CONSIGLIO NAZIONALE INGEGNERI

C3i COMITATO ITALIANO INGEGNERIA INFORMAZIONE

Scenario attuale con i dati relativi agli attacchi informatici in Italia nell'ultimo semestre

Ing. Rosario Russo

Ordine degli Ingegneri della Provincia di Ferrara

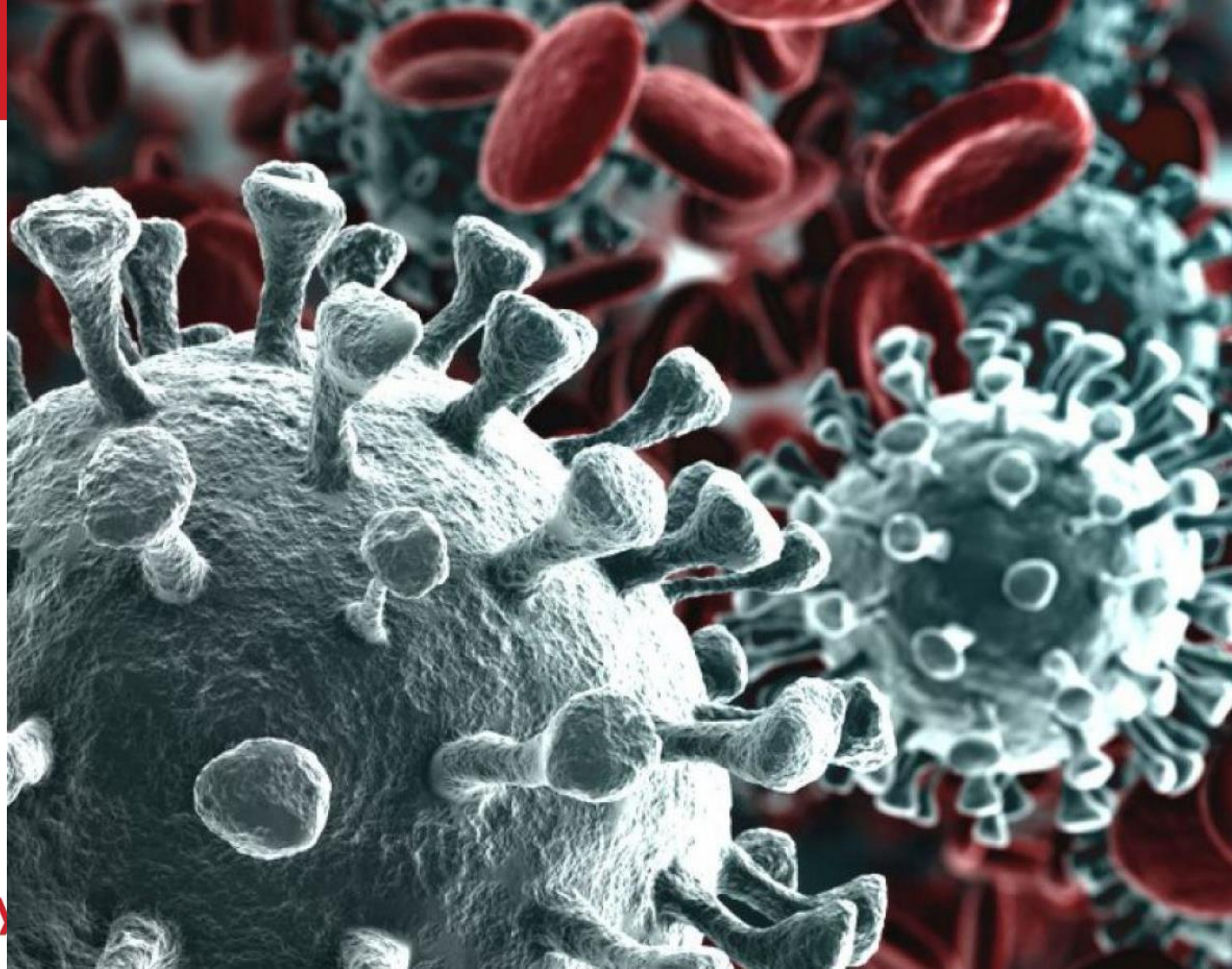
10 dicembre 2020

GdL Cyber Security

CONSIGLIO NAZIONALE INGEGNERI

C3i COMITATO ITALIANO INGEGNERIA INFORMAZIONE

Perché ci fa paura?



