Rapporto

2021

sulla sicurezza ICT
in Italia

Indice

ASTREA Advanced Security, Training Research, Events Agency
Via Copernico, 38 - 20125 Milano

Prefazione

Un anno fa in queste ore scrivevo la prefazione del Rapporto e riflettevo su quanto stava accadendo.
Era l'inizio del lockdown e l'esplosione della pandemia mondiale.
Scrivevo che quanto stava accadendo avrebbe portato alla comprensione dell'importanza del digitale.

Ed è quello che è accaduto.
Il digitale è diventato centrale per la sopravvivenza di aziende e pubbliche amministrazioni, per garantire un minimo di continuità alle attività scolastiche, per rimanere in contatto con amici e parenti.
Tanti, troppi casi di attacchi riusciti ci hanno anche permesso di riflettere ancora sulla importanza della sicurezza informatica. Non esiste digitalizzazione possibile senza sicurezza.

L'anno passato, con gli attacchi agli ospedali, ha reso ancora più evidente che i criminali non hanno alcuna remora, nessuna etica. Tutto quello che può essere fatto per ottenere denaro sarà fatto. Con buona pace dell'impatto degli attacchi sulla vita delle persone.
Abbiamo però anche assistito a un anno in cui nonostante il crollo epocale del PIL la spesa in sicurezza informatica è aumentata del 4%, con tante, tantissime aziende e pubbliche amministrazioni che hanno approfittato del lockdown per fare awareness e formazione in modalità remota anche sui temi della sicurezza cyber.
Abbiamo avuto l'occasione di avere ospiti e di interloquire più volte con le massime Autorità italiane ed europee del settore.

Si tratta del rovescio della medaglia della pandemia.

Pur nella tragedia degli oltre centomila morti solo in Italia, ci sono tante cose che sono state fatte per migliorare la vita delle persone e che hanno un valore immenso nel contesto in cui viviamo.
Si è scoperto che possiamo fruire di servizi che prima erano riservati a pochissimi in presenza.

Non so se il prossimo anno potremo fare un Security Summit incontrandoci nuovamente. Forse saremo ancora in modalità remota. Ma quello di cui sono sicuro è che quando si potrà di nuovo vedersi, lo faremo. Ma manterremo tante delle modalità che oggi stiamo scoprendo. Quanto valgono due ore non passate in macchina nel traffico in termini di attività che si possono svolgere?

Sfrutteremo tutti molto di più le tecnologie digitali rispetto al pre-pandemia.
E se sarà così, dobbiamo progettare un nuovo modo di vivere. Un modo di vivere in larga parte imperniato sul digitale che dovrà necessariamente essere progettato in modo sicuro.
Come CLUSIT, con il nostro nuovo Direttivo e il nuovo Comitato Scientifico, con la passione e la partecipazione di decine fra i più autorevoli esponenti del nostro settore, proveremo a fare la nostra parte.

*** *** ***

Il rapporto CLUSIT che leggerete è il frutto del lavoro di un pool di esperti che ha analizzato e confrontato una ampia serie di fonti. È forse inutile dire, come sempre, che l'ultimo anno è stato il peggiore di tutti. È il trend in atto da anni e non deve stupire. Forse una riflessione si può fare sull'aumento dei casi in Europa. È forse l'effetto degli obblighi di notifica dei data breach che permette l'emersione del fenomeno nella sua vera ampiezza?

E allora buona lettura del Rapporto che avete fra le mani.
Il risultato dello sforzo di un team di altissimo livello che da anni lavora per sensibilizzare il mondo pubblico e privato sui temi della sicurezza informatica.
Quest'anno, peraltro, in un contesto di particolare complessità.

Ringrazio, a nome di tutti gli Associati e di tutti coloro che lo leggeranno, i Colleghi che hanno dedicato tempo e sforzi alla stesura del Rapporto Clusit 2021.
Oltre 70.000 copie scaricate e più di 300 articoli pubblicati nel 2020, sono l'evidenza della rilevanza del rapporto CLUSIT ed è quindi importante diffonderlo, leggerlo, farlo conoscere, perché solo dalla consapevolezza può derivare la conoscenza del problema, la capacità di adottare scelte idonee e quindi la sicurezza nostra e di tutti.

Buona lettura.

Gabriele Faggioli
Presidente CLUSIT

Introduzione al Rapporto

Il Rapporto CLUSIT 2021 inizia con una panoramica degli eventi di cyber-crime più significativi avvenuti a livello globale nel 2020, confrontandoli con i dati raccolti nei 4 anni precedenti. Nell'anno della pandemia si registra il record negativo degli attacchi informatici: a livello globale sono stati infatti **1.871 gli attacchi gravi di dominio pubblico** rilevati nel corso del 2020, ovvero con un impatto sistemico in ogni aspetto della società, della politica, dell'economia e della geopolitica. In termini percentuali, **nel 2020 l'incremento degli attacchi cyber a livello globale è stato pari al 12%** rispetto all'anno precedente; negli ultimi quattro anni il trend di crescita si è mantenuto pressoché costante, facendo segnare un aumento degli attacchi gravi del 66% rispetto al 2017. Proprio la **pandemia** ha caratterizzato il 2020 per andamento, modalità e distribuzione degli attacchi: il 10% degli attacchi portati a termine a partire da fine gennaio è stato a tema Covid-19. In particolare, i cybercriminali hanno sfruttato la situazione di disagio collettivo, nonché di estrema difficoltà vissuta da alcuni settori - come quello della produzione dei presidi di sicurezza (ad esempio, delle mascherine) e della ricerca sanitaria - per colpire le proprie vittime. Diverse operazioni di spionaggio sono state compiute a danno di organizzazioni di ricerca correlate con lo sviluppo dei vaccini. Nello specifico settore della **Sanità**, il 55% degli attacchi a tema Covid-19 è stato perpetrato a scopo di cybercrime, ovvero per estorcere denaro; con finalità di "Espionage" e di "Information Warfare" nel 45% dei casi. Gli attacchi registrati nel 2020 sono stati classificati anche in base ai loro differenti livelli di impatto, sulla base di una valutazione dei danni dal punto di vista geopolitico, sociale, economico (diretto e indiretto) e di immagine. Nel 2020 gli attacchi rilevati e andati a buon fine hanno avuto nel 56% dei casi **un impatto "alto" e "critico"**; il 44% è stato di gravità "media".

Tra i settori colpiti da attacchi cyber gravi negli ultimi dodici mesi, spiccano (in ordine decrescente): "**Multiple Targets**": 20% del totale. Si tratta di attacchi realizzati in parallelo verso obiettivi molteplici, spesso indifferenziati, che vengono colpiti "a tappeto" dalle organizzazioni cyber criminali, secondo una logica "industriale". Gli attacchi verso questa categoria di obiettivi sono tuttavia in calo del 4% rispetto al 2019; **Settore Governativo, Militare, Forze dell'Ordine** e **Intelligence**, che hanno subìto il 14% degli attacchi a livello globale; **Sanità**, colpita dal 12% del totale degli attacchi; **Ricerca/Istruzione**, verso cui sono stati rivolti l'11% degli attacchi; **Servizi Online**, colpiti dal 10% degli attacchi complessivi. Sono cresciuti, inoltre, gli attacchi verso Banking & Finance (8%), Produttori di tecnologie hardware e software (5%) e Infrastrutture Critiche (4%).
Abbiano inoltre registrato nel corso degli ultimi dodici mesi un incremento di attacchi veicolati tramite l'abuso della **supply chain**, ovvero tramite la compromissione di terze parti, il che consente poi a criminali e spie di colpire i contatti (clienti, fornitori, partner) dell'obiettivo, ampliando notevolmente il numero delle vittime e passando più facilmente inosservati. Nel 2020 gli attacchi cyber sono stati messi a segno prevalentemente utilizzando **Malware** (42%), tra i quali spiccano i cosiddetti **Ransomware** - una tipologia di malware che limi-

ta l'accesso ai dati contenuti sul dispositivo infettato, richiedendo un riscatto - utilizzati in quasi un terzo degli attacchi (29%), la cui diffusione è in significativa crescita (erano il 20% nel 2019), sia in termini assoluti che in termini di dimensioni dei bersagli e di ammontare dei danni. Seguono le "tecniche sconosciute" (in riferimento alle quali prevalgono i casi di Data Breach, per il 20%), mentre **Phishing & Social Engineering** continuano ad essere la causa di una buona parte degli attacchi (15% del totale); si registra inoltre negli ultimi dodici mesi una crescita degli attacchi sferrati per mezzo di vulnerabilità note (+ 10%), precedentemente in calo (-29% nel 2019 rispetto al 2018).

Ci siamo avvalsi anche quest'anno dei dati relativi agli attacchi rilevati dal **Security Operations Center (SOC) di FASTWEB**, che ha analizzato la situazione italiana sulla base di oltre 36 milioni di eventi di sicurezza.
Data la nuova crescita del fenomeno Ransomware, pubblichiamo un'analisi specialistica sul **Ransomware in Italia** e sugli attacchi mirati "double extortion", a cura di TG Soft.
Segue un'analisi sull'**Email Security** e sui trend italiani, a cura di Libraesva.

Anche in questa edizione riportiamo uno studio nuovamente realizzato da ricercatori dell'Università degli Studi di Bari e di Exprivia sullo **stato della cybersecurity nel sud d'Italia**.
L'analisi degli attacchi in Italia è poi completata dalle rilevazioni e segnalazioni della **Polizia Postale e delle Comunicazioni**.

