Attacco ransomware:
Lesson learned & action plan nei primi 100 giorni

Viterbo, 20 ottobre 2023

Gerardo Costabile, CEO

DEEPCYBER
a Maggioli Group company

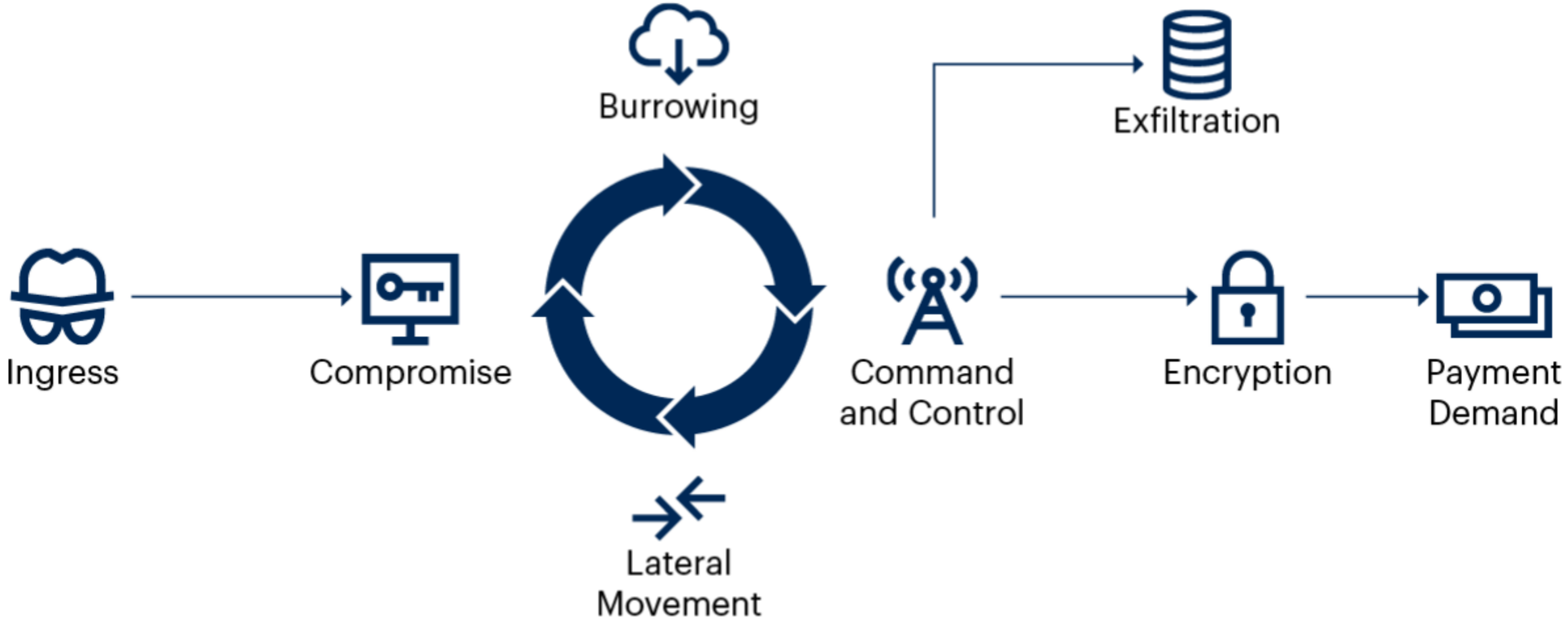
Advanced Intelligence, Protection, Antifraud.

CYBER ACT FORUM 2023

Ransomware: cosa sono?

- ✓ Oggi Ransomware è quasi come dire «accesso abusivo» ad un sistema informatico o telematico di una organizzazione.
- ✓ Doppio o triplo riscatto (per decifrare, per non divulgare, riscatto a terzi i cui dati sono stati esfiltrati).

