Relazione di Network Security

Nome: Marco

N° Matricola: 7025991

Cognome: De Stefano

Data: Dicembre 2024

1 Introduzione

In questo ultimo assignment, il nostro obiettivo è quello di fare **debunking** su degli articoli riguardanti la Network Security,ovvero, prendere delle notizie e verificare se sono state analizzate in modo giusto, se sono state banalizzate o estremizzate. Analizzeremo una notizia confrontando i vari siti che ne parlano cercando anche di analizzare gli argomenti trattati.

2 Droidbot

In particolare, ci concentreremo su articoli che descrivono il malware DroidBot, un nuovo Remote Access Trojan (RAT) progettato per compromettere dispositivi Android e rubare credenziali finanziarie. Esamineremo come questa notizia è stata riportata da diverse fonti, confrontando i livelli di approfondimento, il linguaggio utilizzato e l'accuratezza delle informazioni. L'obiettivo finale è valutare se le notizie aiutino effettivamente il lettore a comprendere la pericolosità del malware oppure se si limitino a fornire dettagli superficiali o sensazionalistici.

Le fonti prese in considerazione includono siti di settore specializzati e media generici, come:

- HDblog
- Cybersecurity360
- SecurityWeek
- Il Giornale
- Trovoprezzi.it

Questa analisi permetterà non solo di valutare la qualità della comunicazione giornalistica in ambito tecnologico, ma anche di comprendere meglio le sfide associate alla diffusione di notizie accurate e utili in un settore complesso come quello della sicurezza informatica.

2.1 HDblog - "DroidBot, il nuovo trojan per Android che svuota il conto in banca"

In questo articolo si apprende delle informazioni fondamentali. Infatti, ci spiegano che Droidbot è un RAT fatto per rubare dati utili ad accedere ai servizi finanziari delle vittime. Viene distribuito tramite servizio MaaS (Malware as a Service) dal costo di tremila dollari al mese. Ci informano che ha preso di mira 77 diverse entità finanziarie tra cui: Francia, Germania, Portogallo, Regno Unito, Spagna, Turchia e Italia.

Esso elenca anche le funzioni di questo trojan, tra cui:

- **Intercettazione degli SMS:** il malware monitora i messaggi SMS in entrata, spesso utilizzati dagli istituti finanziari per fornire i numeri di autenticazione delle transazioni (TAN), consentendo agli aggressori di bypassare i meccanismi di autenticazione a due fattori.
- **Key-Logging:** sfruttando i servizi di accessibilità, DroidBot cattura le informazioni sensibili visualizzate sullo schermo o digitate dall'utente come le credenziali di accesso, i dati personali e i saldi dei conti.
- **Attacco overlay:** viene mostrata una falsa pagina di login sovrapposta all'applicazione bancaria legittima, quando quest'ultima viene avviata, per intercettare le credenziali di accesso della vittima.
- **VNC-Like Routine:** DroidBot scatta periodicamente schermate del dispositivo della vittima, fornendo ai malfattori una panoramica in tempo reale dell'attività del sistema compromesso.
- **Controllo remoto:** sfruttando i Servizi di accessibilità, DroidBot consente il controllo remoto del dispositivo infetto. Questo comprende l'esecuzione di azioni come la compilazione di moduli e la navigazione nelle applicazioni, consentendo agli aggressori di utilizzare il dispositivo come se fossero fisicamente presenti.

Specifica, l'articolo, che questo trojan utilizza una comunicazione a due canali: trasmette i dati tramite MQTT e riceve i comandi in entrata tramite HTTPS. Dopo aver dato queste informazioni senza specificare cosa esso voglia dire, da anche un consiglio per prevenire eventuali infezioni dei nostri dispositivi:

"*Per non correre rischi è consigliabile scaricare esclusivamente applicazioni verificate.*"

2.2 Cybersecurity360 - "DroidBot, lo spyware Android che mette nel mirino gli istituti finanziari: come difendersi"

Nel seguente articolo, oltre alle precedenti informazioni apprese, gli autori specificano che il trojan ha origini turche e che opera come una piattaforma MaaS dove i suoi creatori vendono l'accesso ad affiliati, mettendo a loro disposizione un'infrastruttura dedicata. Infatti agli affiliati viene fornito un pannello di controllo e comando (C2) da cui si può eseguire controllo remoto di dispositivi, raccolta credenziali, attacchi e è possibile personalizzare questi per obiettivi specifici.

L'articolo, soprattutto, da più informazioni sulla tipologia di comunicazione ovvero quella a due canali. Infatti, oltre a dire quello scritto nel precedente articolo, specifica la novità di questo malware citando l'articolo di analisi di Creafy. Il malware, utilizzando il protocollo di trasmissioni dati MQTT, rende più difficile il rilevamento e l'interruzione di queste operazioni poichè è un protocollo

non comunemente associato a queste tipologie di attività.

