L'IoT ci sta spiando? Scopriamolo!

Mettiamo in campo un semplice tool che ci mostra dove finiscono i pacchetti in uscita dai nostri PC, smartphone e device IoT

Siamo al giro di boa del 2020 e, come prevedevano alcuni capolavori Sci-Fi degli anni '70, le case intelligenti sono diventate realtà per molti. Le cosiddette "smart home", abitazioni piene di dispositivi intelligenti che ci aiutano nelle mansioni di tutti i giorni facilitandoci la vita, stanno diventando sempre più comuni. Oltre ai lati positivi, però, vanno considerati anche i rischi e le possibili ripercussioni che possono derivare dall'avere in casa propria una gran numero di dispositivi IoT (**Internet of Things**) connessi in rete. Questi, come ben sappiamo, hanno livelli di sicurezza che, a volte, si rivelano inadeguati. Installare un sistema di telecamere a circuito chiuso CCTV non aggiornato o scegliere l'assistente vocale sbagliato può equivalere a lasciare aperto il "portone d'ingresso" della vostra rete

Il mercato della smart home in Italia vale oltre 530 milioni di euro secondo la School of Management del Politecnico di Milano

GLOSSARIO DI BASE

ARP
è un protocollo di rete che ha lo scopo è fornire la corrispondenza tra l'indirizzo IP e l'indirizzo MAC (MAC Address) di un host presente in una rete locale Ethernet.

ARP SPOOFING
È una tecnica di falsificazione dei messaggi ARP. Con questa tecnica, un attaccante riesce a intercettare i pacchetti di rete indirizzati a un altro computer scambiando l'IP del legittimo destinatario con il suo (ed eventualmente poi rimandando i pacchetti al destinatario originale).

BOTNET
Una rete controllata da un computer detto botmaster e composta da dispositivi infettati da malware. I PC infetti sono chiamati bot o zombie e vengono usati per compiere attacchi DDoS o altri ai danni di una rete/server vittima.

IOT SPIONE

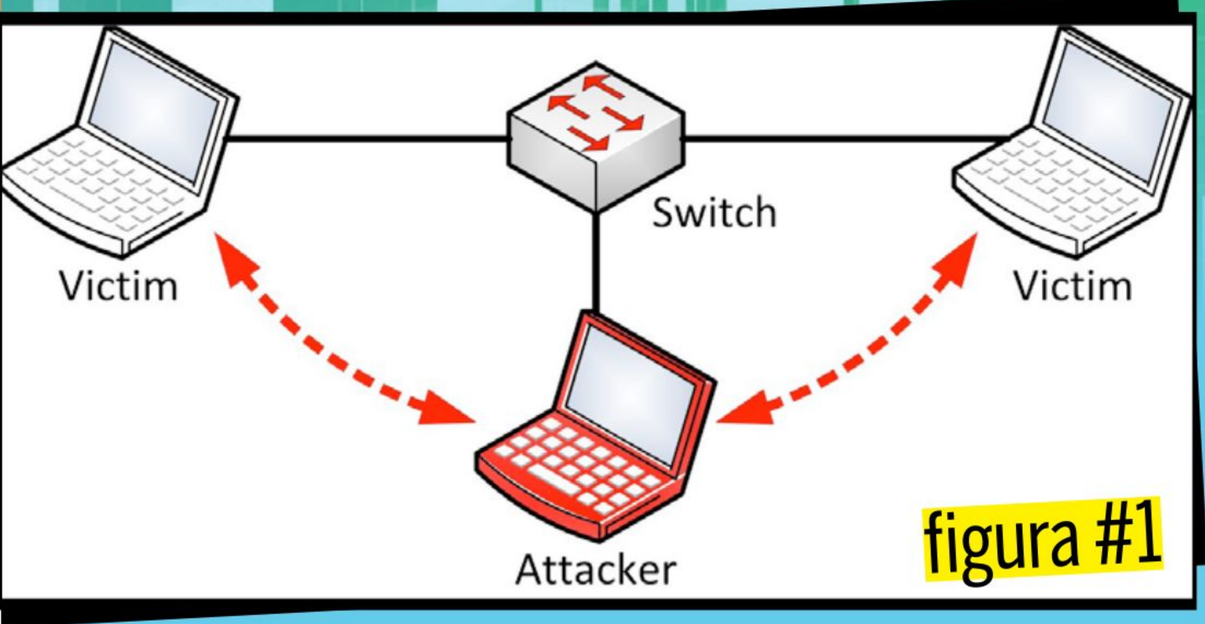

figura #1

L'attacco ARP Spoofing è una delle tecniche più antiche e conosciute della tipologia MITM. IoT Inspector usa questo attacco per estrapolare informazioni dai dispositivi che altrimenti non riusciremmo a vedere!

domestica ai malintenzionati. Per fortuna, esistono degli strumenti per monitorare e verificare la sicurezza dei dispositivi IoT. Oggi parleremo di uno di essi, Open Source e multipiattaforma, **Princeton IoT Inspector**, e di come questo software possa aiutarci a tenere sotto controllo i dispositivi smart della nostra smart home.

