REPORT 2021

IoT in azienda: gli uffici sono vuoti, ma...

Cosa accade quando i dispositivi smart restano incustoditi sul luogo di lavoro?

zscaler™

Nel 2020 e nel 2021, la pandemia di COVID-19 ha lasciato molti uffici aziendali deserti. Nonostante l'assenza del personale, questi edifici brulicavano di attività apparentemente invisibili. Gli edifici non non erano i soli ad essere stati abbandonati a se stessi: smart watch, insegne digitali stampanti di rete e molti altri dispositivi IoT erano rimasti comunque collegati alla rete, ad aggiornare dati, eseguire funzioni e attendere comandi.

E cosi, nel bel mezzo di una rivoluzione planetaria che avrebbe eletto lo smart working quale modo ideale di lavorare ovunque gli hacker se ne sono accorti e in parecchi ne hanno tratto vantaggio. Risultato: un record di 833 malware IoT bloccati ogni ora.

Il numero sempre crescente di dispositivi Iot che si connettono sulle reti aziendali, include di tutto: dagli smart watch alle telecamere IP, dalle automobili ai dispositivi musicali. Il 76% delle transazioni avviene su canali di testo non crittografato, anche se tutti i dispositivi utilizzano l'SSL per almeno una parte delle comunicazioni. Le organizzazioni devono adottare policy e architetture zero trust per proteggere le proprie reti da questi dispositivi. Il team ThreatLabz di Zscaler, specializzato in ricerca e intelligence sulle minacce, ha svolto un'analisi approfondita dei dispositivi IoT autorizzati e non autorizzati e delle tendenze malware Iot, su un periodo di due settimane di dati provenienti dal cloud di Zscaler.

I dati sono stati raccolti in due studi: uno sulla creazione di impronte digitali da parte dei dispositivi IoT, che identifica i dispositivi IoT e il traffico, e uno sui malware IoT, basato sui dati provenienti dal cloud di Zscaler. Poiché i dispositivi IoT, in particolare i quelli non autorizzati, non sono basati su agenti, tutti i dati contenuti in questo resoconto rappresentano dispositivi e attacchi alle reti aziendali nelle sedi fisiche degli uffici. I dati sono stati raccolti tra il 15 e il 31 dicembre del 2020, periodo in cui la maggior parte degli uffici aziendali non essenziali era chiusa.

Risultati chiave

- I malware IoT sulle reti aziendali sono aumentati del 700% rispetto al nostro studio del 2019, nonostante gran parte della forza lavoro globale operasse da casa
- I dispositivi di intrattenimento e domotica sono risultati il rischio maggiore, a causa della varietà, della bassa percentuale di comunicazioni criptate e della loro connessione adestinazioni sospette
- Il 97% del malware IoT bloccato dal cloud di Zscaler era rappresentato da Gafgyt e Mirai, le famiglie di malware maggiormente utilizzate nelle botnet
- Vittima degli attacchi IoT erano per il 98% i settori tecnologia, manifatturiero, vendite al dettaglio e all'ingrosso e sanitario
- La maggior parte degli attacchi aveva origine in Cina, negli Stati Uniti, e in India
- La maggior parte degli obiettivi erano in Irlanda, negli Stati Uniti e in Cina

L’impronta digitale dei dispositivi IoT

Dispositivi più comuni

Analizzando oltre mezzo miliardo di transazioni con dispositivi IoT, ThreatLabz ha identificato 553 diversi tipi di dispositivi di 212 produttori e li ha classificati in 21 categorie. Le tre categorie più comuni, che rappresentano quasi il 65% dei dispositivi totali, erano set-top box (29%), smart TV (20%) e smart watch (15%).

