EUROPEAN UNION AGENCY
FOR CYBERSECURITY

RELAZIONE SUL PANORAMA DELLE MINACCE DELL'ENISA 2021

Aprile 2020 - metà luglio 2021

OTTOBRE 2021

INFORMAZIONI SULL'ENISA

L'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, è l'agenzia dell'Unione impegnata a conseguire un elevato livello comune di cibersicurezza in tutta Europa. Istituita nel 2004 e consolidata dal regolamento dell'UE sulla cibersicurezza, l'Agenzia dell'Unione europea per la cibersicurezza contribuisce alla politica dell'UE in materia di sicurezza informatica, migliora l'affidabilità dei prodotti, dei servizi e dei processi TIC con sistemi di certificazione della cibersicurezza, coopera con gli Stati membri e gli organismi dell'UE e aiuta l'Europa a prepararsi per le sfide informatiche del futuro. Attraverso lo scambio di conoscenze, lo sviluppo di capacità e la sensibilizzazione, l'Agenzia collabora con i suoi principali portatori di interessi per rafforzare la fiducia nell'economia connessa, aumentare la resilienza delle infrastrutture dell'Unione e, in ultima analisi, garantire la sicurezza digitale della società e dei cittadini europei. Maggiori informazioni sull'ENISA e sulle sue attività sono disponibili all'indirizzo seguente: www.enisa.europa.eu.

CONTATTI

Per contattare gli autori, inviare un messaggio di posta elettronica a etl@enisa.europa.eu.
Per maggiori informazioni sul presente documento, inviare un messaggio di posta elettronica a press@enisa.europa.eu.

REDATTORI

Ifigeneia Lella, Marianthi Theocharidou, Eleni Tsekmezoglou, Apostolos Malatras - Agenzia dell'Unione europea per la cibersicurezza

AUTORI

Claudio Ardagna, Stephen Corbiaux, Andreas Sfakianakis, Christos Douligeris

RINGRAZIAMENTI

Vorremmo ringraziare i membri e gli osservatori del gruppo di lavoro ad hoc dell'ENISA sul panorama delle minacce informatiche per i loro preziosi feedback e commenti nella convalida di questa relazione. Vorremmo anche ringraziare il gruppo consultivo dell'ENISA e la rete dei funzionari di collegamento nazionali per il loro prezioso feedback.
Vorremmo inoltre ringraziare i team ENISA per la consapevolezza della situazione e la notifica degli incidenti per il loro contributo attivo e il loro supporto nel consolidare diverse informazioni nel panorama delle minacce.

AVVERTENZA LEGALE

NOTA DI COPYRIGHT

ISBN: 978-92-9204-536-4 – DOI: 10.2824/324797 – ISSN: 2363-3050

INDICE

SINTESI

Questa è la nona edizione della Relazione sul panorama delle minacce dell'ENISA (ETL), una relazione annuale sullo stato del panorama delle minacce alla sicurezza informatica che identifica le principali minacce, le principali tendenze osservate rispetto alle minacce, gli attori delle minacce e le tecniche di attacco e descrive anche la mitigazione pertinente le misure. Nel processo di miglioramento costante della nostra metodologia per lo sviluppo del panorama delle minacce, il lavoro di quest'anno è stato supportato da un gruppo di lavoro ad hoc ENISA sul panorama delle minacce alla sicurezza informatica (CTL) appena formato.

L'intervallo di tempo della relazione ETL 2021 va da aprile 2020 a luglio 2021 ed è denominato "periodo in esame" in tutta la relazione. Durante il periodo in esame, le principali minacce identificate includono:

- **Ransomware**
- **Malware**
- **Cryptojacking**
- **Minacce legate alla posta elettronica**
- **Minacce ai dati**
- **Minacce alla disponibilità e all'integrità**
- **Disinformazione - cattiva informazione**
- **Minacce non dannose**
- **Attacchi alla catena di approvvigionamento**

In questa relazione discutiamo le prime 8 categorie di minacce alla sicurezza informatica. Le minacce alla catena di approvvigionamento, la nona categoria, sono state analizzate in dettaglio, per la loro particolare rilevanza, in una relazione ENISA dedicata "Relazione sul panorama delle minacce dell'ENISA sugli attacchi alla catena di approvvigionamento" [1].

Per ciascuna delle minacce identificate, vengono discusse le tecniche di attacco, gli incidenti rilevanti e le tendenze insieme alle misure di mitigazione proposte. Per quanto riguarda le tendenze, nel periodo in esame si evidenzia quanto segue:

- Il **ransomware** è stato valutato come la **principale minaccia per il 2020-2021.**
- **Le organizzazioni governative hanno intensificato il loro gioco** sia a livello nazionale che internazionale.
- **I criminali informatici sono sempre più motivati dalla monetizzazione** delle loro attività, ad es. ransomware. La **criptovaluta** rimane il metodo di pagamento più comune per gli attori delle minacce.
- Il **declino del malware** osservato nel 2020 continua nel 2021. Nel 2021, abbiamo rilevato un aumento degli attori delle minacce che ricorrevano a linguaggi di programmazione relativamente nuovi o non comuni per veicolare il proprio codice.
- Il volume delle **infezioni da cryptojacking** ha raggiunto un **livello elevato** nel primo trimestre del 2021 rispetto agli ultimi anni. Il **guadagno finanziario** associato al cryptojacking ha incentivato gli attori delle minacce a eseguire questi attacchi.
- La **COVID-19 è ancora l'esca dominante nelle campagne** di attacchi di posta elettronica.
- Si è verificata un'**impennata delle violazioni dei dati relative al settore sanitario**.
- Le **tradizionali campagne DDoS (Distributed Denial of Service)** nel 2021 sono più mirate, più persistenti e sempre più multivettoriali. L'**IoT (Internet of Things)** in combinazione con le **reti mobili** sta provocando una nuova ondata di attacchi DDoS.

