MODULO 09

Memory e network forensics con AI

La memoria volatile e il traffico di rete come fonti primarie per incidenti in corso: Volatility 3, super-timeline con Plaso/Timesketch e rilevamento del beaconing C2.

Volatility 3 | Plaso / Timesketch | Zeek / Arkime

SCHEDA DEL MODULO

Abstract e obiettivi formativi

Abstract

Il modulo affronta l'analisi della memoria volatile e del traffico di rete come fonti primarie per incidenti in corso: acquisizione della RAM, processi e iniezioni di codice, super-timeline con Plaso/Timesketch e relativi analyzer automatici, network forensics con Zeek e Arkime, rilevamento di beaconing e DNS tunneling con tecniche statistiche e ML.

Obiettivi formativi (Bloom)

- **Applicare**: acquisire e analizzare un dump di memoria con Volatility 3
- **Creare**: ricostruire una super-timeline e interrogarla con analisi assistita
- **Analizzare**: individuare pattern di beaconing C2 con tecniche statistiche e ML

Traccia core: 01 02 07

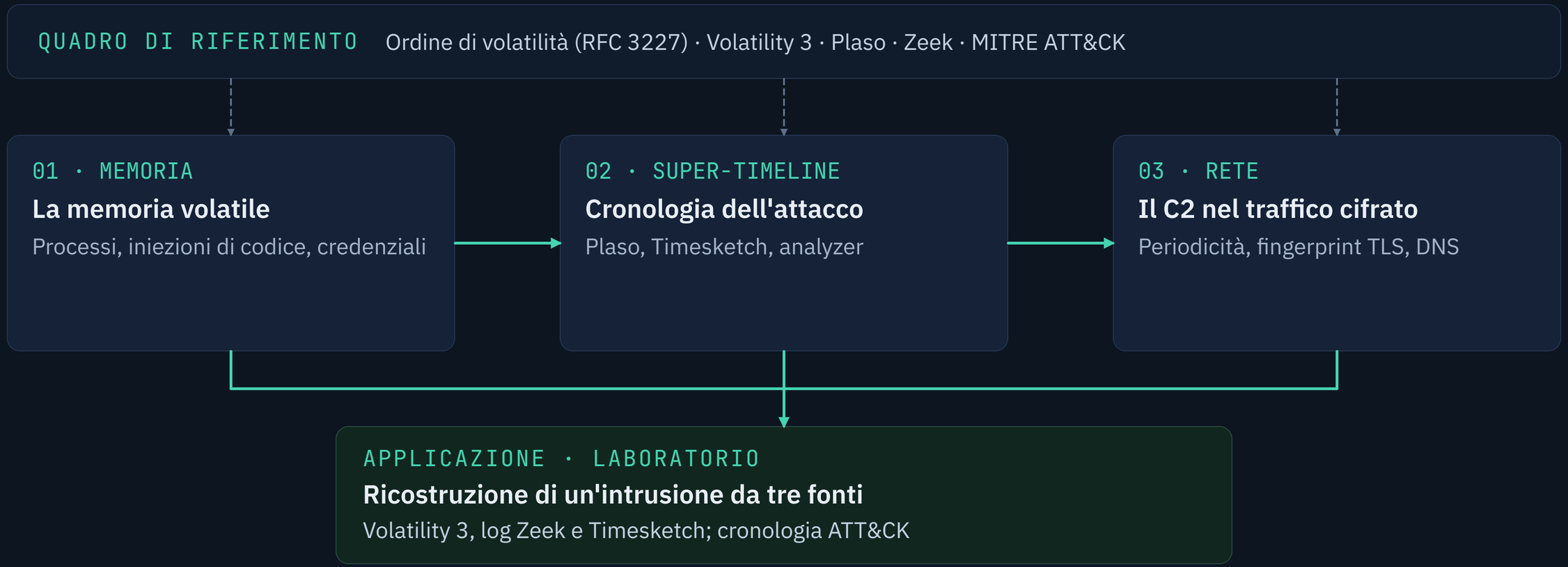
Detection & Response: 03 04 05 06 o Digital Forensics: 08 09 10 11 o Sicurezza dell'AI: 06 12 13 14

