DATA SHIELDS

REPORT TWIN EVIL ATTACK

Giugno 2024

Prepared by
Data Shields Team

Prepared for
Theta

Indice

Introduzione

Twin Evil Attack

Siamo lieti di annunciare che la nostra azienda ha accettato con entusiasmo l'incarico di investigare sull'intrusione informatica subita dall'azienda Theta. Siamo consapevoli dell'importanza cruciale di garantire la sicurezza delle infrastrutture digitali e della necessità di ripristinare rapidamente un ambiente sicuro e affidabile per le operazioni aziendali di Theta.
Il recente attacco subito da Theta, che ha coinvolto l'uso di lampadine IoT per migliorare l'efficienza energetica e l'automazione degli uffici, rappresenta una sfida complessa. Un attaccante sofisticato ha sfruttato la tecnica "Twin Evil" per ottenere accesso non autorizzato alla rete aziendale, lasciando un messaggio inquietante: "**Ya airgeddoned!**" su ogni server e client. Questo ha compromesso la sicurezza di tutta l'infrastruttura digitale di Theta.

- La prima fase del nostro intervento prevede un'analisi dettagliata dell'attacco per identificare le vulnerabilità sfruttate dall'attaccante. Utilizzeremo strumenti avanzati e metodologie consolidate per raccogliere evidenze, analizzare i dati e comprendere le dinamiche dell'intrusione.
-
- Successivamente, elaboreremo un piano di prevenzione su misura per Theta, basato sulle migliori pratiche di sicurezza informatica. Questo piano includerà misure di rafforzamento della sicurezza, raccomandazioni per l'aggiornamento delle politiche aziendali e strategie di monitoraggio continuo per rilevare e prevenire future minacce.

Siamo fiduciosi che la nostra esperienza e il nostro impegno ci permetteranno di ripristinare la sicurezza dell'infrastruttura digitale di Theta e di proteggerla da futuri attacchi. Lavoreremo a stretto contatto con il team di Theta per garantire una transizione senza intoppi verso un ambiente più sicuro e resiliente.

Definizione della tipologia di attacco

Dopo un attenta analisi , la Datashields ha constatato che l'attacco effettuato nei confronti dell'azienda theta è di tipo Twin Evil.
Un "Twin Evil" è un falso punto di accesso Wi-Fi che viene configurato per assomigliare a un punto di accesso legittimo.
Quando ci si connette a una rete Wi-Fi, il dispositivo (degli utenti) cerca il nome della rete (SSID) e si connette automaticamente se trova una rete con lo stesso nome.
Un attaccante può creare un Evil Twin con lo stesso SSID del punto di accesso legittimo, inducendo i dispositivi a connettersi al punto di accesso falso invece che a quello autentico.
Nel vasto panorama delle minacce informatiche, l'attacco Evil Twin emerge come una delle tattiche più insidiose utilizzate dai cyber criminali per compromettere la sicurezza delle reti Wi-Fi.

L'attacco Evil Twin è un tipo di attacco man-in-the-middle (MitM) che si verifica a livello di dominio delle reti wireless.
In questa tattica, un aggressore crea una rete Wi-Fi malevola che imita l'aspetto di una rete legittima, al fine di ingannare gli utenti inconsapevoli a connettersi a essa invece che alla rete originale.

Rischi dell'attacco Twin Evil

- C**attura delle Credenziali**:Quando gli utenti si connettono all'Evil Twin, possono essere reindirizzati a una pagina di login fasulla, dove inseriscono le loro credenziali (come la password della rete Wi-Fi). Queste credenziali vengono catturate dall'attaccante.

- **Intercettazione del Traffico** : L'attaccante può intercettare tutto il traffico che passa attraverso il falso punto di accesso, compresi dati sensibili come informazioni bancarie, credenziali di login e comunicazioni private.

- **Distribuzione di Malware** : L'attaccante può utilizzare il punto di accesso falso per distribuire malware ai dispositivi connessi.

- **Accesso Non Autorizzato alla Rete** : Una volta ottenute le credenziali, l'attaccante può accedere alla rete legittima, potenzialmente accedendo a risorse interne, dati sensibili e altri dispositivi connessi alla rete.

Valutazione Strumenti

Fluxion e Airgeddon

Due strumenti ampiamente utilizzati per eseguire attacchi Twin Evil sono Fluxion e Airgeddon. Questi tool sono potenti e versatili, progettati per testare la sicurezza delle reti Wi-Fi e condurre attacchi di ingegneria sociale.

