

<!--MITIC / CERT-PY-->

# DEFENDIENDO CONTRA ATAQUES DE RANSOMWARE

@CERTpy



Marcos Centurion



@LiquidIv4n

# En este Webinar

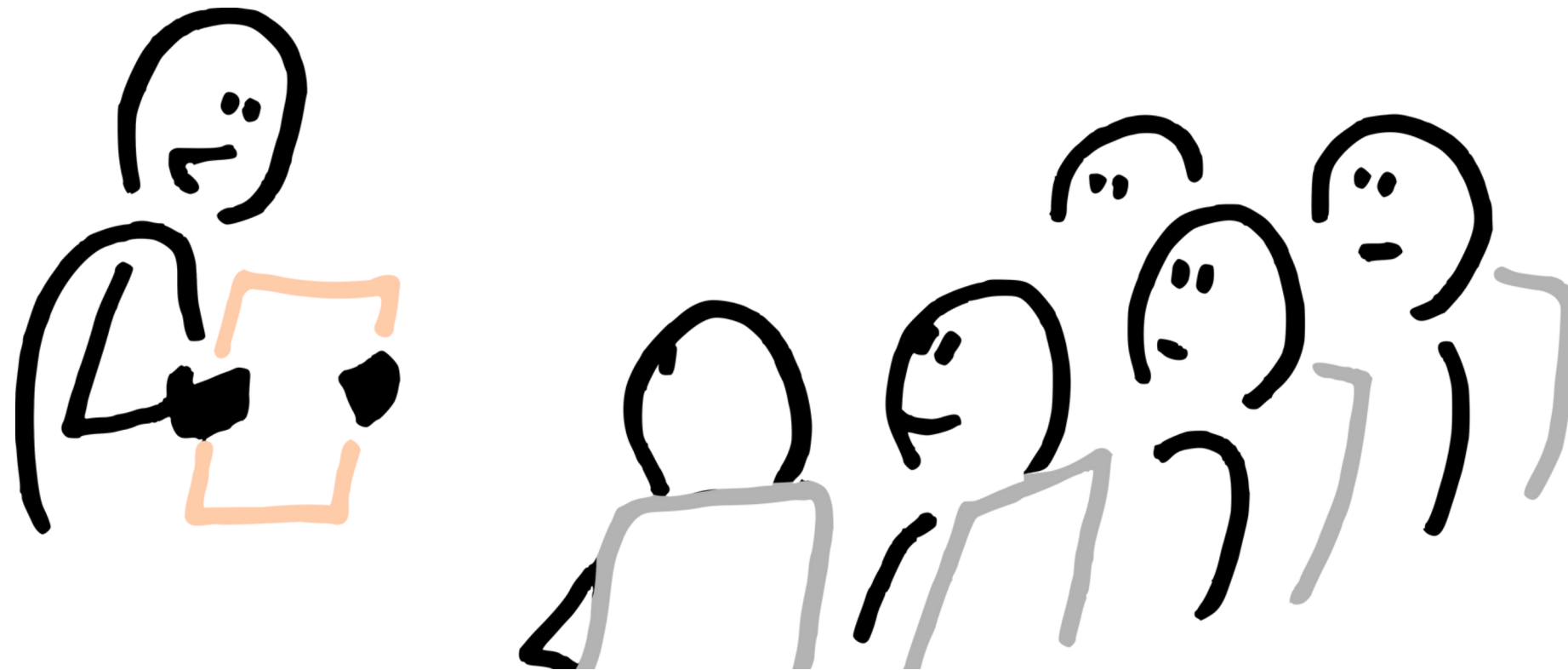


- 01 **Introducción y Resumen General**
  - Objetivos
  - Ransomware Tendencias
- 02 **Ransomware**
  - Perspectiva Global
  - Acciones a tomar
  - Vectores Ataque
  - Cómo prepararse?
- 03 **Ataques de Ransomware**
  - Detección y Análisis
  - Contención, Erradicación y Recuperación
  - Recuperación y Post-Incidente
  - Ransomware como Servicio (RaaS)
  - Human Operated Ransomware
  - Buenas Prácticas
- 04 **Casos de Estudio**
  - Ransomware en Instituciones Paraguayas
  - Lecciones Aprendidas

# Introducción...

# Audiencia

Dirigido para el personal de seguridad informática y los administradores de programas; administradores de sistemas, redes y aplicaciones; equipos de respuesta a incidentes; y otros que sean responsables de realizar funciones relacionadas con la gestión de ciberseguridad



