

lacnic 30
lacnog 2021
11-15 de Octubre de 2021



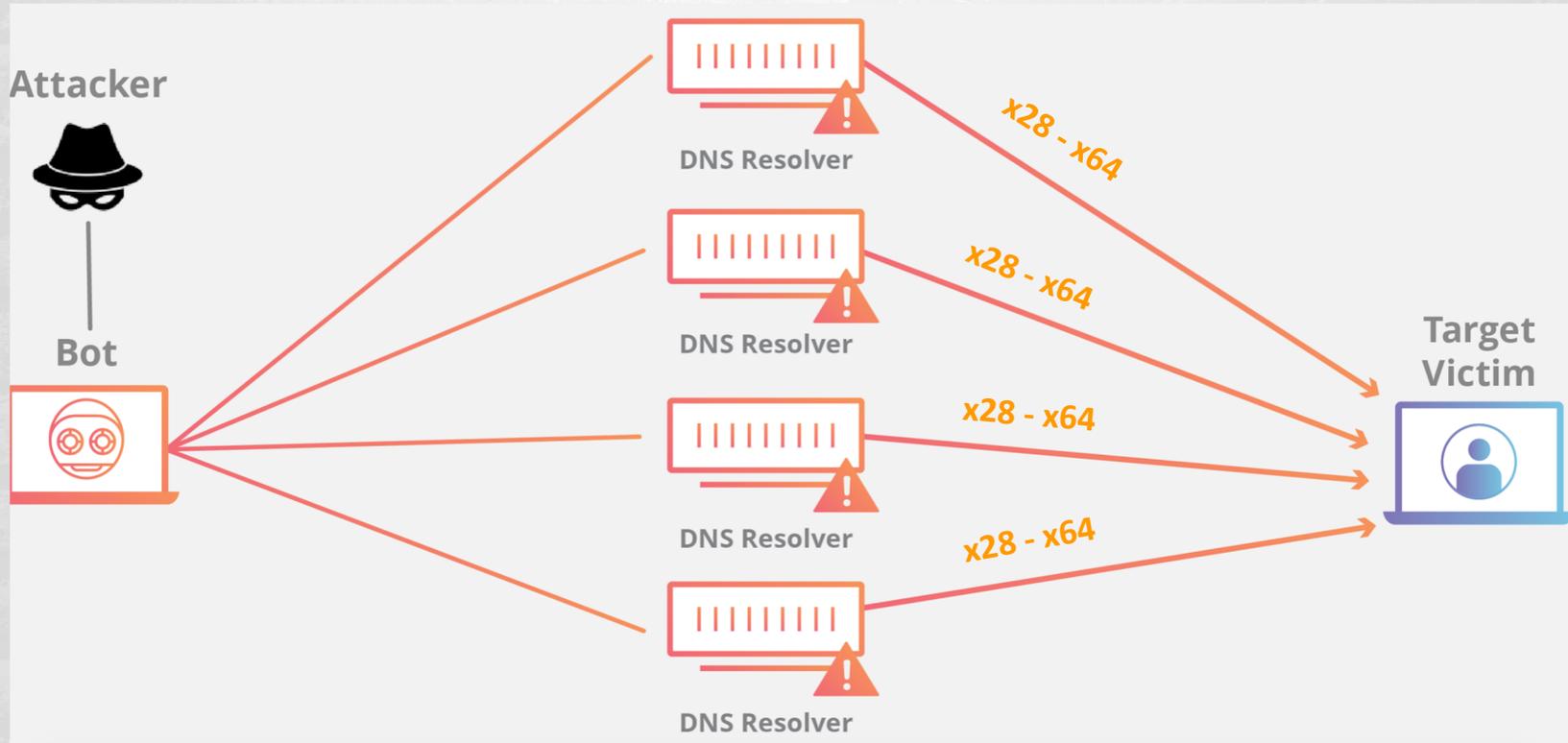
Estudio de protocolos que posibilitan ataques DDoS en la región

Guillermo Pereyra
gpereyra at lacnic.net

AGENDA

- Ataques DDoS por amplificación
- Protocolos que amplifican respuestas
- Proyecto
- Resultados preliminares

