PRESIDENCIA DE LA
REPÚBLICA DOMINICANA

MINISTERIO DE LA PRESIDENCIA

Centro Nacional de Ciberseguridad

Boletín Mensual
Marzo 2021

CNCS CENTRO NACIONAL DE CIBERSEGURIDAD REPÚBLICA DOMINICANA

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

CSIRTamericas.org

FIRST Improving Security Together

@cncs_rd @cncsrd / @csirtrd www.linkedin.com/company/cncsrd • www.linkedin.com/company/csirtrd

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 9 incidentes, los cuales han sido resueltos apoyando la operabilidad de las entidades afectadas.

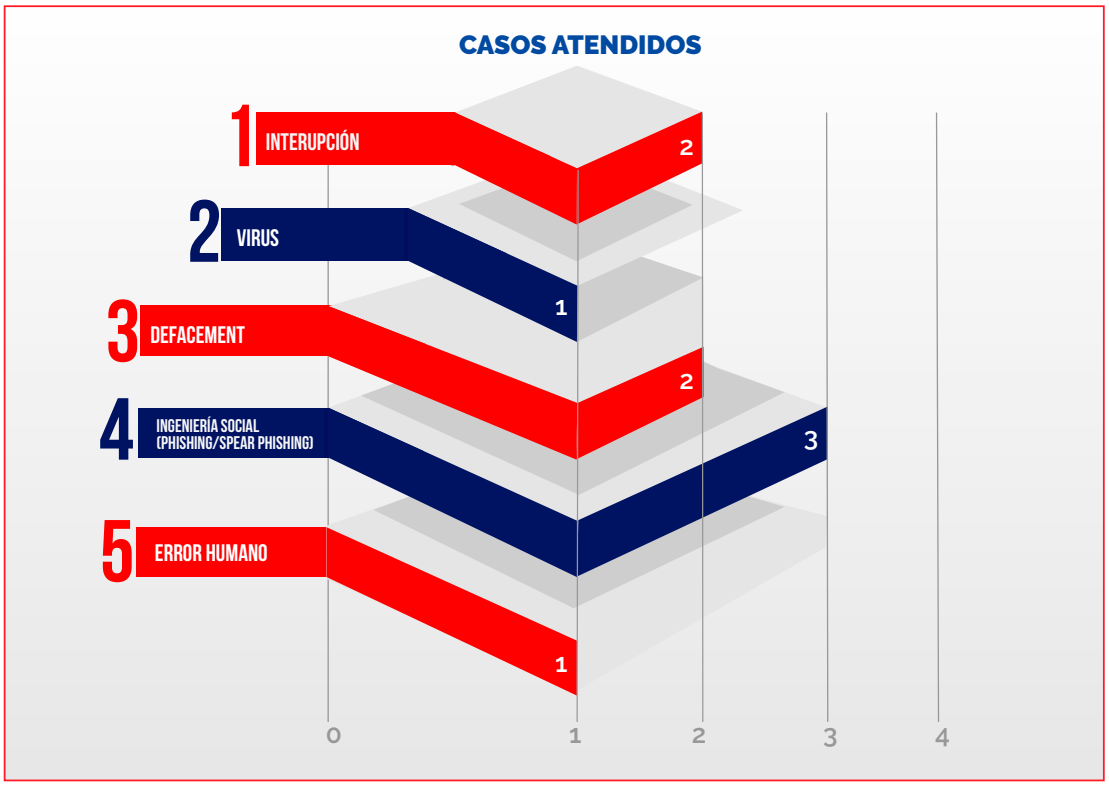
De igual manera se han realizado análisis a los servicios de la comunidad atendida, identificando un total de 36 vulnerabilidades en servicios de institucionales ofrecidos en línea.

