INFORME DE GESTIÓN

Servicio SOC

Tecnología: CylancePROTECT

Frecuencia Informe: Mensual

Periodo: {{date1}} hasta {{date2}}

[{{Logo}}](mailto:marcelo.silenzi@osdipp.com.ar)

**PREPARADO PARA:**

**{{nombre\_cliente}}**

**PREPARADO POR:**

SOC – RPA 01 – Informe automatizado

RAN Security

**REVISADO POR:**

Nombre de analista - Puesto

xxx@ransecurity.com

RAN Security

Tabla de Contenidos

[Objetivo 3](#_Toc135407963)

[Acerca del Informe 4](#_Toc135407964)

[Alcance de la tecnología 5](#_Toc135407965)

[Resumen Ejecutivo 6](#_Toc135407966)

[Resumen Técnico 7](#_Toc135407967)

[1. Información sobre la tecnología y sus activos 7](#_Toc135407968)

[Usabilidad de Licencias 7](#_Toc135407969)

[Políticas asociadas a dispositivos 8](#_Toc135407970)

[Cantidad de equipos por Zona 8](#_Toc135407971)

[Equipos por Sistemas operativos 8](#_Toc135407972)

[2. Cumplimiento 9](#_Toc135407973)

[Versiones Agente Cylance 9](#_Toc135407974)

[Agentes Cylance – Se requiere actualizar (<=1574) 9](#_Toc135407975)

[Cantidad de equipos en políticas no seguras 10](#_Toc135407976)

[Equipos fuera de línea (> 15 días) 11](#_Toc135407977)

[3. Estadísticas sobre detecciones 12](#_Toc135407978)

[Amenazas - Indicadores 12](#_Toc135407979)

[Ubicación de las detecciones 12](#_Toc135407980)

[Eventos por Clasificación 13](#_Toc135407981)

[Amenazas - Acciones tomadas 14](#_Toc135407982)

[Histograma con medidas tomadas sobre las amenazas 14](#_Toc135407983)

[Estado de las amenazas 14](#_Toc135407984)

[Acciones tomadas por Clasificación de Malware 15](#_Toc135407985)

[Amenazas - Top Ten - Listas 16](#_Toc135407986)

[Equipos con más amenazas 16](#_Toc135407987)

[Usuarios con más amenazas 16](#_Toc135407988)

[Amenazas - Quarantined y Cleared 17](#_Toc135407989)

[Exploits de Memoria – Indicadores 18](#_Toc135407990)

[Tipos de violaciones 18](#_Toc135407991)

[Exploits de Memora – Acciones tomadas 18](#_Toc135407992)

[Acciones tomadas por Memory Protection 18](#_Toc135407993)

[Exploits de Memoria – Top Ten – Listas 19](#_Toc135407994)

[Equipos con más Exploits 19](#_Toc135407995)

[Usuarios con más Exploits 19](#_Toc135407996)

[Glosario 20](#_Toc135407997)

[INFORMACIONES Y CONSULTAS 29](#_Toc135407998)

# Objetivo

El presente informe tiene dos focos principales:

* Brindar una síntesis global, resumida y de rápida lectura acerca de la tecnología gestionada por el SOC (**Security Operations Center)** de **RANSecurity**.
* Evaluar de forma continua el Servicio del SOC (Security Operation Center) brindado por RAN Security al cliente **{{nombre\_cliente}}**.

El alcance de este servicio incluye el monitoreo, tratamiento de eventos de seguridad y análisis, de la tecnología definida en la sección Alcance Tecnología.

**SOC:**

* **Personas (Equipo):** Grupo de profesionales con funciones y roles claros.
* **Procesos**: Monitoreo de eventos + tratamiento + análisis + automatización.
* **Tecnología**: Definidas por el cliente (ver sección Alcance Tecnología)

# Acerca del Informe

Esta sección tiene como principal función explicar la estructura de este informe y así brindar al Cliente una compresión sobre el mismo. Este documento fue desglosado en varias secciones:

* Alcance de la tecnología,
* Un resumen ejecutivo,
* Un resumen técnico,
* Glosario.

El [*Resumen Ejecutivo*](#_Resumen_Ejecutivo), es donde el Cliente podrá tener una visión general sobre el estado de situación, es la primera sección por leer. El SOC volcará recomendaciones que requieren su atención en este apartado. En caso de requerir detalles técnicos se recomendará leer otras secciones de este informe.