CHE COS'È IOT INSPECTOR

Questa applicazione è stata ideata dai ricercatori della Princeton University e monitora l'attività di tutti i dispositivi smart installati in casa. Può essere utilizzato da un portatile, da un PC e da qualunque dispositivo vi sia la possibilità di usare Python 3 (vedi box **Su quali sistemi va?** nella prossima pagina).
Questo software è incredibilmente semplice da usare e sfrutta una tecnica conosciuta come ARP spoofing [figura #1] per monitorare l'attività di tutti i dispositivi IoT connessi alla vostra rete di casa.
Gli sviluppatori hanno imposto un tetto massimo di 50 device monitorabili in contemporanea, per evitare congestionamenti a livello di rete. Una volta analizzati, i dati vengono raccolti, catalogati e condivisi con i ricercatori per essere analizzati. IoT Inspector dispone di molte utili funzioni per tutelare la vostra privacy e la sicurezza della vostra rete:

I RISCHI DELL'IOT

Se vi state chiedendo quali e quanti dei dispositivi che avete in casa possano costituire un rischio per la vostra sicurezza, avete bisogno di un piccolo ripasso. Iniziamo col dire che in questa categoria rientrano molti dispositivi comuni, come le smart TV, le videocamere di sorveglianza (CCTV), gli assistenti vocali, gli impianti di riscaldamento e illuminazione automatizzati, i robot aspirapolvere e, più in generale, tutto ciò che orbita attorno al settore della domotica. Basta che anche uno solo dei vostri dispositivi smart abbia un firmware datato o sia stato progettato senza seguire i protocolli di sicurezza standard per trovarsi esposti a rischi considerevoli.
Per esempio, se un hacker riuscisse ad accedere alla vostra rete tramite il sistema di videosorveglianza che avete installato anni fa per controllare il portone del garage, potrebbe spiare le vostre attività casalinghe e ascoltare le conversazioni private o di lavoro. Una volta entrato nella rete di casa vostra, il malintenzionato potrebbe inoltre accedere ai documenti presenti sul vostro PC, o sfruttare i vostri dispositivi per effettuare attacchi DDoS inserendoli nella propria botnet. Il problema principale di questo tipo di attacchi è che, nella maggior parte dei casi, non portano a conseguenze visibili e spesso passano inosservati per lunghi periodi di tempo. Il miglior modo di tutelarsi è impostare correttamente la propria rete domestica e acquistare dispositivi da aziende affidabili mantenendoli sempre aggiornati.

figura #2

Princeton IoT Inspector è disponibile su licenza Open Source per tutte le piattaforme!

è in grado di dirvi dove vanno a finire i dati inviati in Rete dai vostri dispositivi IoT, se questi vengono inviati a indirizzi sconosciuti o se nella vostra rete sono presenti dei **tracker**, quanti dati vengono scambiati tra il dispositivo e il ricevente e con che frequenza. Ovviamente il vostro PC rileverà l'attività di condivisione dei dati come pericolosa. Di fatto, quando installerete IoT inspector, l'antivirus tenterà di bloccarne le funzioni di ARP spoofing e dovrete essere voi ad autorizzarne l'attività. Tenete presente che il software raccoglie e invia dati ai ricercatori solo quando viene attivato e finché non decidete di spegnerlo o disinstallarlo. Potete stare tranquilli, non verranno raccolte informazioni riguardanti le attività di rete di smartphone, computer, tablet o quelle utili a identificare la vostra persona, come l'indirizzo IP o il MAC address dei vostri dispositivi. Potete anche escludere singolarmente i dispositivi che non intendete monitorare. Se non siete ancora convinti potete andare sul sito *https://iotinspector.org*: nella sezione FAQ potete consultare la lista completa di informazioni raccolte dal software e le politiche sul trattamento dei dati condivisi. Princeton IoT Inspector va inteso come un software didattico, volto allo studio dei comportamenti dei dispositivi IoT casalinghi; inoltre (è bene ricordarlo) non va a sostituirsi a un qualunque analizzatore di protocollo (come può esserlo Wireshark, tshark o tcpdump) ma piuttosto ne integra le funzioni. Lo si può intendere dunque come un "grande fratello dell'IoT", capace di conoscere gli endpoint, la sicurezza dei protocolli ma non i contenuti del traffico.

