OEA | Más derechos para más gente

CSIRT Americas.org

Operaciones

Inter-American Committee against Terrorism (CICTE)
Organization of American States

CSIRTAmericas.org

Agenda

- ¿Cómo nos comunicamos en la Región?
- Protocolo de Comunicación
- CSIRTAmericas
- Comunidad | Intercambio de información
- Resultados de CSIRTAmericas
- Próximos pasos

Comunicación Regional entre CSIRTs Nacionales en Latinoamérica

CSIRT (Computer Security Incident Response Team, Equipo de Respuesta ante Incidencias de Seguridad Informáticas)

Diversidad en las operaciones

nCSIRT A
País A

- Despliegue Avanzado de EWS
- CSIRT Operativos

nCSIRT C
País C

- Experiencias en casos bancarios
- CSIRT Operativos

nCSIRT E
País E

- En inicios
- Sin especialidad

nCSIRT B
País B

- Manejo de incidentes de gran escala
- CSIRT Operativos

nCSIRT D
País D

- Desarrollo de herramientas
- CSIRT Investigación

Que estamos haciendo desde la OEA

Intercambio de información

Plataforma Tecnológica

CSIRTAmericas.org

Protocolo de Comunicación

Componentes para el Protocolo de Comunicación

Taxonomía referencia común para incidentes

¿Cómo nos entendemos?

CSIRTAmericas

Ecsirt.net

Circl.lu

Niveles de información

¿Qué tipo información a compartir?

Nivel **1** Bajo nivel

Nivel **2** Indicadores

Nivel **3** Avisos

Nivel **4** Reportes

CSIRTAmericas.org

Canales de Comunicación

Transporte de información

Portal comunidad

Alertas tempranas

MISP (a implementar)

Niveles de Sensibilidad TLP

¿Con quién comparto?

Traffic light protocol

- Red
- Amber
- Green
- White

Taxonomías

Para CSIRTAmericas.org

CSIRTAmericas – Taxonomía Propuesta

Taxonomía seleccionada para

CSIRTAmericas.org

Defacement
Malware
DDOS
Phishing
Spam
Botnet
Fastflux
Cryptojacking
XSS
SQL Injection
Vulnerability
Information leak
System compromise
Other

CIRCL TAXONOMY	REFERENCE TAXONOMY
Spam	Abusive Content
malware	Malicious Code
Scan	Information Gathering
	Intrusion Attempts
system-compromise	Intrusions
XSS	
sql-injection	
denial-of-service	Availability
information-leak	Information Content Security
copyright-issue	Fraud
phishing,	
Scam	
vulnerability	Vulnerable
Fastflux	Other
	Test

Table 5: CIRCL taxonomy vs Reference Taxonomy

Enisa 2018

Componentes para el Protocolo de Comunicación

Taxonomía referencia común para incidentes

¿Cómo nos entendemos?

Taxonomia CSIRTAmericas

Ecsirt.net

Circl.lu

Niveles de información

¿Qué tipo información a compartir?

Nivel **1** Bajo nivel

Nivel **2** Indicadores

Nivel **3** Avisos

Nivel **4** Reportes

CSIRTAmericas.org

Canales de Comunicación

Transporte de información

Portal comunidad

Alertas tempranas

MISP (a implementar)

Niveles de Sensibilidad TLP

¿Con quién comparto?

Traffic light protocol

- Red
- Amber
- Green
- White

Niveles de información manejados

Nivel de información	Tipo	Ejemplo
Nivel 1 Información de bajo nivel		• Capturas de tráfico • Logs de aplicaciones • Documentos • Correos
Nivel 2 Indicadores de Detección		• Direcciones IP • DNS names involucrados botnets y C&C • URL de sitios web maliciosos • Secuencia de eventos del “nivel 1”
Nivel 3 Avisos		• Avisos de vulnerabilidades • Reporte de tendencias de ataques • Caracterización de comportamientos de atacantes
Nivel 4 Reportes Estratégicos		• Estudio de impacto de incidents en procesos electorales • Estudio de tendencias de ataques en sector salud • Reportes gerenciales

ENISA 2018

Componentes para el Protocolo de Comunicación

Taxonomía referencia común para incidentes

¿Cómo nos entendemos?

CSIRTAmericas

Ecsirt.net

Circl.lu

Niveles de información

¿Qué tipo información a compartir?

Nivel **1**

Nivel **2**

Nivel **3**

Nivel **4**

CSIRTAmericas.org

Canales de Comunicación

Transporte de información

Portal comunidad

Alertas tempranas

MISP (a implementar)

Niveles de Sensibilidad TLP

¿Con quién comparto?

Traffic light protocol

- Red
- Amber
- Green
- White

Canales de Comunicación

CSIRT Americas org

Canal	Servicio	Niveles de información
Community portal	• Chat • Mensajería urgente	Nivel 3 Avisos Nivel 4 Reportes estratégicos
Alertas tempranas	• Indicadores por pais • Tendencias subregionales	Nivel 2 Indicadores Nivel 3 Avisos
MISP	• Intercambio data bajo nivel • Tendencias subregionales	Nivel 1 bajo nivel Nivel 2 Indicadores Nivel 3 Avisos

Componentes para el Protocolo de Comunicación

Taxonomía referencia común para incidentes

¿Cómo nos entendemos?

CSIRTAmericas

Ecsirt.net

Circl.lu

Niveles de información

¿Qué tipo información a compartir?

Nivel **1**

Nivel **2**

Nivel **3**

Nivel **4**

CSIRTAmericas.org

Canales de Comunicación

Transporte de información

Portal comunidad

Alertas tempranas

MISP (a implementar)

Niveles de Sensibilidad TLP

¿Con quién comparto?