El [*Resumen Técnico*](#_Resumen_Técnico) incluye 3 capítulos:

* ***Informacion sobre la tecnología y sus activos.***
* ***Cumplimiento.***
* ***Estadísticas sobre detecciones.***

Dentro de la primera sección, **Informacion sobre la tecnología y sus activos,** se incluye datos estadísticos e informativos sobre la usabilidad de licencias (tecnología), politicas de protección y a nivel de activos propios del cliente, se lista cantidad de equipos por Politicas / Zonas y sus sistemas operativos.

En nuestra siguiente sección, **Estadísticas sobre detecciones**, nos centramos en los dos tipos de detecciones, **Amenazas y Exploits**. Por cada tipo de detección, mostramos:

* Indicadores – Ubicación de las detecciones y sus clasificaciones.
* Acciones tomadas – Acciones tomadas por la tecnología.
* Top Ten – Equipos / usuarios con mayores detecciones encontradas.

Finalmente, contamos con el Glosario, muy útil para lograr un mejor entendimiento de la terminología que se utiliza en este informe. Básicamente encontramos definiciones importantes, como, por ejemplo, que las acciones que toma la tecnología para Amenazas y Exploits, son diferentes.

|  |  |  |  |
| --- | --- | --- | --- |
| Informe número: | {{ n\_informe}} | Periodo del informe: | Del: {{date1}} al {{date2}} |

# Alcance de la tecnología

La siguiente tecnología es gestionada por el SOC:

* CylancePROTECT

# Resumen Ejecutivo

El siguiente es resumen ejecutivo que tiene como finalidad brindar al cliente un estado de situación general de la tecnología:

**Recomendaciones que se requiere acciones por parte del cliente:**

De acuerdo con el monitoreo y gestión de la tecnologia y como consecuencia del análisis de los eventos analizados por el SOC, se recomienda tomar acciones inmediatas en las siguientes secciones del Informe:

* Equipos fuera de línea (>15 dias).

# Resumen Técnico

La siguiente sección incluye tres temas principales del informe:

* Información sobre la tecnología y sus activos.
* Cumplimiento.
* Estadísticas sobre amenazas.

## **Información sobre la tecnología y sus activos**

Se detalla datos informativos sobre la tecnología, licencias, activos (sistemas operativos), etc.

### Usabilidad de Licencias

//Copiar grafico de la planilla “Año-Mes - Matriz Master - Cantidad Licencias CylancePROTECT”

|  |  |  |
| --- | --- | --- |
| **Licencias** | **Dispositivos** | **Diferencia** |
| **{%tr for item in licencias %}** | | |
| **{{item[0]}}** | **{{item[1]}}** | **{{item[2]}}** |
| **{%tr endfor %}** | | |

### Políticas asociadas a dispositivos

|  |  |
| --- | --- |
| **Policy** | **Cantidad** |
| **{%tr for item in devicesPolicy %}** | |
| **{{item[1]}}** | **{{item[0]}}** |
| **{%tr endfor %}** | |

### Cantidad de equipos por Zona

|  |  |
| --- | --- |
| **Zone** | **Cantidad** |
| **{%tr for item in devicesZones %}** | |
| **{{item[1]}}** | **{{item[0]}}** |
| **{%tr endfor %}** | |

### Equipos por Sistemas operativos

|  |  |
| --- | --- |
| **Sistema operativo** | **Cantidad** |
| **{%tr for item in operativeSystem %}** | |
| **{{item[1]}}** | **{{item[0]}}** |
| **{%tr endfor %}** | |

## **Cumplimiento**

Esta sección incluye todo lo relacionado acerca de la tecnología y los activos donde se encuentran instalados.

### Versiones Agente Cylance

|  |  |
| --- | --- |
| **Version** | **Cantidad** |
| **{%tr for item in versionesAgenteCy %}** | |
| **{{item[1]}}** | **{{item[0]}}** |
| **{%tr endfor %}** | |

### Agentes Cylance – Se requiere actualizar (<=1574)

|  |  |
| --- | --- |
| **Versión Agente** | **Cantidad** |
| **{%tr for item in versionCylanceSum[0] %}** | |
| **{{item[1]}}** | **{{item[0]}}** |
| **{%tr endfor %}** | |
| **Total** | **{{versionCylanceSum[1]}}** |

A continuación, se listan los equipos que requieren acción para actualizar la versión a una más reciente:

|  |  |  |
| --- | --- | --- |
| **Nombre Dispositivo** | **Version SO** | **Versión Agente** |
| **{%tr for item in devicesActualizar %}** | | |
| **{{item[0]}}** | **{{item[1]}}** | **{{item[2]}}** |
| **{%tr endfor %}** | | |