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

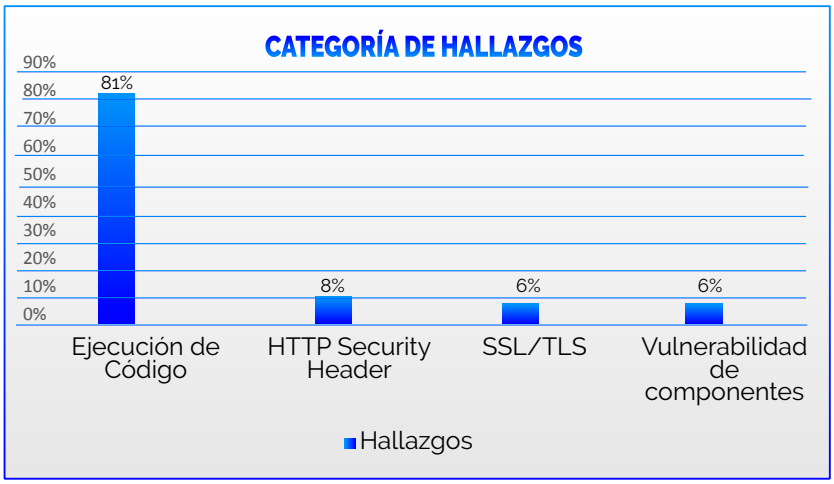
El CSIRT-RD realiza un monitoreo del ciberespacio dominicano de distintos indicadores, durante el mes de marzo destacan 11,981 direcciones IP públicas que han sido comprometidas por infecciones de Botnet, reflejándose en un aumento de un 16% en comparación a febrero del presente año. Este aumento de los eventos de Botnet está correlacionado con el aumento de los casos de fuerza bruta, estando presente varias de estas direcciones IP en la generación de ataques de fuerza bruta. Estos eventos han presentado un aumento en un 50% con respecto al mes de febrero.

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

2. Categoría de casos atendidos por el CSIRT

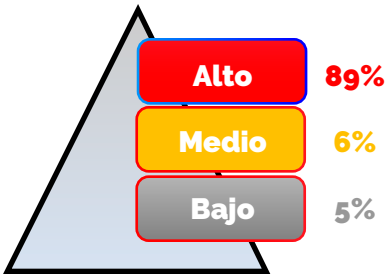


3. Análisis de Vulnerabilidades



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

Criticidad de hallazgos



Vulnerabilidad Microsoft Exchange Server.

El 3 de marzo 2021 Microsoft hizo público múltiples vulnerabilidades de día cero que se utilizaron para atacar versiones en premisa de Microsoft Exchange Server en ataques limitados y dirigidos. En los ataques observados, el actor de la amenaza utilizó estas vulnerabilidades para acceder a los servidores de Exchange en premisa que permitieron

el acceso a las cuentas de correo electrónico y permitieron la instalación de malware adicional para facilitar el acceso a largo plazo a los entornos de las víctimas.

El Equipo Nacional de Respuesta a Incidentes identificó 52 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

- Alerta | Vulnerabilidad de día cero Microsoft Exchange Server.
- Alerta | Vulnerabilidad critica en plugin The Plus Addons para elementos de Wordpress
- Alerta | Múltiples vulnerabilidades en productos de F5.
- Alerta | Múltiples vulnerabilidades en productos SAP.
- Alerta | Múltiples vulnerabilidades en productos Netgear.
- Alerta | Múltiples vulnerabilidades en moodle.
- Alerta | Múltiples vulnerabilidades en la familia General Electric.
- Alerta | Vulnerabilidad en Zoom permite la filtración de información.

