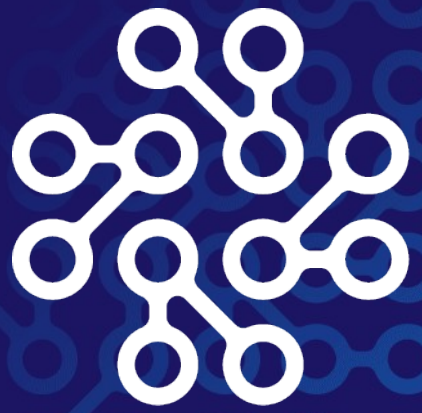


LAC4

Latin America and Caribbean Cyber Competence Centre

Funded by the European Union

PRESIDENCIA DE LA
REPÚBLICA DOMINICANA
MINISTERIO
DE LA PRESIDENCIA

CNCS CENTRO NACIONAL DE CIBERSEGURIDAD
REPÚBLICA DOMINICANA

✣❊❁❄❒ ✣❙❒❑▲❊❋❊➛➝■

República Dominicana

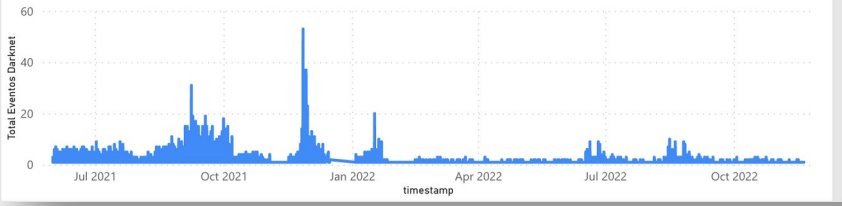
Indicadores de Ciber exposición

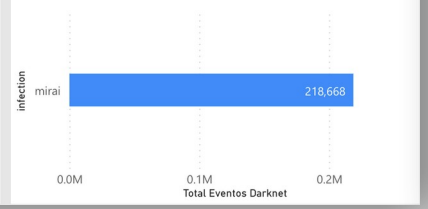
CSIRT-RD
Equipo Nacional de Respuestas a Incidentes Cibernéticos del CNCS

DARKNET

timestamp: 6/1/2021 – 11/19/2022

Total Eventos	IP address Unicas Source	IP Address Unicas Destino
218,668	21,170	2,628

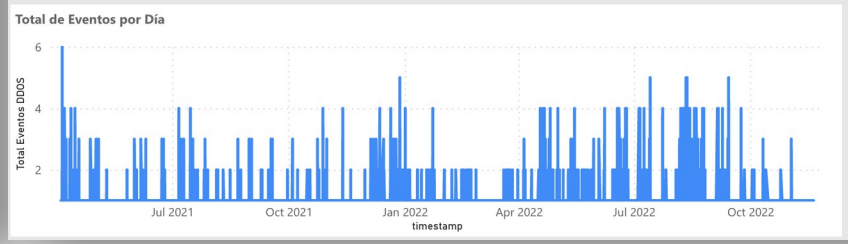




DDOS Amplify

timestamp: 6/1/2021 – 11/19/2022

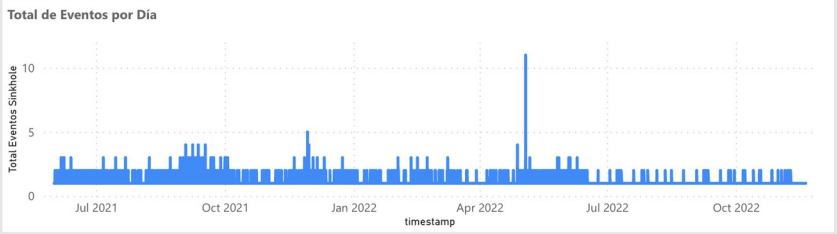
Total Eventos	IP address Unicas Source	Tags
8,070	3,515	22

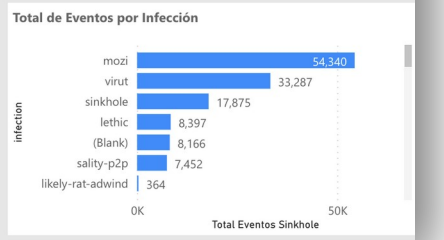


SINKHOLE

timestamp: 6/1/2021 – 11/19/2022

Total Eventos	IP address Unicas Source	IP Address Unicas Destino
133,051	34,881	67