### Cantidad de equipos en políticas no seguras

Se toma como políticas no seguras, las siguientes (que contengan en su nombre las siguientes palabras claves, las mismas obedecen a políticas creadas en la etapa de implementación):

* Default
* Fase 1
* Fase 2

|  |  |
| --- | --- |
| **Política No segura** | **Cantidad** |
| **{%tr for item in politicasNoSeguras %}** | |
| **{{item[1]}}** | **{{item[0]}}** |
| **{%tr endfor %}** | |

### Equipos fuera de línea (> 15 días)

|  |  |  |  |
| --- | --- | --- | --- |
| **Equipo** | **Ultimo Usuario** | **IP** | **Ultima Fecha** |
| **{%tr for item in equiposOffline %}** | | | |
| **{{item[0]}}** | **{{item[1]}}** | **{{item[2]}}** | **{{item[3]}}** |
| **{%tr endfor %}** | | | |

## **Estadísticas sobre detecciones**

Como sección principal sobre foco en temas de seguridad, en esta sección 3, se detalla todo lo relacionado a amenazas y exploits de memoria. En el Resumen Ejecutivo encontrará las recomendaciones del SOC de RAN Security que requieren una acción por parte del cliente.

### Amenazas - Indicadores

#### Ubicación de las detecciones

|  |  |
| --- | --- |
| **Ubicacion** | **Cantidad** |
| **{%tr for item in ubicacionAmenazas %}** | |
| **{{item[1]}}** | **{{item[0]}}** |
| **{%tr endfor %}** | |

Existen tres tipos de ubicaciones de las detecciones:

* + **Internal Hard Drive:** Unidad C:\
  + **Network Drive**: Ruta UNC (unidad de red – Carpeta compartida)
  + **Unknown**: Unidades adicionales, D:\ E:\ F:\ G:\ (Discos adicionales o unidad mapeada)
  + **USB/External Hard Drive**: Unidad extraible, USB.

Nota importante: El grafico anterior no incluye las detecciones en estado “Cleared”. Estos datos son solo obtenidos del archivo “Threats Data Report”.

#### Eventos por Clasificación

A continuación, se listan las clasificaciones por las detecciones, incluyendo las que fueron Cleared (borradas):

Lista de clasificaciones por cada amenaza:

* + Unknown (Blank Entry)
  + Trusted - Local
  + PUP
  + Dual Use
  + Malware

|  |  |
| --- | --- |
| **Clasificacion** | **Cantidad** |
| **{%tr for item in categoriaAmenazas %}** | |
| **{{item[1]}}** | **{{item[0]}}** |
| **{%tr endfor %}** | |

### Amenazas - Acciones tomadas

#### Histograma con medidas tomadas sobre las amenazas

{{ histograma }}

#### Estado de las amenazas

|  |  |
| --- | --- |
| **Estado** | **Cantidad** |
| **{%tr for item in estadoAmenazas %}** | |
| **{{item[1]}}** | **{{item[0]}}** |
| **{%tr endfor %}** | |

#### Acciones tomadas por Clasificación de Malware

|  |  |
| --- | --- |
| **Clasificación** | **Acción tomada** |
| **{%tr for item in accionesPorClasificacion %}** | |
| **{{item.ClassFull}}** | **{{item.valores}}** |
| **{%tr endfor %}** | |

***Clasificaciones en blanco***

Es importante aclarar que hay detecciones que no se van a poder clasificar, esto se puede visualizar cuando el campo es desconocido (Entrada en blanco).

Justificación: El archivo aún no ha sido analizado por el equipo de Investigación de Cylance (Research Team). Una vez analizado, la clasificación se actualizará con un nuevo estado.

Debido a esta situación, CylancePROTECT toma acción utilizando el score asignado por cada detección.

### Amenazas - Top Ten - Listas

#### Equipos con más amenazas

|  |  |
| --- | --- |
| **Equipo** | **Cantidad** |
| **{%tr for item in topEquiposAmenazas %}** | |
| **{{item[0]}}** | **{{item[1]}}** |
| **{%tr endfor %}** | |

#### Usuarios con más amenazas

|  |  |
| --- | --- |
| **Usuario** | **Cantidad** |
| **{%tr for item in topUsersAmenazas %}** | |
| **{{item[0]}}** | **{{item[1]}}** |
| **{%tr endfor %}** | |

#### Amenazas - Quarantined y Cleared

|  |  |  |  |
| --- | --- | --- | --- |
| **Quarantined** | **Path** | **Device** | **Cantidad** |
| **{%tr for item in topAmenazasQuarantined %}** | | | |
| **{{item[0]}}** | **{{item[1]}}** | **{{item[2]}}** | **{{item[3]}}** |
| **{%tr endfor %}** | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Cleared** | **Path** | **Device** | **Cantidad** |
| **{%tr for item in topAmenazasCleared %}** | | | |
| **{{item[0]}}** | **{{item[1]}}** | **{{item[2]}}** | **{{item[3]}}** |
| **{%tr endfor %}** | | | |