Traffic light protocol

- Red
- Amber
- Green
- White

Niveles de sensibilidad (TLP)

Código	¿Cuándo utilizarlo?	¿Cómo compartirlo?
TLP: RED	Cuando la información está limitada a personas concretas, y podría tener impacto en la privacidad, reputación u operaciones si es mal utilizada.	Los receptores no deben compartir información designada como **TLP:RED** con ningún tercero fuera del ámbito donde fue expuesta originalmente.
TLP: AMBER	Cuando la información requiere ser distribuida de forma limitada, pero supone un riesgo para la privacidad, reputación u operaciones si es compartida fuera de la organización.	Los receptores pueden compartir información indicada como **TLP:AMBER** únicamente con miembros de su propia organización que necesitan conocerla, y con clientes, proveedores o asociados que necesitan conocerla para protegerse a sí mismos o evitar daños. El emisor puede especificar restricciones adicionales para compartir esta información.
TLP: GREEN	Cuando la información es útil para todas las organizaciones que participan, así como con terceros de la comunidad o el sector.	Los receptores pueden compartir la información indicada como **TLP:GREEN** con organizaciones afiliadas o miembros del mismo sector, pero nunca a través de canales públicos.
TLP: WHITE	Se debe utilizar **TLP:WHITE** cuando la información no supone ningún riesgo de mal uso, dentro de las reglas y procedimientos establecidos para su difusión pública.	La información **TLP:WHITE** puede ser distribuida sin restricciones, sujeta a controles de Copyright.

Referencia

CSIRTAmericas.org

CSIRTAmericas.org

Plataforma tecnólogica

Consolidar una comunidad operativa en las Américas

Sección: Comunidad

Promover el intercambio de información de alertas de seguridad

Sección: Intercambio de Información

CSIRTAmericas.org

Participantes activos:

16 Países

66 Participantes

- Argentina
- Bolivia
- Chile
- Colombia
- Costa Rica
- Ecuador
- Guatemala
- Guyana
- Jamaica
- México
- Panamá
- Paraguay
- Perú
- Suriname
- Trinidad y Tobago
- Uruguay

Conformado por:

18 CSIRTs

- 15 Nacionales
- 1 Militar
- 1 Gobierno
- 1 Académico

+ 80

Procedimientos, scritps, manuales, reportes.

+ 3500

Alertas enviadas directamente a los CSIRTs

CSIRT Americas.org

Sección: Comunidad

CSIRTAmericas.org

Sección: Comunidad

Chat

Foro

CSIRTs News

Librería

Directorio

Lista de Distribución

Secure | https://sslvpn.csirtamericas.org/index.php/intro/home2

CSIRTamericas.org | Member states | Services | Partners | About | Logout dsubero

ideas and experiences. presentations, scripts CSIRTs.

Admin Announcements: Actualizacion

Priority Message

Send email to all csirtamericas members.

Early Warnings

Alerts, real-time, regional trends.

Latest Forum Posts

Análisis estático de PDF maliciosos + bo...
In Main Forum / Security Audit, Assessments and Artifact Analysis
1 month 4 days ago

Análisis de la amenaza BadRabbit
In Main Forum / Security Audit, Assessments and Artifact Analysis

CSIRTs Latest News

OAS_Team
IMPORTANTE!!! - SOLICITUD DE APOYO TÉCNICO A LA VIII CUMBRE DE JEFES DE ESTADO DE LAS AMÉRICAS
Created on Friday, 06 April 2018 15:07
Estimados Miembros de la Red CSIRT Americas, En nombre de la Secretaría del Com...
Read more

OAS_Team
SUMMERBC18 - CSIRTAMERICAS INFO!!
Created on Thursday, 15 March 2018 21:02
Plazo de registro para el Cybersecurity Summer Bootcamp 2018 que se realizará de...
Read more

Latest Documents

Webinar 1: DDOS - Feb 14 - ES
In Presentations & Courses
14 February 2018 • 5 downloads

Monthly report November 2017
Popular
In csirtamericas reports
05 December 2017 • 9 downloads

Monthly report October 2017
In csirtamericas reports
22 November 2017 • 2 downloads

Monthly report September 2017
In csirtamericas reports
22 November 2017

Tools & Scripts

Chat
Diego Subero
OAS Team
Search people
Fabian Navarrete
Chatting here first time
Luis Martinez
Chatting here first time
Moniphia Hewling
CIRT-JM

Moniphia Hewling | Luis Martinez

Resultados

Sección: Comunidad

CSIRTAmericas.org

Sección: Comunidad

Abril 2018

Cyber
Más derechos para más gente

OAS Cyber Team

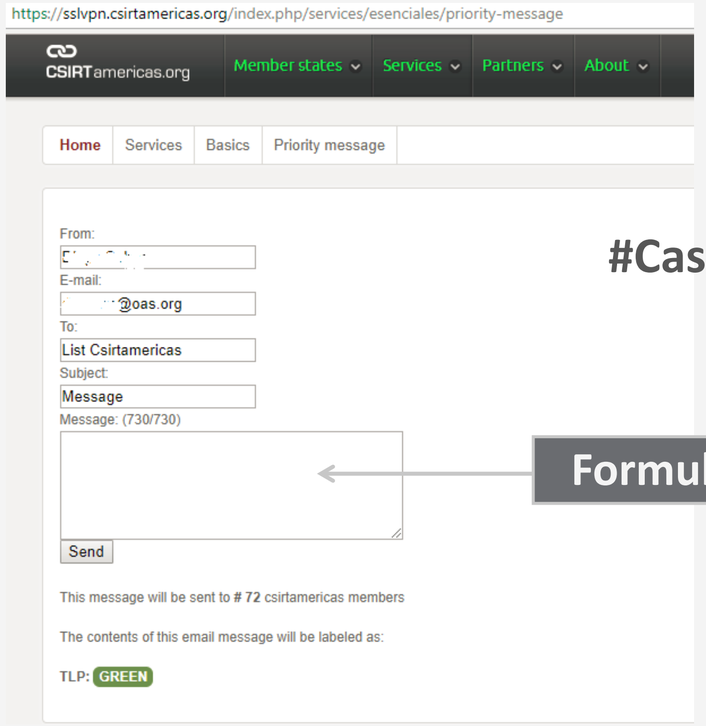
Canales de Comunicación

Lista de Distribución

Niveles de diseminación

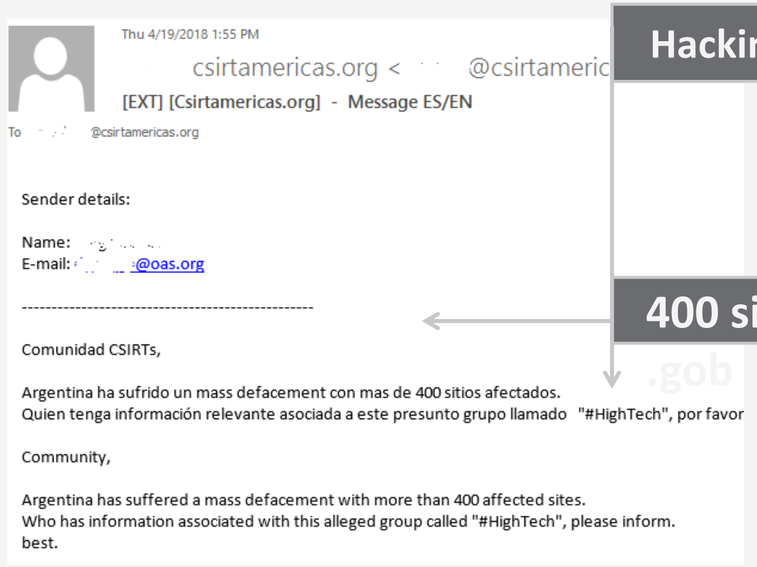
Traffic light protocol (TLP):