# Objetivo General

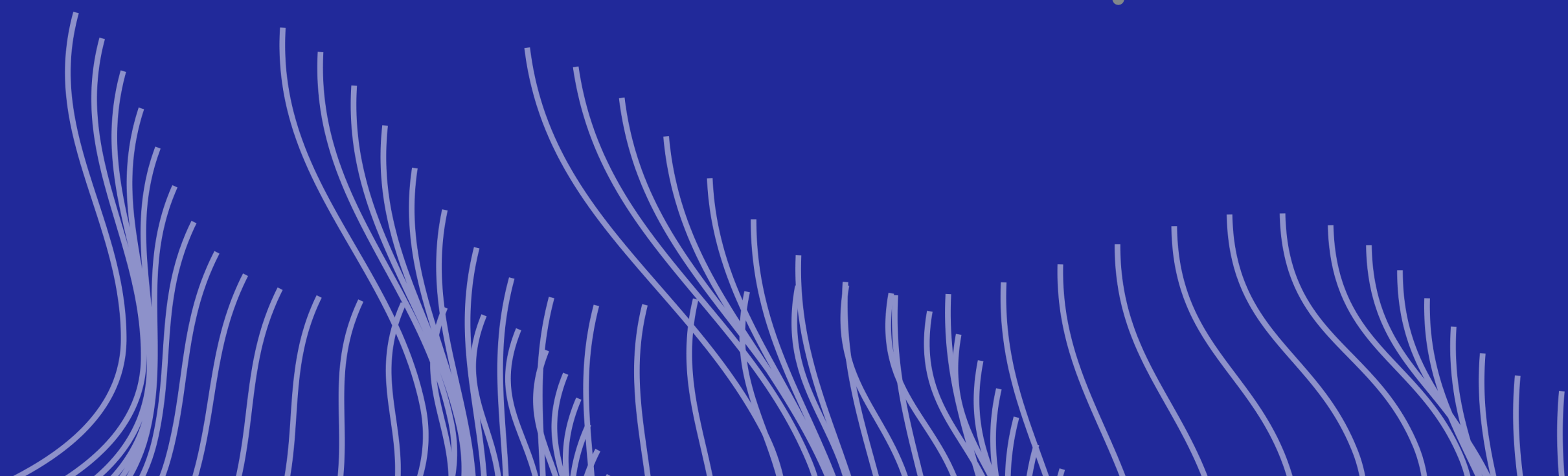
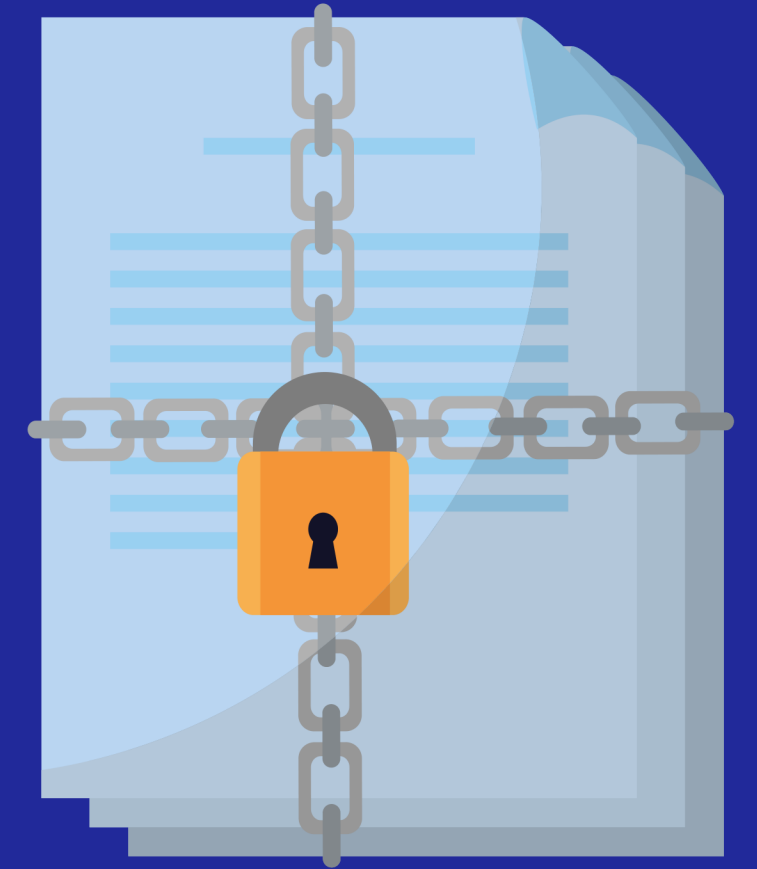
Proveer una introducción general ante eventos de ransomware que le permitan defenderse usted mismo y a su organización de los ataques de ransomware, a través del conocimiento de los puntos de vulnerabilidad individuales y organizacionales.

## Objetivos Específicos

- Definir que es el Ransomware
- Listar Medidas Preventivas
- Citar Medidas de Detección y Respuesta



Explicando que es el ransomware...



# Ransomware

El ransomware es un tipo de software malicioso (malware) utilizado por ciberdelincuentes secuestrar los datos de la organización y extorsionarla bajo distintas amenazas. El ransomware cifra la información almacenada en su computadora y sistemas, para solicitar el pago de un rescate a cambio del descifrado.