### Exploits de Memoria – Indicadores

#### Tipos de violaciones

|  |  |
| --- | --- |
| **Tipo** | **Cantidad** |
| **{%tr for item in exploitsViolationTypes %}** | |
| **{{item[1]}}** | **{{item[0]}}** |
| **{%tr endfor %}** | |

### Exploits de Memora – Acciones tomadas

#### Acciones tomadas por Memory Protection

|  |  |
| --- | --- |
| **Accion** | **Cantidad** |
| **{%tr for item in exploitsAccionTomada %}** | |
| **{{item[1]}}** | **{{item[0]}}** |
| **{%tr endfor %}** | |

### Exploits de Memoria – Top Ten – Listas

#### Equipos con más Exploits

|  |  |
| --- | --- |
| **Equipo** | **Cantidad** |
| **{%tr for item in exploitPorDevices %}** | |
| **{{item[1]}}** | **{{item[0]}}** |
| **{%tr endfor %}** | |

Las detecciones en el listado de equipos se listan a continuación:

|  |  |  |  |
| --- | --- | --- | --- |
| **Equipo** | | **Exploit** | **N° de veces ejecutado** |
| **{%tr for item in equiposTopExploits %}** | | | |
| **{{ item.equipo }}** | |  |  | | --- | --- | | **{%tr for i in item.lista %}** | | | **{{ i[0] }}** | **{{ i[1] }}** | | **{%tr endfor %}** | | | | |
| **{%tr endfor %}** | | | |

#### Usuarios con más Exploits

|  |  |
| --- | --- |
| **Usuario** | **Cantidad** |
| **{%tr for item in exploitPorUsers %}** | |
| **{{item[1]}}** | **{{item[0]}}** |
| **{%tr endfor %}** | |

# Glosario

Protección de Amenazas

**Puntuación de Cylance (Cylance Score): Unsafe y Abnormal**

La puntuación hace referencia al nivel de confianza real que un archivo representa para el entorno. Cuanto mayor sea la puntuación, mayor será el nivel de desconfianza del archivo. Según la puntuación, las amenazas se consideran inseguras (Unsafe) entre 60 y 100 o anormales (Abnormal) entre 1 y 59.

**Tipos de acciones**

|  |  |
| --- | --- |
| **Opción** | **Descripción** |
| Unsafe | Amenazas que se han encontrado y que actualmente se están ejecutando (o) se pueden ejecutar. Puntuación que oscila entre 60 y 100. |
| Abnormal | Esto indica que el archivo puede tener características anormales con un menor riesgo de amenaza. Puntuación que oscila entre 1 y 59. |
| Quarantined | Puede optar por poner en cuarentena un archivo no seguro o anómalo en los dispositivos en los que se encontró. Si es un administrador, también puede optar por poner en cuarentena global la amenaza, en cuyo caso, el archivo se pondrá en cuarentena en cualquier dispositivo cada vez que se encuentre. |
| Waived | Puede otorgar una exención (waiver) a un archivo en los dispositivos en los que se encuentra. Un administrador también puede optar por agregar un archivo a la lista segura, lo que le permitiría ejecutarse en cualquier sistema de su red. Las exenciones/listas seguras generalmente se realizan para archivos anormales. |

**Lista de clasificaciones por cada amenaza:**

* [**Unknown (Blank Entry)**](https://support.blackberry.com/kb/articleDetail?articleNumber=000067437&language=en_US#Unknown)
* [**Trusted - Local**](https://support.blackberry.com/kb/articleDetail?articleNumber=000067437&language=en_US#Trusted)
* [**PUP**](https://support.blackberry.com/kb/articleDetail?articleNumber=000067437&language=en_US#PUP)
* [**Dual Use**](https://support.blackberry.com/kb/articleDetail?articleNumber=000067437&language=en_US#Dual_Use)
* [**Malware**](https://support.blackberry.com/kb/articleDetail?articleNumber=000067437&language=en_US#Malware)

**Unknown (Blank Entry)**

El archivo aún no ha sido analizado por el equipo de investigación de Cylance. Una vez que se analiza el archivo, se actualizará la clasificación del archivo.

