FORMAZIONE AGID – FORMEZ SULLA TRANSIZIONE DIGITALE DELLA PA

Progetto Informazione e formazione per la transizione digitale della PA nell'ambito del progetto «Italia Login – la casa del cittadino»

(A valere sul PON Governance e Capacità Istituzionale 2014-2020)

La sicurezza Informatica nella Pubblica Amministrazione

Esempi di Campagne Malevole e classificazione nei modelli di Cyber Kill Chain

25/11/2021

Massimiliano Rossi - CERT- AGID

CERT-AGID

Breve panoramica sui modelli di identificazione degli attacchi

Riconoscere il tipo di Evento malevolo

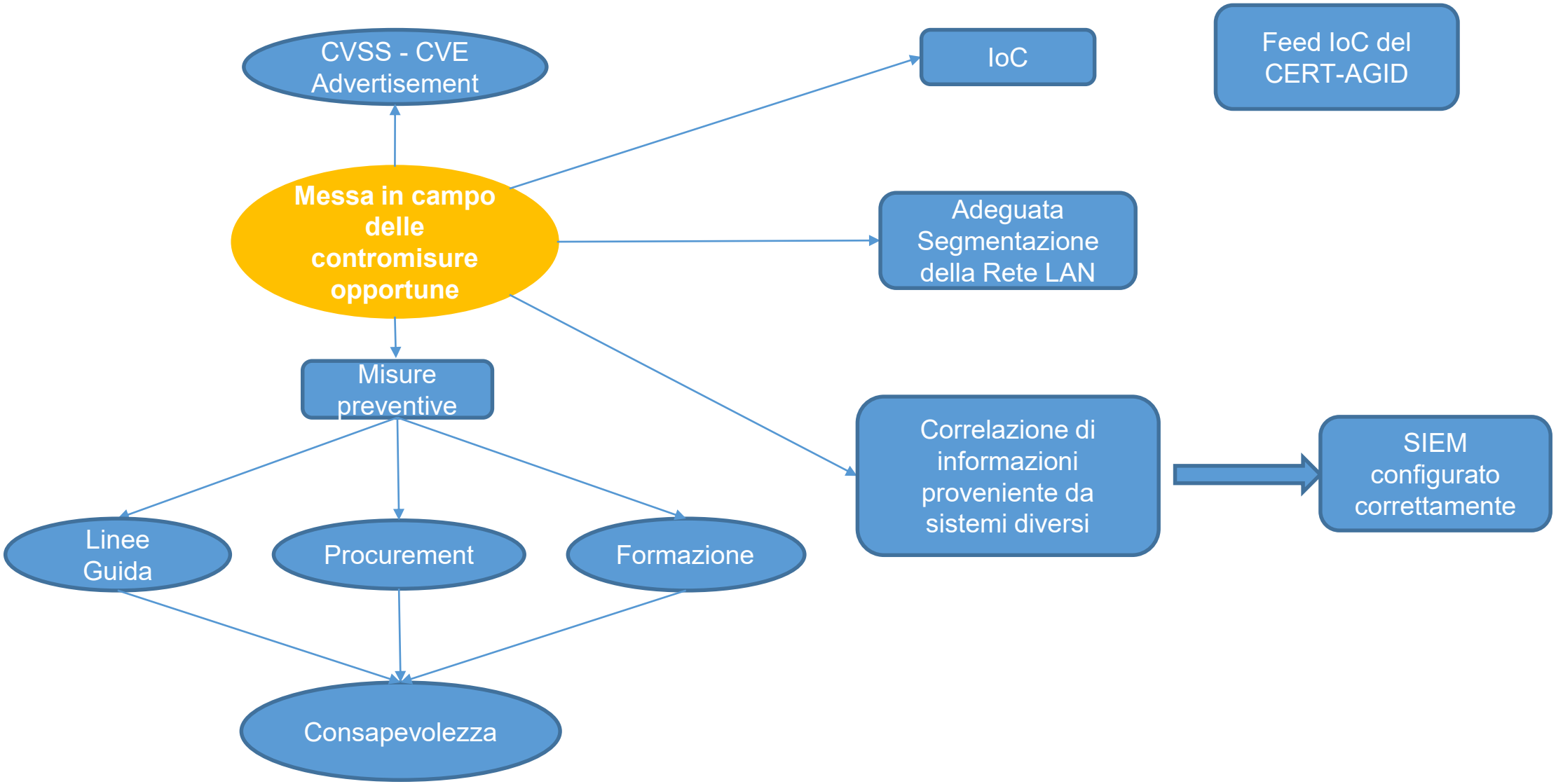
Metodologia utilizzata dall'attaccante

Sistema Complesso di informazioni da interpretare

Sono stati sviluppati alcuni modelli di classificazione

- ✓ Cyber Kill Chain 
- ✓ Diamond Model for Intrusion Analysis 

Breve panoramica sulle contromisure/azioni da intraprendere



Introduzione alla Cyber Kill Chain 1/4

Sette Fasi per Modellare un attacco

La Cyber Kill Chain è un progetto sviluppato dalla Lockheed Martin

Prima Fase

Ricognizione

Ricerca, identificazione e selezione degli obiettivi effettuata da ricerche su siti web, come atti di conferenze, estrazione di indirizzi mail da mailing lists, relazioni sociali, o informazioni su tecnologie specifiche

In altre parole più OSINT e/o Information Gathering

Seconda Fase

Armamento

Accoppiamento di un trojan per l'accesso remoto con una vulnerabilità in un carico da consegnare, di solito tramite uno strumento automatizzato. Spesso si utilizzano PDF o documenti di MS

Malware

Introduzione alla Cyber Kill Chain 2/4

Sette Fasi per Modellare un attacco

Terza Fase

Trasmissione

Consegna dell'arma al destinatario. I tre strumenti di trasmissione più utilizzati sono: allegati e-mail, siti web e supporti rimovibili USB, sfruttando vecchie comunicazioni o facendo leva su debolezze dell'essere umano

Quarta Fase

Sfruttamento

Ciò può avvenire sfruttando una vulnerabilità di un'applicazione del Sistema Operativo, per esempio mediante l'esecuzione automatica del SO oppure, più semplicemente, sono gli utenti stessi che, ignari, lo attivano.