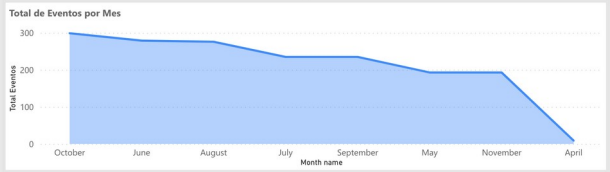


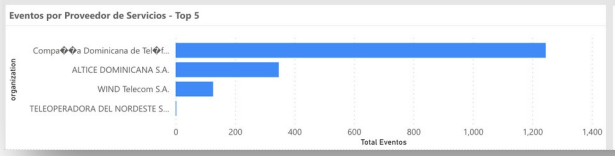


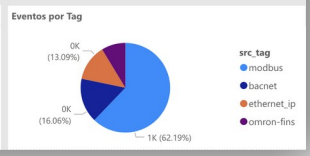
SCAN ICS

timestamp: 4/26/2022 – 11/20/2022

Total Eventos	IP address Unicas Source	IP Address Unicas Destino
1,719	144	5







Funded by the European Union

Latin America and Caribbean Cyber Competence Centre

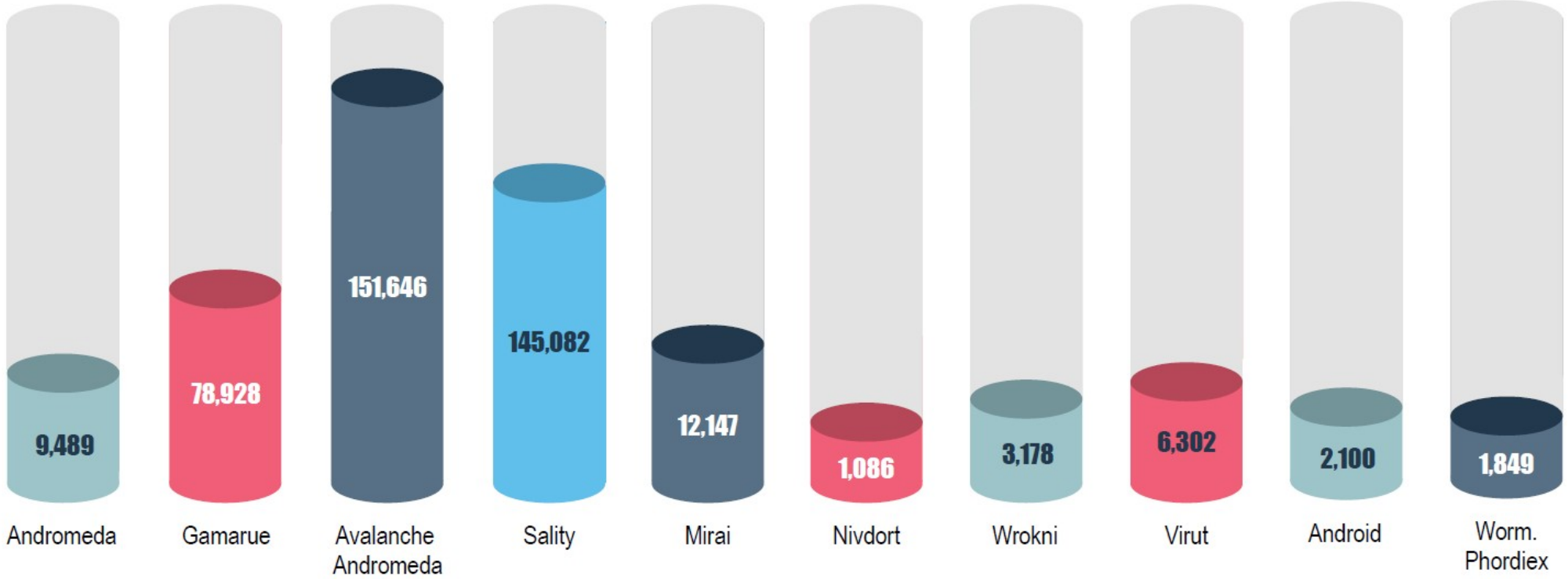
Ataques de Fuerza bruta

Funded by
the European Union

Funded by the European Union

Ciberexposición - Botnet

Ciberexposición - Botnet



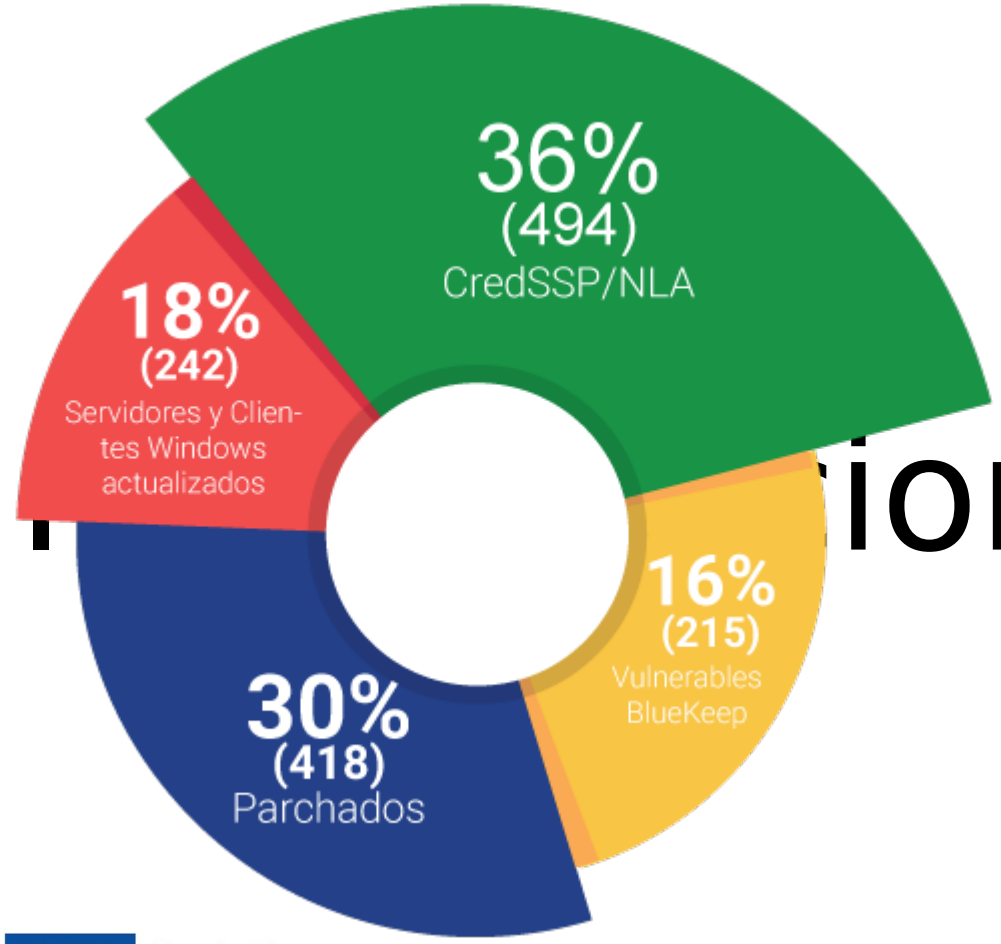
Funded by
the European Union

Ciberexposición - Botnet

No.	Dirección IP	País	IP Únicas
01	208.100.26.251	Estados Unidos	133,731
02	64.95.103.190	Estados Unidos	80,199
03	35.229.93.46	Estados Unidos	73,210
04	35.231.151.7	Estados Unidos	71,102
05	72.26.218.69	Estados Unidos	48,668
06	72.5.161.4	Estados Unidos	46,537
07	107.6.74.84	Estados Unidos	32,767
08	72.26.218.71	Estados Unidos	29,886
09	72.26.218.74	Estados Unidos	29,263
10	72.26.218.75	Estados Unidos	20,590

Funded by the European Union

Ciberexposición - RDP



Accesibles RPD en el ciberespacio dominicano Abril - 2020

De igual manera, se observaron 418 hosts que han sido actualizados y la vulnerabilidad ha sido remediada. Con respecto a la autenticación de nivel de red, conocida por sus siglas en inglés NLA (Network Level Authentication), utilizada en RDP y sugerida por Microsoft, en caso de que el servidor sea crítico y no exista la posibilidad de parcharlo de inm

Categoría	Cantidad
Servidores y Clientes Windows actualizados	242
CredSSP/NLA	494
Parchados	418
Vulnerables BlueKeep	215
TOTAL ACCESIBLES RDP	**1369**

Funded by
the European Union

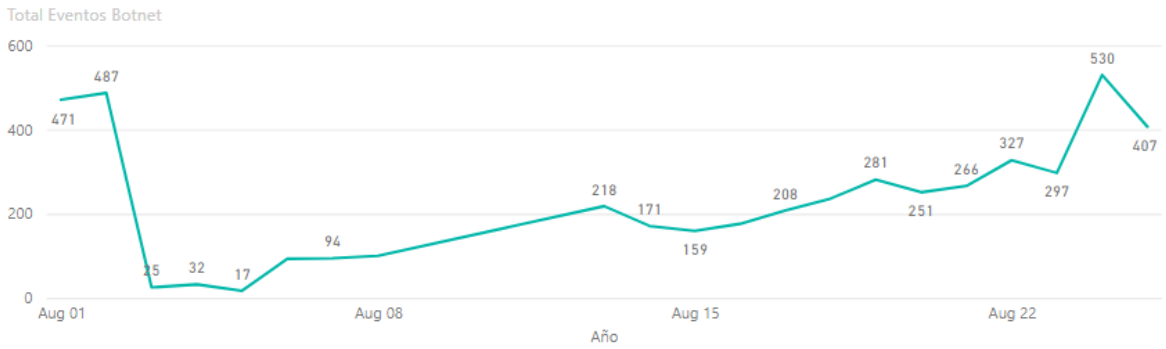
CSIRT-RD
Equipo Nacional de Respuestas a Incidentes Cibernéticos del CNCS

MOZI

4,846
Total eventos Botnet

2,570
IP unico Botnet

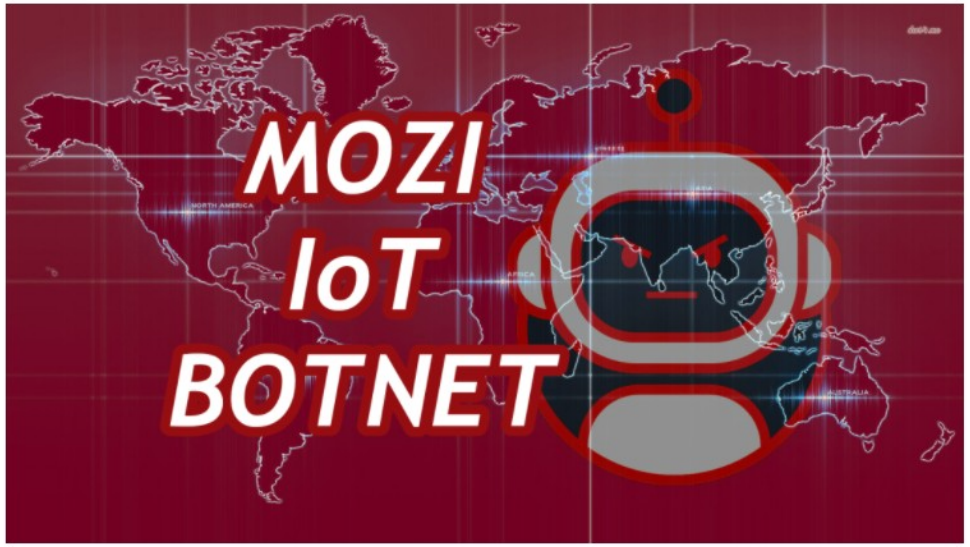
timestamp
8/1/2021 8/31/2021



La Botnet Mozi se actualiza con nuevos objetivos

18 agosto, 2021 Por Jose Ignacio Palacios Ortega — Leave a Comment

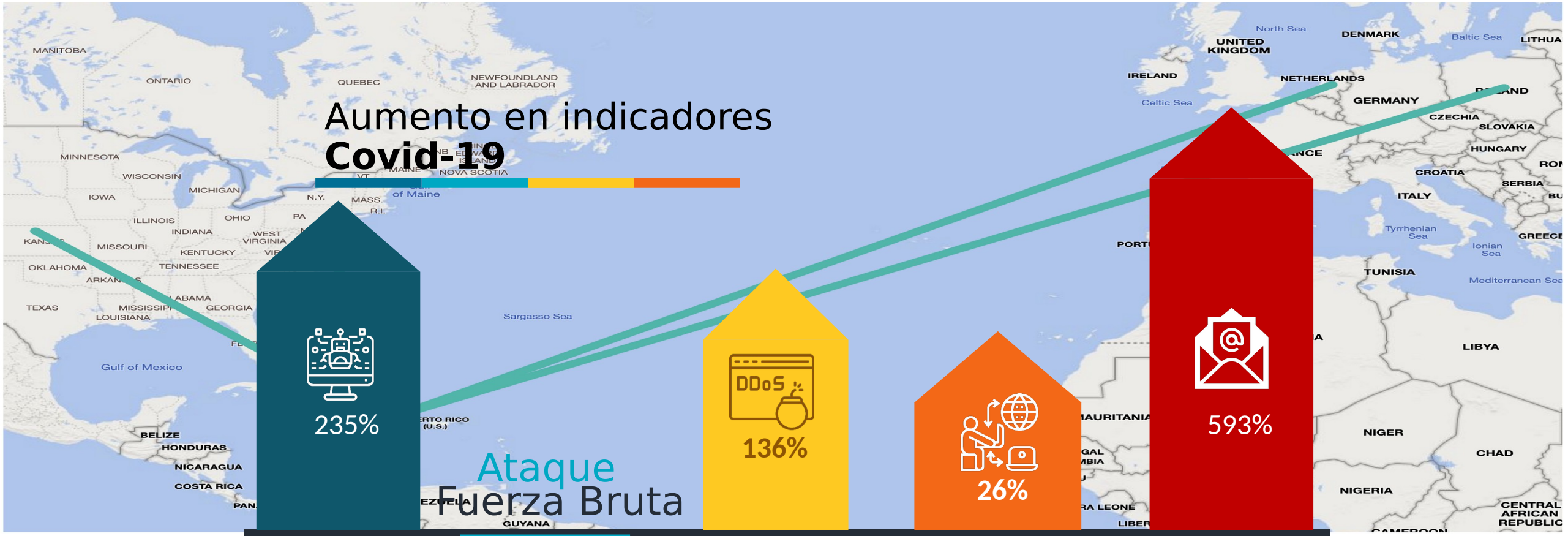
Se ha dado a conocer que la Botnet Mozi ha sido actualizado lo que le permite tener nuevos fabricantes como objetivos como son Netgeat, Huawei y ZTE.