PASSIAMO ALLA PRATICA

Bene, ora che abbiamo chiarito gli aspetti fondamentali del software vediamo come utilizzarlo. Per il nostro test abbiamo usato un PC con Windows ma ricordiamo che sul sito ufficiale di IoT Inspector sono indicate anche le procedure d'installazione, non proprio banali, per GNU/Linux e macOS (vedi box qui in basso). Per cominciare recatevi all'indirizzo https://iotinspector.org [figura #2].
A questo punto dovrete seguire la procedura indicata.
1) Per prima cosa scaricate **Npcap** cliccando sull'icona **Download** nella sezione **step 1**. Si tratta di uno strumento necessario per permettere a IoT Inspector

SU QUALI SISTEMI VA?

Allo stato attuale, solo la versione Windows è supportata dai binari. Le versioni macOS e GNU/Linux sono solo sotto versione source code (in Python3) e richiedono una buona conoscenza del sistema operativo. Il software è attualmente in fase di sviluppo e le procedure potrebbero cambiare da un momento all'altro. Per maggiori informazioni visitate *https://iotinspector.org*.

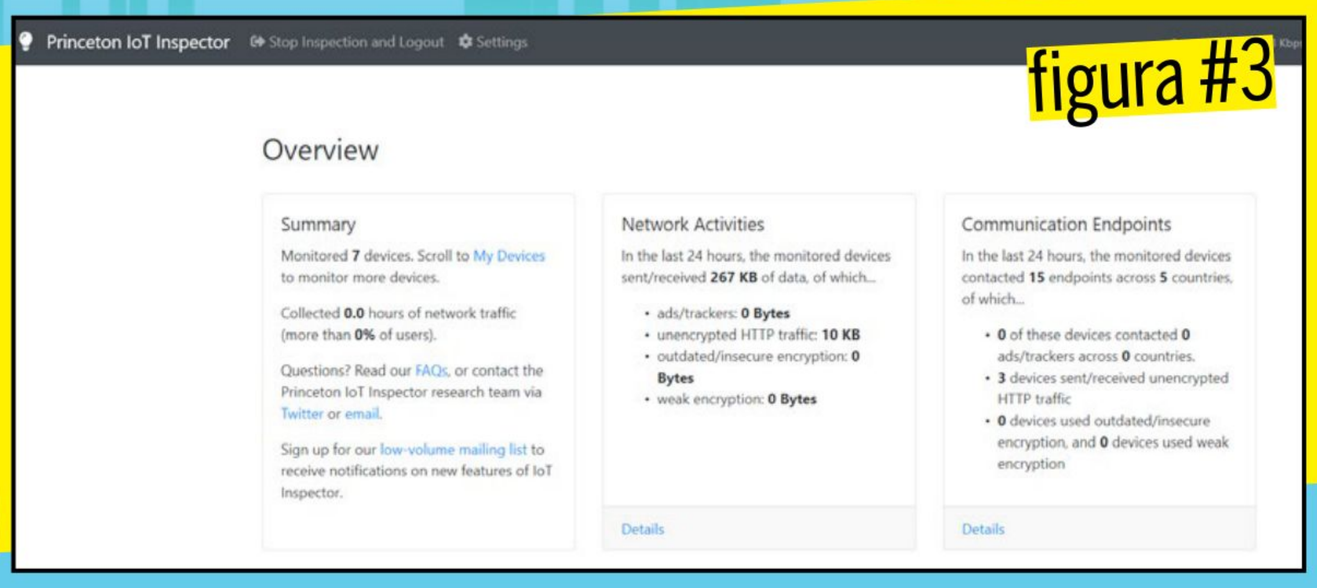

figura #3

La dashboard è il cuore pulsante di IoT Inspector. Grazie ad essa è possibile avere una panoramica dei dispositivi monitorati, del traffico analizzato e degli endpoint in uso.

figura #4

La gestione dei dispositivi viene effettuata tramite questo comodo renamer. Non dimenticate che tutte le informazioni inserite verranno condivise con l'università di Princeton e con altri utenti, perciò evitate di inserire informazioni sensibili!

di analizzare e raccogliere il traffico di rete. L'installazione è molto semplice, vi basterà accettare condizioni e termini d'uso e cliccare su **Finish** a fine procedura.
2) Se utilizzate una VPN, assicuratevi di disattivarla prima di eseguire le operazioni seguenti.