Traccia core: 15 16

Letture di raccordo: § 3.6, 5.9

SCHEMA · TEORIA

Indagine su un'intrusione in corso



TEORIA · MEMORIA VOLATILE

La memoria volatile come fonte di evidenze

Cosa c'è solo in memoria

- Processi e thread in esecuzione, handle e DLL caricate
- Connessioni di rete attive e socket
- Codice iniettato e malware fileless, invisibili su disco
- Credenziali, chiavi crittografiche e dati già decifrati

Metodo e strumenti

- Acquisizione a sistema acceso con WinPmem o AVML; l'ordine di volatilità impone la RAM prima del disco
- Analisi con Volatility 3: pslist/psscan, malfind, netscan, dump dei moduli
- Indicatori di injection: regioni RWX non associate a file, padre incoerente con la gerarchia attesa, hollowing
- Assistenza AI: spiegazione degli esiti e prioritizzazione dei processi sospetti, sempre verificata

TEORIA · SUPER-TIMELINE

La cronologia dell'attacco

SORGENTI
File system, registro, log eventi, browser, memoria

→

PLASO
Estrae e normalizza milioni di eventi datati

→

TIMESKETCH
Analyzer automatici evidenziano anomalie e pattern

→

ANALISTA
Ricostruisce la narrazione, mappa su ATT&CK

Il contributo dell'AI

Gli analyzer e l'interrogazione assistita riducono milioni di righe a un numero gestibile di eventi candidati. Resta il rischio del timestomping, cioè della manipolazione dei timestamp, che l'analista controlla confrontando fonti indipendenti.

TEORIA · NETWORK FORENSICS

Rilevamento del C2 nel traffico cifrato

Segnali di beaconing

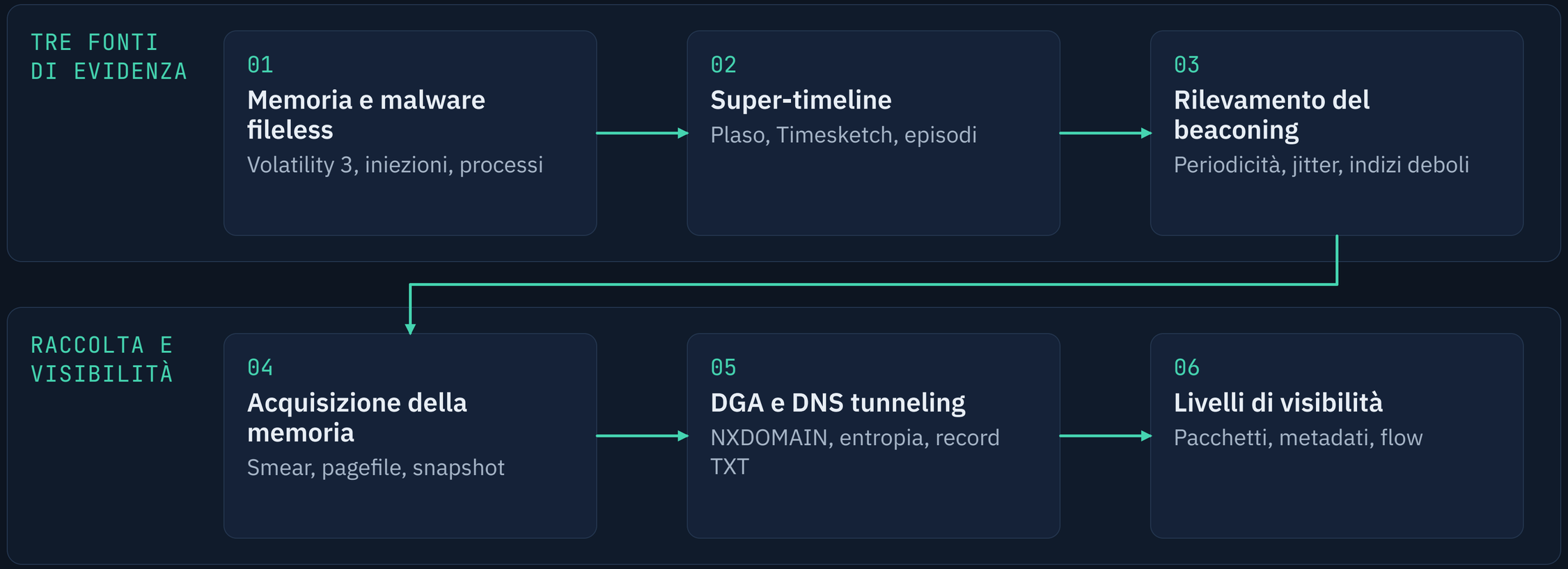
- **Periodicità**: connessioni a intervalli regolari, con jitter limitato
- Dimensioni dei pacchetti quasi costanti nel tempo
- Fingerprint TLS (di preferenza JA4) rari o incoerenti con il client dichiarato
- DNS tunneling: query lunghe, alta entropia, volumi anomali verso un dominio