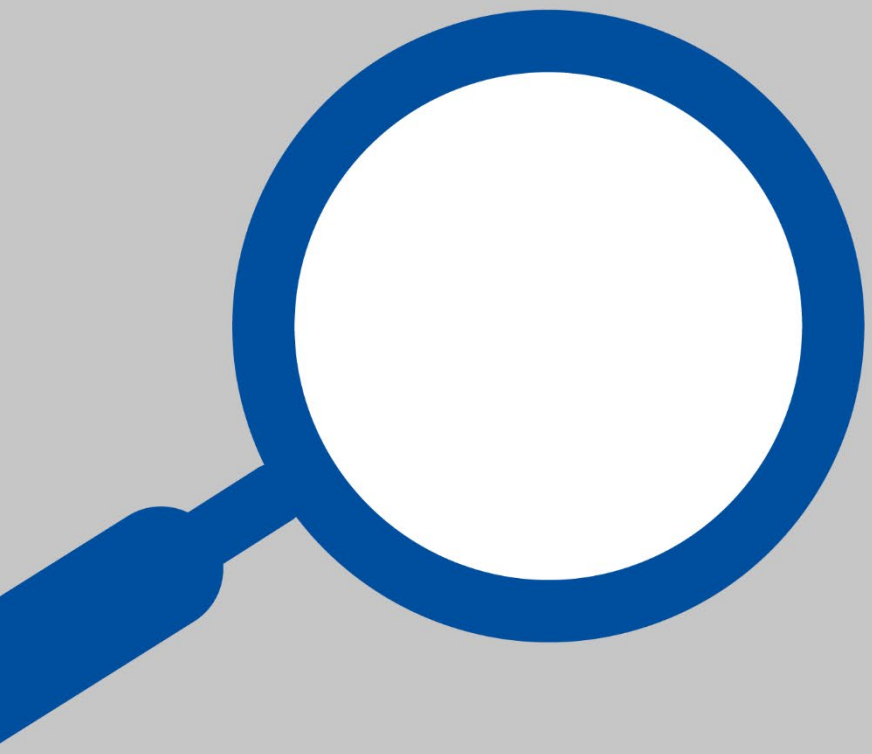
[1] Relazione sul panorama delle minacce dell'ENISA sugli attacchi alla catena di approvvigionamento, luglio 2021. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks.

- Nel 2020 e nel 2021 osserviamo un **picco di incidenti non dannosi** poiché la pandemia di COVID-19 è diventata un moltiplicatore di **errori umani** e **configurazioni errate del sistema** fino al punto che la maggior parte delle violazioni nel 2020 sono state causate da errori.

Comprendere le tendenze relative agli attori delle minacce, alle loro motivazioni e ai loro obiettivi è di grande aiuto nella pianificazione delle difese della sicurezza informatica e delle strategie di mitigazione. Questa è una parte integrante della nostra valutazione complessiva delle minacce poiché consente di dare priorità ai controlli di sicurezza e di elaborare una strategia dedicata in base al potenziale impatto e alla probabilità di concretizzazione della minaccia. In tale ottica, ai fini dell'ETL 2021, vengono considerate le seguenti quattro categorie di attori della minaccia alla sicurezza informatica:

- **Attori sponsorizzati dallo Stato**
- **Attori del crimine informatico**
- **Attori hacker su commissione**
- **Hacktivisti**

Attraverso un'analisi continua, l'ENISA ha derivato tendenze e punti di interesse per ciascuna delle principali minacce presentate nell'ETL 2021. I risultati e i giudizi chiave di questa valutazione si basano su risorse multiple e pubblicamente disponibili fornite nei riferimenti utilizzati per lo sviluppo di questo documento. La relazione si rivolge principalmente a decisori strategici e decisori politici, ma interesserà anche la comunità tecnica della sicurezza informatica.



SGUARDO GENERALE DEL PANORAMA DELLE MINACCE

Nella sua nona edizione, la Relazione sul panorama delle minacce dell'ENISA (ETL) offre uno sguardo generale del panorama delle minacce alla sicurezza informatica. La relazione ETL è in parte strategica e in parte tecnica, con informazioni pertinenti per lettori sia tecnici sia non tecnici. Il lavoro di quest'anno è stato supportato da un gruppo di lavoro ad hoc dell'ENISA recentemente formato sul panorama delle minacce alla sicurezza informatica (CTL) ([2]).

Gli attacchi alla sicurezza informatica hanno continuato ad aumentare negli anni 2020 e 2021, non solo in termini di vettori e numeri, ma anche in termini di impatto. La pandemia di COVID-19 ha anche, come previsto, un impatto sul panorama delle minacce alla sicurezza informatica. Uno degli sviluppi più duraturi derivanti dalla pandemia di COVID-19 è il passaggio duraturo a un modello di ufficio ibrido. Pertanto, le minacce alla sicurezza informatica legate alla pandemia e allo sfruttamento della "nuova normalità" stanno diventando mainstream. Questa tendenza ha aumentato la superficie di attacco e, di conseguenza, abbiamo assistito a un aumento del numero di attacchi informatici rivolti a organizzazioni e aziende attraverso gli uffici domestici ([3]).

In generale, le minacce alla sicurezza informatica sono in aumento. Partito da una presenza online in continua crescita, dalla transizione delle infrastrutture tradizionali a soluzioni online e basate su cloud, dall'interconnettività avanzata e dallo sfruttamento di nuove funzionalità di tecnologie emergenti come l'intelligenza artificiale (AI) ([4]) ([5]), il panorama della sicurezza informatica è cresciuto in termini di sofisticatezza degli attacchi, la loro complessità e il loro impatto. In particolare, la minaccia alle catene di approvvigionamento e la loro importanza a causa dei loro effetti a cascata potenzialmente catastrofici ha raggiunto la posizione più alta tra le principali minacce, tanto che l'ENISA ha prodotto un panorama di minacce dedicato per questa categoria di minacce ([6]).