- Red
- Amber
- Green
- White



#Caso_Argentina

Formulario Web



Hacking group

400 sitios

CSIRTAmericas.org

Sección: Comunidad

2018 Abril

Chile

Canales de Comunicación

Lista de Distribución

Niveles de Diseminación

Traffic light protocol (TLP):

- Red
- Amber
- Green
- White

RCE - Drupal

CVE-2018-7600

Email official & nombre

Thu 4/19/2018 3:32 PM

csirtamericas.org < @csirtamericas.org>

[EXT] [Csirtamericas.org] - Message

To @csirtamericas.org

Sender details:

Name:

E-mail: gob.cl

Boletín de Seguridad Altamente Critica CMS Drupal versión 6.x 7.x 8.x

Se ha detectado una vulnerabilidad que permite ejecutar código remoto arbitrario sin autentificación prev
un atacante efectuar varios vectores de ataque con el fin de tomar el control de un sitio Web Drupal por co

Se debe actualizar inmediatamente a una versión de Drupal segura.

CVE Vulnerabilidad de Drupal:

CVE-2018-7600 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-7600

https://github.com/pimps/CVE-2018-7600 (validar vulnerabilidad)

This message was sent to # 74 csirtamericas members

TLP: GREEN | Please DO NOT replay to this email | Email disclaimer: visit csirtamericas.org

74 miembros | TLP:green

CSIRTAmericas.org

Sección: Comunidad

May 2018

ColCERT

Canales de Comunicación

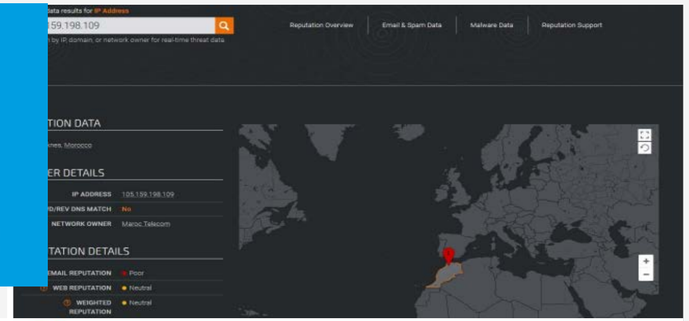
Forum

Distribution List

Niveles de Diseminación

Traffic light protocol (TLP):

- Red
- Amber
- Green
- White



MINDEFENSA

TODOS POR UN NUEVO PAÍS
PAZ EQUIDAD EDUCACIÓN

colCERT

CVE-2018-7600

Official email & name

RCE - Drupal

Explotación masiva de Drupal a través de herramienta "Drupalgeddon"

Mayo 08 de 2018

Introducción:

El 28 de marzo de 2018, se lanzó un parche para una vulnerabilidad altamente crítica, que facilita la ejecución remota de código contra el sistema de gestión de contenido Drupal. La vulnerabilidad fue identificada por Jasper Mattson de Druid y está cubierta por SA-2018-002 y CVE-2018-7600. Antes del lanzamiento del parche, Drupal había avisado con anticipación de su inminente liberación y las posibles consecuencias relacionadas

Tue 5/8/2018 2:38 PM

csirtamericas.org <[redacted]@csirtamericas.org>

[EXT] [Csirtamericas.org] - Explotación masiva de Drupal ("Drupalgeddon")

To members@csirtamericas.org

Custom Technical report

Sender details:

Name: [redacted]
E-mail: [redacted]

Comparto con ustedes esta información importante:

https://[redacted].csirtamericas.org/index.php/services/esenciales/foro/gestion-de-incidentes/50-explotacion-masiva-de-drupal-drupalgeddon#127

This message was sent to # 72 csirtamericas members

TLP: GREEN | Please DO NOT replay to this email | Email disclaimer: visit csirtamericas.org

CSIRTAmericas.org

Sección: Comunidad

Mayo 2017

Cyber
Más derechos para más gente

OAS Cyber Team

Canales de Comunicación

Lista de distribución

Niveles de Diseminación

Traffic light protocol (TLP):

- Red
- Amber
- Green
- White

INFORMACIÓN GENERAL

Notificación general
a los CSIRTs de la red por el incidente de una empresa de telecomunicaciones

14 países **56** personas

Búsqueda d
de primera n
aliados inter

Microsof

Análisis pri
de documer

Se reportar
(distribución d
CSIRTAmeric

CSIRTS EN ACCIÓN

CSIRTGob.cl compartió C&C y clientes con actividad maliciosa (ransomware #WannaCry).

TTCSIRT desarrolló un script para buscar hits en redes internas de las IPs maliciosas compartidas por CSIRTGov.

ColCERT compartió un boletín restringido de análisis de una muestra del #WannaCry.

