PRESIDENCIA DE LA
REPÚBLICA DOMINICANA

MINISTERIO DE LA PRESIDENCIA

Boletín Mensual

Abril 2021

CNCS CENTRO NACIONAL DE CIBERSEGURIDAD REPÚBLICA DOMINICANA

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

CSIRTamericas.org

FIRST

1. Situación en el ciberespacio de República Dominicana

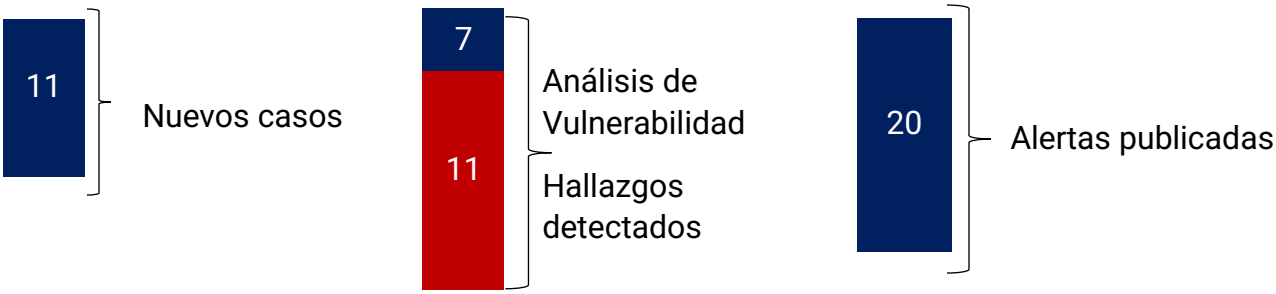
Como parte de las labores del Centro Nacional de Ciberseguridad de salvaguardar el ciberespacio dominicano, ha atendido a través del Equipo Nacional de Respuestas a Incidentes Cibernéticos CSIRT-RD once (**11)** incidentes, los cuales han sido corregidos apoyando la operabilidad de las entidades afectadas.

De igual manera se han realizado análisis a los servicios de la comunidad atendida identificando un total de 11 vulnerabilidades en servicios de institucionales ofrecidos en línea.

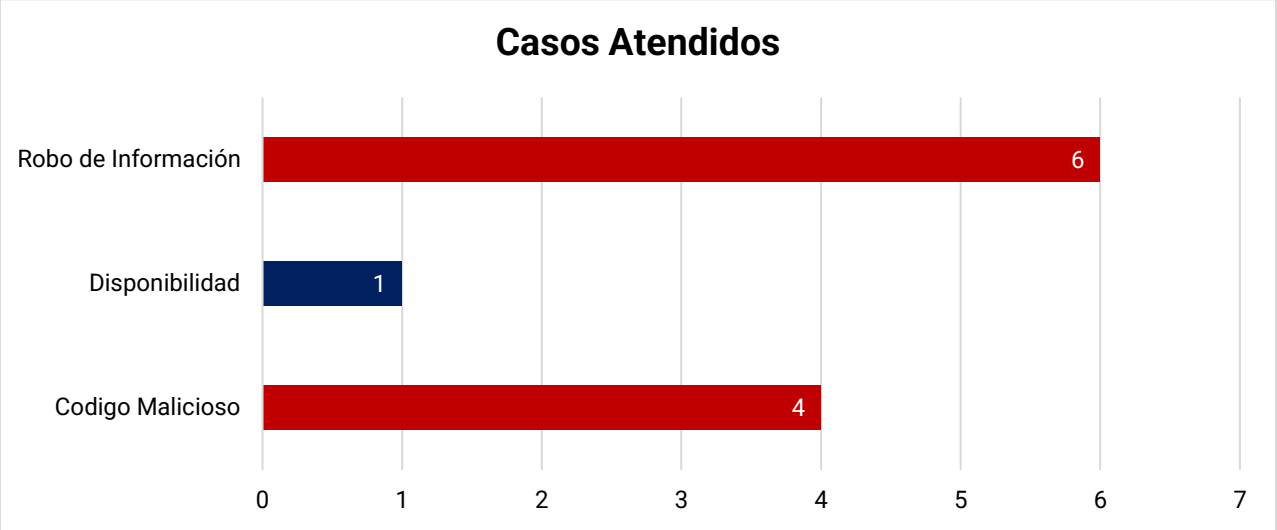
Con el compromiso de mantener alerta e informada a la comunidad atendida, el Centro Nacional de Ciberseguridad a través del CSIRT-RD ha publicado alertas de seguridad para que las mismas puedan realizar acciones preventivas ante exposiciones.