GdL Cyber Security

Perché ci fa paura?

- Ci fa paura perché è invisibile e non sappiamo se ci colpirà (e se non ci colpisce il SARS-COV-2, ci saranno migliaia di altri virus o batteri pronti ad attaccarci)
- Non sappiamo come il nostro corpo reagirà al suo attacco e se sarà pronto a difendersi

Why me?

Minima spesa, massima resa

- Gli attaccanti sanno valutare molto meglio dell’impresa il valore dei dati
- Identificano le vittime scandagliando la Rete alla ricerca di vulnerabilità
- Si servono anche di motori di ricerca come Google per individuare servizi esposti e indicizzati per attaccare IoT

You

07/27/2020 17:47:17

So in your message that you left us, you mentioned a "very SPECIAL PRICE" if we reached out to you within 2 days, which we did. There's no way that $10M is a "very SPECIAL PRICE" right?

07/27/2020 18:07:05

Support

This price isn't a Special price, correct! However it is a standard amount for company of your size and it's probably much cheaper than lawsuits expenses, reputation loss caused by leakage.
Yes we did offered a special price and you are eligible for it, so if you are ready to process the payment promptly, we can make a step forward to your direction and give you a discount.

Customer care dei cybercriminali

Cybercrime vs Spionaggio

- Ricerca delle vulnerabilità cercando di «sparare nel mucchio»
- Minima spesa, massima resa
- Predisposizione di strumenti automatici
- Difficoltà di rilevare l'attacco: **bassa**
- Tempo di attacco: **pochi minuti**
- Danno: **medio-alto**
- Costo per proteggersi: **poco**

- Attacco studiato per lungo tempo contro una vittima ben definita e attentamente selezionata
- Risorse enormi a disposizione
- Utilizzo di strumenti studiati e sviluppati *ad hoc*
- Difficoltà di rilevare l'attacco: **molto alta**
- Tempo di attacco: mesi
- Danno: **altissimo**
- Costo per proteggersi: **molto alto**

You cannot defend, what you do not see

- Gli attaccanti sanno tutto di noi e di come sfruttare meglio di noi i dati che abbiamo
- Una determinazione sbagliata della superficie d'attacco può comportare falle nella protezione
- Dobbiamo essere consapevoli che il pericolo maggiore è quello più facilmente risolvibile
- Dobbiamo però fronteggiare una minaccia che è molto cambiata ultimamente

Unicredit (marzo 2020)

GEOX – Giugno 2020 Domenica -

SICUREZZA INFORMATICA

Enel sotto attacco: rubati 5 TB di dati dagli hacker, riscatto di 14 milioni

Un gruppo di hacker afferma di aver rubato quasi 5 TB di dati a Enel, ma la società ha la bocca cucita

28 Ottobre 2020

Il **Gruppo Enel**, leader italiano ed internazionale nella produzione di energia elettrica, è di nuovo sotto **attacco hacker**. Per la precisione un attacco "*ransomware*", con il virus **NetWalker** che è stato infiltrato nella rete dell'azienda e ha criptato circa **5 TeraByte di dati riservati**. Gli hacker hanno chiesto un riscatto di **14 milioni di dollari** per decriptare i file e minacciano di renderne pubblico il contenuto.

Nessuna dichiarazione in merito da parte di Enel Group, mentre gli hacker stanno parlando e anche molto: per la precisione sul blog dedicato al malware NetWalker che viene pubblicato sul Dark Web ed è accessibile tramite browser TOR. A scoprire il post in cui gli attaccanti annunciano di aver violato la rete di Enel è stata l'azienda italiana di cybersicurezza **TG Soft**, che lo ha comunicato su Twitter. A giugno 2020 Enel era già stata attaccata con un altro malware, Snake, sempre di tipo ransomware. Questa volta gli hacker hanno anche pubblicato diversi screenshot in cui si vedono le **cartelle dei file criptati**, grazie al quale è possibile intuire quali dati sono stati attaccati.