**Trusted – Local**

El archivo fue analizado por el equipo de investigación de Cylance y ha sido considerado seguro (no malicioso, no un PUP). La razón de la designación 'Local' se debe al hecho de que el archivo no procede de una fuente de confianza (como Microsoft u otro instalador de confianza) y, por lo tanto, no se puede añadir al repositorio de confianza en la nube.

**PUP**

El archivo ha sido identificado como un Programa Potencialmente No Deseado (PUP). Esto indica que el programa puede ser no deseado, a pesar de la posibilidad de que los usuarios hayan consentido en descargarlo. Algunas PUPs pueden ser permitidas para ejecutarse en un conjunto limitado de sistemas en su organización (por ejemplo, una aplicación VNC permitida para ejecutarse en los dispositivos de administración de dominio). Un administrador de Cylance puede elegir entre renunciar o bloquear las PUP por dispositivo, ponerlas en cuarentena global o en una lista segura según las políticas de la empresa. Dependiendo de la cantidad de análisis que se pueda realizar contra una PUP, puede ser posible una subclasificación adicional. Estas subclases se muestran a continuación y ayudarán a un administrador a determinar si una PUP en particular debe ser bloqueada o si se debe permitir que se ejecute:

| **Subclase** | **Definición** | **Ejemplos** |
| --- | --- | --- |
| Adware | software de publicidad que se instala en un equipo sin consentimiento por parte del usuario. | Gator, Adware Info |
| Corrupt | Cualquier ejecutable que esté malformado y no pueda ejecutarse. |  |
| Game | Tecnologías que crean un entorno interactivo con el que un -usuario puede jugar. | Steam Games, League of Legends |
| Generic | Cualquier PUP que no encaje en una categoría existente. |  |
| HackingTool | Tecnologías que están diseñadas para ayudar en los intentos de piratería informática. | Cobalt Strike, MetaSp0it |
| Portable Application | Programa diseñado para ejecutarse en un ordenador de forma independiente, sin necesidad de instalación. | Turbo |
| Scripting Tool | Cualquier script que pueda funcionar como si fuera un ejecutable. | AutoIT, py2exe |
| Toolbar | Tecnologías que colocan botones o cuadros de entrada adicionales en pantalla dentro de una interfaz de usuario. | Nasdaq Toolbar, Bring Me Sports |
| Other | Es una categoría utilizada para clasificar archivos que no son clasificados por las categorías anteriores, de los cuales la mayoría no son maliciosos, pero existen varios que aún deben ser llevados a la atención de los administradores. Usualmente se produce porque tienen usos potencialmente negativos o impactan negativamente sobre un sistema o red. |  |

**Dual Use**

“Doble uso” que el archivo puede utilizarse con fines tanto maliciosos y no maliciosos. Es importante resaltar que se debe tener cuidado al permitir el uso de estos archivos en su organización. Por ejemplo, mientras que PsExec puede ser una herramienta útil para ejecutar procesos en otro sistema, ese mismo beneficio puede ser utilizado para ejecutar archivos maliciosos en otro sistema:

| **Subclase** | **Definición** | **Ejemplos** |
| --- | --- | --- |
| Crack | Tecnologías que pueden alterar (o crackear) otra aplicación con el fin de eludir las limitaciones de licencia o la protección de la gestión de derechos digitales (DRM). |  |
| Generic | Cualquier herramienta de doble uso que no encaje en una categoría existente. |  |
| KeyGen | Tecnologías que permiten generar o recuperar/revelar claves de productos que pueden utilizarse para evitar la gestión de derechos digitales (DRM) o la protección de licencias de software y otros medios digitales. |  |
| MonitoringTool | Tecnologías que rastrean las actividades en línea de un usuario sin conocerlo mediante el registro y, posiblemente, también la transmisión de registros de uno o más de los siguientes elementos:  -pulsaciones de teclas de usuario  -mensajes de correo  -chat y mensajería instantánea  -actividad de navegación web  -capturas de pantalla  -uso de aplicaciones | Veriato 360, Refog Keylogger |
| Pass Crack | Tecnologías que pueden revelar una contraseña u otras credenciales de usuario confidenciales, ya sea mediante la inversión criptográfica de contraseñas o la revelación de contraseñas almacenadas. | l0phtcrack, Cain & Abel |
| RemoteAccess | Tecnologías que pueden acceder a otro sistema de forma remota y administrar comandos en el sistema remoto, o monitorear las actividades del usuario sin notificación o consentimiento del usuario. | Putty, PsExec, TeamViewer |
| Tool | Programas que ofrecen funciones administrativas pero que pueden utilizarse para facilitar ataques o intrusiones. | Nmap, Nessus, P0f |