Malware

Introduzione alla Cyber Kill Chain 3/4

Sette Fasi per Modellare un attacco

Quinta Fase

Installazione

Questa fase è definita anche come fase della persistenza, in quanto descrive le attività eseguite dall'aggressore per attivare una backdoor sul sistema che gli consenta di avere un accesso duraturo e persistente

L'attaccante/criminale è in grado di accedere al sistema ogni volta che vuole

Sesta Fase

Comando e Controllo

Indicato anche come C2 o CnC, è la fase in cui un host compromesso tenta di stabilire un canale di comunicazione con un host esterno da cui ricevere comandi.

Il Malware esegue azioni automatizzate

Introduzione alla Cyber Kill Chain 4/4

Sette Fasi per Modellare un attacco

Settima Fase
Obiettivi

In questa fase vengono descritte le azioni intraprese sugli obiettivi, azioni che sono lo scopo per cui si sono affrontate le fasi precedenti. Tra esse possiamo elencare:

- ✓ Furto di proprietà intellettuale
- ✓ Furto di dati aziendali
- ✓ Furto di connettività (banda) per effettuare spam o attacchi DDOS
- ✓ Utilizzo per il mining di bit-coin

Quando l'aggressore è riuscito a raggiungere questo livello, il difensore deve fare uno sforzo non indifferente per poter eliminare completamente la minaccia dal proprio sistema o rete. Infatti, gli avversari, dopo aver effettuato l'accesso ed attivato la comunicazione con il CnC, tenteranno di espandere la propria presenza e cercheranno di integrarsi nelle attività ordinarie per evitare di essere rilevati e scoperti.

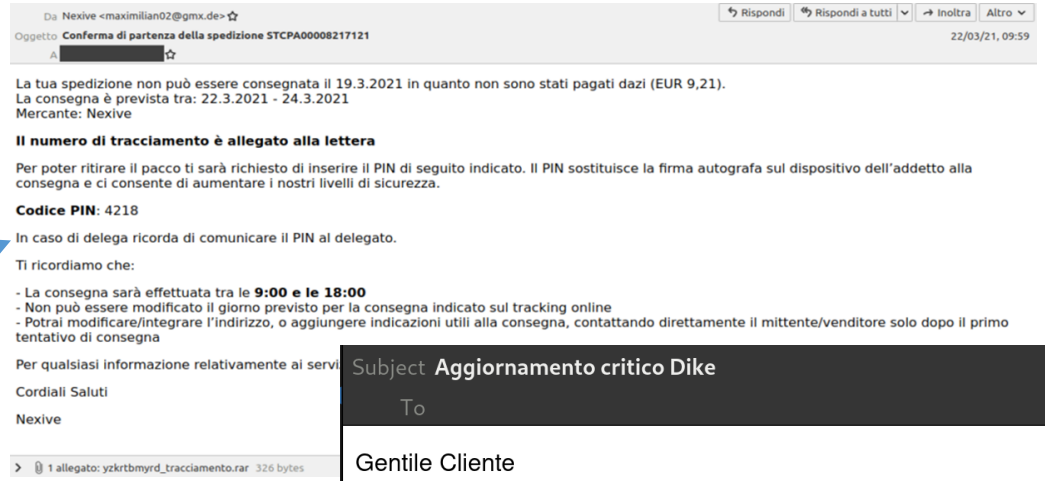
Esempi di classificazione – LockTheSystem
Analisi tramite CKC 1/7 – Fase 1 -Ricognizione

https://cert-agid.gov.it/news/nuova-campagna-ransomware-lockthesystem/

- ✓ **OSINT=Open Source Intelligence dell'attaccante sul target struttura della mail….ufficio amministrativo**
- ✓ **Prestare la massima attenzione in periodi determinati**

Per gli uffici amministrativi, controllare attentamente qualsiasi tipo di anomalia nelle e-mail

Pacco



Da Nexive <maximilian02@gmx.de>
Oggetto **Conferma di partenza della spedizione STCPA00008217121**
22/03/21, 09:59

La tua spedizione non può essere consegnata il 19.3.2021 in quanto non sono stati pagati dazi (EUR 9,21).
La consegna è prevista tra: 22.3.2021 - 24.3.2021
Mercante: Nexive

Il numero di tracciamento è allegato alla lettera

Per poter ritirare il pacco ti sarà richiesto di inserire il PIN di seguito indicato. Il PIN sostituisce la firma autografa sul dispositivo dell'addetto alla consegna e ci consente di aumentare i nostri livelli di sicurezza.

Codice PIN: 4218

In caso di delega ricorda di comunicare il PIN al delegato.

Ti ricordiamo che:

- La consegna sarà effettuata tra le **9:00 e le 18:00**
- Non può essere modificato il giorno previsto per la consegna indicato sul tracking online
- Potrai modificare/integrare l'indirizzo, o aggiungere indicazioni utili alla consegna, contattando direttamente il mittente/venditore solo dopo il primo tentativo di consegna

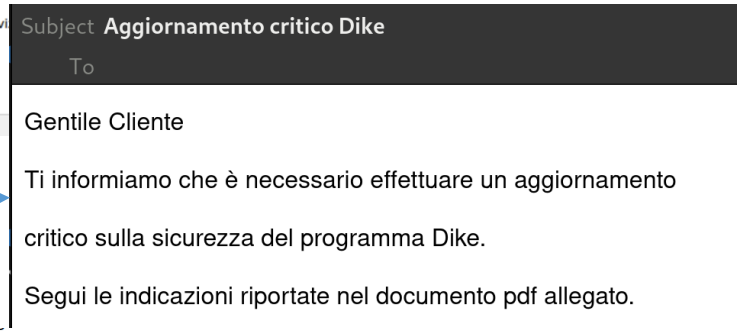
Per qualsiasi informazione relativamente ai servi