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-Marzo

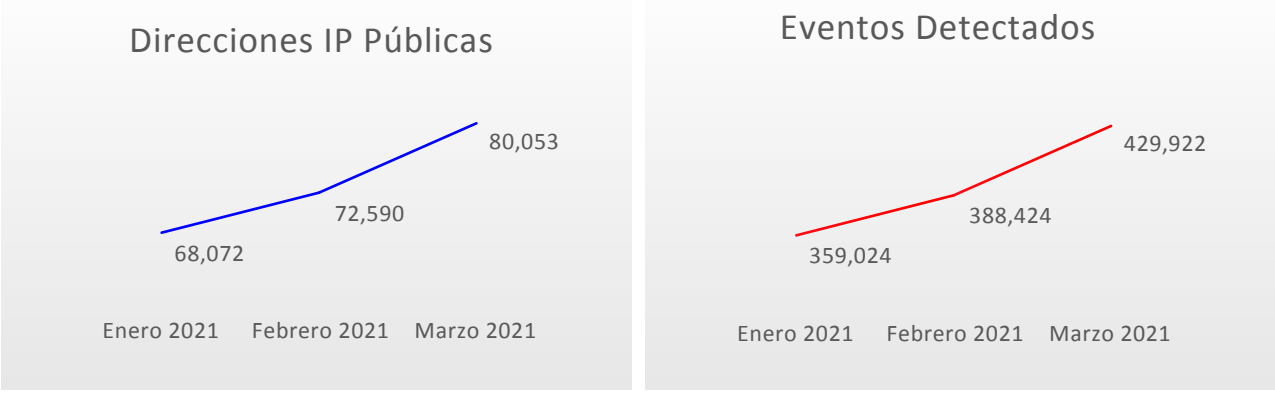
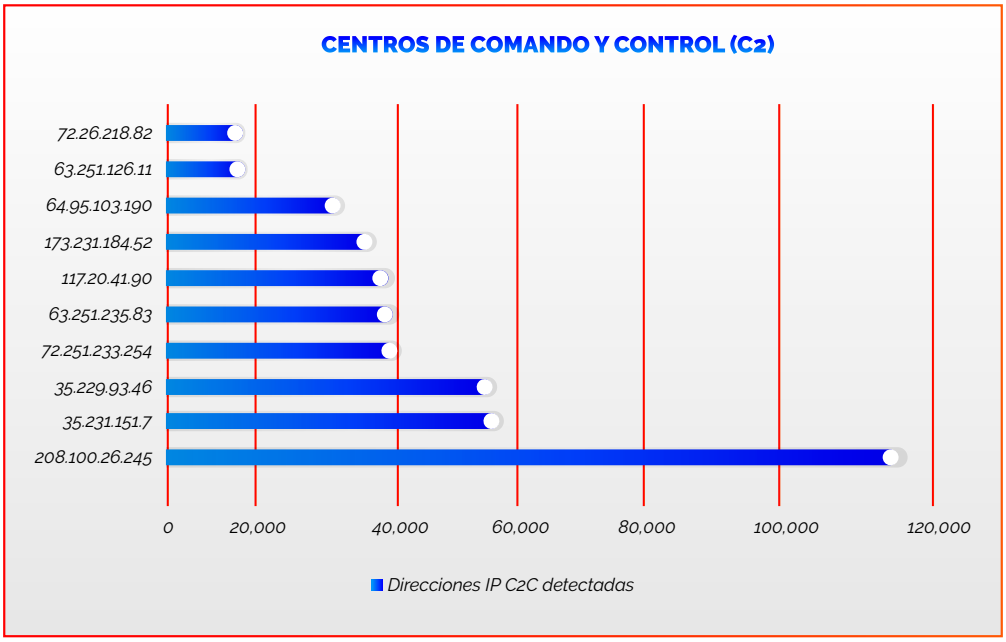
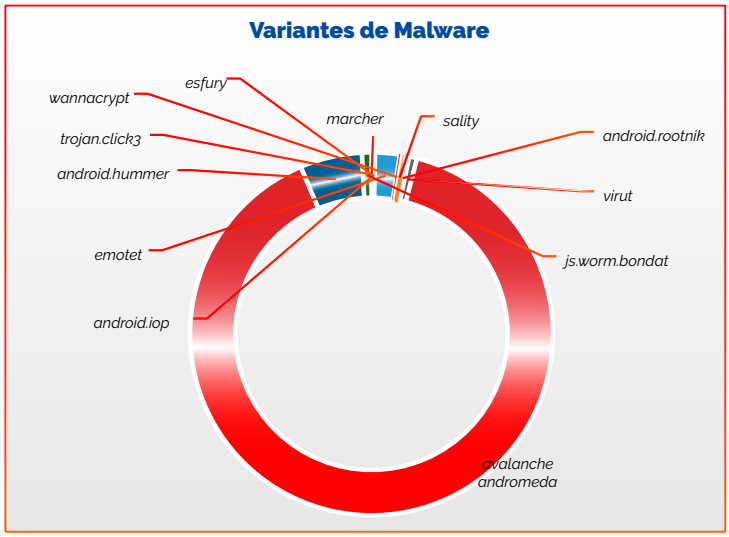


Ilustración 1. Eventos que indican que a través del servicio de internet realiza actividad de código malicioso.

