Quanto co$ta un **ransomware**?

Michele Pinassi

Responsabile cybersecurity dell'Università degli Studi di Siena. Da oltre 25 anni mi occupo di ICT per lavoro e per passione. Convinto utente e sostenitore del FOSS, partecipo attivamente a progetti nel mondo open source cercando di contribuire alla divulgazione della consapevolezza del mondo cyber.

www.zerozone.it

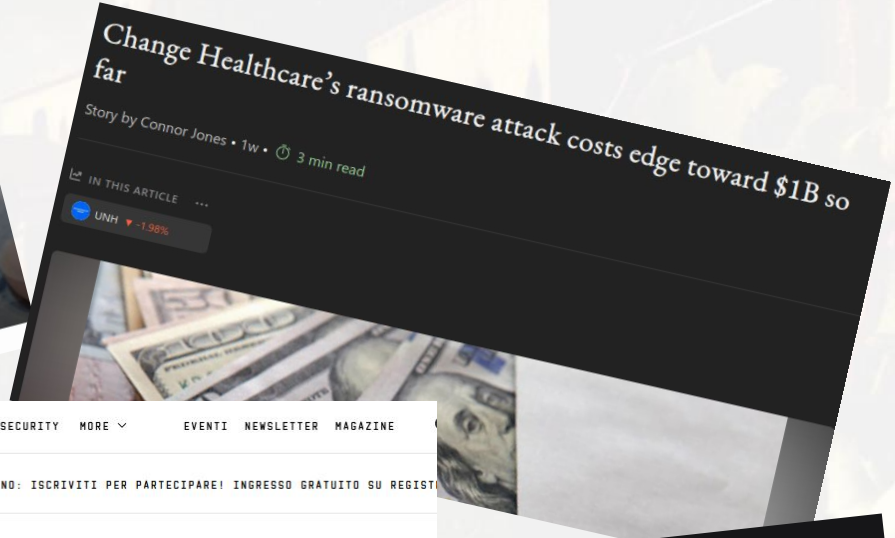
@michelepinassi

github.com/michelep

“State facendo

terrorismo!”

(cit.)



RANSOMWARE

Attacco al sistema sanitario lucano: unità di crisi attivata su ASP Basilicata

Home > Attacchi Hacker E Malware: Le Ultime News In Tempo Reale E Gli Approfondimenti

Colpita da attacco informatico una nuova struttura sanitaria italiana, l'ASP Basilicata conferma il rilevamento dell'attacco post disservizi su almeno quattro ospedali lucani. Può essersi trattato di ransomware, si prosegue con le verifiche e azioni per contenere il danno in attesa di maggiori dettagli sui fatti accaduti

WIRED SCIENZA ECONOMIA CULTURA GADGET SECURITY MORE EVENTI NEWSLETTER MAGAZINE

NA LA DATA: TORNA IL WIRED NEXT FEST, A MILANO IL 15 E 16 GIUGNO: ISCRIVITI PER PARTECIPARE! INGRESSO GRATUITO SU REGIST

KEVIN CARBONI DIRITTI 10.04.2024

Per l'attacco ransomware a Regione Lazio scattano 400mila euro di multa

Secondo il Garante privacy, mancavano misure di sicurezza adeguate. Nel 2021 sistemi nel piano della campagna vaccinale

72%

delle realtà aziendali è stata coinvolta in un attacco ransomware nel 2023

https://www.blackfog.com/what-is-ransomware/

Aziende fallite dopo un attacco ransomware

2023 – St. Margaret's Health (SMH)
2020 - Travelex
2020 – Vastaamo
2019 – The Heritage Company
2019 – Wood Ranch Medical
2017 – FlexiSpy
2014 – Code Space
2011 – DigiNotar
…

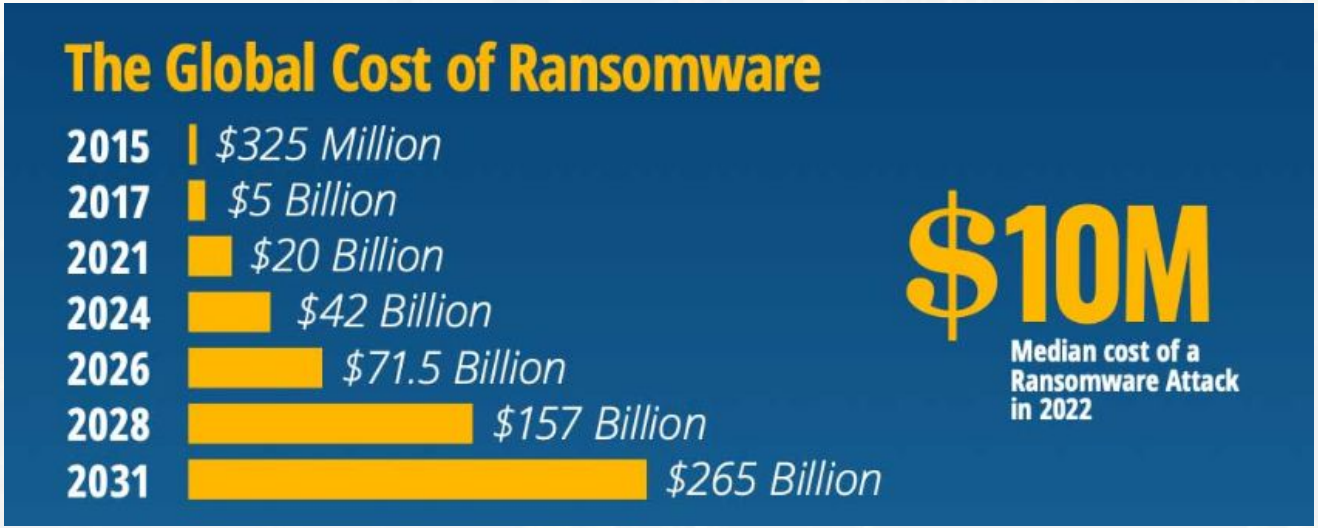
L'Italia è il paese europeo più colpito

3,56%

degli attacchi subiti a livello globale.
Quinta al mondo dopo USA (19,82%), Turchia (12,13%), Giappone (5,81%), Taiwan (5,73%) e India (5,71%).