Cordiali Saluti

Nexive

1 allegato: yzkrtbmyrd_tracciamento.rar 326 bytes

Dike



Subject **Aggiornamento critico Dike**
To

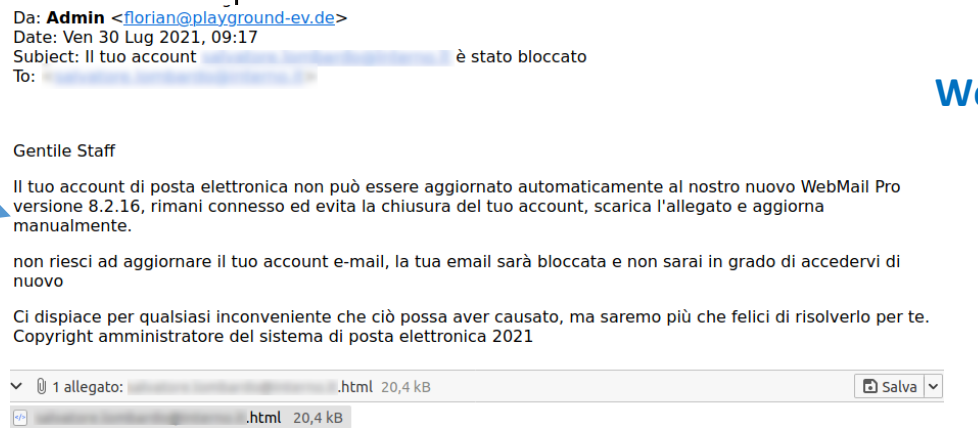
Gentile Cliente

Ti informiamo che è necessario effettuare un aggiornamento

critico sulla sicurezza del programma Dike.

Segui le indicazioni riportate nel documento pdf allegato.

WebMail



Da: **Admin** <florian@playground-ev.de>
Date: Ven 30 Lug 2021, 09:17
Subject: Il tuo account è stato bloccato
To:

Gentile Staff

Il tuo account di posta elettronica non può essere aggiornato automaticamente al nostro nuovo WebMail Pro versione 8.2.16, rimani connesso ed evita la chiusura del tuo account, scarica l'allegato e aggiorna manualmente.

non riesci ad aggiornare il tuo account e-mail, la tua email sarà bloccata e non sarai in grado di accedervi di nuovo

Ci dispiace per qualsiasi inconveniente che ciò possa aver causato, ma saremo più che felici di risolverlo per te.
Copyright amministratore del sistema di posta elettronica 2021

1 allegato: .html 20,4 kB Salva

.html 20,4 kB

Esempi di classificazione – LockTheSystem
Analisi tramite CKC 2/7 – Fase 2 -Armamento

Da Nexive <maximilian02@gmx.de>
Rispondi | Rispondi a tutti | Inoltra | Altro
Oggetto **Conferma di partenza della spedizione STCPA00008217121** 22/03/21, 09:59
A [redacted]

La tua spedizione non può essere consegnata il 19.3.2021 in quanto non sono stati pagati dazi (EUR 9,21).
La consegna è prevista tra: 22.3.2021 - 24.3.2021
Mercante: Nexive

Il numero di tracciamento è allegato alla lettera

Per poter ritirare il pacco ti sarà richiesto di inserire il PIN di seguito indicato. Il PIN sostituisce la firma autografa sul dispositivo dell'addetto alla consegna e ci consente di aumentare i nostri livelli di sicurezza.

Codice PIN: 4218

In caso di delega ricorda di comunicare il PIN al delegato.

Ti ricordiamo che:

- La consegna sarà effettuata tra le **9:00 e le 18:00**
- Non può essere modificato il giorno previsto per la consegna indicato sul tracking online
- Potrai modificare/integrare l'indirizzo, o aggiungere indicazioni utili alla consegna, contattando direttamente il mittente/venditore solo dopo il primo tentativo di consegna

Per qualsiasi informazione relativamente ai servizi offerti da Nexive puoi visitare il nostro sito www.nexive.it

Cordiali Saluti

Nexive

1 allegato: yzkrtbmyrd_tracciamento.rar 326 bytes Salva

LockTheSystem è un ransomware veicolato molto recentemente in Italia (al momento è in corso una nuova campagna) tramite email scritte in lingua italiana corretta.

L'e-mail è stato il vettore di attacco

Contromisura: Questa è una fase essenziale per capire la fase di attacco.
Sebbene per chi difende non si può rilevare la fase di armamento mentre accade. È possibile rilevare quando l'attacco potrebbe cominciare analizzando i componenti del malware.

Nel caso in cui la vittima non faccia doppio click la catena si interrompe….

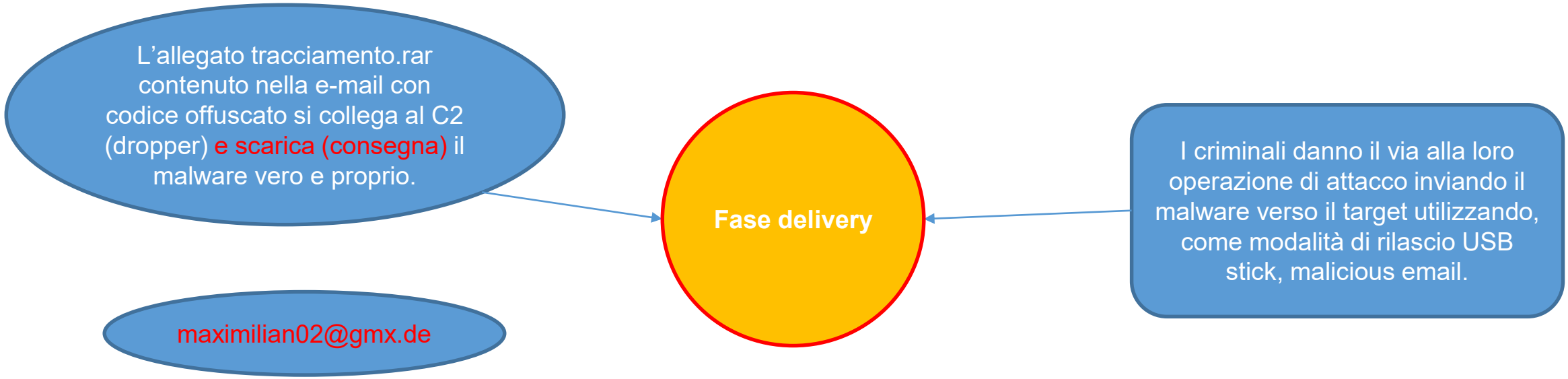
Armamento!!!