Dati criptati Enel: cosa contengono

I dati Enel sotto attacco sono di due tipi: una lunga lista di cartelle che sembrerebbero contenere **dati relativi alle centrali elettriche** del gruppo, come quelle di Augusta (SR), Bari, Bastardo (PG), Brindisi, Fusina (VE), e molte altre in Italia e all'estero (in Grecia, Francia, Romania), una cartella chiamata "*Dossier Impianti*", e poi un'altra serie di cartelle che sembrerebbero invece contenere dati non relativi alla produzione di energia ma **dati più strettamente aziendali**.

Che tipo di dati sono? Solo Enel lo sa: potrebbero essere dati riservati sulla produzione di energia elettrica nei singoli impianti, come anche dati che sono già pubblici sul sito del gruppo. Gli hacker, però, per fare **pressione** affermano che "*analizzeranno ogni file in cerca di cose interessanti*" e, **se Enel non paga**, pubblicheranno tutto.

Attacco hacker Enel: la richiesta di riscatto

Come sempre accade in caso di attacco ransomware anche in questo caso è stato richiesto un **riscatto in bitcoin**. Per la precisione gli hacker vogliono da Enel ben 1.234 bitcoin, che al cambio attuale valgono **14 milioni di dollari**.

Di solito, se le aziende ricattate non pagano entro i tempi stabiliti, chi mette a segno questi attacchi allo scadere del tempo concesso procede a pubblicare parte dei dati rubati per fare **ulteriore pressione** sulle vittime.

Enel, l'attacco di giugno 2020

Non è la prima volta che Enel viene presa di mira dagli hacker. Recentemente è successo **il 7 giugno scorso** quando, improvvisamente, la rete informatica interna dell'azienda ha iniziato ad accusare problemi. Immediatamente si è scoperto che i problemi erano causati da un **ransomware** (**Snake**, chiamato anche **Ekans**) e, per questo, la rete interna fu isolata per contenere l'eventuale fuga di dati.

ottobre 2020 – 14M$

(fonte: tecnologia.libero.it)

Luxottica – Domenica 20 settembre 2020 – 2 GB

Luxottica, pubblicati sul dark web

key4biz.it/luxottica-pubblicati-sul-dark-web-i-dati-rubati-dal-rece...

App | VoIP | Security | WebMail Aruba | Interessanti! | Bookmarks | GDPR | Altri Preferiti

key4biz

Luxottica, pubblicati sul dark web i dati rubati dal recente attacco hacker

di **Piero Boccellato** | 23 Ottobre 2020, ore 12:00

ERSECURITY

Pubblicati sul dark web i dati sensibili rubati nel recente attacco hacker avvenuto nei confronti di Luxottica. Se il data breach dovesse risultare vero, l'azienda rischia una multa per violazione del GDPR.

r molti, la reazione di **Luxottica** all'attacco hacker subito di recente, era stata da manuale. Ma secondo **lisseus**, esperto indipendente di sicurezza informatica, non sembra affatto così.

traverso un tweet, Odisseus fa sapere che il gruppo criminale **Nefilim** ha pubblicato sul **dark web 2 GB** di ti che sembrano provenire dall'hacking dello scorso 20 settembre ai danni della multinazionale.

Pubblicati i dati sul dark web!

