Seloom
www.selcomintelligence.com

M2B-01

RILEVATORE DI SPYWARE PER SMARTPHONE E TABLET

Una soluzione avanzata di cybersecurity per rilevare la presenza di Trojan e spyware su smartphone e tablet, senza toccare fisicamente il dispositivo.

ANALISI RAPIDA E RESPONSO IMMEDIATO

M2B-01 è un dispositivo di bonifica forense che analizza il traffico dati Wi-Fi di smartphone e tablet per individuare spyware e Trojan. Agisce senza toccare il dispositivo, creando una rete locale e generando in pochi minuti un report certificato sui pattern sospetti.

Attraverso lo sniffing passivo (Man-in-the-Middle), identifica anomalie di rete e domini malevoli, generando un report certificato utilizzabile in sede legale.

Grazie alla sua flessibilità algoritmica, alla versatilità di adattamento e alla capacità di analizzare comportamenti anomali e complessi, M2B-01 offre la possibilità di individuazione verso un'ampia gamma di minacce, dalle più comuni alle più sofisticate.

CARATTERISTICHE:

- **Analisi veloce e automatizzata: circa 5 minuti.**
- **Rilevazione Avanzata: Individuazione di anomalie DNS, certificati sospetti e connessioni malevole.**
- **Blocco attivo dei microfoni degli smartphone: contromisure a ultrasuoni integrate per analisi senza allertare l'attaccante.**
- **È possibile analizzare qualsiasi dispositivo con qualunque sistema operativo.**
- **Analisi non invasiva: nessun intervento fisico sul dispositivo da analizzare, nessuna copia di dati.**
- **Tecnologia Sniffing (MITM Passivo): monitoraggio in tempo reale del traffico tramite Wi-Fi locale.**
- **Report forense: generazione automatica di un PDF ammissibile in procedimenti legali, e file capture.pcap.**
- **Massima sicurezza: nessun invio dati a server esterni.**
- **Aggiornamenti software sempre disponibili.**

Indice di compromissione ALTO

Sono presenti uno avvisi con priorità elevata, il dispositivo è compromesso da Trojan Software Spy.

Indice di compromissione MODERATO

Sono presenti due avvisi con priorità moderata, è necessario eseguire approfondimenti.

Indice di compromissione BASSO

Abbiamo verificato la NON presenza di Trojan Software Spy, sono presenti tre avvisi con priorità bassa da controllare.

Il cuore di M2B-01 è un motore di analisi avanzato che monitora costantemente il traffico di rete, alla ricerca di pattern sospetti. Il sistema si basa su un set di Indicatori di Compromissione accuratamente selezionati, che includono:

- ✓ Anomalie nella gestione dei certificati di sicurezza.
- ✓ Utilizzo improprio di servizi di certificazione gratuiti.
- ✓ Impiego sospetto di infrastrutture DNS.
- ✓ Comunicazioni su canali non convenzionali.
- ✓ Attività legate a domini di recente creazione.
- ✓ Trasmissioni non sicure o anomale.
- ✓ Connessioni verso domini e/o IP potenzialmente malevoli.
- ✓ Interazioni con reti anonimizzate.
- ✓ Comunicazioni con reti note per attività illecite.

SPECIFICHE	M2B-01
Alimentazione	Continua 220V / Batteria 12V integrata
Autonomia	Fino a 10 ore. Ricarica circa 4 ore
Connettività	WiFi / 4G LTE (SIM card non inclusa)
Dimensioni	36x26x15 cm
Peso	4,2 Kg

ESEMPIO DI REPORT IN PDF (si genera automaticamente)

Rapporto di Acquisizione	
Dispositivo utilizzato da: Mario Rossi	Marca e modello: Samsung Galaxy S10
Numero telefonico: 33826985412	Rapporto generato in data e ora: 02/07/2024 - 15:12:13

Durata acquisizione: 113,277351391 secondi	Indirizzo MAC dispositivo: 7a:18:da:77:a7:29
Inizio acquisizione: 2024/07/02 - 15:10:06	IMEI 1: 355962378921453
Termine acquisizione: 2024/07/02 - 15:11:59	IMEI 2: 352661578921841
Numero di pacchetti: 11007	BLAKE2s acquisizione: 98116a7eb405886164ad978112350ac8 38a47e6d1cb391d333737720a54fe76c
Note: Analisi effettuata dal tecnico Ing. Paolo Brambilla presso la sede del cliente.	

Il dispositivo è compromesso da Trojan Software Spy poiché sono presenti uno avvisi con priorità elevata.

INDICE DI COMPROMISSIONE
ALTO
ANALISI DMTRO

È stata effettuata una richiesta DNS a mobile-tracker-data.com con contrassegno Trojan Software Spy.

Il nome di dominio **mobile-tracker-data.com** visualizzato nell'acquisizione è stato esplicitamente contrassegnato come dannoso. Questo comportamento è palesemente indicativo. Sicuramente il dispositivo è compromesso da un Trojan Software Spy.

INDICE DI COMPROMISSIONE
MODERATO
ANALISI INPRD

UDP comunicazione in uscita dalla rete locale a 157.240.203.14.

Il protocollo **UDP** è comunemente utilizzato nelle reti interne. Verificare se l'host **157.240.203.14** ha sfruttato altri avvisi, fattore che potrebbe indicare un possibile comportamento dannoso.

INDICE DI COMPROMISSIONE
BASSO
ANALISI NCHST

Il server 149.154.167.151 non è stato risolto da nessuna query DNS durante la sessione

Questo indica che il server **149.154.167.151** probabilmente non è stato risolto da nessun nome di dominio o che la risoluzione è già stata memorizzata nella cache dal dispositivo. Se l'host viene visualizzato in altri avvisi, controllarlo.

INDICE DI COMPROMISSIONE
BASSO
ANALISI HTPBG

Sono state generate comunicazioni HTTP dirette all'host www.semanticscholar.org

Il dispositivo ha effettuato uno scambio con l'host **www.semanticscholar.org** utilizzando HTTP, un protocollo non criptato. Anche se questo comportamento non è dannoso in sé, è raro rilevare comunicazioni HTTP generate da applicazioni per smartphone in esecuzione in background. Controllare la reputazione dell'host effettuando una ricerca in Internet.