Sicurezza dei Sistemi (id)IoT

Author : Daniele Rigitano

Date : 30 ottobre 2018

Il fenomeno della domotica “fai da te” ultimamente sta prendendo sempre più piede. Ormai è alquanto facile trovare elettrodomestici o piccoli dispositivi di uso comune che permettono la connessione alla rete interna della propria abitazione in modo da poter svolgere alcuni compiti “da remoto”.

Siamo partiti dalle Smart TV e dalle Smart Cam. Passando per le Smart Plug e le Smart Light, siamo giunti agli Smart Fridge, agli Smart Cooling, alle Smart Washing Machine.

Tutto questo “smart” e tutti questi inglesismi stando rendendo l’automazione, la domotica, uno *status simbol* del quale vantarsi.

Il solito reiterato errore che si fa al momento dell’acquisto di un qualsiasi dispositivo sta nel concentrarsi unicamente sul tipo di esperienza che questo è in grado di fornirci, o basare la nostra scelta in base al marchio di produzione perché lo prediligiamo ostinatamente rispetto alla concorrenza.

Si tende quindi a tralasciare del tutto la valutazione della qualità del supporto/assistenza che è in grado di fornire il produttore.

Ultimo ulteriore sbaglio che si compie con i dispositivi IoT è che una volta installati spesso ci si dimentica della loro esistenza (vedasi le smart cam di sorveglianza).

Il problema quindi sta **sempre** nel sottovalutare i problemi di sicurezza che possono scaturire a causa di un erroneo acquisto, installazione e configurazione di un dispositivo di rete IoT.

INTERESSE ALL’ATTACCO

Analizziamo le criticità dal punto di vista software: è estremamente raro che un utente medio si preoccupi di aggiornare periodicamente il software/firmware dei sistemi IoT installati nella propria abitazione.

È altresì vero che spesso i dispositivi messi in commercio con una data versione di firmware, vengano poi velocemente abbandonati dal produttore senza ricevere mai alcun aggiornamento di sicurezza.

C'è da sottolineare anche che per dispositivi *poco conosciuti*, è realisticamente raro che un utente malintenzionato perda tempo nello sviluppo di exploit in grado di colpire una manciata di vittime.

Naturalmente quanto detto non garantisce una protezione de facto: tali dispositivi garantiscono un'esposizione ad agenti malevoli pressoché totale, lasciando l'utenza esposta ad eventuali attacchi mirati.

Di contro, munirsi di dispositivi largamente utilizzati espone l'utenza ad altri pericoli e pensare che l'installazione delle patch di sicurezza garantisca una copertura totale da agenti malevoli è quantomeno ingenuo.

Basti considerare dispositivi perfettamente aggiornati, ma con errate impostazioni di configurazione/manutenzione. I danni risultanti da un eventuale attacco potrebbero essere catastrofici su scala mondiale.

LE NON VULNERABILITÀ

Quando si parla di IoT, la più grande ingenuità si compie nel momento in cui si mantiene la password di default del dispositivo. L'esempio lampante della gravità di tale azione è quanto avvenuto con la famosissima la BotNet Mirai.

Per compromettere i dispositivi IoT, la versione iniziale di Mirai faceva affidamento esclusivamente su un set fisso di 64 combinazioni predefinite di login/password note, comunemente utilizzate dai produttori di dispositivi IoT.

USER:	PASS:	USER:	PASS:
root	xc3511	admin1	password
root	vizxv	administrator	1234
root	admin	666666	666666
admin	admin	888888	888888
root	888888	ubnt	ubnt
root	xmhdipc	root	klv1234
root	default	root	Zte521
root	juantech	root	hi3518
root	123456	root	jvbzd
root	54321	root	anko
support	support	root	zlxx.
root	(none)	root	7ujMko0vizxv
admin	password	root	7ujMko0admin
root	root	root	system
root	12345	root	ikwb
user	user	root	dreambox
admin	(none)	root	user
root	pass	root	realtek
admin	admin1234	root	00000000
root	1111	admin	1111111
admin	smcadmin	admin	1234
admin	1111	admin	12345
root	666666	admin	54321
root	password	admin	123456
root	1234	admin	7ujMko0admin
root	klv123	admin	1234
Administrator	admin	admin	pass
service	service	admin	meinsm
supervisor	supervisor	tech	tech
guest	guest	mother	fucker
guest	12345		
guest	12345		

Come si può facilmente intendere, questo attacco molto poco tecnologico, si è rivelato estremamente efficace e ha portato alla compromissione di oltre 600.000 dispositivi in poco tempo.