Los incidentes de ransomware pueden afectar gravemente los procesos operativos de su organización y dejarla sin los datos que necesitan para operar, paralizando a la organización

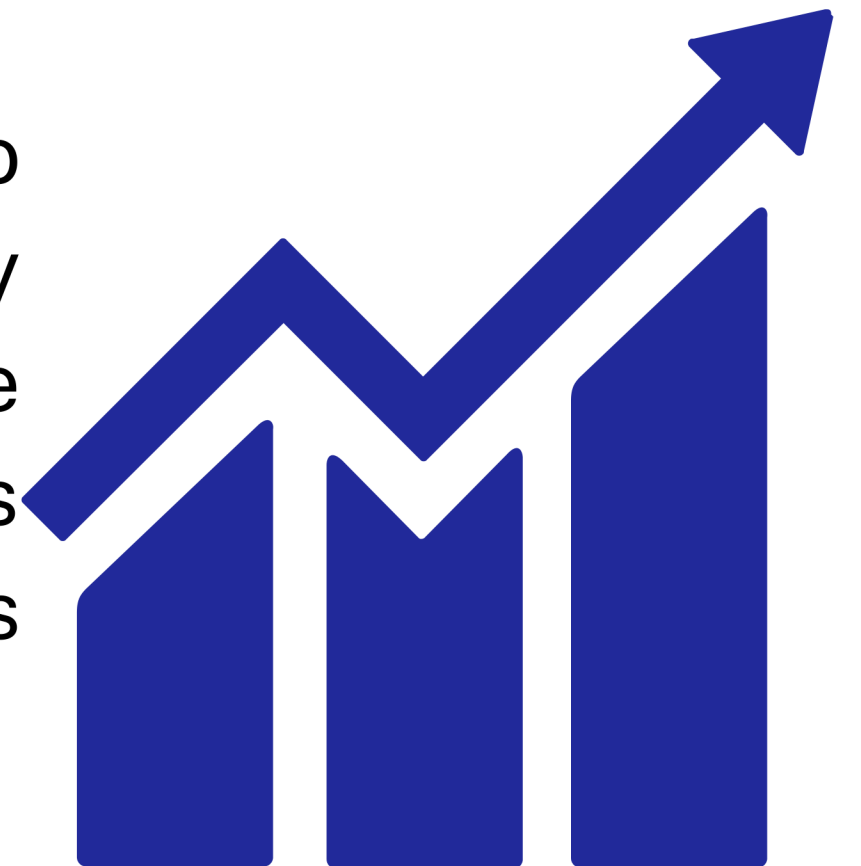


El impacto económico y reputacional de los incidentes de ransomware, durante la interrupción inicial y, en ocasiones, la recuperación extendida, también han demostrado ser un desafío para las organizaciones grandes y pequeñas.

# Ransomware en constante desarrollo

El ransomware se encuentra en constante evolución, los actores maliciosos se encuentran día a día desarrollando, mejorando el código fuente de sus malware, agregando nuevos algoritmos de cifrado y combinaciones de técnicas de encriptación, agregando nuevas capacidades, para cifrar archivos en los dispositivos de sus víctimas, inutilizando cualquier archivo y los sistemas que dependen de ellos.

Luego, los actores malintencionados exigen un rescate a cambio del descifrado. Los actores de ransomware a menudo apuntan y amenazan con vender o filtrar datos extraídos o información de autenticación si no se paga el rescate. En los últimos años, los incidentes de ransomware se han vuelto cada vez más frecuentes en nuestra region de latinoamerica.





# Ransomware en Latinoamérica

- Ransomware como LockBit 3.0, Hive, Onyx
- Ventas de accesos en foros de cibercrimen
- Sectores afectados
  - Tecnológico
  - Construcción
  - Portuario
  - Educación
  - Gubernamental
- Filtraciones de información con afectación a entidades públicas y empresas privadas en América Latina



31 May 

Conti  
Gobierno CR

8 Ago 

Hive  
Entidad Gubernamental

19 Sep 

Lockbit 3.0  
OKI Ltda

21 Sep 

Qilin  
Magazine Torra Ltda

21 Sep 

Lockbit 3.0  
Universidad Int. Ecuador

22 Sep 

Hive  
Agencia Marítima Global

26 Sep 

Lockbit 3.0  
Poder Judicial de Chile

# Ransomware en Latinoamérica



Se espera que se mantenga un nivel elevado de actividad cibercriminal con afectación en América Latina. Los sectores educativo, sanidad, gubernamental, tecnología y manufacturero continuarán siendo los más afectados por incidentes de ransomware y filtraciones de información.

Aumentarán el número de incidentes de insiders en empresas con un gran número de clientes y con sedes en terceros países con una renta per cápita baja. Se ha observado un aumento significativo en el interés de los actores por obtener acceso inicial a dichas empresas a través de sus propios empleados ofreciendo, a través de redes sociales como LinkedIn o canales de comunicación externos con las empresas, elevadas cantidades de dinero por su colaboración. También se identificaron nuevos incidentes de ciberseguridad que hacían uso de técnicas de ingeniería social sobre los empleados de la empresa para aprobar solicitudes de acceso o código recursivas a segundos factores de autenticación.


El grupo de ransomware LockBit 3.0 continuará siendo el grupo más activo. Se espera que la actividad de otros grupos de ransomware conocidos aumente significativamente.



## En Perpestiva

El ransomware continúa dominando el panorama de amenazas en 2022. Las organizaciones están bajo el asedio de una amplia variedad de amenazas, pero el ransomware ofrece a los actores de amenazas una combinación única de muy bajo riesgo con muy alta recompensa, razón por la cual el volumen de los ataques de ransomware casi se duplicaron desde el año anterior y el costo total del ransomware se estimó que superaba los 20.000 millones de dólares.

<https://www.cybereason.com/hubfs/dam/collateral/reports/Ransomware-The-True-Cost-to-Business-2022.pdf>



# Ataques de ransomware, acciones a tomar

## Estar preparado

Mantener copias de seguridad cifradas y fuera de línea de los datos y probar periódicamente sus copias de seguridad.