Metodo con Zeek e ML

- Zeek produce metadati per sessione; Arkime indicizza i pacchetti
- Analisi statistica degli intervalli e punteggio di regolarità per coppia host-destinazione
- Modelli ML sui metadati: si analizzano le caratteristiche del traffico senza accedere al contenuto cifrato
- Limite: beacon lenti o mascherati in traffico legittimo (domain fronting)

SCHEMA · APPROFONDIMENTI

Analisi della memoria e del traffico di rete



APPROFONDIMENTO 1

Memoria volatile e malware fileless

Molto malware recente è progettato per lasciare poche tracce su disco: risiede in memoria (fileless), si inietta in processi legittimi (process hollowing, DLL injection), cifra le proprie stringhe e le decifra solo durante l'esecuzione. Per essere eseguito, però, il codice deve trovarsi in chiaro in memoria, insieme alle chiavi in uso, alle connessioni di rete attive, alle credenziali in cache e alle righe di comando effettive. **Volatility 3** analizza le strutture del sistema operativo, come le liste dei processi, le tabelle degli handle e le regioni di memoria mappate, e ne evidenzia le incoerenze: un processo chiamato svchost.exe con un processo padre anomalo, oppure regioni eseguibili non associate ad alcun file su disco.

Scenario didattico

Antivirus e scansione del disco non rilevano nulla, ma l'EDR segnala traffico anomalo. Il dump di memoria mostra nel processo explorer.exe una regione eseguibile con un beacon Cobalt Strike mai scritto su disco, da cui strumenti dedicati estraggono indirizzo del C2 e configurazione.

Ruolo dell'AI

Un dump contiene centinaia di processi e migliaia di moduli e regioni di memoria. Modelli addestrati su dump benigni e malevoli possono ordinare le anomalie per grado di sospetto, e un LLM può tradurre l'output dei plugin in ipotesi leggibili. La conferma resta manuale: estrazione della regione, calcolo dell'hash, analisi del campione.

APPROFONDIMENTO 2

Super-timeline e ricostruzione cronologica

Ogni fonte registra una parte della sequenza con il proprio orologio: file system (timestamp MACB), registro di Windows, log applicativi, cronologia del browser, eventi di autenticazione. Plaso normalizza queste fonti in un'unica **super-timeline**, che spesso conta milioni di righe, e Timesketch la rende consultabile. A questa scala la lettura integrale non è praticabile. L'AI rileva anomalie negli intervalli, come un'attività di sistema alle 03:12 in un ufficio chiuso, raggruppa in episodi gli eventi correlati e risponde a interrogazioni in linguaggio naturale che verificano un'ipotesi, per esempio le esecuzioni di binari nuovi nei dieci minuti successivi a un accesso.

Scenario didattico

Una timeline di 4,2 milioni di eventi riguarda tre host. Il raggruppamento isola un episodio di undici minuti: accesso RDP da un indirizzo interno già compromesso, creazione di un servizio, esecuzione di rclone, cancellazione del servizio. L'esaminatore verifica i 40 eventi dell'episodio sulle fonti originali e li riporta in relazione.

Cautele

Gli host possono avere fusi orari diversi e orologi non sincronizzati, l'attaccante può alterare le date dei file con il **timestomping** e lo stesso timestamp ha significati diversi a seconda del file system. La coerenza temporale di un episodio segnalato dall'analisi statistica va dimostrata confrontando fonti indipendenti.

