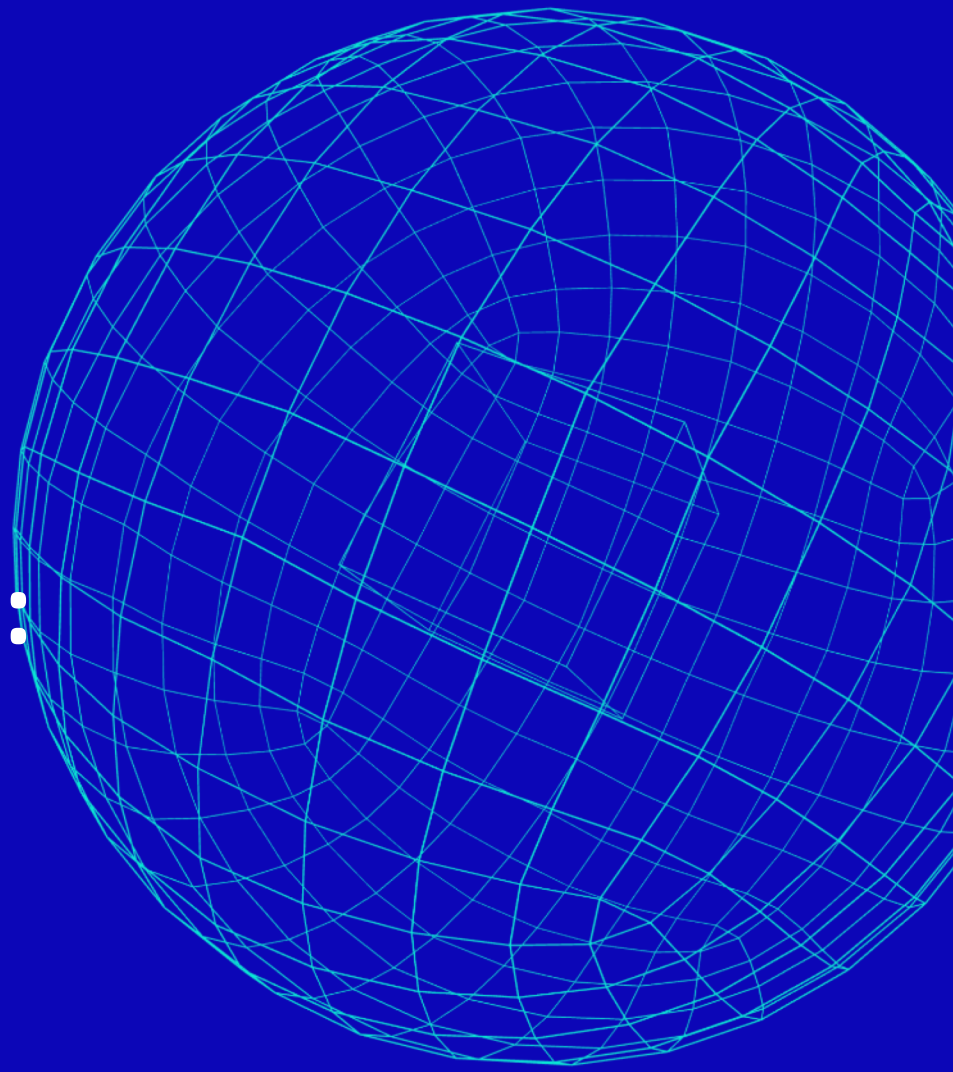
CERTFin

15 maggio 2024

Nuovi malware e vecchie insidie: affrontarli con l’aiuto della Threat Intelligence



