enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

IT

Da gennaio 2019 ad aprile 2020

Analisi delle minacce settoriali/ tematiche

Panorama delle minacce analizzato dall'ENISA

Quadro generale

Oltre a indicare le motivazioni degli avversari, fornisce prove sulle più comuni tecniche di attacco e sull'esposizione alle minacce attinenti a un particolare settore, indicando così i requisiti e le priorità di protezione. Per quanto riguarda i temi, l'analisi delle minacce e delle sfide associate a specifiche tecnologie emergenti contribuisce al processo di accertamento, valutazione e mitigazione dei rischi futuri.

L'intelligence sulle minacce informatiche (CTI) contestualizzata per i settori è uno strumento di preparazione importante per trarre conclusioni sugli attacchi informatici previsti all'interno di uno specifico settore.

_Statistiche sugli incidenti nel settore vs esposizione valutata dei settori emergenti

La contestualizzazione della CTI di settore si basa principalmente sugli incidenti di cibersicurezza rilevati in un settore. Pur trattandosi di un metodo standard per le componenti IT e i servizi digitali esistenti e consolidati, non include le tecnologie emergenti. Ciò è dovuto principalmente all'assenza di informazioni sugli incidenti per le tecnologie ancora in fase pilota o sperimentale. La CTI per le tecnologie emergenti è contestualizzata attraverso la valutazione delle minacce di categorie di asset attinenti a un settore specifico. L'ENISA esegue tali valutazioni per settori emergenti come 5G, IoT[5] e auto intelligenti.[6]. I panorami delle minacce settoriali e tematiche e le valutazioni della protezione di base sono i metodi utilizzati dall'ENISA per contestualizzare la CTI.

In questa relazione, oltre alla CTI di settore fondata sulle statistiche basate sugli incidenti, viene presentata una sintesi della CTI valutata per i settori tecnologici emergenti, sulla scorta del lavoro dell'ENISA.


«Nel corso del prossimo decennio, i rischi legati alla cibersicurezza diventeranno più difficili da valutare e interpretare a causa della crescente complessità del panorama delle minacce, dell'ecosistema degli aggressori e dell'espansione della superficie di attacco.»
in ETL 2020

Quadro generale

_Necessità urgente di statistiche accurate e aggiornate degli incidenti per settore

Le statistiche sugli incidenti settoriali sono uno strumento essenziale per comprendere le dinamiche dell'evoluzione delle minacce, i moventi degli avversari, l'esposizione degli asset e le azioni sugli obiettivi. A causa della complessità degli attacchi, delle dipendenze tra gli asset presi di mira e della natura intersettoriale delle vulnerabilità sfruttate, le statistiche degli incidenti presentano alcune incertezze intrinseche derivate dai fatti seguenti.

- In varie statistiche di settore si nota una serie di **incidenti classificati come «sconosciuti»**[12]. Questa percentuale varia tra l'1,5% e il 5%. Se questi incidenti potessero essere associati ad alcuni dei settori noti, tale percentuale potrebbe influenzare l'ordine dei bersagli. Inoltre, la mole significativa di tecniche di attacco sconosciute (circa il 15%) aggiunge incertezza alla valutazione dei moventi degli agenti delle minacce.
- La maggior parte degli **attacchi richiede più di una fase** (in media tre) per raggiungere gli obiettivi del bersaglio finale. In molti casi, in un singolo attacco sono coinvolti più bersagli di vari settori. Pertanto un incidente registrato nell'ambito di un settore può derivare da diversi incidenti in altri settori, che costituiscono fasi intermedie dell'attacco. Tali dipendenze tra gli incidenti possono influire sull'accuratezza delle statistiche degli incidenti.
- A parte il numero di incidenti per settore, un elemento importante per l'analisi statistica è la **natura delle tecniche di attacco utilizzate**. Queste informazioni possono fornire prove utili sul vettore di attacco più frequentemente utilizzato e contribuire a definire la priorità delle misure di protezione necessarie per un particolare settore.