Elabore un plan básico de respuesta a incidentes cibernéticos y un plan de comunicaciones asociado que incluya procedimientos de respuesta y notificación para un incidente de ransomware

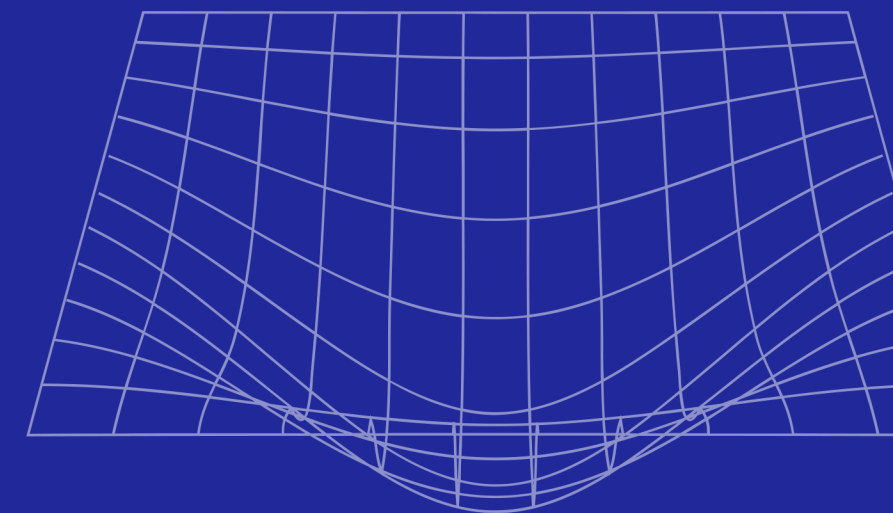
## Conocer los vectores de ataques

Vulnerabilidades y errores de configuración relacionados con Internet

Vector de infección de ransomware: phishing

Vector de infección de ransomware: Infección de malware precursor

Vector de infección de ransomware: terceros y proveedores de servicios gestionados



# Estar preparado..

**Mantener copias de seguridad cifradas y fuera de línea de los datos y probar periódicamente sus copias de seguridad.**

CIRCULAR MITIC - N"01/2021

[https://www.cert.gov.py/wp-content/uploads/2022/02/CIRCULAR\\_MITIC\\_01-21.pdf](https://www.cert.gov.py/wp-content/uploads/2022/02/CIRCULAR_MITIC_01-21.pdf)

1. Todo Organismo y Entidad del Estado (OEE) debe contar con un inventario de activos, en el cual tenga identificado claramente aquellos activos de información digitales imprescindibles para el funcionamiento de su organización
2. Todo OEE debe establecer una política o protocolo de gestión de respaldo de seguridad, con procedimientos, mecanismos o herramientas específicas para cada activo de información digital identificado como imprescindible.
3. Los procedimientos de respaldo de cada activo de información digital identificado como imprescindible deben contener, como mínimo, la siguiente información (responsable, criticidad, etc)

# Estar preparado.. Parte 2

**Elabore un plan básico de respuesta a incidentes cibernéticos y un plan de comunicaciones asociado que incluya procedimientos de respuesta y notificación para un incidente de ransomware**

CIRCULAR MITIC - N°01/2021

[https://www.cert.gov.py/wp-content/uploads/2022/02/CIRCULAR\\_MITIC\\_01-21.pdf](https://www.cert.gov.py/wp-content/uploads/2022/02/CIRCULAR_MITIC_01-21.pdf)

4. Todo OEE deberá implementar medidas de seguridad básicas tendientes a minimizar el riesgo de infección de ransomware...

6. El Responsable de Seguridad de la Información o en su defecto el Director de TIC del OEE o equivalente, serán los responsables de realizar las acciones y gestiones necesarias tendientes a la implementación de las directivas de la presente Circular en su organización.