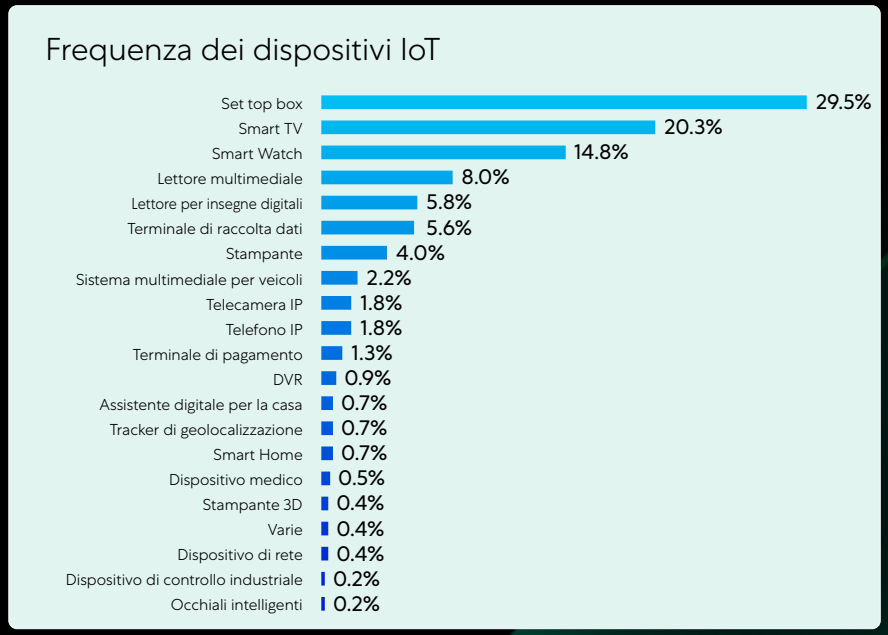
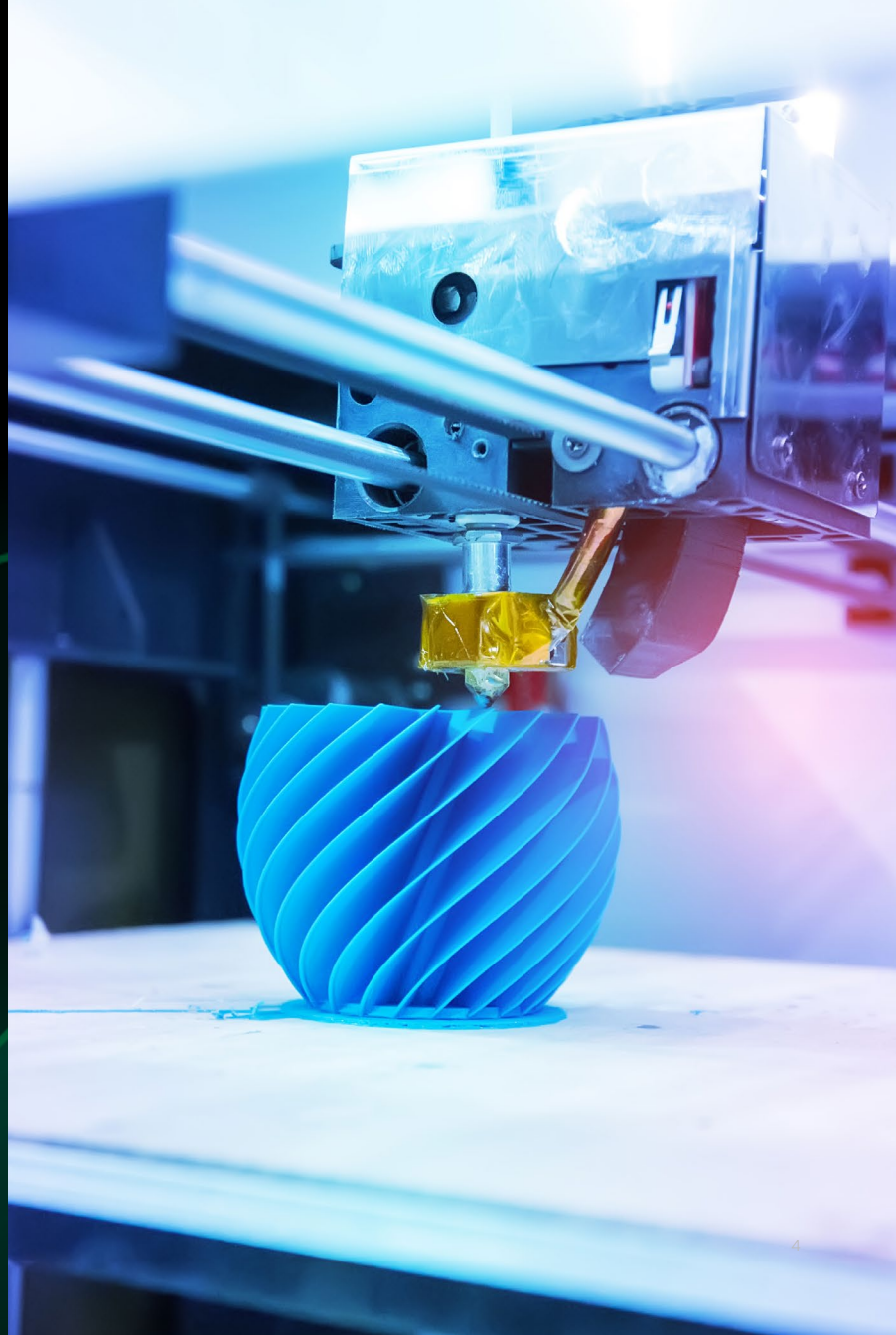