L'analisi degli artefatti degli attaccanti intesa anche come awareness è una delle la difese più efficaci

FormezPA

Esempi di classificazione – LockTheSystem
Analisi tramite CKC 3/7 – Fase 3 - Delivery

Possibile contromisura
Record SPF DMARK, DKIM - spoofing



Esempi di classificazione – LockTheSystem
Analisi tramite CKC 4/7 – Fase Sfruttamento-

Strategia di **attacco**: gli avversari devono sfruttare una vulnerabilità per ottenere l'accesso al sistema target. Le vulnerabilità possono essere software, hardware o **vulnerabilità umane**. Spesso si usa uno **zero day exploit**.
L'avversario accede alle falle sfruttando vulnerabilità server-based e la vittima innesca l'exploit aprendo allegati contenuti in malicious email o cliccando su malicious links

Attacco: ad esempio Esegue una istruzione powershell per la rimozione delle copie shadow (tramite powershell.exe) o Get-WmiObject Win32_Shadowcopy | ForEach-Object { $_Delete(); } Cerca le copie di backup…..per poi

Strategia di difesa: l'obiettivo principale è l'analisi dei vettori di attacco aperti. Questi possono provenire dalla tecnologia utilizzata o da comportamenti del personale, non adeguatamente formato.

Nel caso in esame **http://URLdelC2/Client-0.exe è scaricato mediante l'apertura dell'allegato alla mail indicatore di compromissione, se opportunamente intercettato dai sistemi perimetrali avrebbe fermato e spezzato la catena.**

In questo esempio la contromisura possibile è disabilitare PowerShell nel profilo utente.

Esempi di classificazione – LockTheSystem
Analisi tramite CKC 5/7 – Fase Istallazione

Fase Istallazione

Contromisura

Possibile contromisura: Se aggiungo una policy per disabilitare powershell – interrompo la catena

Fase in cui il sistema viene silenziosamente modificato, possono essere modificate anche le chiavi di registro in alcuni sistemi operativi.

È possibile utilizzare gli strumenti degli EndPoint al fine di rilevare e memorizzare in un file di log tutte le attività di installazione, per poi eseguire sistematicamente un processo di audit con lo scopo di rilevare anomalie! Antivirus avanzati

Esempi di classificazione – LockTheSystem
Analisi tramite CKC 6/7 – Fase Command&Control

Fase Command and Control

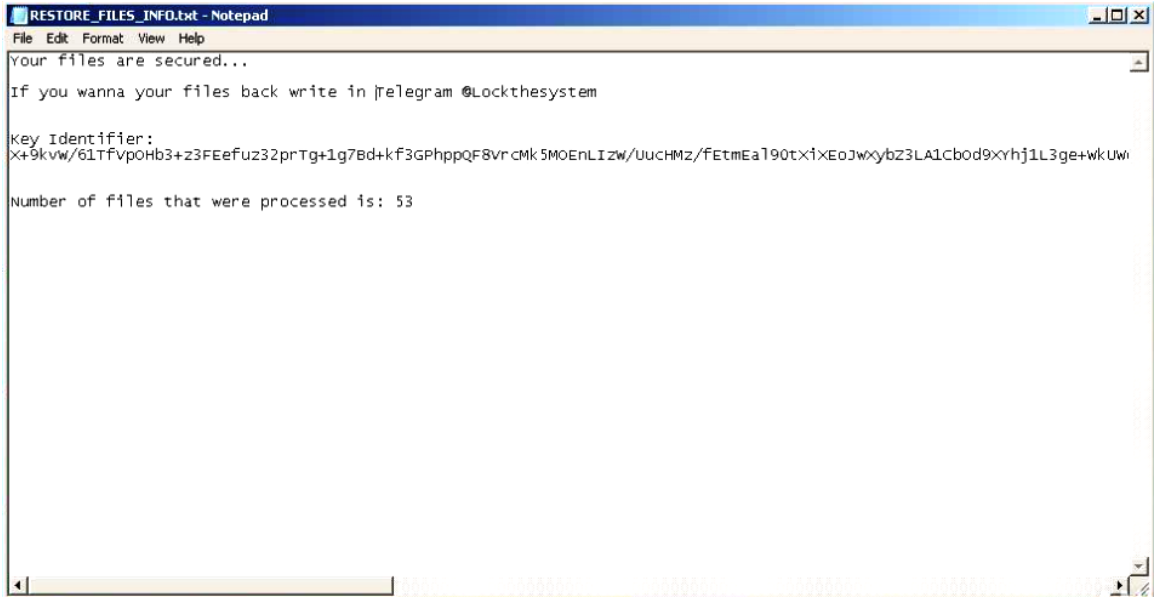
L'attacco avviene attraverso l'apertura di un canale bidirezionale di comando e controllo per gestire le risorse interne da remoto.

Se gli attaccanti non possono impartire comandi, il difensore può prevenire l'impatto dell'attacco.

regole di blocco dei protocolli C2 ed inclusione dei domini "none" o "non categorizzato".

Esempi di classificazione – LockTheSystem
Analisi tramite CKC 7/7 – Fase Azioni sugli obiettivi

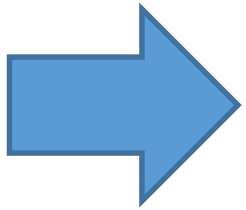
L'attaccante raggiuge l'obiettivo della propria missione (dopo aver preso il controllo del sistema target) che consiste nella raccolta delle credenziali di utente, privilege escalation, collezione di informazioni riservate sul network target.