Campari – Domenica 1 novembre 2020 – 15M$ - 2 TB

cybersecurity360.it/nuove-minacce/ransomware/campari-furto-dati-con-minaccia-perche-ce-boom-di-questi-attacchi-e-come-difendersi/

App VoIP Security WebMail Aruba Interessanti! Bookmarks GDPR Simple Long Polling... CASA DI LEGNO! Dynamic System - I... Search for roy

RANSOMWARE

Campari, attacco hacker con furto dati: perché sta capitando a tante aziende e come difendersi

Anche Campari colpita dalla tecnica del doppio attacco, due terabyte di dati trafugati e la minaccia di pubblicarli se l'azienda non pagherà 15 milioni di dollari. Vediamo perché c'è un boom del fenomeno (Geox, Luxottica, Enel...) e che deve fare un'azienda per difendersi

HELLO Campari_Group !

If you reading this message, it means your network was PENETRATED and all of your files and data has been ENCRYPTED

by R A G N A R L O C K E R !

****

YOU HAVE TO CONTACT US via LIVE CHAT IMMEDIATELY TO RESOLVE THIS CASE AND MAKE A DEAL
(contact information you will find at the bottom of this notes)

!!!!! WARNING !!!!!

DO NOT Modify, rename, copy or move any files or you can DAMAGE them and decryption will be impossible.
DO NOT Use any third-party or public Decryption software, it also may DAMAGE files.
DO NOT Shutdown or Reset your system, it can DAMAGE files

There is ONLY ONE possible way to get back your files - contact us via LIVE CHAT and pay for the special DECRYPTION KEY !
For your GUARANTEE we will decrypt 2 of your files FOR FREE, to show that it Works.

Don't waste your TIME, the link for contact us will be deleted if there is no contact made in closest time and you will NEVER restore your DATA.
!!! HOWEVER if you will contact us within 2 day since get penetrated - you can get a very SPECIAL PRICE.

! WARNING !
! Whole your International Corporate Network was fully COMPROMISED !

We have BREACHED your security perimeter and get access to every server of company's Network in different countries across all your international offices.
So we has DOWNLOADED more than 2TB total volume of your PRIVATE SENSITIVE Data, including:
-Accounting files, Banking Statements, Government letters, Licensing certificates
-Confidential and/or Proprietary Business information, Celebrity Agreements, Clients and Employees Personal information (including Social Security Numbers, Addresses, Phone numbers and etc.)
-Corporate Agreements and Contracts with distributors, importers, retailers, Non-Disclosure Agreements
-Also we have your Private Corporate Correspondence, Emails and Workbooks, Marketing presentations, Audit reports and a lot of other Sensitive Information

If NO Deal made than all your Data will be Published and/or Sold through an auction to any third-parties

- There are some screenshots just as a proofs of what we got on you. (you can find more on Temporary Leak Page)
Screenshots:

Attacco hacker a un ospedale in

repubblica.it/tecnologia/sicurezza/2020/09/18/news/germania_donna_muore_durante_attacco_ransomware_all_ospedale-2677352...

App | VoIP | Security | WebMail Aruba | Interessanti! | Bookmarks | GDPR | Simple Long Polling... | CASA DI LEGNO! | Dynamic System - I...

