PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 25 - numero 5413 di Lunedì 19 giugno 2023

Il rapporto annuale sul panorama delle minacce alla sicurezza informatica

ENISA mette ancora una volta a disposizione una preziosa ed aggiornata rassegna degli attacchi informatici nella UE. Ecco una sintesi del documento che rappresenta una lettura obbligata per ogni responsabile della sicurezza informatica aziendale.

Conoscere gli attaccanti e le più diffuse tecniche di attacco rappresentano preziosi strumenti, per chi da questi attacchi deve difendersi. La guerra in Ucraina ha modificato in modo significativo lo scenario di attacco e il documento di ENISA (European Network Information Security Agency) rappresenta una lettura obbligata per ogni responsabile della sicurezza informatica aziendale.

Questa è la decima edizione del rapporto ENISA Threat Landscape (ETL), un rapporto annuale sullo stato del panorama delle minacce alla sicurezza informatica. Esso identifica:

- le principali minacce,
- le principali tendenze osservate rispetto alle minacce, agli autori delle minacce e alle tecniche di attacco, nonché
- l'analisi dell'impatto e della motivazione.

ETL 2022 descrive inoltre le misure di mitigazione pertinenti. Il lavoro di quest'anno è stato nuovamente supportato dal gruppo di lavoro ad hoc dell'ENISA sugli scenari delle minacce alla sicurezza informatica (CTL). Durante il periodo di riferimento dell'ETL 2022, le principali minacce identificate includono:

1. Ransomware
2. Malware
3. Minacce di social engineering
4. Minacce contro i dati
5. Minacce contro la disponibilità: Denial of Service
6. Minacce contro la disponibilità: minacce Internet
7. Disinformazione ? mala informazione
8. Attacchi alla catena di approvvigionamento

Per ciascuna delle minacce individuate, vengono illustrate le tecniche di attacco, gli incidenti e le tendenze degni di nota, insieme a misure di mitigazione. Per quanto riguarda le tendenze analizzate durante il periodo di riferimento, è doveroso sottolineare quanto segue.

Impatto della geopolitica sul panorama delle minacce alla sicurezza informatica

Il conflitto tra Russia e Ucraina ha rimodellato il panorama delle minacce durante il periodo di riferimento. Alcuni dei cambiamenti interessanti sono stati gli aumenti significativi dell'attività degli attivisti informatici, attori informatici che conducono operazioni di concerto con l'azione militare vera e propria, la mobilitazione di attivisti informatici, la criminalità informatica e l'aiuto da parte di gruppi di stati-nazione durante questo conflitto.

La geopolitica continua ad avere un impatto rilevante sulle operazioni informatiche.

Gli attacchi distruttivi sono una componente importante delle operazioni degli attaccanti statali.

Durante il conflitto Russia-Ucraina, sono stati osservati soggetti informatici che conducevano operazioni in concomitanza con azioni militari sul campo.

Una nuova ondata di hacktivism è stata osservata soprattutto dall'inizio della crisi Russia-Ucraina.

La disinformazione è uno strumento della guerra informatica. È stato utilizzato anche prima dell'inizio della guerra "fisica" come attività preparatoria all'invasione russa dell'Ucraina.

Gli autori delle minacce aumentano le loro capacità

Gli autori delle minacce, ricchi di risorse, hanno utilizzato attacchi 0-day per raggiungere i loro obiettivi operativi e strategici. Più le organizzazioni aumentano la maturità delle proprie difese e dei programmi di sicurezza informatica, più aumentano i costi per gli avversari, spingendoli a sviluppare e/o acquistare attacchi 0-day, poiché le strategie di difesa in profondità riducono la disponibilità di vulnerabilità sfruttabili.

I continui "ritiri" e il rebranding dei gruppi di ransomware vengono utilizzati per evitare l'applicazione della legge e delle sanzioni.

Il modello di business Hacker-as-a-Service sta guadagnando terreno, in crescita rispetto al 2021.

I gruppi attaccanti hanno un interesse crescente e mostrano una capacità crescente negli attacchi alla catena di approvvigionamento e negli attacchi contro i fornitori di servizi gestiti (MSP).

Il ransomware e gli attacchi contro la disponibilità sono i più frequenti durante il periodo di riferimento

Aumento significativo degli attacchi contro la disponibilità, in particolare DDoS, e la guerra in corso è la ragione principale dietro tali attacchi.

Il phishing è ancora una volta il vettore più comune per l'accesso iniziale. I progressi nella sofisticazione del phishing, l'affaticamento degli utenti e il phishing mirato e basato sul contesto hanno portato a questo aumento. Le nuove lusinghe delle minacce di ingegneria sociale si stanno concentrando sul conflitto Ucraina-Russia in modo simile a quanto accaduto durante la situazione COVID

Il malware è di nuovo in aumento dopo la diminuzione notata e collegata alla pandemia COVID-19

Le tecniche di estorsione si stanno ulteriormente evolvendo con l'uso diffuso di siti temporanei.

Gli attacchi DDoS stanno diventando sempre più grandi e complessi, si stanno spostando verso le reti mobili e l'IoT e vengono utilizzati nel contesto della guerra informatica.

Minacce nuove, ibride ed emergenti stanno contrassegnando il panorama delle minacce con un impatto elevato

Il caso Pegasus ha innescato copertura mediatica e azioni governative, che si sono poi riflesse anche in altri casi riguardanti la sorveglianza e l'attacco alla società civile.

Gli attaccanti utilizzano il phishing del consenso per inviare agli utenti collegamenti che, se cliccati, concedono all'attaccante l'accesso e le autorizzazioni ad applicazioni e servizi.

La compromissione dei dati aumenta di anno in anno. Il ruolo centrale dei dati nella nostra società ha prodotto un forte aumento della quantità di dati raccolti e dell'importanza di una corretta analisi dei dati.

Il prezzo che paghiamo per tali attacchi è un continuo e inarrestabile aumento dei dati compromessi.

I modelli di Machine Learning (ML) sono al centro dei moderni sistemi distribuiti e stanno diventando sempre più il bersaglio di attacchi.

Disinformazione e deepfake abilitati dall'intelligenza artificiale.

La proliferazione di bot che modellano i personaggi può facilmente interrompere il processo normativo di "avviso e commento", nonché l'interazione della comunità, inondando le agenzie governative di commenti falsi. Inoltre, comprendere le tendenze relative agli autori delle minacce, le loro motivazioni e i loro obiettivi aiuta notevolmente nella pianificazione delle difese e delle strategie di mitigazione della sicurezza informatica. Pertanto, ai fini dell'ETL 2022, vengono nuovamente prese in considerazione le seguenti quattro categorie di autori di minacce alla sicurezza informatica:

- Attori sponsorizzati dagli Stati
- Attori della criminalità informatica
- Hackers a pagamento
- Hacktivisti.

Attraverso un'analisi continua, l'ENISA ha ricavato tendenze, modelli e approfondimenti per ciascuna delle principali minacce presentate nell'ETL 2022.

I risultati e i giudizi chiave in questa valutazione si basano su risorse multiple e pubblicamente disponibili, che sono messe a disposizione nei riferimenti utilizzati per lo sviluppo di questo documento.

Il rapporto si rivolge principalmente ai decisori strategici e ai responsabili politici, ma interessa anche la comunità tecnica della sicurezza informatica.

ENISA threat landscape 2022 (pdf)

Adalberto Biasiotti

---

www.puntosicuro.it