REPORTES DE CIBERSEGURIDAD

Los reportes están divididos en dos grandes grupos, por un lado, se encuentran los reportes de incidencias **REACTIVAS**, estas están conformadas por reportes recibidos sobre incidentes informados por terceros en reportes del tipo Blacklist, Blocklist, Botnes y Brute Force, etc. Para facilitar la interpretación de los incidentes en forma visual se organizan los mismos agrupados por criticidad y están definidos en cuatro rangos: **CRITICO, ALTO, MEDIO y BAJO.**

Cada tipo de incidencia se agrupan en forma correlacionada y en el resumen se puede verificar la **Descripción**, **Fecha de Inicio**, **IP**, **Días desde Inicio** del primer reporte recibido por cada incidente, esto información permite poder realizar un análisis y verificar desde cuando se esta reportando este problema al Tablero de Control. Una vez remediado el evento en el próximo reporte el mismo es eliminado y dejara de figurar en el listado correspondiente a los incidentes activos.

En otra solapa se pueden verificar las incidencias del tipo **PROACTIVAS**, estas incidencias se producen mediante el análisis de las redes en base a información gestionada y procesada en forma proactiva lo cual permite trabajar en solucionar potenciales vulnerabilidad aplicando las mejores practicas que puedan producir problemas en el futuro y son potencialmente potencialmente buscado por usuarios maliciosos. El formato de la agrupación e información tiene el mismo formato que en los incidencias del tipo **REACTIVAS**.

En base a los reportes de incidencias recibidas se les asigno un **TIPO DE INCIDENCIA**, **Nombre Descriptivo** y **Nivel de Criticidad**, esto funciona como una definición inicial y categorización de los incidentes, a medida que se reciban nuevo reportes se agregan a esta lista siguiente:

TIPOS DE REPORTES

Accessible ADB Report
Este informe identifica los hosts que tienen el Android Debug Bridge (ADB) en ejecución, vinculado a un puerto de red (5555 / tcp) y accesible en Internet. Es un análisis de servicio y se actualiza cada 24 horas.

Accessible AFP Report
Este informe identifica hosts que tienen el Protocolo de archivo de Apple (AFP) en ejecución y accesible en Internet. Es un análisis de servicio y se actualiza cada 24 horas.

Accessible Apple Remote Desktop (ARD) Report
Este informe identifica los hosts que tienen el servicio Apple Remote Desktop en el puerto 3283 / udp en ejecución y accesible en Internet. Es un análisis de servicio y se actualiza cada 24 horas.

Accessible Cisco Smart Install Report
Este informe identifica hosts que tienen la función de instalación inteligente de Cisco en ejecución y son accesibles a Internet en general. Es un análisis de servicio y se actualiza cada 24 horas.

Accessible CoAP Report
Este informe identifica hosts que tienen el servicio de Protocolo de aplicación restringido (CoAP) habilitado en el puerto 5683 / UDP y accesible en Internet. Es un análisis de servicio y se actualiza cada 24 horas.

Accessible FTP Report
Este informe identifica los hosts que tienen una instancia de FTP ejecutándose en el puerto 21 / TCP que es accesible en Internet. Es un análisis de servicio y se actualiza cada 24 horas.

Accessible Hadoop Report
Este informe identifica los hosts que ejecutan Hadoop y tienen las interfaces web NameNode o DataNode ejecutándose y accesibles para el mundo en Internet. Es un análisis de servicio y se actualiza cada 24 horas.

Accessible Radmin Report
Este informe identifica hosts que tienen el servicio Radmin ejecutándose en el puerto 4899 / TCP y son accesibles para el mundo en Internet. Es un análisis de servicio y se actualiza cada 24 horas.

Accessible RDP Report
Este informe identifica los hosts que tienen el servicio de escritorio remoto (RDP) en ejecución y son accesibles para todo el mundo en Internet. Es un análisis de servicio y se actualiza cada 24 horas.

