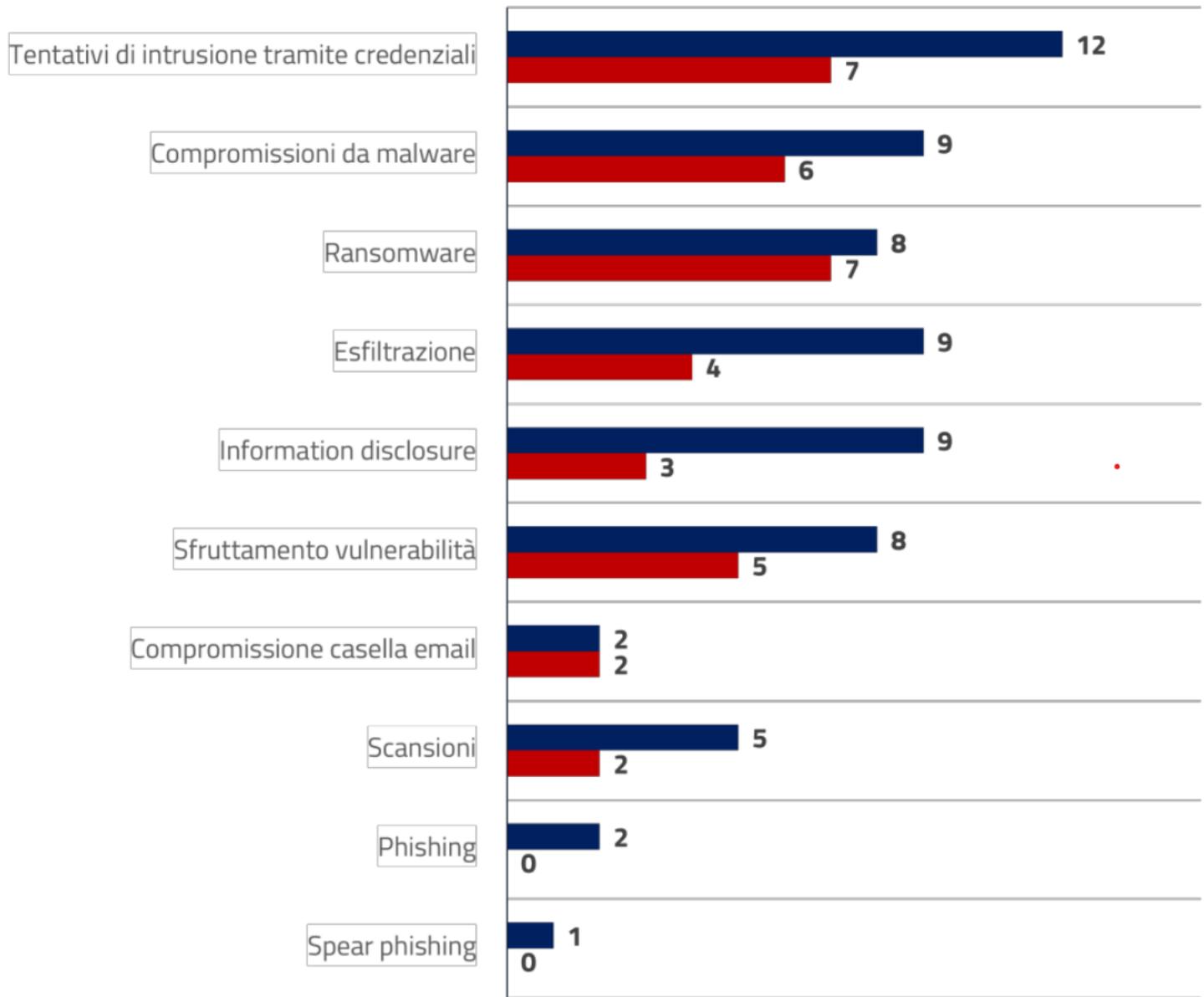


Fonte: «LA MINACCIA CIBERNETICA AL SETTORE SANITARIO Analisi e raccomandazioni Gennaio 2022 – Settembre 2022»