7. en caso de sufrir un incidente cibernético

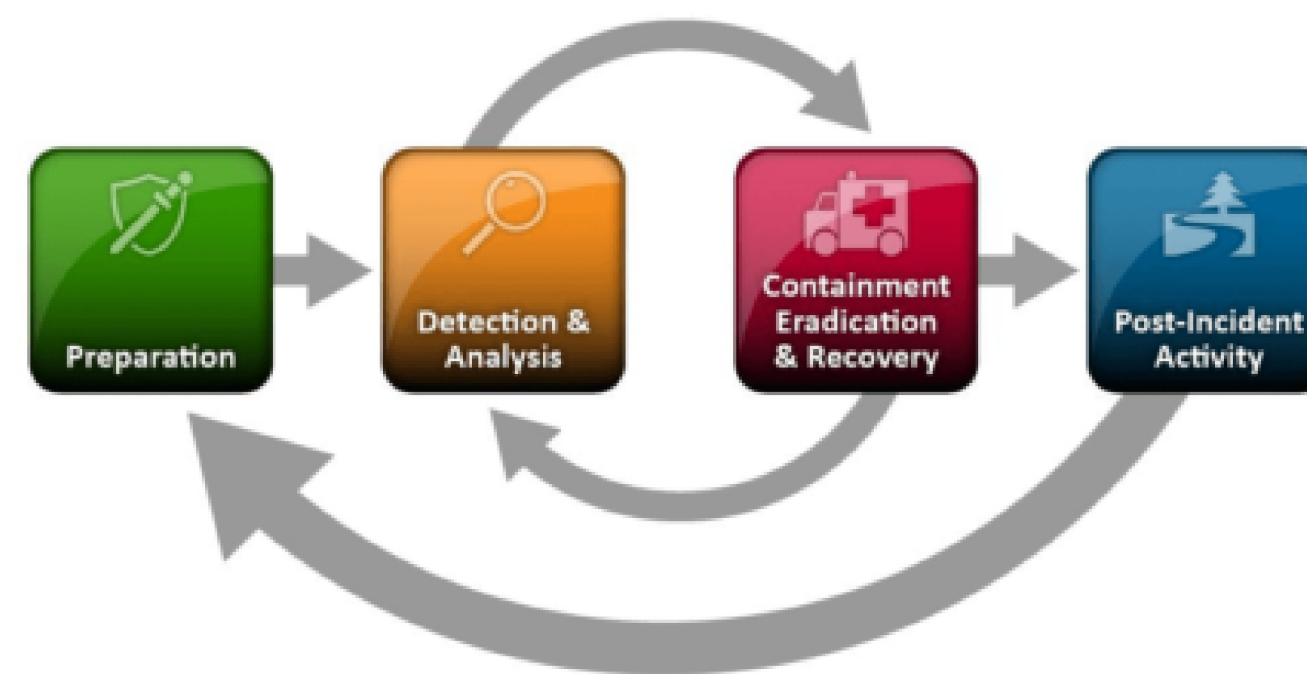
relacionado a ransomware o cualquier otro incidente de seguridad, el mismo debe ser reportado obligatoriamente al MITIC, conforme lo establecido en la Resolución MITIC N° 346/2020.

# Estar preparado / CERT-PY Parte 3

Mantener copias de seguridad cifradas y fuera de línea de los datos y probar periódicamente sus copias de seguridad.

Elabore un plan básico de respuesta a incidentes cibernéticos y un plan de comunicaciones asociado que incluya procedimientos de respuesta y notificación para un incidente de ransomware

- Equipo cualificado
- Capacidades de Detección y Análisis
- Playbooks
  - Específicos
  - Generalidades
- Comunidad Regional
- Feeds de información



# Conocer los vectores de ataques

## Vulnerabilidades y errores de configuración relacionados con Internet

- Vulnerabilidades conocidas presentes en dispositivos y sistemas
  - Regularmente parchear y actualizar el software
- Dispositivos y sistemas desactualizados, sin soporte y sistemas en EOL
  - Parchee y actualice periódicamente el software y los sistemas operativos a las últimas versiones disponibles.
- Dispositivos configurados incorrectamente y funciones de seguridad deshabilitadas
  - Deshabilite los puertos y protocolos que no se utilizan para fines relacionados con el negocio de la organización, habilite funciones y características de seguridad
- Aplicar las mejores prácticas para el uso de RDP y otros servicios de escritorio remoto
  - Solo equipos permitidos, comunicación cifrada, autenticación de doble factor
- Deshabilite el protocolo SMB saliente y elimine o deshabilite las versiones obsoletas de SMB
  - Deshabilitar SMBv1 y SMBv2 de la red interna de la organización
- Bloquear todas las versiones de SMB para que no sean accesibles desde internet hacia la red interna de la organización
  - Bloquear el puerto 445, puertos 137, 138 y 139



# Conocer los vectores de ataques

## Vector de infección de ransomware relacionado con el phishing

- Usuarios víctimas de técnicas de phishing
  - Implemente un programa de capacitación y concientización del usuario sobre seguridad cibernética que incluya orientación sobre cómo identificar y reportar actividades sospechosas
  - Realice pruebas de phishing en toda la organización para medir la conciencia del usuario y reforzar la importancia de identificar posibles correos electrónicos maliciosos.
- Correo malicioso
  - Implemente filtros en la puerta de enlace de correo electrónico para filtrar los correos electrónicos con indicadores maliciosos conocidos, como líneas de asunto maliciosas conocidas
  - bloquee las direcciones IP (Protocolo de Internet) sospechosas en el firewall.
  - Implemente política DMARC
- Deshabilitar el envío de archivos tipo scripts en el sistema de correos, deshabilitar la ejecución de macros para los archivos de Microsoft Office transmitidos por correo electrónico