Più a lungo un attaccante ha accesso a CKC7, maggiore sarà l'impatto. I difensori devono rilevare questo stadio il più rapidamente possibile, utilizzando analisi e prove forensi, comprese l'acquisizione di pacchetti di rete, per la valutazione dei danni. E' utile stabilire un manuale di risposta agli incidenti (Incident Response playbook), incluso il coinvolgimento operativo/esecutivo e il piano di comunicazione sia interno che esterno

Esempi di classificazione – Riassumiamo…

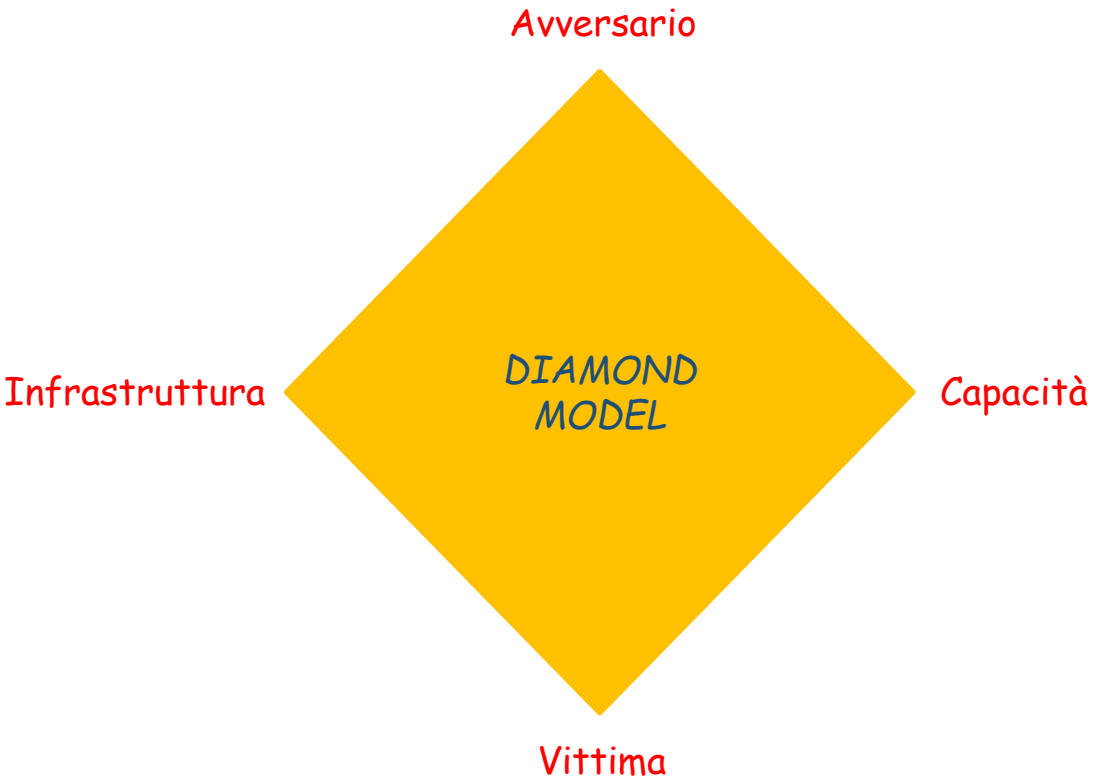
Esempio: Cosa devo fare per migliorare la mia capacità di migliorare le azioni da intraprendere? E decidere quale strumento sia più efficace per «rompere» la catena



Phase	Detect	Deny	Disrupt	Degrade	Deceive	Contain
Reconnaissance	Web Analytics Threat Intelligence NIDS	Information Sharing Policy Firewall ACLs				
Weaponization	Threat Intelligence NIDS	NIPS				
Delivery	Endpoint Malware Protection	Change Management Application Whitelisting Proxy Filter HIPS	Inline AV	Queuing		Router ACLs App-aware Firewall Trust Zones Inter-zone NIPS
Exploitation	Endpoint Malware Protection HIDS	Secure Password Patch Management	DEP			App-aware Firewall Trust Zones Inter-zone NIPS
Installation	SIEM HIDS	Privilege Separation Strong Passwords Two-Factor Authentication	Router ACLs			App-aware Firewall Trust Zones Inter-zone NIPS
Command & Control	NIDS HIDS	Firewall ACLs Network Segmentation	HIPS	Tarpit	DNS Redirect	Trust Zones DNS Sinkholes
Actions on Objectives	Endpoint Malware Protection	Data-at-Rest Encryption	Endpoint Malware Protection	Quality of Service	Honeypot	Incident Response
Exfiltration	DLP SIEM	Egress Filtering	DLP			Firewall ACLs

Introduzione al Diamond Model 1/2

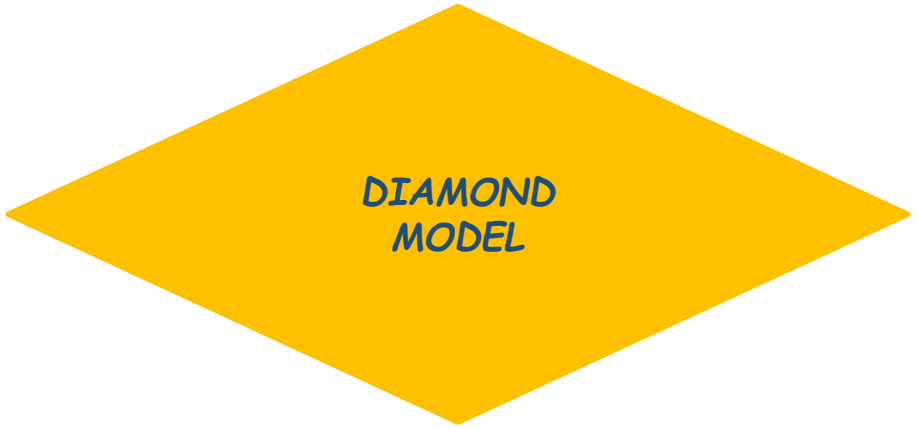
Un altro modello sviluppato per analizzare e **correlare** gli eventi in modo che le minacce possano essere organizzate, monitorate ordinate e contrastate. Il modello è così chiamato in quanto è costituito da quattro nodi connessi tra loro



