enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

IT

Da gennaio 2019 ad aprile 2020

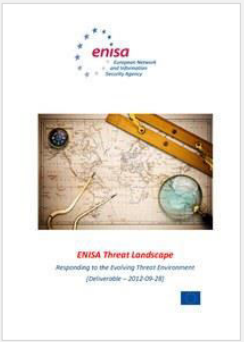
L'anno in rassegna

Panorama delle minacce analizzato dall'ENISA

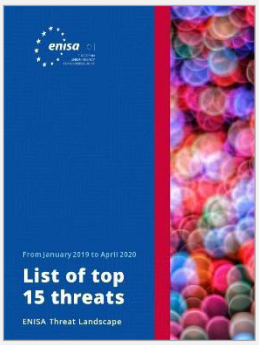
Prima di iniziare

_ 8 anni di analisi del panorama delle minacce

In questo 2020 l'**Agenzia dell'Unione europea per la cibersicurezza (ENISA)** festeggia un anno dall'entrata in vigore del nuovo regolamento sulla cibersicurezza e l'ottava edizione della relazione sul panorama delle minacce (ETL). Il regolamento sulla cibersicurezza[1] rinnova e rafforza il ruolo dell'ENISA conferendole un mandato permanente, maggiori risorse e nuovi compiti. L'agenzia inizia inoltre un nuovo capitolo, con un nuovo direttore esecutivo, una nuova strategia e una nuova struttura organizzativa. Alla luce di tutti questi cambiamenti, è tempo che anche la relazione sul panorama delle minacce si evolva e adotti una nuova struttura e un carattere moderno, abbandonando prolissità e staticità. Con una nuova identità visiva e un nuovo formato, la relazione sul panorama delle minacce è diventata un report digitale versatile, dinamico e di facile utilizzo, che punta a soddisfare le aspettative di un pubblico sempre più ampio ed esigente.



ETL 2012



ETL 2020

Il percorso della relazione sul panorama delle minacce dell'ENISA dal 2012 al 2020

_ Formato della relazione

Questa edizione prende in esame il panorama delle minacce per il periodo compreso tra gennaio 2019 e aprile 2020 ed è strutturata nel modo seguente.

L'ANNO IN RASSEGNA. Questa relazione offre un quadro generale del panorama delle minacce, delineando gli argomenti più importanti richiamati in tutte le altre relazioni. Fornisce inoltre l'elenco delle prime 15 minacce, le conclusioni e le raccomandazioni a cura dell'ENISA.

QUADRO GENERALE DELL'INTELLIGENCE SULLE MINACCE INFORMATICHE. Questa relazione riassume gli argomenti più rilevanti per la comunità dell'intelligence sulle minacce informatiche (Cyber Threat Intelligence, CTI) e quelli trattati in diversi forum.

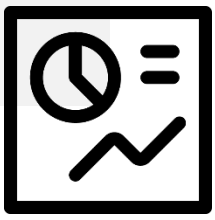
ANALISI DELLE MINACCE SETTORIALI E TEMATICHE. Questa relazione riassume il lavoro più recente prodotto dall'ENISA, con la descrizione del panorama delle minacce per settori e tecnologie specifici. Quest'anno vengono presentati i risultati del lavoro svolto per 5G, Internet degli oggetti (Internet of Things, IoT) e auto intelligenti.

INCIDENTI PRINCIPALI NELL'UE E A LIVELLO MONDIALE. Questa relazione fornisce un quadro generale dei principali incidenti di cibersicurezza verificatisi nell'UE e a livello mondiale, evidenziando gli insegnamenti che è possibile trarne.

ARGOMENTI DI RICERCA. Questa relazione presenta gli aspetti essenziali legati alla ricerca e all'innovazione nella cibersicurezza.

TENDENZE EMERGENTI. Questa relazione individua le tendenze emergenti, puntando l'attenzione sulle sfide e sulle opportunità per il futuro nel campo della cibersicurezza.

ELENCO DELLE PRIME 15 MINACCE. A ogni minaccia è dedicata una relazione, con presentazione del quadro generale, dei risultati, degli incidenti principali, delle statistiche, dei vettori di attacco e delle relative misure di mitigazione.