Col tempo le tecniche di iniezione del codice Mirai si sono evolute. Una delle più ingegnose sfrutta una falla nella gestione dei protocolli di gestione remota TR-064 (obsoleto) e TR-069, serviti entrambi erroneamente tramite la porta 7547, aperta di default.

L’attacco prevede iniezione di codice arbitrario verso il protocollo TR-064 senza alcuna autenticazione, poiché in origine non era stato pensato per funzionare nella WAN. L’esecuzione di codice arbitrario ha portato a vari scenari, tra i quali:

- invio di specifici comandi che portano il dispositivo ad aprire la porta 80 per l’accesso alla console web di amministrazione. L’utenza e la password per l’accesso sono ottenute sempre tramite specifici comandi TR-064;
- nel caso il precedente metodo non andasse a buon fine, vi è il modo di forzare tramite crash di sistema il reset del dispositivo alle impostazioni di fabbrica, in modo da vedersi reimpostata l’utenza/password di default nota;

A questo punto diventa facile per l’hacker impadronirsi del dispositivo attaccato.

Un altro possibile *Point of Failure* che riguarda i dispositivi IoT diffusi su larga scala consiste nel rischio derivante dagli aggiornamenti automatici: il patching automatico può portare ad eventi molto rari, ma estremamente catastrofici.

Quando gli hacker compromettono il sito di un fornitore, hanno la possibilità di distribuire patch di sicurezza virate generate ad-hoc. È il caso di *notPetya*, l’evento più catastrofico mai visto su Internet, lanciato sovvertendo una patch automatizzata di software di contabilità.

Analizzando però più attentamente i fatti, Mirai non è conseguenza di bug accidentali, ma di errate decisioni prese consapevolmente. Stessa cosa vale per NotPetya: dopo la sua iniziale manifestazione, si è propagato sfruttando una vulnerabilità derivata da un’inopportuna configurazione della rete di Windows.

In altre parole, né Mirai, né NotPetya in realtà hanno sfruttato vulnerabilità imputabili ai dispositivi commercializzati, ma configurazioni errate definite dall’utente utilizzatore.

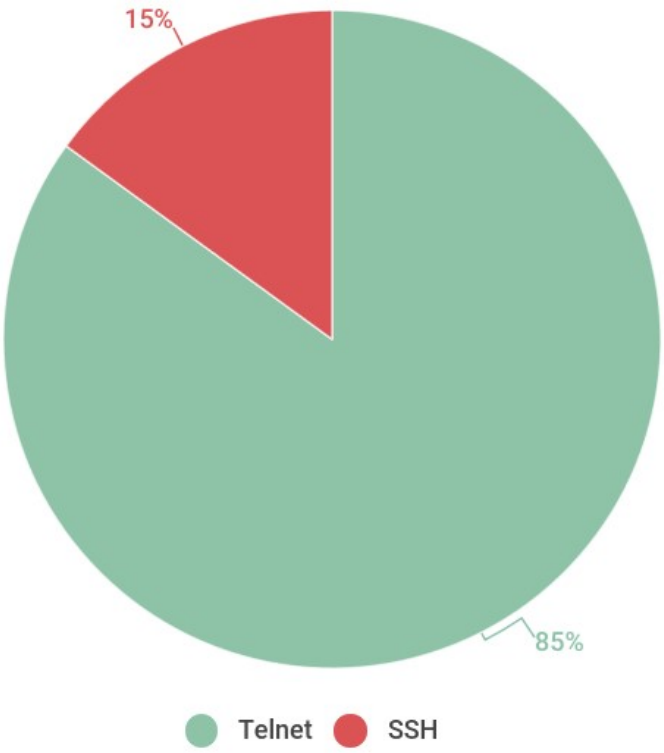
VITTIME PREFERITE

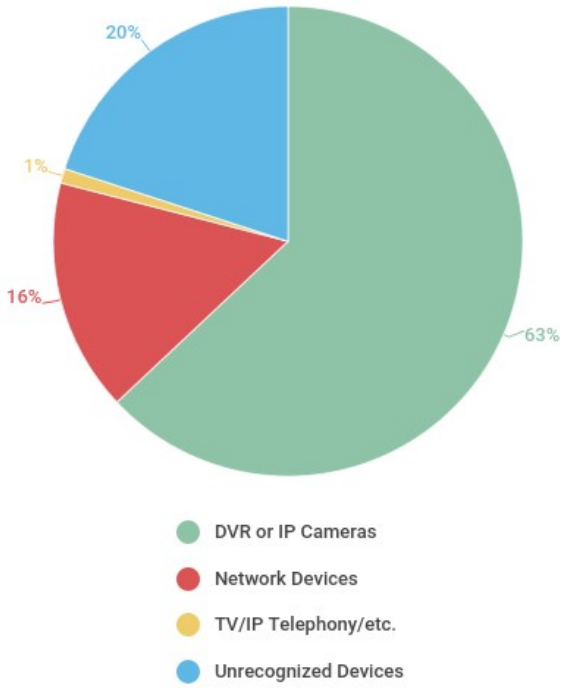
Secondo il report del primo quadrimestre 2018 di Kaspersky, i dispositivi più spesso violati rimangono i router. La restante parte di gadget IoT compromessi include una varietà di tecnologie diverse, come i dispositivi DVR, stampanti ed addirittura le lavatrici.