Figura 1: frequenza dei dispositivi IoT



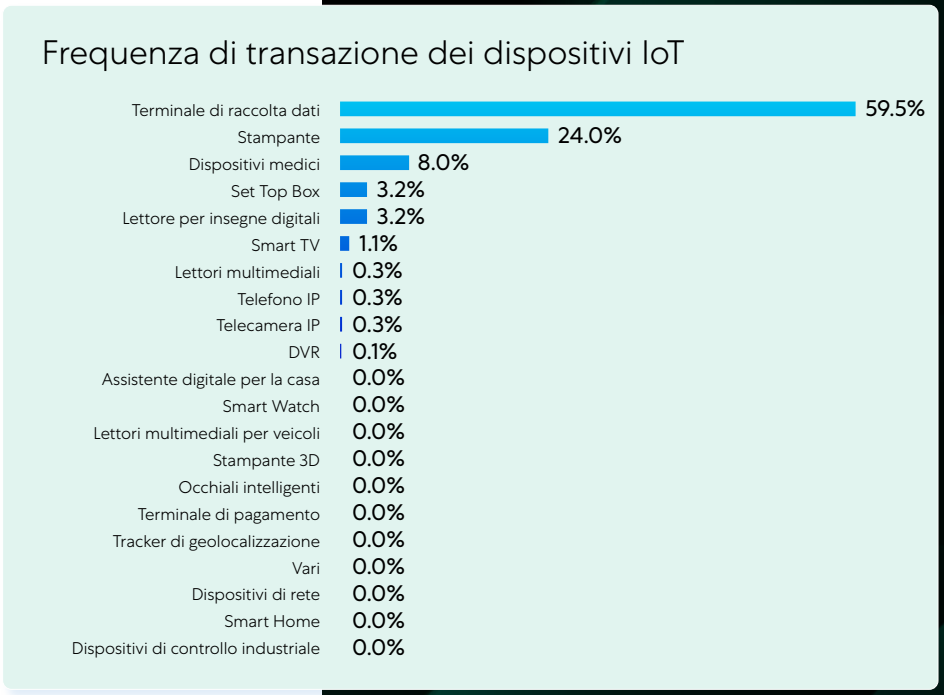
Internet nei dispositivi musicali?

L'Internet delle cose continua a espandersi in nuove categorie, alcune delle quali potrebbero essere completamente fuori dal radar dei team IT. ThreatLabz ha scoperto che si era connesso al cloud un certo numero di dispositivi imprevisti tra cui:

- **Frigoriferi intelligenti:** un frigorifero intelligente di Samsung è in grado di trasmettere musica, video e contenuti dal telefono del proprietario a uno schermo sullo sportello del frigorifero.
- **Lampada musicale:** Ikea e Sonos hanno creato una combinazione tra una lampada da tavolo e un lettore multimediale smart, chiamata Symfonisk.
- **Automobili:** si è scoperto che i lettori multimediali per auto di Tesla e Honda si connettono alle reti aziendali.
- **Schede di memoria Wi-Fi:** le schede di memoria Wi-Fi di Eye Fi, generalmente utilizzate nelle telecamere per archiviare e condividere foto, inviavano traffico attraverso il cloud di Zscaler.

I dispositivi più loquaci

Durante queste due settimane, le transazioni dei dispositivi IoT hanno rappresentato lo 0,038% delle transazioni totali sul cloud di Zscaler. Alcuni dispositivi hanno registrato molte più transazioni rispetto ad altri, con terminali di raccolta dati e stampanti che hanno rappresentato da soli oltre l'80% del traffico IoT totale, come illustrato nella Figura 2.



Base: 575.091.158 transazioni su dispositivi IoT
Figura 2: transazioni dei dispositivi IoT

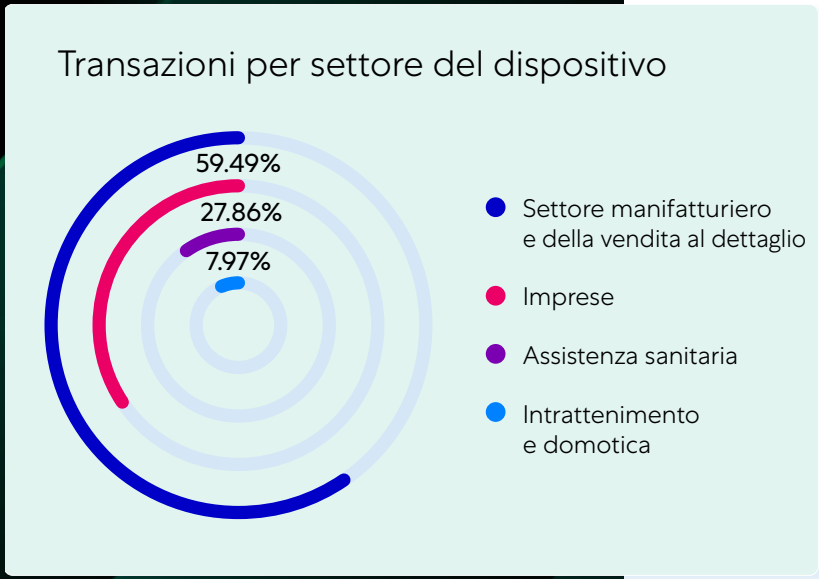


Figura 3: dispositivi IoT per tipo

Traffico per dispositivo: classificazione per settore

I dispositivi IoT sono stati ulteriormente raggruppati in quattro categorie in base ai relativi settori:

- **I dispositivi per il settore manifatturiero/vendita al dettaglio** rappresentavano il 59% delle transazioni e comprendevano 57 tipologie di 20 diversi produttori, nonché stampanti 3D, tracker di geolocalizzazione, dispositivi di controllo industriale, sistemi multimediali per veicoli, terminali di raccolta dati e terminali di pagamento.
- **I dispositivi aziendali** costituivano il 28% delle transazioni e comprendevano lettori per insegne digitali, videoregistratori digitali, telecamere IP e telefoni, stampanti e dispositivi di rete.
- **I dispositivi sanitari** rappresentavano l'8% delle transazioni e includevano una serie di dispositivi medici provenienti principalmente da tre produttori: GE Healthcare, Abbott Laboratories e HOLOGIC.
- **I dispositivi di intrattenimento e di domotica** infine costituivano il 4,2% delle transazioni generate da un'ampia varietà di dispositivi, come assistenti digitali per la casa, lettori multimediali, set-top box, occhiali intelligenti, dispositivi smart home, smart TV e smart watch. Pur rappresentando la percentuale più bassa di transazioni, questa categoria è la più variegata e comprende una serie di dispositivi elettronici di consumo, per un totale di 150 dispositivi di produttori diversi.

Per la maggior parte del tempo, i dispositivi IoT comunicano attraverso testo non crittografato

ThreatLabz ha osservato che il 76% delle transazioni totali provenienti dai dispositivi IoT si svolgeva su canali di testo non crittografato, con solo il 24% delle transazioni su canali crittografati sicuri. Anche se questo rapporto sembra inaccettabilmente basso, si tratta di un miglioramento di quasi 3 volte rispetto al nostro studio del 2019, in cui solo l'8,5 per cento delle comunicazioni IoT era crittografato. Tuttavia, il rischio per la sicurezza persiste: le comunicazioni in testo non crittografato sono molto più facili da spiare o, peggio, intercettare e modificare da parte degli aggressori, e questo consente di sfruttare i dispositivi IoT per scopi malevoli.

Tutti i 553 dispositivi osservati nello studio utilizzavano l'SSL in qualche misura, ma la percentuale di comunicazioni che in realtà era effettivamente criptata variava ampiamente in base al tipo di dispositivo. I dispositivi aziendali e di intrattenimento domestico comunicavano quasi interamente in modalità non crittografata, mentre i dispositivi sanitari comunicavano tramite SSL per circa la metà del tempo.