El CSIRT-RD realiza el monitoreo del ciberespacio dominicano de distintos indicadores, durante el mes de abril destacan la identificación de explotación de servicios vulnerables al CVE-2018-13379 relacionado al servicio SSL-VPN de Fortinet.

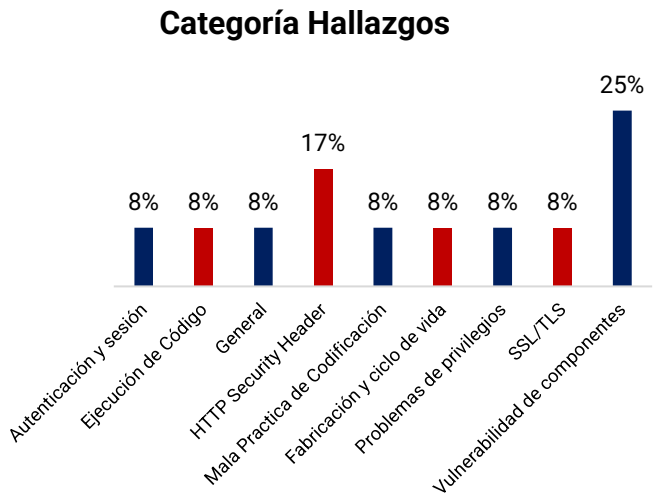
Resumen de los registros del Equipo Nacional de Respuestas a Incidentes Cibernéticos (CSIRT-RD) durante el mes de abril 2021:



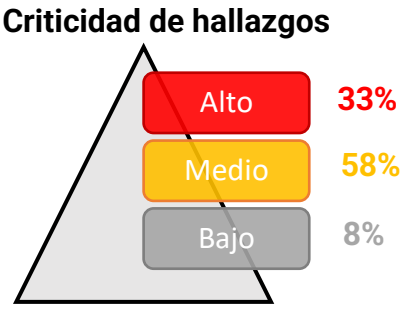
2. Categoría de casos atendidos por el CSIRT



3. Análisis de Vulnerabilidades



El CSIRT-RD realizó análisis de vulnerabilidades de los servicios en línea, identificando las principales vulnerabilidades en la comunidad atendida.



Vulnerabilidad SSL-VPN Fortinet.

El CSIRT-RD realizó la identificación de los hosts vulnerables al CVE-2018-13379 que afecta el servicio SSL-VPN de Fortinet en las versiones FortiOS 6.0 - 6.0.0 al 6.0.4, FortiOS 5.6 - 5.6.3 al 5.6.7 y FortiOS 5.4 - 5.4.6 al 5.4.12.

El Equipo Nacional de Respuesta a Incidentes identificó 14 organizaciones públicas y privadas vulnerables a la amenaza, realizando la notificación oportuna y seguimiento a las remediaciones realizadas en la comunidad atendida.