Operativo WannaCry

CSIRT Americas.org

Sección: Intercambio de Información

CSIRTAmericas – Taxonomía Propuesta

Taxonomía seleccionada para

CSIRTAmericas.org

Defacement
Malware
DDOS
Phishing
Spam
Botnet
Fastflux
Cryptojacking
XSS
SQL Injection
Vulnerability
Information leak
System compromise
Other

CSIRTAmericas.org

Sección: Intercambio de Información

- Defacements
  - Zone-h 20MIN
    - Defacements
      - yyyymmdd-defacements-cc.csv
- DDoS
  - Arbor 24H
    - Inbound
      - yyyymmdd-inbound_ddos-cc.csv
    - Outbound
      - yyyymmdd-outbound_ddos-cc.csv
- Phishing_and_spam
  - Arbor 24H
    - phishing_servers
      - yyyymmdd-phishing_servers-cc.csv

ALERTS

7 main categories

- Main Category
  - Provider
    - Provider format
      - CSV file

- Botnets
  - Arbor 24H
    - Observed_attack_commands
      - yyyymmdd-observed_attack_commands-cc.csv
    - Malicious_servers
      - yyyymmdd-malicious_servers-cc.csv
- Malware
  - Arbor 24H
    - Malicious_links
      - yyyymmdd-malicious_links-cc.csv
    - Malicious_clients
      - yyyymmdd-malicious_clients-cc.csv
    - Ftp_servers
      - yyyymmdd-ftp_servers-cc.csv
    - Scans
      - yyyymmdd-scans-cc.csv
- Fast_flux
  - Arbor 24H
    - Fast_flux
      - yyyymmdd-fast_flux-cc.csv
- ICS-Scada IN PROCESS
  - Shodan
    - yyyymmdd-ics-scada-cc.csv

Algunos Proveedores

Defacement

zone-h unrestricted information

DDOS

ARBOR NETWORKS
The Security Division of NETSCOUT

Botnets

SHODAN

BAD PACKETS REPORT
Research regarding cryptojacking, botnets, network abuse, and other security topics.

ARBOR NETWORKS
The Security Division of NETSCOUT

Malware

ARBOR NETWORKS
The Security Division of NETSCOUT

Phishing

PhishTank

Cryptojacking

publicWWW

ICS/SCADA

SHODAN

Info leak

En proceso

XSS

En proceso

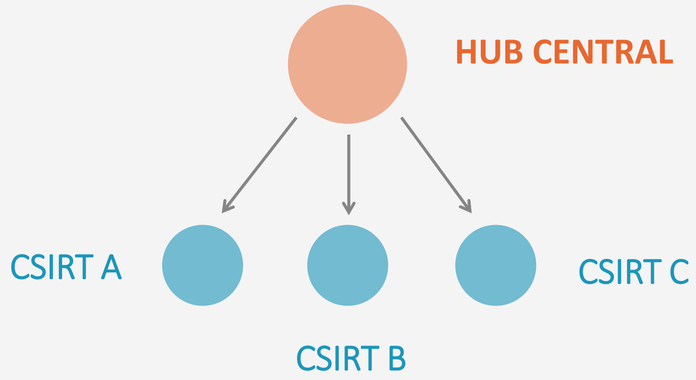
Vulnerabilities

En proceso

CSIRTAmericas.org

Sección: Intercambio de Información | Early Warning Service

Early warning



Indicador por País 24/7

- DDOS
- Botnet
- Malware
- Phishing
- Criptojacking

Tendencias Subregionales 24/7

- Trending report

Beneficios para CSIRTs / LEAs

FORMAT

CSV

FREQUENCY

Daily
Every: 20 minutes

DELIVERY METHOD

FTP Server

(Ftp.Csirtamericas.org)
Restricted access

CURRENT BENEFICIARIES

Algunos proveedores

zone-h unrestricted information

ARBOR NETWORKS
The Security Division of NETSCOUT

SHODAN

BAD PACKETS REPORT
Research regarding cryptojacking, botnets, network abuse, and other security topics.

publicWWW

Resultados

Sección: Intercambio de Información

CSIRTAmericas.org

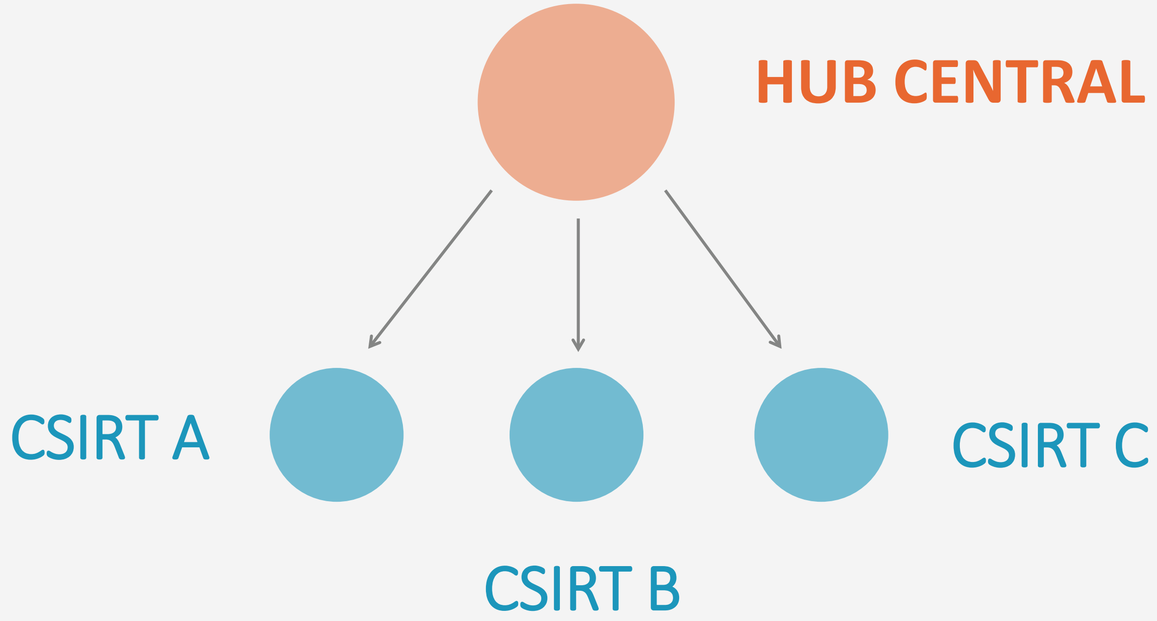
Intercambio de Información

Early Warning System

Resultados de Alertas de Intercambio de Información

Alertas Tempranas

Alertas Tempranas



Entregas de feeds 24/7

CSIRTAmericas.org

Intercambio de Información

Early Warning System

Individual CSIRT

Nivel 2

```
2018-04-29 07:06:57,B0c4H_Id30T,http://secyt-test.psi...edu.../you.htm,,,,Heh..
2018-04-29 07:06:58,B0c4H_Id30T,http://siges.p...edu.../you.htm,,,,Heh...just
2018-04-29 07:06:58,B0c4H_Id30T,http://sinarame...edu.../you.htm,,,,Heh...j
2018-04-29 07:06:59,B0c4H_Id30T,http://sistemas.secyt...edu.../you.htm,,,,Heh..
2018-04-29 07:07:00,B0c4H_Id30T,http://squid-repo...edu.ar/you.htm,,,,Heh
2018-04-29 07:07:00,B0c4H_Id30T,http://ticket...edu.ar/you.htm,,,,Heh...j
```