Funded by the European Union

CSIRT-RD
Equipo Nacional de Respuestas a Incidentes Cibernéticos del CNCS

Aumento en indicadores **Covid-19**

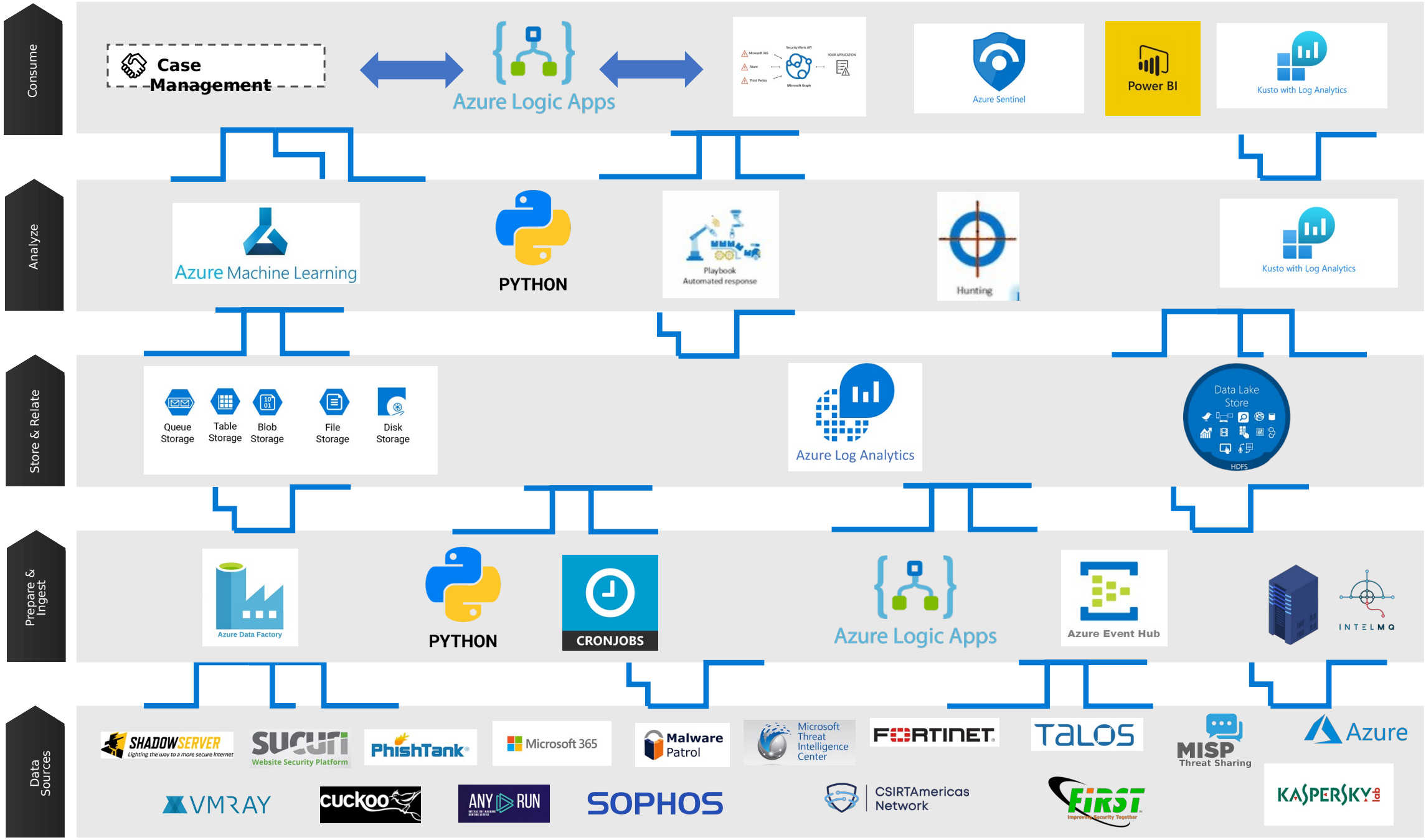


PRESIDENCIA DE LA REPÚBLICA DOMINICANA
MINISTERIO DE LA PRESIDENCIA
Funded by the European Union

Latin America and Caribbean Cyber Competence Centre

Programa de Madurez de Respuesta a Incidentes

Funded by the European Union


Consume
Case Management
Azure Logic Apps
Azure Sentinel
Power BI
Kusto with Log Analytics
Analyze
Azure Machine Learning
PYTHON
Playbook
Automated response
Hunting
Kusto with Log Analytics
Store & Relate
Queue Storage
Table Storage
Blob Storage
File Storage
Disk Storage
Azure Log Analytics
Data Lake Store
HDFS
Prepare & Ingest
Azure Data Factory
PYTHON
CRONJOBS
Azure Logic Apps
Azure Event Hub
INTELMQ
Data Sources
SHADOWSERVER
Lighting the way to a more secure Internet
Sucuri
Website Security Platform
PhishTank
Microsoft 365
Malware Patrol
Microsoft Threat Intelligence Center
FORTINET
TALOS
MISP
Threat Sharing
Azure
VMRAY
cuckoo
ANY RUN
SOPHOS
CSIRTAmericas Network
FIRST
KASPERSKY lab

CNCS CENTRO NACIONAL DE CIBERSEGURIDAD REPÚBLICA DOMINICANA

República Dominicana

INICIO MAPA DEL SITIO CONTÁCTANOS

INICIO SOBRE NOSOTROS CSIRT-RD NOTICIAS BOLETINES CIBER-OBSERVATORIO BLOG CONTÁCTANOS CONSULTAR CIBEREXPOSICIÓN

CIBER-OBSERVATORIO

El Observatorio Nacional de Ciberseguridad (Ciberobservatorio) es un espacio diseñado para observar, investigar y analizar las características de los principales indicadores de ciberexposición, brindándole al ciudadano información accionable sobre los indicadores de compromiso relacionados a las vulnerabilidades e infecciones que afectan el ciberespacio dominicano.

Inicio » Ciber-observatorio

Funded by the European Union

Latin America and Caribbean Cyber Competence Centre

Periodo de Tiempo

2/12/2019 — 11/16/2022

service: All

dst_geo: All

Ataques de Fuerza Bruta desde República Dominicana

Total de Eventos	IP's Unicas	IP Destino Afectadas
294,740	27,832	3,205

service	IP Unicas SRC
	18,162
	2,249
ftp	1
http	8
imap	1
imaps	2
rdp	5
smtp	3
ssh	4,501
telnet	9,499
vnc	6
Total	**27,832**

dst_port	IP Unicas SRC
23	20,712
	6,789
22	5,833
5555	1,685
7547	33
143	11
37777	9
5900	9
80	9
3389	5
6789	5
Total	**27,832**

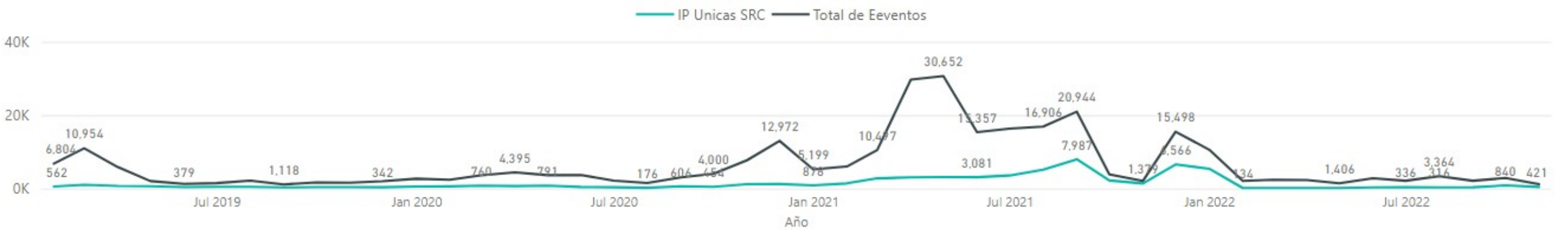
dst_geo	IP Unicas SRC
US	12,861
UK	7,024
	7,004
SE	6,715
DE	5,968
FR	5,180
NL	5,024
AU	4,910
JP	4,274
SG	3,922
ZA	3,803
Total	**27,832**

Total de Casos por Mes

Año	Mes	Total de Eeventos
2022	enero	10,574
2022	febrero	2,046
2022	marzo	2,384
2022	abril	2,293
2022	mayo	1,406
2022	junio	2,816
2022	julio	2,110
2022	agosto	3,364
2022	septiembre	2,110
2022	octubre	2,868
Total		**294,740**

Mapa IP destino afectadas

Gráfica Total Casos, IP Unicas por Mes



Periodo de Tiempo

2/12/2019 — 11/16/2022

Infección

All

Geolocalización CC

All

Infecciones Botnet en República Dominicana

Total de Eventos	IP's Unicas	IP's CC
15,765,838	735,096	2,556

Mapa de Centros de Mando y Control (CC)

IP Unica por Infección

infection	IP Unicas
avalanche-andromeda	684,065
sality	166,696
gamarue	134,684
sality-p2p	127,615
mirai	72,449
android.hummer	52,722
virut	46,555
js.worm.bondat	31,248
necurs	19,297
lethic	17,887
Total	**735,096**

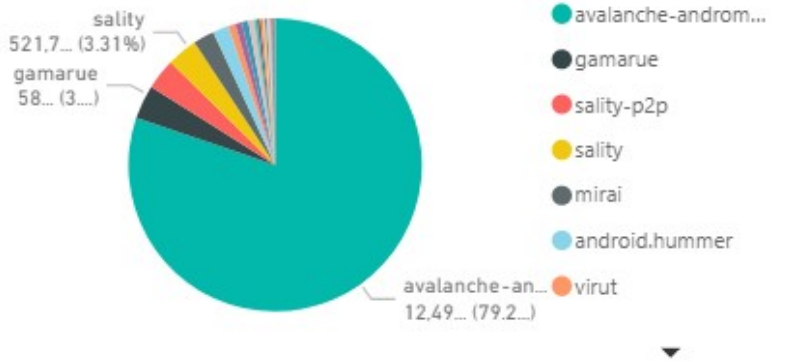
IP Unica por CC y Tipo de Infección

infection	dst_ip	IP Unicas
avalanche-andromeda	208.100.26.245	430,099
avalanche-andromeda	35.231.151.7	357,695
avalanche-andromeda	35.229.93.46	354,320
avalanche-andromeda	184.105.192.2	320,996
avalanche-andromeda	107.6.74.81	264,398
avalanche-andromeda	72.26.218.75	171,874
avalanche-andromeda	72.5.161.7	158,056
avalanche-andromeda	72.26.218.82	141,786
avalanche-andromeda	63.251.126.11	141,497
sality-p2p		127,615
Total		**735,096**