Fluxion

Fluxion è uno strumento open-source che utilizza un approccio di ingegneria sociale per ottenere le credenziali delle reti wireless. Funziona clonando un access point legittimo e inducendo l'utente a inserire le proprie credenziali su una falsa pagina di autenticazione. Fluxion sfrutta tecniche di deautenticazione per disconnettere i dispositivi dagli AP originali, costringendoli a connettersi al falso AP creato dall'attaccante.

Airgeddon

Airgeddon è un framework di sicurezza wireless completo che integra diverse tecniche e strumenti per condurre attacchi e test di penetrazione. Tra le sue numerose funzionalità, Airgeddon supporta anche gli attacchi Twin Evil. Questo strumento facilita la creazione di un falso access point, permettendo di intercettare il traffico degli utenti e raccogliere informazioni critiche. Airgeddon automatizza molte fasi del processo, rendendolo accessibile anche a utenti con conoscenze tecniche di base.

Confronto tra Fluxion e Airgeddon

Fluxion è altamente specializzato e focalizzato sull'ingegneria sociale per il recupero delle credenziali Wi-Fi. Airgeddon, d'altra parte, offre un approccio più versatile e integrato, combinando vari tipi di attacchi e strumenti di sicurezza in un'unica interfaccia.

Caratteristica	Airgeddon	Fluxion
Focus	Multitool, ampia gamma di attacchi	Evil-Twin , Phishing
Automazione	Moderato, richiede configurazioni Manuali	Alta , Altamente Automatizzato
Strumenti integrati	Aircrack-ng , mdk3, ettercup e molti altri	Aircrack-ng, Hostapd , DNSmasq, LIGHTTPD

Utilizzo Tipico	Penetration Test Completo(educativo)	Attacchi mirati , rapido e semplice
Modularità ed estendibilità	Si, facilmente estendibile con nuovi tool	No
Compatibilità	Funziona su diversi sistemi operativi Linux based	Ottimizzato solo per Kali

Airgeddon

Funzionalità del tool

Airgeddon è uno strumento di auditing per la sicurezza delle reti Wi-Fi. È progettato per aiutare a testare la sicurezza delle reti wireless attraverso una serie di attacchi e tecniche di monitoraggio. Airgeddon consente agli utenti di scoprire vulnerabilità nelle reti Wi-Fi, come password deboli o configurazioni insicure, aiutando a migliorare la sicurezza complessiva della rete.

- **Scansione delle Reti Wi-Fi** : Airgeddon può scansionare le reti Wi-Fi nelle vicinanze e fornire informazioni dettagliate su di esse, come l'SSID (nome della rete), la potenza del segnale, e il tipo di sicurezza utilizzato (WEP, WPA, WPA2).

- **Attacchi di Deautenticazione** : Può disconnettere forzatamente i dispositivi dalla rete Wi-Fi, utilizzando un attacco di deauthenticazione. Questo può essere utile per costringere i dispositivi a riconnettersi, rivelando ulteriori dettagli sulla rete.

- **Creazione di Falsi Punti di Accesso** : Airgeddon può creare falsi punti di accesso (Evil Twin) con lo stesso nome della rete target, ingannando i dispositivi affinché si connettano al falso punto di accesso.

- **Attacchi di Phishing** : Una volta che un dispositivo è connesso a un falso punto di accesso, Airgeddon può reindirizzare l'utente a una pagina di login falsa, raccogliendo le credenziali di accesso della rete Wi-Fi.

- **Test di Forza Bruta e Attacchi di Dizionario** : Può eseguire attacchi di forza bruta o di dizionario per tentare di decifrare le password delle reti Wi-Fi.

Uso Etico e Legale

- **Utilizzare Airgeddon solo su reti per le quali si ha autorizzazione esplicita**. L'uso non autorizzato può essere illegale e punibile per legge.

- **Protezione delle Proprie Reti:** Utilizzare strumenti come Airgeddon per testare la sicurezza delle proprie reti e implementare misure correttive per rafforzare la sicurezza.

- **Educazione e Consapevolezza**: Formare utenti e personale sull'importanza della sicurezza delle reti Wi-Fi e su come difendersi da potenziali attacchi.

In conclusione, Airgeddon è uno strumento versatile e potente per l'auditing delle reti Wi-Fi, fornendo una suite completa di funzionalità per identificare e sfruttare le vulnerabilità delle reti wireless.

Fluxion

Introduzione a Fluxion

Fluxion è un tool di auditing di sicurezza Wi-Fi, progettato per testare la sicurezza delle reti wireless tramite attacchi di phishing e tecniche di ingegneria sociale. È uno strumento avanzato e potente, utilizzato principalmente dai penetration tester e dagli esperti di sicurezza per individuare le vulnerabilità nelle reti Wi-Fi.