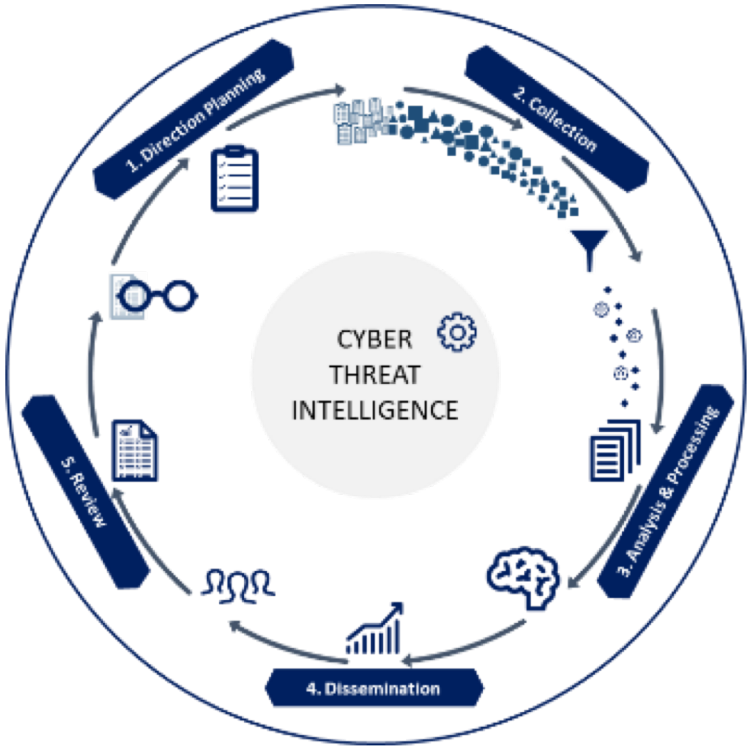
Romano Stasi
Chief Operating Officer

An Italian Threat Landscape Scenario

CERTFin

L'obiettivo del CERTFin è descrivere il **PANORAMA DELLE MINACCE CYBER** per preparare il settore finanziario italiano ad affrontarle al meglio.

LE ATTIVITÀ DI INTELLIGENCE SVOLGONO UN RUOLO CHIAVE al fine di migliorare la conoscenza delle minacce cyber, sia consolidate che emergenti, e comprenderne la loro evoluzione.



Threat Landscape Scenario (2024 H1)

CERTFin

Conflitto Russia–Ucraina / Israele-Hamas & Hacktivismo

- L'impatto di gran lunga maggiore sul panorama delle minacce cyber nel 2023 è stato causato dalle guerre tra Russia-Ucraina ed Israele-Hamas.
- Le tensioni geopolitiche esistenti, esacerbate dai conflitti in corso, hanno portato all'intensificazione delle attività dei gruppi hacktivist.
- Nuove sinergie e collaborazioni si stanno creando tra gruppi hacktivist (e.g., NoName057(16), Anonymous Russia, Mysterious Team Bangladesh, 22C, ecc.).
- Da evidenziare inoltre che i PSP aventi attività in giurisdizioni interessate in primis dai conflitti potrebbero dover affrontare gravi interruzioni di servizio.
- **Previsione: potremmo osservare la formazione di nuove coalizioni ed ulteriori tentativi di attacco alle infrastrutture critiche occidentali.**

AI Generativa

- L'Intelligenza Artificiale Generativa è una forma di intelligenza artificiale che ha la capacità di creare testi, immagini, suoni e altri contenuti sulla base di istruzioni in linguaggio naturale o input di dati (ad esempio ChatGPT).
- Cresce l'utilizzo di tali strumenti all'interno delle organizzazioni con l'obiettivo di accrescere l'efficienza dei team di sicurezza nell'esecuzione di compiti operativi.
- Allo stesso tempo tali strumenti possano essere utilizzati per:
  - Identificare e sfruttare vulnerabilità
  - Creare e-mail di phishing per la distribuzione di malware ed attività fraudolente
  - Generare malware
  - Clonare la voce

Attacchi DDos

- Gli attacchi DDoS aumentando in frequenza a livello globale e talvolta sono associati all'estorsione.
- Per quanto riguarda le dimensioni e la durata degli attacchi, la maggior parte di loro è breve e di piccole dimensioni, ed i vettori di attacco più popolari sono gli attacchi DDoS basati su DNS, flood SYN nonché attacchi basati su UDP.
- Si assiste ad incremento degli attacchi DDoS di livello 7, talvolta combinati con attacchi DDoS di livello 4, principalmente condotti e rivendicati da gruppi hacktivist.
- Il settore finanziario rimane uno dei settori più colpiti.
- **Previsione: Possibile aumento del tasso di successo degli attacchi DDoS.**

Attacchi alla Supply chain & Compromissione di terze parti

- Con l'aumentare dell'interconnessione e della complessità delle organizzazioni, la minaccia della supply-chain sta crescendo.
- Le PMI italiane, di solito fornitori di PSP, continuano ad essere colpite da attacchi ransomware (e.g. abbiamo recentemente osservato un aumento di Akira a livello nazionale). Nonostante gli impatti registrati siano stati finora limitati, il rischio di propagazione ad altri PSP rimane elevato.
- **Previsione: Le minacce alla supply-chain continueranno ad essere un tema chiave, poiché queste ultime diventano sempre più complesse ed interconnesse.**

Threat intelligence a supporto del DORA

CERTFin

Articolo 8: Identificazione

[…] 2. Le entità finanziarie **identificano** costantemente **tutte le fonti di rischio** relative alle TIC, in particolare l'esposizione al rischio da e verso altre entità finanziarie, e **valutano le minacce informatiche e le vulnerabilità** in materia di TIC pertinenti per le loro funzioni commerciali supportate dalle TIC, per i loro patrimoni informativi e per i loro risorse TIC. Le entità finanziarie riesaminano periodicamente, e almeno una volta all'anno, gli scenari di rischio che esercitano un impatto su di loro.