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

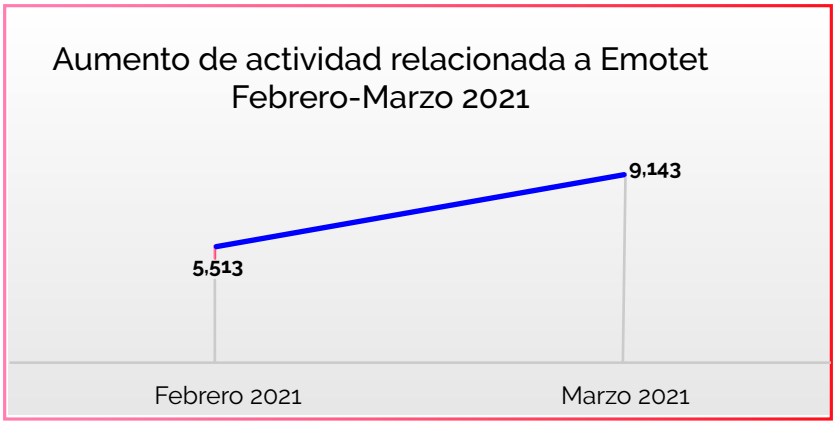


Principales variantes de malware identificadas



Durante el mes de marzo fueron detectadas las variantes de infecciones de código malicioso de mayor actividad, visualizándose la presencia de nuevas variantes en comparación con el mes anterior, como el malware bancario ***marcher***, y otras variantes de troyanos como ***betabot, banatrix.*** Así como algunos genéricos destinados a la infección de ***criptomineria.***

Los eventos de actividad maliciosa relacionado al malware bancario emotet presentaron un aumento de un 66% en comparación al mes de febrero 2021.



FUERZA BRUTA
Tendencia de tráfico de Fuerza Bruta | Enero-Marzo

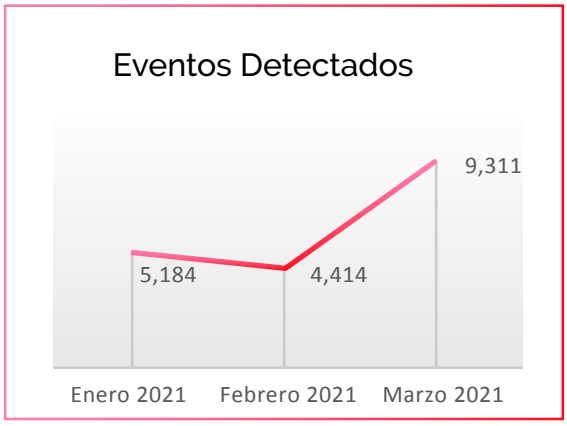
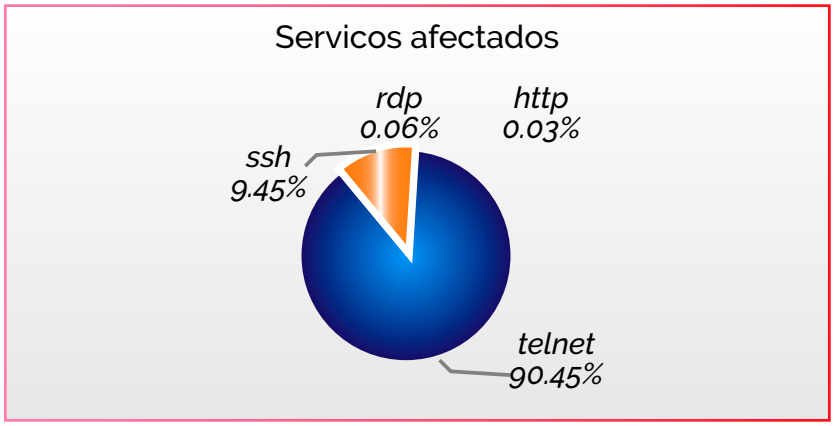


Ilustración 2. Indicador que refleja los servicios de internet a través de los cuales se generan ataques para vulnerar otras localidades.