- La materializzazione delle minacce dipende fortemente dalle esistenti **opportunità che vengono esplorate dagli avversari**. In seguito alla pandemia di COVID-19, ad esempio, gli ambienti IT sono diventati decentrati. Ciò indebolisce i controlli di sicurezza applicati all'interno della rete di un'azienda, il che spiega lo spostamento degli attacchi da bersagli aziendali a bersagli individuali.[1] L'esempio è indicativo della necessità di «tradurre» i cambiamenti osservati nelle statistiche alla luce delle opportunità emergenti.
- Le statistiche attuali vengono elaborate tenendo conto di vari criteri. Le **variazioni nei criteri** delle statistiche impediscono confronti tra le statistiche degli incidenti. Ad esempio:
    - A seconda dei portatori di interessi/contributori del soggetto che raccoglie le informazioni, la base dei dati sulle statistiche potrebbe non coprire tutti i settori in modo uniforme;
    - La classificazione degli incidenti può essere basata sulla frequenza di accadimento, indipendentemente dall'entità del danno (ad esempio le dimensioni delle informazioni violate) o dal suo impatto.
- Un elemento essenziale delle statistiche settoriali è la **frequenza di accadimento** delle singole minacce informatiche. Ciò dà un'idea del metodo di attacco più comune impiegato in un settore. Tali statistiche possono offrire un'indicazione sul livello di preparazione richiesto o sulla maturità dei singoli controlli di sicurezza che riducono l'esposizione alle minacce informatiche pertinenti.
- Considerati i fatti sopra citati in merito alle statistiche degli incidenti, la presente relazione fornisce una classificazione approssimativa dei settori in termini di incidenti osservati, unitamente a una tendenza tracciata dalle dinamiche emergenti della potenziale esposizione di ciascun settore. Vengono fornite inoltre alcune informazioni sui vettori di attacco più diffusi per settore. A tale scopo, sono state consolidate le informazioni provenienti da varie pubblicazioni.[1][2][3][4]

Tendenze negli incidenti

SETTORE	MINACCE/ATTACCHI PIÙ DIFFUSI	TENDENZE DEGLI INCIDENTI
Persona fisica	• Phishing • Malware • Fuga di informazioni • Furto di dati	Stabile
Molteplicità di settori	• Attacchi alle applicazioni web • Phishing • Malware	In aumento
Pubblica amministrazione, difesa, servizi sociali	• Malware • Phishing • Attacchi basati sul web	Stabile, in leggera diminuzione
Finanziario/bancario/assicurativo	• Attacchi alle applicazioni web • Minaccia interna (abuso non intenzionale) • Malware • Furto di dati	Stabile
Sanitario/medico	• Malware • Minaccia interna (abuso/errore non intenzionale) • Attacchi alle applicazioni web	In aumento
Istruzione	• Malware • Ransomware • Attacchi basati sul web	Stabile, in leggera diminuzione
Informazione e comunicazione	• Attacchi alle applicazioni web • Minaccia interna (abuso/errore non intenzionale) • Malware	Stabile
Servizi professionali/digitali	• Attacco alle applicazioni web • Minaccia interna (abuso/errore non intenzionale) • Malware	Stabile
Arti, intrattenimento e giochi[8]	• Attacchi alle applicazioni web • Malware • Phishing	Stabile
Produzione	• Malware • Attacchi alle applicazioni web • Minaccia interna (abuso/errore non intenzionale)	Stabile