Vale la pena notare che in questa iterazione dell'ETL, è stata prestata particolare attenzione all'impatto delle minacce informatiche in vari settori, inclusi quelli elencati nella Direttiva sulla sicurezza delle reti e delle informazioni (NISD). Informazioni interessanti possono essere tratte dalle particolarità di ciascun settore quando si tratta del panorama delle minacce, delle potenziali interdipendenze e delle aree di importanza. Di conseguenza, i panorami delle minacce settoriali meritano ulteriore attenzione.

Ci sono stati anche alcuni passi importanti da parte dei difensori nella comunità informatica quest'anno e dei responsabili politici. La comunità globale ha iniziato a rendersi conto dell'importanza della comunicazione e della cooperazione nell'esame e nel tracciamento dei criminali informatici, laddove il ransomware (la minaccia più importante per il periodo in esame di ETL 2021) in particolare è diventato un elemento primario nelle agende degli incontri sulla strategia tra i leader globali.

I lettori affezionati delle passate edizioni dell'ETL 2021 noteranno una differenza nella mappatura delle principali minacce. Quest'anno l'ENISA ha fatto un passo indietro e ha consolidato le categorie di minacce verso l'integrazione e una migliore rappresentazione di minacce simili. Questo fa parte degli sforzi in corso verso una tassonomia delle minacce rinnovata e aiuterà a stabilire le tendenze metodologicamente nei prossimi anni.

L'ETL 2021 si basa su una varietà di informazioni open source e fonti di intelligence sulle minacce informatiche. Identifica le principali minacce, tendenze e risultati e fornisce strategie di mitigazione di alto livello pertinenti.

([2]) https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/ad-hoc-working-group-cyber-threat-landscapes
([3]) IBM - Cost of a Data Breach Report 2020 (Relazione sul costo di una violazione dei dati 2020) - https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/
([4]) Panorama delle minacce AI ENISA: https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges
[5] https://www.stealthlabs.com/blog/top-10-cybersecurity-trends-in-2021-and-beyond/
([6]) Relazione sul panorama delle minacce dell'ENISA sugli attacchi alla catena di approvvigionamento, luglio 2021. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

L'ENISA sta attualmente lavorando per consolidare la metodologia per la segnalazione del panorama delle minacce per promuovere la trasparenza e la coerenza del lavoro.

1.1. PRINCIPALI MINACCE

Una serie di minacce informatiche è emersa e si è materializzata nel corso del 2020 e del 2021. Sulla base dell'analisi presentata in questa relazione, la Relazione sul panorama delle minacce dell'ENISA 2021 identifica e si concentra sui seguenti 8 principali gruppi di minacce (vedere Figura 1). Questi 8 gruppi di minacce sono evidenziati per la loro importanza durante il periodo in esame, la loro popolarità e l'impatto che la materializzazione di queste minacce ha avuto.

- **Ransomware**
  Il ransomware è un tipo di attacco dannoso in cui gli aggressori crittografano i dati di un'organizzazione e richiedono un pagamento per ripristinare l'accesso. Il ransomware è stata la principale minaccia durante il periodo in esame, con diversi incidenti di alto profilo e molto pubblicizzati. Il significato e l'impatto della minaccia del ransomware è evidenziato anche da una serie di iniziative politiche correlate nell'Unione europea (UE) e nel mondo.

- **Malware**
  Il malware è software o firmware destinato a eseguire un processo non autorizzato con un impatto negativo sulla riservatezza, integrità o disponibilità di un sistema. La minaccia del malware è stata costantemente classificata come elevata per molti anni, anche se a un tasso decrescente durante il periodo in esame di ETL 2021. L'utilizzo di nuove tecniche di collegamento e alcuni importanti successi per la comunità delle forze dell'ordine hanno avuto un impatto sulle operazioni dei principali attori delle minacce.

- **Cryptojacking**
  Il cryptojacking o cryptomining nascosto è un tipo di crimine informatico in cui un criminale utilizza segretamente la potenza di calcolo di una vittima per generare criptovaluta. Con la proliferazione delle criptovalute e la loro sempre maggiore diffusione da parte del grande pubblico, è stato osservato un aumento dei corrispondenti incidenti di sicurezza informatica.

- **Minacce legate alla posta elettronica**
  Gli attacchi relativi alla posta elettronica sono un insieme di minacce che sfruttano le debolezze nella psiche umana e nelle abitudini quotidiane piuttosto che le vulnerabilità tecniche nei sistemi informativi. È interessante notare che, nonostante le numerose campagne di sensibilizzazione e di educazione contro questi tipi di attacchi, la minaccia persiste in misura notevole. In particolare, sono in aumento i compromessi tra messaggi di posta elettronica aziendali e tecniche sofisticate avanzate nell'estrazione di guadagni monetari.

- **Minacce ai dati**
  Questa categoria comprende violazioni/perdite di dati. Una violazione o una perdita di dati è il rilascio di dati sensibili, riservati o protetti in un ambiente non affidabile. Le violazioni dei dati possono verificarsi a seguito di un attacco informatico, un lavoro interno, una perdita involontaria o l'esposizione dei dati. La minaccia continua a essere elevata poiché l'accesso ai dati è un obiettivo primario per gli aggressori per numerose ragioni, ad es. estorsione, riscatto, diffamazione, disinformazione e cattiva informazione ecc.