Articolo 13: Apprendimento ed evoluzione

1. Le entità finanziare dispongono capacità e personale per raccogliere informazioni in relazione alle vulnerabilità e alle minacce informatiche, agli incidenti connessi alle TIC, in particolare agli attacchi informatici, e analizzarne i probabili effetti sulla loro resilienza operativa digitale.

Articolo 18: Classificazione degli incidenti connessi alle TIC e delle minacce informatiche

[…] 2.Le entità finanziarie **classificano le minacce informatiche** come significative in base alla criticità dei servizi a rischio,

Articolo 28: Principi generali rischi informatici derivanti da terzi)

[…] 4. Prima di stipulare un accordo contrattuale per l'utilizzo di servizi TIC, le entità finanziarie:

[…] c) **identificano** e valutano tutti **i rischi** pertinenti relativi all'accordo contrattuale,

[…] d) effettuano **controlli di dovuta diligenza** (due diligence) sui potenziali fornitori terzi di servizi TIC […];

Articolo 27: Requisiti per i soggetti incaricati dello svolgimento dei test per lo svolgimento dei TLPT

2.c) il soggetto che fornisce analisi delle minacce è esterno all'entità finanziaria.

Articolo 45: Meccanismi di condivisione delle informazioni e delle analisi delle minacce informatiche

1. Le entità finanziarie possono **scambiarsi** reciprocamente **informazioni e analisi delle minacce informatiche**, tra cui indicatori di compromissione, tattiche, tecniche e procedure, segnali di allarme per la cibersicurezza e strumenti di configurazione,,[…]

In diversi articoli del **Regolamento** è richiesta la identificazione raccolta, classificazione ed analisi delle minacce che **necessita strumenti di Threat Intelligence** anche a supporto della qualificazione dei fornitori di servizi ICT

Threat intelligence per la resilienza:

CERTFin

Un'adeguata **gestione dei rischi aziendali**, in particolare quelli operativi, concorre a rafforzare la resilienza operativa dell'ente. Una delle chiavi per una gestione dei rischi è la definizione e **attuazione del processo di "Intelligence"** quale processo ciclico attraverso cui un ente studia e analizza nel continuo dati/informazioni relativi all'ambiente in cui opera, **determinando preventivamente le fonti e le categorie di rischio** cui è esposto per valutarne gli impatti e definire le adeguate misure di mitigazione.

Potential benefit	&	Obiettivi
Approccio proattivo piuttosto che reattivo		Costruzione di una base informativa completa e aggiornata sulle minacce e i rischi cui l'ente è esposto
Prevenzione contro la perdita e il furto di dati		Evoluzione dei processi interni, nell'ottica di assicurare nel continuo la resilienza aziendale
Allerta precoce su nuove minacce		Ciclicità del processo
Accrescimento della *situational awareness*		

La **Cyber Threat Intelligence** (CTI) si concentra principalmente sull'analisi grezza di dati raccolti da eventi recenti e passati per monitorare, rilevare e prevenire minacce con adeguate misure di sicurezza, adottando un approccio preventivo piuttosto che reattivo.

La CTI viene spesso presentata in termini di intelligence tattica, operativa o strategica:

- **Intelligence tattica (a breve termine)**: informazioni provenienti da attacchi noti, che hanno il potenziale per influenzare immediatamente la sicurezza informatica del processo decisionale
- **Intelligence operativa (a medio termine):** offre informazioni sulle motivazioni, capacità e obiettivi degli attori della minaccia, aiuta i team a valutare incidenti specifici relativi a eventi e indagini e guida e supporta la fase di risposta agli incidenti
- **Intelligenza strategica (a lungo termine):** riassume dati più ampi e di alto livello per identificare le minacce associate, ad esempio, alla politica estera o ad eventi globali e si concentra sugli impatti a lungo termine delle minacce informatiche.