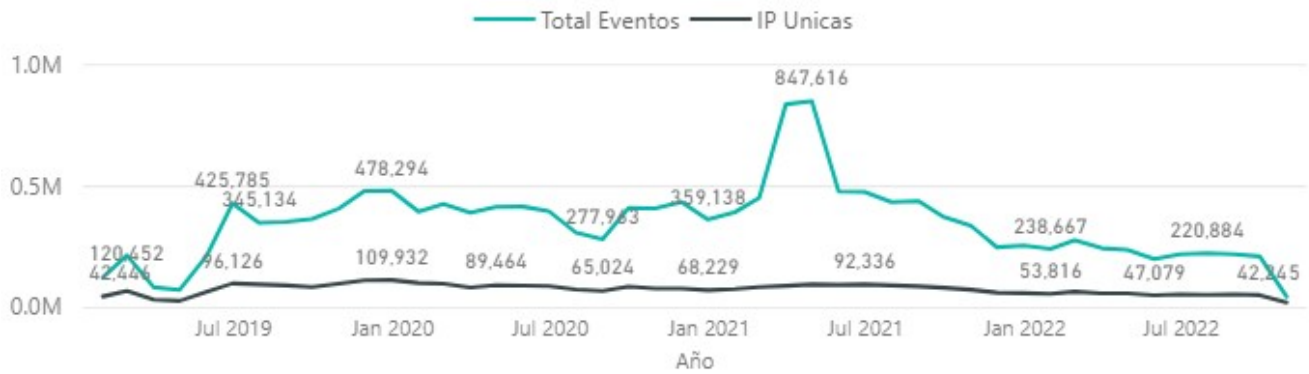
IP Unica por CC

dst_ip	dst_geo	IP Unicas
		262,825
103.86.49.11	TH	2
104.131.11.150	US	2
104.131.41.185	US	141
104.16.173.80	US	4,289
104.16.6.63	US	13
104.17.244.81	US	4,145
104.18.150.55	US	12
104.244.14.252	US	15,381
104.42.225.122	US	4
Total		**735,096**

Total Casos por Infección



Gráfica Total Casos, IP Unicas por Mes



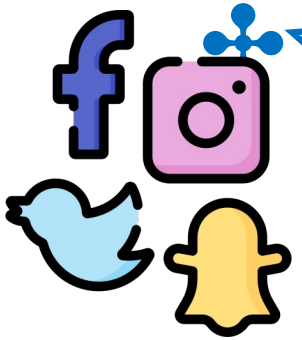
Total de Casos por Mes

Año	Mes	Total Eventos
2019	febrero	120,452
2019	marzo	211,423
2019	abril	80,494
2019	mayo	69,856
2019	junio	209,139
2019	julio	425,785
2019	agosto	345,134
2019	septiembre	350,158
2019	octubre	361,460
Total		**15,765,838**

DNS de CC

IP Unicas	src_hostname
451,772	
1,705	ns1432.ztomy.com
444	nat.tvm.televiaducto.net
243	undefined.hostname.localhost
167	nat.tmb.telecableinternacional.com
28	customer.atlagax1.pop.starlinkisp.net
15	cache.google.com
8	msg.zolmobi.com
735,096	

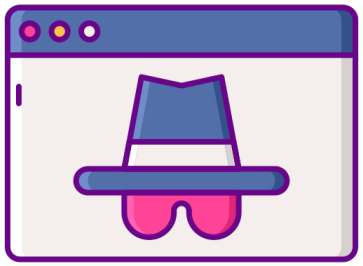

INTELIGENCIA
DE
CIBERAMENAZAS
Detección avanzada de
amenazas, Captura y Análisis
“Detectar amenazas
cibernéticas proactivamente
reduce el riesgo de ataque”



OSINT

Monitoreo de las Cosas

Investigaciones Dirigidas



Monitoreo de Deep Web y Dark Web

- ¿Quién me quiere/pudiera atacar?
- ¿Hay alguien que esté planeando atacarme?
- ¿Están atacando empresas similares a la mía en el país o en otra parte del mundo?
- ¿Se está usando el nombre de mi institución en sitios para phishing?
- ¿Hay información de mi institución a la venta en el mercado negro?

Funded by the European Union

CUENTAS DE CORREO FILTRADAS

Gobierno

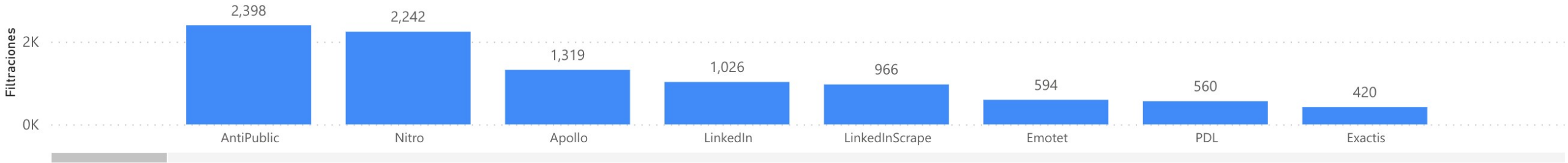
257
Dominios filtrados

7,834
Cuentas filtradas

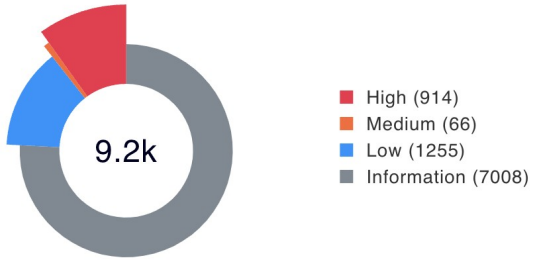
12,527
Filtraciones

Dominio

Brecha de Datos



Current issues

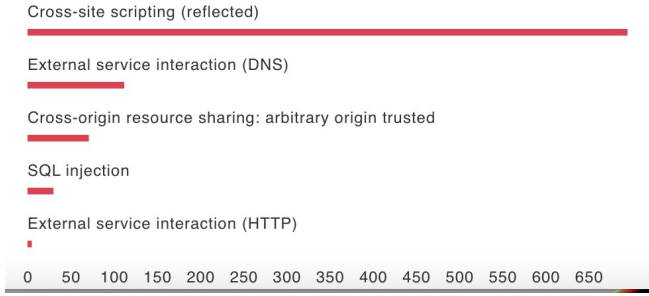


Most vulnerable sites

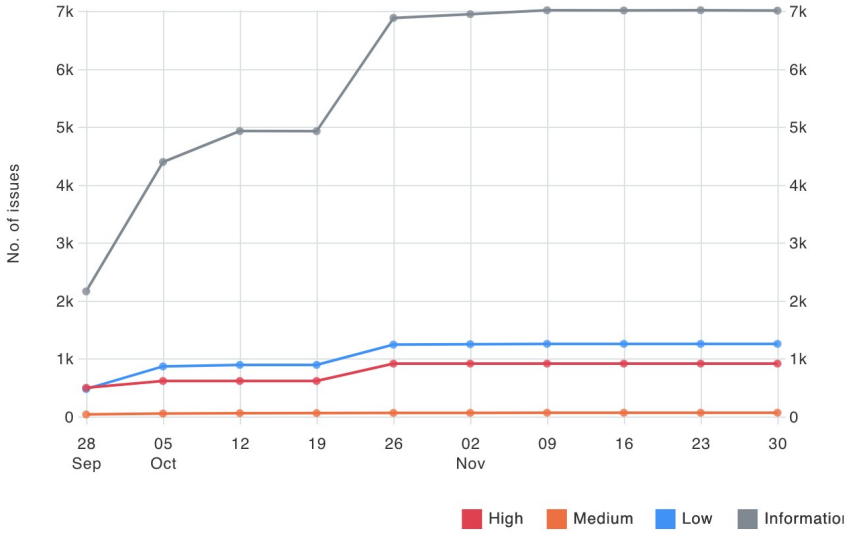
[redacted]	350	2	176	970
[redacted]	276	4	286	1k
[redacted]	143	27	28	314
[redacted]	71	5	236	743
[redacted]	41	1	23	759

View sites

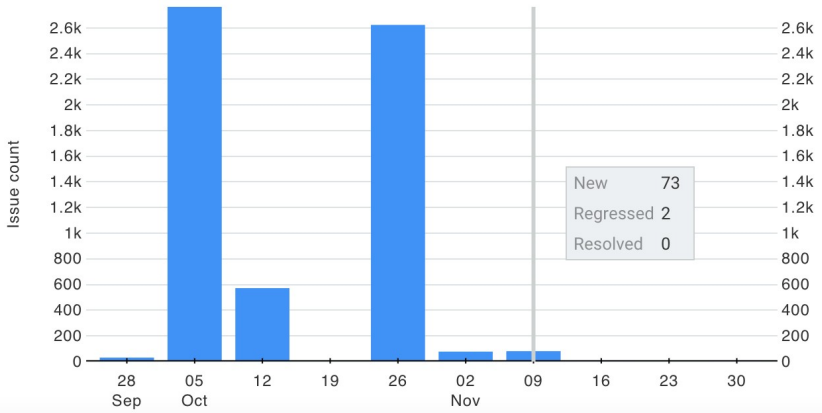
Most serious vulnerabilities



Issue count over time



New and resolved issues over time



Recent scans

[redacted]	2		5
[redacted]	1		12
[redacted]	2		8
[redacted]	2	3	27
[redacted]	2		37