SETTORE	FATTORI D'INFLUENZA
Persona fisica	L'autoisolamento dovuto alle misure di confinamento per la COVID-19 ha portato ad ambienti IT dispersi/decentrati e all'isolamento degli utenti, che rappresentano bersagli più facili da ingannare e hanno meno controlli di sicurezza rispetto a quanto avviene negli ambienti centralizzati.
Molteplicità di settori	Gli utenti che operano da remoto per via delle misure di confinamento imposte dalla COVID-19 hanno reso più facili gli attacchi tramite phishing e la fuga di informazioni sensibili (ad esempio le credenziali).
Pubblica amministrazione, difesa, servizi sociali	L'utilizzo di servizi cloud può avere influito sulla sicurezza delle offerte pubbliche. Nondimeno, i servizi sociali sono stati oggetto di un numero significativo di attacchi a causa degli aiuti finanziari offerti ai cittadini durante la pandemia di COVID-19.
Finanziario/ bancario/assicurativo	La complessità del settore finanziario rende difficile l'interpretazione del panorama delle minacce, poiché campi diversi all'interno dei servizi finanziari e bancari possono confrontarsi con rischi e minacce informatici del tutto differenti.
Sanitario/medico	L'attenzione rivolta dai criminali informatici ai bersagli del settore sanitario è aumentata notevolmente a causa delle motivazioni finanziarie e dell'importanza del settore durante la pandemia di COVID-19.
Istruzione	Seppur stabile, nel 2020 questo settore è stato preso di mira da campagne di ciberspionaggio a causa dell'interesse verso i risultati della ricerca sulla COVID-19.
Informazione e comunicazione	Si tratta di un settore costantemente sotto pressione per via della difficoltà di proteggere una superficie d'attacco enorme, introdotta dalle piattaforme di media digitali. Per le organizzazioni di media online, gli attacchi che causano danni reputazionali sono una delle minacce più temibili.
Servizi professionali/ digitali	Sebbene stabile, nel 2020 questo settore è stato vittima di varie campagne nel tentativo di estrarre informazioni dagli utenti di servizi digitali che lavorano da casa durante la pandemia di COVID-19.
Arti, intrattenimento e giochi	Il passaggio da un modello di business su licenza a un modello su abbonamento, adottato dall'industria dei giochi, ha reso questo settore più appetibile per i criminali informatici.[8]
Produzione	Gli attacchi alla catena di fornitura e ai sistemi di controllo industriale costituiscono la principale minaccia per le aziende manifatturiere, che non possono chiudere una linea di produzione completa. Il furto di dati di proprietà intellettuale è un'altra grave minaccia per questo settore.

Minacce sulle tecnologie emergenti

La prossima generazione delle comunicazioni mobili o 5G

COMPONENTI CORRELATI – GRUPPI DI ASSET	ESPOSIZIONE ALLE MINACCE
Rete centrale	Abuso da accesso remoto, picchi di traffico di autenticazione, abuso dei dati di autenticazione/autorizzazione degli utenti, abuso di funzioni di rete ospitate da terzi, abuso della funzione di intercettazione legale, sfruttamento delle interfacce di programmazione delle applicazioni (API), sfruttamento di architettura e pianificazione mal progettate, sfruttamento di sistemi/reti configurati in modo errato o scadente, uso o amministrazione erronei della rete, dei sistemi e dei dispositivi, scenari di frode correlati a interconnessioni in roaming, movimento laterale, memory scraping, manipolazione del traffico di rete, ricognizione della rete e raccolta di informazioni, manipolazione dei dati di configurazione della rete, flooding doloso dei componenti della rete principale, dirottamento malevolo del traffico, manipolazione dell'orchestratore delle risorse di rete, uso improprio di strumenti di audit, usi opportunistici e fraudolenti di risorse condivise, registrazione di funzioni di rete malevole, traffic sniffing, attacchi sui canali laterali
Rete di accesso	Abuso di risorse dello spettro, falsificazione dell'ARP (Address Resolution Protocol), falso nodo della rete di accesso, attacco di flooding, cacciatori di IMSI, jamming su radiofrequenza, MAC spoofing, manipolazione dei dati di configurazione della rete di accesso, interferenze radio, manipolazione del traffico radio, dirottamento di sessione, frode di segnali, tempeste di segnali

COMPONENTI CORRELATI – GRUPPI DI ASSET	ESPOSIZIONE ALLE MINACCE
Multi-edge computing	Gateway MEC fasullo o malevolo, sovraccarico dei nodi edge, abuso di interfacce di programmazione delle applicazioni (API) aperte edge
Virtualizzazione delle funzioni di rete e reti software (Software Defined Network)	Abuso del protocollo DCI (Data Center Interconnect), abuso delle risorse computazionali del cloud, bypass della virtualizzazione di rete, abuso dell'host virtualizzato
Infrastruttura fisica	Manipolazione di apparecchiature hardware, calamità naturali che colpiscono l'infrastruttura di rete, sabotaggio/vandalismo fisico dell'infrastruttura di rete, minaccia da parte di personale di terzi che accede alle strutture dell'operatore di rete mobile (Mobile Network Operator, MNO), sfruttamento del formato UICC (Universal Integrated Circuit Card), compromissione delle apparecchiature dell'utente
Tutti i gruppi di asset 5G sopra indicati	Negazione del servizio (Denial of Service, DoS), violazione, fuga e furto di dati, distruzione e manipolazione delle informazioni, intercettazioni, sfruttamento delle vulnerabilità di software e hardware, codice o software malevolo, compromissione di catena di fornitura, fornitori e prestatori di servizi, minacce/attacchi mirati, sfruttamento di falle nella sicurezza, nella gestione e nelle procedure operative, abuso di autenticazione, furto o spoofing d'identità

