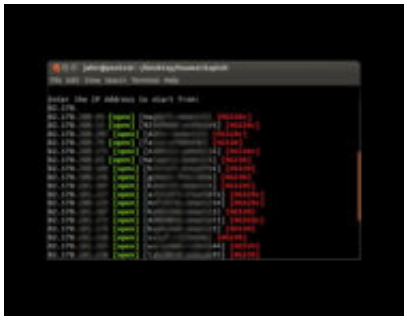
Exploit IoT: l'analisi degli ultimi 120 giorni. Il 94% del traffico degli attacchi è legato all’exploit Huawei Router

Author : Redazione

Date : 28 Febbraio 2019



Le botnet dell’Internet of Things si propagano il più delle volte sfruttando le vulnerabilità dei dispositivi IoT. La telemisurazione degli honeypot IoT di NETSCOUT mostra come il numero di tentativi di exploit originati da bot sia in continua crescita. Le vulnerabilità sfruttate sono vecchie ma di certo non obsolete: l'exploit più visto meglio honeypot è stato diffuso per la prima volta più di quattro anni fa. Inoltre, i tentativi di exploit mostrano come alcuni Paesi abbiano una maggior affinità per determinati tipi di dispositivi.

- I dati raccolti mostrano attacchi indirizzati a vulnerabilità ben note dei dispositivi IoT. Nel mese di Gennaio 2019 il numero di tentativi di exploit è raddoppiato rispetto al Dicembre 2018;
- Il CVE-2014-8361 è in cima alla lista degli exploit IoT che hanno colpito gli honeypot negli ultimi quattro mesi. Il vettore di exploit, rivelato pubblicamente nell’Aprile del 2015, rimanda a botnet IoT di alto profilo come Satori e JenX;
- Sulla base della telemisurazione degli honeypot, è possibile ottenere una panoramica unica della dispersione geografica delle vulnerabilità IoT e dei tentativi di sfruttarle.

Osservando i dati degli ultimi quattro mesi, si è assistito ad un’ondata di attacchi legati all’exploit di Hadoop Yarn descritto in Mirai: l’obiettivo non è più soltanto l’Internet of Things. Disgregando i voluminosi attacchi Yarn, emerge un modello di exploit comunemente usato per prendere di mira dispositivi IoT.

I dati mostrano che gli assalti ai dispositivi IoT avvengono mediante l’uso di un’ampia gamma di exploit, vecchi e nuovi. Un exploit IoT può, infatti, continuare a svolgere la propria funzione per anni, e il CVE-2014-8361 ne è un chiaro esempio.

Alcuni Paesi sono più propensi a sfruttare determinate vulnerabilità. Si può osservare, ad esempio, come gli exploit provenienti dal Regno Unito tendano a favorire l’uso dell’exploit Realtek SDK Miniigd Command Execution (CVE-2014-8361). Ancora, è possibile contare un totale di sole 10 fonti impiegate per questi attacchi. Ciò potrebbe indicare che i 10 indirizzi IP di

origine si trovano nella stessa botnet.

A differenza degli exploit Miniigd e Huawei Router, l'uso dell'epxloit D-Link Devices HNAP Command Execution è stato osservato in diversi Paesi. Esaminando il payload di questi attacchi, è possibile capire se l'exploit è sfruttato da una o più botnet.

Spostando l'obiettivo verso una panoramica dei dati degli ultimi 120 giorni, ne emerge un'immagine differente. Il 94% del traffico degli attacchi in questo intervallo di tempo è legato all'exploit Huawei Router.

Confrontando il numero di attacchi per questo specifico exploit tra Dicembre 2018 e Gennaio 2019, si assiste ad un aumento del 218%. Sempre più botnet sono alla ricerca di queste vulnerabilità con l'obiettivo di sfruttarle. I payload di questi attacchi mostrano che la maggior parte dei malware impiegati sono varianti di Mirai, dimostrando così che quest'ultimo ha ancora qualche asso nella manica.

Mentre i bot IoT che sfruttano nomi utente e password predefiniti tendono ad adottare un approccio di propagazione più casuale, i bot che usano gli exploit sono generalmente più orientati per Paese. Poiché i fornitori si servono di password predefinite o codificate per risolvere determinati problemi, i bot IoT devono adattarsi a questo panorama in continua evoluzione. Gli operatori di botnet IoT si stanno evolvendo per adeguarsi ai cambiamenti nella sicurezza dei dispositivi, adottando sempre di più un approccio che si potrebbe definire "ibrido".

"In qualità di operatori della sicurezza, siamo in grado di imparare dalle tattiche degli aggressori e di capire quali dispositivi tendono ad essere presi di mira nell'area di interesse, al fine di difenderli meglio. Patch, test, monitoraggio e risposta agli incidenti sono elementi essenziali della protezione dell'IoT, che non può mancare nel programma di sicurezza di un'Azienda." ha commentato **Ivan Straniero**, Regional Manager, Southern & Eastern Europe di **NETSCOUT**.

A cura della redazione