View scans

Running scans

CNM

View scans

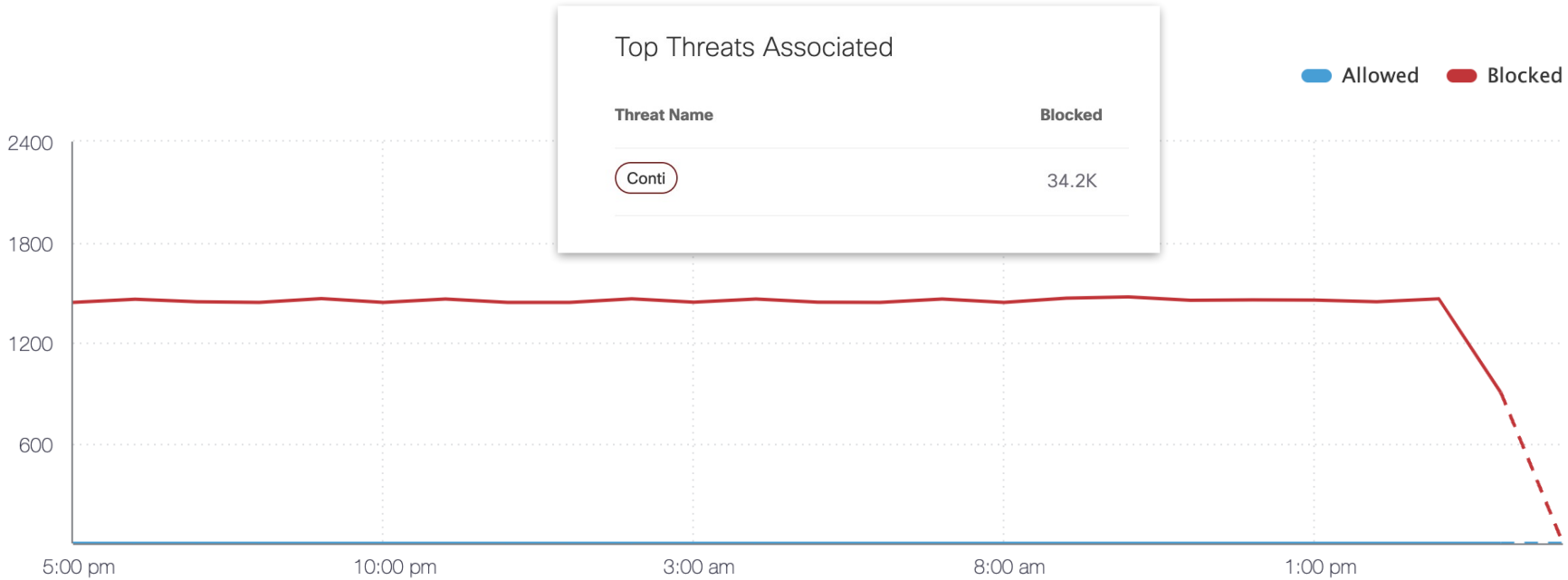
Upcoming scans

[redacted]	
2022-12-05	1:42 PM
[redacted]	
2022-12-07	9:16 AM

Ransomware Activity

See All Ransomware Details

34.3K Total ▼ **5%** vs. previous 24 hours



Top Threats Associated

Top Active Identities

Funded by the European Union

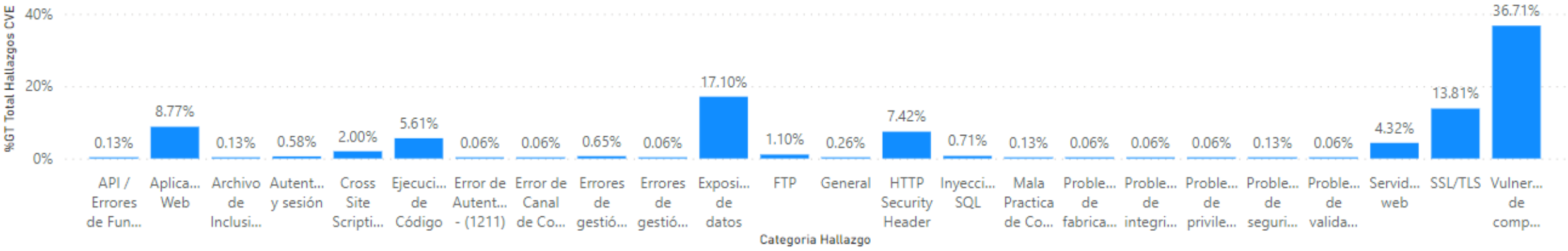
CNCS CENTRO NACIONAL DE CIBERSEGURIDAD REPÚBLICA DOMINICANA

CUADRO DE MANDO DE OPERACIONES

CSIRT-RD Equipo Nacional de Respuestas a Incidentes Cibernéticos del CNCS

Monitor de Vulnerabilidades y Exposiciones Comunes (CVE)

Total Hallazgos por Categoria



ID

Search

Hallazgo

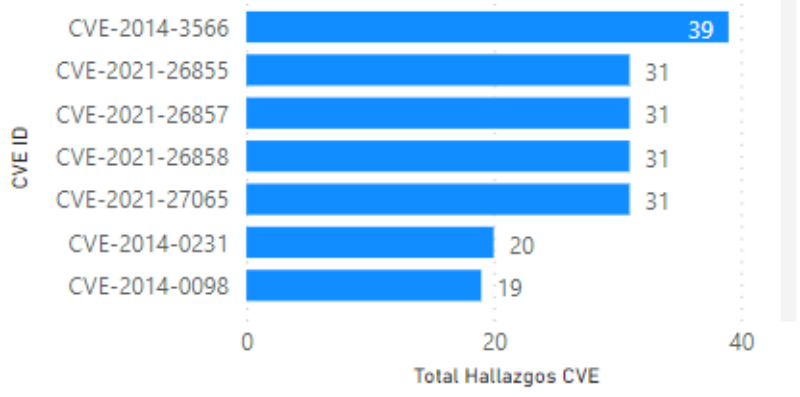
Search

CVE ID

Search

ID	Hallazgo	CVE ID	CVE Descripcion
CSIRT-HALL-001776	Exchange Server Vulnerable ProxyShell	CVE-2021-34523	Microsoft Exchange Server Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-33768, CVE-2021-34470.
CSIRT-HALL-001777	Exchange Server Vulnerable ProxyShell	CVE-2021-34523	Microsoft Exchange Server Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-33768, CVE-2021-34470.
CSIRT-HALL-001780	Exchange Server Vulnerable ProxyShell	CVE-2021-34523	Microsoft Exchange Server Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-33768, CVE-2021-34470.
CSIRT-HALL-001781	Exchange Server Vulnerable ProxyShell	CVE-2021-34523	Microsoft Exchange Server Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-33768

Total Hallazgos por CVE ID



Eventos Críticos

CSIRT-RD
Equipo Nacional de Respuestas a Incidentes Cibernéticos del CNCS

solarwinds

Exchange
Microsoft

FORTINET

Funded by the European Union

.DO Reporte de configuración de resiliencia

Configuración de seguridad web de los principales servicios bajo el dominio de nivel superior (TLD) DO. Mantenido por Centro Nacional de Ciberseguridad de la República Dominicana.

CSIRT-RD
Equipo Nacional de Respuestas a Incidentes Cibernéticos del CNCS

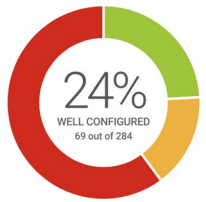
315 HOSTS

705 CERTIFICATES

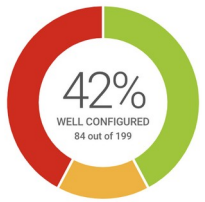
901 IP ADDRESSES

Infrastructure Configuration Overview

Key aspects of web application and email infrastructure configuration and security.



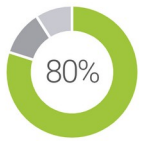
WEB CONFIGURATION



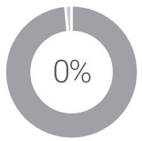
EMAIL CONFIGURATION

Email Infrastructure Configuration

Key aspects of email security of the hosts monitored by this dashboard.



STARTTLS



DANE

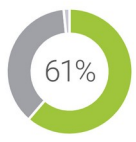
SPF

DMARC

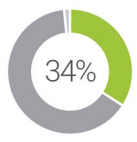
Web Application Configuration

Key aspects of web application security of the hosts monitored by this dashboard.

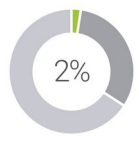
HTTPS



HTTPS Redirection



HSTS

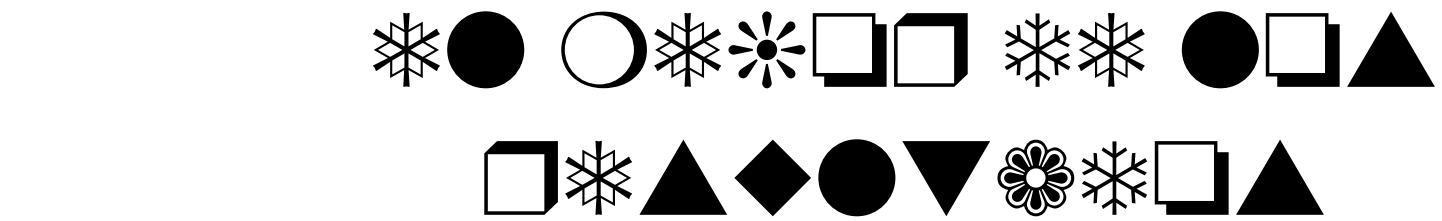


HSTS Preloaded

		HTTPS	HTTPS Redirection	HSTS	HSTS Preloaded	DNSSEC
Educacion / Education 35 host(s)	23% 7 out of 31	97%	68%	29%	3%	0%
Energia / Energy 17 host(s)	24% 4 out of 17	100%	76%	12%	0%	0%
Financiero / Financial 29 host(s)	33% 9 out of 27	100%	89%	48%	0%	0%
Gobierno / Government 61 host(s)	35% 20 out of 57	100%	77%	46%	4%	0%
Gobierno Municipales /Municipal Government 7 host(s)	50% 3 out of 6	100%	83%	83%	33%	0%
Militar / Military 42 host(s)	29% 11 out of 39	97%	74%	54%	3%	0%