Le statistiche mostrano che il metodo più popolare di propagazione del malware dell'IoT è ancora l’attacco a *Forzatura Bruta* delle password, utilizzata nel 93% degli attacchi rilevati. Nella maggior parte dei casi rimanenti, l’accesso a un dispositivo IoT è stato acquisito utilizzando exploit ben noti.

Service	Port	% of attacks	Attack vector	Malware families
Telnet	23, 2323	82.26%	Bruteforce	Mirai, Gafgyt
SSH	22	11.51%	Bruteforce	Mirai, Gafgyt
Samba	445	2.78%	EternalBlue, EternalRed, CVE-2018-7445	–
tr-069	7547	0.77%	RCE in TR-069 implementation	Mirai, Hajime
HTTP	80	0.76%	Attempts to exploit vulnerabilities in a web server or crack an admin console password	–
winbox (RouterOS)	8291	0.71%	Used for RouterOS (MikroTik) authentication and WinBox-based attacks	Hajime
Mikrotik http	8080	0.23%	RCE in MikroTik RouterOS < 6.38.5 Chimay-Red	Hajime
MSSQL	1433	0.21%	Execution of arbitrary code for certain versions (2000, 2005, 2008); changing administrator password; data theft	–
GoAhead httpd	81	0.16%	RCE in GoAhead IP cameras	Persirai, Gafgyt
Mikrotik http	8081	0.15%	Chimay-Red	Hajime
Etherium JSON-RPC	8545	0.15%	Authorization bypass (CVE-2017-12113)	–
RDP	3389	0.12%	Bruteforce	–
XionMai uc-httpd	8000	0.09%	Buffer overflow (CVE-2018-10088) in XionMai uc-httpd 1.0.0 (some Chinese-made devices)	Satori
MySQL	3306	0.08%	Execution of arbitrary code for certain versions (2000, 2005, 2008); changing administrator password; data theft	–

Il compito di questi ultimi viene poi ulteriormente agevolato dal fatto che una significativa parte dei dispositivi “intelligenti” comunica con l’esterno tramite le porte Telnet e/o SSH.





COSA FARE?

Sembrerebbe quindi non esservi una soluzione semplice al problema, ma esaminando più attentamente i fatti ci si rendere conto che delle contromisure sono sempre attuabili.

Di seguito alcune buone pratiche da intraprendere per limitare l'esposizione agli attacchi.

Dovrebbe essere prassi l'acquisto di dispositivi provenienti da produttori che garantiscano un buon periodo di longevità del supporto, in modo da assicurare la costante correzione dei bug che possono verificarsi nel tempo.

Le patch di sicurezza dovrebbero essere preferibilmente installate in maniera manuale, per evitare quanto detto nei paragrafi precedenti, previa verifica sul sito del produttore della bontà del software rilasciato.

Le password pre-configurate vanno immediatamente sostituite appena si installa un nuovo dispositivo. L'utilizzo di password complicate che includano lettere maiuscole, minuscole, numeri e simboli è preferibile.

- Se il dispositivo è provvisto di una password standard che non può essere modificata, oppure di un account predefinito che non può essere disattivato, disabilitate i servizi di rete in cui vengono utilizzati tali elementi, oppure impedite l'accesso alla rete dall'esterno relativamente ai servizi in causa.
- I dispositivi non sicuri, inoltre, finiscono su Shodan, un motore di ricerca che aiuta i

malintenzionati a cercare gli oggetti dell’Internet of Things senza password.

A meno che non si riveli necessario per l’utilizzo stesso del dispositivo, è consigliabile inibire l’accesso a quest’ultimo da reti esterne (WAN);

Infine, disattivare tutti i servizi di rete non necessari per l’utilizzazione del dispositivo, con particolare attenzione alle porte Telnet, SSH, SAMBA, TR-069, ove non necessario, permette un isolamento migliore della propria rete.

Articolo a cura di **Daniele Rigitano**