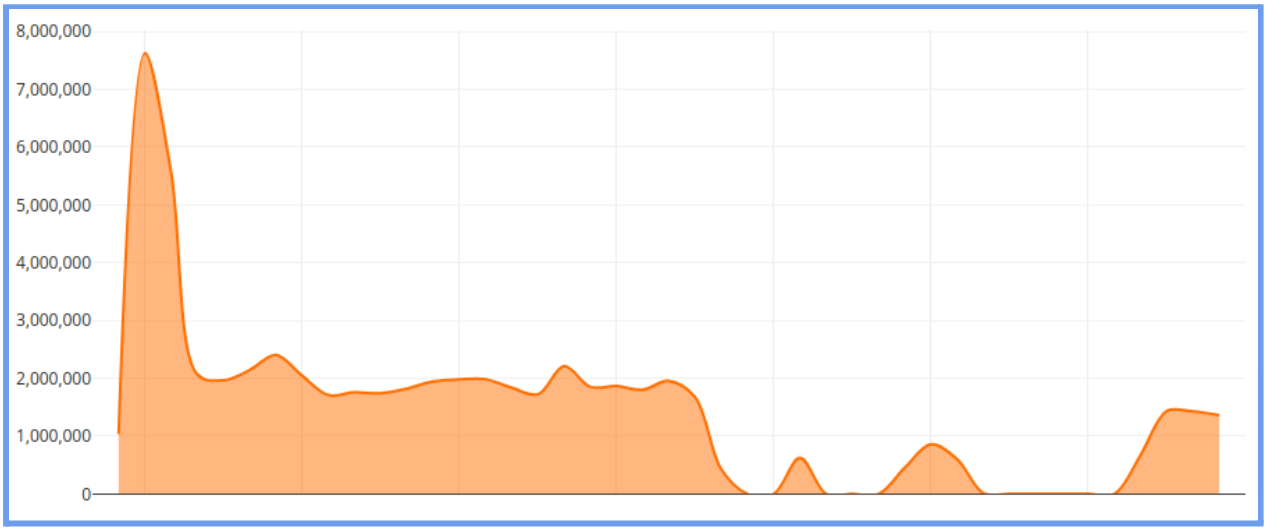
Reporte de actividad del proyecto

Despliegue de un IoT honeypot en América Latina y el Caribe

Junio 2021

Desde este mes, se ha podido desarrollar la capacidad de extracción de datos para la generación de reportes. Hay una enorme cantidad de campos generados de la actividad del proyecto que se están recolectando en un equipo que los almacena en Elasticsearch, pero hemos escogido un conjunto de campos que pueden ser relevantes para este informe y los subsecuentes que a partir de hoy se generarán de forma mensual.

Actividad de registro de datos en el sistema



A inicios de mes hubo un pico de actividad que se acercó a los 8 millones de mensajes procesados, manteniéndose luego en un promedio de aproximadamente 2 millones. Este mes de junio tuvimos algunos inconvenientes con el sistema de procesamiento, al incrementarse el número de colaboradores a quienes les remitimos la data completa de sus sensores. Tomó un tiempo estabilizar el sistema con una combinación de mejoras de recursos y tuning para aprovecharlos.

Totales de mensajes y direcciones IP origen

Mensajes procesados:	Direcciones IP de origen:
60,584,399	406,410

Durante el mes se procesaron algo más de 60 millones y medio de mensajes provenientes del proyecto de sensores. Originados de poco más de 400 mil direcciones IP de origen distintas, alrededor del mundo. Más abajo se desglosan estos orígenes por países.

Productos: Fabricantes y tipos más accedidos

Fabricante	Producto	Tipo	Eventos
Microsoft	Exchange	email	20759
MVPower	MVPower DVR	video-system	14833
Fortinet	FortiOS	firewall	7875
Dasan	Dasan GPON Home Router	router	7732
	Dasan GPON ONT WiFi Router H640X	router	1
Realtek	Realtek SDK	embedded-system	7611
Huawei	Huawei Home Gateway HG532	router	7173
Oracle	WebLogic Server	app-server	2343
	Oracle Weblogic Server	app-server	1989
Zyxel	Eir D1000	router	2456
Netgear	Netgear DGN1000	router	2051
	NETGEAR R/D Series Routers	router	290
MobileIron	MobileIron Mobile Device Management (MDM)	device-management-platform	2323

