«Data Integrity Ransomware Attack»

Le attività di prevenzione e contrasto

Roma, 16 giugno 2020

Gerardo Costabile, Founder & CEO

DEEPCYBER
Advanced Intelligence, Protection, Antifraud.

2020 FORUM PA
FOR A SMART NATION

FORUM PA 2020
6-11 luglio | On line | #road2forumpa2020

Cosa è un Ransomware

Con la parola **Ransomware** viene indicata una classe di *malware* che rende inaccessibili i dati dei computer infettati e chiede il pagamento di un riscatto, in inglese *ransom*, per ripristinarli. Tecnicamente sono *Trojan Horse* crittografici ed hanno come unico scopo l'estorsione di denaro, attraverso:

- un "*sequestro di file*" che porta al blocco del normale accesso al sistema della vittima;
- la crittografia dei dati memorizzati sul disco della vittima, impedendo in tal modo l'accesso alle informazioni.

I vettori di attacco

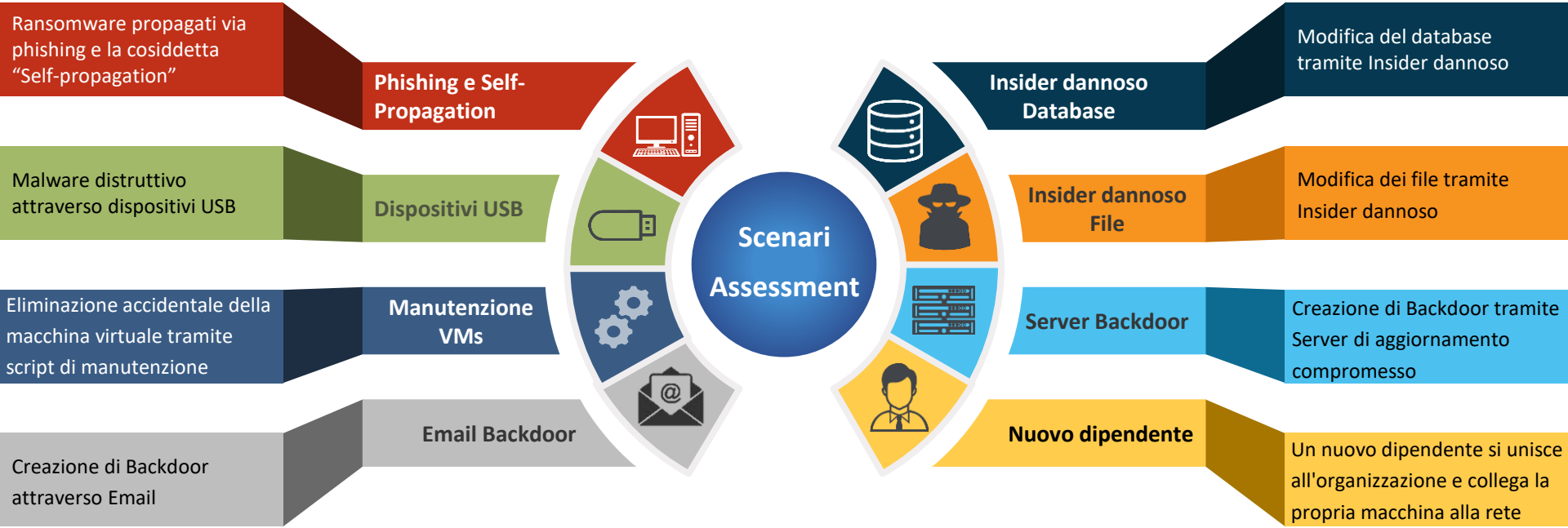
I vettori di attacco più comuni del *trojan* **Ransomware** sono:

Le e-mail di phishing

Accessi RDP o accessi abusivi con cifratura «manuale»

Gli accessi a siti Web contenenti un programma nocivo (ad es. nei banner pubblicitari)