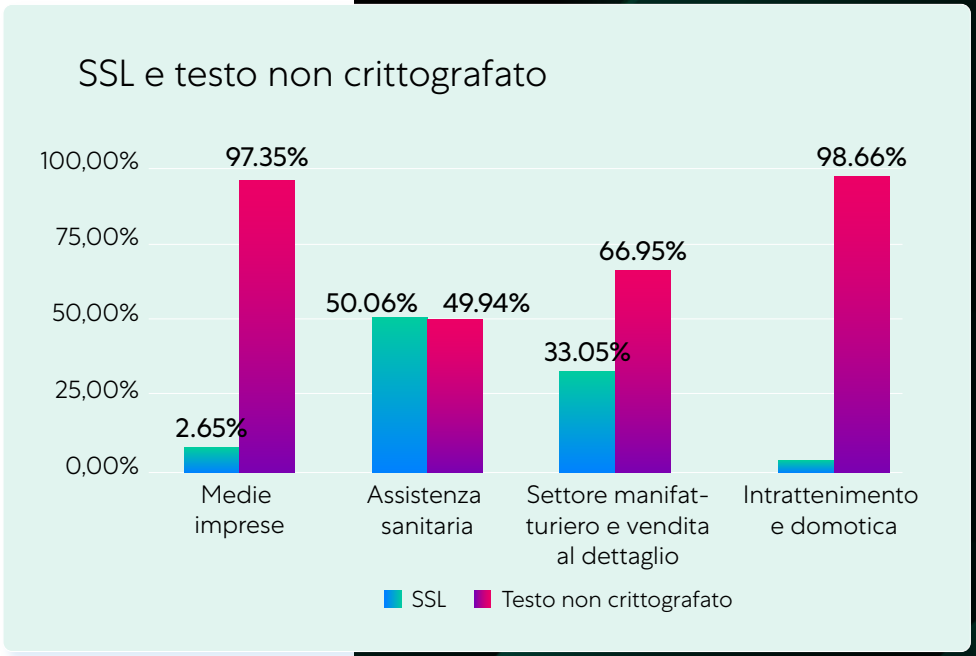


Figura 4: percentuale di comunicazioni crittografate per tipo di dispositivo

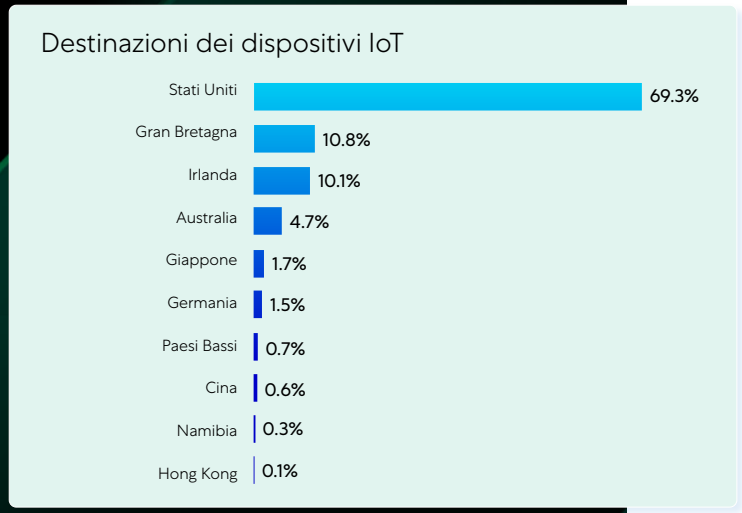


Figura 5: le principali destinazioni delle comunicazioni IoT

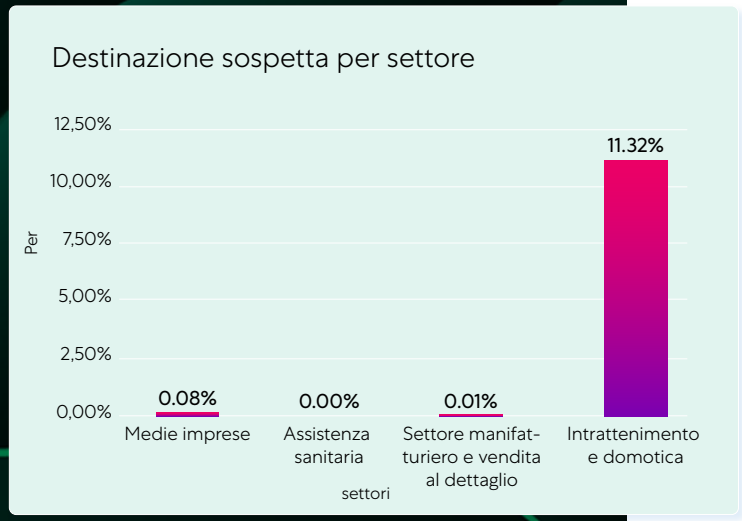


Figura 6: percentuale di traffico sospetto per tipo di dispositivo

Con quali Paesi comunicano i dispositivi IoT?

ThreatLabz ha esaminato i Paesi verso cui i dispositivi IoT instradavano i dati, denominati "destinazioni". La maggior parte di queste comunicazioni è legittima, con i dispositivi IoT che fanno ciò per cui sono progettati, ovvero inviare e ricevere dati. Gli Stati Uniti costituivano di gran lunga la destinazione principale, ricevendo il 69% del traffico, seguiti dalla Gran Bretagna (11%) e dall'Irlanda (10%). Di seguito, vengono mostrati i primi dieci Paesi di destinazione.

I dispositivi di intrattenimento e domotica tendono maggiormente a reindirizzare il traffico verso Cina e Russia

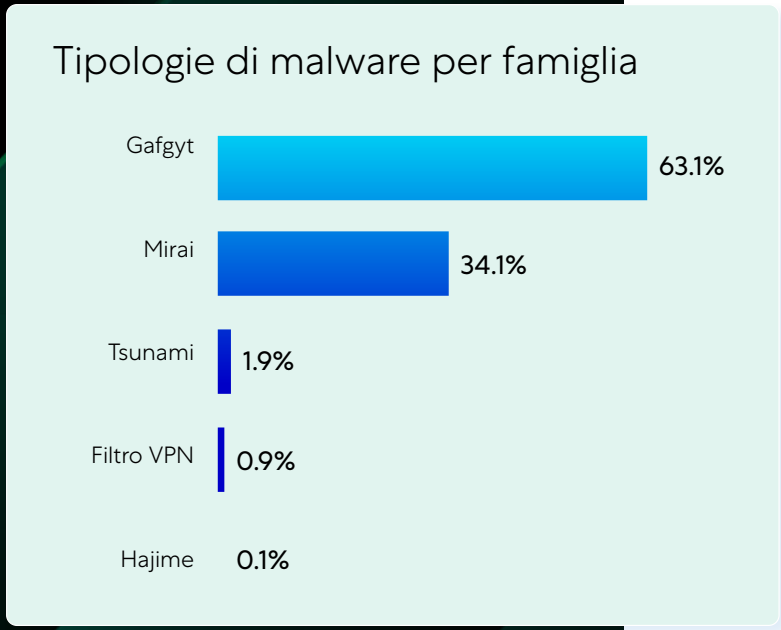
L'11% del traffico proveniente dall'intrattenimento e dai dispositivi di domotica era indirizzato verso Cina e Russia. Sebbene gran parte di questo traffico fosse legittimo e non dannoso, queste sono destinazioni che ThreatLabz ritiene sospette, a causa del loro alto tasso di spionaggio governativo e altre vulnerabilità informative. Quasi tutto questo traffico sospetto (99,9%) proviene da smart TV e set-top box.