Prima di iniziare

Metodologia

I contenuti prodotti per la relazione sul panorama delle minacce si basano su informazioni disponibili da fonti aperte, prevalentemente di natura strategica, e coprono più settori, tecnologie e contesti. 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, chiaramente identificati nel testo in diverse note finali.

Nella compilazione della relazione sul panorama delle minacce dell'ENISA si è seguito un duplice approccio. In primo luogo, 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 rapporti di ricerca sulla sicurezza. Secondariamente, sono state condotte interviste con i componenti del gruppo di portatori di interessi ETL, che sono esperti del settore e membri della Cyber Threat Intelligence Community dell'UE. Quest'ultima ci ha aiutato a definire l'elenco delle prime 15 minacce e a convalidare le ipotesi sulle tendenze e sulle sfide future della cibersicurezza.

Desideriamo ringraziare anche i componenti del gruppo di portatori di interessi sulla CTI per il sostegno fornito nella compilazione delle relazioni nel corso di queste otto edizioni. I componenti di questo gruppo esaminano e convalidano l'analisi prodotta per ogni relazione ETL ed esprimono il loro voto sull'elenco annuale delle prime 15 minacce informatiche.

Saremmo lieti di ricevere il vostro feedback su questa relazione.
Dedicate un momento alla compilazione del questionario. Per accedere al modulo, fare clic qui.

Chi sono i destinatari delle relazioni

La relazione ETL è in parte strategica e in parte tecnica, con informazioni pertinenti per lettori sia tecnici sia non tecnici. L'ETL si rivolge a un pubblico eterogeneo, con diversi livelli di linguaggio tecnico, a seconda del campo e dell'importanza dell'argomento per lettori non specialisti. La tabella seguente descrive il tipo di pubblico e di contenuto per ogni relazione ETL.

Relazione ETL	TIPO DI CONTENUTO	PUBBLICO DESTINATARIO
L'ANNO IN RASSEGNA	Generico	Tutti
QUADRO GENERALE DELLA CTI	Specifico	Membri della comunità CTI e professionisti.
ANALISI DELLE MINACCE SETTORIALI E TEMATICHE	Strategico	Esperti di gestione strategica, responsabili delle politiche e decisori, analisti del rischio, gestori e responsabili della cibersicurezza.
INCIDENTI PRINCIPALI NELL'UE E A LIVELLO MONDIALE	Strategico	Esperti di gestione strategica, responsabili delle politiche e decisori, analisti del rischio, gestori e responsabili del rischio.
ARGOMENTI DI RICERCA	Strategico	Esperti di gestione strategica, responsabili delle politiche e decisori, analisti del rischio, gestori e responsabili del rischio.
TENDENZE EMERGENTI	Strategico	Esperti di gestione strategica, responsabili delle politiche e decisori, analisti del rischio, gestori e responsabili del rischio.
ELENCO DELLE PRIME 15 MINACCE	Tecnico	Gestori della sicurezza delle informazioni (ISM), direttori della sicurezza delle informazioni (CISO), specialisti della cibersicurezza e specialisti di CTI.

Le prime 15 minacce

Principali minacce nel 2018		Tendenze valutate
1	Malware	---
2	Attacchi basati sul web	↗
3	Attacchi alle applicazioni web	---
4	Phishing	↗
5	Negazione del servizio (denial of service)	↗
6	Spam	---
7	Botnet	↗
8	Violazioni dei dati	↗
9	Minacce interne	↙
10	Manipolazione fisica, danneggiamento, furto e perdita	---
11	Fuga di informazioni	↗
12	Furto d'identità	↗
13	Cryptojacking	↗
14	Ransomware	↙
15	Ciberspionaggio	↙

Principali minacce nel periodo 2019 -2020		Tendenze valutate	Variazione in classifica
1	Malware	---	---
2	Attacchi basati sul web	---	↗
3	Phishing	↗	↗
4	Attacchi alle applicazioni web	---	↙
5	Spam	↙	↗
6	Negazione del servizio (denial of service)	↙	↙
7	Furto d'identità	↗	↗
8	Violazioni dei dati	---	---
9	Minacce interne	↗	---
10	Botnet	↙	↙
11	Manipolazione fisica, danneggiamento, furto e perdita	---	↙
12	Fuga di informazioni	↗	↙
13	Ransomware	↗	↗
14	Ciberspionaggio	↙	↗
15	Cryptojacking	↙	↙