# Conocer los vectores de ataques

## Vector de infección de ransomware relacionado con infección de malware precursor(Droppers, programas maliciosos)

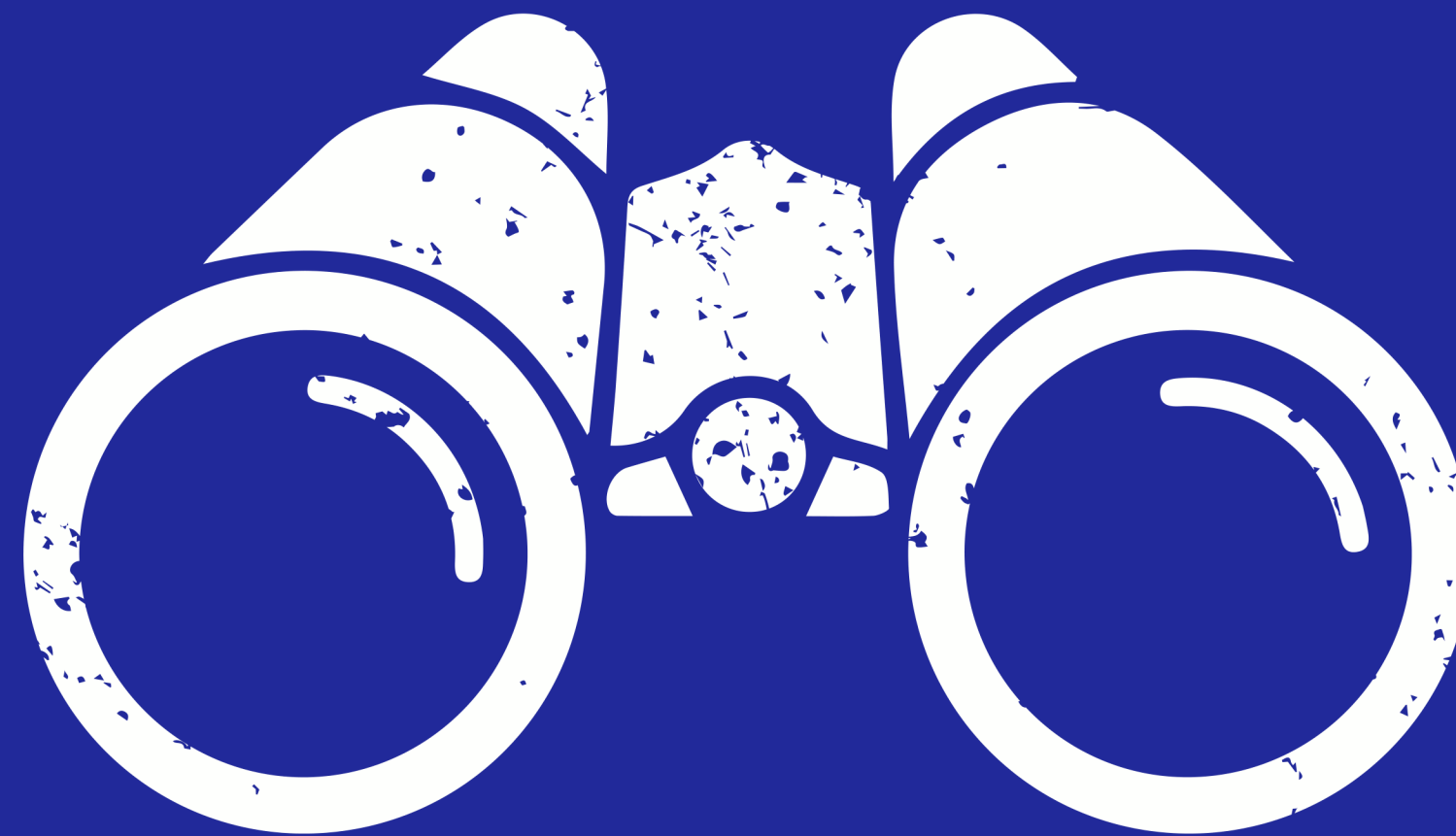
- Bases de firmas de datos desactualizadas en el servidor y endpoints
  - Asegúrese de el software y las firmas de antivirus, antimalware estén actualizados, active las actualizaciones automáticas para ambas soluciones
    - Una infección de ransomware puede ser evidencia de un compromiso de red del caso anterior no resuelto
- Ausencia de políticas de restricción aplicaciones
  - Aplicar una lista de blanca o lista de software permitido, para garantizar que solo el software autorizado y fidedigno se ejecute, bloquear software no autorizado
- Ausencia controles de detección de amenazas
  - Considere implementar un sistema de detección de intrusiones (IDS) para detectar actividad maliciosa como actividad de comando y control y otra actividad potencial de la red.

# Conocer los vectores de ataques

## Vector de infección de ransomware relacionado con terceros y proveedores de servicios gestionados (cadena de suministros)

- Proveedores de Servicios Gestionados como vector de infección
  - Asegúrese que su Proveedor de Servicios Gestionados adopte las mejores prácticas
  - Promueva el uso del lenguaje contractual para formalizar su seguridad
- Atacantes pueden falsificar la identidad de un proveedor, usar información comprometida (cuentas de correo electrónico, accesos de red) para ingresar malware dentro de la organización
- Atacantes pueden apuntar como objetivo al Proveedor de Servicios Gestionados, comprometerlo y utilizarlo para ingresar a la organización

# Detección & Análisis



# Detección y Análisis

- Análisis del Impacto
  - Consulte con su equipo para desarrollar y documentar una comprensión inicial de lo que ha ocurrido en base al análisis inicial
- Determine qué sistemas se vieron afectados e inmediatamente aislelos
  - Si varios sistemas o subredes parecen afectados, desconecte la red en el nivel del conmutador
  - Después de un compromiso inicial, los actores maliciosos pueden monitorear la actividad o las comunicaciones de su organización para entender si sus acciones han sido detectadas
  - Solo en caso de que no pueda desconectar los dispositivos de la red, apáguelos para evitar una mayor propagación de la infección de ransomware.
- Triage - Clasificar sistemas afectados para restauración y recuperación
  - Identifique y priorice los sistemas críticos para la restauración y confirme la naturaleza de los datos alojados en los sistemas afectados
  - Priorice la restauración y recuperación en función de una lista de activos críticos predefinida.
- Comunicar
  - Comparte la información que tienes a tu disposición para recibir la asistencia más oportuna y pertinente. Mantenga informados a la gerencia y líderes de su organización.