https://www.ansa.it/sito/notizie/tecnologia/software_app/2022/07/13/cybercrime-a-maggio-italia-prima-in-europa-per-ransomware_f64dd5dd-433b-4293-91f2-2ed42364cc74.html

"The cost of cybercrime is estimated to reach $10.5 trillion USD annually by 2025 ***with a 15 percent yearly increase****. During the period from 2021 to 2025, global cybersecurity spending is expected to exceed $1.75 trillion USD."*



https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/

I 7 costi di un attacco ransomware

The Ransom

You should NOT pay the ransom. There's a risk that the ransom will only be raised, recovered data have been damaged from the encryption, or you will simply never hear back...

Legal Expenses

You must always inform your clients immediately about a breach of personal data according to the EU's GDPR regulation. Also, in some industries a data breach can result in fines by default ...

Cost of Downtime

As long as your systems are down, your whole operation is paralyzed and you're unable to service clients, sell or produce products, etc. The negative impact is counted in minutes rather than hours ...

Data Loss

Even if you are able to restore from your backup, there is a risk that not all of your files were backed up completely or correctly, meaning you might have forever lost valuable data ...

Labor Cost

While your IT resources are focused on restoring your systems, most other employees are dependent on access to data, resulting in a backlog of work throughout your organization ...

Collateral Damage

Hackers trade stolen data and credentials and have become highly organized. After having resolved an incident there is still a risk that your company data could be exploited in future ...

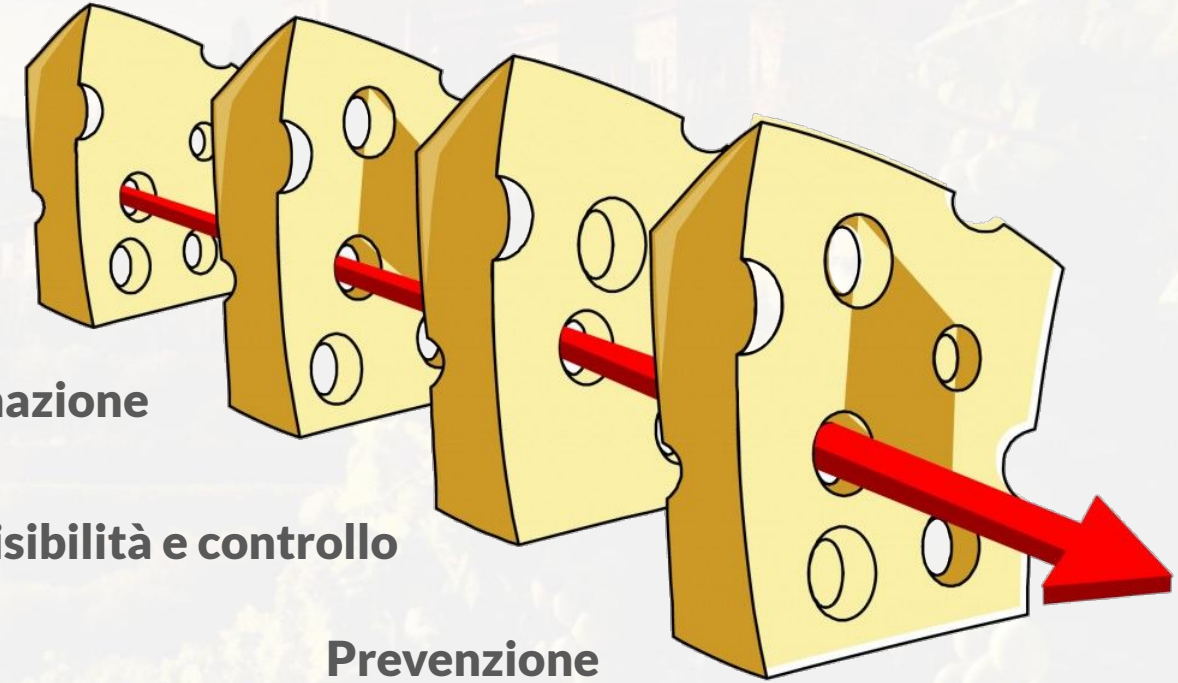
Brand Reputation

You can restore data, but a damaged reputation is hard to fix. And remember: the public includes not only your customers, but also your employees, investors and other stakeholders ...

Strategie di difesa

1) procedure di disaster recovery chiare e periodicamente verificate
2) formazione e consapevolezza, a tutti i livelli
3) visibilità sui sistemi e sulle reti
4) strategie di layered security

Swiss cheese model



Tendere verso
zero trust

I vettori di attacco più comuni

1) vulnerabilità su sistemi non patchati o vulnerabili (anche 0-day)
2) campagne di social engineering (*phishing*)

3) credenziali rubate (*infostealer*)

Proteggere la Rete

- Implementare un SOAR
- Monitoring del traffico DNS nord-sud
- Monitoring traffico est-ovest
- XDR sui client
- WAF, IDS, IPS su edge

Attenti a Dave e… **GRAZIE** per l’attenzione!