**Malware**

| **Subclase** | **Definición** | **Ejemplos** |
| --- | --- | --- |
| Backdoor | Malware que proporciona acceso no autorizado a un sistema, eludiendo las medidas de seguridad. | Back Orifice, Eleanor |
| Bot | Malware que se conecta a un servidor central de botnets de Comando y Control (C&C). | QBot, Koobface |
| Downloader | Malware que descarga datos al sistema host. | Staged-Downloader |
| Dropper | Malware que instala otro malware en un sistema. |  |
| Exploit | Malware que ataca una vulnerabilidad específica del sistema. |  |
| FakeAlert | Malware que se disfraza de software de seguridad legítimo para engañar al usuario a fin de que solucione problemas de seguridad falsos a un precio asequible. | Fake AV White Paper |
| Generic | Cualquier malware que no encaje en una categoría existente. |  |
| InfoStealer | Malware que registra credenciales de inicio de sesión y/u otra información confidencial. | Snifula |
| Parasitic | Los virus parasitarios, también conocidos como virus de archivo, se propagan al adjuntarse a los programas. Normalmente, cuando se inicia un programa infectado con un virus parasitario, se ejecuta el código del virus. Para esconderse, este pasa el control al programa original. |  |
| Ransom | Malware que restringe el acceso al sistema o a los archivos y exige el pago por la eliminación de la restricción, lo que hace que el sistema quede sujeto a un pago. | CryptoLocker, CryptoWall |
| Remnant | Cualquier archivo que contenga restos de malware intentará eliminarlo. |  |
| Rootkit | Malware que permite el acceso a un ordenador mientras se protege a sí mismo o a otros archivos para evitar su detección y/o eliminación por parte de administradores o tecnologías de seguridad. | TDL, Zero Access Rootkit |
| Trojan | Malware que se disfraza de programa o archivo legítimo. | Zeus |
| Virus | Malware que se propaga insertandose o añadiéndose a otros archivos. | Sality, Virut |
| Worm | Malware que se propaga copiándose a sí mismo a otro dispositivo. | Code Red, Stuxnet |

Protección de Memoria

Provee diferentes opciones para manejar exploits de memoria, incluyendo inyecciones y escalamiento de procesos.

**Tipos de acciones**

|  |  |
| --- | --- |
| **Opción** | **Descripción** |
| Alert | El agente registrará la violación y reportará el incidente a la consola. |
| Ignore | El agente no tomará ninguna acción contra violaciones de memoria identificadas. |
| Block | Si una aplicación intenta llamar a un proceso con violación de memoria, el agente bloquea la llamada del mismo. La aplicación que hizo la llamada puede seguir ejecutándose. |
| Terminate | Si una aplicación intenta llamar a un proceso con violación de memoria, el agente bloquea la llamada del mismo y también cierra la aplicación que la realizó. |

**Tipos de violaciones de explotación**

|  |  |  |
| --- | --- | --- |
| **Tipo** | **Descripción** | **SO soportados** |
| Stack Pivot | El stack para un thread ha sido reemplazado por un stack diferente. Generalmente el sistema sólo asigna un stack por thread. Un atacante podría usar un stack diferente para controlar la ejecución de manera que no sea bloqueada por el Data Execution Prevention (DEP). | Windows  macOS\*  Linux |
| Stack Protect | Esta protección ha sido modificada para permitir el permiso de ejecución. La memoria stack no debería ser ejecutable, esto puede significar que un atacante se está preparando para correr código malicioso almacenado en la memoria stack como parte de un exploit, un intento que de otra manera sería bloqueado por el DEP. | Windows  macOS\*  Linux |
| Overwrite Code | Código que reside en la memoria de un proceso que fue modificada usando una técnica que podría indicar un intento de bypass del DEP. | Windows |
| RAM Scrapping | Un proceso está tratando de leer datos de rastreo válidos de la cinta magnética de otro proceso. Normalmente, esta violación es asociada con los Point of sale Systems (POS). | Windows |
| Malicious Payload | Una detección genérica de código shell y payloads asociada con explotación ha sido detectada. | Windows |

\*Sólo soportado en macOS Catalina y anteriores.