Minacce sulle tecnologie emergenti

Internet degli oggetti (IoT)

COMPONENTI CORRELATI – GRUPPI DI ASSET	ESPOSIZIONE ALLE MINACCE
Fattore umano	Minaccia interna, problemi nel lavoro di squadra, limitazioni interne, hacktivismo, perdita di servizi di supporto, interruzione dell'erogazione di servizi, interruzione della rete, modifiche involontarie, sabotaggio, violazione di norme e regolamenti, violazione della legislazione, requisiti contrattuali, inosservanza dei requisiti contrattuali (ad esempio manutenzione del software), sfruttamento del software, ingegneria sociale, furto d'identità.
Progettazione del software	Minaccia interna, hacktivismo, modifiche involontarie, uso o amministrazione erronei di dispositivi e sistemi, sabotaggio, difetti nel ciclo di sviluppo di software sicuro (SDLC), difetti di terzi, inosservanza dei requisiti contrattuali (ad esempio manutenzione del software), sfruttamento del software, perdita/fuga di informazioni.
Sviluppo del software	Minaccia interna, hacktivismo, perdita di servizi di supporto, modifiche involontarie, uso o amministrazione erronei di dispositivi e sistemi, sabotaggio, vandalismo e furto, vulnerabilità del software, difetti nel processo SDLC, difetti di manutenzione, abuso di autorizzazione, sfruttamento del software, manipolazione dell'infrastruttura SDLC, perdita/fuga di informazioni.
Distribuzione del software	Minaccia interna, hacktivismo, perdita di servizi di supporto, modifiche involontarie, uso o amministrazione erronei di dispositivi e sistemi, sabotaggio, vandalismo e furto, vulnerabilità del software, difetti nel processo SDLC, difetti di terzi, abuso di autorizzazione, sfruttamento del software, manipolazione dell'infrastruttura SDLC, negazione del servizio, manipolazione delle informazioni, divulgazione, perdita/fuga di informazioni.

COMPONENTI CORRELATI – GRUPPI DI ASSET	ESPOSIZIONE ALLE MINACCE
Dati	Minaccia interna, hacktivismo, perdita di servizi di supporto, modifiche involontarie, uso o amministrazione erronei di dispositivi e sistemi, sabotaggio, vandalismo e furto, vulnerabilità del software, difetti nel processo SDLC, difetti di terzi, abuso di autorizzazione, sfruttamento del software, manipolazione dell'infrastruttura SDLC, negazione del servizio, manipolazione delle informazioni, divulgazione, perdita/fuga di informazioni.
Manutenzione	Minaccia interna, hacktivismo, interruzione dell'erogazione di servizi, interruzione della rete, modifiche involontarie, uso o amministrazione erronei di dispositivi e sistemi, danni causati da terzi, sabotaggio, vandalismo e furto, attacchi con accesso fisico, accesso forzato, requisiti contrattuali, vulnerabilità del software, difetti nel processo SDLC, difetti di terzi, inosservanza dei requisiti contrattuali (ad esempio manutenzione del software), difetti di manutenzione, abuso di autorizzazione, sfruttamento del software, manipolazione dell'infrastruttura SDLC, negazione del servizio, manipolazione delle informazioni, divulgazione, perdita/fuga di informazioni.
Componenti software	Minaccia interna, hacktivismo, perdita di servizi di supporto, modifiche involontarie, uso o amministrazione erronei di dispositivi e sistemi, danni causati da terzi, fuga di informazioni, sabotaggio, vandalismo e furto, attacchi con accesso fisico, accesso forzato, requisiti contrattuali, vulnerabilità del software, difetti nel processo SDLC, difetti di terzi, inosservanza dei requisiti contrattuali (ad esempio manutenzione del software), difetti di manutenzione, abuso di autorizzazione, sfruttamento del software, manipolazione dell'infrastruttura SDLC, negazione del servizio, manipolazione delle informazioni, divulgazione, perdita/fuga di informazioni.