Ministero delle Imprese e del Made in Italy





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:

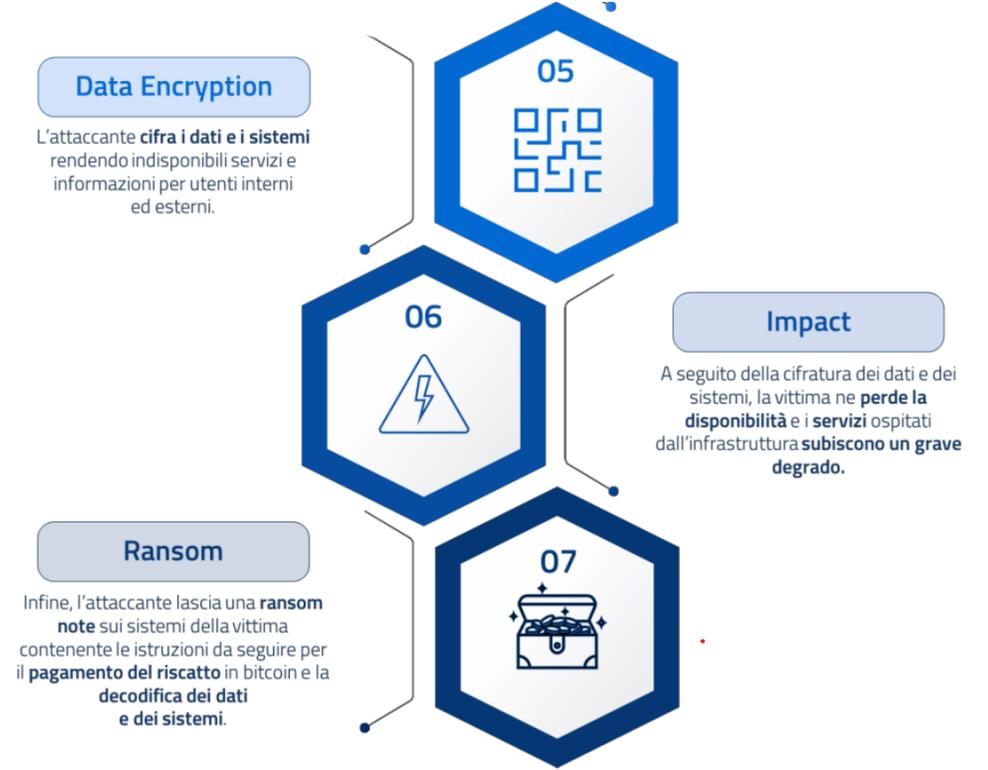
- **Blocco temporaneo** dell'erogazione di almeno un servizio nella maggioranza dei casi, con variazioni nella distribuzione che includono: o blocco di tutti i servizi IT; o blocco di tutti i servizi tranne uno; o blocco di almeno due servizi;
- **Esfiltrazione di dati** con e senza cifratura;
Modifiche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

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



Ministero delle Imprese
e del Made in Italy





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



Ministero delle Imprese e del Made in Italy



Assenza di autenticazione multi-fattore sulle Virtual Private Network (VPN).			Implementazione dell'autenticazione multifattore (MFA).
Utilizzo di protocolli di autenticazione e cifratura obsoleti.			Utilizzo di versioni recenti di protocolli di autenticazione e comunicazione e disabilitazione protocolli obsoleti sul Domain Controller).
Password Policy inadeguata.			Creazione di una password policy che rispetti le best practice, anche supportata dagli strumenti preposti quali password manager.
Errata gestione dei privilegi utente.			Applicazione del principio del privilegio minimo su account utente e di servizio e revisione periodica dei privilegi ad essi assegnati.
Assenza di inventario dei servizi critici.			Redazione e costante aggiornamento di una lista aggiornata dei servizi IT critici e una lista delle funzionalità e dati critici degli ospedali.

