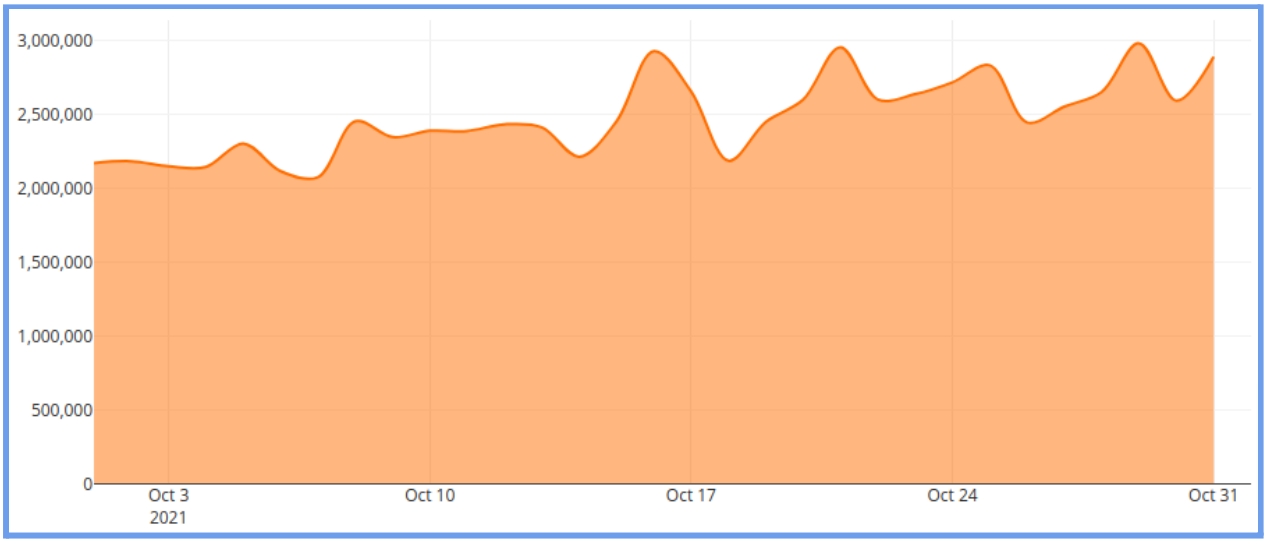
Reporte de actividad del proyecto

Despliegue de un IoT honeypot en América Latina y el Caribe

Octubre 2021

Gracias a la capacidad de extracción de datos para la generación de reportes, se pueden reportar para este mes los siguientes resultados.

Actividad de registro de datos en el sistema



Los días 16, 21 y 29 hubo picos de actividad que llegaron a cerca de los 3 millones de mensajes procesados, manteniéndose normalmente en un promedio cercano a los 2 millones y medio. El día 7 fue el de más baja actividad, con poco más de 2 millones de mensajes. Todo responde a un comportamiento normal.

Totales de mensajes y direcciones IP origen

Mensajes procesados:	Direcciones IP de origen:
76,850,364	667,867

Durante el mes se procesaron cerca de 77 millones de mensajes provenientes del proyecto de sensores, algo más de 8 millones más que el mes anterior. Originados de casi 668 mil direcciones IP de origen distintas, alrededor del mundo, unas 48 mil más en relación al mes anterior. Más abajo se desglosan estos orígenes por países.

Productos: Fabricantes y tipos más accedidos

Fabricante	Producto	Tipo	Eventos
Realtek	Realtek SDK	embedded-system	162885

Fortinet	FortiOS	firewall	113595
Huawei	Huawei Home Gateway HG532	router	80078
MVPower	MVPower DVR	video-system	36125
Microsoft	Exchange	email	21916
D-Link	D-Link DIR-645, DAP-1522 revB, DAP-1650 revB, DIR-880L, DIR-865L, DIR-860L revA, DIR-860L revB DIR-815 revB, DIR-300 revB, DIR-600 revB, DIR-645, TEW-751DR, TEW-733GR	router	16163
	DNS-320	nas	1
Dasan	Dasan GPON Home Router	router	8576
Oracle	WebLogic Server	app-server	4410
	Oracle Weblogic Server	app-server	2452
MobileIron	MobileIron Mobile Device Management (MDM)	device-management-platform	3989
Zyxel	Eir D1000	router	3862
Realtek	Realtek SDK	embedded-system	162885