Minacce sulle tecnologie emergenti

Auto intelligenti

COMPONENTI CORRELATI – GRUPPI DI ASSET	ESPOSIZIONE ALLE MINACCE
Sensori e attuatori per auto	Negazione del servizio, malware, manipolazione delle informazioni, attacchi mirati a OEM, attività non autorizzate, furto d'identità, abuso di autorizzazioni, manipolazione di informazioni, minacce contro sensori autonomi, minacce contro IA e apprendimento automatico, sabotaggio, vandalismo, furto, attacchi sui canali laterali, iniezione di guasti, furto, guasto o malfunzionamento di un sensore/attuatore, sfruttamento delle vulnerabilità del software, dirottamento del protocollo di comunicazione, attacchi man-in-the-middle/dirottamento di sessione, modifica involontaria dei dati o della configurazione di componenti dell'auto, utilizzo di informazioni e/o dispositivi di origine inaffidabile, uso errato della configurazione dei componenti dell'auto, interruzione della rete, inosservanza dei requisiti contrattuali, violazione di norme e regolamenti/violazione della legislazione/abuso di dati personali.
Algoritmi decisionali **Unità di controllo elettronico delle auto, componenti di elaborazione e decisionali** **Auto intelligenti Infrastruttura e sistemi backend**	Negazione del servizio, malware, manipolazione delle informazioni, attacchi mirati a OEM, attività non autorizzate, furto d'identità, abuso di autorizzazioni, manipolazione di informazioni, minacce contro IA e apprendimento automatico, sabotaggio, vandalismo, furto, guasto o malfunzionamento di un sensore/attuatore, sfruttamento delle vulnerabilità del software, guasto o interruzione di servizi, dirottamento del protocollo di comunicazione, data replay, attacchi man-in-the-middle/dirottamento di sessione, modifica involontaria dei dati o della configurazione di componenti dell'auto, utilizzo di informazioni e/o dispositivi di origine inaffidabile, uso errato della configurazione dei componenti dell'auto, perdita di segnale GNSS, interruzione della rete, inosservanza dei requisiti contrattuali, violazione di norme e regolamenti/violazione della legislazione/abuso di dati personali.

COMPONENTI CORRELATI – GRUPPI DI ASSET	ESPOSIZIONE ALLE MINACCE
Funzioni del veicolo Sensori e attuatori per auto Unità di controllo elettronico delle auto, componenti di elaborazione e decisionali	Negazione del servizio, malware, manipolazione delle informazioni, attacchi mirati a OEM, attività non autorizzate, furto d'identità, abuso di autorizzazioni, manipolazione di informazioni, minacce dirette a sensori autonomi, minacce contro IA e apprendimento automatico, sabotaggio, attacchi sui canali laterali, iniezione di guasto, furto, guasto o malfunzionamento di un sensore/attuatore, sfruttamento delle vulnerabilità del software, guasto o interruzione di servizi, dirottamento del protocollo di comunicazione, data replay, attacchi man-in-the-middle/dirottamento di sessione, modifica involontaria dei dati o della configurazione di componenti dell'auto, utilizzo di informazioni e/o dispositivi di origine inaffidabile, uso errato della configurazione dei componenti dell'auto, batteria dell'auto esaurita, interruzione della rete, inosservanza dei requisiti contrattuali, violazione di norme e regolamenti/violazione della legislazione/abuso di dati personali.
Gestione del software Unità di controllo elettronico delle auto, componenti di elaborazione e decisionali Componenti di comunicazione a bordo del veicolo	Negazione del servizio, malware, manipolazione delle informazioni, attacchi mirati a OEM, attività non autorizzate, furto d'identità, abuso di autorizzazioni, sabotaggio, attacchi sui canali laterali, iniezione di guasto, furto, guasto o malfunzionamento di un sensore/attuatore, sfruttamento delle vulnerabilità del software, guasto o interruzione di servizi, dirottamento del protocollo di comunicazione, attacchi man-in-the-middle/dirottamento di sessione, modifica involontaria dei dati o della configurazione di componenti dell'auto, utilizzo di informazioni e/o dispositivi di origine inaffidabile, interruzione della rete, inosservanza dei requisiti contrattuali, violazione di norme e regolamenti/violazione della legislazione/abuso di dati personali.
Componenti di comunicazione all'interno del veicolo	Negazione del servizio, malware, manipolazione delle informazioni, attacchi mirati a OEM, attività non autorizzate, furto d'identità, abuso di autorizzazioni, manipolazione di informazioni, sabotaggio, attacchi sui canali laterali, iniezione di guasto, furto, guasto o malfunzionamento di un sensore/attuatore, sfruttamento delle vulnerabilità del software, dirottamento del protocollo di comunicazione, data replay, attacchi man-in-the-middle/dirottamento di sessione, modifica involontaria dei dati o della configurazione di componenti dell'auto, utilizzo di informazioni e/o dispositivi di origine inaffidabile, uso errato della configurazione dei componenti dell'auto, interruzione della rete, inosservanza dei requisiti contrattuali, violazione di norme e regolamenti/violazione della legislazione/abuso di dati personali.