Defacement file example -cc

```
50:24;gru...;>30M;CoinHive
50:24;juegos...blogspot...;>30M;CoinHive
50:24;herfa...;>30M;CoinHive
50:24;que-cosas.blogspot.com...;>30M;CoinHive
50:24;super-pelis-online.blogspot.com...;>30M;CoinHive
50:24;perezsan...;>30M;CoinHive
50:34;diariolacuenca.cc...3528364;mineralt
50:34;revistafotoptica.cor...;12809874;mineralt
50:34;palaciopaz...;13032279;mineralt
50:34;seri...;>30M;mineralt
50:34;librosen...;>30M;mineralt
50:34;r...blogspot.com...;>30M;mineralt
50:40;para...;267034;CoinHive_obfuscated
50:40;packpara*doom...;275380;CoinHive_obfuscated
50:40;zonadjsgroupra...ogspot.cc...358252;CoinHive_obfuscated
50:40;saltaal...;364161;CoinHive_obfuscated
```

Cryptojacking - cc

```
File  Edit  Format  View  Help
MALICIOUS SERVERS
Botnet C&C Servers
Based on malicious software analysis and botnet tracking.
CC, ASN, IP, port, malware MD5
...216,157,c80b06b530a5be6b63bd4eee1fc98ace
...6,157,6dec686afcc901675be262986f100cd7
...6,157,52bcb77a9e33f90f737c88bef779fd36
...6,157,ea299c52dbb01ea482543c78bf2ccca6
...6,157,f871cdd4de91694422693586906f3db1
...6,157,6fc72407a8f07ed096be1b7a0891f3b8
...6,157,511068b55175f21b153d467190742ca1
...6,157,60f8f7e0083ade195ca15ccd49263425
...6,157,f93be44fa823cf6f76030239daa010a3
...6,157,0c010f3a9ded8abbe5454ca7d257860f
...6,157,8257bc535ffd2f6f9d800566699abeed
...6,157,33d70177d30a0b7a1580940416bed81f
...16,157,89ed964b81cd58acff938e9708c25dde
...6,157,4a88e51c2148394a2596091370fc6ccb
...6,157,779967b46019ae975ed01785253699a4
...6,157,de395e3c9debe3a9813a864d927d3fbd
...6,157,8f119152733e2f352d418f3fce4923fb
...6,157,c38c8a7d12cc1710c2b43a19f68b389f
...6,157,f995c6d01412db60999eda333f408868
```

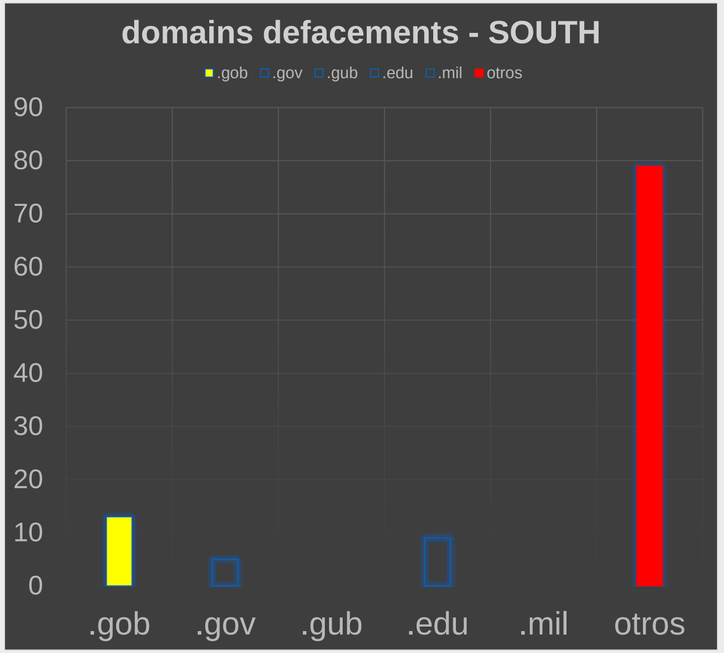
Malicious servers - cc

CSIRTAmericas.org

Intercambio de Información

Early Warning System

Sub-regional




```
Current month: May

Date: 05/09/2018 07:58:01 PM UTC

#  South America total Defacements per month - validated state | 9 OAS member states - ve|py|cl|bo|cc

# South America  --> Total defaced sites: 106

  + Domains Affected in South America

  .gob: 13 (12%)|  .gov: 5 (4%)|  .gub: 0 (0%)|  .edu: 9 (8%)|  .mil: 0 (0%)|


# South America TOP 7 attackers
     10 TeaM_CC
      9 SAHARA H4xOR
      9 008
      8 ErrOr SquaD
      6 X-Force Cyber Army
      6 Hunter Hassam
      5 Mister Spy

# South America  TOP 7 Common paths in affected
      9 root.html
      7 Box.html
      6 r00t.html
      5 mnm.php
      3 vuln.htm
      3 spy.html
      3 nr.php

# South America   TOP 7 Common methods (subjetiv
     53 known vulnerability (i.e. unpatched syst
     12 SQL Injection
     11 Not available
```

May 9

.gob (12%) - .gov 4%

South region file

```
# South America   TOP 7 Common methods (subjetive)
     53 known vulnerability (i.e. unpatched system)
     12 SQL Injection
     11 Not available
     10 URL Poisoning
      7 Other Web Application bug
      4 Web Server intrusion
      2 undisclosed (new) vulnerability

# South America  TOP 7 Webserver affected
     71 Apache
     17 nginx
     14 Unknown
      1 8.5
      1 8.0
      1 7.5
```