Legenda: Tendenze: In calo, --- Stabile, In aumento ↗ **Classifica**: In rialzo, --- Invariato, ↗ In discesa ↙

Quadro generale

Che cosa è cambiato nel panorama

Gli anni 2019 e 2020 hanno portato cambiamenti significativi nel panorama delle minacce informatiche descritto in queste relazioni. Due fatti distinti hanno contribuito in misura significativa a questi cambiamenti: le forze di trasformazione improvvisa, senza precedenti nella storia, determinate dalla **pandemia di malattia da coronavirus 2019 (COVID-19)** e la tendenza di costante aumento delle **capacità avanzate degli autori delle minacce**. Sorprendentemente, questi ultimi hanno finito per amplificare l'impatto della pandemia di COVID-19 nel ciberspazio.

La pandemia di COVID-19 ha imposto l'adozione su larga scala della tecnologia per gestire una serie di aspetti critici della crisi, come il coordinamento dei servizi sanitari, la risposta internazionale alla diffusione di COVID-19, l'adozione di regimi di telelavoro, l'apprendimento a distanza, la comunicazione interpersonale, il controllo delle misure di confinamento, la teleconferenza e molti altri. Considerata la situazione, i leader aziendali hanno valutato i rischi emergenti da un'adozione improvvisa (della tecnologia) scaturita dalla trasformazione imposta dalla pandemia di COVID-19[2]. E la **cibersicurezza si è trovata di fronte a un paradosso: essere al tempo la sfida e l'opportunità in questa trasformazione**. I cambiamenti imposti nel panorama della tecnologia dell'informazione (IT) hanno indebolito le misure di cibersicurezza esistenti, trasformandone il rapido adattamento in uno sfida. Allo stesso tempo, **la cibersicurezza è lo strumento generatore di fiducia nei casi d'uso emergenti per i servizi digitali e ha perciò l'opportunità di agevolare la trasformazione.**

Lavorando da casa, **gli specialisti della cibersicurezza hanno dovuto adattare le difese esistenti** a un nuovo paradigma infrastrutturale, nel tentativo di ridurre al minimo l'esposizione a una serie di nuovi attacchi, dove i punti di ingresso sono costituiti dalle case collegate a Internet e da altri dispositivi intelligenti dei dipendenti. Contemporaneamente e sotto una forte pressione, hanno dovuto attuare soluzioni basate su componenti precedentemente meno affidabili, come l'accesso remoto attraverso la rete Internet pubblica, servizi cloud, servizi di video streaming e dispositivi e applicazioni mobili non protetti. La necessaria reazione alla pandemia di COVID-19 per garantire la sicurezza e ridurre nel contempo l'impatto sulle imprese ha spinto al limite la capacità delle organizzazioni di rispondere ai cambiamenti. Inoltre, numerosi *modi operandi* si sono rapidamente adattati all'evoluzione dei modelli di lavoro, **per cui anche i professionisti della cibersicurezza si sono trovati ad agire ai limiti delle loro capacità**.

In tempi brevissimi, i professionisti della sicurezza IT hanno dovuto rispondere rapidamente alle sfide introdotte dal lavoro da casa, come i movimenti di dati aziendali ogni volta che i dipendenti utilizzano la rete Internet domestica per accedere ad applicazioni basate su cloud, software aziendali, videoconferenze e condivisione di file.

Non essendo ancora completamente sotto controllo, e considerata l'incertezza della sua diffusione futura, si prevede che la pandemia di COVID-19 continuerà a costituire una sfida per i professionisti della cibersicurezza. Inoltre, dato il tempo che intercorre prima che gli incidenti vengano individuati e analizzati, lascerà la sua impronta sul panorama delle minacce informatiche ancora per molto tempo. La pandemia di COVID-19 ha dimostrato negli attori malintenzionati un livello di capacità che ha permesso loro di adattarsi rapidamente a questa trasformazione. Nel 2019-2020 il *modus operandi* degli avversari si è concentrato sulla personalizzazione dei vettori di attacco. Metodi avanzati di furto di credenziali, credential stuffing, attacchi di phishing altamente mirati, attacchi avanzati di ingegneria sociale, tecniche avanzate di offuscamento del malware e una più estesa penetrazione delle piattaforme mobili sono i principali risultati conseguiti dagli avversari nel periodo in esame. Se i criminali informatici inizieranno a combinare questi progressi con l'intelligenza artificiale e l'apprendimento automatico, assisteremo in futuro a un aumento di attacchi andati a buon fine e di campagne non rilevabili.