**Con agentes en versión 1580 o posteriores**

|  |  |  |
| --- | --- | --- |
| **Tipo** | **Descripción** | **SO soportados** |
| System Call Monitoring | Una llamada de sistema hecha a una aplicación o sistema operativo ha sido detectada. | Windows |
| System DLL Overwrite | Un intento de sobreescribir un archivo DLL del sistema ha sido detectado. | Windows |
| Dangerous COM Object | Código malicioso que tiene una referencia a un Component Object Model (COM) ha sido detectado. | Windows |
| Injection via APC | Se ha detectado un proceso que está inyectando código arbitrario en el proceso objetivo utilizando una Asynchronous Procedure Call (APC) o iniciando un thread remoto para llamar a la LoadLibrary, o una función similar.  Si esta política está configurada como Alert, puede esperar ver alertas tanto para inyecciones válidas como maliciosas que tengan lugar para aplicaciones en dispositivos Windows. La alerta reporta sobre la aplicación que recibió la inyección, pero se debe determinar el origen del ejecutable que causó la alerta. Para obtener información sobre la recopilación de los datos necesarios que pueden ayudar a determinar si una inyección era válida o maliciosa, visite support.blackberry.com para leer el artículo KB 92422.  Si esta política está configurada como Block o Terminate, impide la ejecución de cualquier aplicación reportada en el dispositivo, incluso si es válida. Esto puede causar una interrupción en las actividades diarias del usuario. La compatibilidad con las exclusiones se añadirá en una próxima versión del agente CylancePROTECT Desktop 3.1. | Windows |

**Con agentes en versión 3.0.1000 o posteriores**

|  |  |  |
| --- | --- | --- |
| **Tipo** | **Descripción** | **SO soportados** |
| Dangerous VBA Macros | Un macro que contiene implementaciones peligrosas ha sido detectado.  Para proteger dispositivos con agentes versión 1580 y posteriores contra macros maliciosos, activar y configurar la política de Protección de Memoria. La misma soporta exclusiones en agentes versión 3.0 y posterior.  Para proteger dispositivos con agentes versión 1578 y previas contra macros maliciosos, activar y configurar la política de Script Control y sus exclusiones. | Windows |

**Tipos de violaciones de inyección de procesos**

|  |  |  |
| --- | --- | --- |
| **Tipo** | **Descripción** | **SO soportados** |
| Remote Allocation of Memory | Un proceso ha asignado memoria en otro proceso. La mayoría de las asignaciones sólo ocurren dentro del mismo proceso. Esto puede indicar un intento de inyectar código o información en otro proceso para reforzar una presencia maliciosa en un sistema | macOS |
| Remote Mapping of Memory | Un proceso ha introducido código y/o información en otro proceso. Esto puede indicar un intento de comenzar la ejecución de código en otro proceso y por lo tanto reforzar una presencia maliciosa. | Windows  macOS |
| Remote Write to Memory | Un proceso ha modificado la memoria de otro proceso. Esto puede indicar un intento de almacenar código o datos en la memoria previamente asignada, pero es posible que un atacante esté intentando sobrescribir la memoria existente para desviar la ejecución con un propósito malicioso. | Windows  macOS |
| Remote Write PE to Memory | Un proceso ha modificado la memoria de otro proceso para contener una imagen ejecutable. Generalmente esto indica que un atacante está intentando ejecutar código sin escribir primero ese código en el disco. | Windows |
| Remote Overwrite Code | Un proceso ha modificado la memoria ejecutable de otro proceso. En condiciones normales, la memoria ejecutable no sería modificada, especialmente por otro proceso. Esto suele indicar un intento de desviar la ejecución en otro proceso. | Windows |
| Remote Unmap of Memory | Un proceso ha eliminado un ejecutable de Windows de la memoria de otro proceso. Esto puede indicar una intención de sustituir la imagen del ejecutable por una copia modificada con el fin de desviar la ejecución. | Windows  macOS |
| Remote Thread Creation | Un proceso ha creado un nuevo thread en otro proceso. Los threads de un proceso suelen ser creados únicamente por ese mismo proceso. Esto es generalmente utilizado por un atacante para activar una presencia maliciosa que ha sido inyectada en otro proceso. | Windows  macOS\* |
| Remote APC Scheduled | Un proceso ha desviado la ejecución del thread de otro proceso. Esto es generalmente utilizado por un atacante para activar una presencia maliciosa que ha sido inyectada en otro proceso. | Windows |
| DYLD Injection | Se ha establecido una variable de entorno que hará que se inyecte una biblioteca compartida en un proceso iniciado. Los ataques pueden modificar la lista de aplicaciones como Safari o reemplazar aplicaciones con scripts bash, que hacen que sus módulos se carguen automáticamente cuando se inicia una aplicación. | macOS\*  Linux |