Mnm.php | root.hmtl

Region Sur | Reporte de tendencia

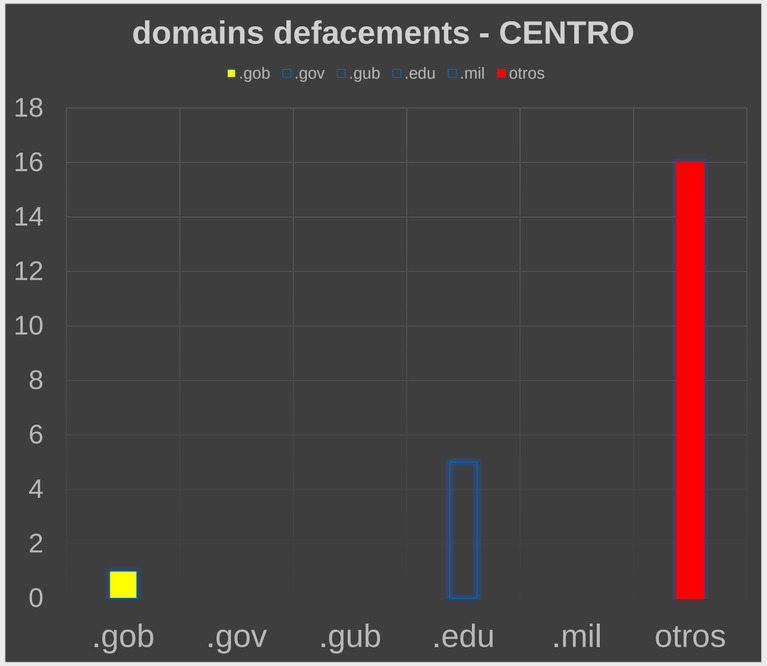
Nivel 2

CSIRTAmericas.org

Intercambio de Información

Early Warning System

Sub-regional




```
Current month: May

Date: 05/09/2018 07:58:02 PM UTC

#  Central America total Defacements per month - validated state | 9 OAS member states - cr|pa|gt|do|ni|s

# Central America  --> Total defaced sites: 22

 + Domains Affected in Central America

 .gob: 1 (4%)|  .gov: 0 (0%)|  .gub: 0 (0%)|  .edu: 5 (22%)|  .mil: 0 (0%)|


# Central America TOP 7 attackers
      5 Mr-Cakil
      5 BlackWeb
      4 Gse7en
      2 ./SahaainG/.
      2 bl4ck_cod3
      1 TeaM_CC
      1 p0r7s

# Central America  TOP 7 Common paths in affected websites (Certain types of patterns are excluded)
      5 example.sites.php
      5 dead.html
      2 eue.html
      2 coder.html
      1 update.php
      1 hc.php
      1 h0d3.html
```

Blackweb

Centro region file

```
# Central America   TOP 7 Common methods (subjetive)
     17 known vulnerability (i.e. unpatched system)
      5 File Inclusion

# Central America  TOP 7 Webserver affected
     14 Apache
      6 nginx
      2 8.5
```

Dead.html example.

Region Central | Reporte de tendencia

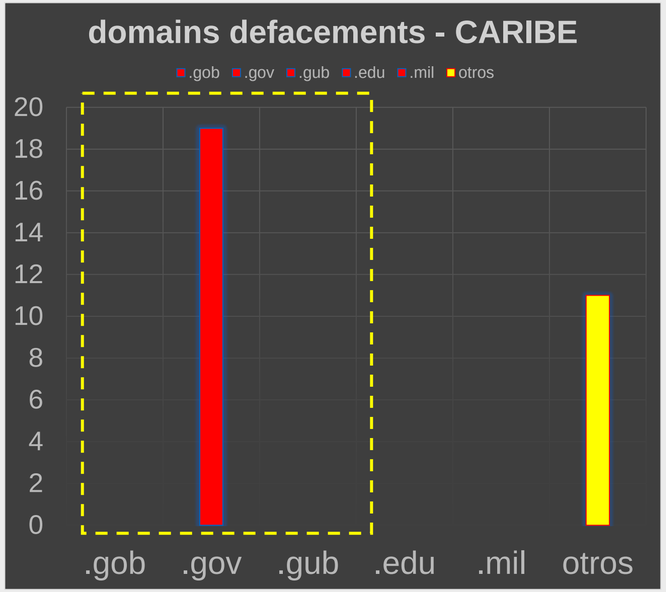
Nivel 2

CSIRTAmericas.org

Intercambio de Información

Early Warning System

Sub-regional




```
Current month: May

Date: 05/09/2018 11:58:02 PM UTC

#  Caribbean Region total Defacements per month - validated state | 13 OAS member states - gy|tt|jm|sr|ag|bb|dm|gd|ht|kn|lc|vc|bs

# Caribbean Region  --> Total defaced sites: 30

  + Domains Affected in Caribbean Region

  .gob: 0 (0%)|  .gov: 19 (63%)|  .gub: 0 (0%)|  .edu: 0 (0%)|  .mil: 0 (0%)|


# Caribbean Region TOP 7 attackers
     29 BALA SNIPER
      1 ZoRRoKiN

# Caribbean Region  TOP 7 Common paths in affected websites (Certain types of patterns are excluded)
      1 firehackturk-1525804867

# Caribbean Region   TOP 7 Common methods (subjetive)
     29 File Inclusion
      1 undisclosed (new) vulnerability

# Caribbean Region  TOP 7 Webserver affected
     29 Apache
      1 Unknown
```

May 9

.gov sites (63%)

Bala sniper

Caribbean region file

Attention!

```
kn: 30 total
   .gob: 0 - (0%)
   .gov: 19 - (63%)
   .gub: 0 - (0%)
   .edu: 0 - (0%)
   .mil: 0 - (0%)
```

Region Caribe | Reporte de tendencia

Nivel 2

CSIRTAmericas.org

Intercambio de Información

Early Warning System

Regional

Nivel 4

Caso de studio Regional

def_south_201804 - Notepad

File Edit Format View Help

```
Current month: April

Date: 04/30/2018 11:58:01 PM UTC

#  South America total Defacements per month - validated state | 9 OAS member states - ve|py|cl|bo|co|ec|uy|pe|ar

# South America  --> Total defaced sites: 1376

  + Domains Affected in South America

  .gob: 460 (33%)|  .gov: 48 (3%)|  .gub: 0 (0%)|  .edu: 141 (10%)|  .mil: 1 (0%)|


# South America TOP 7 attackers
    421 HighTech
    125 Electronic Thunderbolt Team
    113 3xp1r3
     57 TheMario
     57 SatTaR
     47 RxR
     35 Santi boy
```