Anatomy of a Ransomware Attack



Source: Gartner

772397_C

Gartner

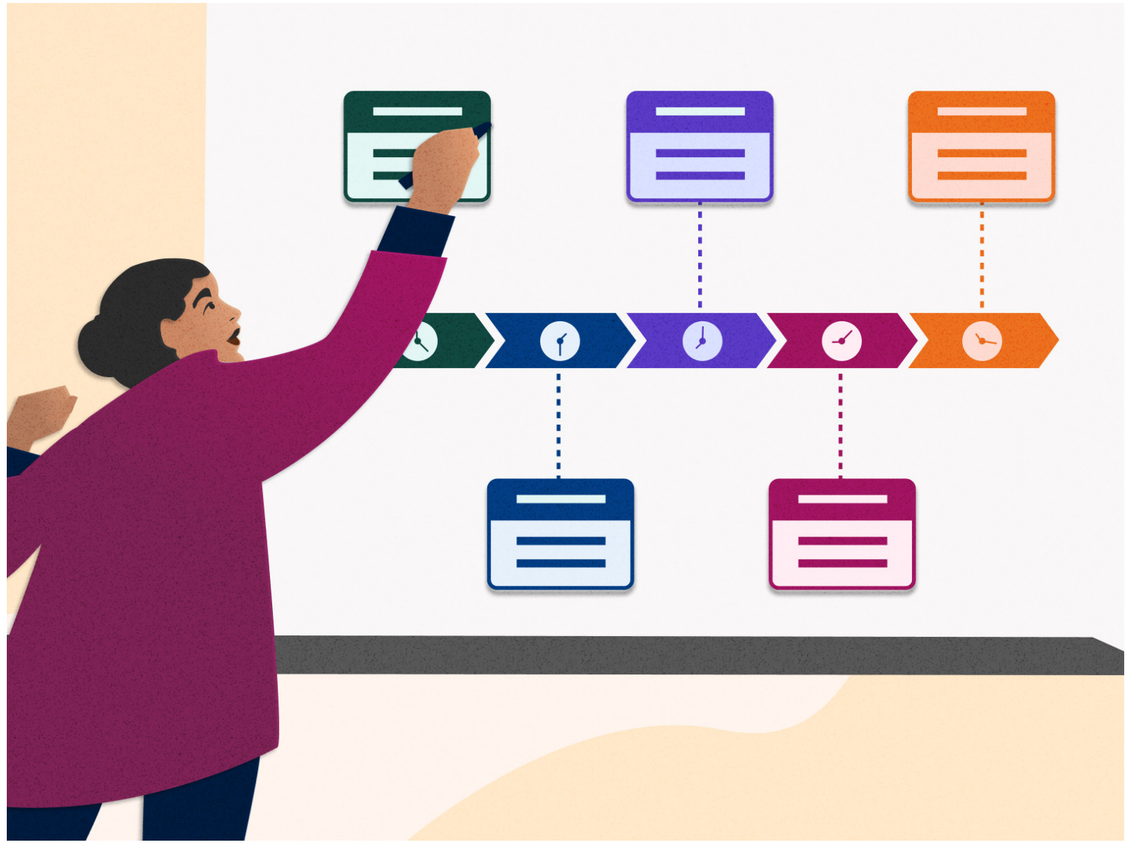
MITRE ATT&CK heatmap

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise (T1189)	User Execution (T1204)	Registry Run Keys / Startup Folder (T1060)	Valid Accounts (T1078)	Disabling Security Tools (T1089)	Brute Force (T1110)	Network Service Scanning (T1046)	Remote Desktop Protocol (T1076)	Data from Local System (T1005)	Remote Access Tools (T1219)	Transfer Data to Cloud Account (T1537)	Data Encrypted for Impact (T1486)
External Remote Services (T1133)	PowerShell (T1086)	External Remote Services (T1133)	Exploitation for Privilege Escalation (T1068)	Group Policy Modification (T1484)	Credential Dumping (T1003)	Network Share Discovery (T1135)	Windows Admin Shares (T1077)	Data from Network Shared Drive (T1039)	Remote File Copy (T1105)	Exfiltration Over Other Network Medium (T1011)	Inhibit System Recovery (T1490)
Spearphishing Attachment (T1193)	Command-Line Interface (T1059)	Create Account (T1136)		Redundant Access (T1108)	Credentials in files (T1081)	Remote System Discovery (T1018)	Windows Remote Management (T1028)		Multi-hop Proxy (T1188)	Data Encrypted (T1022)	Resource Hijacking (T1496)
Spearphishing Link (T1192)	Scripting (T1064)	Scheduled Task (T1053)		Masquerading (T1036)	Credentials from Web Browsers (T1503)	System Information Discovery (T1082)				Exfiltration Over Command and Control Channel (T1041)	
Valid Accounts (T1078)	Windows Management Instrumentation (T1047)	Valid Accounts (T1078)		Bypass User Account Control (T1088)		Permission Groups Discovery (T1069)					
Supply Chain Compromise (T1195)	Exploitation for Client Execution(T1203)	New Service (T1050)		NTFS File Attributes (T1096)		Password Policy Discovery (T1201)					
Trusted Relationship (T1199)	Mshta (Mshta)	Modify Existing Service (T1031)		Obfuscated Files or Information (T1027)		Domain Trust Discovery (T1482)					
Exploit Public-Facing Application (T1190)	Scheduled Task (T1053)	WMI Event Subscription (T1084)		Deobfuscate/ Decode Files or Information (T1140)		Network Configuration (T1016)					
				File and Directory Permissions Modification (T1222)							