Introduzione al Diamond Model 2/2

Avversario: è il responsabile dell'attacco. Questo nodo potrebbe talvolta rimanere vuoto in quanto non si riesce ad individuare, mentre a volte si riesce ad individuare sia il mandatario dell'intrusione che l'operatore/i che l'ha fisicamente eseguita

Infrastruttura è l'insieme dei nodi di comunicazione, logici o fisici, che l'attaccante utilizza per stabilire e mantenere il CnC sulle proprie "capacità", come ad esempio Internet od una chiavetta USB.



Capacità: si riferisce allo strumento o alla tecnica utilizzata. Potrebbe essere un exploit, oppure una tecnica usata per individuare le password.

Vittima: è il bersaglio dell'attacco. Potrebbe essere una persona od un gruppo di esse oppure una risorsa, fisica o logica, come un server o un account email. La risorsa potrebbe a sua volta essere l'obiettivo di un evento per poi essere utilizzata come infrastruttura in un evento successivo.

Esempi di classificazione – LockTheSystem

Analisi tramite Diamond Model 1/5

LockTheSystem è un ransomware veicolato molto recentemente in Italia (al momento è in corso una nuova campagna) tramite email scritte in lingua italiana corretta.

L'e-mail è stato il vettore di attacco

Esempi di classificazione – LockTheSystem

Analisi tramite Diamond Model 2/5

L'attaccante fa leva su informazioni plausibili

Esistono una serie di possibili attaccanti (interni, esterni, individui, gruppi e organizzazioni e Stati) che cercano, secondo i loro obiettivi (attivisti, script kiddy, APT, insider threat ed ecc…) di compromettere i sistemi o le reti di un target specifico. Rileva notare che nel nostro caso si potrebbe trattare di Criminali non necessariamente tecnicamente evoluti

L'email è il vettore di attacco. L'allegato spesso non è identificabile come malevolo

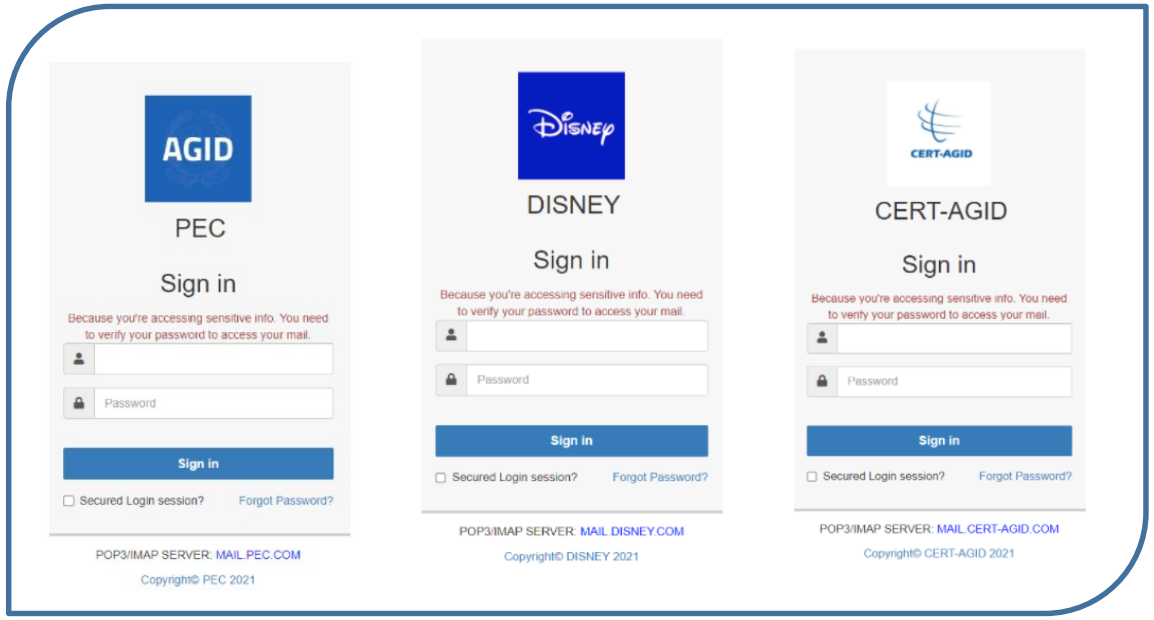
Esempi di classificazione – LockTheSystem

Analisi tramite Diamond Model 3/5

Vittima (Victim): è il bersaglio dell'avversario contro il quale lo stesso criminale cerca di trovare delle vulnerabilità da sfruttare. Quest'ultima non riguarda solo la singola persona o un'organizzazione ma tutto ciò che appartiene a loro: interessi, indirizzi IP, domini, account, social network, host, ovvero il dominio tecnologico della ipotetica vittima.
Nel caso di lockthesystem le potenziali vittime sono gli utenti di e-commerce che aspettano un pacco

Al momento dell'invio, il server ritorna volutamente un messaggio di errore per indurre la vittima a reinserire la password. Questa tecnica serve ad ingannare anche le vittime più sospettose che al primo tentativo inseriscono una password falsa (come prova).