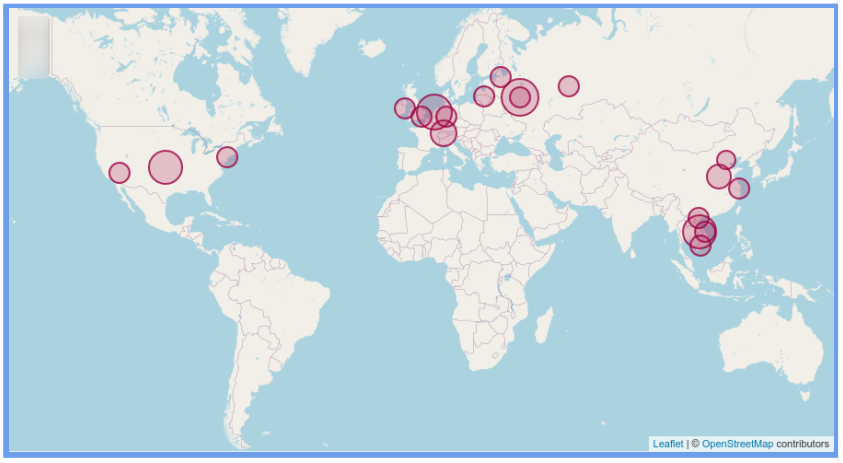
En el período, el sistema más asediado fue el sistema embebido Realtek SDK. Le sigue el firewall de Fortinet y en tercer lugar, el gateway de hogar huawei HG532, aunque no tan detrás está está el sistema de video de MVPower.

Países de origen de conexiones

Tabla de conexiones por país:

País	Conexiones
US	14493291
RU	12297496
VN	9447902
NL	8066249
CN	6239703
CH	3350202
DE	2936623
GB	1338704
LT	1296272
IE	1120146
IN	1025490

Representación Geográfica de orígenes:



Algo más del 21% de las conexiones provinieron de EEUU, un 17% más que las de Rusia, siendo estos dos los que en total abarcan prácticamente el 40% de las conexiones tabuladas. Vietnam está

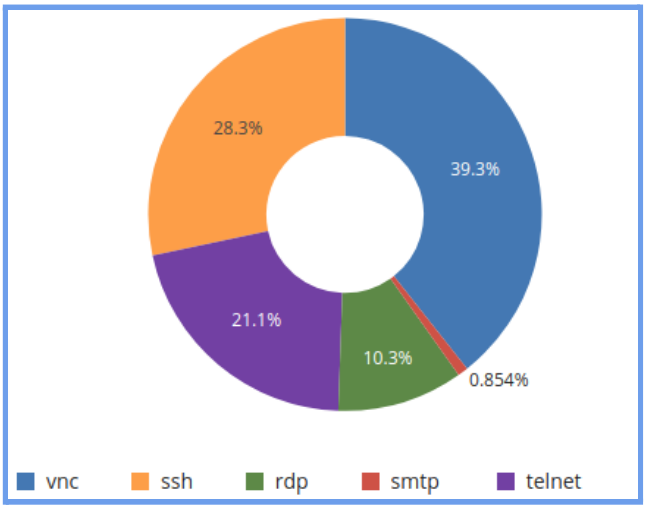
BR	949553
KR	853518
EE	751650
AU	698312
PL	672980
HK	666456
FR	552193
MD	532535
BG	520608

cerca de Rusia con poco más del 14% y le siguen los Países Bajos con casi el 12%.
En LAC, Brasil destaca con el 1.40%, siendo el único de LAC este mes.

💡 Es de notar que en el mapa no se representan todos los países de la lista tabulada, pues algunos países, como Estados Unidos, tienen geográficamente más de una ubicación (Ciudad) de origen, por lo que en el mapa se grafican sólo las 20 principales ubicaciones, no necesariamente consolidadas por país, que es lo que justamente se tabula a la izquierda.

Protocolos más accedidos

De las conexiones registradas, los protocolos que más se usan para acceder a los sistemas, son los representados en la siguiente imagen.



Cabe indicar que sólo se grafican los 5 primeros, pues a partir del 6to en adelante los valores realmente son muy pequeños, considerando que el propio protocolo SMTP en la gráfica (5to en presencia) sólo tiene un 0,85% de ocurrencia.

Usuarios y contraseñas más usados

Finalmente se presenta el top 20 de usuarios y contraseñas más comúnmente usados para acceder a los sistemas emulados por los distintos sistemas de honeypot en los diferentes sensores de la red:

Usuario	Ocurrencias	Porcentaje	Contraseña	Ocurrencias	Porcentaje
`root`	1149698	76.02 %	`admin`	41086	12.00 %
`admin`	180415	11.93 %	`123456`	31641	9.24 %
`user`	34485	2.28 %	`1234`	30323	8.86 %

default	24249	1.60 %	password	26717	7.80 %
guest	22617	1.50 %	root	25569	7.47 %
hadoop	17890	1.18 %	12345	25249	7.37 %
test	12199	0.81 %	default	16737	4.89 %
support	11989	0.79 %	user	14334	4.19 %
administrator	6869	0.45 %	1111	13859	4.05 %
Admin	6636	0.44 %	vizxv	12808	3.74 %
ubnt	6439	0.43 %	pass	11930	3.48 %
supervisor	5976	0.40 %	solokey	11657	3.40 %
postgres	5063	0.33 %	1	11497	3.36 %
service	4991	0.33 %	xc3511	10773	3.15 %
ftp	4423	0.29 %	666666	10641	3.11 %
oracle	4093	0.27 %	5up	9986	2.92 %
www	3991	0.26 %	7ujMko0admin	9962	2.91 %
tech	3699	0.24 %	1234567890	9926	2.90 %
admin1	3409	0.23 %	support	8948	2.61 %
Administrator	3302	0.22 %	zlxx.	8792	2.57 %