Al contrario, meno dell'1% del traffico complessivo dei dispositivi progettati per i casi d'uso in aziende, nella sanità, nel settore manifatturiero e nella vendita al dettaglio era indirizzato verso destinazioni sospette.

Studio sui malware IoT

Durante le stesse due settimane in cui è stato svolto lo studio sulle impronte digitali IoT, ThreatLabz ha inoltre esaminato le attività specifiche correlate ai malware IoT nel cloud di Zscaler.

ThreatLabz ha osservato circa 300.000 transazioni bloccate a causa di malware IoT, exploit e comunicazioni C&C un aumento di quasi il 700% rispetto all'anno precedente. Nel volume di transazioni malware è stato osservato un totale di 18.000 host univoci e circa 900 diversi tipi di paylod o modus operandi in un periodo di 15 giorni.



Base: 900 diversi modi operandi
Figura 7: tipologie di malware per famiglia

Le principali minacce IoT

Le famiglie di malware Gafgyt e Mirai sono state di gran lunga le due famiglie di malware IoT più prolifiche nel nostro studio. Infatti, il 97% dei 900 diversi modi operandi osservati apparteneva a queste due famiglie. Altre attive includevano Tsunami, VPNFilter e Hajime.

Sebbene Gafgyt abbia registrato un maggior numero di modalità operative diverse, quelle legate al malware Mirai risultavano utilizzate più frequentemente negli attacchi IoT, durante il nostro studio. Guardando ai volumi delle transazioni, il 76% degli attacchi bloccati proveniva dalla famiglia di malware Mirai, il 5% da Gafgyt e il 19% da altre famiglie.

Botnet IoT
Gli exploit dei dispositivi IoT possono fornire agli aggressori l'accesso sia al dispositivo sia alle reti connesse, consentendo pertanto qualsiasi tipo di attività malevola. Mirai e Gafgyt sono particolarmente noti per la creazione di reti botnet di dispositivi sotto il controllo di un aggressore, che consentono attacchi coordinati su larga scala. Le botnet sono state utilizzate per attacchi DDoS (Distributed Denial-of-service), violazioni finanziarie, estrazione di criptovalute e intrusioni mirate, solo per citare alcune tipologie di attacco. La botnet di Mirai è nota per aver sferrato il maggior attacco DDoS della storia nel 2016, causando interruzioni di Internet diffuse. In questo studio sui malware, ThreatLabz ha valutato i tentativi di callback delle botnet scoprendo che portare a termine i loro attacchi gli aggressori miravano non solo i dispositivi IoT, ma anche a una serie di router e altri dispositivi di rete popolari:

I principali dispositivi di callback delle botnet	
CCTV e DVR di oltre 70 fornitori	DVR MVPower
Dispositivi multipli che utilizzano l'SDK Realtek con il daemon miniigd	Dispositivi Linksys
Huawei HG532	Dispositivi Netgear R7000/R6400
Router ZyXEL	Router Netgear DGN1000
Router Dasan GPON	Dispositivi D-Link
Router Eir D1000	Dispositivi Vacron NVR
Dispositivi D-Link	

I settori più colpiti

Le aziende operanti nel settore tecnologico hanno registrato il tasso più elevato di attacchi da malware IoT, pari al 40% delle infezioni. I settori più presi di mira sono stati quello manifatturiero (28%) e la vendita al dettaglio e all'ingrosso (24%).

Paesi da cui ha origine la maggior parte degli attacchi malware

Nel nostro studio, l'88,5% dei dispositivi IoT compromessi reindirizzava i dati ai server in uno di questi tre Paesi: Cina (56%), Stati Uniti (19%) o India (14%). Designati Paesi di "destinazione dei malware" e in ciascun caso consegnavano il malware direttamente o effettuavano la connessione ad esso dopo l'infezione. In realtà, poiché alcuni hacker configurano server C&C all'interno del Paese di destinazione, la posizione del server potrebbe non indicare necessariamente la sede effettiva dell'aggressore.