Presenteremo a questo punto l'abituale capitolo dedicato al settore FINANCE, con un'analisi sugli "**Elementi sul Cyber-crime nel settore finanziario in Europa**", a cura di IBM ed un contributo inedito del CERT di Banca d'Italia.
Quest'anno abbiamo aggiunto un capitolo sulla **Supply Chain Security**, che comprende anche un contributo sulla maturità delle organizzazioni in Italia, a cura dell'**Osservatorio Cybersecurity & Data Protection della School of Management del Politecnico di Milano**.

Questi saranno infine i temi trattati nella sezione FOCUS ON:
- "**Ahi Ahi Ahi IoT!**", di Alessandro Vallega e Roberto Obialero.
- "**Attacchi e minacce alle Infrastrutture Critiche Italiane**", a cura di Fortinet.
- "**La metà dei CISO italiani crede che la guerra informatica sia una minaccia imminente per le loro aziende**", a cura di Bitdefender.
- "**La sicurezza dei dati Cloud nel 2020**", a cura di Netwrix.
- "**Business Continuity & Cyber Security: la necessità di un approccio convergente**", di Federica Maria Rita Livelli.

Ransomware 2020 in Italia – Dalla pesca a "strascico" agli attacchi mirati double extortion… ma non solo

[A cura di Enrico e Gianfranco Tonello, TG Soft]

Nel 2020, anche in Italia, i Ransomware, malware in grado di cifrare i file di dati con l'obiettivo di richiederne un riscatto in denaro generalmente attraverso pagamenti in crypto valute (BTC Bitcoin o altre), per raggiungere l'obiettivo ed eludere i sistemi di difesa di cui gli enti ed imprese si sono progressivamente muniti, hanno iniziato anche ad esfiltrare i file di dati delle vittime minacciandone la diffusione pubblica.

I ransomware fino a qualche tempo fa si "limitavano":
- a cifrare i file di dati;
- a tentare di cancellare i file di ripristino dei più comuni sistemi di backup se, erano, in qualche modo accessibili;
- alla cancellazione delle copie Shadow.

L'obiettivo era quello di costringere la malcapitata vittima al pagamento del riscatto per ottenere la chiave di de-cifratura dei file e riconquistarne l'accesso.

Già dal 2019, o forse prima, si sono iniziati a vedere attacchi ransomware che, oltre a cifrare i file, ne facevano anche una copia di "sicurezza" con il loro trasferimento sui computer dei cyber criminali minacciando di procedere alla loro diffusione pubblica e/o metterli all'asta nel dark web per la vendita al miglior offerente.
Questa tecnica di "doppia" estorsione viene oggi chiamata **double extortion**.

Tutto questo per indurre la vittima a pagare il riscatto non solo per la decifratura, ma anche (e soprattutto) per evitare di vedere i propri dati aziendali, contabilità, dati della clientela, progetti, segreti industriali e quant'altro diventare di pubblico dominio. Questa situazione oltre al danno d'immagine, nel caso di diffusione di dati personali e ancora di più se sensibili, può essere sanzionata pesantemente dal Garante Privacy in attuazione al GDPR che, è bene ricordarlo, possono arrivare fino al 4% del fatturato aziendale WW (World Wide) fino ad un massimo di 20 milioni di €.

Le modalità di attacco Ransomware più comuni

Come già noto, nel passato, gli attacchi Ransomware avvenivano principalmente sfruttando l'ingegneria sociale dove attraverso una "semplice" comunicazione via e-mail i cyber malfattori tentavano di far cadere il malcapitato ricevente nella loro trappola. Questa metodologia è andata scemando nell'ultimo periodo, prediligendo l'attacco mirato ad importanti aziende.

I vettori di infezione dei ransomware nel 2020 sono stati i seguenti:
1. Campagna Malspam per attacchi massivi:
   a. aprire un allegato dove da questo si scatenava nell'immediatezza la cifratura dei file;
   b. cliccare su un link che portava all'esecuzione di un file dal quale si attivava il processo di cifratura malevolo.
2. Navigazione su siti compromessi
3. Attacchi mirati:
   a. accesso via RDP (Remote Desktop Protocol).
4. Vulnerabilità della rete aziendale.

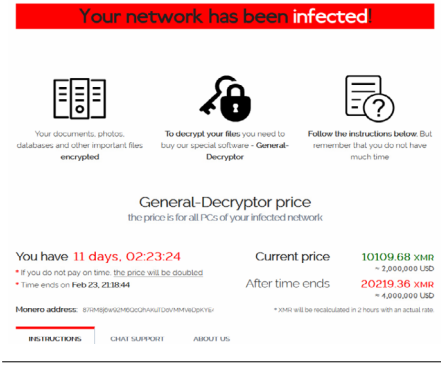
Già nel 2017 si erano iniziati a vedere attacchi un po' più sofisticati che, non solo attraverso le e-mail e la "complicità" di un utente disattento, procedevano attaccando PC o Server esposti sul Web ove fossero presenti vulnerabilità non "patchate" sfruttandole per inoculare malware. Attraverso lo spostamento laterale si propagavano poi nella rete locale per cifrare il maggior numero di computer possibili.
Un'altra metodologia utilizzata in quegli anni è stata la "Supply Chain" che attraverso aggiornamenti di software legittimi veicolavano malware.
Tra gli esempi più noti ricordiamo WannaCry (2017 vulnerabilità EternalBlue) e il ransomware NotPetya (aggiornamento software MEDoc e vulnerabilità EternalBlue), attribuito al governo della Russia.

Oltre a questo i cyber ricattatori si sono mossi andando ad utilizzare tecniche ancora più sofisticate e, seppur continuando con la "pesca" a strascico, hanno intuito che per poter cercare di ottenere riscatti elevati era necessario procedere con attacchi mirati, certamente più complessi, ma che se andati a segno potevano portare a richiedere riscatti ben più corposi. Non più "solamente" qualche centinaia o migliaia di €uro in crypto valuta ma arrivando anche a richiedere centinaia di migliaia di €uro/U$D fino ai casi più estremi, superando il milione di dollari/euro soprattutto nel caso di esfiltrazione di dati.

Due casi recentissimi di attacchi sferrati con il medesimo ransomware #**REvil** aka #**SodinoKibi** praticamente in contemporanea:
(1) attacco via RDP (Remote Desktop Protocol) di sola cifratura file ai danni di un'azienda italiana, che ha visto richiedere:
   - poco più di 963 XMR {Monero} che al cambio del 12/02/2021 corrispondevano circa 200mila U$D / 165mila € se pagato entro le prime 48 ore;
   - riscatto che poi raddoppia passando a quasi 1927 XMR {Monero} che, al cambio del 12/02/2021, equivalevano a 400mila U$D / 330mila €!

(2) attacco ai danni di un'azienda francese con sedi operative anche in Italia che, oltre a cifrare i file di dati segnala, nella richiesta di riscatto anche l'esfiltrazione degli stessi. Il riscatto richiesto è di 2 milioni di dollari che raddoppierà a 4 milioni dopo il 23 febbraio.

(1) *Riscatto Sodinokibi solo cifratura file Fonte: CRAM di TG Soft*



(2) *Riscatto Sodinokibi cifratura+esfiltrazione file - Fonte: CRAM di TG Soft*

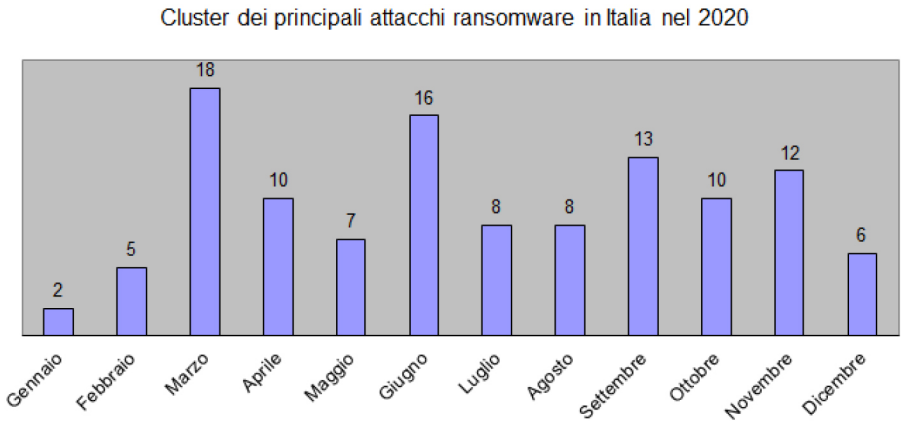
Come si può notare si tratta di due attacchi avvenuti con lo stesso ransomware, ma su due aziende diverse. Il riscatto richiesto, seppur rimanendo importante e raddoppiando dopo una certa data, nel caso della sola cifratura, l'importo richiesto è dell'ordine di qualche centinaia di migliaia di dollari (200/400mila U$D) mentre nel caso di doppia estorsione (double extortion: cifratura + esfiltrazione di dati) la richiesta di riscatto è superiore di un ordine di grandezza passando da qualche centinaia di migliaia di dollari a Milioni di dollari (da 2 a 4 Milioni di U$D).

I Ransomware circolanti in Italia nel 2020

Anche nel 2020, come nei primi mesi del 2021 i Ransomware non hanno mollato la presa "mixando", come detto, campagne di malspam indifferenziate sull'utenza ed attacchi specifici mirati sfruttando gli accessi RDP maldestramente lasciati esposti o vulnerabilità della rete aziendale.