- **Minacce alla disponibilità e all'integrità**
  Disponibilità e integrità sono l'obiettivo di una pletora di minacce e attacchi, tra cui spiccano le famiglie di Denial of Service (DoS) e Web Attacks. Strettamente correlato agli attacchi basati sul Web, il DDoS è una delle minacce più critiche ai sistemi IT che prende di mira la loro disponibilità esaurendo le risorse, causando riduzioni delle prestazioni, perdita di dati e interruzioni del servizio. Il trattamento è costantemente classificato in alto nel panorama delle minacce ENISA, sia per la sua manifestazione in incidenti reali sia per il suo potenziale di impatto elevato.

- **Disinformazione - cattiva informazione**
  Le campagne di disinformazione e cattiva informazione sono in aumento, stimolate dal maggiore utilizzo delle piattaforme di social media e dei media online e a seguito dell'aumento della presenza online delle persone a causa della pandemia di COVID-19. Questo gruppo di minacce sta facendo la sua prima apparizione nell'ETL, tuttavia la sua importanza nel mondo cibernetico è alta. Le campagne di disinformazione e cattiva informazione sono spesso utilizzate negli attacchi ibridi per ridurre la percezione generale di fiducia, uno dei principali sostenitori della sicurezza informatica.

- **Minacce non dannose**
  Le minacce sono comunemente considerate attività volontarie e dannose condotte da avversari che hanno alcuni incentivi per attaccare un obiettivo specifico. In questa categoria rientrano le minacce in cui l'intento dannoso non è evidente. Si basano principalmente su errori umani e configurazioni errate del sistema ma possono anche riferirsi a disastri fisici che colpiscono le infrastrutture IT. Anche attribuite alla loro natura, queste minacce hanno una presenza costante nel panorama delle minacce annuali e sono una delle principali preoccupazioni per le valutazioni del rischio.

Figura 1. Relazione sul panorama delle minacce dell'ENISA 2021 - Principali minacce

Occorre rilevare che le predette minacce riguardano le categorie e l'insieme delle minacce, consolidate nelle otto aree sopra menzionate. Ciascuno dei gruppi di minacce viene ulteriormente analizzato in un capitolo dedicato di questa relazione che ne elabora le particolarità e fornisce informazioni, risultati, tendenze, tecniche di attacco e vettori di mitigazione più specifici.

1.2. TENDENZE CHIAVE

L'elenco seguente riassume le principali tendenze osservate nel panorama delle minacce informatiche durante il periodo in esame. Tali tendenze vengono inoltre esaminate nel dettaglio nei vari capitoli che comprendono la Relazione sul panorama delle minacce dell'ENISA 2021.

- Sono proliferati i **compromessi della catena di approvvigionamento altamente sofisticati e di forte impatto**, come evidenziato dalla Relazione sul panorama delle minacce dall'ENISA sulla catena di approvvigionamento. I **fornitori di servizi gestiti** sono obiettivi di alto valore per i criminali informatici.
- La **COVID-19 ha guidato le attività di spionaggio informatico** e ha creato **opportunità per i criminali informatici**.
- **Le organizzazioni governative hanno intensificato il loro gioco** sia a livello nazionale che internazionale. Sono stati osservati maggiori sforzi da parte dei governi per interrompere e intraprendere azioni legali contro gli attori delle minacce sponsorizzati dallo stato.
- **I criminali informatici sono sempre più motivati dalla monetizzazione** delle loro attività, ad es. ransomware. La **criptovaluta** rimane il metodo di pagamento più comune per gli attori delle minacce.
- Gli attacchi criminali informatici **prendono sempre più di mira e incidono sulle infrastrutture critiche**.
- I **compromessi tramite messaggi di posta elettronica di phishing e la forzatura bruta su Remote Desktop Services (RDP)** rimangono i due **vettori di infezione ransomware** più comuni.
- L'attenzione ai **modelli di business di tipo Ransomware as a Service (RaaS)** è aumentata nel 2021, rendendo difficile l'attribuzione corretta dei singoli attori delle minacce.
- Il verificarsi di schemi **ransomware a tripla estorsione** è aumentato notevolmente nel corso del 2021.
- Il **declino del malware** osservato nel 2020 continua nel 2021. Nel 2021, abbiamo rilevato un aumento degli attori delle minacce che ricorrevano a linguaggi di programmazione relativamente nuovi o non comuni per veicolare il proprio codice.
- Il **malware indirizzato agli ambienti container** è diventato molto più diffuso, con nuove evoluzioni come il malware senza file eseguito dalla memoria.
- Gli sviluppatori di malware continuano a trovare modi per **rendere più difficile il reverse engineering e l'analisi dinamica**.
- Il volume delle **infezioni da cryptojacking** ha raggiunto un **livello elevato** nel primo trimestre del 2021, rispetto agli ultimi anni. Il **guadagno finanziario** associato al cryptojacking ha incentivato gli attori delle minacce a eseguire questi attacchi.
- **Il volume di cryptomining nel 2021 e le attività di cryptojacking sono a livelli record**.
- Possiamo vedere che sta avvenendo un **passaggio dal browser al cryptojacking basato su file.**
- La **COVID-19 è ancora l'esca dominante nelle campagne** di attacchi tramite posta elettronica.
- Il **Business E-mail Compromise (BEC)** è **aumentato**, è diventato più **sofisticato** e più mirato.
- Il modello di business **Phishing-as-a-Service (PhaaS)** sta prendendo sempre più piede.
- Gli attori delle minacce hanno spostato la loro attenzione verso le **informazioni sui vaccini** nel contesto delle minacce ai dati e alle informazioni.
- Si è verificata un'**impennata delle violazioni dei dati relative al settore sanitario**.
- I tradizionali attacchi DDoS (Distributed Denial of Service) si stanno spostando verso le **reti mobili e l'IoT (Internet of Things)**.
- **Ransom Denial of Service (RDoS)** è la nuova frontiera degli attacchi Denial of Service.
- La **condivisione delle risorse in ambienti virtualizzati** funge da amplificatore degli attacchi DDoS.
- Le **campagne DDoS** nel 2021 sono diventate più mirate e molto più persistenti e sempre più multivettoriali.
- La **disinformazione abilitata dall'intelligenza artificiale (AI)** supporta gli aggressori nello svolgimento dei loro attacchi.
- Il **phishing è al centro degli attacchi di disinformazione** e sfrutta fortemente le convinzioni delle persone.