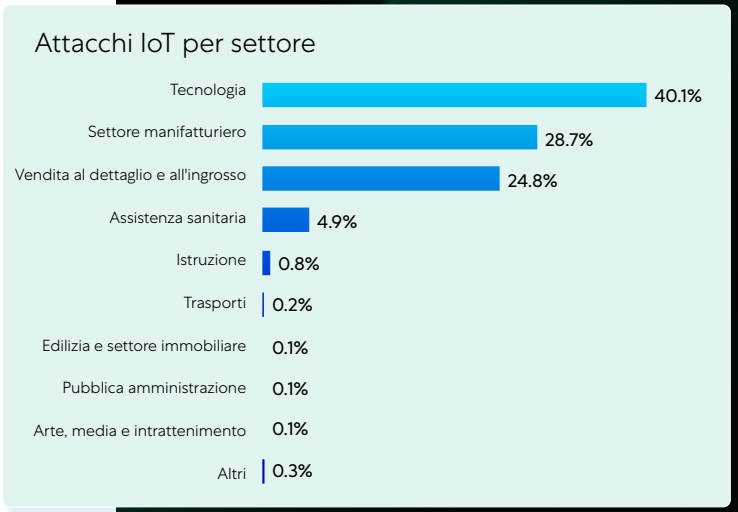


Figura 8: attacchi IoT per settore

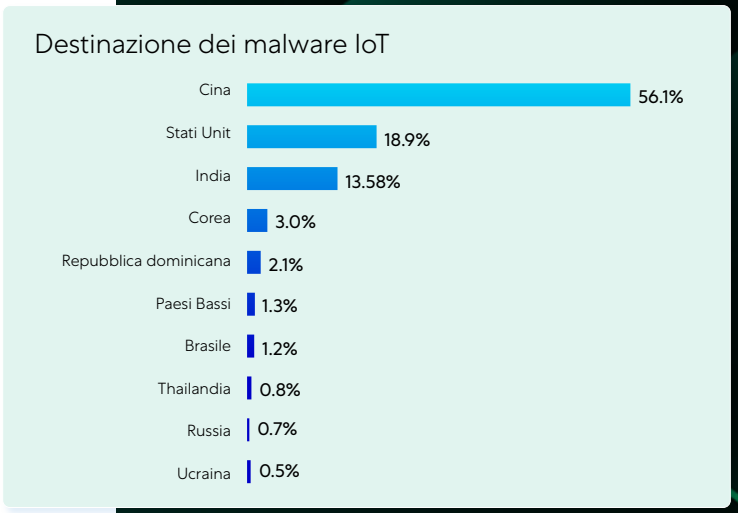


Figura 9: principali destinazioni malware IoT

Principali ASN degli autori delle minacce

Per una panoramica più approfondita sulle destinazioni malware, di seguito sono riportati i principali numeri di sistema autonomo (ASN) e gli indirizzi IP che, secondo quanto osservato da ThreatLabz, si sono collegati a malware IoT.

ASN	IP	Nome AS
16276	158.69.0.77	OVH, FR
398468	193.42.137.107	VMSNETWORKS, US
213035	193.239.147.144	SERVERION-AS Serverion B.V., NL
36352	107.173.125.167	AS-COLOCROSSING, US
202448	86.105.252.203	MVPS https://www.mvps.net, CY
46606	162.241.126.53	UNIFIEDLAYER-AS-1, US
53667	198.251.81.249	PONYNET, US
212953	46.102.106.25	MRS-BILISIM, TR
35913	45.15.143.175	DEDIPATH-LLC, US
213371	37.49.230.52	SQUITTER-NETWORKS, NL
35913	45.15.143.140	DEDIPATH-LLC, US
42864	45.95.169.218	GIGANET-HU GigaNet Internet Service Provider Co, HU
63916	103.42.214.181	IPTELECOM-AS-AP IPTELECOM Global, HK
134520	103.42.214.181	GIGSGIGSCLOUD-AS-AP GigsGigs Network Services, HK
3462	111.248.163.38	HINET Data Communication Business Group, TW
36352	107.173.181.189	AS-COLOCROSSING, US
36352	192.227.147.157	AS-COLOCROSSING, US
212369	45.155.125.116	TRDESERVER, TR
206898	185.172.110.205	BLADESERVERS, AU
213035	193.239.147.245	SERVERION-AS Serverion B.V., NL

Figura 10: i principali ASN degli autori delle minacce

Obiettivi principali dei malware IoT

ThreatLabz ha inoltre valutato i Paesi “bersaglio” dei malware in base all'indirizzo IP del client. Le prime tre nazioni vittime degli attacchi IoT sono risultate l'Irlanda (48%), gli Stati Uniti (32%) e la Cina (14%).

