M2 Bridge

Bonifiche su Smartphone e Tablet

Con l'apparato *M2 Bridge* possiamo analizzare il traffico rete di qualsiasi Cellulare o Tablet e comprendere se vi è un Trojan-Software Spy al suo interno.

- Il Cellulare o Tablet da analizzare non viene neppure "toccato dall'operatore"
  M2 Bridge è un dispositivo che utilizza la tecnologia di Sniffing - "Man in the Middle".
- E' sufficiente che il proprietario del cellulare da analizzare si agganci alla rete Wi-Fi locale che *M2 Bridge* andrà a generare e segua le indicazioni dell'operatore.
- In automatico verrà generato un Report (pdf in italiano) + un file *capture.pcap* per utilizzo forensico.
- E' possibile analizzare qualsiasi dispositivo con qualunque sistema operativo.
- Analisi estremamente veloce (circa 10 min.).
- Utilizzo semplicissimo e completamente automatizzato.
- *M2 Bridge* utilizza specifici Indicatori di Compromissione abbinati a delle White List e a delle Black List interne.

Avremo immediatamente un responso:

Sono presenti avvisi con priorità elevata, il dispositivo è compromesso da Trojan-Software Spy oppure ***E' tutto OK, sono presenti due avvisi con priorità bassa da controllare*** oppure ***Sono presenti avvisi con priorità moderata, è necessario eseguire approfondimenti***.

Verrà quindi generato automaticamente un Report completo in PDF, comprendente:

- Il nome del dispositivo.
- La durata dell'acquisizione.
- L'SHA1 di acquisizione.
- Data del rapporto generato.
- Il numero di pacchetti.
- Le descrizioni date dagli Indicatori di Compromissione.

Il posizionamento delle Comunicazioni e di tutte le trasmissioni intercettate:

- Il Protocollo.
- L'indirizzo IP.
- Il Dominio (se disponibile).
- Il numero della Porta di Destinazione.

Inoltre, sempre automaticamente verrà generato un file *capture.pcap* per successive analisi forensiche.

Esempio di Report in PDF

Report Sniffing M2 Bridge

Nome dispositivo: MYA-L11
Indirizzo MAC dispositivo: c4:86:e9:e4:57:07
Rapporto generato in data 28/02/2022 - 14:10:01
Durata acquisizione: 99.622975895 secondss
Numero di pacchetti: 14170
SHA1 acquisizione: 3ca4ebd94ec6df777ccda196e943580aa1720b02

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

Indice di Compromissione **ALTO**

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**

Comunicazione a mobile-tracker-data.com con il CIDR 51.15.183.209/32 con contrassegno Trojan Software Spy.

Il server mobile-tracker-data.com risiede in una rete conosciuta per l'esecuzione di attività dannose. Questo comportamento è esplicitamente sospetto. Sicuramente il dispositivo è compromesso da un Trojan Software Spy.

Indice di Compromissione **BASSO**

Sono state generate comunicazioni HTTP dirette all'host 31.13.71.50

Il dispositivo ha effettuato uno scambio con l'host 31.13.71.50 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.

Indice di Compromissione **BASSO**

Il server 31.13.71.50 non è stato risolto da nessuna query DNS durante la sessione.

Questo indica che il server 31.13.71.50 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.

Comunicazioni che necessitano approfondimenti

Protocollo	Dominio	Indirizzo IP di destinazione	Numero della porta di destinazione
TCP	--	157.240.203.60	443
TCP	--	31.13.71.50	80
TCP	mobile-tracker-data.com	51.15.183.209	443

Comunicazioni inserite nella whitelist

Protocollo	Dominio	Indirizzo IP di destinazione	Numero della porta di destinazione
UDP	--	192.168.100.1	63
UDP	--	192.168.100.1	57
UDP	--	255.255.255.255	67
TCP	clients3.google.com	216.58.198.14	80
TCP	connectivitycheck.gstatic.com	142.250.180.99	80
TCP	geomobileservices-pa.googleapis.com	216.58.209.42	443
TCP	mtalk.google.com	108.177.126.188	5228
UDP	play-fe.googleapis.com	142.250.180.110	443
TCP	play.googleapis.com	142.250.180.138	443
	play.googleapis.com	142.250.180.138	443
TCP	push.instal.com	35.186.194.156	443
UDP	r3---sn-uxaxpu5ap5- apoe.gvt1.com	151.99.110.14	443
TCP	www.google.com	142.250.180.132	443
TCP	www.google.com	142.250.180.132	80
TCP	youtubei.googleapis.com	142.250.184.106	443
TCP	www.googleadservices.com	142.250.184.98	443
TCP	firebasesettings.crashlytics.com	142.250.184.35	443
UDP	beacons.gvt2.com	216.58.208.131	443
TCP	app-measurement.com	216.58.208.142	443
UDP	asia.pool.ntp.org	121.174.142.81	443
TCP	clients3.google.com	216.58.198.14	80
TCP	static.whatsapp.net	31.13.86.51	443

Esempio di file capture.pcap