Classificazione dei più importanti attacchi ransomware in Italia

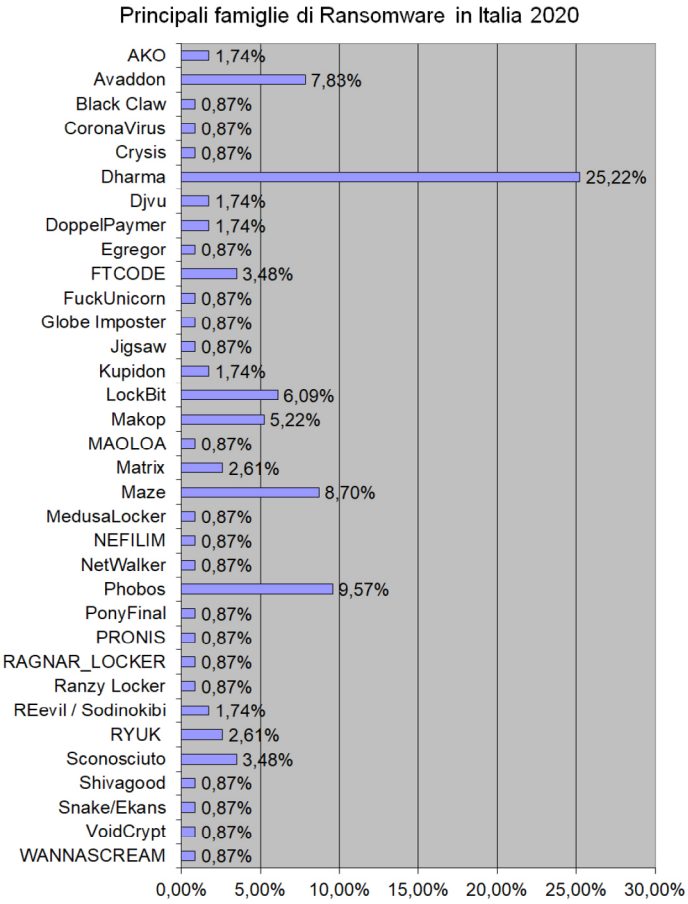
Sono stati verificati e classificati non meno di 115 cluster di attacchi ransomware sia di sola cifratura come anche di esfiltrazione dati (double extortion).



Fonte: Centro Ricerche AntiMalware #CRAM di TG Soft Cyber Security Specialist

Dall'analisi del grafico dei Cluster per mese possiamo notare che vi è un picco nel mese di marzo quando in fretta e furia, a causa dell'emergenza epidemiologia Covid-19, molte aziende sono state costrette, causa provvedimenti governativi (DPCM) che hanno introdotto il *lockdown*, a mettere in tutto o in parte in SMART Working / Lavoro Agile molti dipendenti.

Lo SMART Working / Lavoro Agile ha, di fatto, "autorizzato" i dipendenti ad utilizzare i propri computer fissi o portatili personali che, a causa della vetustà e/o del poco manutenzionamento o per la mancanza di software di protezione aggiornati essendo collegati via internet ai computer della rete aziendale sono diventati, in molte occasioni, la porta d'ingresso di questi attacchi.



**Sconosciuto ➔ Casi di attacchi ransomware, le cui vittime non hanno reso nota la tipologia del ransomware da cui sono stati colpiti. Fonte: Centro Ricerche AntiMalware #CRAM di TG Soft Cyber Security Specialist.*

Come si evince dal grafico sono non meno di trentaquattro le famiglie/tipologie di ransomware distinte che sono state utilizzate per attacchi agli utenti italiani di cui una di queste tipologie è, quasi certamente, di realizzazione italiana o di re-ingegnerizzazione italiana. Si tratta del ransomware FuckUnicorn scoperto/utilizzato nel secondo trimestre 2020. Questo esemplare "autoctono" ha sfruttato l'emergenza epidemiologica Covid-19 per sferrare i suoi attacchi.

Dharma è il ransomware che è stato utilizzato maggiormente dai cyber criminali per attaccare l'utenza italiana. Più di ¼ degli attacchi è avvenuto utilizzando questo agente patogeno.
Phobos, che viene considerato il successore di Dharma in particolare negli attacchi in modalità RDP è stato utilizzato in poco meno del 10% degli attacchi.
Maze, con il suo 8,70% conquista la terza piazza che, visto che si tratta di un ransomware utilizzato per lo più per attacchi mirati di cifratura+esfiltrazione dati (double extortion) è un "ottimo" risultato.
Avaddon, con il suo 7,83% si piazza solo in quarta posizione ma, visto che viene utilizzato con varie modalità di diffusione sia attraverso campagne Malspam come anche per attacchi mirati è ipotizzabile che, nel 2021, possa recuperare qualche posizione.
LockBit, con il suo 6,09% guadagna la quinta posizione.

Ransomware 2020 in Italia ➔ primo trimestre 1 gennaio – 31 marzo

In questo trimestre [3] [4] [5] si è rilevata una flessioni di attacchi ransomware di **Ryuk** [6] e **FTCode** [7] molto attivi nel 2019. Sebbene, dal mese di gennaio fino a circa metà febbraio siano continuate le campagne di malspam di Emotet con la veicolazione anche di **Trickbot**, quest'ultimo però non ha attivato lo stadio dell'attacco ransomware di **Ryuk**.

A parziale compensazione di queste "mancanze" sono stati registrati attacchi di nuovi attori nel mondo dei ransomware:
- **AKO** riconducibile ad una variante di **MedusaLocker**
- **PrOnIs**, molto probabilmente deriva da "**0p3nSOurc3 X0r157**"
- **CoronaVirus**
- **Jigsaw**

In questa prima parte dell'anno sono stati riscontrati cluster di attacchi che hanno visto l'utilizzo dei seguenti ransomware:

- Phobos	- AKO	- PrOnIs	- Dharma	- FTCode
- MedusaLocker	- Jigsaw	- Ryuk	- CoronaVirus	- Maze

Nel trimestre gli attacchi ransomware sono stati sferrati attraverso le modalità:
- RDP (Remote Desktop Protocol) [8];
- Drive-By-Download.

Segnaliamo che gli attacchi **RDP** avvenuti a gennaio che hanno permesso un accesso abusivo al sistema per eseguire direttamente il ransomware, nello specifico i cyber criminali hanno utilizzato nella maggior parte dei casi **Phobos** che deriva e sta raccogliendo l'eredità di **Dharma** il quale aveva la peculiarità di essere uno dei preferiti dai cyber malfattori negli attacchi **RDP**.
In marzo rispetto a febbraio si rileva un aumento degli attacchi via RDP.

L'incremento degli attacchi è probabilmente riconducibile al lockdown causato dal Covid-19 che ha comportato un maggiore utilizzo del protocollo RDP, esponendo l'infrastruttura aziendale a rischi di attacchi attraverso gli accessi esterni permettendo ai cyber criminali attacchi ransomware diretti.
Per la massiva offensiva degli attacchi via **RDP**, in marzo, i cyber criminali hanno utilizzato **RYUK, Phobos, Dharma** e **MedusaLocker.**
Per gli attacchi double extortion il **Maze** ha rivendicato l'attacco ad un'importante azienda meccanica lombarda.

Ransomware 2020 in Italia ➔ secondo trimestre 1 aprile – 30 giugno

In Italia i principali attacchi ransomware [11] [12] [13] sono giunti da:

- REvil aka Sodinokibi	- Makop	- Dharma	- LockBit
- FuckUnicorn	- Kupidon	- Avaddon	- Maze

Le principali new entry sono state: **Makop, LockBit** e **Avaddon.**

Prosegue il trend di progressivo incremento degli attacchi via RDP, dovuto al lockdown causato dall'emergenza epidemiologica Covid-19 che, come già segnalato, ha obbligato molti italiani a lavorare da casa, lasciando esposti gli accessi esterni della rete aziendale ad attacchi.
I cyber malfattori, in questo trimestre, per gli attacchi RDP hanno preferito utilizzare **Dharma**. A maggio, in Italia, a dare man forte a Dharma negli attacchi RDP si è notato anche l'utilizzo del ransomware **LockBit**.
Inoltre, sembrerebbe che gli autori di **LockBit** si siano affiliati a quelli del **Maze** per condividere le loro piattaforme di data leak. La richiesta di riscatto del LockBit varia dalla tipologia della vittima, con riscatti richiesti da 1600 U$D in su.

Il nuovo ransomware **Avaddon** [9] ha utilizzato diversi vettori d'infezione per attaccare l'utenza italiana:

- **Phorpiex** (worm, che si è diffuso in Italia attraverso campagne di malspam a giugno). Le vittime infettate entrano a far parte della botnet Phorpiex, che ha diffuso il ransomware Avaddon;
- **Campagne malspam dirette**. Il 30 giugno Avaddon è stato distribuito con una campagna malspam diretta che aveva per oggetto "*Notifica (A2QCS) ufficiale riguardanti possibili violazioni*", con allegato un documento Excel che scaricava direttamente il ransomware.

Un'altra new entry tra i ransomware che hanno attaccato l'Italia nel mese di giugno è **Kupidon.**
Gli attacchi di Kupidon analizzati sono avvenuti via RDP. Il riscatto richiesto era di 1200 $ (dollari USD) in BTC (Bitcoin). La gang dei cyber criminali è probabilmente di origine russa dall'indirizzo email (yandex.ru) visibile nella loro home page.

Per quanto riguarda l'utenza italiana colpita da attacchi double extortion (cifratura & esfiltrazione file), il ransomware **Maze** ha rivendicato gli attacchi a:

- Studio di Architettura e Design
- Primaria Società di costruzioni generali

Nello stesso periodo, a livello mondiale, Maze ha colpito grandi produttori elettronici come LG e Xerox.
A giugno due grandi società italiane, primaria società energetica e primaria società produttrice di calzature, sono state colpite da attacchi informatici.
La società del settore energetico è stata attaccata domenica 7 giugno dal ransomware **Snake/Ekans**, che in precedenza aveva colpito la multinazionale giapponese Honda.