Quadro generale

_ Sintesi

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 nelle diverse relazioni che compongono il panorama delle minacce del 2020.

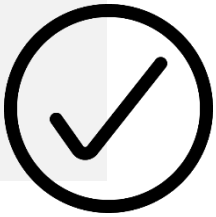
01_ **La superficie di attacco nella cibersicurezza continua a espandersi in concomitanza con l'ingresso in una nuova fase della trasformazione digitale.**

02_ **Vi sarà una nuova norma sociale ed economica dopo la pandemia di COVID-19, ancora più dipendente da un ciberspazio sicuro e affidabile.**

03_ **L'uso delle piattaforme dei social media negli attacchi mirati è una tendenza seria e tocca diversi campi e tipi di minacce.**

04_ **Attacchi finemente mirati e persistenti a dati di alto valore (ad esempio proprietà intellettuale e segreti di Stato) vengono pianificati ed eseguiti con meticolosità da attori sponsorizzati da Stati.**

05_ **Attacchi massicci di breve durata e di vasto impatto vengono utilizzati con diversi obiettivi, come il furto di credenziali.**



_ Sintesi

06_ La motivazione dietro la maggior parte degli attacchi informatici è sempre quella economica.

07_ Il ransomware rimane diffuso, con conseguenze onerose per molte organizzazioni.

08_ È ancora alto il numero di incidenti di cibersicurezza che passano inosservati o richiedono molto tempo per essere rilevati.

09_ Con una maggiore automazione della sicurezza, le organizzazioni investiranno maggiormente nella preparazione utilizzando l'intelligence sulle minacce informatiche (Cyber Threat Intelligence) come funzionalità principale.

10_ Il numero delle vittime del phishing continua a crescere, poiché questa tecnica sfrutta la dimensione umana che costituisce l'anello più debole.

Con tutti i cambiamenti osservati nel panorama delle minacce informatiche e le sfide generate dalla pandemia di COVID-19, la strada da percorrere perché il ciberspazio diventi un ambiente affidabile e sicuro per tutti è ancora molto lunga.

Quadro generale

_ I cittadini dell'UE sono più consapevoli dei rischi e delle sfide che il ciberspazio comporta?

La Commissione europea ha preparato una speciale indagine Eurobarometro[4] nel 2019, con l'obiettivo di comprendere la consapevolezza, le esperienze e le percezioni dei cittadini dell'UE in merito alla cibersicurezza.

EUROBAROMETRO

I risultati di questa indagine mostrano che l'uso di Internet in Europa continua a crescere, in particolare attraverso gli smartphone, e che i cittadini sono più consapevoli dei potenziali pericoli quando navigano in rete.

Secondo i risultati dell'indagine, i timori per la privacy e la sicurezza online hanno già portato più di 9 utenti di Internet su 10 a modificare il loro comportamento online, per lo più evitando di aprire e-mail di sconosciuti, installando software antivirus, visitando solo siti web noti e fidati e utilizzando solo i propri computer.

Anche se questi risultati sono piuttosto incoraggianti, molti utenti continuano essere vittime di frodi online e di phishing via posta elettronica. Ciò rivela che gli attori malintenzionati utilizzano attacchi sofisticati, più difficili da individuare ed evitare. Le strategie di mitigazione devono perciò essere aggiornate regolarmente, tenendo conto dell'intelligence (CTI) più recente sulle tecniche di attacco.