Si parla, poi, della sua pericolosità: viene specificato che è ancora in fase di sviluppo e che quindi potrebbe essere migliorata rendendo essa una continua minaccia e che potrebbe crescere il suo grado di pericolosità. La notizia riporta anche le parole del rapporto di Cleafy:

> "*Il vero punto di preoccupazione risiede in questo nuovo modello di distribuzione e affiliazione, che eleverebbe il monitoraggio della superficie di attacco a un livello completamente nuovo.", continua il rapporto e conclude, "Questo potrebbe essere un punto critico, poiché cambiare la scala di un set di dati così importante potrebbe aumentare significativamente il carico cognitivo. Se non supportato in modo efficiente da un sistema di monitoraggio in tempo reale, ciò potrebbe sopraffare gravemente i team antifrode all'interno degli istituti finanziari.*"

Questa citazione, non mi sembra efficace ai fini del comprendere la vera pericolosità del malware, che viene effettivamente spiegata nel rapporto di CLeafy, dopo aver spiegato la definizione di MaaS.

2.3 Geopop - "Arriva il trojan delle app bancarie su Android che svuota il conto: come difendersi da DroidBot" ,MSN - "DroidBot, il nuovo trojan per Android che svuota il conto in banca, Cryptocurrency Applications", Il Giornale - "App bancarie, la nuova "arma" dei cybercriminali: ecco come svuotano i conti"

Nei seguenti articoli non viene aggiunto niente in più rispetto agli articoli precedenti e ripetono parola per parola quello scritto dal rapporto Cleafy.

2.4 trovaprezzi.it - "DroidBot è il trojan Android che vi svuota il conto in banca!"

Questo articolo rappresenta un esempio di come non dovrebbe essere affrontato un argomento di sicurezza informatica in modo professionale. Oltre a ripetere frasi già presenti in altri articoli, viene formulata un'affermazione non solo non confermata, ma addirittura smentita dal rapporto ufficiale di Cleafy.
In particolare, l'articolo afferma:

> "*L'evoluzione del malware (al momento sembra essere ancora in fase di sviluppo) e le sue capacità avanzate richiederanno una vigilanza attiva da parte delle organizzazioni e sopratutto aggiornamenti costanti della sicurezza.*"

Tuttavia, il rapporto ufficiale di Cleafy ridimensiona chiaramente l'allarme, specificando:

> "*The malware presented here may not shine from a technical standpoint, as it is quite similar to known malware families.*"

Cleafy evidenzia quindi che il malware non si distingue per innovazione tecnica, sottolineando che è ancora in fase di evoluzione e non rappresenta, al momento, una minaccia significativa rispetto ad altre famiglie già note. Questa discrepanza mette in luce come un'informazione inaccurata o esagerata possa generare inutili preoccupazioni.

2.5 Conclusioni sulla seguente notizia

Dopo aver analizzato le diverse fonti, Cybersecurity360 si distingue come l'unico sito che offre un approfondimento significativo sulla pericolosità di questo malware. In particolare, evidenzia che il problema principale non risiede tanto nelle tecniche utilizzate, quanto nel modello di distribuzione adottato. DroidBot opera infatti come una piattaforma Malware-as-a-Service (MaaS), in cui gli sviluppatori non si limitano a fornire il malware, ma offrono un'infrastruttura completa, codice e supporto per consentire a terzi di condurre attacchi. Questo modello di business amplifica la complessità della superficie di attacco, rendendo più difficile il monitoraggio e la mitigazione. Con un'adozione di massa del modello MaaS, le superfici di attacco diventano molteplici e frammentate, poiché diversi attori possono condurre attacchi simultanei su obiettivi diversi.

È inoltre interessante notare che nessuno degli articoli analizzati menziona il concetto di una rete MaaS privata, che potrebbe ulteriormente aggravare le difficoltà di monitoraggio e prevenzione. Questo punto avrebbe potuto essere un'importante aggiunta per comprendere appieno la pericolosità del malware.

Dal punto di vista della comunicazione mediatica, Cybersecurity360 si distingue per il suo approccio informativo e tecnico, fornendo un'analisi approfondita e precisa. Al contrario, siti come HDblog, Geopop, Il Giornale e trovaprezzi.it adottano titoli sensazionalistici, come "*Ecco come svuotano i conti*" chiaramente pensati per attirare clic. Tuttavia, va notato che il contenuto di HDblog risulta più equilibrato rispetto al titolo, mentre l'articolo de Il Giornale appare meno approfondito, una caratteristica prevedibile vista la natura generalista del quotidiano.

Si osserva che la sezione 2.3 non offre un'analisi dettagliata, poiché i siti citati non aggiungono informazioni rispetto a quanto già noto. E' è stata comunque inclusa per evidenziare come numerosi siti si limitino a fare copia e incolla di altre notizie, senza verificare o approfondire i contenuti.

Infine, viene citato trovaprezzi.it, un sito che, già dal nome, non sembra avere una particolare specializzazione nel campo della cybersecurity. L'analisi della notizia risulta completamente assente: l'articolo si limita a ripetere le informazioni già riportate da altre fonti, enfatizzando il problema in modo eccessivo e presentando il malware come una minaccia avanzata, in contrasto con le valutazioni tecniche più precise e moderate.

3 Post Scrittum

Questa sezione è per fare presente al professore che tutti i compiti consegnati con la seguente matricola 7025991 (triennale) corrispondono, invece, alla matrice 7174515(magistrale).