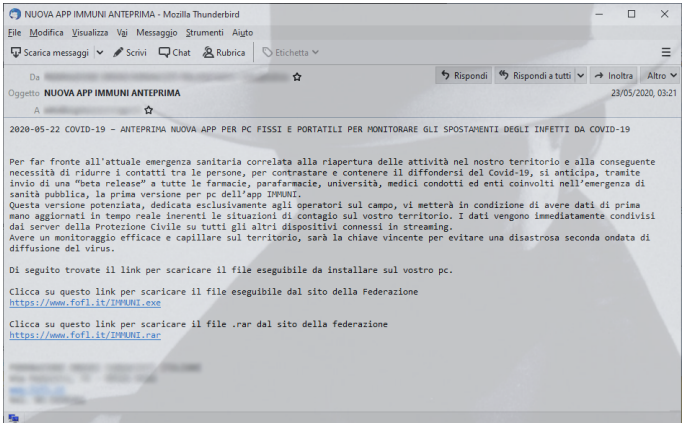
Per quanto riguarda l'attacco subito dalla primaria società del ramo calzaturiero, che è avvenuto domenica 14 giugno, non sono state rilasciate informazioni sulla tipologia di ransomware utilizzato.

FUCKUNICORN – Il ransomware italiano

Il 23 maggio 2020 è stata avviata una campagna malspam in italiano con oggetto "**NUOVA APP IMMUNI ANTEPRIMA**".
Il messaggio invitava ad installare nel proprio PC l'app IMMUNI da un link presente all'interno del messaggio, per far fronte all'attuale emergenza epidemiologica del Covid-19.
Il link in realtà scaricava il ransomware denominato **FUCKUNICORN**.

In figura la nuova immagine dello sfondo cambiata dal ransomware **FUCKUNICORN** al termine della cifratura

Fonte: Centro Ricerche AntiMalware #CRAM di TG Soft Cyber Security Specialist



Mentre il Ransomware cifra i file viene mostrata all'utente la seguente schermata di una mappa raffigurante l'infezione da Covid-19:
Il malware contiene diversi indicatori che fanno ipotizzare che la realizzazione del Ransomware sia italiana.

Il riscatto richiesto è di 300 Euro, da versare in cryptovaluta BitCoin.

"La lunga serpe sul bastone di Asceplio si è ribellata, ed una nuova era sta per sopraggiungere! Questa è la vostra possibilità per redimervi dopo anni di peccati e soprusi. Sta a voi scegliere. Entro 3 giorni il pegno pagare dovrai o il fuoco di Prometeo cancellerà, i vostri dati così come ha cancellato il potere degli Dei sugli uomini. Il pegno è di solamente 300 euros, da pagare, con i Bitcoin al seguente indirizzo: 195naAM74WpLtGHsKp9azSsXWmBCaDscxJ dopo che pagato avrai, una email mandarci dovrai. xxcte2664@protonmail.com il codice di transazione sarà la prova. Dopo il pegno pagato riceverai la soluzione per spegnere il fuoco di Prometeo. Andare dalla polizia o chiamare tecnici a niente servirà, nessun essere umano aiutarti potrà."

Contenuto del file del riscatto

Ransomware 2020 in Italia ➔ Terzo trimestre 1 luglio – 30 settembre

Nel terzo trimestre 2020 [14] [15] [16], gli attacchi ransomware continuano ad utilizzare differenti vettori d'infezione (RDP, navigazione su siti compromessi e campagne malspam).

Sono stati monitorati gli attacchi dei seguenti ransomware:

- Globe Imposter
- Black Claw
- LockBit
- DoppelPaymer
- Matrix
- Phobos
- Crysis
- Makop
- WannaScream
- Avaddon

La maggior parte dei ransomware identificati nel 3° trimestre sono stati veicolati attraverso il desktop remoto (RDP) dopo aver guadagnato un accesso abusivo al sistema.

A luglio hanno fatto la loro comparsa in Italia due nuovi ransomware denominati:

- Black Claw
- WannaScream

Gli attacchi di **Black Claw** analizzati sono avvenuti attraverso intrusione via RDP.
Il ransomware durante la cifratura ai file aggiunge l'estensione ".bclaw".
WannaScream utilizza un'infrastruttura di tipo RaaS (Ransomware-as-a-Service) e all'interno della sua configurazione troviamo il parametro "SOLDIER" che contiene l'ID dell'attaccante. Nel sample analizzato l'attaccante era identificato con la sigla "M-k".

A luglio anche la società ENAC (Ente Nazionale per l'Aviazione Civile) è stata colpita da un attacco ransomware. L'attacco molto probabilmente è avvenuto a partire da venerdì 10 luglio e ha colpito alcuni server dell'Ente Nazionale per l'Aviazione Civile, come indicato in un tweet del 12 luglio. Il sito è stato ripristinato parzialmente alle sue funzionalità solamente dal 17 luglio, circa una settimana dopo l'attacco subito.

Ad agosto il gruppo cyber criminale di **REvil** (aka **Sodinokibi**) [10] ha colpito un'azienda italiana distributrice di ricambi auto del modenese chiedendo un riscatto di 125.000 dollari per non far partire l'asta dei dati esfiltrati.

Nel mese di settembre è stata individuata una campagna di malspam atta a veicolare il ransomware della famiglia Avaddon. La campagna di malspam con oggetto "*È stata presentata una citazione a carico della Sua società, in merito a una fattura non dichiarata*", si spacciava come proveniente dall'Agenzia delle Entrate e conteneva un link malevolo che reindirizzava la vittima verso un finto portale dell'Agenzia delle Entrate.

Nel 3° trimestre il gruppo cyber criminale del **Maze** ha attaccato diverse società italiane alle quali, oltre ad operare la cifratura dei file ha effettuato esfiltrazione dati dandone notizia nel loro sito di data leak:

- S.p.A. lombarda distributrice di dispositivi medici
- S.p.A. lombarda leader pressofusione leghe di zinco
- Primaria Fondazione Culturale veneta
- S.r.l. campana gestione rifiuti
- S.p.A. piemontese produttrice film per imballaggi alimentari
- S.p.A. piemontese ramo alimentare distributrice formaggi grattugiati
- Società altoatesina specialista ICT e telecomunicazioni

Nel 3° trimestre DoppelPaymer ha rivendicato l'attacco informatico ad una S.p.A. campana Multiutility fornitrice di energia e telefonia con esfiltrazione di documenti riservati.

A settembre non sono finiti gli attacchi ransomware in Italia.
S.p.A. veneta leader mondiale dell'occhialeria è stata costretta a bloccare la produzione per l'intera giornata del 21 settembre a causa di un attacco del ransomware NEFILIM. Università laziale è stata colpita da un attacco che ha compromesso più di 100 computer.

Ransomware 2020 in Italia ➔ Quarto trimestre 1 ottobre – 31 dicembre

Questo trimestre [17] [18] [19] registriamo un aumento degli attacchi ransomware i principali hanno utilizzato le seguenti tipologie/famiglie:

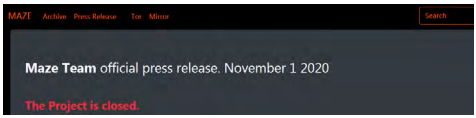
- Dharma
- Avaddon
- VoidCrypt
- RAGNAR_LOCKER
- Makop
- Phobos
- MAOLOA
- Stop/Djvu
- DoppelPaymer
- Ranzy Locker
- ShivaGood
- LockBit
- Matrix
- Egregor

ShivaGood non è un ransomware "nuovo", le prime versione risalgono al 2019.
L'attacco ransomware **Avaddon** questa volta è avvenuto attraverso la navigazione su siti compromessi.
VoidCrypt è stato veicolato attraverso la vulnerabilità della VPN del firewall FortiGate di Fortinet, la quale ha permesso di accedere alla rete locale e quindi di conseguenza ai server tramite RDP.
Gli attacchi attuati dal ransomware **MAOLOA** sono avvenuti attraverso il malware downloader **QakBot** con cui il pc era precedentemente infetto e da cui è stato scaricato il ransomware.
Il ransomware **Stop/Djvu** è stato diffuso attraverso il download di software infetti. La richiesta di riscatto è stata di 490 $.
Anche **Ranzy Locker** è stato diffuso attraverso accesso abusivo via RDP.

Attacchi ransomware double extortion

Il 27 ottobre primaria S.p.A. distributrice di energia è stata colpita da un attacco ransomware con esfiltrazione di dati. A darne notizia è stato il gruppo di cyber criminali di **NetWalker** attraverso un post nel proprio blog nel dark web. Secondo NetWalker avrebbero esfiltrato circa 5 TB di dati.

Il 28 ottobre un'altra S.p.A. italiana multiutility energia e telecomunicazioni è stata colpita da un attacco ransomware con esfiltrazione di dati. A darne notizia questa volta è stato il gruppo di cyber criminali **DoppelPaymer** attraverso un post nel proprio portale nel dark web.



Il mese di novembre inizia con il comunicato stampa di **Maze** che annuncia la chiusura ufficiale del progetto ransomware. Nel comunicato viene rinnegata l'esistenza del cartello Maze e indicato il motivo della chiusura del progetto stesso.

Ad inizio novembre la società italiana tra i leader mondiali del beverage (aperitivi e bevande alcoliche) è stata colpita da un attacco ransomware con esfiltrazione di dati.
A darne notizia questa volta è stato il gruppo di cyber criminali **RAGNAR_LOCKER** attraverso un post nel proprio portale nel dark web.