PAULSÉE



## **Aviso!**



Recuerde: pagar un rescate no garantizará que sus datos se descifren o que sus sistemas o datos ya no se vean comprometidos, tampoco elimina la amenaza



# Contención, Erradicación





# Contención, Erradicación y Recuperación

- Resguardar Evidencias
  - Resguardar archivos ejecutables
  - Copiar el archivo README.xx no eliminar ninguno de ellos, copia de la nota de rescate
  - Capturar estado de la memoria RAM
  - Muestras de malware
  - Ejemplos de archivos cifrados (Copiar)
  - Archivos de registro (Registro de eventos Microsoft) de sistemas comprometidos
  - Cualquier script de PowerShell encontrado que tenga ejecutado en los sistemas
  - Cualquier cuenta de usuario creada en Active Directory o máquinas agregadas a la red durante la explotación
  - Direcciones de correo electrónico utilizadas por los atacantes y cualquier correo electrónico de phishing asociado
  - Carteras de Bitcoin utilizadas por los atacantes
- Claves de decripción
  - Consulte a las organizaciones competentes sobre posibles descifradores disponibles

# Contención, Erradicación y Recuperación Parte 2

- Investigar Guías
  - Investigue la guía confiable, para la variante de ransomware en particular y siga los pasos adicionales recomendados para identificar y contener sistemas o redes que se confirmen afectados
  - Eliminar o deshabilitar la ejecución de archivos binarios de ransomware conocidos; esto minimizará el daño y el impacto en sus sistemas.
- Desarrollar Análisis de Registros/Logs
  - Llevar a cabo un examen de la detección organizacional existente o sistemas de prevención (antivirus, Endpoint Detection & Response, IDS, Sistema de prevención de intrusiones, etc.) y registros. Hacerlo puede resaltar la evidencia de sistemas adicionales o malware involucrado en etapas anteriores del ataque.
- Priorizar Servicios Críticos
  - Reconstruir sistemas basados en una priorización de servicios críticos (por ejemplo, salud y seguridad o servicios generadores de ingresos), utilizando imágenes estándar preconfiguradas, si es posible.

# Contención, Erradicación y Recuperación Parte 3

- Cambiar las contraseñas
  - Una vez que el entorno se haya limpiado y reconstruido por completo (incluidas las cuentas afectadas asociadas y la eliminación o corrección de los mecanismos de persistencia maliciosos), restablezca las contraseñas de todos los sistemas afectados.
- Parchear y actualizar el software
  - Luego de una reinstalación de un sistema base, mitigue las vulnerabilidades asociadas. Esto puede incluir la aplicación de parches, la actualización del software y la adopción de otras medidas de seguridad no tomadas previamente.

# Recuperación y Post-Incidente



# Actividad de recuperación y posterior al incidente

- Vuelva a conectar los sistemas y restaure los datos de las copias de seguridad cifradas fuera de línea en función de una priorización de servicios críticos.
  - Tenga cuidado de no volver a infectar los sistemas limpios durante la recuperación. Por ejemplo, si se ha creado una nueva red de área local virtual con fines de recuperación, asegúrese de que solo se le agreguen sistemas limpios.
- Documente las lecciones aprendidas del incidente y las actividades de respuesta asociadas para informar las actualizaciones y refinar las políticas, los planes y los procedimientos organizacionales y guiar los ejercicios futuros de los mismos.
- Considere compartir las lecciones aprendidas y los indicadores relevantes de compromiso con el CERT-PY para compartir y beneficiar a otras organizaciones