ATAQUES DE AMPLIFICACIÓN



PROTOCOLOS QUE AMPLIFICAN RESPUESTA

Protocol	Bandwidth Amplification Factor	Vulnerable Command
DNS	28 to 54	see: TA13-088A [4]
NTP	556.9	see: TA14-013A [5]
SNMPv2	6.3	GetBulk request
NetBIOS	3.8	Name resolution
SSDP	30.8	SEARCH request
CharGEN	358.8	Character generation request
QOTD	140.3	Quote request
BitTorrent	3.8	File search
Kad	16.3	Peer list exchange
Quake Network Protocol	63.9	Server info exchange
Steam Protocol	5.5	Server info exchange
Multicast DNS (mDNS)	2 to 10	Unicast query
RIPv1	131.24	Malformed request
Portmap (RPCbind)	7 to 28	Malformed request
LDAP	46 to 55	Malformed request [6]
CLDAP [7 [†]]	56 to 70	—
TFTP [23 [†]]	60	—
Memcached [25]	10,000 to 51,000	—
WS-Discovery	10 to 500	—

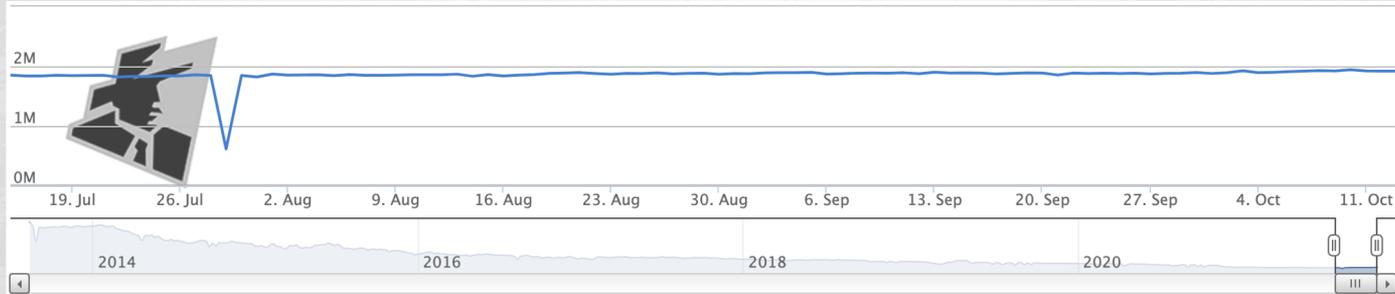
OBJETIVO DEL PROYECTO

Mejorar los niveles de seguridad de los sistemas que utilizan recursos IP de la región que administra LACNIC, para colaborar con la estabilidad y resiliencia de Internet minimizando el posible uso de los mismos en ataques DDoS.

ACCIONES REALIZADAS

- Identificación de los sistemas que exponen estos protocolos abiertos en la región
- Alertar a los afectados
 - Correo electrónico con recomendaciones
 - Reuniones en conjunto para colaborar en la solución del problema

ESTADÍSTICAS PÚBLICAS - DNS



Americas	266116	269669	-1.32%	
Caribbean	5238	5191	0.89%	
Central America	19122	19229	-0.56%	
Northern America	148813	149265	-0.30%	
South America	92943	95982	-3.17%	

ESTADÍSTICAS PÚBLICAS - SSDP

Top 20 Countries With Open SSDP

Country	Total
Korea, Republic of	438,638
Venezuela	182,072
China	170,868
Taiwan	113,435
United States	90,769
Brazil	85,189
Japan	58,414
Russian Federation	43,412
Vietnam	34,149
India	33,431
Chile	30,340
Ukraine	29,153
Canada	25,875
Argentina	25,452
Romania	22,679
Hong Kong	19,282
Colombia	18,790
Italy	18,459
Kazakhstan	17,692
Spain	15,527

ESTADÍSTICAS PÚBLICAS - CHARGEN

Country	Total
Korea, Republic of	10,350
United Arab Emirates	4,213
China	2,236
Italy	1,936
United States	1,549
Russian Federation	700
Taiwan	610
Germany	592
India	440
Serbia	388
Japan	310
Brazil	305
Mexico	249
Thailand	221
Philippines	220
France	189
Canada	182
Poland	153
Chile	115
-	114

Antes del 28/9

Country	Total
Korea, Republic of	15,739
United Arab Emirates	4,212
China	2,100
Italy	1,914
United States	1,556
Russian Federation	715
Taiwan	629
Germany	575
India	419
Serbia	403
Japan	304
Brazil	301
Mexico	250
Thailand	227
Philippines	227
France	190
Canada	178
Poland	162
Spain	111
-	109

Después del 28/9

GRACIAS!!

csirt at lacnic.net