3) Scaricate IoT inspector e avviate l'installer. Apparirà una schermata di Windows che indicherà il software come dannoso. Cliccate sulla voce **Maggiori informazioni** e in basso comparirà la voce **Esegui comunque**. Cliccateci e inizierete l'installazione. A questo punto si aprirà il terminale e IoT Inspector verrà aggiornato all'ultima versione disponibile. Apparirà una finestra che vi chiederà di autorizzare il software ad apportare modifiche al vostro dispositivo: per consentire a IoT Inspector di analizzare il traffico di rete dovrete cliccare su **Sì**. Se avete Windows Defender attivo, il firewall bloccherà l'esecuzione del file **start_inspector.exe** notificandolo con una finestra all'interno della quale dovrete selezionare la voce **Consenti accesso**.
4) Una volta avviato il programma si aprirà una finestra nel vostro browser nella quale vi verrà chiesto il consenso a partecipare alla ricerca. Acconsentendo accederete al menu del software, che risponde all'URL *https://dashboard.iotinspector.org* [figura #3] all'interno del quale troverete diverse voci:

- **Overview** - elenca i singoli dispositivi connessi alla rete rilevati da IoT Inspector;
- **Summary** - indica il numero di dispositivi collegati e il tempo di attività del programma;
- **Network activities** - questa voce è presente per ogni dispositivo rilevato e riporta il quantitativo di dati inviati e ricevuti nelle ultime 24 ore e la tipologia degli stessi. Qui potete, per esempio, verificare se sono presenti dei tracker, vale a dire il tracciamento dei dati e il traffico non cifrato. All'interno di questa sezione viene mostrato

Circa il 70% dei device IoT è vulnerabile ad attacchi o ha problemi legati alla privacy

anche un pratico grafico molto utile per avere un quadro completo della situazione;

• **Communication Endpoints** - mostra i destinatari dei dati inviati e i rispettivi paesi.

Cliccando sulla voce **Details** presente in ogni sezione otterrete dei dati approfonditi. Subito sotto noterete una finestra chiamata **My device** contenente l'elenco dei dispositivi IoT rilevati dal software, che potrete rinominare [figura #4] per capire senza sforzo di quale device si tratta qualora vogliate monitorarla [figura #5].

Ora siete pronti a utilizzare IoT inspector. Ricordiamo che qualora decidiate di non voler condividere i dati analizzati o non vogliate più usare questo strumento sarà sufficiente disinstallarlo.

COME FUNZIONA

Il compito di IoT Inspector è quello di mostrare quali dispositivi potrebbero essere potenzialmente

Nel 2024, nel mondo, ci saranno 83 miliardi di device IoT connessi in Rete. Quanti saranno resi sicuri?

dannosi; il condizionale è d'obbligo, in quanto un'analisi più dettagliata è necessaria per un resoconto affidabile. IoT Inspector, difatti, permette di scremare prima gli IoT, poi di comprendere se e come sono presenti connessioni non cifrate, mal cifrate o endpoint pubblicitari e/o tracking.

I campanelli d'allarme possono essere di quattro tipi:

• **ads/trackers** - qui è menzionato il traffico che finisce direttamente in tracker di terzi. In questi casi è lecito pensare che l'IoT effettui analisi d'uso e ne invii i resoconti al produttore;

• **unencrypted HTTP traffic** - qui troviamo del traffico non cifrato. In questi casi possiamo trovare diversi falsi positivi, per esempio l'IoT che cerca nuovi aggiornamenti oppure check di status online dei server di comunicazione;

• **outdated/insecure encryption** - qui troviamo del traffico cifrato tramite cifrari insicuri e antiquati, facilmente violabili grazie a falle note. Se dovesse essere presente del traffico bisogna immediatamente verificare la presenza di aggiornamenti del dispositivo, in quanto è plausibile pensare che vengano veicolate informazioni sensibili (username, password, chiavi API etc...).

• **weak encryption** - qui troviamo del traffico cifrato tramite cifrari deboli. I rischi sono simili alla voce precedente; ci si riferisce a cifrari violabili tramite tecniche di bruteforcing, rainbow tables e altri metodi che non rientrano nelle security flaws e/o CVE.

È possibile (anzi, inizialmente è obbligatorio) definire quali dispositivi si vuole monitorare. Le flag in descrizione possono aiutarci a capire di quale dispositivo stiamo parlando, così da poterlo monitorare con più facilità.

figura #5