CONTROMISURE

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

PEGGIORI PRATICHE RILEVATE

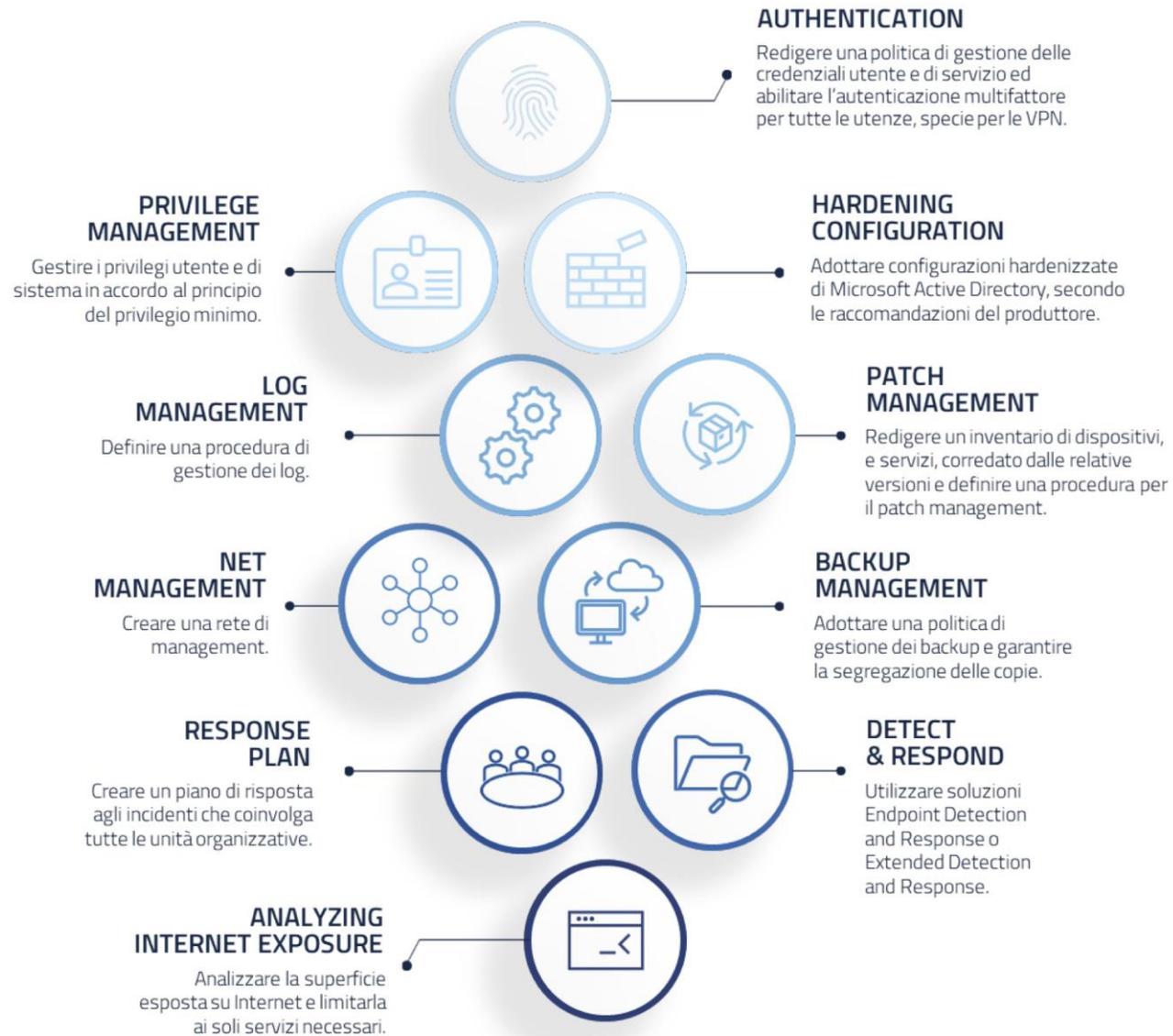
Prodotti non aggiornati.			Creazione di un asset inventory dei dispositivi con relativa versione del software e firmware in uso; applicazione degli aggiornamenti di sicurezza ed eventuali patch rilasciati dai produttori; isolamento o dismissione dei dispositivi non più supportati e non aggiornabili.
Errata gestione di Microsoft Active Directory.			Corretta architettura e gestione dell'AD secondo le indicazioni di hardening fornite dal Vendor e utilizzo di tool specifici che consentano il monitoraggio e il rilevamento di criticità nella configurazione.
Errata gestione dei log.			Redazione di una policy di gestione dei log per il rilevamento e l'analisi degli eventi, adozione di strumenti dedicati quali SIEM, SOAR, XSOAR e log collector e backup dei log e corretta conservazione degli stessi.
Errata gestione dei backup.			Implementazione di una politica di gestione dei backup per la memorizzazione in porzioni di rete segregate ed una frequenza di backup proporzionata alla criticità delle informazioni memorizzate, nonché un piano di ripristino in caso di perdita dei dati.
Rete non segmentata.			Rete isolata e segmentata per gestire proattivamente la sicurezza e la conformità, e utilizzo approccio Zero Trust in caso di gestione decentralizzata dell'infrastruttura IT.
Mancanza di procedure di Incident Response.			Redazione e aggiornamento costante di un piano di risposta agli incidenti informatici che individui ruoli e responsabilità di tutti i soggetti incaricati nelle varie fasi della gestione degli incidenti, e che includa elenchi di eventuali fornitori di servizi, di hardware e di software.
Assenza di Endpoint Detection and Response.			Adozione di soluzioni EDR o XDR in grado di rilevare e bloccare comportamenti anomali negli host.