4. Alertas de Seguridad Emitidas

- FBI advierte que grupos de hacking explotan activamente multiples vulnerabilidades de Fortinet.
- Vulnerabilidad Critica en Aruba Instant Access Point (IAP)
- Ejecución de Código Arbitrario en Routers Cisco Small Business
- Actualización de Seguridad Del DSM (Diskstation Manager) En NAS De Synology.
- Vulnerabilidad de Dia Zero de Google Chrome y Microsoft Edge permite la Ejecución de Código Remoto en Twitter.
- Falla de whatsapp permite bloquear cualquier cuenta.
- Actualizaciones de seguridad de Microsoft para abril 2021
- Actualización de seguridad de Joomla 3.9.26.
- Multiples vulnerabilidades en Adobe Suite
- Boletin de actualizaciones Junos OS: PTX series, QFX series de la familia Juniper
- Vulnerabilidad de kernel Panic en Juniper Junos OS
- Multiples vulnerabilidades en productos Mozilla
- Bug ataques man in the disk en Whatsapp
- Ransomware aprovechan debildiades de VMWARE ESXI
- Aviso de actualizaciones críticas de seguridad en productos Oracle
- Google corrige multiples vulnerabilidades en Google Chrome
- Vulnerabilidad crítica en Drupal
- Explotación activa de las vulnerabilidades en NAS de QNAP
- Google anuncia nuevas actualizaciones para Google Chrome
- Múltiples vulnerabilidades en productos Cisco

5. Monitoreo del Ciberespacio Dominicano

Monitoreo de Indicadores de Amenaza de los servicios tecnológicos publicados a internet. Relación de evolución de total de eventos y cantidad de direcciones IP comprometidas.