CSIRT-RD
Equipo Nacional de Respuestas a Incidentes Cibernéticos del CNCS

Información + Poder de acción =



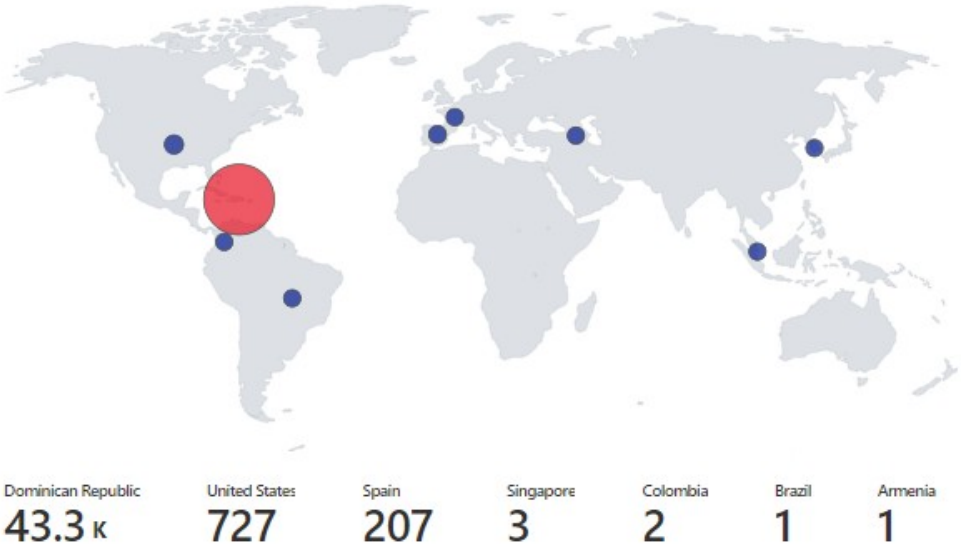
Funded by the European Union

CSIRT-RD
Equipo Nacional de Respuestas a Incidentes Cibernéticos del CNCS

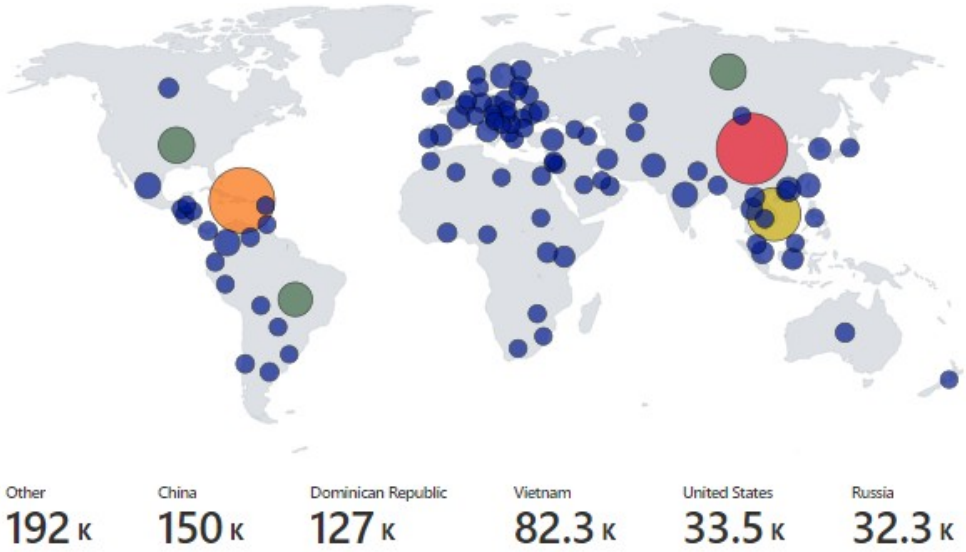
MONITOREO

1,014%

21 – 28
febrero 2022



7 días



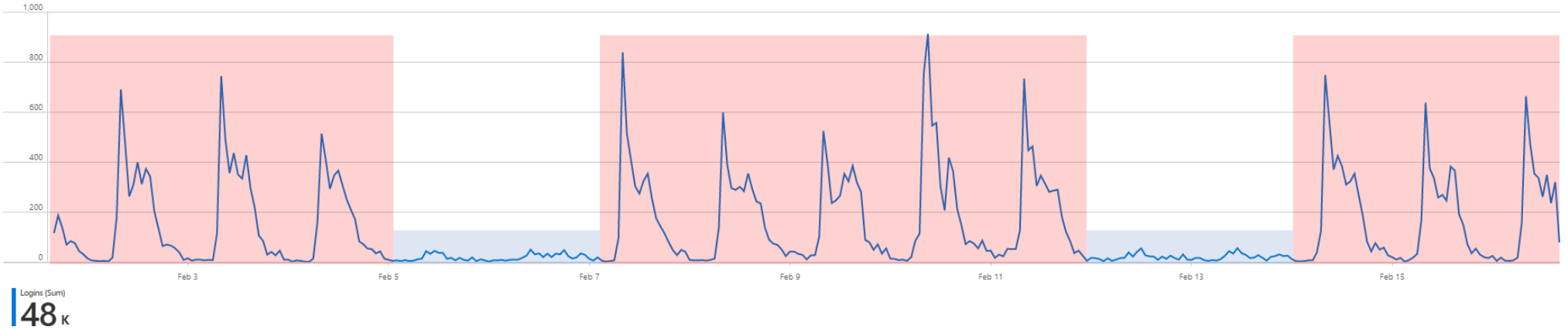
Funded by the European Union

Latin America and Caribbean Cyber Competence Centre

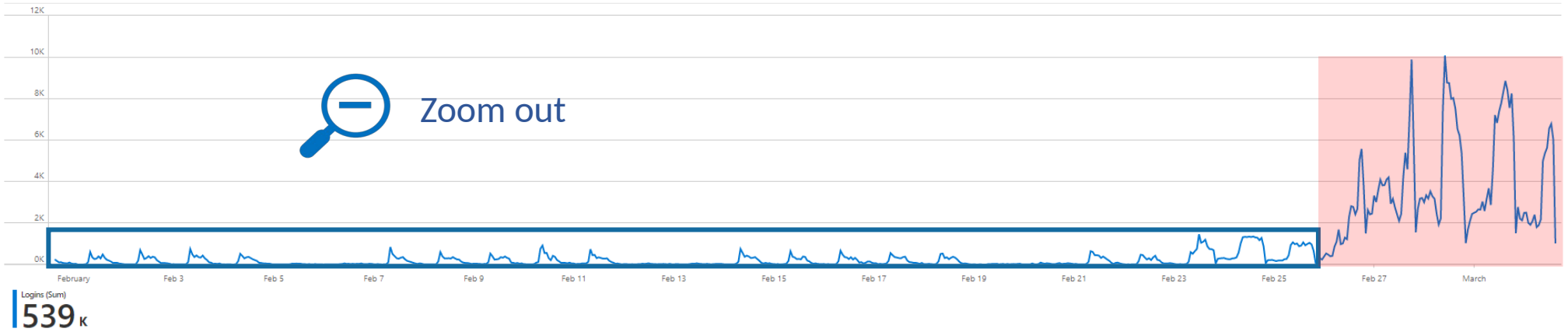
CSIRT-RD
Equipo Nacional de Respuestas a Incidentes Cibernéticos del CNCS

MONITOREO

1 – 16 febrero 2022



26 febrero – 2 marzo 2022



Funded by the European Union

ALERTAS

+ 450 SITES (gob.do) + 30 PAISES + 150 IP UNICAS 1 USER-AGENT → “Python request 2.27.1”

Funded by the European Union

342,728

Blocked Requests

Request Time

6/17/2020 — 10/23/2020

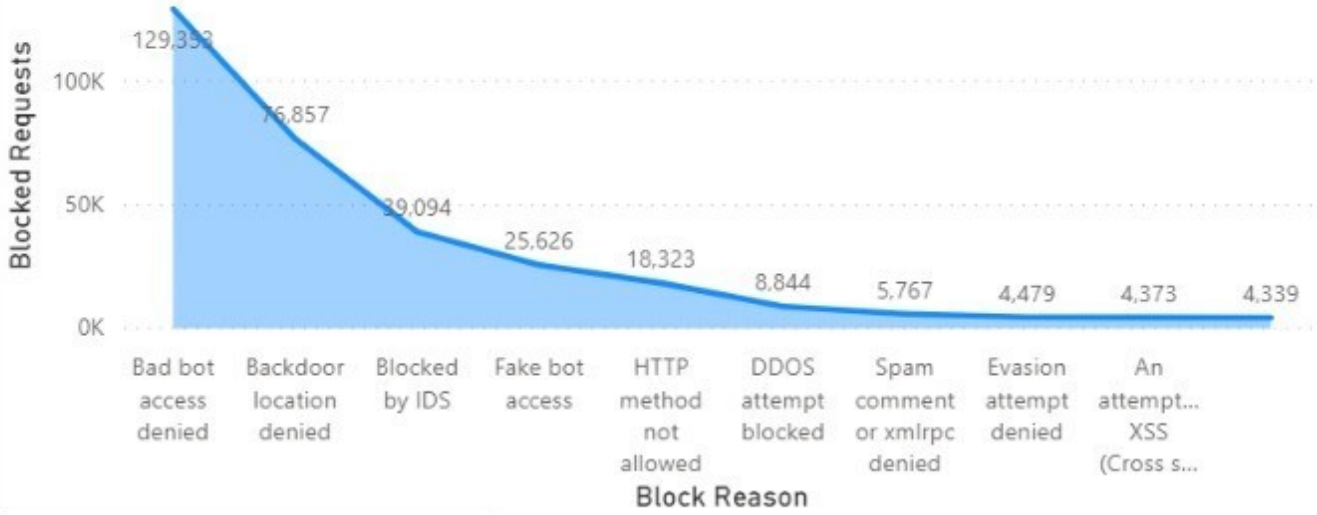
CNCS CENTRO NACIONAL DE CIBERSEGURIDAD REPÚBLICA DOMINICANA

CSIRT-RD
Equipo Nacional de Respuestas a Incidentes Cibernéticos del CNCS

Country of Origin	Blocked Requests
Dominican Republic	121,300
France	87,430
United States	83,846
false	5,570
Russian Federation	5,510
China	5,384
Ukraine	4,939
Germany	4,021
Mexico	2,172
United Kingdom	1,998
Netherlands	1,923
Canada	1,806
Total	**342,728**