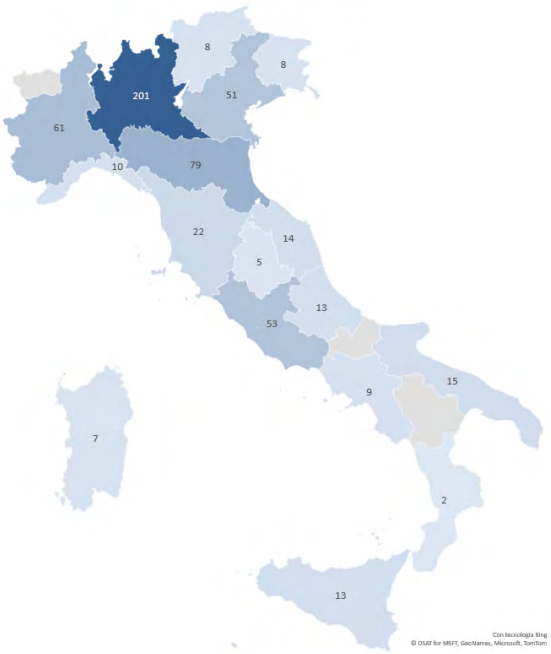
Sempre a novembre il gruppo di cyber criminali di **Egregor** miete un'altra vittima italiana. Si tratta di una coop agricola romagnola che produce ortofrutta biologica.
Il 28 dicembre un'altra società italiana la Snaitech, uno dei principali operatori di gioco legale in Italia, ha annunciato, con un comunicato stampa, di essere stata colpita da un attacco informatico a partire dal 27 dicembre 2020, che ha messo fuori uso il proprio portale.

Vulnerabilità VPN sfruttata per attacchi ransomware

Nel mese di novembre vari cyber criminali hanno pubblicato nei forum del dark web varie liste di IP gestiti dal firewall Fortinet vulnerabili all'exploit CVE-2018-13379.

Il 5 novembre è stato analizzato un attacco ransomware di VoidCript perpetrato sfruttando la vulnerabilità CVE-2018-13379, dove è stato ritrovato un file contenente una lista di 571 IP italiani. In figura la distribuzione geografica di questi IP con target Italia.

Le regioni più colpite sono:
- Lombardia
- Emilia Romagna
- Piemonte
- Lazio
- Veneto



Ditribuzione degli IP per Regione.
Fonte: Centro Ricerche AntiMalware #CRAM di TG Soft

CONCLUSIONI

Il 2020 non è stato solamente un anno difficile a causa della pandemia Covid-19 ma che ha visto i creatori/diffusori di ransomware diventare sempre più agguerriti.
Affinata ormai da anni la corretta implementazione degli algoritmi di cifratura senza particolari errori che non permettono la decifratura senza pagare il riscatto, si sono concentrati sulle tecniche di attacco più efficaci e devastanti dove l'accesso ai PC / Server avviene via RDP o attraverso vulnerabilità della rete aziendale.
L'attacco non si limita alla sola cifratura dei file, ma ne trasferisce una copia per ricattare la vittima anche se questa dovesse essere in grado di ripristinare i file cifrati attraverso, ad esempio, delle copie di backup recenti.
È chiaro che per difendersi da questi attacchi è necessario non solo dotarsi di sistemi di mitigazione che si attivino efficacemente nella fase iniziale dell'attacco e permettano di limitare i danni, ma soprattutto evitare l'esfiltrazione dei dati cioè ridurre le esposizioni di PC e Server agli accessi esterni.

Non è azzardato ipotizzare che il trend-topic degli attacchi ransomware 2021 sarà la double extortion.

Bibliografia

[1] CRAM di TG Soft - *Attacchi #RDP veicolano #Ransomware #REvil aka #Sodinokibi in Italia* - Febbraio 2021
https://twitter.com/VirITeXplorer/status/1360143703906648064?s=1002

[2] CRAM di TG Soft - *Attacco hacker Trigano paralizzata* - Febbraio 2021
https://www.linkedin.com/posts/tg-soft attacco-hacker-trigano-paralizzata-la-activity

[3] CRAM di TG Soft - *Telemetria e statistiche dei virus/malware circolanti in Italia 2020-01* - Febbraio 2020
https://www.tgsoft.it/italy/news_archivio.asp?id=1061

[4] CRAM di TG Soft - *Telemetria e statistiche dei virus/malware circolanti in Italia 2020-02* - Marzo 2020
https://www.tgsoft.it/italy/news_archivio.asp?id=1067

[5] CRAM di TG Soft - *Telemetria e statistiche dei virus/malware circolanti in Italia 2020-03* - Aprile 2020
https://www.tgsoft.it/italy/news_archivio.asp?id=1076

[6] CRAM di TG Soft - *Analisi tecnica del ransomware Ryuk che colpisce le grandi organizzazioni* – Luglio 2019
https://www.tgsoft.it/italy/news_archivio.asp?id=1010

[7] CRAM di TG Soft - *2019W38 Report settimanale => 23-27/09 2K19 campagne MalSpam target Italia* – Settembre 2019 https://www.tgsoft.it/italy/news_archivio.asp?id=1024

[8] CRAM di TG Soft - *Continuano gli attacchi Ransomware con violazione degli accessi RDP* – Agosto 2019
https://www.tgsoft.it/italy/news_archivio.asp?id=1013

[9] CRAM di TG Soft - *2020W26 Report settimanale => 27/06-03/07 2K20 campagne MalSpam target Italia* – Giugno 2020 https://www.tgsoft.it/italy/news_archivio.asp?id=1102

[10] CRAM di TG Soft - *Analisi tecnica del ransomware REvil - Sodinokibi e Threat Intelligence Report* – Giugno 2019 https://www.tgsoft.it/italy/news_archivio.asp?id=1004

[11] CRAM di TG Soft - *Telemetria e statistiche dei virus/malware circolanti in Italia 2020-04* - Maggio 2020
https://www.tgsoft.it/italy/news_archivio.asp?id=1084

[12] CRAM di TG Soft - *Cyber-Threat Report degli attacchi informatici di maggio 2020 in Italia* - Giugno 2020
https://www.tgsoft.it/italy/news_archivio.asp?id=1093

[13] CRAM di TG Soft - *Cyber-Threat Report degli attacchi informatici di giugno 2020 in Italia* - Luglio 2020
https://www.tgsoft.it/italy/news_archivio.asp?id=1103

[14] CRAM di TG Soft - *Cyber-Threat Report degli attacchi informatici di luglio 2020 in Italia* - Agosto 2020
https://www.tgsoft.it/italy/news_archivio.asp?id=1118

[15] CRAM di TG Soft - *Cyber-Threat Report degli attacchi informatici di agosto 2020 in Italia* - Settembre 2020
https://www.tgsoft.it/italy/news_archivio.asp?id=1125

[16] CRAM di TG Soft - *Cyber-Threat Report degli attacchi informatici di settembre 2020 in Italia* - Ottobre 2020
https://www.tgsoft.it/italy/news_archivio.asp?id=1137

[17] CRAM di TG Soft - *Cyber-Threat Report degli attacchi informatici di ottobre 2020 in Italia* - Novembre 2020
https://www.tgsoft.it/italy/news_archivio.asp?id=1149
[18] CRAM di TG Soft - *Cyber-Threat Report degli attacchi informatici di novembre 2020 in Italia* - Dicembre 2020 èhttps://www.tgsoft.it/italy/news_archivio.asp?id=1161
[19] CRAM di TG Soft - *Cyber-Threat Report degli attacchi informatici di dicembre 2020 in Italia* - Febbraio 2021
https://www.tgsoft.it/italy/news_archivio.asp?id=1169

Gli autori del Rapporto Clusit 2021

Andrea Antonielli si è laureato in Giurisprudenza presso l'Università degli Studi di Milano. È Ricercatore presso gli Osservatori Digital Innovation del Politecnico di Milano e si occupa dei temi connessi alla Cybersecurity & Data Protection, con particolare focus sulle normative europeee in materia di protezione dei dati personali.

Liviu Arsene è Global Cybersecurity Researcher per Bitdefender, con un forte background in sicurezza e tecnologia. Facendo ricerche sulle tendenze e sugli sviluppi globali della sicurezza informatica, Arsene si concentra sulle minacce persistenti avanzate e sugli incidenti di sicurezza, valutando il loro impatto nelle infrastrutture critiche sia pubbliche che private. Le sue passioni ruotano attorno a tecnologie e gadget innovativi, in particolare sulle loro applicazioni di sicurezza e sull'impatto strategico a lungo termine.

Vita Santa Barletta dottoranda in Informatica e Matematica presso l'Università degli Studi di Bari Aldo Moro svolge le sue ricerche sui temi del "Secure Project Management". L'attività di ricerca si colloca nell'area della Ingegneria del Software con l'obiettivo di definire strumenti e tecniche per lo sviluppo sicuro del software; processi e strutture organizzative per la gestione sicura di progetti software. Ha contribuito all'avvio del laboratorio di Cyber Security dell'Università di Bari, The Hack Space, e ha svolto un periodo di ricerca presso IBM. È attualmente membro del Board del Branch Puglia del Project Management Institute – Southern Italy Chapter.

Giancarlo Butti ha acquisito un master in Gestione aziendale e Sviluppo Organizzativo presso il MIP Politecnico di Milano. Si occupa di ICT, organizzazione e normativa dai primi anni 80. Auditor ed esperto di sicurezza e privacy ha all'attivo oltre 800 articoli e collaborazioni con oltre 30 testate. Ha pubblicato 25 fra libri e white paper alcuni dei quali utilizzati come testi universitari; ha partecipato alla redazione di 17 opere collettive. Già docente del percorso professionalizzante ABI - Privacy Expert e Data Protection Officer in Banca è docente/relatore presso eventi di ISACA/AIEA, ORACLE/CLUSIT, ITER, INFORMA BANCA, CONVENIA, CETIF, IKN, UNISEF, Università Statale di Milano, Università degli Studi Suor Orsola Benincasa Napoli…, Politecnico di Milano, Cefriel. Partecipa ai gruppi di lavoro di ABI LAB, ISACA/AIEA, Oracle Community for Security, UNINFO, Assogestioni... È fra i coordinatori di europrivacy.info e socio di CLUSIT, ISACA, BCI. Ha inoltre acquisito le certificazioni/qualificazioni LA BS7799, LA ISO/IEC27001, CRISC, CDPSE, ISM, DPO, CBCI, AMBCI.