Funzionalità

- **Deauthenticazione e Evil Twin** : Fluxion utilizza la tecnica di deauthenticazione per disconnettere i dispositivi legittimi dalla rete target. Questo viene fatto inviando pacchetti di deauthenticazione (deauth packets) al client e al punto di accesso (AP).Successivamente, Fluxion crea un "Evil Twin", ovvero un falso punto di accesso con lo stesso nome della rete target. Gli utenti, una volta disconnessi, si connetteranno automaticamente o manualmente a questo falso AP, pensando che sia quello legittimo.

- **Portale di Phishing** : Quando gli utenti si connettono all'Evil Twin, vengono reindirizzati a un portale di phishing che sembra la pagina di login della rete Wi-Fi legittima. Il portale di phishing richiede agli utenti di inserire la password della rete Wi-Fi per accedere a Internet, catturando così le credenziali reali degli utenti.

- **Monitoraggio del Traffico** : Fluxion monitora e cattura il traffico tra il client e l'AP, analizzando i pacchetti per estrarre informazioni utili come le credenziali di rete.Utilizza strumenti come aircrack-ng per eseguire attacchi di dizionario o di forza bruta sui pacchetti catturati, tentando di decifrare la chiave WPA/WPA2.

- **Compatibilità con più interfacce e sistemi operativi** : Fluxion è compatibile con un'ampia gamma di schede wireless e funziona su vari sistemi operativi basati su Linux, con Kali Linux essendo uno dei più comunemente usati per via delle sue numerose utility di sicurezza preinstallate.

- **Deauthentication Attack** : Utilizza aireplay-ng per inviare pacchetti di deauth ai client connessi alla rete target, costringendoli a disconnettersi.

- **Fake Access Point (Evil Twin)** : Configura un falso AP con hostapd o Airbase-ng che emula l'SSID della rete target. Gli utenti, una volta disconnessi, tendono a riconnettersi automaticamente all'AP con il segnale più forte, che sarà quello creato da Fluxion.

- **DNS Spoofing e Redirection** : Utilizza dnsmasq per rispondere alle richieste DNS dei client connessi all'Evil Twin, reindirizzandoli al portale di phishing.

- **Captive Portal Phishing** : Esegue un server web che ospita una pagina di login falsa che imita quella del router o del servizio di autenticazione della rete Wi-Fi, inducendo l'utente a inserire le proprie credenziali.

Esempio di Flusso di Lavoro

- **Identificazione della Rete Target** : L'utente avvia Fluxion e seleziona l'interfaccia wireless per cercare le reti Wi-Fi disponibili.

- **Selezione e Attacco alla Rete Target** : L'utente sceglie la rete da attaccare e avvia l'attacco di deautenticazione per disconnettere i client.

- **Creazione dell'Evil Twin** : Fluxion crea un falso AP con lo stesso nome della rete target.

- **Reindirizzamento al Portale di Phishing** : Quando gli utenti si connettono all'Evil Twin, vengono reindirizzati alla pagina di login falsa.

- **Cattura delle Credenziali** : Le credenziali inserite dagli utenti nella pagina di phishing vengono catturate e salvate, permettendo all'attaccante di ottenere l'accesso alla rete reale.

Uso Etico e legale di Fluxion

È fondamentale ricordare che Fluxion deve essere utilizzato esclusivamente per scopi etici e legali. L'uso di Fluxion per accedere a reti senza autorizzazione è illegale e può comportare gravi conseguenze legali.
Gli esperti di sicurezza utilizzano Fluxion per testare la robustezza delle proprie reti Wi-Fi e per identificare e correggere eventuali vulnerabilità.

In sintesi, Fluxion è uno strumento avanzato per il penetration testing delle reti Wi-Fi, combinando tecniche di deautenticazione, creazione di falsi AP, e phishing per testare la sicurezza delle reti wireless

Rapporto Di Sicurezza

Linee Guida Dipendenti

Difendersi dall'Attacco Evil Twin

- **Verificare l'Autenticità del Punto di Accesso** : Prima di connettersi a una rete Wi-Fi, verificare se il punto di accesso è autentico. Questo può essere fatto chiedendo al proprietario della rete o controllando l'indirizzo MAC del punto di accesso (se noto).

- **Utilizzare VPN** : Una VPN (Virtual Private Network) crittografa tutto il traffico tra il dispositivo e il server VPN, rendendo difficile per l'attaccante intercettare dati sensibili anche se si è connessi a un Evil Twin.