Subregional trending South

.gob 460 sites

Attacker

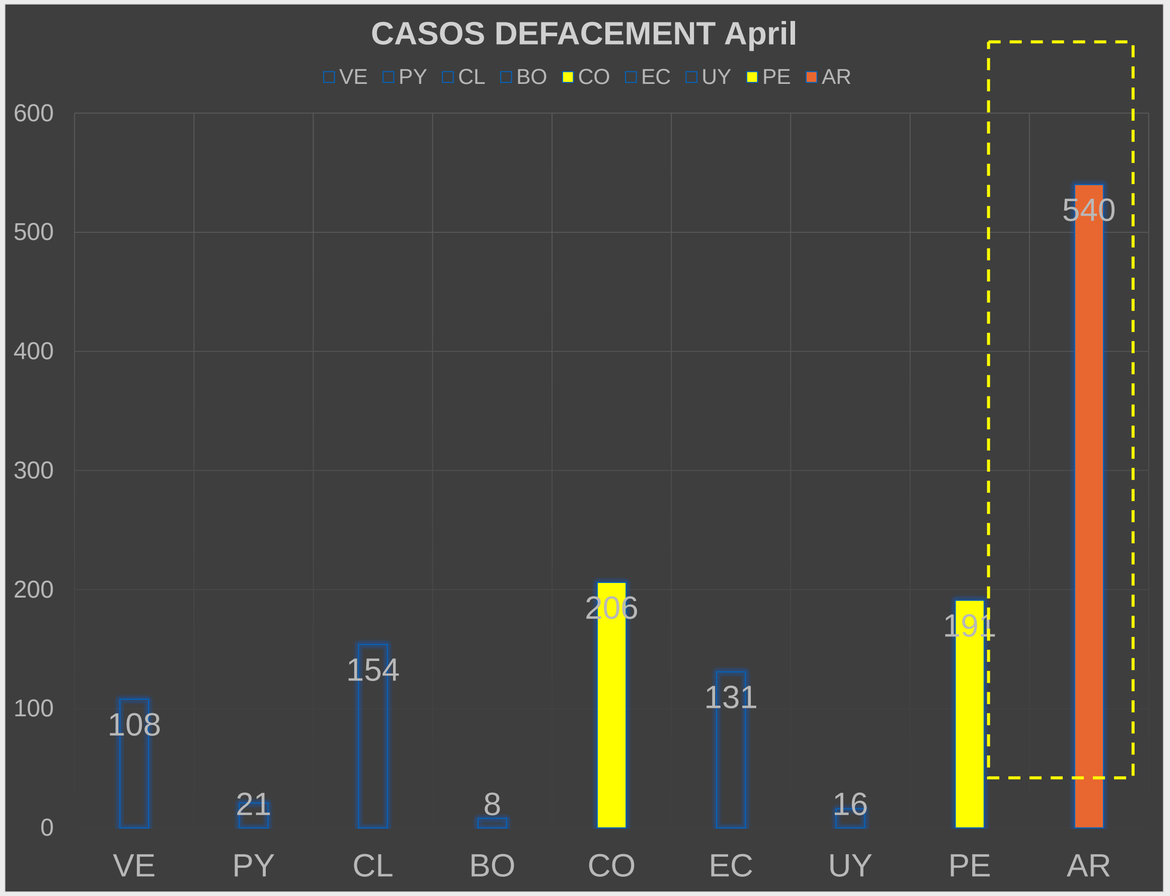
Nivel 2

CSIRTAmericas.org

Sección: Intercambio de Información | Early Warning System

April 2018

Defacement en Argentina




```
ar: 540 total
  .gob: 405 - (75%)
  .gov: 19 - (3%)
  .gub: 0 - (0%)
  .edu: 12 - (2%)
  .mil: 0 - (0%)
```

```
pe: 191 total
  .gob: 27 - (14%)
  .gov: 0 - (0%)
  .gub: 0 - (0%)
  .edu: 10 - (5%)
  .mil: 0 - (0%)
```

```
ve: 108 total
  .gob: 5 - (4%)
  .gov: 0 - (0%)
  .gub: 0 - (0%)
  .edu: 0 - (0%)
  .mil: 0 - (0%)
```

```
cl: 154 total
  .gob: 1 - (0%)
  .gov: 0 - (0%)
  .gub: 0 - (0%)
  .edu: 0 - (0%)
  .mil: 0 - (0%)
```

```
ar total: 466 -> gob|gov|gub|mil: 405 (86%)

# TOP 7 attackers - ar
    416 HighTech
      8 ByMechaclaw
      6 B0c4H_Id30T
      4 RxR
      4 BALA SNIPER
      3 Mr.ToKeiChun69
      2 ZoRRoKiN

# TOP 7 Common paths in affected websites (Certain types of
patterns are excluded) - ar
      6 bc.php
      5 mechaclaw.html
      4 sniper.txt
      4 null.php
      3 readthis.html
      2 eg.php
      1 toch.txt

# TOP 7 Common methods (subjetive) - ar
    415 social engineering
     16 known vulnerability (i.e. unpatched system)
     11 SQL Injection
      7 Other Server intrusion
      6 Web Server intrusion
      4 File Inclusion
      2 Not available

# TOP 7 Webserver affected -  ar
    454 Apache
      5 Unknown
      3 nginx
      2 8.5
      1 LiteSpeed
      1 7.5
```