Danilo Caivano è Professore di Ingegneria del Software e Cyber Security presso il Dipartimento di Informatica dell'Università degli Studi di Bari Aldo Moro, consulente di aziende ed enti soprattutto nell'ambito di progetti di ricerca e sviluppo. Responsabile Scientifico del laboratorio di ricerca SERLAB (serlab.di.uniba.it), Direttore dello short master in Cyber Security, ha contribuito alla realizzazione di The Hack Space, il laboratorio di cyber security dell'Università di Bari. Membro del Board of Director del Project Management Institute Southern Italy Chapter e coordinatore della PMI-SIC Academy. È componente del Comitato Tecnico Scientifico del Distretto dell'informatica Pugliese e del Comitato di Indirizzo Strategico dell'Osservatorio IT.

Nunzia CIARDI, Dirigente Superiore della Polizia di Stato, è il Direttore del Servizio Polizia Postale e delle Comunicazioni. Laureata in giurisprudenza, con anni di esperienza nel contrasto al cybercrime, coordina attualmente le unità specializzate della Polizia di Stato nel contrasto al cyberterrorismo, al financial cybercrime, alla pedopornografia on-line nonché di tutti i reati che coinvolgono i minori on-line, alla tutela delle infrastrutture critiche informatiche nazionali, all'hacking e ai crimini informatici in generale. Partecipa, come membro nazionale in rappresentanza dell'Italia, alle riunioni dell'European Union Cybercrime Taskforce di Europol; ha preso parte alla realizzazione del progetto europeo EU-

OF2CEN per l'adozione di strategie comuni contro il crimine organizzato nel settore delle frodi on-line. E'rappresentante del Ministero dell'Interno in seno al Nucleo Sicurezza Cibernetica ed al Tavolo Tecnico Cyber. E'coordinatore di una Struttura di missione per la realizzazione di un polo centrale della sicurezza cibernetica del Ministero dell'Interno. E'membro dell'Unità Informativa Scommesse Sportive, del "Gruppo Nazionale di Cybersecurity per i Servizi Sanitari". E'membro componente del Consiglio del "*Women4Cyber*", iniziativa avviata dall'Organizzazione Europea per la Sicurezza Cibernetica (ECSO), volta a implementare il coinvolgimento delle donne nel settore della sicurezza cibernetica. E'componente dell'Organismo permanente di supporto al "Centro di coordinamento per le attività di monitoraggio, analisi e scambio permanente di informazioni sul fenomeno degli atti intimidatori nei confronti dei giornalisti". Svolge attività di docenza presso diverse scuole di Polizia, presso la scuola Ufficiali dei Carabinieri, presso il Centro Alti Studi per la Difesa, nonché presso diverse università ed enti, sulle principali attività di competenza della Specialità. Autrice di libri e pubblicazioni a carattere scientifico in materia di cybercrime, ha collaborato alla redazione del Rapporto Clusit 2018, 2019 e 2020.

Luisa Colucci ha conseguito la laurea in Informatica presso l'Università degli Studi di Pisa. Attualmente ricopre il ruolo di Solution Design Manager nella unit di CyberSecurity di Exprivia. Precedentemente ha ricoperto il ruolo di Security Architect nella divisione Security di IBM. Ha lavorato negli ultimi 10 anni nel campo della CyberSecurity acquisendo un'ampia conoscenza dei processi, delle tecnologie e del mercato. Nel suo passato ha ricoperto ruoli di leadership in un contesto lavorativo europeo ed è stata speaker in eventi nazionali e internazionali sulla Cybersecurity come ITASEC e Cybertech Tel Aviv.

Pasquale Digregorio è un ex-Ufficiale d'Accademia, attualmente Vice Capo Divisione del Computer Emergency Response Team della Banca d'Italia, dove mette al servizio dell'Istituto la sua esperienza in cyber intelligence e cybersecurity, sviluppata in 20 anni di servizio, svolti presso il Ministero della Difesa e la Presidenza del Consiglio. Dopo la laurea magistrale in ingegneria delle telecomunicazioni presso il Politecnico di Torino ha conseguito un master di secondo livello in Sistemi avanzati di comunicazione e localizzazione satellitare presso l'Università Tor Vergata ed uno in Protezione Strategica del Sistema Paese presso la SIOI. Nel corso della sua carriera ha fatto parte di commissioni e organismi permanenti in seno alla NATO; svolge attività formative e di docenza presso enti universitari e Istituzioni. È autore di diverse pubblicazioni e inventore di un brevetto internazionale.

Aldo Di Mattia è entrato in Fortinet nel 2012 con il titolo di System Engineer per poi diventare nel 2018 Principal System Engineer & team leader e a gennaio del 2020 Manager System Engineering per il centro/sud Italia. Oggi è il responsabile di un team di System Engineer che coprono il territorio del centro/sud Italia e Malta nei settori Telco, PAC/Defense, PAL/Industry, Energy/Utilities. Nel 2005 si è laureato in informatica all'università La Sapienza di Roma con una tesi sperimentale sulla sicurezza di rete, lavorando tra il 2014 e il 2012 per due tra i più importanti System Integrar italiani nella sicurezza informatica in qualità di Systems Engineer, Security Consultant, Sr. Security Engineer and Team Leader. In questi anni di lavoro ha maturato importanti competenze ed esperienze nel settore, conseguendo nel tempo più di venticinque certificazioni specialistiche sui principali vendor di sicurezza informatica, la certificazione indipendente CISSP di ISC2 e ha depositato tre brevetti con Fortinet presso USPTO (United States Patent and Trademark Office's) su: Security Fabric Cooperation; End-point protection; Deception.

Giorgia Dragoni si è laureata nel 2014 in Ingegneria Gestionale al Politecnico di Milano, indirizzo Manufacturing & Management, e nello stesso anno ha iniziato a lavorare negli Osservatori Digital Innovation occupandosi di trasformazione digitale e cybersecurity. Attualmente è ricercatrice sui temi della Cybersecurity & Data Protection e dei Big Data Analytics e dal 2020 è Direttore dell'Osservatorio Digital Identity. Sta frequentando l'Executive Master in Management presso il MIP.

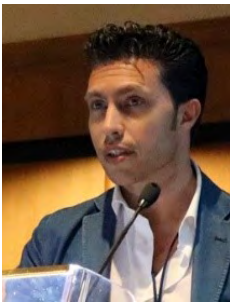
Gabriele Faggioli, legale, è amministratore delegato di Digital360 e di Partners4Innovation, Presidente del Clusit e Responsabile Scientifico dell'Osservatorio Cybersecurity & Data Protection del Politecnico di Milano. Gabriele inoltre è Adjunct Professor del MIP – Politecnico di Milano ed è stato membro del Gruppo di Esperti sui contratti di cloud computing della Commissione Europea. È specializzato in contrattualistica informatica e telematica, in information & telecommunication law, nel diritto della proprietà intellettuale e industriale e negli aspetti legali della sicurezza informatica, in progetti inerenti l'applicazione delle normative inerenti la responsabilità amminstrativa degli enti e nel diritto dell'editoria e del markerting. Ha pubblicato diversi libri fra cui: "I contratti di cloud computing: Comprendere, affrontare e negoziare i contratti con i cloud"(Franco Angeli), "I

contratti per l'acquisto di servizi informatici" (Franco Angeli), "Computer Forensics" (Apogeo), "Privacy per posta elettronica e internet in azienda" (Cesi Multimedia) oltre ad innumerevoli articoli sui temi di competenza ed è stato relatore a molti seminari e convegni.

Paolo Giudice è segretario generale del CLUSIT. Negli anni '80 e '90 ha svolto attività di consulenza come esperto di gestione aziendale e rischi finanziari. L'evoluzione del settore IT, che ha messo in evidenza le carenze esistenti in materia di Security, lo ha spinto ad interessarsi alla sicurezza informatica e, nel luglio 2000, con un gruppo di amici, ha fondato il CLUSIT. Dal 2001 al 2008 ha coordinato il Comitato di Programma di Infosecurity Italia e dal 2009 coordina il Comitato Scientifico del Security Summit. Dal 2011 coordina il Comitato di Redazione del Rapporto Clusit. Paolo è Partner di C.I.S.C.A. (Critical Infrastructures Security Consultants & Analysts) a Ginevra.

Federica Maria Rita Livelli è In possesso della certificazione Business Continuity - AMBCI BCI, UK e Risk Management FERMA Rimap ®, consulente di Business Continuity & Risk Management, svolge attività di diffusione e di sviluppo della cultura della resilienza presso varie istituzioni ed università. Membro del Board del BCI Italy Chapter, socia ANRA, AIPSA, CLUSIT ed UNI. Membro di diversi Comitati: CLUSIT-Artificial Intelligence, UNI/CT 016/GL 02 «Sistemi di gestione per la qualità» (ISO/TC 176/SC 2), UNI/CT 016/GL 09 «Governance delle organizzazioni» (ISO/TC 309) e UNI/CT 016/GL 89 «Gestione dell'innovazione» (ISO/TC 279) (Commissione Tecnica UNI/CT 016 «Gestione per la qualità e metodi statistici»). Membro della Community: Women for Cyber Security e Ambassador della Community Donne 4.0. Docente di moduli di introduzione di: ISO 22301 - Business Continuity & Resilience (Università POLIMI–BOCCONI e Università di Verona); ISO 31000 - Risk Management (Università Statale di Milano). Relatrice e moderatrice in diversi seminari, conferenze nazionali ed internazionali. Autrice di numerosi articoli su diverse riviste online, (i.e.: AgendaDigitale, Cybersecurity360, AI4Business, Risk Management360, EnergyUp, Blockchain4Innovation, Internet4Things, Industry4Business, ANRA - RM Magazine, ISPI online, Insurance Review, UNI Magazine online, The BCI Blog). Partecipato, in qualità di co-autrice alle edizioni 2020 del Rapporto Clusit - Cyber Security.