Accessible SMB Report
Este informe identifica hosts que tienen una instancia de SMB ejecutándose en el puerto 445 / TCP a los que se puede acceder en Internet. Es un análisis de servicio y se actualiza cada 24 horas.

Accessible SSH Report
Este informe identifica los hosts que tienen el servicio Secure Shell (SSH) en ejecución y accesible en Internet. Es un análisis de servicio y se actualiza cada 24 horas.

Accessible Telnet Report
Este informe identifica hosts que tienen una instancia de Telnet ejecutándose en el puerto 23 / TCP a los que se puede acceder en Internet. Es un análisis de servicio y se actualiza cada 24 horas.

Accessible VNC Report
Este informe identifica los hosts que tienen una instancia de VNC ejecutándose en el puerto 5900 / TCP a los que se puede acceder en Internet. Es un análisis de servicio y se actualiza cada 24 horas.

Accessible Rsync Report
Este informe identifica hosts que tienen el servicio rsync en ejecución, vinculados a un puerto de red (873 / tcp) y accesibles en Internet sin contraseña. Es un análisis de servicio y se actualiza cada 24 horas.

Accessible XDMCP Service Report
Este informe identifica los hosts que tienen el servicio X Display Manager en ejecución y accesible en Internet. Es un análisis de servicio y se actualiza cada 24 horas.

Amplification DDoS Victim Report
Este informe contiene eventos DDoS de amplificación observados. Procedente de Honeypots. Actualizado cada 24 horas.

ASN Summary Report
En este informe, resumimos la actividad total a lo largo de todo el tiempo de los 25 ASN principales relacionados con comando y control para redes de bots. Este es un resumen de todas las fuentes de datos. Actualizado semanalmente (domingo).

Block List Report
Este informe es la agregación de una variedad de diferentes proveedores de listas de bloqueo, para referencia de los usuarios finales. Estos datos provienen de proveedores de listas negras. Actualizado cada 24 horas.

Botnet Drone Hadoop Report
Este informe enumera todas las máquinas, drones y zombies infectados que pudimos capturar del monitoreo de control y comando de IRC, la captura de conexiones IP a redes de bots HTTP o las IP de los relés de spam. Obtenido de una variedad de fuentes.
Actualizado cada 24 horas.

Botnet URL Report
Este informe identifica las URL capturadas de las comunicaciones de la botnet. Se informa de cualquier URL que se haya visto en un canal de botnet. La URL podría ser una actualización, denuncia o información relacionada con los delincuentes. Todo está incluido por si hay algo de valor en la URL. Estos datos provienen del monitoreo de Botnet. Actualizado cada 24 horas.

Brute Force Attack Report
Este informe identifica hosts que se han observado realizando ataques de fuerza bruta. Procedente de Honeypots. Actualizado cada 24 horas.

CAIDA IP Spoofer report
Este informe basado en CAIDA tiene la intención de proporcionar una visión actual del filtrado de entrada / salida y la susceptibilidad a la falsificación de paquetes de origen IP (suplantación) en una red determinada. Actualizado cada 24 horas.

Click-Fraud Report
Este informe identifica los intentos de fraude de clics, que vemos cuando las botnets reciben la dirección para hacer clic en las URL que generan ingresos. Se enumeran las URL específicas de destino. Procedente de Botnet Monitoring. Actualizado cada 24 horas.

Compromised Host Report
Este informe proporciona información sobre hosts específicos que se vieron comprometidos por una botnet. Por lo general, se ven cuando otro sistema infectado informa sobre cada host que se ha visto comprometido. Procedente de Botnet Monitoring. Actualizado cada 24 horas.

Compromised Website Report
Este informe es una lista de todos los sitios web que nosotros o nuestros socios hemos verificado que están comprometidos y que, por lo tanto, es probable que sean objeto de abuso para varios tipos de ataques. Procedente de sistemas de seguimiento. Actualizado cada 24 horas.