BOTNET

Tráfico de código malicioso (Botnet) | enero – abril 2021

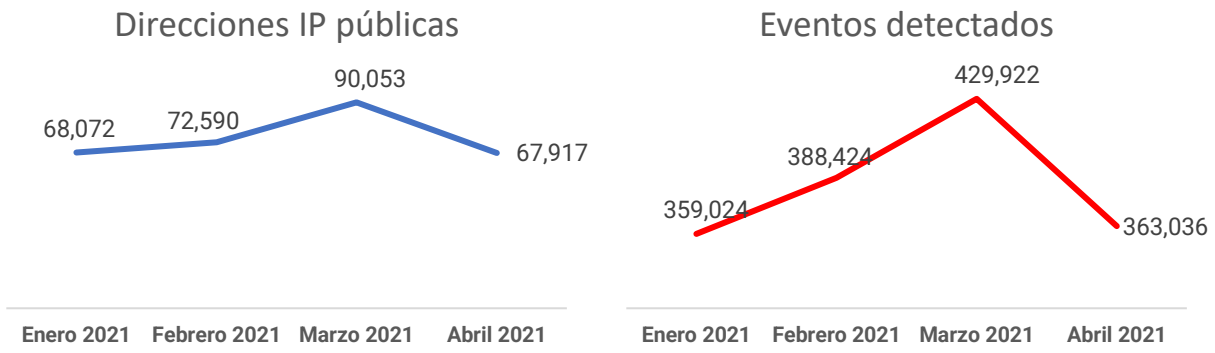
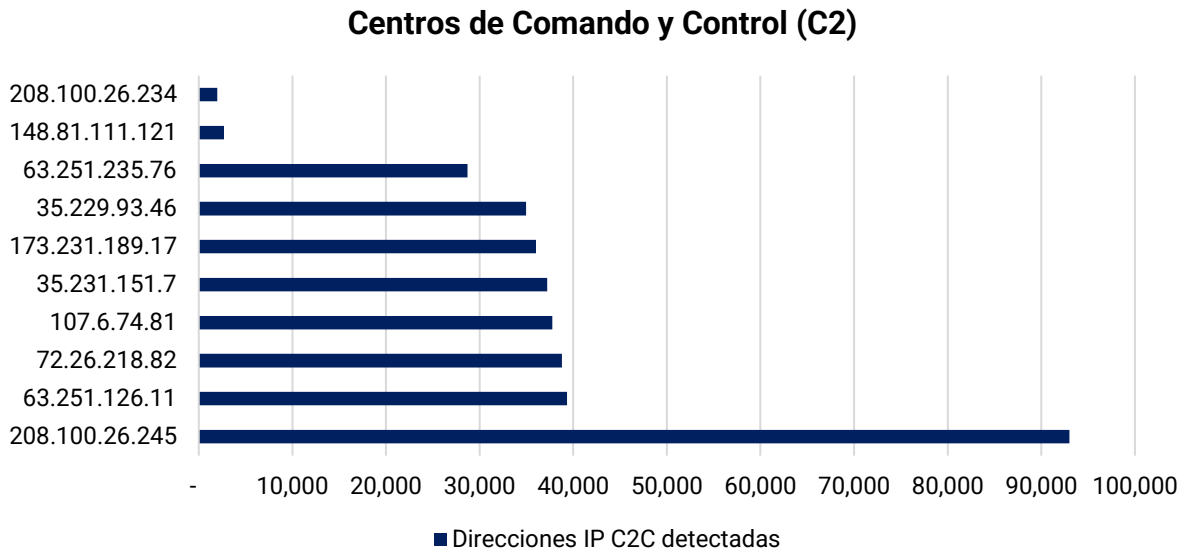
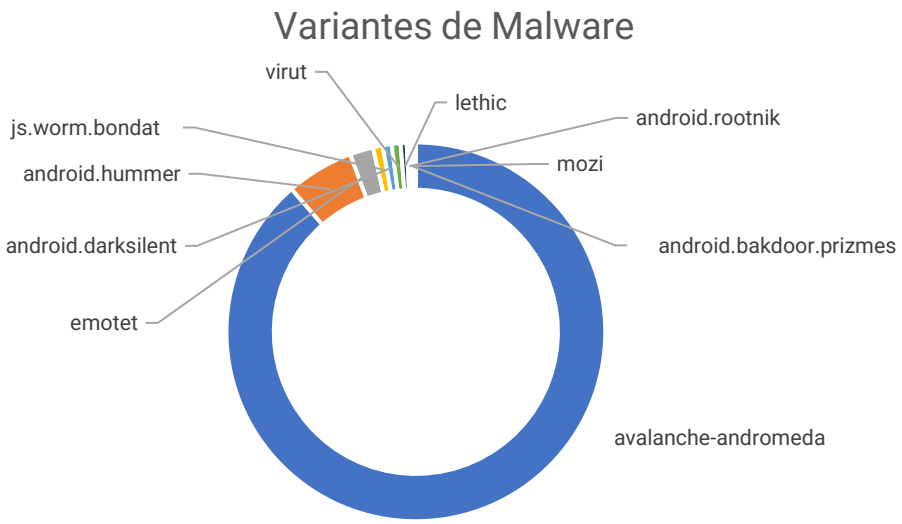


Ilustración 1 *Eventos que indican que a través del servicio de internet realiza actividad de código malicioso.*

Centros de Comando y Centros de Botnet con más tráfico malicioso registrado.