APPROFONDIMENTO 3

Rilevamento statistico del beaconing

Un impianto malevolo contatta periodicamente il server di comando e controllo (C2) per ricevere istruzioni. La cifratura nasconde il contenuto ma lascia osservabili le caratteristiche del traffico: periodicità dei contatti, dimensioni quasi costanti dei pacchetti, durata delle sessioni, rapporto tra dati inviati e ricevuti. L'analisi statistica dei metadati di **Zeek** misura la regolarità: un beacon ogni 60 secondi con jitter del 10% produce una distribuzione degli intervalli stretta. I modelli di machine learning combinano più indizi deboli: dominio registrato di recente, certificato autofirmato nelle sessioni fino a TLS 1.2, fingerprint TLS raro, attività costante anche nelle ore notturne.

Scenario didattico

Nei log Zeek di 30 giorni un host contatta lo stesso dominio in HTTPS ogni 300 secondi, con scarti di circa 20 secondi, giorno e notte, con pacchetti di circa 1,2 KB; nessuna firma si attiva e il dominio non compare nelle liste di reputazione. La regolarità anche notturna esclude la navigazione di un utente. Il traffico ha quindi le caratteristiche del beaconing e, se il contesto ne conferma la natura malevola, il primo contatto colloca nel tempo la compromissione.

Limiti

Anche il software legittimo genera traffico periodico: aggiornamenti, telemetria, NTP, controllo della posta. Per qualificare il traffico come malevolo servono, oltre alla periodicità, la destinazione, la data di inizio, il processo sorgente e la correlazione con memoria e timeline.

APPROFONDIMENTO 4

Aspetti pratici dell'acquisizione della memoria

L'analisi dell'approfondimento 1 presuppone un dump corretto, e l'acquisizione è la fase più fragile. Strumenti come WinPmem, AVML o la funzione di acquisizione dell'EDR vanno scelti e provati prima dell'emergenza. Il dump di una memoria in uso è soggetto a **smear**: le pagine cambiano durante la copia e alcune strutture possono perdere coerenza. Il file di paging (pagefile.sys) e il file di ibernazione (hiberfil.sys) conservano pagine e stati precedenti della memoria e vanno acquisiti insieme al dump. Nei sistemi virtualizzati lo **snapshot dell'hypervisor** è spesso l'acquisizione più pulita, perché è atomico e non richiede agenti sul sistema osservato. Ogni acquisizione su sistema acceso va verbalizzata con strumento, versione, orario e hash del dump, perché modifica lo stato che misura (Modulo 7).

Scenario didattico

Un server critico non può essere riavviato né rallentato da un dump. Lo snapshot della macchina virtuale, eseguito dall'hypervisor, congela memoria e disco in un istante coerente senza intervenire sul sistema guest. Il file di memoria, dopo il calcolo dell'hash, si analizza con Volatility; alcuni formati richiedono i file di stato associati o una conversione.

Errori frequenti

Installare lo strumento sul disco del sistema compromesso, anziché avviarlo da un supporto esterno, sovrascrive evidenze e segnala l'attività a un attaccante attivo. Ricorrono anche il salvataggio del dump su una condivisione di rete non protetta, l'omissione di pagefile e hiberfil e la mancata annotazione dell'ora esatta, necessaria per la correlazione con timeline e traffico di rete.

APPROFONDIMENTO 5

DGA e DNS tunneling nei log DNS

I log DNS sono una fonte forense rilevante, perché quasi ogni attività di rete inizia con una risoluzione DNS e la loro conservazione ha costi contenuti. Con i **DGA** (Domain Generation Algorithm) il malware genera ogni giorno molti domini pseudocasuali e tenta di contattarli; l'operatore ne registra solo alcuni, rendendo inefficace il blocco tramite liste. La traccia statistica consiste in sequenze di risposte NXDOMAIN; i classificatori basati su n-grammi, entropia e pronunciabilità riconoscono bene i nomi pseudocasuali, meno quelli generati concatenando parole reali. Il **DNS tunneling** trasporta dati dentro query e risposte DNS e si riconosce da query lunghe e frequenti verso lo stesso dominio, record TXT voluminosi e rapporto anomalo tra query e traffico.