Command and Control Report
Estos informes enumeran todos los C & C activos conocidos actualmente. Procedente del sistema de seguimiento. Actualizado cada 7 días.

Darknet Report
Este informe registra el tráfico observado en las redes darknet. Fuente de Darknet (Network Telescope). Actualizado cada 24 horas.

DDoS Report
Estos informes enumeran todos los ataques y objetivos de un DDoS en su área de responsabilidad, ya sea que el destinatario sea el objetivo o la fuente del ataque. Procedente de Botnet Monitoring. Actualizado cada 24 horas.

DNS Open Resolvers Report
Este informe identifica los servidores DNS que tienen el potencial de ser utilizados en ataques de amplificación de DNS por parte de delincuentes que desean realizar ataques de denegación de servicio. Procedente de Service Scan. Actualizado cada 24 horas.

Drone/Botnet-Drone Report
Este informe es una lista de todas las máquinas, drones y zombis infectados que pudimos capturar a partir del monitoreo de los controles y comandos de IRC, capturando

conexiones IP a redes de bots HTTP o las IP de retransmisiones de correo no deseado. Procedente de Botnet Monitoring (IRC y HTTP) y Sinkholes. Actualizado cada 24 horas.

Geographical Summary Report
Este informe resume la actividad total a lo largo de todo el tiempo de los 25 países principales relacionados con el comando y control de las redes de bots. Este es un resumen de todas las fuentes de datos. Actualizado semanalmente (domingo).

Honeypot URL Report
Este es un informe de las URL de origen desde las que los sistemas Honeypot descargaron el malware. Procedente de Honeypots. Actualizado cada 24 horas.

HTTP Scanners Report
Este informe identifica los hosts que se han observado realizando una actividad de análisis basada en HTTP. Procedente de Honeypots. Actualizado cada 24 horas.

ICS Scanners Report
Este informe identifica los hosts que se han observado realizando una actividad de escaneo contra los sensores del Sistema de control industrial (ICS). Procedente de Honeypots. Actualizado cada 24 horas.

IRC Port Summary Report
Estos informes resumen los puertos utilizados por los servidores de IRC como Comando y Control para una Botnet, ordenados por los más vistos, la tasa más alta de apagado y la tasa más baja de apagado. Este es un resumen de todas las fuentes de datos. Actualizado semanalmente (domingo).

Microsoft Sinkhole Report
Este informe identifica las direcciones IP de todos los dispositivos que se informaron a Shadowserver desde Microsoft después de comunicarse con los servidores Sinkhole de Microsoft. Procedente de sumideros. Actualizado cada 24 horas.

Netcore/Netis Router Vulnerability Scan Report
Este informe identifica hosts que parecen tener una puerta trasera de acceso abierto en un enrutador Netcore / Netis. Es un análisis de servicio y se actualiza cada 24 horas.

NTP Monitor Report
Este informe identifica los servidores NTP que tienen el potencial de ser utilizados en ataques de amplificación por delincuentes que desean realizar ataques de denegación de servicio. Es un análisis de servicio y se actualiza cada 24 horas.

NTP Version Report
Este informe identifica hosts que parecen tener un servicio NTP de acceso abierto en ejecución que responde a las solicitudes del Modo 6. Es un análisis de servicio y se actualiza cada 24 horas.

Open CWMP Report
Este informe identifica hosts que tienen el Protocolo de administración de WAN CPE (CWMP) en ejecución y accesible en Internet. Es un análisis de servicio y se actualiza cada 24 horas.

Open DB2 Discovery Service
Este informe identifica hosts que tienen DB2 Discovery Service en ejecución y accesible en Internet. Es un análisis de servicio y se actualiza cada 24 horas.

Open CharGen Report
Este informe identifica los hosts que parecen tener un servicio Chargen de acceso abierto en ejecución. Es un análisis de servicio y se actualiza cada 24 horas.