«Il panorama delle minacce sta diventando estremamente difficile da mappare. Non solo gli autori degli attacchi sviluppano nuove tecniche per eludere i sistemi di sicurezza, ma le minacce diventano sempre più complesse e precise in attacchi mirati».

in ETL 2020

Che cosa aspettarsi

_ È probabile che gli attori sponsorizzati da Stati nazionali

TENDENZA	DESCRIZIONE	MINACCIA
→	**Continuino** a servirsi del ciberspazio per sferrare attacchi contro i processi elettorali di paesi stranieri, minacciando i sistemi democratici e i diritti umani.[5]	**Attacchi contro i diritti umani e i sistemi democratici**
→	**Continuino** a vessare le opposizioni e a monitorare i loro cittadini attraverso la manipolazione delle informazioni sui social network, abbinata a campagne di spyware.	**Attacchi contro i diritti umani e i sistemi democratici**
↗	**Lancino** sofisticate campagne di disinformazione[6] volte a influenzare le percezioni o a manipolare le opinioni a favore di una determinata agenda politica o di obiettivi di speculazione finanziaria.	**Campagne di disinformazione**
↗	**Intensifichino** la corsa agli armamenti informatici[7] nel tentativo di sviluppare capacità informatiche. Se il ciberspazio è considerato un campo di battaglia, è probabile che gli Stati nazionali vadano in cerca di armi informatiche tramite agenti sponsorizzati in preparazione di un ciberconflitto.	**Corsa incontrollata agli armamenti informatici**
↗	**Perseguano** obiettivi strategici, quali carpire segreti industriali attraverso lo spionaggio, ottenere un'influenza sul processo decisionale politico, finanziare il regime attraverso la frode finanziaria, condurre operazioni di informazione con il supporto dell'informatica e, infine, indebolire o demoralizzare l'avversario attraverso attività perturbanti o distruttive.	**Furto di dati**

È probabile che gli autori di reati informatici

TENDENZA	DESCRIZIONE	MINACCIA
→	**Continuino** a prendere di mira adolescenti e giovani adulti con attacchi di sextortion (ricatto sessuale) che colpiscono psicologicamente e, in definitiva, fisicamente le vittime.[8]	**Sextortion (ricatto sessuale)**
↗	**Aumentino** il numero di attacchi di cyberbullismo durante e dopo la pandemia di COVID-19, dato l'incremento dell'uso di piattaforme digitali da parte degli adolescenti per scopi personali e didattici.[9]	**Cyberbullismo**

È probabile che i criminali informatici

TENDENZA	DESCRIZIONE	MINACCIA
↗	**Aumentino** il ricorso a strumenti basati sull'intelligenza artificiale (IA) per creare contenuti contraffatti (in formato immagine, audio e video) altamente credibili, noti come «deepfake», per frodare le aziende.	**Deepfake**
→	**Migliorino** le tattiche per compromettere i processi aziendali allo scopo di ottenere un vantaggio economico.	**Compromissione dei processi aziendali (Business process compromise, BPC)**
→	**Abbassare** un livello nell'organizzazione, al di sotto del dirigente, per compromettere le e-mail aziendali.	**Compromissione delle e-mail aziendali (Business e-mail compromise, BEC)**
→	**Incrementino** il ricorso a fornitori di servizi gestiti (managed service provider, MSP) per la diffusione di malware.	**Malware**