Overview del processo di Intelligence: Le fasi cicliche

CERTFin

Definizione ed adozione delle Tassonomie

consentono di classificare gli elementi caratterizzanti i rischi/minacce cui l'ente è esposto al fine di guidarne la corretta classificazione

Individuazione ambiti di interesse

In ragione della mission, e degli obiettivi strategici (**Analisi del contesto**)

informazioni riguardo l'organizzazione, la sua mission, gli obiettivi strategici, (**Organizational Analysis**) Censimento e analisi dei servizi e i relativi asset (es. risorse umane, applicativi e procedure IT, ecc.) che devono essere difesi dalle minacce, al fine di poter realizzare la mission dell'organizzazione.

informazioni di tipo tecnologico, socio politico, relative all'evoluzione del business e al legal environment che possano inficiare sulla capacità dell'organizzazione di difendere i propri servizi e i propri asset (**Environmental Analysis**)

Identificazione e valutazione delle fonti

Discriminazione **fra fonti, interne ed esterne (umane o tecniche), (libere o riservate**). Stabilire il grado di utilizzo ed affidabilità di fonti di origine Web Surface, Deep Web e Dark Web

Avvio dell'attività di raccolta, selezione e normalizzazione delle informazioni

Raccolta strutturata delle informazioni relative agli **incidenti subiti in passato** dall'ente
Apertura **dei canali di accesso alle fonti**

Analisi dei dati

Normalizzazione, riorganizzazione, arricchimento e classificazione dei dati; raccolta di fattori ed eventi di rischio correnti; Identificazione di potenziali threat actors; stima degli effetti economici, reputazionali e gestionali; Verifica della pertinenza delle informazioni raccolte

Integrazione dell'intelligence nei sistemi di sicurezza aziendali

Per assicurare informazioni aggiornate ai sistemi di difesa aziendali circa le minacce esterne

Reporting

Sintesi dei risultati delle analisi in report operativi, comprensibili per personale non specializzato

RTS – Elements related to threat led penetration tests

CERTFin

L'RTS stabilisce i criteri per **identificare le FE** tenute a svolgere TLPT, i requisiti per il ricorso a **tester interni**, la **metodologia** e l'approccio di ogni fase del test, la tipologia di **supervisione** e altre **cooperazioni** necessarie per lo svolgimento di TLPT.

Identificazione delle FE

Approccio a 2 livelli:

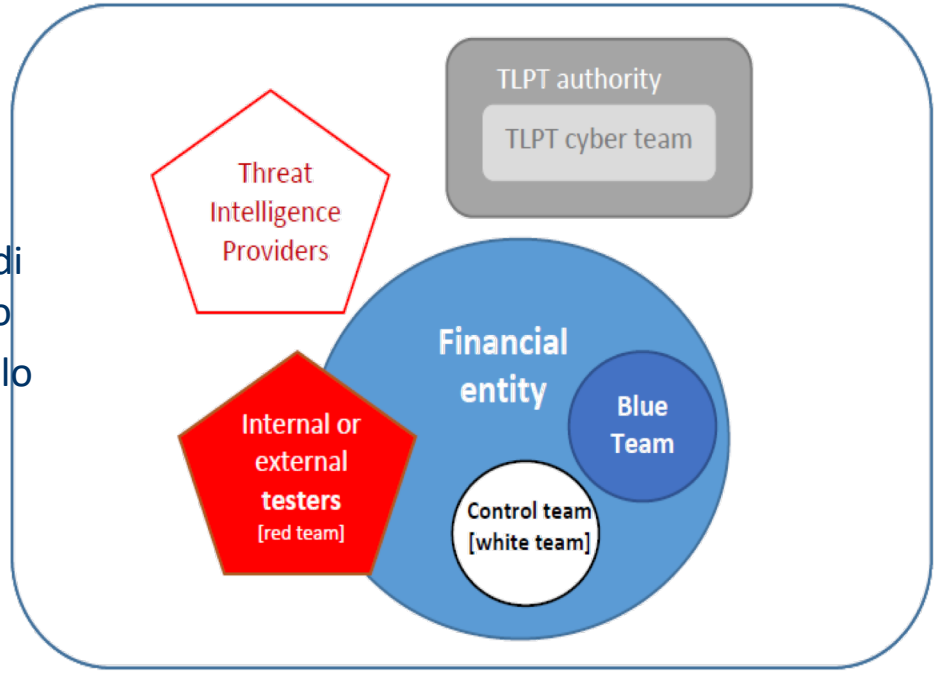
1. **Tipologie di FE** tenute a svolgere i TLPT
2. **Criteri di valutazione** dell'impatto sistemico (es. dimensioni, importanza del servizio erogato) o legato al rischio ICT (es. profilo di rischio, servizi ICT forniti da terzi)

Le FE elencate nell'RTS sono escluse dallo svolgimento dei TLPT se la valutazione dei criteri elencati indica che gli impatti non giustificano lo svolgimento di tali test.