Nivel 2

CSIRT Americas org’s **future**

Incrementar Fuentes de informacion de alertas

Integración con equipos de FCSE

Mejorar documentación y experiencia de Usuario

Incluir mapa de tiempo real

Creación de working groups

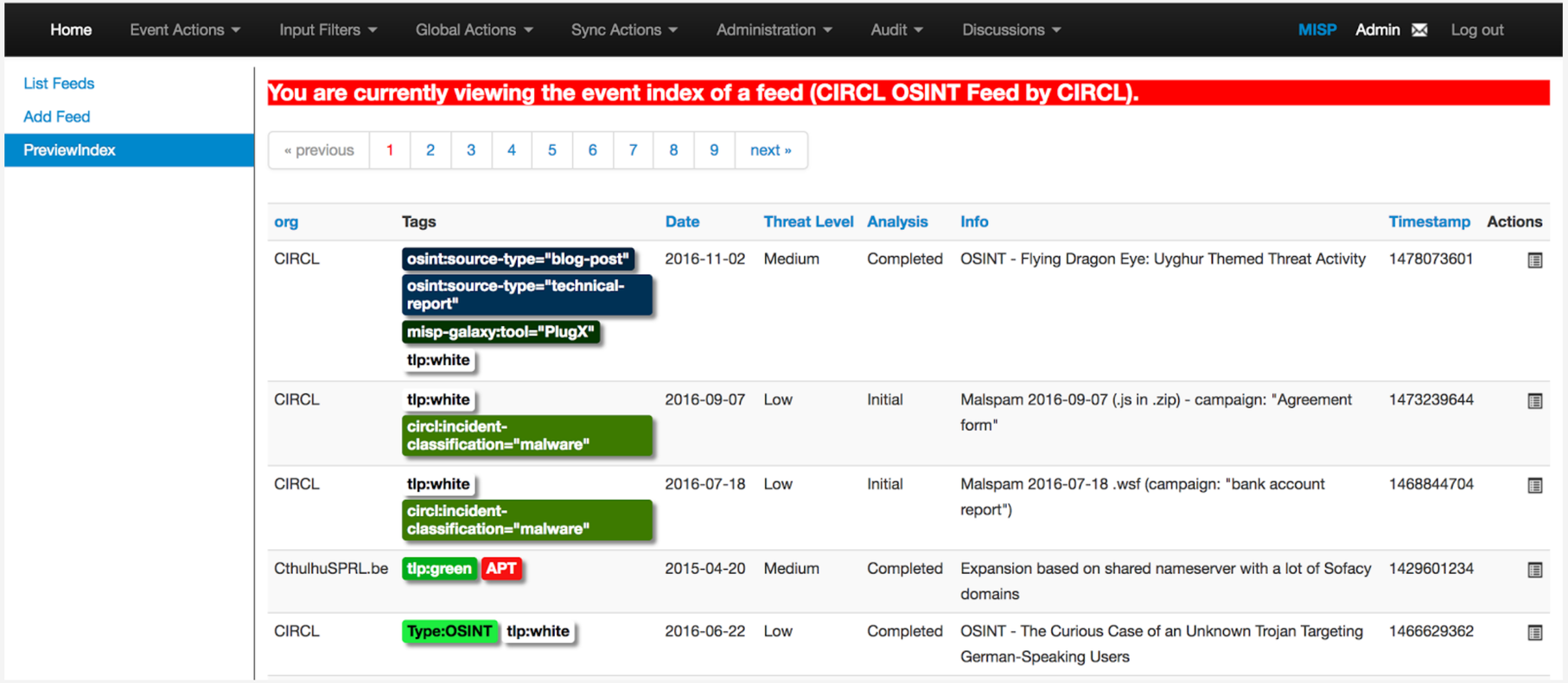
Example:

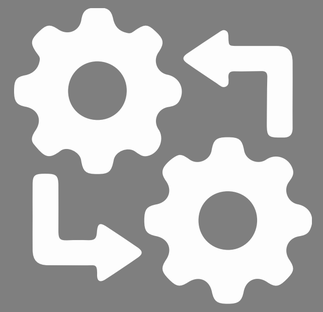
MISP

HIVE

Pentesting

MISP
Threat Sharing





Working group:
Ticket tracking system

Found 3,887 tickets

New ticket in Testing | Search...

Edit Search | Advanced | Show Results | Bulk Update | Chart | Feeds

#	Subject Requestor	Status Created	Queue Told	Owner Last Updated	Priority Time Left
26518	**Double-encoding with Encode > 2.52** <maayant@qbalitech.net>, <mail@psvlan.com>	open 3 days ago	rt3 3 days ago	Nobody in particular 3 days ago	50
26502	**RT should not assume that indexes are in the 'public' schema** "Brian Almeida" <bma@thunderkeys.net>	open 3 days ago	rt3 3 days ago	Nobody in particular 3 days ago	50
26447	RT 4.2.0rc4 pie chart label encoding Loos, Christian <CLoos@netcologne.de>	resolved 7 days ago	rt3 6 days ago	Nobody in particular 6 days ago	50
26429	**rt-4.2.0rc3 make testdeps error if there are missing dependencies** Loos, Christian <CLoos@netcologne.de>	resolved 8 days ago	rt3 7 days ago	Nobody in particular 7 days ago	50
26416	**MarkAsSeen not available in self service** todd (Todd Wade)	new 8 days ago	rt3	todd (Todd Wade) 8 days ago	50
26407	**Merging into yourself says "Merge Successful" but errors (4.2)** alexmv (Alex Vandiver)	new 9 days ago	rt3	Nobody in particular 9 days ago	50
26369	**History display on 4.2 rudder is not styled like 4.0 rudder** alexmv (Alex Vandiver)	resolved 10 days ago	rt3 9 days ago	jesse (Jesse Vincent) 9 days ago	50
26368	**Self-service CF grouping titles are mis-colored** alexmv (Alex Vandiver)	resolved 10 days ago	rt3 9 days ago	jesse (Jesse Vincent) 9 days ago	50
26300	**rt-mailgate MailPlugins docs are outdated**	new 14 days ago	rt3	Nobody in particular 14 days ago	50
26299	**RT 4.2.1 Release**	new 14 days ago	rt3	Nobody in particular 14 days ago	50
26274	**rt-setup-database --action create,acl errors out**	resolved 2 weeks ago	rt3	Nobody in particular 13 days ago	50
26114	**Fwd: Scrip "too fast" or dirty read from db or what?** BÁLINT Bekény <balint.bekeny@docca.hu>	rejected 3 weeks ago	rt3 3 weeks ago	Nobody in particular 3 weeks ago	50
26103	**Custom field grouping partially implemented for Self Service** jbrandt (Jim Brandt)	open 3 weeks ago	rt3 14 days ago	Nobody in particular 14 days ago	50
26096	etc/upgrade/4.1.23 drop failures	resolved 3 weeks ago	rt3	ruz (Ruslan U. Zakirov) 13 days ago	50
25977	Custom RT theme not picked up in rudder title bar	resolved	rt3	jesse (Jesse Vincent)	50

A 3-IN-1 SECURITY INCIDENT RESPONSE PLATFORM

A scalable, open source and free Security Incident Response Platform, tightly integrated with MISP (Malware Information Sharing Platform), designed to make life easier for SOCs, CSIRTs, CERTs and any information security practitioner dealing with security incidents that need to be investigated and acted upon swiftly.

GITHUB DOCUMENTATION

Face-to-face Meeting

CSIRTAmericas.org

Se aceptan sugerencias!

Thank you!
Merci
Gracias
Obrigado

Cyber Team

OAS Cybersecurity Program
Organization of American States

cybersecurity@oas.org

@OEA_Cyber