- La **disinformazione e la cattiva informazione** sono al centro delle attività di criminalità informatica e stanno aumentando a un ritmo senza precedenti.
- Il **modello di business Disinformation-as-a-Service (DaaS)** è cresciuto in modo significativo, stimolato dal crescente impatto della pandemia di COVID-19 e dalla necessità di avere più informazioni.
- Nel 2020 e nel 2021 abbiamo osservato un **picco di incidenti non dannosi** poiché la pandemia di COVID-19 è diventata un moltiplicatore di **errori umani** e **configurazioni errate del sistema** fino al punto che la maggior parte delle violazioni nel 2020 sono state causate da errori.
- Si è verificato un **picco di incidenti non dannosi per la sicurezza del cloud**.

1.3. VICINANZA DELLE PRINCIPALI MINACCE NELL'UE

Un aspetto importante da considerare nel contesto della Relazione sul panorama delle minacce dell'ENISA riguarda la vicinanza di una minaccia informatica rispetto all'Unione Europea (UE). Ciò è particolarmente importante per assistere gli analisti nella valutazione dell'importanza delle minacce informatiche, correlarli con potenziali attori e vettori di minacce e persino per guidare la selezione di vettori di mitigazione mirati appropriati. In linea con la classificazione proposta per la politica di sicurezza e difesa comune (PSDC) dell'UE ([7]), classifichiamo le minacce informatiche in quattro categorie, come illustrato nella Tabella 1.

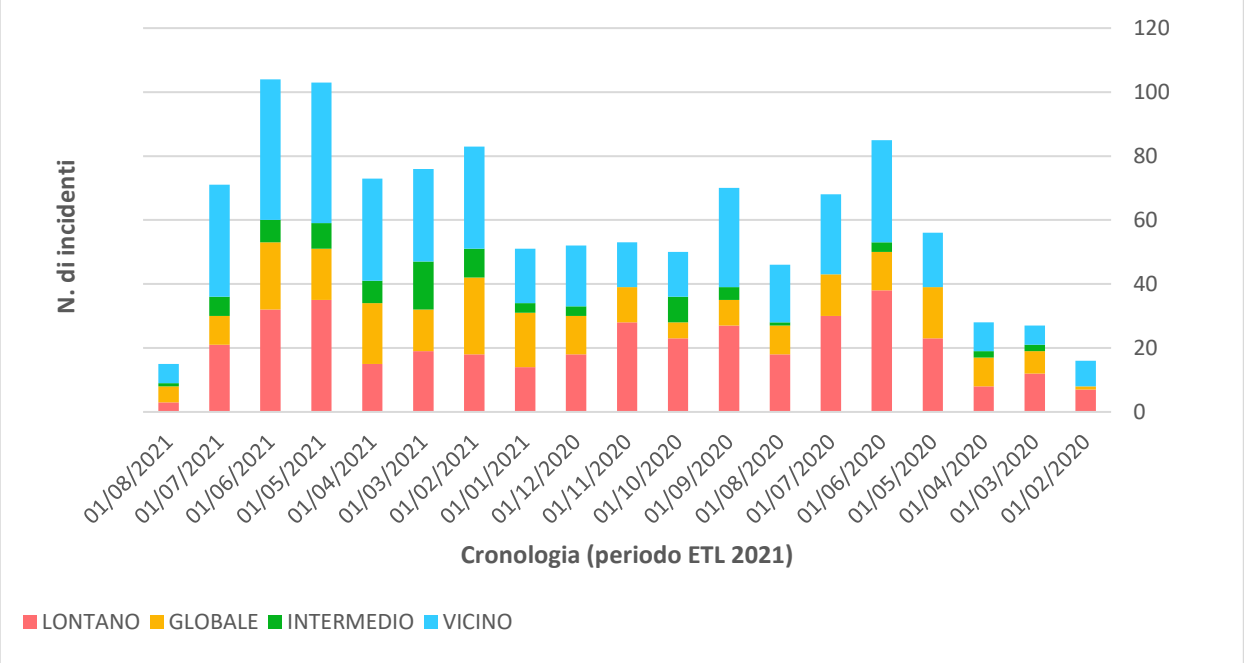
Tabella 1. Classificazione di prossimità delle minacce informatiche

Prossimità	Preoccupazioni
NEAR	Reti, sistemi interessati, controllati e assicurati all'interno dei confini dell'UE. Popolazione colpita all'interno dei confini dell'UE.
MID	Reti e sistemi ritenuti vitali per gli obiettivi operativi nell'ambito del mercato unico digitale dell'UE e dei settori NISD, ma il loro controllo e la loro garanzia dipendono da autorità istituzionali o pubbliche o private non appartenenti all'UE. Popolazione colpita in aree geografiche vicine ai confini dell'UE.
FAR	Reti e sistemi che, se influenzati, avranno un impatto critico sugli obiettivi operativi nell'ambito del mercato unico digitale dell'UE e dei settori NISD. Il controllo e la garanzia di tali reti e sistemi esulano dalle autorità istituzionali dell'UE o dalle autorità pubbliche o private degli Stati membri (SM). Popolazione interessata in aree geografiche lontane dall'UE.
GLOBAL	Tutte le aree indicate in precedenza

La Figura 2 illustra una cronologia degli incidenti relativi alle categorie di principali minacce segnalate nell'ETL 2021. Si precisa che le informazioni nel grafico sono basate su OSINT (Open Source Intelligence) ed è frutto del lavoro di ENISA nell'area della Situational Awareness ([8]).