Minacce sulle tecnologie emergenti

_ Auto intelligenti

COMPONENTI CORRELATI – GRUPPI DI ASSET	ESPOSIZIONE ALLE MINACCE
Reti e protocolli di comunicazione. **Unità di controllo elettronico delle auto, componenti di elaborazione e decisionali** **Componenti di comunicazione a bordo del veicolo**	Negazione del servizio, malware, manipolazione delle informazioni, attacchi mirati a OEM, attività non autorizzate, furto d'identità, abuso di autorizzazioni, sabotaggio, furto, guasto o malfunzionamento di un sensore/attuatore, sfruttamento delle vulnerabilità del software, dirottamento del protocollo di comunicazione, data replay, attacchi man-in-the-middle/dirottamento di sessione, modifica involontaria dei dati o della configurazione di componenti dell'auto, utilizzo di informazioni e/o dispositivi di origine inaffidabile, uso errato della configurazione dei componenti dell'auto, interruzione della rete, inosservanza dei requisiti contrattuali, violazione di norme e regolamenti/violazione della legislazione/abuso di dati personali.
Componenti esterni di prossimità **Auto intelligenti Infrastruttura e sistemi backend**	Negazione del servizio, malware, manipolazione delle informazioni, attacchi mirati a OEM, attività non autorizzate, furto d'identità, abuso di autorizzazioni, sabotaggio, vandalismo, furto, sfruttamento delle vulnerabilità del software, guasto o interruzione di servizi, dirottamento del protocollo di comunicazione, attacchi man-in-the-middle/dirottamento di sessione, modifica involontaria dei dati o della configurazione di componenti dell'auto, utilizzo di informazioni e/o dispositivi di origine inaffidabile, perdita di segnale GNSS, interruzione della rete, inosservanza dei requisiti contrattuali, violazione di norme e regolamenti/violazione della legislazione/abuso di dati personali.