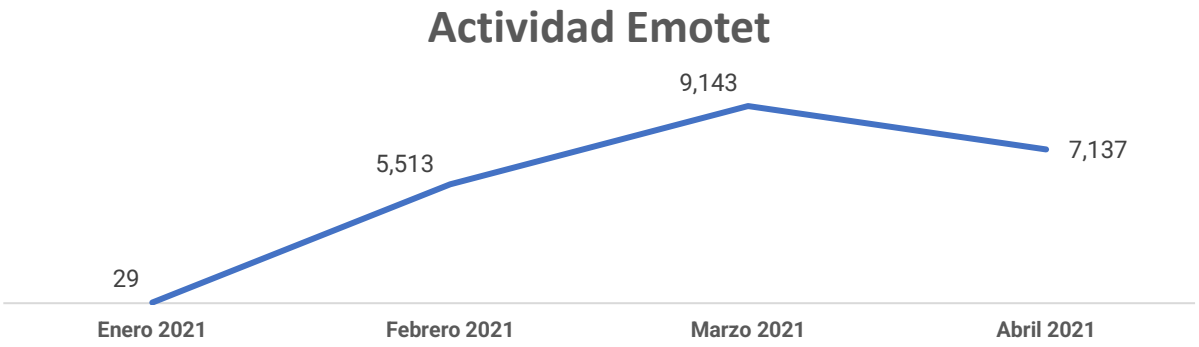


Principales variantes de malware identificadas



Durante el mes de abril fueron detectadas nuevas variantes de malware en comparación con el mes de marzo, incluyendo variantes como proxyback, expiro, el ransomware dircrypt y extenbro, el cual realiza cambios en los DNS para evitar las actualizaciones del antivirus. También fuero detectados casos de ransomware ocasionados por el wkrme (hello).

A pesar de que ya podemos hablar de **Emotet** en términos del pasado luego de su eliminación, aún persisten varios hosts infectados que intentan crear conexión con el Centro de Comando y Control eliminado por las autoridades de Europol.



FUERZA BRUTA

Tendencia de tráfico de Fuerza Bruta | enero-marzo

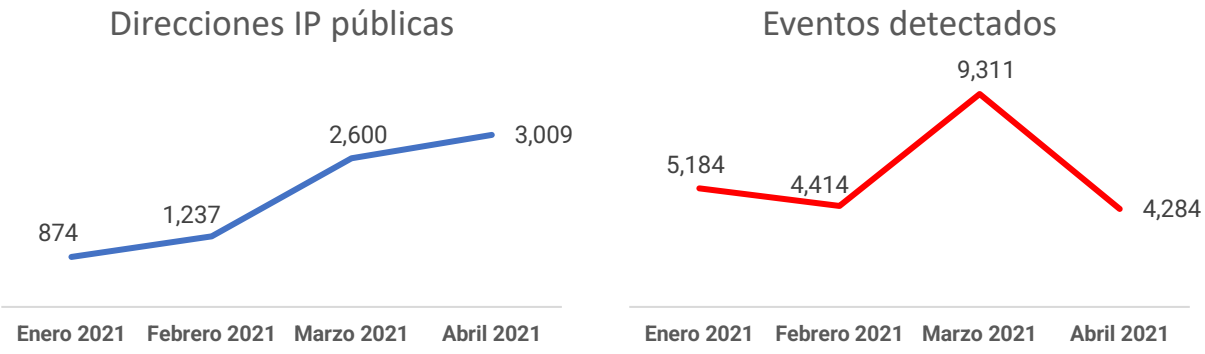
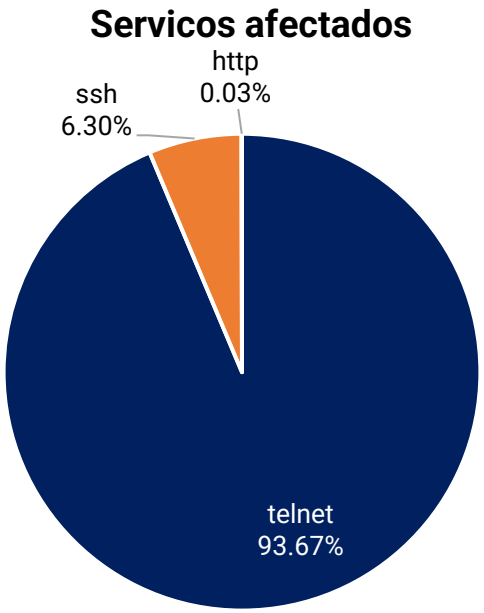


Ilustración 2 *Indicador que refleja los servicios de internet a través de los cuales se generan ataques para vulnerar otras localidades.*