Scenario didattico

Nei log DNS di un mese un host produce circa 4.000 risposte NXDOMAIN al giorno per domini come xk2v9qp[.]net, comportamento tipico di un DGA. La data d'inizio delle sequenze colloca nel tempo l'infezione anche se il C2 contattato con successo non è più attivo; timeline e dump di memoria dello stesso host (approfondimenti 1 e 2) confermano l'ipotesi e identificano il processo.

Limiti

Anche servizi legittimi usano nomi generati: reti di distribuzione dei contenuti, telemetria, antivirus. Il DNS-over-HTTPS sposta le query fuori dalla vista del resolver aziendale, e la policy di rete che impone il resolver interno, prerequisito della visibilità, va decisa prima dell'incidente.

APPROFONDIMENTO 6

Livelli di visibilità della rete e conservazione

La visibilità di rete ha costi diversi secondo il livello di dettaglio. La **cattura integrale dei pacchetti** conserva tutto, compresi i file trasferiti, ma richiede molto spazio, pone problemi di riservatezza e, con il traffico TLS, rende disponibile poco contenuto; si conserva in genere per pochi giorni. I metadati di sessione di Zeek riportano origine, destinazione, volumi, protocollo, fingerprint TLS e, fino a TLS 1.2, il certificato. Occupano una frazione dello spazio, si conservano per mesi e sono la base delle analisi di beaconing e DGA. Il **NetFlow** registra volumi e coppie di indirizzi e si conserva anche per anni. Una configurazione tipica combina flow su tutta la rete, Zeek nei punti di transito principali e cattura integrale attivabile durante un incidente.

Scenario didattico

Un'esfiltrazione viene scoperta sei mesi dopo. La cattura integrale è stata sovrascritta, ma i log Zeek mostrano 40 GB verso un indirizzo esterno in tre notti, con il fingerprint TLS di un client non usato in azienda. I file trasferiti non sono identificabili; volume, date e destinazione sono accertabili, e il fingerprint TLS indica il tipo di client usato, da confermare con gli artefatti dell'host.

Nota normativa

Conservazione e punti di cattura si decidono in anticipo, bilanciando costi, esigenze d'indagine e proporzionalità: la cattura integrale del traffico dei dipendenti va giustificata alla luce del GDPR e dell'art. 4 della L. 300/1970.

LABORATORIO · ESERCITAZIONE

Ricostruzione di un'intrusione da tre fonti

Svolgimento su un caso d'intrusione simulato

1. Analisi del dump di memoria dell'host compromesso con Volatility 3: individuare il processo malevolo
2. Correlazione con i log Zeek del laboratorio: identificare il canale C2
3. Costruzione della super-timeline in Timesketch con gli analyzer automatici
4. Cronologia dell'attacco mappata su ATT&CK, con evidenze per ogni passaggio

Consegna

- Processo e canale C2 identificati, con prova
- Timeline annotata in Timesketch
- Cronologia ATT&CK dell'intera intrusione

CHIUSURA DEL MODULO

Letture e autovalutazione

Letture obbligatorie

- Ligh et al., *The Art of Memory Forensics*
- Documentazione Volatility 3 e Timesketch
- Hu et al., *BAYWATCH*, IEEE/IFIP DSN 2016

Domande di autovalutazione

1. Perché la memoria va acquisita prima dello spegnimento?
2. Quali indicatori in memoria rivelano una code injection?
3. Cosa aggiunge un analyzer di Timesketch rispetto alla timeline grezza?
4. Quali caratteristiche statistiche distinguono il beaconing dal traffico legittimo?
5. Quali limiti incontra la network forensics con traffico cifrato?

FINE DELLA LEZIONE · MODULO 09

Grazie

Memory e network forensics con AI · Corso «Incident Response potenziata dall'AI»

Domande e materiali: ricevimento del docente. Profilo e contatti: vincenzocalabro.it

Vincenzo Calabrò

CYBER SECURITY · DIGITAL FORENSICS

VINCENZOCALABRO.IT