COMPONENTI CORRELATI – GRUPPI DI ASSET	ESPOSIZIONE ALLE MINACCE
Server, sistemi e cloud computing **Auto intelligenti** **Infrastruttura e sistemi backend**	Negazione del servizio, malware, manipolazione delle informazioni, attacchi mirati a OEM, attività non autorizzate, furto d'identità, abuso di autorizzazioni, manipolazione di informazioni, sabotaggio, sfruttamento delle vulnerabilità del software, guasto o interruzione dei servizi, dirottamento del protocollo di comunicazione, data replay, attacchi man-in-the-middle/dirottamento di sessione, modifica involontaria dei dati o della configurazione di componenti dell'auto, utilizzo di informazioni e/o dispositivi di origine inaffidabile, perdita di segnale GNSS, interruzione della rete, inosservanza dei requisiti contrattuali, violazione di norme e regolamenti/violazione della legislazione/abuso di dati personali.
Informazioni	Negazione del servizio, malware, manipolazione delle informazioni, attacchi mirati a OEM, attività non autorizzate, furto d'identità, abuso di autorizzazioni, manipolazione di informazioni, minacce dirette a sensori autonomi, minacce contro IA e apprendimento automatico, sabotaggio, vandalismo, furto, attacchi sui canali laterali, iniezione di guasto, furto, guasto o malfunzionamento di un sensore/attuatore, sfruttamento delle vulnerabilità del software, guasto o interruzione di servizi, dirottamento del protocollo di comunicazione, data replay, attacchi man-in-the-middle/dirottamento di sessione, modifica involontaria dei dati o della configurazione di componenti dell'auto, fuga di informazioni, utilizzo di informazioni e/o dispositivi di origine inaffidabile, uso errato della configurazione dei componenti dell'auto, perdita di segnale GNSS, interruzione della rete, inosservanza dei requisiti contrattuali, violazione di norme e regolamenti/violazione della legislazione/abuso di dati personali.
Esseri umani	Negazione del servizio, malware, manipolazione delle informazioni, attacchi mirati a OEM, attività non autorizzate, furto d'identità, abuso di autorizzazioni, manipolazione di informazioni, sabotaggio, vandalismo, furto, guasto o malfunzionamento di un sensore/attuatore, sfruttamento delle vulnerabilità del software, guasto o interruzione di servizi, dirottamento del protocollo di comunicazione, data replay, attacchi man-in-the-middle/dirottamento di sessione, modifica involontaria dei dati o della configurazione di componenti dell'auto, fuga di informazioni, utilizzo di informazioni e/o dispositivi di origine inaffidabile, uso errato della configurazione dei componenti dell'auto, perdita di segnale GNSS, batteria dell'auto esaurita, interruzione della rete, inosservanza dei requisiti contrattuali, violazione di norme e regolamenti/violazione della legislazione/abuso di dati personali.

Riferimenti bibliografici

1. «April 2020 Cyber Attacks Statistics». 3 giugno 2019. HACKMAGEDDON. https://www.hackmageddon.com/2020/06/03/april-2020-cyber-attacks-statistics/

2. «Data Breach Investigation Report» 2019. Verizon. https://enterprise.verizon.com/resources/reports/dbir/

3. «CIRCL - Operational Statistics» 2019. CIRCL. https://www.circl.lu/opendata/statistics/

4. «Survey: The Third Annual Study on the State of Endpoint Security Risk». 2020. https://engage.morphisec.com/2020-endpoint-security-risk-study

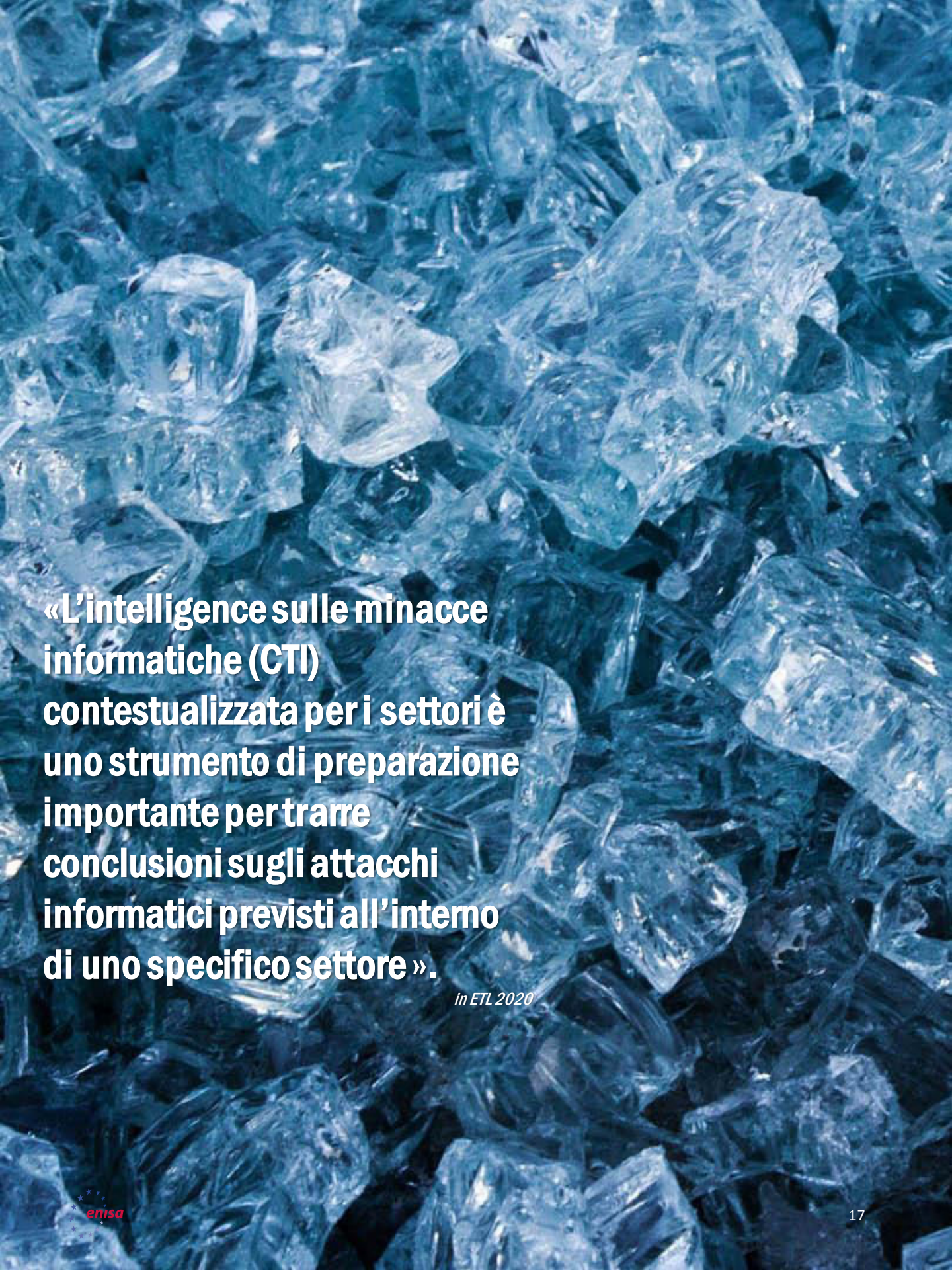
5. «Good Practices for Security of IoT - Secure Software Development Lifecycle». 19 novembre 2019. ENISA. https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1