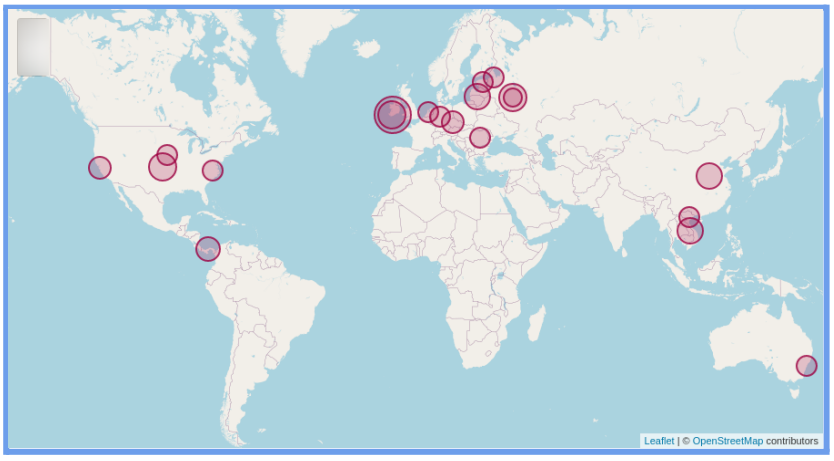
En el período, el sistema más asediado fue el servidor de correo Exchange, con algo más del 26% del total tabulado. Con casi el 20% el sistema de grabación de video (DVR) MVPower y en tercer lugar, con poco más del 10%, el firewall de Fortinet, aunque le siguen muy de cerca el ruteador de hogares de marca Dasan y el sistema embebido de Realtek.

Países de origen de conexiones

Tabla de conexiones por país:

País	Conexiones
IE	10555281
US	10492123
RU	5970001
VN	5024979
CN	4599612
LT	2623637
PA	2420183
NL	1791256
CZ	1595045
DE	1586507

Representación Geográfica de orígenes:



Poco más del 19% de las conexiones provinieron de Irlanda, con un valor muy cercano al de Estados Unidos, siendo estos dos los que en

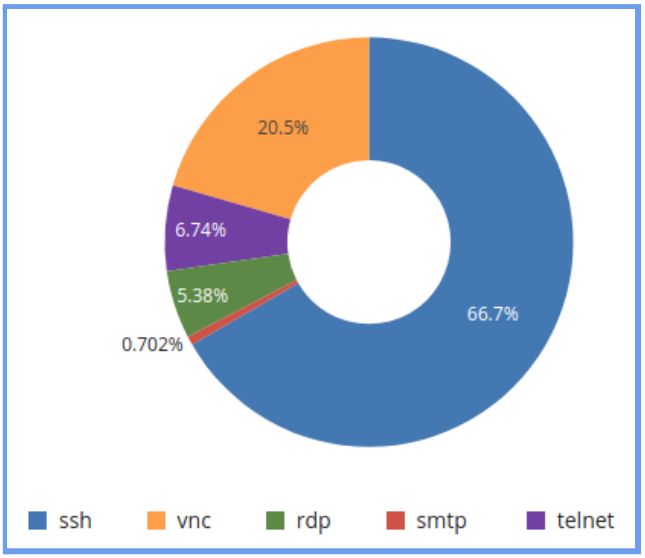
KR	1332320
IN	1089632
GB	1010304
EE	883927
AU	853012
RO	728382
BR	678233
FR	569454
HK	548271
SG	481642

total abarcan poco más del 38% de las conexiones tabuladas. Les siguen Rusia y Vietnam con casi el 11% y poco más del 9% respectivamente. China se acerca al 8.5%.
En LAC, Panamá destaca con cerca el 4.41%, siguiéndole Brasil con el 1.24%.

💡 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 0,7% 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`	983346	74.53 %	`123456`	41048	12.12 %
`admin`	106348	8.06 %	`password`	36773	10.86 %

user	27083	2.05 %	1234	33187	9.80 %
default	26818	2.03 %	admin	32944	9.73 %
support	18587	1.41 %	12345	28274	8.35 %
test	18479	1.40 %	root	19502	5.76 %
guest	17812	1.35 %	123	17125	5.06 %
administrator	13833	1.05 %	1	16546	4.89 %
ubnt	12712	0.96 %	default	11969	3.53 %
admin1	11831	0.90 %	12345678	11739	3.47 %
web	11314	0.86 %	test	11430	3.37 %
tech	10484	0.79 %	qwerty	11189	3.30 %
user1	10479	0.79 %	123456789	11148	3.29 %
MikroTik	9599	0.73 %	1234567	9218	2.72 %
demo	9477	0.72 %	pass	8580	2.53 %
profile1	9398	0.71 %	admin123	8568	2.53 %
telecomadmin	8511	0.65 %	88888888	7659	2.26 %
postgres	4453	0.34 %	support	7367	2.18 %
oracle	4395	0.33 %	user	7247	2.14 %
supervisor	4376	0.33 %	passw0rd	7163	2.12 %