Germania: donna muore durante attacco ransomware all'ospedale

di ALESSANDRO LONGO

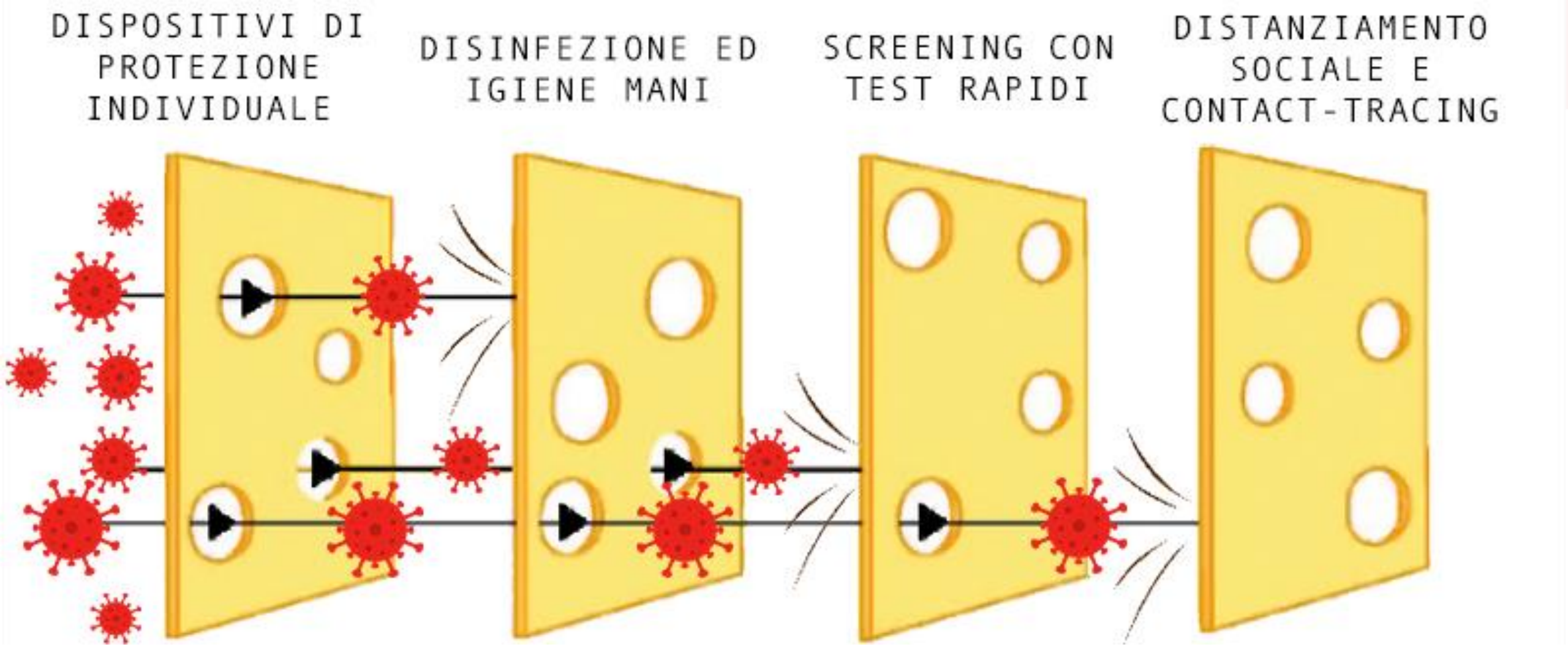
E' il primo decesso legato a cyberattacco contro una struttura sanitaria. La paziente, destinata all'ospedale di Duesseldorf, è stata trasferita ed è deceduta per il ritardo delle cure. Nel 2017 Wannacry contribuì ad un incremento della mortalità ospedaliera

18 SETTEMBRE 2020

2 MINUTI DI LETTURA

Una donna è morta a causa di un attacco informatico che ha bloccato la rete dell'ospedale di Duesseldorf, in Germania, il 10 settembre. Lo riportano i media tedeschi, definendolo il primo caso di morte legato direttamente al ransomware, codice malevolo che blocca i computer delle vittime a scopo di ricatto. La paziente, al momento identificata come una donna che necessitava di cure mediche urgenti, è deceduta dopo essere stata reindirizzata in un ospedale della città di Wuppertal, a più di 30 km dalla sua destinazione iniziale, che era appunto l'ospedale universitario di Duesseldorf. La struttura non ha potuto accogliere la paziente a causa di un blocco informatico ma il trasferimento è stato fatale per la donna deceduta in seguito al ritardo delle cure

Primo morto in seguito ad attacco informatico (settembre 2020)



Che cosa possiamo fare?

Cyber-hygiene

- Occorre intervenire su più fronti
  - Difese perimetrali
  - Antivirus e sistemi di protezione avanzata
  - Backup aggiornato e offline
  - Password sempre diverse e memorizzate in un programma apposito
  - Identico livello di protezione di tutti i dispositivi
  - Comportamenti corretti (PC lavoro vs PC casa vs PC figli)
  - Diffidenza e paranoia
  - Consapevolezza e formazione

GRAZIE!

studio@rosariorusso.it