Metodologia di test

L'RTS assegna le funzioni a ciascun partecipante dei TLPT e indica i requisiti che devono essere rispettati nell'assegnazione dei ruoli

- **TLPT cyber team**: staff dell'autorità TLPT
- **Control team**: staff interno alla FE che gestisce e guida il test
- **Blue team**: staff interno responsabile di difendere la FE dell'attacco informatico
- **Threat intelligence provider**: sviluppa lo scenario di test;
  deve essere **esterno alla FE;**
- **Red Team**: esegue il test;
  può essere interno alla FE



RTS – Elements related to threat led penetration tests

CERTFin

Article 1: Definitions

(8) '**threat intelligence provider**' means the expert(s), **external to the financial entity**, who **collect and analyse targeted threat intelligence relevant for the financial entities** in scope of a specific TLPT exercise and develop matching relevant and realistic threat scenarios;

Article 7 - Testing phase: Threat intelligence

1. Following approval of the scope specification document by the TLPT authority, **the threat intelligence provider shall analyse generic and sector-specific threat intelligence relevant for the financial entity.** The threat intelligence provider shall **identify cyber threats and discovered or potential vulnerabilities concerning the financial entity**. Furthermore, the threat intelligence provider shall **gather information on, and analyse concrete, actionable and contextualized target and threat intelligence concerning the financial entity**, including through consulting the control team and the test managers.

2. The threat intelligence provider shall present the relevant threats and targeted threat intelligence, and **propose** appropriate **scenarios** to the control team, testers and test managers. […]

3. The control team shall **select at least three scenarios** to conduct the TLPT, […]

5. The threat intelligence provider shall provide the **targeted threat intelligence report** to the control team, including the scenarios selected […]

6. The control team shall **submit the targeted threat intelligence report to the TLPT authority for approval**. The TLPT authority shall inform the financial entity of their approval.

Per i TLPT la **Targeted Threat Intelligence**

- deve essere prodotta da un soggetto esterno , qualificato
- a partire da threat intelligence settoriali
- condotta sulla base delle minacce pertinenti alla FE
- pervenire alla selezione di tre scenari di test (che saranno implementati dal Red Team) soggetti alla approvazione della autorità

DNS4EU

CERTFin

DNS4EU è un'iniziativa della Commissione Europea per fornire un'alternativa ai risolutori DNS pubblici dominanti sul mercato.

Sovranità Digitale
La Commissione europea mira a mantenere i dati degli utenti nello spazio digitale dell'Unione per sostenerne l'indipendenza e la sovranità digitale.

Privacy
Cittadini europei dovrebbero utilizzare risolutori DNS conformi ai più alti standard di *pricacy,* nonché a tutte le normative EU sulla data *privacy*

Security
Il consorzio riunisce esperti di cybersecurity di differenti paesi EU per progettare risolutori DNS sicuri.

Obiettivo: Proteggere 100 milioni di cittadini europei a livello DNS.

Il raggiungimento di tali obiettivo passa anche dal il **rafforzamento della collaborazione con CERT e CSIRT**, sostenendo la loro partecipazione per migliorare lo scambio di informazioni sulle minacce, affrontando efficacemente le minacce alla sicurezza informatica sia globali che locali.

Soluzione: Creare una protezione DNS indipendente con sede nell'UE con reazione in tempo reale alle minacce cyber per cittadini e istituzioni.

Co-funded by the European Union

DNS4EU Consortium

CERTFin

Project Leader: Whalebone, s.r.o.

Consortium members

- CZ.NIC
- Czech Technical University Prague
- Time.lex
- deSEC
- Sztaki
- ABI Lab Centro di Ricerca e Innovazione per la Banca
- Naukowa i Akademicka Sieć Komputerowa
- Directoratul Național de Securitate Cibernetică

Associated partners

- Ministry of Electronic Governance
- CESNET
- F-Secure
- Centro Nacional de Cibersegurança

Il contributo del CERTFin in DNS4EU

Lo **scambio** e la **condivisione di Cyber Threat intelligence** è uno dei *pillar* di DNS4EU.

Il CERTFin contribuisce alla condivisione di **Cyber Threat Intelligence per la prevenzione di crimini informatici** collaborando con altri CSIRT/CERT e community.

CERTFin

Grazie!

ricerca@certfin.it