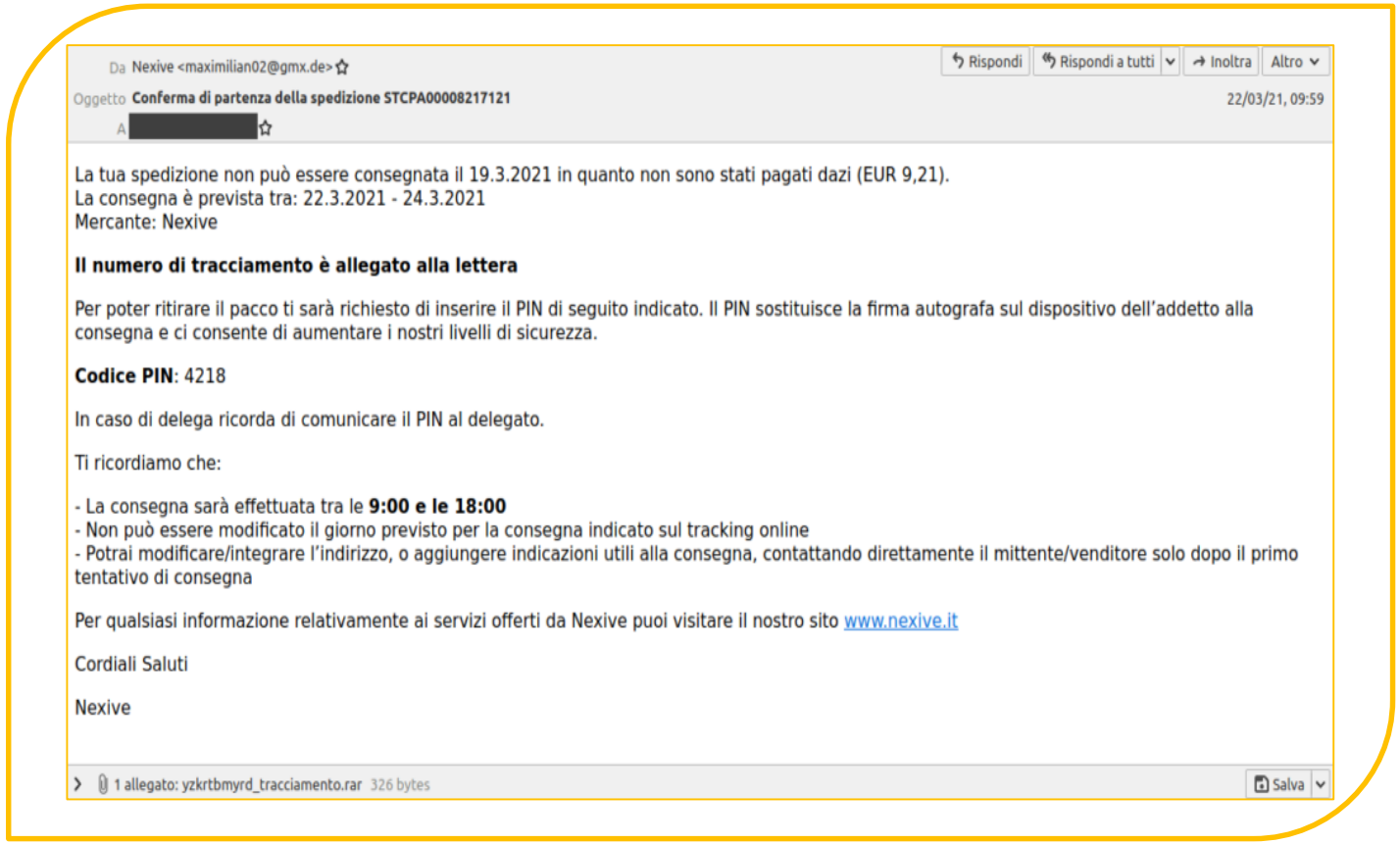
Altro Esempio In crescita il fenomeno delle campagne di phishing adattivo
https://cert-agid.gov.it/news/in-crescita-il-fenomeno-delle-campagne-di-phishing-adattivo/



Esempi di classificazione – LockTheSystem

Analisi tramite Diamond Model 4/5

Descrive le strutture di comunicazione fisiche e logiche, utilizzate dall'attaccante per raggiungere i suoi scopi, strettamente interconnesse alle sue capacità compreso il C2 (command-and-control). Tra esse rientrano gli asset di identification, indirizzi IP, Providers, indirizzi e-mail, domini e threat & Enviroment manipulation. Nel nostro caso abbiamo chiaramente identificato l'email mittente "maximilian02@gmx.de"



Da Nexive <maximilian02@gmx.de>

Rispondi | Rispondi a tutti | Inoltra | Altro

Oggetto **Conferma di partenza della spedizione STCPA00008217121**

22/03/21, 09:59

A [redacted]

La tua spedizione non può essere consegnata il 19.3.2021 in quanto non sono stati pagati dazi (EUR 9,21).
La consegna è prevista tra: 22.3.2021 - 24.3.2021
Mercante: Nexive

Il numero di tracciamento è allegato alla lettera

Per poter ritirare il pacco ti sarà richiesto di inserire il PIN di seguito indicato. Il PIN sostituisce la firma autografa sul dispositivo dell'addetto alla consegna e ci consente di aumentare i nostri livelli di sicurezza.

Codice PIN: 4218

In caso di delega ricorda di comunicare il PIN al delegato.

Ti ricordiamo che:

- La consegna sarà effettuata tra le **9:00 e le 18:00**
- Non può essere modificato il giorno previsto per la consegna indicato sul tracking online
- Potrai modificare/integrare l'indirizzo, o aggiungere indicazioni utili alla consegna, contattando direttamente il mittente/venditore solo dopo il primo tentativo di consegna

Per qualsiasi informazione relativamente ai servizi offerti da Nexive puoi visitare il nostro sito www.nexive.it

Cordiali Saluti

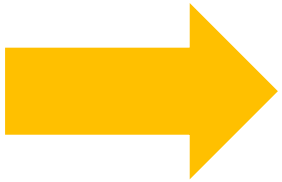
Nexive

1 allegato: yzkrtbmyrd_tracciamento.rar 326 bytes

Salva

Esempi di classificazione – LockTheSystem
Analisi tramite Diamond Model 5/5

Capacità (Capability): insieme di tattiche, tecniche, procedure e strumenti, utilizzati dall'avversario per raggiungere i suoi scopi. Ovviamente rientrano tutta una serie di casistiche che vanno dai metodi manuali di tipo non tecnico (la ricerca manuale delle password) a sofisticate e automatizzate tecniche di ricerca e attacco.