6. «ENISA good practices for security of Smart Cars». 25 novembre 2019. https://www.enisa.europa.eu/publications/smart-cars

7. L'ordine dei settori selezionato è stato effettuato consolidando le statistiche di vari rapporti basati sugli incidenti. Esso fornisce valori medi per il periodo esame (2019-primo trimestre 2020) e può discostarsi leggermente dai valori presentati nei rapporti mensili o trimestrali.

8. «Player vs. Hacker: Cyberthreats to Gaming Companies and Gamers». 16 marzo 2020. Security Intelligence. https://securityintelligence.com/posts/player-vs-hacker-cyberthreats-to-gaming-companies-and-gamers/

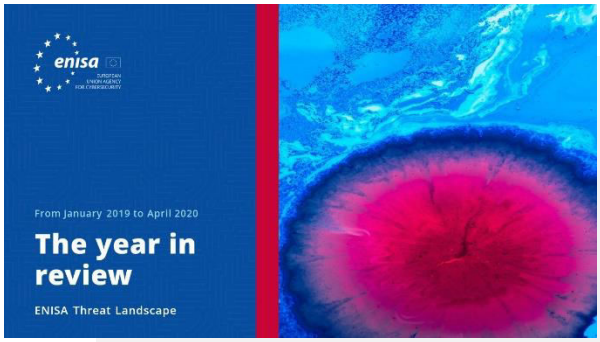
9. È opportuno menzionare che l'esposizione alle minacce è stata valutata attraverso categorie di minaccia dettagliate sviluppate dall'ENISA (vedere https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy/view) ed è utilizzata per varie valutazioni settoriali. A causa dell'assenza di dati sugli incidenti per i settori emergenti, la valutazione delle minacce scende in maggiore dettaglio per un approccio più esaustivo.



«L'intelligence sulle minacce informatiche (CTI) contestualizzata per i settori è uno strumento di preparazione importante per trarre conclusioni sugli attacchi informatici previsti all'interno di uno specifico settore ».

in ETL 2020

Correlati



Relazione sul panorama delle minacce dell'ENISA **L'anno in rassegna**

Una sintesi delle tendenze nella cibersicurezza per il periodo tra gennaio 2019 e aprile 2020.

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 **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 contattare il seguente indirizzo press@enisa.europa.eu.
Per richieste dei media sul documento, si prega di contattare il seguente indirizzo press@enisa.europa.eu.

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

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