				File Deletion (T1107)							

Initial Access	Execution	Persistence	Privilege Escalation
Drive-by Compromise (T1189)	User Execution (T1204)	Registry Run Keys / Startup Folder (T1060)	Valid Accounts (T1078)
External Remote Services (T1133)	PowerShell (T1086)	External Remote Services (T1133)	Exploitation for Privilege Escalation (T1068)
Spearphishing Attachment (T1193)	Command-Line Interface (T1059)	Create Account (T1136)	
Spearphishing Link (T1192)	Scripting (T1064)	Scheduled Task (T1053)	
Valid Accounts (T1078)	Windows Management Instrumentation (T1047)	Valid Accounts (T1078)	

I primi 100 giorni, le prime 100 ore!

- ✓ Le **prime ore** sono molto importanti e stressanti, dopo un attacco ransomware.
- ✓ L'importante è **schematizzare**, in una ipotetica linea del tempo, le azioni da fare appena possibile da quelle da avviare (e in alcuni casi terminare) entro 30, 60, 100 giorni.
- ✓ Ci sono **2 questioni** preliminari molto importanti: gestione dello stress durante il problem solving e trovare un equilibrio tra ripristino e indagini.



Prima possibile in ordine sparso (ma non troppo!)

- ✓ **Isolamento e Indagine:**
- ✓ Isola i sistemi compromessi e avvia un'indagine per identificare il vettore di ingresso e la portata dell'attacco.

- ✓ **Coinvolgimento delle Autorità:**
- ✓ Comunica l'incidente alle autorità competenti e collabora con loro durante l'indagine.

- ✓ **Comunicazione Interna ed Esterna:**
- ✓ Informa il personale interno e gestisci la comunicazione esterna in modo trasparente.

- ✓ **Valutazione dei Danni:**
- ✓ Valuta l'impatto sull'azienda e identifica i dati compromessi.

- ✓ **Backup e Ripristino:**
- ✓ Utilizza backup affidabili per ripristinare i sistemi colpiti.

Entro i primi 30 giorni

- ✓ **Aggiornamento delle configurazioni e/o delle difese:**
- ✓ Aggiorna le configurazioni dei sistemi di sicurezza e le misure tecnologiche, inclusi firewall, EDR/NDR/ITR e soluzioni anti-ransomware, compresi strumenti di filtraggio del traffico per limitare le comunicazioni non necessarie

- ✓ **Monitoraggio Continuo:**
- ✓ Verifica/Implementa sistemi di monitoraggio continuo per rilevare attività anomale in tempo reale.