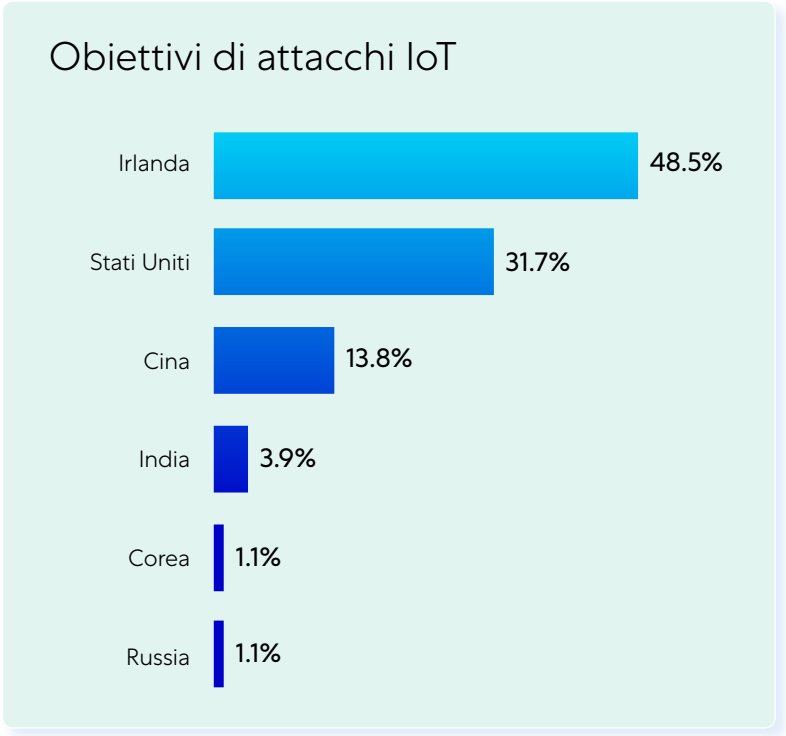


Figura 12: i principali Paesi bersaglio dei malware Iot

Fondamenti per difendersi dai malware IoT

Con il quotidiano incremento del numero di nuovi dispositivi intelligenti, impedirne l'accesso nei sistemi di un'organizzazione è diventato impossibile. L'unica arma è istituire politiche di accesso che impediscano a tali dispositivi di fungere da tramite ai dati e alle applicazioni sensibili.

Le seguenti best practice contribuiranno a mitigare la minaccia dei malware IoT, con dispositivi autorizzati o non autorizzati:

- **Monitorare e gestire i dispositivi di rete.** Molti dispositivi IoT non sono gestiti. Non è pertanto possibile basarsi su agenti endpoint per visualizzare i dispositivi in uso nelle sedi. È opportuno dunque: distribuire una soluzione per sorvegliare i registri di rete, per capire quali dispositivi stiano comunicando all'interno della rete e cosa fanno; implementare architetture che consentano di ispezionare il traffico di rete crittografato e non crittografato, alla ricerca di comunicazioni su eventuali dispositivi di non si è a conoscenza; quindi implementare delle misure di sicurezza.

- **Cambiare le password predefinite.** Sembra una storia antica quanto il mondo. Eppure, uno dei modi più semplici e comuni per gli aggressori di sfruttare i dispositivi è usare le password predefinite. Il controllo delle password può non avere alcun effetto sui dispositivi IoT non autorizzati, tuttavia costituisce un primo passo fondamentale per la distribuzione di dispositivi IoT di proprietà aziendale e dovrebbe essere parte della formazione sulla sicurezza per tutti i dipendenti che utilizzano dispositivi sul lavoro.

- **Essere sempre informati in merito a patch e aggiornamenti.** Molti settori, in particolare quello manifatturiero e sanitario, si affidano ai dispositivi IoT per i flussi di lavoro quotidiani. Per tali dispositivi autorizzati, è opportuno assicurarsi di essere sempre informati su eventuali nuove vulnerabilità rilevate e di mantenere la sicurezza del dispositivo sempre aggiornata attraverso le patch.

- **Implementare un'architettura di sicurezza Zero Trust.** È utile applicare policy rigorose per le risorse aziendali, in modo che utenti e dispositivi possano accedere solo a ciò di cui hanno bisogno e solo dopo l'autenticazione; limitare la comunicazione a IP, ASN e alle porte pertinenti necessarie per l'accesso esterno. I dispositivi IoT non autorizzati, che richiedono l'accesso a Internet, devono superare l'ispezione del traffico ed essere isolati da tutti i dati aziendali, idealmente tramite un proxy. L'unico modo per impedire ai dispositivi IoT di costituire una minaccia per le reti aziendali consiste nell'eliminare le policy che ne danno per scontata l'attendibilità e controllare invece rigorosamente l'accesso ai dati sensibili, utilizzando l'autenticazione dinamica basata sull'identità, nota anche come Zero Trust.

Informazioni su ThreatLabZ

ThreatLabz è il braccio di ricerca sulla sicurezza di Zscaler. Questo team di prim'ordine è responsabile della ricerca di nuove minacce e di garantire la protezione costante delle migliaia di organizzazioni che utilizzano la piattaforma globale Zscaler Zero Trust Exchange™. Oltre alla ricerca sui malware e all'analisi comportamentale, i membri del team sono coinvolti nella ricerca e nello sviluppo di nuovi moduli prototipo per una protezione avanzata dalle minacce sulla piattaforma Zscaler e conducono regolarmente controlli di sicurezza interni, per garantire che i prodotti Zscaler e l'infrastruttura soddisfino gli standard di conformità della sicurezza. ThreatLabz pubblica regolarmente analisi approfondite sulle minacce nuove ed emergenti sul suo portale, research.zscaler.com.

Informazioni su 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 dagli attacchi informatici e dalla perdita dei dati, grazie alla connessione sicura di utenti, dispositivi e applicazioni in qualsiasi luogo. Distribuita in più di 150 datacenter a livello globale, Zero Trust Exchange basata su SASE è la maggiore piattaforma di cloud security in linea del mondo. Scopri di più su **zscaler.com** o seguici su Twitter **@zscaler**.