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



Ministero delle Imprese
e del Made in Italy





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



Ministero delle Imprese
e del Made in Italy



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



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

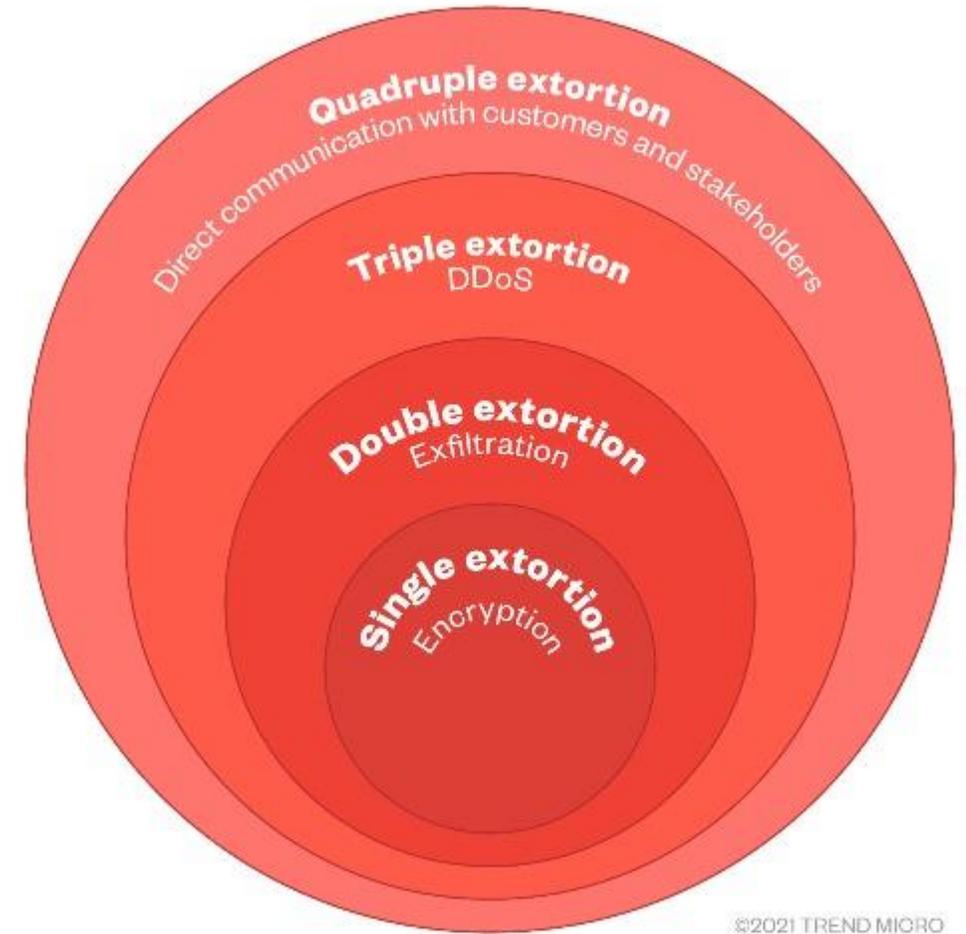
Molte organizzazioni riescono a superare la minaccia della crittografia dei file grazie a un sistema di backup semplice e aggiornato. Per contrastare questa tendenza, gli operatori di malware hanno aggiunto un'altra fase di estorsione, che prevede l'esfiltrazione di dati, una tattica resa popolare da 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.