([7]) https://www.europarl.europa.eu/RegData/etudes/STUD/2017/603175/EPRS_STU(2017)603175_EN.pdf
([8]) In conformità con l'art. 7, par. 6 del regolamento UE sulla cibersicurezza https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN

Figura 2. Cronologia degli incidenti osservati relativi alle principali minacce ETL (consapevolezza situazionale basata su OSINT) in termini di prossimità.



Come evidenziato dalla figura sopra, il 2021 ha visto un numero maggiore di incidenti rispetto al 2020. In particolare, la categoria NEAR ha un numero in costante aumento di incidenti osservati relativi a minacce principali, il che implica la loro importanza nel contesto dell'UE. Non sorprende che le tendenze mensili (non mostrate nella figura per brevità) siano abbastanza simili tra le diverse classificazioni poiché la sicurezza informatica non conosce confini e nella maggior parte dei casi le minacce si materializzano a tutti i livelli di prossimità. È interessante notare che, durante gli ultimi mesi coperti da ETL 2021, si osserva una maggiore vicinanza all'UE NEAR, una tendenza che l'ENISA continuerà a monitorare per vedere come si evolve e come si collega alle attività degli attori della minaccia e dei vettori di minaccia in corso.

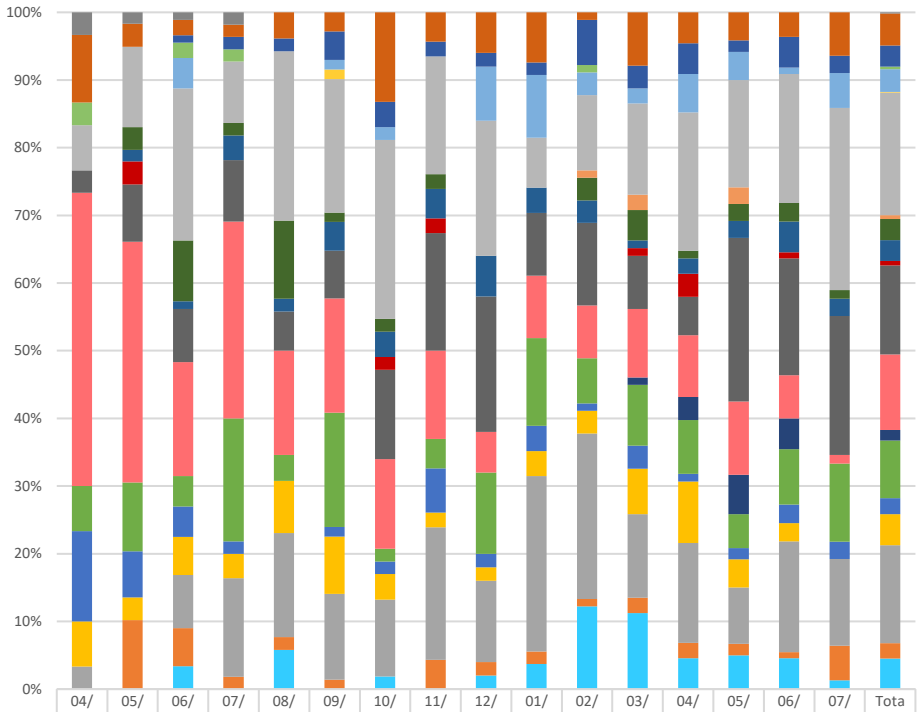
1.4. PRINCIPALI MINACCE PER SETTORE

Le minacce informatiche di solito non sono limitate a un particolare settore e nella maggior parte dei casi colpiscono più di uno di essi. Ciò è effettivamente vero poiché in molti casi le minacce si manifestano sfruttando le vulnerabilità nei sistemi ICT sottostanti che vengono utilizzati in una varietà di settori. Tuttavia, gli attacchi mirati e gli attacchi che sfruttano le differenze nella maturità della sicurezza informatica tra i settori e la popolarità/prominenza di determinati settori sono tutti fattori che devono essere considerati. Questi fattori contribuiscono alle minacce che si manifestano come incidenti in settori specifici ed è per questo che è importante esaminare in profondità gli aspetti settoriali degli incidenti e delle minacce osservati. Inoltre, le tendenze rilevate in ciascun settore e le dipendenze intersettoriali sono osservazioni che possono essere tratte da tale analisi.

La figura 3 e la figura 4 evidenziano i settori interessati relativi agli incidenti osservati sulla base di OSINT (Open Source Intelligence) ed è il risultato del lavoro dell'ENISA nell'area della Situational Awareness ([9]). Si riferiscono a incidenti legati alle principali minacce di ETL 2021. Si tratta del primo tentativo dell'ENISA di mappare l'impatto delle minacce su settori specifici. Nei prossimi anni e nelle future iterazioni del panorama delle minacce, si cercherà di allineare i settori con quelli elencati nella Direttiva sulla sicurezza delle reti e dell'informazione (NISD) e nella proposta per la sua revisione (NISD 2.0).