Conclusioni e raccomandazioni

Conclusioni/raccomandazioni di natura politica

- Negli ultimi decenni i responsabili delle politiche e i tecnici hanno vissuto in mondi separati e parlato lingue diverse. Per affrontare le sfide poste dalla digitalizzazione, ora devono **lavorare insieme** sin dall'inizio e sviluppare un approccio comune. Essendo la maggior parte della tecnologia attuale connessa al ciberspazio, il contributo degli esperti di sicurezza informatica in molte di queste discussioni è essenziale.
- Con la crescita dell'innovazione tecnologica e la rapida espansione del ciberspazio, politiche di cibersicurezza efficaci ed esaurienti a livello dell'UE sono di fondamentale importanza. **Politiche di cibersicurezza mature** forniranno la necessaria capacità di difesa a tutti i livelli della società: pubbliche amministrazioni, infrastrutture critiche, aziende, settore terziario e singoli individui. La capacità di difesa deve essere efficace e flessibile per affrontare le nuove sfide che si presentano, tenendo testa alla costante evoluzione del ciberspazio.
- Dato il numero crescente di portatori di interessi a livello dell'UE e degli Stati membri coinvolti in attività di CTI, **la cooperazione e il coordinamento** rispetto a queste attività in tutta l'Unione sono essenziali. L'ENISA promuoverà la cooperazione con vari portatori di interessi e compirà il tentativo iniziale di individuare i requisiti in termini di CTI dei vari gruppi di portatori di interessi, in particolare all'interno dell'UE (vale a dire la Commissione, gli organismi, le agenzie e gli Stati membri dell'UE).
- La CTI deve essere considerata lo strumento principale per la **preparazione in materia di cibersicurezza** e la promozione di approcci basati sul rischio. L'integrazione della CTI con i processi di gestione della sicurezza ne favorirà la diffusione nelle aree correlate e aumenterà l'agilità di processi solitamente lunghi, come la certificazione e la valutazione del rischio. La CTI sarà vista inoltre come «facilitatore» delle decisioni di emergenza necessarie nella gestione delle crisi.
- La pertinenza della CTI per le decisioni strategiche e politiche è ampiamente accettata e ritenuta essenziale per agevolare il **collegamento con le informazioni geopolitiche** e i sistemi ciberfisici. Ciò consentirà l'inclusione della CTI nei processi decisionali a livello dell'UE, permettendo inoltre di ampliarne il contesto all'identificazione delle minacce ibride.

Conclusioni/raccomandazioni di natura commerciale

- Nel corso del 2019 si è reso disponibile un numero crescente di **laboratori di prova e poligoni virtuali**[10], in locale e con offerte cloud. Si tratta di risorse importanti per la formazione del personale, con la possibilità di simulare gli attacchi e sperimentare diverse strategie di difesa: tutto in un ambiente virtuale polivalente.
- Sebbene siano stati elaborati alcuni criteri e requisiti di CTI per vari profili di utente, **requisiti analoghi** saranno necessari per ulteriori prodotti, servizi e strumenti di CTI. Per favorire l'adozione di prodotti e servizi di CTI, sarà necessario che i relativi fornitori tengano maggiormente conto delle esigenze degli utenti.
- Gli investimenti in alcuni concetti di base, in particolare **maturità della CIT e gerarchia delle minacce**, sono molti utili per la diffusione della CTI. I fornitori dovranno orientare le offerte a vari livelli di maturità della CTI per favorirne l'uso intelligente all'interno di organizzazioni di dimensioni e con budget diversi.
- Nel lungo periodo, sembra che **OpenCTI**[11] possa essere una valida soluzione alla frammentazione delle offerte, data la sua capacità intrinseca di integrare fonti di CTI di vario tipo in un unico ambiente di strumenti. I fornitori di CTI dovranno prevedere i necessari «raccordi», per consentire l'integrazione dei loro prodotti con OpenCTI. Il concetto di poligono virtuale è stato inizialmente definito nel 2013 dall'Agenzia europea per la difesa (AED) nel rapporto «Common Staff target for military cooperation on cyber ranges in the European Union» (obiettivo comune in materia di personale per la collaborazione militare sui poligoni virtuali nell'Unione europea), come ambiente polivalente a sostegno di tre processi primari: sviluppo, garanzia e diffusione delle conoscenze.