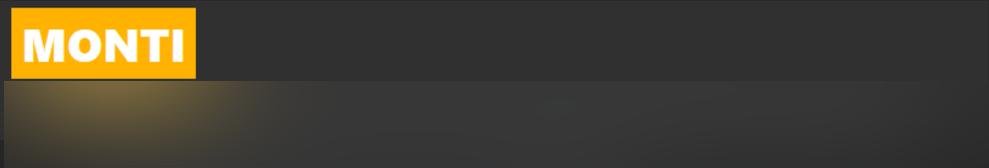
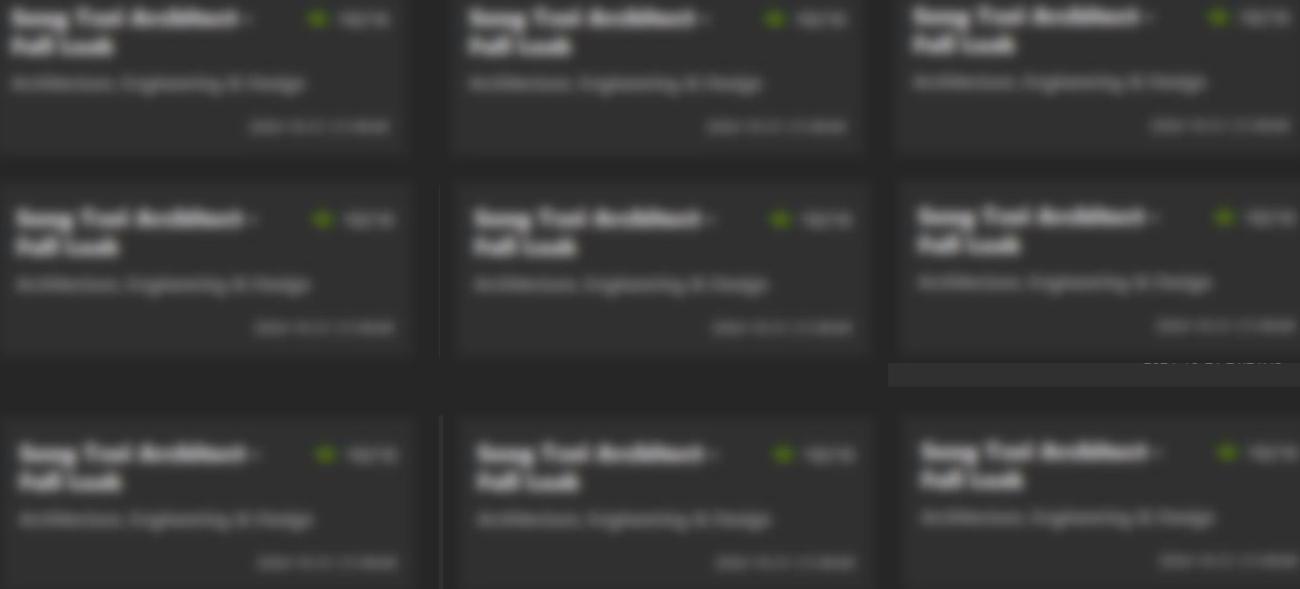