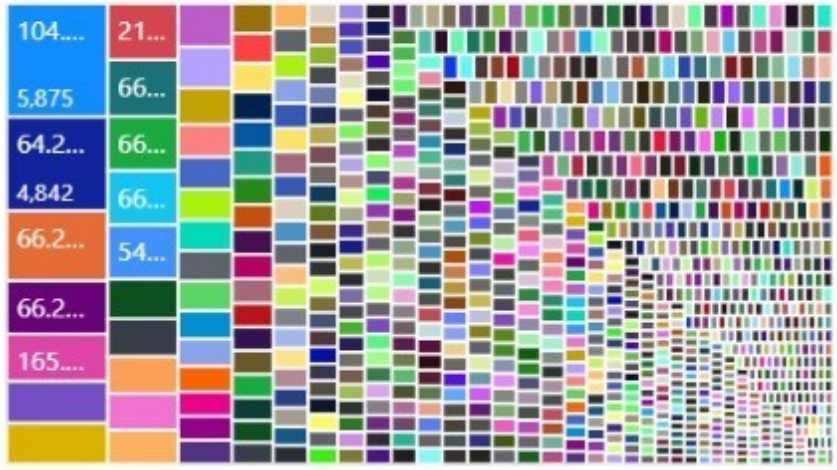
Blocked Requests by Domain

Blocked Requests by Block Reason



Blocked Requests by Country of Origin

Blocked Requests by Remote Address



Incident

Incident ID 215

Refresh

Botnet Drone Detection

Incident ID: 215

Unassigned	New	High
Owner	Status	Severity

Alert product names

- Azure Sentinel

Evidence

1	1	0
Events	Alerts	Bookmarks

Last update time
06/02/21, 09:53 PM

Creation time
06/02/21, 09:53 PM

Entities (5)

- 186.149.199.246
- 35.231.151.7
- http://differentia.ru/...
- onamet.gov.do

View all >

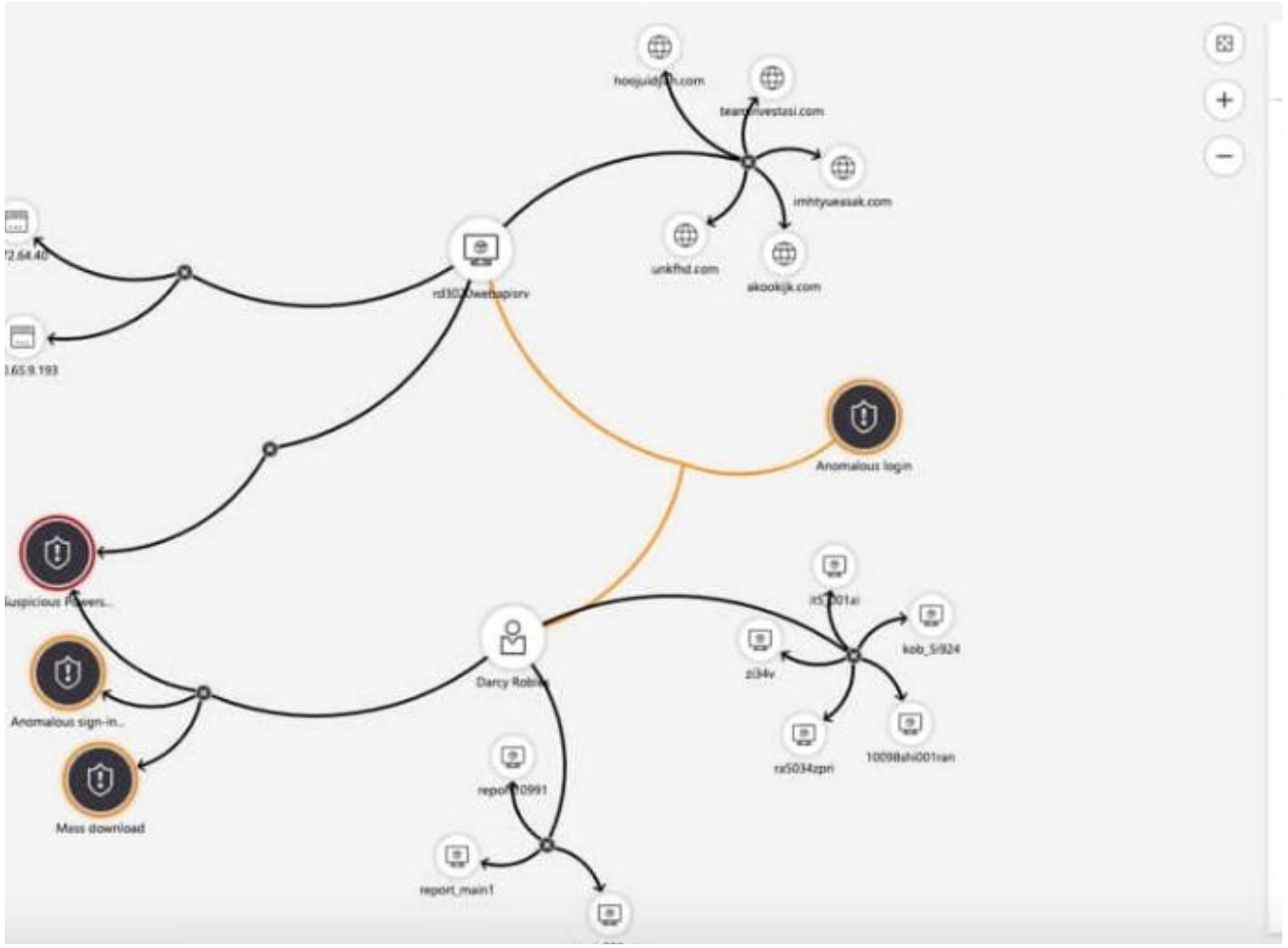
Tactics (4)

- Initial Access
- Discovery
- Execution
- Command and Control

Incident workbook
Incident Overview

Analytics rule
Botnet Drone Detection

Correlación de eventos



Funded by the European Union

1 – 10 - 60

Funded by
the European Union

CUADRO DE MANDO DE OPERACIONES

CNCS CENTRO NACIONAL DE CIBERSEGURIDAD REPÚBLICA DOMINICANA

CSIRT-RD Equipo Nacional de Respuestas a Incidentes Cibernéticos del CNCS

Resumen Ejecutivo

648 Total de Casos

89% % Resolución de...

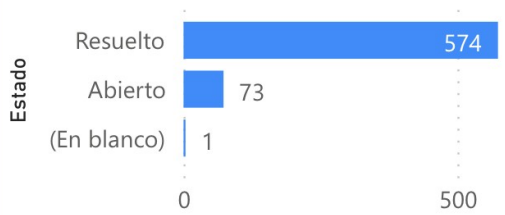
1555 Total Hallazgos

57,56% % Resolución de Hallazgos

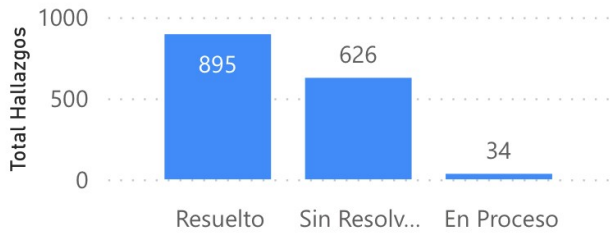
346 No. Organizaciones

400 Total Analisis Vulnerabilidades

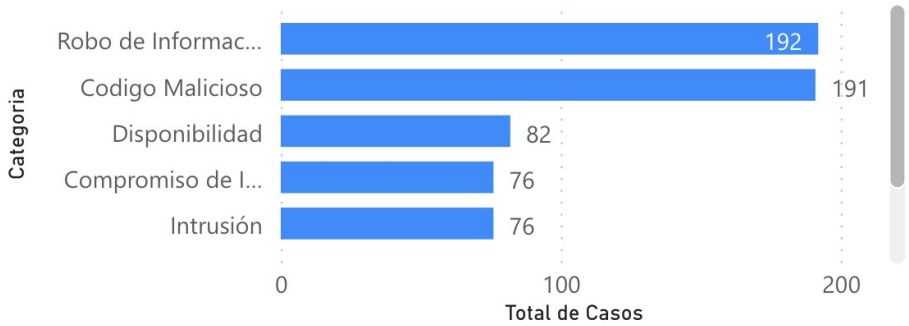
Total de Casos por Estado



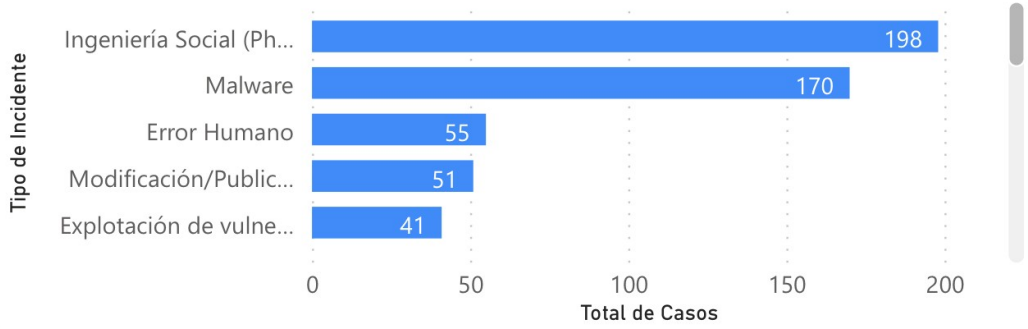
Total Hallazgos por Estado



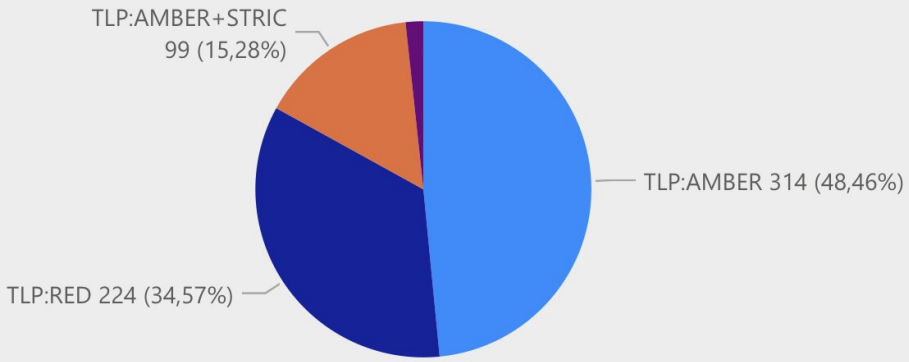
Total de Casos por Categoria



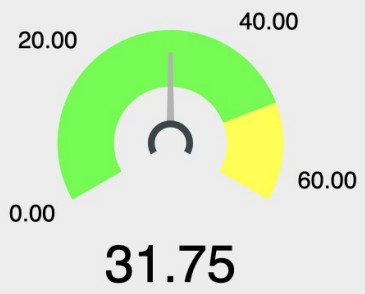
Total de Casos por Tipo Incidente



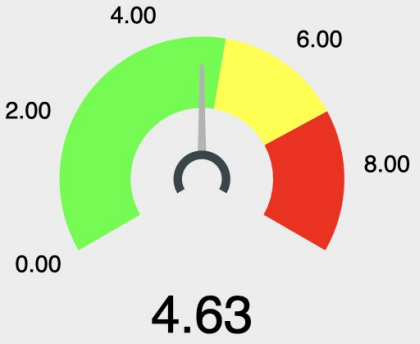
Total de Casos por TLP (Traffic Light Protocol)