Conclusioni e raccomandazioni

_ Conclusioni e raccomandazioni relative alla ricerca e alla formazione

- L'UE deve continuare a investire nella **R&S in tema di cibersicurezza**, con particolare accento sulle iniziative di ricerca a lungo termine e ad alto rischio. La ricerca e l'innovazione a lungo termine sono un esercizio oneroso, fuori dalla portata della maggior parte delle organizzazioni del settore privato.
- Espandere le conoscenze e le competenze in materia di cibersicurezza è fondamentale per migliorare la preparazione e la resilienza. L'UE deve continuare a **costruire capacità** investendo in programmi di formazione, certificazioni professionali, esercizi e campagne di sensibilizzazione in materia di sicurezza informatica.
- La ricerca sulla cibersicurezza dovrebbe includere competenze provenienti da discipline sociali, comportamentali ed economiche. La **ricerca multidisciplinare** nella sicurezza informatica deve essere promossa e incentivata in tutta l'UE.
- I risultati dei progetti di ricerca nell'area della cibersicurezza, e della CTI in particolare, devono essere valutati e mappati in un contesto più ampio al fine di individuare **sovrapposizioni e lacune** e di renderli confrontabili con i prodotti, i servizi e le prassi commerciali esistenti. Ciò favorirà la diffusione di tali risultati alla comunità di utenti.
- È necessario sviluppare approcci nuovi per l'acquisizione della conoscenza in materia di CTI da parte dei domini che possono trarne vantaggio. **Alcuni esempi sono i poligoni virtuali, le minacce ibride e le valutazioni geopolitiche.** Le sinergie conseguite possono incrementare i casi d'uso e migliorare la qualità dei contenuti in modo multidirezionale.
- L'uso dell'**intelligenza artificiale (IA)** e dell'apprendimento automatico nell'ambito della CTI merita un ulteriore approfondimento. Consentirà di ridurre il numero di operazioni manuali nell'analisi della CTI e aumenterà il valore delle funzioni di apprendimento automatico all'interno delle attività di CTI.
- Dovranno essere promossi la fornitura e l'impiego di materiale open source sulla CTI, allo scopo di facilitare il **trasferimento delle conoscenze** ma anche di abbassare la soglia delle competenze richieste in questo campo.

«La complessità delle competenze in materia di minacce è aumentata nel 2019, con molti avversari che utilizzano exploit, furto di credenziali e attacchi a più livelli».

in ETL 2020

Riferimenti bibliografici

1. «Regolamento UE sulla cibersicurezza». Aprile 2019. Parlamento europeo e Consiglio dell'Unione europea https://eur-lex.europa.eu/eli/reg/2019/881/oj

2. «COVID-19 Risks Outlook: A Preliminary Mapping and its Implications». 19 maggio 2020. FEM. https://www.weforum.org/reports/covid-19-risks-outlook-a-preliminary-mapping-and-its-implications

3. «Comunicazione congiunta al Parlamento europeo, al Consiglio europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni. Contrastare la disinformazione sulla Covid-19 – Guardare ai fatti». Giugno 2020. Commissione europea. https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A52020JC0008

4. «Special Eurobarometer 499: Europeans' attitudes towards cyber security». 29 gennaio 2020. https://data.europa.eu/euodp/en/data/dataset/S2249_92_2_499_ENG

5. «EUvsDisinfo» https://euvsdisinfo.eu/european-elections-2019/

6. "Manipulating Social Media to Undermine Democracy". 2017. Freedom House. https://freedomhouse.org/report/freedom-net/2017/manipulating-social-media-undermine-democracy

7. «Conceptualising Cyber Arms Races» 2016. Centro di eccellenza per la ciberdifesa cooperativa della NATO (NATO CCD COE). https://ccdcoe.org/uploads/2018/10/Art-10-Conceptualising-Cyber-Arms-Races.pdf

8. «How online 'sextortion' drove one young man to suicide». 8 febbraio 2018. Today. https://www.today.com/parents/how-online-sextortion-drove-one-young-man-suicide-t122735

9. «Cyberbullying may increase during COVID-19 pandemic, expert says». 30 marzo 2020. Healio. https://www.healio.com/news/pediatrics/20200330/cyberbullying-may-increase-during-covid19-pandemic-expert-says

10. Il concetto di poligono virtuale è stato inizialmente definito nel 2013 dall'Agenzia europea per la difesa (AED) nel rapporto «Common Staff target for military cooperation on cyber ranges in the European Union» (obiettivo comune in materia di personale per la collaborazione militare sui poligoni virtuali nell'Unione europea), come ambiente polivalente a sostegno di tre processi primari: sviluppo, garanzia e diffusione delle conoscenze.

