Zscaler: uno studio conferma che i dispositivi IoT sono una fonte importante di violazioni della sicurezza e sottolinea la necessità di adottare una sicurezza Zero trust

Lo studio rivela un aumento del 700% del malware specifico per l'IoT e i dispositivi IoT più 'chiacchieroni'

Risultati principali

- Il 98% delle vittime di attacchi malware IoT è rappresentato dai settori della tecnologia, del manifatturiero, della vendita al dettaglio e della sanità
- I dispositivi di intrattenimento e di domotica, compresi gli assistenti virtuali, rappresentano il rischio maggiore
- La maggior parte degli attacchi IoT ha avuto origine in Cina, Stati Uniti e India
- Le prime tre nazioni vittime di attacchi IoT sono state Irlanda, Stati Uniti e Cina
- Le famiglie di malware Gafgyt e Mirai hanno rappresentato il 97% del malware IoT

Milano – 23 luglio 2021 – Zscaler, Inc. (NASDAQ: ZS), leader nella sicurezza del cloud, pubblica oggi un nuovo studio che esamina lo stato dei dispositivi IoT collegati alle reti aziendali nel periodo in cui le aziende sono state costrette a ad adottare rapidamente e diffusamente il telelavoro. Il nuovo studio "IoT in the Enterprise: Empty Office Edition", ha analizzato oltre 575 milioni di transazioni tramite dispositivi e 300.000 attacchi malware volti specificamente contro dispositivi IoT bloccati da Zscaler nel corso di due settimane nel dicembre 2020 – riscontrando un aumento del 700% rispetto ai risultati pre-pandemia. Questi attacchi hanno preso di mira 553 diversi tipi di dispositivi, tra cui stampanti, soluzioni di digital signage e smart TV, tutti connessi e comunicanti con le reti IT aziendali mentre molti dipendenti erano in telelavoro durante la pandemia di COVID-19. Il team di ricerca Zscaler™ ThreatLabz ha identificato i dispositivi IoT più vulnerabili, le origini e gli obiettivi degli attacchi più comuni e le famiglie di malware responsabili della maggior parte del traffico pericoloso per aiutare meglio le aziende a proteggere i loro dati.

"Per più di un anno, la maggior parte degli uffici aziendali è rimasta per lo più inutilizzata, poiché i dipendenti hanno continuato a lavorare in remoto durante la pandemia COVID-19. Tuttavia, i nostri team di servizio hanno riscontrato che, nonostante la mancanza di dipendenti in ufficio, le reti aziendali erano ancora animate da attività IoT", ha dichiarato Deepen Desai, CISO di Zscaler che ha poi proseguito : “Il volume e la varietà dei dispositivi IoT collegati alle reti aziendali è vasto e comprende diverse tipologie di dispositivi, dalle lampade musicali alle telecamere IP. Il nostro team ha rilevato che il 76% di questi dispositivi ancora comunica su canali di testo in chiaro non criptati, il che significa che la maggior parte delle transazioni IoT rappresenta un grande rischio per le aziende".

Quali sono i dispositivi più a rischio?

Su oltre mezzo miliardo di transazioni di dispositivi IoT, Zscaler ha identificato 553 diversi dispositivi di 212 produttori, il 65 per cento dei quali rientrava in tre categorie: set-top box (29%), smart TV (20%) e smartwatch (15%). La categoria dell'intrattenimento domestico e dell'automazione ha registrato la più grande varietà di dispositivi individuali, ma il minor numero di movimenti rispetto ai dispositivi in ambito produzione, aziendale e sanitario.

La maggior parte del traffico proveniva invece da dispositivi impiegati nel settore manifatturiero e retail - il 59% di tutte le transazioni proveniva da dispositivi in questo settore e includeva stampanti 3D, geolocalizzatori, sistemi multimediali automobilistici, terminali di raccolta dati come lettori di codici a barre e terminali di pagamento. I dispositivi aziendali si sono posizionati al secondo posto, con il 28% dei movimenti, seguiti dai dispositivi sanitari con quasi l'8% del traffico.

ThreatLabz ha anche scoperto una serie di dispositivi che inaspettatamente si collegano al cloud, tra cui frigoriferi intelligenti e lampade musicali che ancora stavano inviando traffico attraverso le reti aziendali.

I responsabili

Il team ThreatLabz ha anche esaminato attentamente le attività specifiche dei malware IoT tracciate nel cloud di Zscaler. In termini di volume, sono stati osservati un totale di 18.000 host unici e circa 900 consegne di payload uniche in un periodo di 15 giorni. Le famiglie di malware Gafgyt e Mirai sono state le due famiglie più rilevate da ThreatLabz, pari al 97% dei 900 payload unici. Queste due famiglie sono note per il dirottamento dei dispositivi al fine di creare botnet, ovvero grandi reti di computer privati che possono essere controllati in gruppo per diffondere malware, sovraccaricare le infrastrutture o inviare spam.