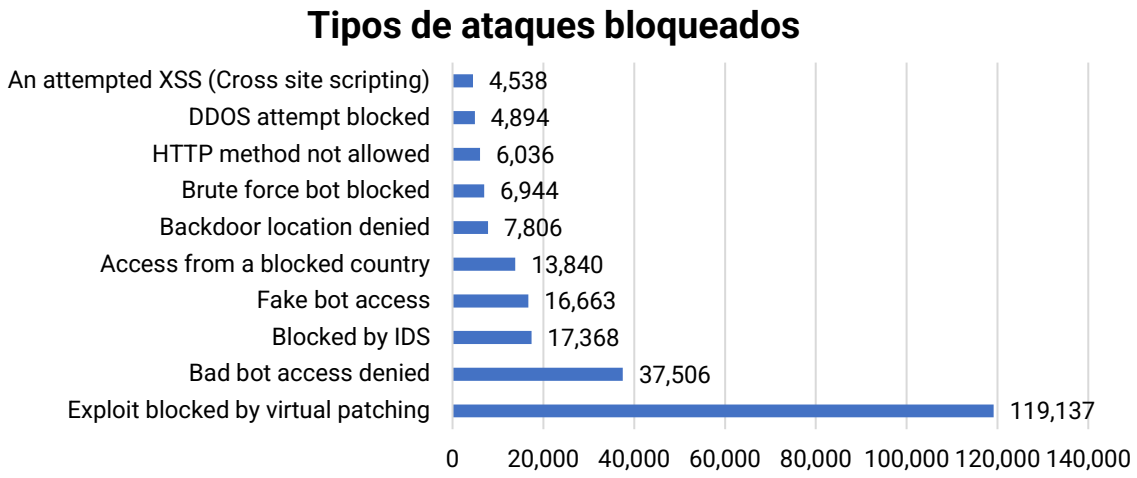
Principales servicios atacados por fuerza bruta desde host comprometidos



6. Ataques bloqueados a través del Servicio de ciber-protección

De cara a proveer servicios a la comunidad atendida, en el mes de abril fueron agregados nuevos portales gubernamentales al servicio de ciber-protección del Centro Nacional de Ciberseguridad.

Dentro de las principales amenazas detectadas y bloqueadas de encuentra la ***ejecución de exploits*** automatizados.



7. Ciberdelitos - Principales delitos cibernéticos denunciados durante abril 2021

Estafas	Extorsión	Phishing	Robo de Identidad	Acceso Ilícito	Skimming
52%	17%	11%	5%	4%	2%

Fuente: Departamento de Investigación de Crímenes y Delitos de Alta Tecnología (DICAT), Policia Nacional.

8. Eventos realizados

Capacitación avanzada en administración de CSIRT

Taller impartido por expertos de la Unión Europea a través del proyecto Cyber4Dev, dirigido a los miembros del equipo de respuesta a incidentes cibernéticos de nivel gerencial. Se trató desde las perspectivas de la organización, el factor humano, los servicios prestados (basados en el Marco de Servicios de FIRST), las políticas, procesos y las herramientas esenciales. Incluyó el modelo de madurez SIM3 (Security Incident Management Maturity Model) utilizado como marco, con el objetivo de permitir a los gerentes evaluar y mejorar la madurez del equipo.

Capacitación técnica avanzada en operación de CSIRT

Impartido por expertos de **NRD Cyber Security, Lithuania** en colaboración con **Cyber4Dev** donde los participantes recibieron capacitación en las operaciones técnicas de CERT/CSIRT/SOC.

9. Campaña de concienciación a instituciones públicas

Durante el mes de abril el Centro Nacional de Ciberseguridad continuó con el despliegue de las campañas de concienciación a los colaboradores públicos, donde los usuarios conocen sobre los riesgos cibernéticos y como provenirlos. Las campañas están focalizadas en temas como Phishing, Ransomware e Ingeniería Social en sentidos general.