11. Open CTI. https://www.opencti.io/en/

«La CTI si è saldamente affermata nel campo della cibersicurezza come strumento essenziale per migliorare l'agilità e l'efficienza nella difesa dagli attacchi informatici».

in ETL 2020

Correlati

LEGGI LA RELAZIONE

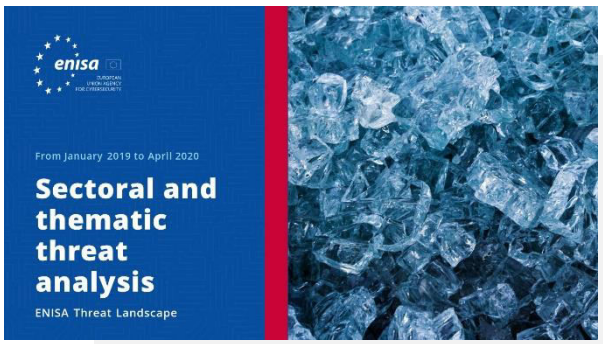
Relazione sul panorama delle minacce dell'ENISA
Elenco delle prime 15 minacce

Elenco stilato dall'ENISA delle prime 15 minacce nel periodo tra gennaio 2019 e aprile 2020.

LEGGI LA RELAZIONE

Relazione sul panorama delle minacce dell'ENISA
Argomenti di ricerca

Raccomandazioni su argomenti di ricerca di vari quadranti nella cibersicurezza e nell'intelligence sulle minacce informatiche.



LEGGI LA RELAZIONE

Relazione sul panorama delle minacce dell'ENISA **Analisi delle minacce settoriali e tematiche**

Analisi contestualizzata delle minacce tra gennaio 2019 e aprile 2020.

Relazione sul panorama delle minacce dell'ENISA **Incidenti principali nell'UE e a livello mondiale**

Principali incidenti di cibersicurezza verificatisi tra gennaio 2019 e aprile 2020.

LEGGI LA RELAZIONE

Relazione sul panorama delle minacce dell'ENISA **Tendenze emergenti**

Principali tendenze nella cibersicurezza osservate tra gennaio 2019 e aprile 2020.

LEGGI LA RELAZIONE

Relazione sul panorama delle minacce dell'ENISA
Quadro generale dell'intelligence sulle minacce informatiche

Situazione attuale dell'intelligence sulle minacce informatiche nell'UE.

LEGGI LA RELAZIONE

Informazioni

_ L'agenzia

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 UE sulla cibersicurezza, l'Agenzia dell'Unione europea per la cibersicurezza
contribuisce alla politica dell'UE in questo campo, aumenta 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 di domani. 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 al seguente indirizzo: www.enisa.europa.eu.

Autori

Christos Douligeris, Omid Raghimi, Marco Barros Lourenço (ENISA), Louis Marinos (ENISA) e *tutti i componenti del gruppo di portatori di interessi sulla CTI dell'ENISA:* Andreas Sfakianakis, Christian Doerr, Jart Armin, Marco Riccardi, Mees Wim, Neil Thaker, Pasquale Stirparo, Paul Samwel, Pierluigi Paganini, Shin Adachi, Stavros Lingris (CERT EU) e Thomas Hemker.

Redattori

Marco Barros Lourenço (ENISA) e Louis Marinos (ENISA).

Contatti

Per informazioni sul documento, si prega di rivolgersi al seguente indirizzo press@enisa.europa.eu.

Per richieste dei media sulla relazione, si prega di utilizzare il seguente indirizzo press@enisa.europa.eu.

Avvertenza legale

Si rammenta che, salvo diversamente indicato, la presente pubblicazione riflette l'opinione e l'interpretazione dell'ENISA. La presente pubblicazione non deve intendersi come un'azione legale intrapresa dall'ENISA o da suoi organi, a meno che non venga adottata ai sensi del regolamento (UE) N. 526/2013. La presente pubblicazione non rappresenta necessariamente lo stato dell'arte e l'ENISA si riserva il diritto di aggiornarla di volta in volta.

Secondo necessità, sono state citate anche fonti di terze parti. L'ENISA non è responsabile del contenuto delle fonti esterne, quali i siti web esterni riportati nella presente pubblicazione.

La presente pubblicazione è unicamente a scopo informativo. Deve essere accessibile gratuitamente. L'ENISA, o chiunque agisca in suo nome, declina ogni responsabilità per l'uso che può essere fatto delle informazioni di cui alla presente pubblicazione.

ISBN: 978-92-9204-354-4
DOI: 10.2824/552242

Vasilissis Sofias Str 1, Maroussi 151 24, Attiki, Grecia
Tel.: +30 28 14 40 9711
info@enisa.europa.eu
www.enisa.europa.eu

enisa
EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

https://www.enisa.europa.eu