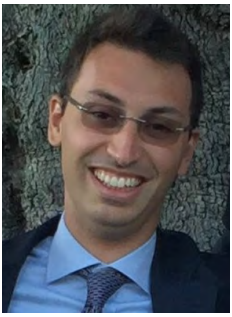
Roberto Obialero è Cybersecurity & Data Protection Advisor, in possesso di una esperienza ventennale in ruoli, manageriali, di sviluppo business e tecnici nell'ambito dell'offerta di servizi di sicurezza informatica. Collabora a titolo di advisor freelance nel ruolo CISO e nella realizzazione di importanti progetti sulle tematiche cybersecurity e data protection svolgendo attività di gestione del rischio, definizione strategie e roadmap cybersecurity, business continuity e vulnerability management, gestione di incidenti informatici, training & awareness. È in possesso delle certificazioni indipendenti GSTRT, GPPA e GCFA ottenute attraverso il programma SANS-GIAC americano, della certificazione ISO 27000 Lead Auditor e si è perfezionato in "Computer Forensics & Data Protection" e "Data Protection & Data Governance" presso l'Università Statale di Milano. Membro del Comitato Direttivo Clusit collabora attivamente alla realizzazione di progetti di ricerca nell'ambito Cybersecurity & Data Protection con le principali community di settore; è stato speaker in occasione di diversi eventi di rilevanza nazionale, oltre ad aver contribuito alla redazione di diverse pubblicazioni ed articoli per conto di riviste specializzate.



Marco Pericò ha conseguito la Laurea Magistrale in Ingegneria Informatica presso l'Università degli Studi di Palermo e successivamente un Master in Cybercrime e Informatica Forense presso l'Università degli Studi di Roma "La Sapienza". Lavora nel CERT della Banca d'Italia occupandosi di cyber threat intelligence e ricoprendo anche il ruolo di esperto nell'ambito del sistema di gestione del rischio operativo. In precedenza, in qualità di Funzionario Informatico del Dipartimento dell'Amministrazione Generale del Personale e dei Servizi del Ministero dell'Economia e delle Finanze, si è occupato di gestione della sicurezza e governance pianificando, progettando, sviluppando e acquisendo architetture e infrastrutture informatiche per il Dipartimento e per il Ministero. Nel suo precedente incarico in ISTAT ha progettato e realizzato sistemi di sicurezza informatica, curandone la gestione e l'evoluzione tecnologica.

Alessandro Piva, laureato in Ingegneria delle Telecomunicazioni e in Ingegneria Gestionale al Politecnico di Milano nel 2006, ha conseguito in seguito un Executive Master in Business Administration (EMBA) presso il MIP Politecnico di Milano. Alla School of Management del Politecnico di Milano, dove lavora da circa 15 anni, è Direttore degli Osservatori Cybersecurity & Data Protection, Cloud Transformation, Artificial Intelligence e Responsabile della Ricerca dell'Osservatorio Big Data & Business Analytics.

Domenico Raguseo è Responsabile della Unit di CyberSecurity del gruppo Exprivia|Italtel. Precedentemente ha ricoperto il ruolo di CTO della divisione IBM Security nel Sud Europa. Ha una decennale esperienza manageriale e nel campo della cybersecurity in diverse aree. Domenico collabora con diverse università nell'insegnamento su tematiche relative alla cybersecurity sia come Professore a contratto che invitato come lettore per seminari. Domenico è stato IBM Master inventor grazie a una moltitudine di brevetti e pubblicazioni in diverse discipline (Business Processes, ROI, Messages and Collaborations, Networking). Infine, è apprezzato speaker, autore e blogger in eventi nazionali ed internazionali. In particolare, da diversi anni collabora con il Clusit come autore.



Marco Raimondi, nato nel 1987, si laurea in Ingegneria delle Telecomunicazioni presso il Politecnico di Milano. Ha iniziato la sua carriera nell'ambito IT per poi orientare la sua attività nel mondo commerciale, con un focus particolare sul mercato Enterprise. Dal 2012 ha lavorato presso Vodafone Italia dove ha ricoperto nella Business Unit Enterprise dapprima il ruolo di Presales e successivamente il ruolo di Marketing Product Manager nel mercato delle PMI. Dal 2017 in Fastweb ricopre dapprima il ruolo di Marketing Product Manager in ambito security, quindi il ruolo di Marketing Manager responsabile dello sviluppo dei prodotti di Sicurezza, Cloud e IoT.

Pier Luigi Rotondo (**@PGRotondo**) lavora per il gruppo di Technical Sales IBM. Ha contribuito a molti progetti internazionali su soluzioni di sicurezza per l'Identity e l'Access Management, il Single Sign-on, e la Threat Intelligence. Con una la laurea in Scienze dell'Informazione presso Sapienza Università di Roma, Pier Luigi è coinvolto in attività accademiche su temi di sicurezza delle informazioni in Corsi di Laurea e Master presso l'Università di Roma e di Perugia. Per conto di IBM Italia scrive articoli divulgativi, e contribuisce permanentemente dal 2015 al Rapporto Clusit sulla Sicurezza ICT in Italia sul cybercrime nel settore finanziario, presentando i risultati IBM.

Stefano Russo ha conseguito nel 2015 la laurea magistrale in Ingegneria Informatica presso l'Università degli Studi Roma Tre, con una tesi riguardante lo sviluppo di un framework per la modellazione automatica e l'interrogazione di basi di dati a grafo distribuite. Da sempre appassionato di IT Security, sin dall'inizio della sua carriera si è focalizzato su questo ambito occupandosi di diverse attività: progettazione e sviluppo backend di sistemi di monitoraggio e log management, system integration, penetration testing e cyber threat intelligence. Dal 2019 ricopre il ruolo di Cyber Security Analyst nel CERT della Banca d'Italia.

Rodolfo Saccani, Security R&D Manager in Libra Esva, vive l'IT dal 1994, in qualità di sviluppatore, sistemista, consulente e project manager. Ha vissuto e lavorato negli USA e in Danimarca. Da sempre interessato al mondo della *security*, ha un'esperienza tecnica eterogenea: sistemi linux embedded, avionica sperimentale, telecomunicazioni sicure in ambienti ostili, TV connessa, controllo di processo e automazione industriale, ricerca clinica, piattaforme web SaaS. Per passione si occupa anche di sicurezza nel volo libero: consigliere alla sicurezza in FIVL (Federazione Italiana Volo Libero) dal 2007, è expert presso il CEN (Comitato Europeo di Normazione) e partecipa alla stesura delle norme europee di certificazione delle attrezzature da volo libero. In Libraesva coordina la ricerca e sviluppo per l'e-mail security.

Sofia Scozzari si occupa con passione di informatica dall'età di 16 anni. Ha lavorato come consulente di sicurezza presso primarie aziende italiane e multinazionali, curando gli aspetti tecnologici ed organizzativi di numerosi progetti. Già Chief Executive Officer de iDIALOGHI, società milanese dedicata alla formazione e alla consulenza in ambito Cyber Security, è Founder e Managing Director di Hackmanac, società che elabora dati sulle minacce Cyber a supporto di attività di Risk Management. Negli anni si è occupata di Social Media Security, ICT Security Consulting & Training e della gestione di progetti di Sicurezza Gestita, quali Vulnerability Management, Penetration Testing, Mobile Security e Threat Intelligence. Membro del Comitato Scientifico di CLUSIT, è autrice di articoli e guide in tema di Social Media Security. È tra gli autori dei papers "La Sicurezza nei Social Media", pubblicato nel 2014 dalla Oracle Community for Security, e «Blockchain & Distributed Ledger: aspetti di governance, security e compliance», pubblicato nel 2019 da Clusit. Fin dalla prima edizione contribuisce alla realizzazione del "Rapporto Clusit sulla Sicurezza

ICT in Italia" curando l'analisi dei principali attacchi a livello internazionale.

Maurizio Taglioretti, esperto di IT Audit, Security & Compliance è Regional Manager SEUR di Netwrix Corporation. Vanta una ventennale esperienza nel settore della sicurezza IT: prima di assumere questo incarico ha ricoperto diversi ruoli di crescente importanza a livello nazionale e internazionale in note aziende di sicurezza informatica. Maurizio è socio Clusit e socio (ISC)2 Italy Chapter, partecipa attivamente come relatore ad eventi sulla Sicurezza e la Compliance.

Enrico Tonello, laureato in ingegneria a Padova, è socio co-fondatore di TG Soft S.r.l. Cyber Security Specialist. Da sempre attento agli aspetti di sicurezza informatica ed in particolare ad attacchi da virus&malware. Autore di numerosi articoli su virus&malware informatici pubblicati su alcune delle principali riviste italiane del settore. Co-autore della suite AntiVirus-AntiSpyware-AntiMalware Vir.IT eXplorer PRO per Windows® Microsoft, con motore proprio dotata di tecnologie AntiRansomware protezione Crypto-Malware. Relatore in conferenze e seminari sui virus&malware informatici e su come difendersi come Security Evangelist.