Open Elasticsearch Report
Este informe identifica los hosts que parecen tener un servidor Elasticsearch de acceso abierto en ejecución. Es un análisis de servicio y se actualiza cada 24 horas.

Open HTTP Report
Este informe identifica hosts que tienen el Protocolo de transferencia de hipertexto (HTTP) ejecutándose en algún puerto y son accesibles en Internet. Es un análisis de servicio y se actualiza cada 24 horas.

Open IPMI Report
Este informe identifica hosts que parecen tener un servicio IPMU de acceso abierto en ejecución que responde a un ping de IPMI. Es un análisis de servicio y se actualiza cada 24 horas.

Open IPP Report
Este informe identifica los dispositivos que tienen un servicio IPP (Protocolo de impresión de Internet) abierto habilitado en el puerto 631 / TCP. Es un análisis de servicio y se actualiza cada 24 horas.

Open LDAP Report
Este informe identifica hosts que tienen una instancia LDAP ejecutándose en el puerto 389 / UDP a los que se puede acceder en Internet. Es un análisis de servicio y se actualiza cada 24 horas.

Open LDAP TCP Report
Este informe identifica los hosts que tienen una instancia LDAP ejecutándose en el puerto 389 / TCP a los que se puede acceder en Internet. Es un análisis de servicio y se actualiza cada 24 horas.

Open mDNS Report
Este informe identifica los hosts que tienen el servicio mDNS en ejecución y accesible desde Internet. Es un análisis de servicio y se actualiza cada 24 horas.

Open Memcached Report
Este informe identifica los hosts que parecen tener un servidor de clave-valor Memcached de acceso abierto en ejecución. Es un análisis de servicio y se actualiza cada 24 horas.

Open MQTT Report
El informe identifica hosts que parecen tener un MQTT de acceso abierto en ejecución. Es un escaneo de servicio y se actualiza cada 24 horas.

Open MongoDB Report
Este informe identifica hosts que parecen tener un servidor MongoDB NoSQL de acceso abierto en ejecución. Es un análisis de servicio y se actualiza cada 24 horas.

Open MS-SQL Server Resolution Service Report
Este informe identifica hosts que parecen tener en ejecución un servicio de resolución de servidor MS-SQL de acceso abierto. Es un análisis de servicio y se actualiza cada 24 horas.

Open NAT-PMP Report
Este informe identifica hosts que parecen tener un servicio NetBIOS de acceso abierto en ejecución. Es un análisis de servicio y se actualiza cada 24 horas.

Open NetBIOS Report
Este informe identifica hosts que parecen tener un servicio NetBIOS de acceso abierto en ejecución. Es un análisis de servicio y se actualiza cada 24 horas.

Open Portmapper Report
Este informe identifica cualquier host que parezca tener un servicio portmapper de acceso abierto en ejecución que responda a una solicitud rpcinfo. Es un análisis de servicio y se actualiza cada 24 horas.

Open Proxy Report
Este informe detecta proxies abiertos o puntos de salto, ya sea utilizados directamente o vendidos a otros delincuentes. Obtenido de Search Engine Scraping, Botnets y otras fuentes. Actualizado cada 24 horas.

Open QOTD Report
Este informe identifica los hosts que parecen tener un servicio de Cotización del día de acceso abierto en ejecución. Es un análisis de servicio y se actualiza cada 24 horas.

Open Redis Report
Este informe identifica los hosts que parecen tener un servidor clave-valor de Redis de acceso abierto en ejecución. Es un análisis de servicio y se actualiza cada 24 horas.

Open SNMP Report
Este informe identifica hosts que parecen tener un servicio SNMP de acceso abierto en ejecución. Es un análisis de servicio y se actualiza cada 24 horas.

Open SSDP Report
Este informe identifica hosts que parecen tener en ejecución un servicio de Protocolo simple de descubrimiento de servicios de acceso abierto. Es un análisis de servicio y se actualiza cada 24 horas.