Ministero delle Imprese
e del Made in Italy



Wall of Shame

MONTI



Data Breach Report 522 GB CORP DATA



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

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

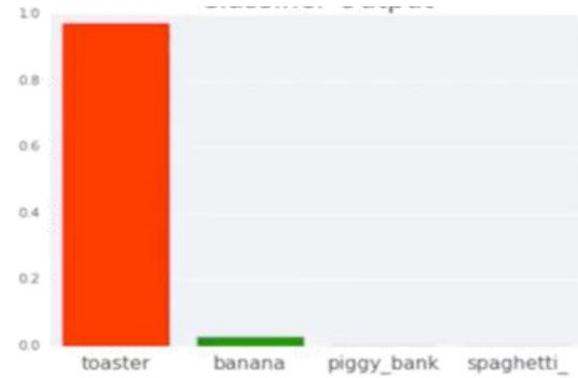
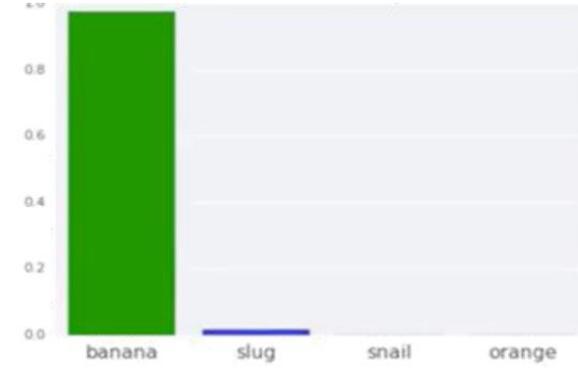


www.ospedale.com 10000	www.ospedale.it 10000	www.ospedale.com 10000	www.ospedale.com 10000
www.ospedale.com 10000	www.ospedale.com 10000	www.ospedale.com 10000	www.ospedale.com 10000
www.ospedale.com 10000	www.ospedale.com 10000	www.ospedale.com 10000	www.ospedale.com 10000

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



ADVERSARIAL MACHINE LEARNING



Original image

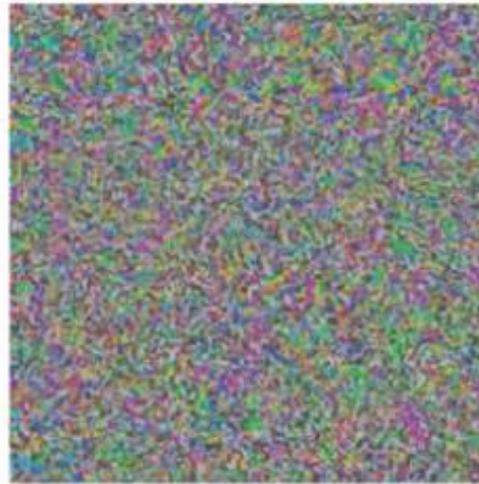


Dermoscopic image of a benign melanocytic nevus, along with the diagnostic probability computed by a deep neural network.