- **Configurare il Dispositivo per Non Connettersi Automaticamente** : Impostare i dispositivi per richiedere conferma prima di connettersi a una rete Wi-Fi sconosciuta.

- **Utilizzare Certificati di Autenticazione** : Le reti Wi-Fi aziendali possono utilizzare certificati di autenticazione per assicurarsi che solo dispositivi autorizzati possano connettersi.

- **Abilitare la Protezione WPA3**: Utilizzare reti Wi-Fi che supportano lo standard WPA3, che offre una sicurezza migliorata rispetto a WPA2.

Linee Guida Per i Tecnici

- **Configurare la Rete con WPA3** : WPA3 fornisce una crittografia più robusta e meccanismi di protezione avanzati, come l'Autenticazione Simultanea degli Equals (SAE), che rende più difficile per gli attaccanti utilizzare la forza bruta per decifrare le password.

- **Monitorare il Segnale Wi-Fi** : Utilizzare strumenti come Wireshark o Kismet per monitorare le reti Wi-Fi vicine e identificare eventuali punti di accesso sospetti con lo stesso SSID della rete legittima.

- **Educare gli Utenti** : Formare gli utenti sulle tecniche di phishing e sugli attacchi Evil Twin, insegnando loro a non inserire mai credenziali in pagine di login non familiari e a verificare sempre l'autenticità della rete.

- **Implementare un Sistema di Rilevamento delle Intrusioni (IDS)**:Utilizzare un IDS per monitorare la rete alla ricerca di attività sospette, come la presenza di punti di accesso non autorizzati.

Esempi di Strumenti Utilizzati per Difendersi

- **Wireshark** : Un analizzatore di protocollo di rete che consente di catturare e analizzare pacchetti di rete in tempo reale.

- **Kismet** : Un rilevatore di reti wireless e sistema di rilevamento delle intrusioni che può identificare punti di accesso sospetti.

- **VPN Services** : Servizi VPN come NordVPN, ExpressVPN o altri che crittografano il traffico e proteggono le comunicazioni dagli attacchi di intercettazione.

In sintesi, l'attacco Evil Twin è una minaccia seria per la sicurezza delle reti Wi-Fi. Comprendere i rischi e implementare misure di sicurezza adeguate è fondamentale per proteggere le informazioni sensibili e mantenere l'integrità delle comunicazioni wireless.

Dispositivi IoT

Introduzione

Le lampadine IoT sono dispositivi di illuminazione che si connettono a internet, permettendo agli utenti di controllarle a distanza tramite app per smartphone, assistenti vocali o sistemi di automazione domestica. Queste lampadine possono offrire una serie di funzionalità avanzate, come la regolazione della luminosità, la selezione del colore e la programmazione automatica.

Vulnerabilità Alla Pirateria Informatica

Le lampadine IoT, come altri dispositivi IoT, possono essere vulnerabili a hacking e attacchi informatici. I cyber criminali possono sfruttare le falle di sicurezza per prendere il controllo dei dispositivi, integrandoli in botnet per attacchi DDoS (Distributed Denial of Service) o accedendo a reti domestiche per scopi malevoli.Le lampadine IoT raccolgono dati sull'uso domestico e sul comportamento degli utenti, che possono essere potenzialmente intercettati o utilizzati senza il consenso degli utenti. La violazione della privacy può derivare dalla condivisione non autorizzata dei dati con terze parti o dall'accesso non autorizzato ai dati stessi

Esempi di scenari Possibili

- **Attacco Botnet:** Una lampadina IoT compromessa può essere utilizzata come parte di una botnet per lanciare attacchi su larga scala contro altri sistemi e reti.

- **Spionaggio Domestico:** Un hacker potrebbe accedere alle informazioni raccolte dalle lampadine IoT per tracciare le abitudini degli utenti, ad esempio quando sono a casa o fuori, rappresentando un rischio per la sicurezza personale.

Conclusione

Il collegamento tra lampadine IoT e "twin evil" risiede nelle vulnerabilità intrinseche dei dispositivi IoT che possono essere sfruttate per scopi malevoli, rappresentando una duplice minaccia sia alla sicurezza informatica che alla privacy degli utenti.
L'adozione di misure di sicurezza robuste, come l'aggiornamento regolare del firmware e l'uso di reti sicure, è essenziale per mitigare questi rischi

Contattaci

Phone	**06 989055942**
Email	**info@datashield.tech**
Website	**www.datashields.tech**
Address	**Via Della Sicurezza 20, Roma, Italia.**