Le modalità «operative» tipiche dell'infezione



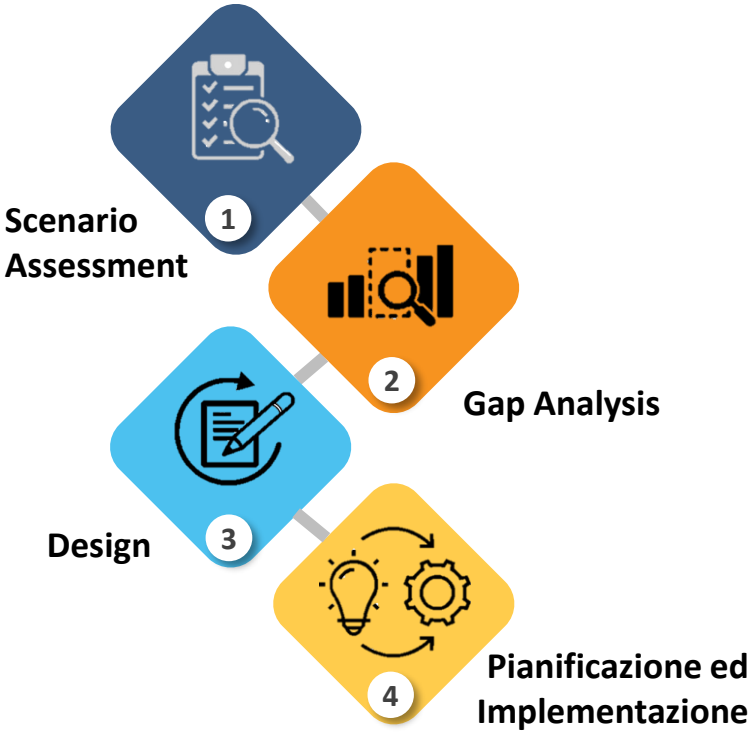
Spunti del rapporto Clusit 2019 (marzo 2020) sulle estorsioni in Italia

- Il rapporto del Clusit afferma che in Italia, nell'**83%** dei casi la causa degli attacchi è il **Cybercrime**, fenomeno che nell'ultimo anno è cresciuto del 12,3% rispetto al 2018 e del 162% rispetto al 2014.

- Andando a monitorare le tecniche utilizzate negli attacchi, a farla da padrone è il **Malware nel 44% dei casi.** Nel dettaglio si parla di **Ransomware** (**46% del totale**, in crescita del 21% rispetto al 2018).

Una visione d'insieme

PREVENZIONE



CONTRASTO

Una visione d’insieme: Contrasto «post infezione»

1

Check-Up

Fase preliminare di diagnosi per verificare la presenza dell’infezione e lo stato dei sistemi eventualmente colpiti + **Lockdown**

Forensics Investigation

individuare l’origine dell’infezione e, laddove sia possibile, recuperare le informazioni perdute o inaccessibili + **Data breach analysis ai fini GDPR**

2

3

Decontaminazione

Fase nella quale avviene la bonifica dei sistemi colpiti dal ransomware e la messa in sicurezza dell’ambiente “infettato”.

Restore

ripristino in sicurezza dei sistemi.

4

5

Prevenzione

A seguito del ripristino, la fase di prevenzione risulterà importante per non incorrere in una nuova infezione in futuro.

Una visione d’insieme: prevenzione e security by design

1

Scenario Assessment

Assessment focalizzato sugli scenari di azione tipici e altamente probabili dell’infezione da ransomware.

3

Design

Identificazione dei processi, soluzioni tecnologiche e formazione secondo le best practices

Gap Analysis

Valutazione degli standard applicati rispetto alle normative più accreditate per contrastare le minacce ransomware.

2

Pianificazione ed Implementazione

La fase conclusiva si sviluppa con la pianificazione di interventi *ad hoc* e l’implementazione delle soluzioni definite nella fase di design

4

Design

Identificare i processi e gli asset che necessitano protezione

Protezione del software e dei dati

Monitoraggio

Gestione degli incidenti

Continuità operativa

Function	Category
Identify	Asset Management
	Business Environment
	Governance
	Risk Assessment
	Risk Management Strategy
	Supply Chain Risk Management
Protect	Identity Management & Access Control
	Awareness and Training
	Data Security
	Information Protection Processes & Procedures
	Maintenance
	Protective Technology
Detect	Anomalies and Events
	Security Continuous Monitoring
	Detection Processes
Respond	Response Planning
	Communications
	Analysis
	Mitigation
	Improvements
Recover	Recovery Planning
	Improvements
	Communications


NEW THREATS EVOLVE, READY TO GO DEEP