Open/Accessible TFTP
Este informe identifica hosts que tienen el servicio TFTP en ejecución y accesible en Internet. Es un análisis de servicio y se actualiza cada 24 horas.

Open Ubiquiti Report
Este informe identifica los hosts que tienen el servicio Ubiquiti Discovery en ejecución y accesible en Internet. Es un análisis de servicio y se actualiza cada 24 horas.

Outdated DNSSEC Key Report
Este informe identifica hosts IPv4 que se han observado utilizando una clave DNSSEC desactualizada. Es un análisis de servicio y se actualiza cada 24 horas.

Outdated DNSSEC Key IPv6 Report
Este informe identifica hosts IPv6 que se han observado utilizando una clave DNSSEC desactualizada. Es un análisis de servicio y se actualiza cada 24 horas.

Proxy Report
Este informe detecta servidores proxy, que se utilizan comúnmente para hacer que la actividad maliciosa parezca anónima. Estos datos provienen del monitoreo de Botnet. Actualizado cada 24 horas.

Sandbox URL Report
Este informe incluye conjuntos de URL a las que ha accedido malware. Hay dos versiones de este informe: filtrado y sin filtrar. Obtenido de nuestros sistemas de espacio aislado. Actualizado cada 24 horas.

Sandbox Connection Report
Este informe es un resumen de todas las conexiones que vio el sistema sandbox para el intervalo específico. Obtenido de nuestros sistemas de espacio aislado. Actualizado cada 24 horas.

Sandbox IRC Report
Este informe es un resumen de todas las redes basadas en IRC que se encontraron después de analizar el malware. Obtenido de nuestros sistemas de espacio aislado. Actualizado cada 24 horas.

Sandbox SMTP Report
Una lista de direcciones de correo electrónico utilizadas por el malware durante la ejecución de una zona de pruebas. Obtenido de nuestros sistemas de espacio aislado. Actualizado cada 24 horas.

Scan Report
El análisis de vulnerabilidades es una parte estándar de cualquier arsenal de botnets. Informamos sobre estos como una advertencia de que se están atacando bloques de red específicos. Es un análisis de servicio y se actualiza cada 24 horas.

Sinkhole HTTP Drone Report
Este informe identifica todas las direcciones IP que se unieron al servidor del sumidero que no se unieron a través de una URL de referencia. Procedente de sumideros. Actualizado cada 24 horas.

Sinkhole6 HTTP Drone Report
Este informe enumera las direcciones IPv6 de todos los dispositivos que se conectaron a nuestro servidor de IPv6. Procedente de sumideros. Actualizado cada 24 horas.
Sinkhole HTTP Referrer Report
Una lista de URL de referencia que enviaron sistemas al servidor del sumidero. Procedente de sumideros. Actualizado cada 24 horas.

Spam URL Report
Una lista de las URL y retransmisiones de spam que se recibieron. Procedente de correo no deseado y correo electrónico. Actualizado cada 24 horas.

SSL FREAK Report
Este informe identifica cualquier host (IP) que podría usarse en un ataque SSL FREAK. Es un análisis de servicio y se actualiza cada 24 horas.

SSL POODLE Report
Este informe identifica cualquier host (IP) que parece ser vulnerable a un ataque SSL POODLE. Es un análisis de servicio y se actualiza cada 24 horas.

Synful Scan Report
Este informe identifica hosts que están potencialmente comprometidos con la puerta trasera de SYNful. Es un análisis de servicio y se actualiza cada 24 horas.

Vulnerable ISAKMP Report
Este informe identifica hosts que tienen un servicio IKE vulnerable accesible en Internet. Es un análisis de servicio y se actualiza cada 24 horas.

Por cualquier consulta relacionada a los reportes recibidos se deberán canalizar por medio de la casilla de correo : **ciberseguridad@central.uncoma.edu.ar**