Gianfranco Tonello, laureato in ingegneria informatica a Padova, è CEO di TG Soft S.r.l. Cyber Security Specialist. Malware Analyst, riconosciuto a livello internazionale quale analista di virus&malware di nuova generazione e sviluppatore di tecnologie AntiMalware. Dal 1990 analista di Virus/Malware con pubblicazione di analisi tecniche presso il VTC (Virus Test Center) dell'Università di Amburgo e numerose riviste italiane. Autore/Sviluppatore software specializzato nella produzione di tecnologie AntiVirus-AntiSpyware-AntiMalware: dal 1992 sviluppa software di identificazione euristica e dal 1993 il software AntiVirus VirIT per l'univoca identificazione, la corretta rimozione dotato di scudo residente in tempo reale per S.O. DOS; dal 1997 sviluppa la suite AntiVirus-AntiSpyware-AntiMalware Vir.IT eXplorer PRO per Windows® Microsoft, con motore proprio dotata di tecnologie AntiRansomware protezione Crypto-Malware; Dal 2013 sviluppa il software AntiMalware per Androd[TM] VirIT Mobile Security. Docente CLUSIT Associazione Italiana per la Sicurezza Informatica. WildList reporter (www.wildlist.org): analista/reporter della WildList, che individua i virus/malware on the wild cioè realmente circolanti a livello mondiale.

Membro AMTSO Anti-Malware Testing Standards Organization (www.amtso.org). Membro VIA Virus Information Alliance di Microsoft. Membro MVI Microsoft Virus Initiative.

Alessandro Vallega, Dirigente in Partners4Innovation, si occupa dei programmi di innovazione della capogruppo Digital 360 (scouting, acquisizioni, contratti di partnership), di cybersecurity e della linea d'offerta GRC della società. Prima del novembre 2018, è stato Business Development Director, Security e GDPR, in Oracle EMEA con la responsabilità di un team centrale e regionale sul tema del GDPR. Alessandro è nel direttivo di Clusit dal 2010, ed è il fondatore e chairman della Clusit Community for Security. È coautore, editor e team leader di undici pubblicazioni su diversi temi legati alla sicurezza (misure, rischio, frodi, ritorno dell'investimento, compliances, privacy, cloud...) liberamente scaricabili dal sito Clusit (http://c4s.clusit.it). Al momento è impegnato nella produzione della 12esima pubblicazione che tratterà il tema della sicurezza, rischio e compliance dell'Intelligenza Artificiale (previsto per marzo 2021). Contribuisce fin dal 2012 ai Rapporti Clusit sulla Sicurezza ICT in Italia. Quest'anno insegna Analisi e gestione del rischio all'Università Statale di Milano. Ha una laurea in Scienza Politiche conseguita all'Università degli Studi di Miano.

Andrea Zapparoli Manzoni si occupa con passione di ICT dal 1997 e di Information Security dal 2003, mettendo a frutto un background multidisciplinare in Scienze Politiche, Computer Science ed Ethical Hacking. È stato membro dell'Osservatorio per la Sicurezza Nazionale (OSN) nel 2011-12 e del Consiglio Direttivo di Assintel dal 2012 al 2016, coordinandone il GdL Cyber Security. Dal 2012 è membro del Consiglio Direttivo di Clusit, e Board Advisor del Center for Strategic Cyberspace + Security Science (CSCSS) di Londra. Per oltre 10 anni è stato Presidente de iDialoghi, società milanese dedicata alla formazione ed alla consulenza in ambito ICT Security. Nel gennaio 2015 ha assunto il ruolo di Head of Cyber Security Services della divisione Information Risk Management di KPMG Advisory. Dal giugno 2017 è Managing Director di un centro di ricerca internazionale in materia di Cyber Defense. È spesso chiamato come relatore a conferenze ed a tenere lezioni presso Università, sia in Italia che all'estero. Come docente Clusit tiene corsi di formazione su temi quali Cyber Crime, Mobile Security, Cyber Intelligence e Social Media Security, e partecipa come speaker alle varie edizioni del Security Summit, oltre che alla realizzazione di white papers (FSE, ROSI v2, Social Media) in collaborazione con la Oracle Community for Security. Fin dalla prima edizione (2011) del "Rapporto Clusit sulla Sicurezza ICT in Italia", si è occupato della sezione relativa all'analisi dei principali attacchi a livello internazionale e alle tendenze per il futuro.

Il Clusit, nato nel 2000 presso il Dipartimento di Informatica dell'Università degli Studi di Milano, è la più numerosa ed autorevole associazione italiana nel campo della sicurezza informatica. Oggi rappresenta oltre 600 organizzazioni, appartenenti a tutti i settori del Sistema-Paese.

Gli obiettivi

- Diffondere la cultura della sicurezza informatica presso le Aziende, la Pubblica Amministrazione e i cittadini.
- Partecipare alla elaborazione di leggi, norme e regolamenti che coinvolgono la sicurezza informatica, sia a livello nazionale che europeo.
- Contribuire alla definizione di percorsi di formazione per la preparazione e la certificazione delle diverse figure professionali operanti nel settore della sicurezza.
- Promuovere l'uso di metodologie e tecnologie che consentano di migliorare il livello di sicurezza delle varie realtà.

Le attività e i progetti in corso

- Formazione specialistica: i Webinar CLUSIT.
- Ricerca e studio: Premio "Innovare la Sicurezza delle Informazioni" per la migliore tesi universitaria arrivato alla 16a edizione.
- Le Conference specialistiche: i Security Summit Streaming Edition, i Security Summit On Site (che riprenderanno speriamo presto a Milano, Treviso, Verona e Roma), gli Atelier della Security Summit Academy, Le Tavole Rotonde Verticali (Energy & Utilities, Health Care, Finance, Manufacturing).
- I Gruppi di Lavoro: della Clusit Community for Security.
- Rapporti Clusit: Rapporto annuale, con aggiornamento semestrale, sula sicurezza ICT in Italia, in produzione dal 2012.
- Il Mese Europeo della Sicurezza Informatica, iniziativa di sensibilizzazione promossa e coordinata ogni anno nel mese di ottobre in Italia da Clusit, in accordo con l'ENISA e con l'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione del Ministero dello Sviluppo Economico (ISCOM).

Il ruolo istituzionale

In ambito nazionale, Clusit opera in collaborazione con: Presidenza del Consiglio, numerosi ministeri, Banca d'Italia, Polizia Postale e delle Comunicazioni, Arma dei Carabinieri e Guardia di Finanza, Agenzia per l'Italia Digitale, Autorità Garante per la tutela dei dati personali, Autorità per le Garanzie nelle Comunicazioni, CERT Nazionale e CERT P.A., Università e Centri di Ricerca, Associazioni Professionali e Associazioni dei Consumatori, Confindustria, Confcommercio e CNA.

I rapporti internazionali

In ambito internazionale, Clusit partecipa a svariate iniziative in collaborazione con: i CERT, i CLUSI, Università e Centri di Ricerca in oltre 20 paesi, Commissione Europea,

ENISA (European Union Agency for Network and Information Security), ITU (International Telecommunication Union), OCSE, UNICRI (Agenzia delle Nazioni Unite che si occupa di criminalità e giustizia penale), le principali Associazioni Professionali del settore (ASIS, CSA, ISACA, ISC², ISSA, SANS) e le associazioni dei consumatori.

Security Summit è il più importante appuntamento italiano per tutti coloro che sono interessati alla sicurezza dei sistemi informatici e della rete e, più in generale, alla sicurezza delle informazioni.

Progettato e costruito per rispondere alle esigenze dei professionals di oggi, Security Summit è un convegno strutturato in momenti di divulgazione, di approfondimento, di formazione e di confronto. Aperto alle esperienze internazionali e agli stimoli che provengono sia dal mondo imprenditoriale che da quello universitario e della ricerca, il Summit si rivolge ai professionisti della sicurezza e a chi in azienda gestisce i problemi organizzativi o legali e contrattuali dell'Ict Security.

La **partecipazione è libera e gratuita**, con il solo obbligo dell'iscrizione online.
Il Security Summit è organizzato dal Clusit e da Astrea, agenzia di comunicazione ed organizzatore di eventi di alto profilo contenutistico nel mondo finanziario e dell'Ict.

Certificata dalla folta schiera di relatori (più di 700 sono intervenuti nelle scorse edizioni), provenienti dal mondo della ricerca, dell'Università, delle Associazioni, della consulenza, delle Istituzioni e delle imprese, la manifestazione è stata frequentata da oltre 18.000 partecipanti, e sono stati rilasciati circa 14.000 attestati validi per l'attribuzione di oltre 46.000 crediti formativi (CPE).

L'edizione 2021

La 13esima edizione del Security Summit parte con una edizione interamente in streaming, che si terrà dal 16 al 18 marzo. Hanno ripreso gli **Atelier della Security Summit Academy**, che si terranno tutto l'anno. Abbiamo inoltre messo in campo una nuova iniziativa: una serie di Eventi Verticali programmati in maggio (Energy & Utilities), giugno /Health Care), settembre (Finance) e ottobre (Manufacturing). Tra i temi più in evidenza per il 2020: Cyber Crime, Sicurezza del e nel Cloud, Intelligenza Artificiale, Supply Chain, IoT, Industria 4.0., Compliance, GDPR, Certificazioni (professionali, di sistema, di prodotto).

Informazioni

- **Agenda e contenuti:** info@clusit.it, +39 349 7768 882
- **Altre informazioni:** info@astrea.pro
- **Informazioni per la stampa:** press@securitysummit.it
- **Sito web:** www.securitysummit.it/
- **Foto reportage:** www.facebook.com/groups/64807913680/photos/?filter=albums
- **Video riprese e interviste:** www.youtube.com/user/SecuritySummit

In collaborazione con

www.securitysummit.it