- ✓ **Consapevolezza degli Utenti:**
- ✓ Verifica/migliora/programma programmi di awareness e phishing simulation

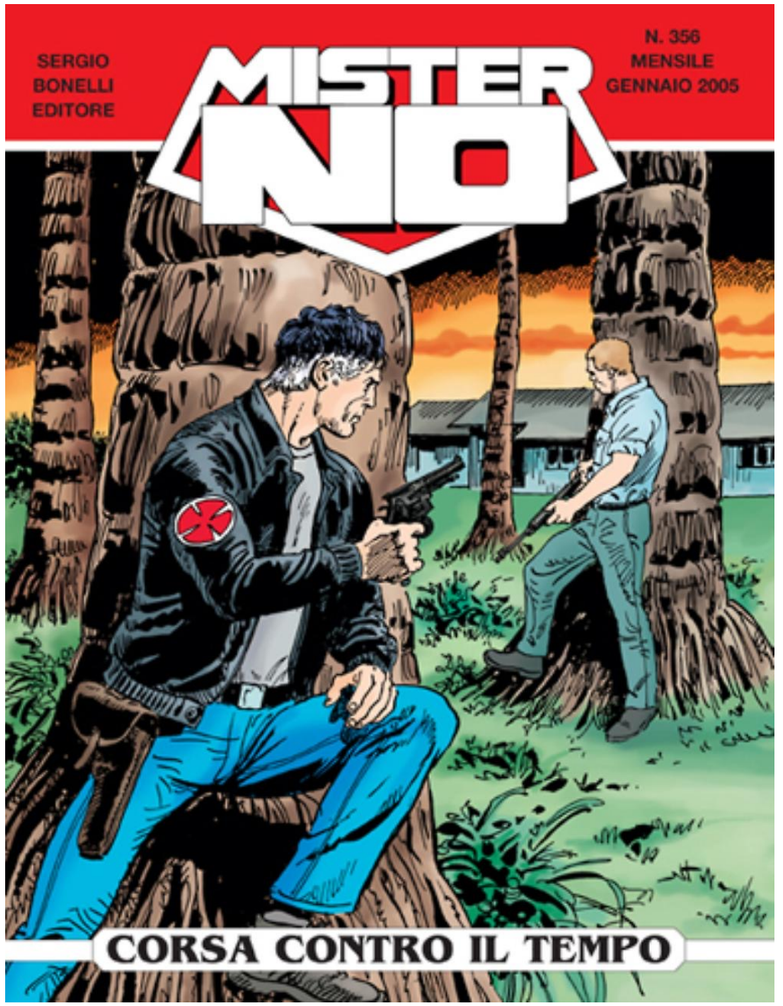
Entro i primi 60 giorni

- ✓ **Pianificazione di Emergenza:**
- ✓ Sviluppa e aggiorna un piano di risposta agli incidenti per affrontare futuri attacchi (RTO/RPO compresi). Avvia una analisi di BC/DR.

- ✓ **Valutazione dei Rischi:**
- ✓ Rivedi, se necessario, il programma di risk management & vulnerability management di sistemi, applicazioni e processi aziendali.

- ✓ **Collaborazione con Esperti:**
- ✓ Coinvolgi esperti esterni di sicurezza informatica per una valutazione obiettiva e ulteriori raccomandazioni.

- ✓ **Coinvolgi il board:**
- ✓ Coinvolgi il board ed il top management, in modo costruttivo per mettere la cyber nella loro agenda



Entro i primi 100 giorni

Patching e Aggiornamenti:
Assicurati che esista e venga applicato in modo approfondito un processo di patch management.