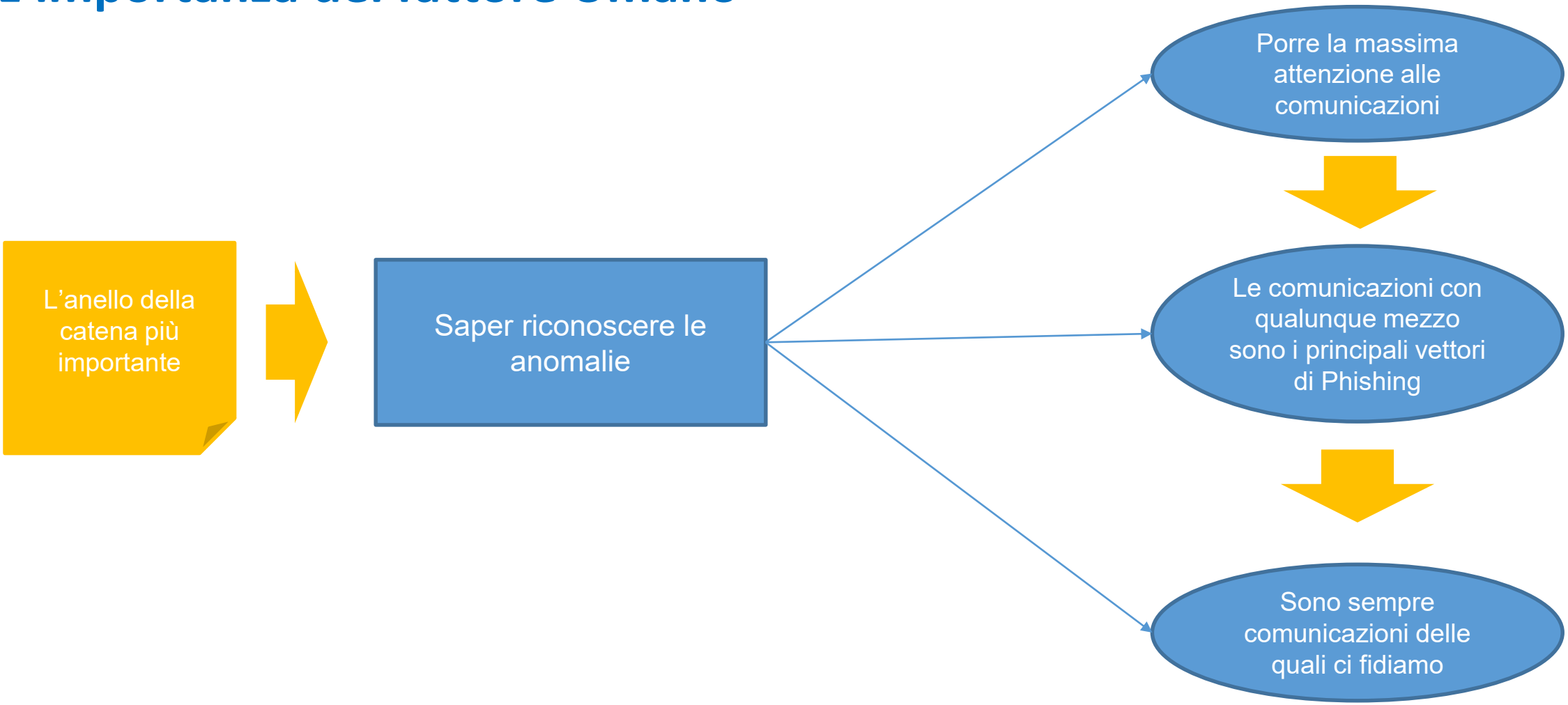


Tecniche di social Enginering per individuare le vittime

Esempi di classificazione – Comparazione IoC nei modelli di Classificazione

IoC	Tipo	Cyber Kill Chain stage	Diamond Model
maximilian02@gmx.de	[E-mail]	Delivery	Infrastructure
http://URLC2.com/mar/Client-0.exe	[URL]	C2	Infrastructure
Client-0.exe	[Allegato]	Exploit/ /Armamento/ Install/c2c	Capability / Infrastructure
Compila una lista delle estensioni di file di immagine disco o di backup	[Comando per individuare I file da cifrare]	Actions on Objectives/ Azioni sugli obiettivi	Capability

L’importanza del fattore Umano



Condivisione di indicatori di compromissione per la protezione della Pubblica Amministrazione

Le Pubbliche Amministrazioni interessate possono esprimere la volontà di aderire al flusso di Indicatori di compromissione (**Feed IoC**) del **CERT-AGID** per la protezione della propria Amministrazione da minacce Malware e Phishing compilando l'apposito modulo.

Come aderire

1. Scarica e compila il modulo di accreditamento in formato Libre Office o in formato Microsoft Office.
2. Compila il modulo con i riferimenti della persona tecnica e l'elenco (max 20) di indirizzi IPv4 da abilitare.
3. Invia il modulo compilato per e-mail a **info@cert-agid.gov.it.**

Per maggiori informazioni: https://cert-agid.gov.it/scarica-il-modulo-accreditamento-feed-ioc/

Contatti utili del CERT-AGID:

e-mail : info@cert-agid.gov.it
web : https://cert-agid.gov.it
twitter : @agidcert
telegram : @certagid

Per segnalarci nuove campagne **malware / phishing / scam** da analizzare basta allegare l'email originale sospetta e inviarla all'indirizzo:

malware@cert-agid.gov.it

Esempi di Phishing e classificazione nei modelli di Cyber Kill Chain

Massimiliano Rossi

UNIONE EUROPEA
Dipartimento della Funzione Pubblica
AGID Agenzia per l'Italia digitale
FormezPA

www.agid.gov.it

Riferimenti dei docenti (facoltativi)
Altri riferimenti ritenuti necessari (facoltativi)