Gli obiettivi

Le prime tre nazioni prese di mira dagli attacchi IoT sono state l'Irlanda (48%), gli Stati Uniti (32%) e la Cina (14%). La maggior parte dei dispositivi IoT compromessi, quasi il 90%, sono stati osservati rimandare i dati ai server in uno dei tre paesi: Cina (56%), Stati Uniti (19%) o India (14%).

Le misure da adottare per proteggersi

Poiché l'elenco dei dispositivi "intelligenti" disponibili cresce ogni giorno, è quasi impossibile impedire loro di entrare in azienda. Piuttosto che cercare di eliminare la cosiddetta shadow IT, i team IT dovrebbero implementare policy di accesso che impediscano a questi dispositivi di servire come porte aperte ai dati e alle applicazioni aziendali più sensibili. Queste policy e strategie possono essere impiegate sia che i team IT (o altri dipendenti) siano in loco o meno. ThreatLabz raccomanda i seguenti suggerimenti per mitigare la minaccia del malware IoT, sia sui dispositivi gestiti che BYOD:

- **Avere visibilità dei dispositivi di rete**. Distribuire soluzioni in grado di rivedere e analizzare i log di rete per monitorare tutti i dispositivi che comunicano attraverso la rete e le azioni che compiono.
- **Cambiare tutte le password di default**. Il controllo delle password potrebbe non essere sempre possibile, ma un primo passo fondamentale per l'implementazione di dispositivi IoT di proprietà aziendale dovrebbe essere quello di aggiornare le password e implementare l'autenticazione a due fattori.
- **Aggiornare e applicare patch regolarmente.** Molti settori, in particolare il manifatturiero e la sanità, si affidano ai dispositivi IoT per i loro flussi di lavoro quotidiani; è necessario essere aggiornati su tutte le nuove vulnerabilità che vengono scoperte e mantenere la sicurezza dei dispositivi aggiornata con le ultime patch.
- **Implementare un'architettura di sicurezza Zero Trust**. Applicare policy rigorose per le risorse aziendali in modo che gli utenti e i dispositivi possano accedere solo a ciò di cui hanno bisogno, e solo dopo l'autenticazione. Limitare la comunicazione agli IP rilevanti, ASN e porte necessarie per l'accesso esterno. I dispositivi IoT non autorizzati che richiedono l'accesso a Internet dovrebbero passare attraverso l'ispezione del traffico ed essere bloccati da tutti i dati aziendali, idealmente attraverso un proxy. L'unico modo per impedire che i dispositivi shadow IoT rappresentino una minaccia per le reti aziendali è quello di eliminare le policy di fiducia implicita e controllare strettamente l'accesso ai dati sensibili utilizzando l'autenticazione dinamica basata sull'identità - nota anche come Zero Trust.

Zscaler ThreatLabz
Il team di ricerca Zscaler ThreatLabz è composto da esperti di sicurezza, ricercatori e ingegneri di rete responsabili dell'analisi e dell'eliminazione delle minacce nel cloud di sicurezza Zscaler e dello studio del panorama globale delle minacce. Il team condivide la sua ricerca e i dati del cloud con il settore per contribuire a promuovere la sicurezza online.

Tutti i dati presentati in questo report provengono direttamente dalla piattaforma Zscaler, che facilita oltre 160 miliardi di transazioni al giorno. I dati per questo report sono stati raccolti tra il 15 dicembre e il 31 dicembre 2020, e rappresentano solo i dispositivi e gli attacchi sulle reti aziendali in sedi fisiche. ThreatLabz ha osservato circa 300.000 transazioni bloccate relative a malware IoT, exploit e comunicazioni command-and-control, compreso un totale di 18.000 host unici e circa 900 consegne di payload uniche in questo periodo di 15 giorni.
Per ulteriori informazioni, e per accedere al report completo, consultare "IoT in the Enterprise: Empty Office Edition".

A proposito di Zscaler

Zscaler (NASDAQ: ZS) accelera la trasformazione digitale in modo che i clienti possano essere più agili, efficienti, resilienti e sicuri. Zscaler Zero Trust Exchange protegge migliaia di clienti da attacchi informatici e dalla perdita di dati collegando in modo sicuro utenti, dispositivi e applicazioni in qualsiasi luogo. Distribuita in oltre 150 data center a livello globale, Zero Trust Exchange, basato su SASE, è la più grande piattaforma di sicurezza cloud in line del mondo.

Per ulteriori informazioni:
Tania Acerbi
Monica Fecchio
Prima Pagina
Piazza Giuseppe Grandi 19 - 20129 Milano
e-mail: tania@primapagina.it
e-mail: monica@primapagina.it
Tel. +39 02 91339811