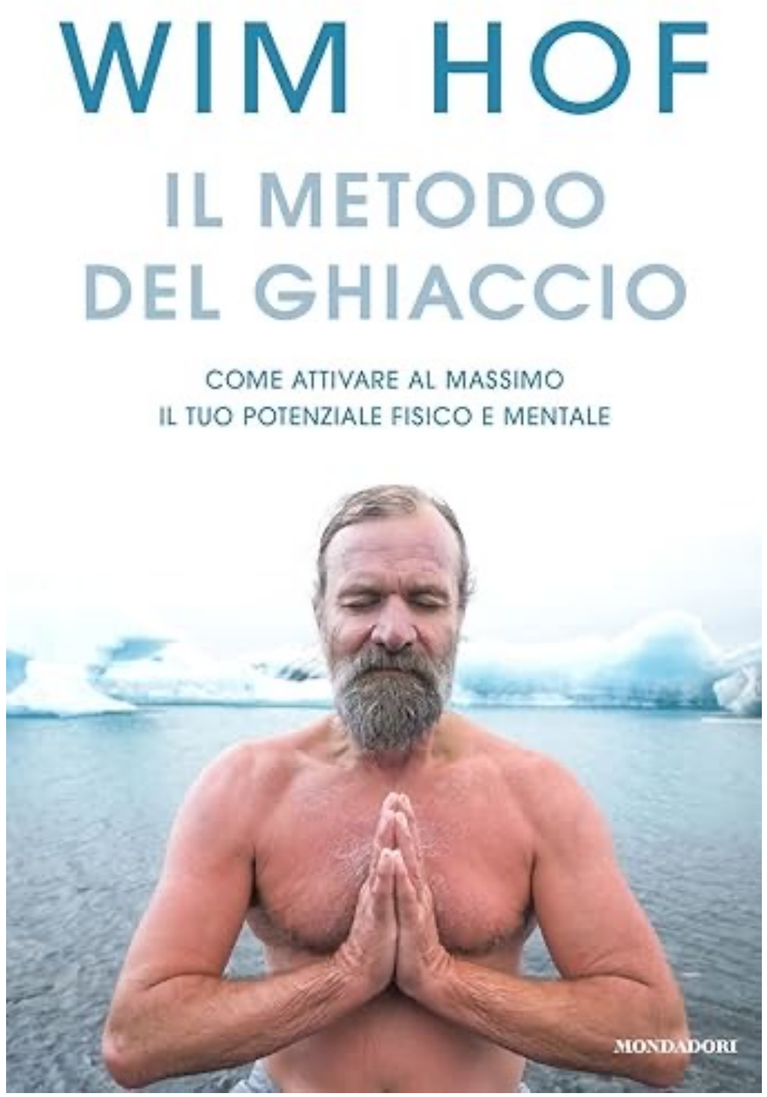
Controllo degli Accessi:
Assicurati che sia implementata una gestione rigorosa degli accessi per limitare l'accesso alle risorse.

Hardening delle Configurazioni ICT:
Disponi che siano riconfigurati correttamente server, dispositivi di rete e applicazioni, eliminando servizi non necessari.

Analisi dei Log:
Verifica e migliora il sistema di log management, per monitorare e identificare comportamenti sospetti.

Segmentazione di Rete:
Fai in modo che la rete sia segmentata (per limitare la diffusione di un attacco) e che tutto sia documentato adeguatamente.

Auditing e Conformità:
L'organizzazione dovrà condurre audit di sicurezza per assicurare al board la realizzazione del piano di sicurezza post incidente e l'efficacia del sistema.



In conclusione

- ✓ Fare attenzione alla troppa obsolescenza dell'ICT (sia infrastrutture che applicativi) per riduzione costi negli anni di crisi
- ✓ Attenzione a non perdere i fondamentali
- ✓ I progetti vanno iniziati e finiti
- ✓ «La formazione o i test di sicurezza li facciamo ogni 2/3 anni»
- ✓ Poca indipendenza dei CISO in alcune organizzazioni (oltre a centri di costo non sempre indipendenti)

Ma, la cosa più importante è:

- ✓ Prepararsi ad un incidente di elevata magnitudo

(letture consigliate di Gartner «How to Prepare for Ransomware Attacks" del 16/06/2022 e "Ransomware Recovery Requires a Layered Recovery Response» del 23 August 2023.

Grazie e alla prossima occasione….

gerardo.costabile@deepcyber.it

www.deepcyber.it

DEEPCYBER

Advanced Inteligence, Protection, Antifraud.