+ 0.04 ×

Adversarial noise



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

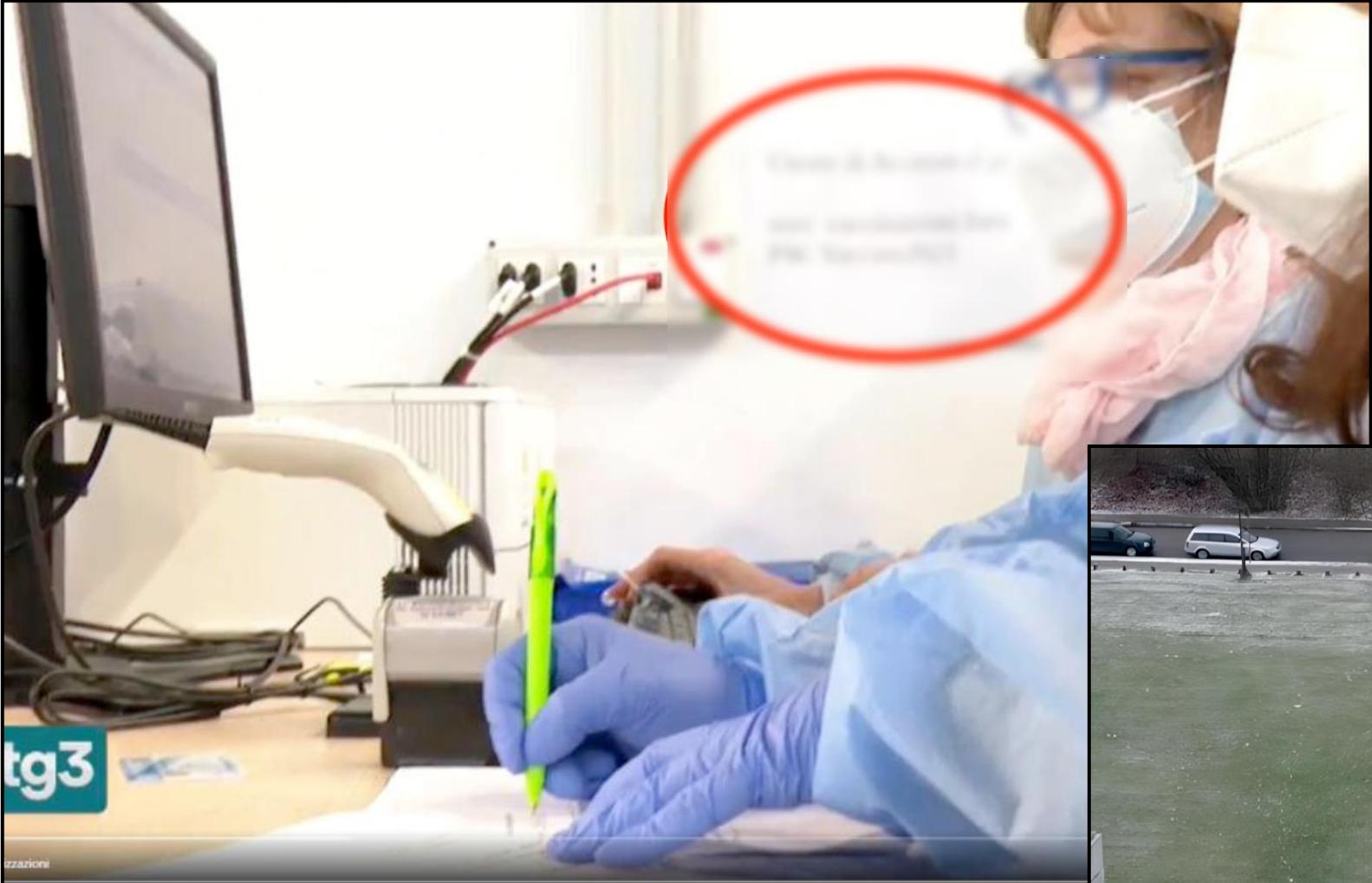
=

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