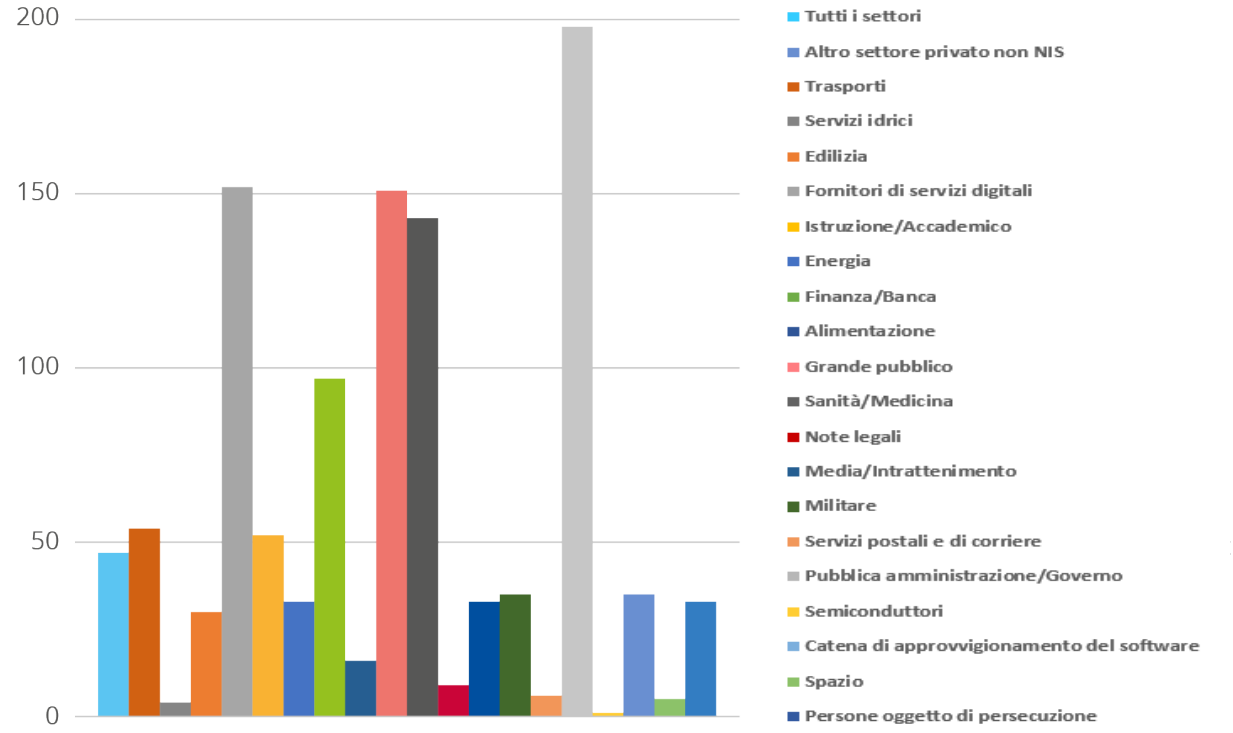
([9]) In conformità con l'art. 7, par. 6 del regolamento UE sulla cibersicurezza https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN)

Figura 3. Cronologia degli incidenti osservati relativi alle principali minacce ETL in termini di settore interessato.



	04/20	05/20	06/20	07/20	08/20	09/20	10/20	11/20	12/20	01/21	02/21	03/21	04/21	05/21	06/21	07/21	Totale
Servizi idrici	1	1	1	1													2
Trasporti	3	2	2	1	2	2	7	2	3	4	1	7	4	5	4	5	49
Persone oggetto di persecuzione			1	1	1	3	2	1	1	1	6	3	4	2	5	2	33
Spazio	1		2	1							1						4
Catena di approvvigionamento del software			4			1	1		4	5	3	2	5	5	1	4	35
Semiconduttori						1											1
Pubblica amministrazione/Governo	2	7	20	5	13	14	14	8	10	4	10	12	18	19	21	21	189
Servizi postali e di corriere											1	2		3			6
Militare		2	8	1	6	1	1	1			3	4	1	3	3	1	33
Media/Intrattenimento		1	1	2	1	3	2	2	3	2	3	1	2	3	5	2	32
Note legali		2					1	1				1	3		1		7
Sanità/Medicina	1	5	7	5	3	5	7	8	10	5	11	7	5	29	19	16	137
Grande pubblico	13	21	15	16	8	12	7	6	3	5	7	9	8	13	7	1	117
Alimentazione												1	3	7	5		16
Finanza/Banca	2	6	4	10	2	12	1	2	6	7	6	8	7	6	9	9	89
Energia	4	4	4	1		1	1	3	1	2	1	3	1	2	3	2	25
Istruzione/Accademico	2	2	5	2	4	6	2	1	1	2	3	6	8	5	3		48
Fornitori di servizi digitali	1		7	8	8	9	6	9	6	14	22	11	13	10	18	10	151
Edilizia		6	5	1	1	1		2	1	1	1	2	2	2	1	4	24
Tutti i settori			3		3		1		1	2	11	10	4	6	5	1	47

Figura 4. Settori interessati per numero di incidenti (aprile 2020-luglio 2021)



Durante questo periodo in esame, un gran numero di incidenti ha preso di mira la pubblica amministrazione, il governo e i fornitori di servizi digitali. Quest'ultimo è prevedibile data la fornitura orizzontale di servizi per questo settore e quindi il suo impatto su molti altri settori. Abbiamo anche osservato un numero significativo di incidenti rivolti agli utenti finali e non necessariamente a un settore particolare. Anche il settore sanitario è stato preso di mira in modo significativo e questa attività mostra segnali di aumento negli ultimi mesi del periodo in esame (maggio-luglio 2021). È interessante notare che il settore finanziario affronta un numero consistente di incidenti durante tutto l'anno. La catena di approvvigionamento del software mostra anche un aumento del numero di incidenti durante il 2021 che è anche un'osservazione nella Relazione sul panorama delle minacce dell'ENISA sulla catena di approvvigionamento ([10]).