**Con agentes en versión 1580 o posteriores**

|  |  |  |
| --- | --- | --- |
| **Tipo** | **Descripción** | **SO soportados** |
| Remote Allocation of Memory | Un proceso ha asignado memoria en otro proceso. La mayoría de las asignaciones sólo ocurren dentro del mismo proceso. Esto puede indicar un intento de inyectar código o información en otro proceso para reforzar una presencia maliciosa en un sistema | macOS |
| Doppelganger | Se ha iniciado un nuevo proceso malicioso desde un archivo que aún no se ha escrito en el sistema de archivos. La transacción de escritura del archivo se suele revertir después de que se inicie el proceso (para que el archivo malicioso nunca se consigne en el disco), y cualquier intento de analizar el archivo en el disco sólo verá el archivo benigno sin modificar. | Windows |
| Dangerous Environmental Variable | Se ha detectado una variable de entorno que puede tener código malicioso adjunto. | Windows |

\*Sólo soportado en macOS Catalina y anteriores.

**Tipos de violaciones de escalamiento**

|  |  |  |
| --- | --- | --- |
| **Tipo** | **Descripción** | **SO soportados** |
| LSASS Read | Se ha accedido a la memoria perteneciente al proceso Windows Local Security Authority de una manera que indica un intento de obtener las contraseñas de los usuarios. | Windows |
| Zero Allocate | Se ha asignado una página null. La región de memoria está normalmente reservada, pero en ciertas circunstancias puede ser asignada. Los ataques pueden usar esto para establecer una escalada de privilegios aprovechando algún exploit de null de-reference conocido, normalmente en el kernel. | Windows  macOS\* |

**Con agentes en versión 1580 o posteriores**

|  |  |  |
| --- | --- | --- |
| **Tipo** | **Descripción** | **SO soportados** |
| Memory Permission Changes in Other Processes | Un proceso infractor ha modificado los permisos de acceso a la memoria dentro de otro proceso. Esto se suele hacer para inyectar código en otro proceso y hacer que la memoria sea ejecutable modificando los permisos de acceso a la memoria. | Windows |
| Memory Permission Changes Child Processes | Un proceso infractor ha creado un proceso hijo y ha modificado los permisos de acceso a la memoria en ese proceso hijo. | Windows |
| Stolen System Token | Un token de acceso ha sido modificado para permitir al usuario saltarse los controles de acceso de seguridad | Windows |
| Low Integrity Process Start | Un proceso ha sido ejecutado con un bajo nivel de integridad | Windows |

\*Sólo soportado en macOS Catalina y anteriores.

# INFORMACIONES Y CONSULTAS

|  |
| --- |
| Security Operations Center  [soc@ransecurity.com](mailto:soc@ransecurity.com) |

|  |  |
| --- | --- |
| **H:\Disco local\Andres Mellizo\RANSecurity (amellizo)\IMAGENES\LOGOTIPOS\NUEVOS LOGOS RAN2016\RAN_logo\RAN_box.jpg** | [www.ransecurity.com](http://www.ransecurity.com) |
| **1450816303_square-linkedin** | [/RANsecurity](http://www.linkedin.com/company/ransecurity) |
| **1450816313_square-twitter** | [@RANsecurity](https://twitter.com/RANSecurity) |

**Sobre RANsecurity®.**  |  Somos una empresa  líder en Seguridad Informática establecida en Argentina desde 1991, y con operaciones en Chile, Perú y Uruguay, ofreciendo soluciones de seguridad informática de primera calidad en las áreas de: •Firewall de próxima generación (NGFW) •Control de acceso a la red (NAC) •Seguridad y cumplimiento para entornos virtuales •Protección y Antivirus para servidores y estaciones de trabajo •Gestión y protección de dispositivos móviles •Protección de e-mail y web •Correlación de eventos (SIEM) •Gestión de Vulnerabilidades •Control de cambios para servidores y puntos de venta •Gestión de licencias de software y control de activos tecnológicos •Gestión de permisos privilegiados, entre otros.

Somos el VAR más importante de Intel Security (McAfee) en la región y socio estratégicos de: •ForeScout •Forcepoint•Cylance •Tripwire •Varonis, •Blackberry Good •Proofpoint, también desarrolla la solución de gestión de activos de IT y soporte técnico con su marca fixIQ®.

Adicionalmente contamos con un área especializada de servicios llamada servicios expertos®, que ofrece servicios de: •Implementación de soluciones de seguridad informática •Actualizaciones y migraciones •Gestión de infraestructura informática •Administración remota y en sitio •Auditoría •Análisis GAP •Outsourcing •co-sourcing, y •Capacitaciones. Contamos con un plantel de expertos certificados con experiencia en entornos heterogéneos, distribuidos y envergaduras diversas.

Más de 500 empresas avalan nuestros servicios. Para mayor información, visite: [www.ransecurity.com](http://www.ransecurity.com)