Principales servicios atacados por fuerza bruta desde host comprometidos

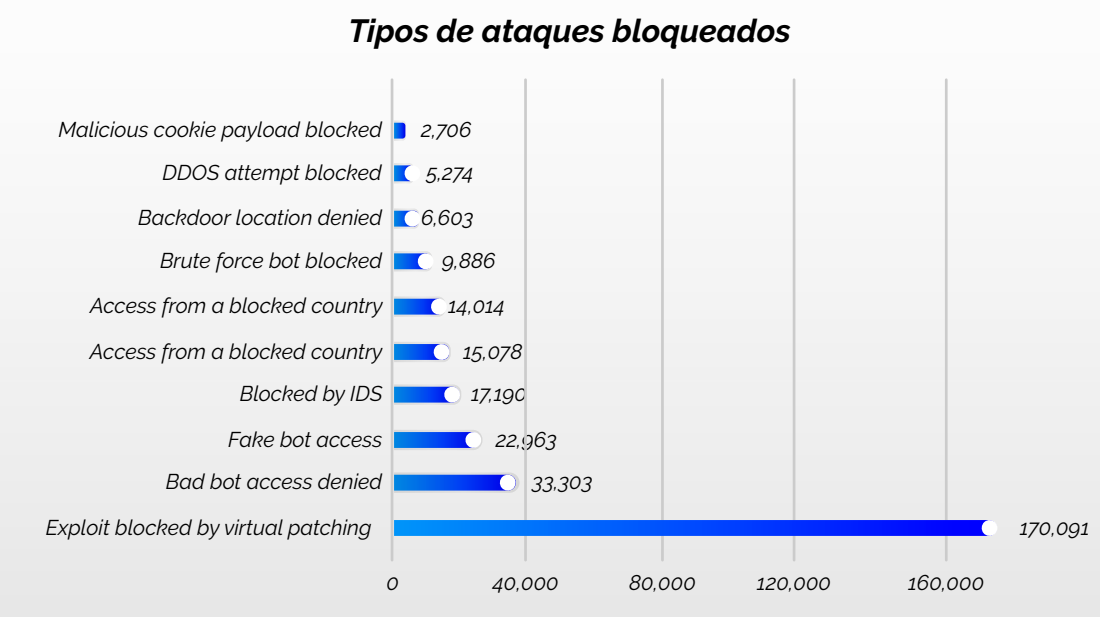


6. Ataques bloqueados a través del Servicio de ciber-protección

En el mes de marzo fueron agregados 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.***

En segundo lugar, los ***bad bots***, los cuales son apropiados por actores maliciosos y sirven como herramienta para intentar acceder a los portales de administración de los manejadores de contenido (CMS). También usados para realizar ***web scraping***, y recopilar datos (Información personal y financiera), recolección de precios para ser usado como estrategia de comercio desleal, ataques de fuerza bruta, Spam y ataques de denegación de servicios (DDoS).



7. Notificaciones y alertas sobre ciber-exposición

A través de monitoreo de ciber-exposición se realizaron 69 notificaciones a la comunidad atendida, relacionadas a los distintos servicios expuesto y vulnerables, como ***NTP, Telnet, FTP, SSL Poodle, SSL Freak, DNS-Open-Resolvers, SMB y RDP.***

8. Ciberdelitos - Principales delitos cibernéticos denunciados durante los meses enero-marzo 2021

Estafas	Extorsión	Robo de Identidad	PhiShing	Skimming	Acceso Ilícito
65%	12%	6%	5%	4%	3%

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

9. Eventos realizados

TALLER: CIBERSEGURIDAD Y CUMPLIMIENTO PARA GOBIERNO

Evento impartido a líderes de seguridad de TI en agencias de gobierno, entregado por expertos en seguridad de Microsoft quienes instruyeron sobre el panorama actual de ataques cibernéticos. El evento abordó las amenazas modernas, los pasos para mitigar estas amenazas y las acciones practicas a tomar en caso de un evento de seguridad cibernética.

TALLER VIRTUAL SOBRE LAS INFRAESTRUCTURAS CRÍTICAS Y LA CIBERSEGURIDAD

El Centro Nacional de Ciberseguridad en colaboración con S21SEC y TechnologyINT impartió el Taller Virtual sobre las Infraestructuras Críticas y la Ciberseguridad. Durante el mismo, especialistas de la región abordaron sobre las mejores prácticas de protección de las infraestructuras críticas.

TALLER DE CIBERDEFENSA PARA TÉCNICOS Y TOMADORES DE DECISIONES

El Ministerio de Defensa de la República Dominicana con el apoyo de la Junta Interamericana de Defensa y el gobierno de Canadá junto a la Inter American Defense Foundation impartieron durante 2 semanas cursos especializados sobre Estrategias de Ciberdefensa para Tomadores de Decisiones y Forense Digital para Técnicos.

"BE THE HACKER, BEAT THE HACKER"

Durante 4 horas, 20 participante realizaron laboratorios guiados por especialistas de inteligencia de amenazas de SOPHOS, donde realizaron ejercicios prácticos de técnicas de RedTeam y respuesta a incidentes.

10. Campaña de concienciación a instituciones públicas

Durante el mes de marzo 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.