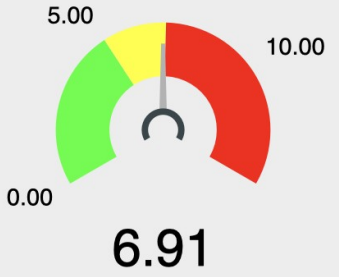
Score de Riesgo



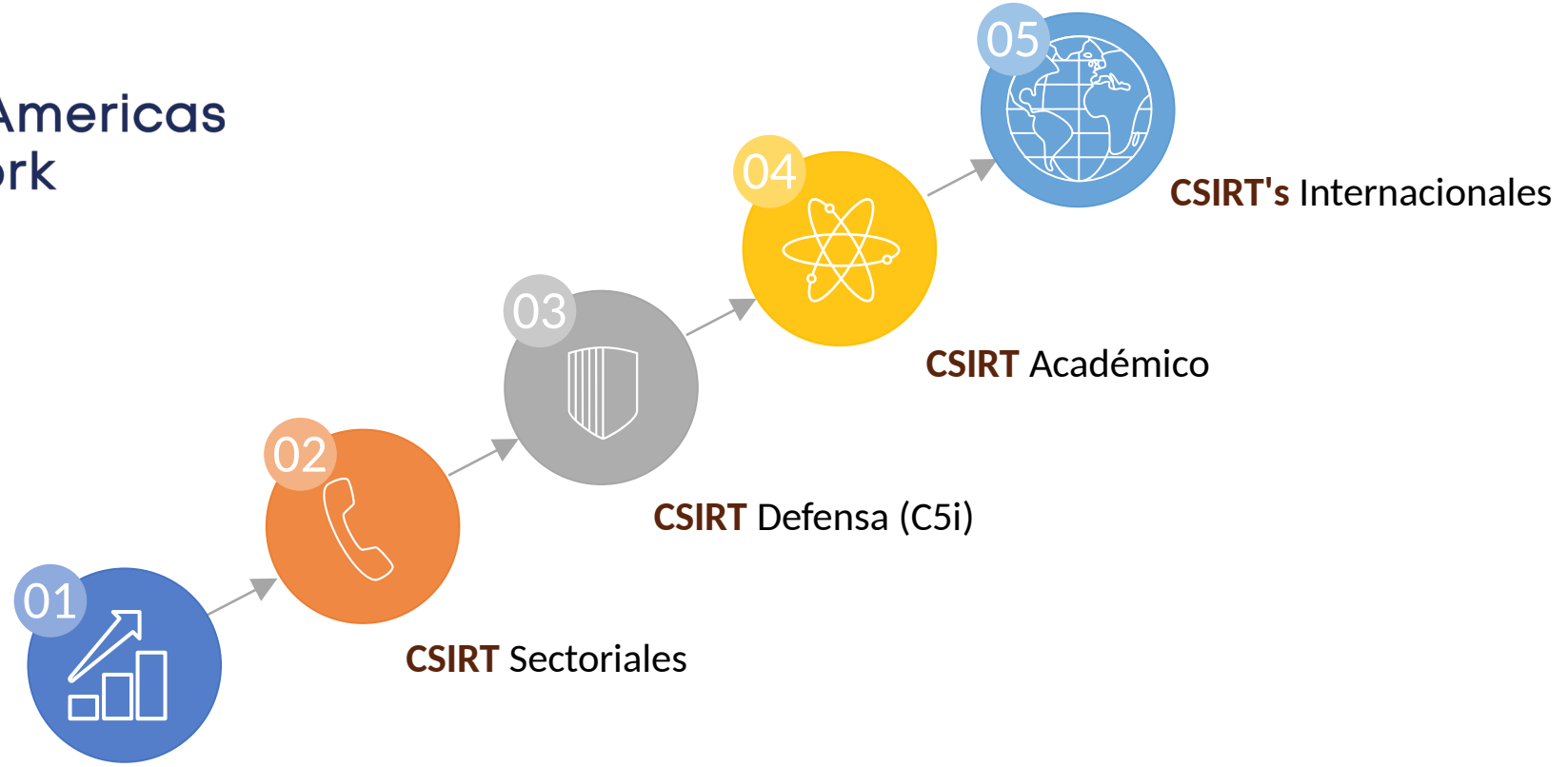
Score Impacto



Promedio Score Peligrosidad



Prevención – Coordinación – Defensa



Funded by the European Union

CSIRT-RD

MISP Threat Sharing

CNCS

List Events
Add Event
Import from…
REST client

List Attributes
Search Attributes

View Proposals
Events with proposals
View delegation requests
View periodic summary

Export
Automation

Events

« previous 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 next »

My Events | Org Events | Enter value to search | Event info | Filter

Creator org	Owner org	ID	Clusters	Tags	#Attr.	#Corr.	Creator user
ORGNAME_9729	CSIRTCosta Rica	93639		Ransomware, Threat:Ransomware	35	19	edgar.mora@
FUERZA AEREA DE COLOMBIA	CSIRTCosta Rica	93638		Actor: Lazarus, APT, Backdoor, csirt-americas:malware, enisa:nefarious-activity-abuse="malicious-code-software-activity"	13	9	edgar.mora@
CUDESO	CSIRT-RD	87176	Exploit-Kit: GreenFlash Sundown; Ransomware: Hermes Ransomware	tlp:white	42	1	oavilez@csirt
ESET	CSIRT-RD	85889	Threat Actor: Turla Group; Enterprise Attack - Attack Pattern: Email Collection - T1114, Component Object Model Hijacking - T1122	misp-galaxy:mitre-attack-pattern="Component Object Model Hijacking", misp-galaxy:mitre-attack-pattern="Email Collection", tlp:white, type:OSINT, osint:lifetime="perpetual", osint:certainty="50", cert-ist:threat_targeted_sector="Academic and Research", cert-ist:threat_targeted_sector="Gov", cert-ist:threat_targeted_region="Western Europe", cert-ist:enriched, cert-ist:ioc_accuracy="medium", cert-ist:threat_level="medium", cert-ist:threat_type="apt"	53	4	oavilez@csirt
CUDESO	CSIRT-RD	87233	Threat Actor: Sofacy	tlp:white, misp-galaxy:mitre-intrusion-set="APT28"	35	6	oavilez@csirt
ORGNAME_9729	CSIRTCosta Rica	93637	Banker: Geodo	malware_classification:malware-category="Botnet", emotet, Emotet, malware:emotet	20	8	edgar.mora@
NTTDATA-ES-CERT_7698	CSIRTCosta Rica	93635	Attack Pattern: Phishing - T1566; Malpedia: QakBot	tlp:green	43		edgar.mora@
CUDESO	CSIRTCosta Rica	93634		misp:tool="misp-scraper", osint:source-type="blog-post"	37	34	edgar.mora@

HERRAMIENTAS

El Centro Nacional de Ciberseguridad a través del CSIRT pone a disposición de la comunidad objetivo, empresarios y ciudadanos en general, herramientas de ciberseguridad enfocadas a la prevención, detección con la finalidad de los usuarios puedan protegerse y fortalecer su entorno tecnológico.

- VERIFICACIÓN CORREO COMPROMETIDO
- VERIFICACIÓN CONTRASEÑA COMPROMETIDA
- VERIFICACIÓN IP COMPROMETIDO
- VERIFICACIÓN ENLACE MALICIOSO
- REPORTAR INCIDENTE
- ANÁLISIS DE VULNERABILIDADES
- EXTENSION DE CHROME

CNCS | CENTRO NACIONAL DE CIBERSEGURIDAD
REPÚBLICA DOMINICANA

97

Sitios Bloqueados

Ultima actualización: 2:02 minutos

Página principal > Extensiones > CNCS Anti-Phishing

CNCS Anti-Phishing

Ofrecido por: https://cncs.gob.do

★★★★★ 1 | Productividad | 46 usuarios

Funded by the European Union

CSIRT-RD
Equipo Nacional de Respuestas a Incidentes Cibernéticos del CNCS

* ~~Cambios~~ Nuevos recientes Paradigmas:

- Reactivo → Proactivo/preventivo hunting

Riesgo ↕ Exposición

- Procesos → Datos Data-centric information/Data bus for tools integration

- Gestión de vulnerabilidades + inteligencia de amenazas. Detección señales tempranas

- Concienciación + construcción de capacidades especializadas. Cyber range. usuarios + técnicos

- Islas/silos → Information Sharing MISP/ISACs

No se trata de tecnología

$$\frac{\left(3.5\,G+\frac{V}{2}\right)}{4\;¿\;¿}$$

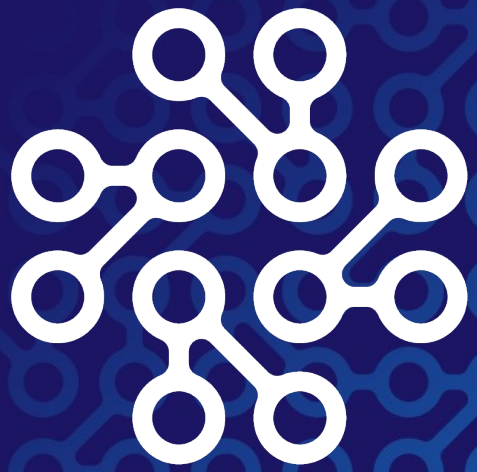
Funded by
the European Union

CSIRT-RD
Equipo Nacional de Respuestas a Incidentes Cibernéticos del CNCS

Carlos Leonardo

carlos@csirt.gob.do

Latin America and Caribbean Cyber Competence Centre



Thank you!

Funded by
the European Union

Contact us:

eucybernet@ria.ee

https://www.lac4.eu/

www.lac4.com