1.5. METODOLOGIA

La Relazione sul panorama delle minacce dell'ENISA (ETL) 2021 si basa su informazioni disponibili da fonti aperte, principalmente di natura strategica e sulle capacità di Cyber Threat Intelligence (CTI) dell'ENISA, e copre più di un settore, tecnologia e contesto. La relazione si propone di essere neutrale rispetto al settore e al fornitore e richiama o cita il lavoro di varie ricerche e di blog nel campo della sicurezza e articoli di stampa, nel testo in diverse note a piè di pagina. L'intervallo di tempo della relazione ETL 2021 va da aprile 2020 a luglio 2021 ed è denominato "periodo in esame" in tutta la relazione.

Per la produzione della relazione ETL 2021 è stato utilizzato il seguente approccio. Per tutto il periodo di tempo in questione, l'ENISA, per mezzo della consapevolezza situazionale, ha raccolto un elenco dei principali incidenti così come apparivano nelle fonti aperte. Questo elenco è servito come base per l'identificazione dell'elenco delle principali minacce e il materiale di partenza per diverse tendenze e statistiche nella relazione.

Successivamente, è stata condotta una ricerca approfondita della letteratura disponibile da fonti aperte, come articoli di stampa, pareri di esperti, rapporti di intelligence, analisi degli incidenti e sono stati condotti rapporti di

([10]) Relazione sul panorama delle minacce dell'ENISA sugli attacchi alla catena di approvvigionamento, luglio 2021. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

ricerca sulla sicurezza dall'ENISA ed esperti esterni. Attraverso un'analisi continua, l'ENISA ha derivato tendenze e punti di interesse per ciascuna delle principali minacce presentate in ETL 2021. I risultati e i giudizi chiave di questa valutazione si basano su risorse multiple e pubblicamente disponibili fornite nei riferimenti utilizzati per lo sviluppo di questo documento.

All'interno della relazione, cerchiamo di distinguere tra ciò che è stato riportato dalle nostre fonti e ciò che è la nostra valutazione. (Lo facciamo utilizzando specificamente la frase "nella nostra valutazione"). Infine, quando conduciamo una valutazione, trasmettiamo la probabilità utilizzando parole che esprimono una stima della probabilità (ad es. probabile, molto probabile, certamente) ([11]).

Il framework MITRE ATT&CK®([12]) è stato utilizzato in questa relazione per evidenziare le tattiche e le tecniche di attacco rilevanti per una determinata minaccia (vedi Allegato A). Per ogni tattica ATT&CK® vengono presentate le tecniche utilizzate dall'avversario. Questo può portare a un elenco di mitigazioni ([13]) ATT&CK che si possono applicare. MITRE ATT&CK® è una knowledge base, un linguaggio comune per tattiche e tecniche contraddittorie basate su osservazioni del mondo reale. La knowledge base MITRE ATT&CK® viene utilizzata come base per lo sviluppo di modelli e metodologie di minaccia specifici nel settore privato, nel governo e nella comunità di prodotti e servizi di sicurezza informatica.

La relazione è stata convalidata dal gruppo di lavoro ad hoc l'ENISA sul panorama delle minacce informatiche ([14]), istituito nell'aprile 2021, un gruppo composto da esperti di enti pubblici e privati europei e internazionali.

Per il futuro sviluppo della Relazione sul panorama delle minacce, l'ENISA sta formalizzando una nuova metodologia per promuovere la trasparenza e porre le basi per processi strutturati e ben allineati. In questo sforzo, insieme a una tassonomia delle minacce rivista, la metodologia per i panorami delle minacce sarà resa pubblica in futuro.

1.6. STRUTTURA DELLA RELAZIONE

La Relazione sul panorama delle minacce dell'ENISA (ETL) 2021 ha mantenuto la struttura dei precedenti report ETL utilizzando una struttura simile per evidenziare le principali minacce informatiche nel 2021. I lettori delle passate iterazioni noteranno che le categorie di minacce sono state consolidate in linea con il passaggio a una nuova tassonomia delle minacce alla sicurezza informatica da utilizzare in futuro.

La relazione è così articolata:

Il **capitolo 2** esplora le tendenze relative agli attori delle minacce (ovvero attori sponsorizzati dallo stato, attori della criminalità informatica, attori hacker su commissione e attivisti informatici).
Il **capitolo 3** discute i principali risultati, incidenti e tendenze riguardanti il ransomware.
Il **capitolo 4** presenta i principali risultati, incidenti e tendenze riguardanti il malware.
Il **capitolo 5** descrive i principali risultati, incidenti e tendenze riguardanti il cryptojacking.
Il **capitolo 6** mette in evidenza i principali risultati, incidenti e tendenze riguardanti le minacce legate alla posta elettronica.
Il **capitolo 7** discute i principali risultati, incidenti e tendenze riguardanti le minacce ai dati.
Il **capitolo 8** presenta i principali risultati, incidenti e tendenze riguardanti le minacce alla disponibilità e all'integrità.
Il **capitolo 9** sottolinea l'importanza delle minacce ibride e descrive i principali risultati, incidenti e tendenze in materia di disinformazione e cattiva informazione.
Il **capitolo 10** si concentra sui principali risultati, incidenti e tendenze riguardanti le minacce non dannose.
L'**allegato A** presenta le tecniche comunemente utilizzate per ogni minaccia, basate sul framework MITRE ATT&CK®.
L'**allegato B** include incidenti degni di nota per minaccia, come osservato durante il periodo in esame.

([11]) CIA - Parole di probabilità di stimahttps://www.cia.gov/static/0aae8f84700a256abf63f7aad73b0a7d/Words-of-Estimative-Probability.pdf
([12]) MITRE ATT&CK® , https://attack.mitre.org/
([13]) https://attack.mitre.org/mitigations/enterprise /
([14]) https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/ad-hoc-working-group-cyber-threat-landscapes