# Ransomware as a Service (RaaS)

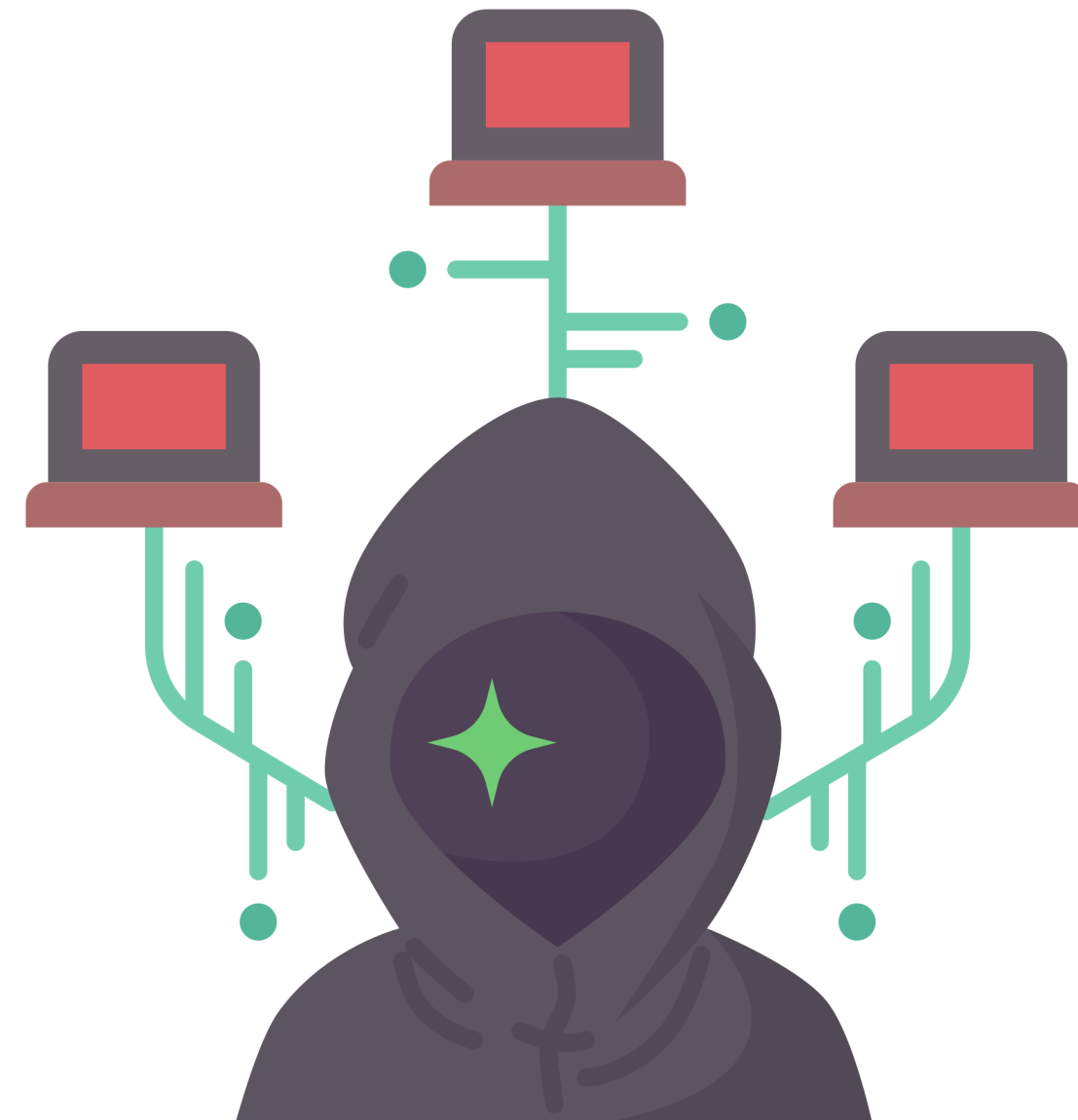
# Ransomware como Servicio (RaaS)

**El ransomware como servicio es un modelo de negocio? en el que actores maliciosos contratan los servicios de un ransomware a través de un programa de afiliados y se encargan de llevar adelante los ataques.**

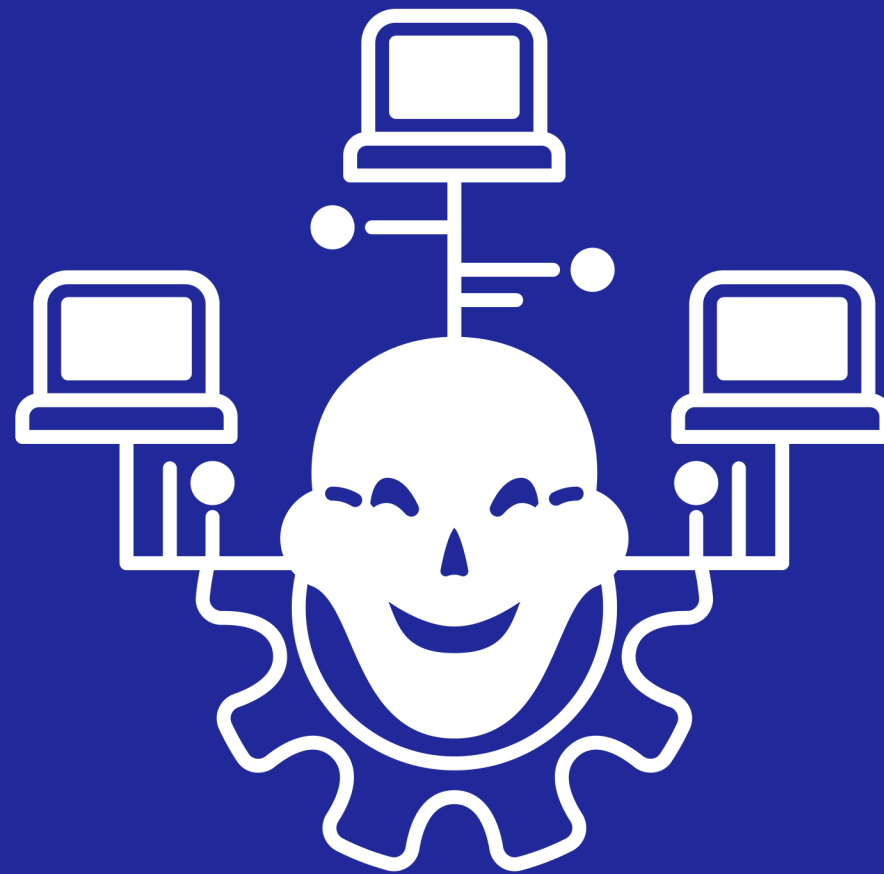
Pre-programados

Automatizados

Atacan miles de dispositivos al mismo tiempo

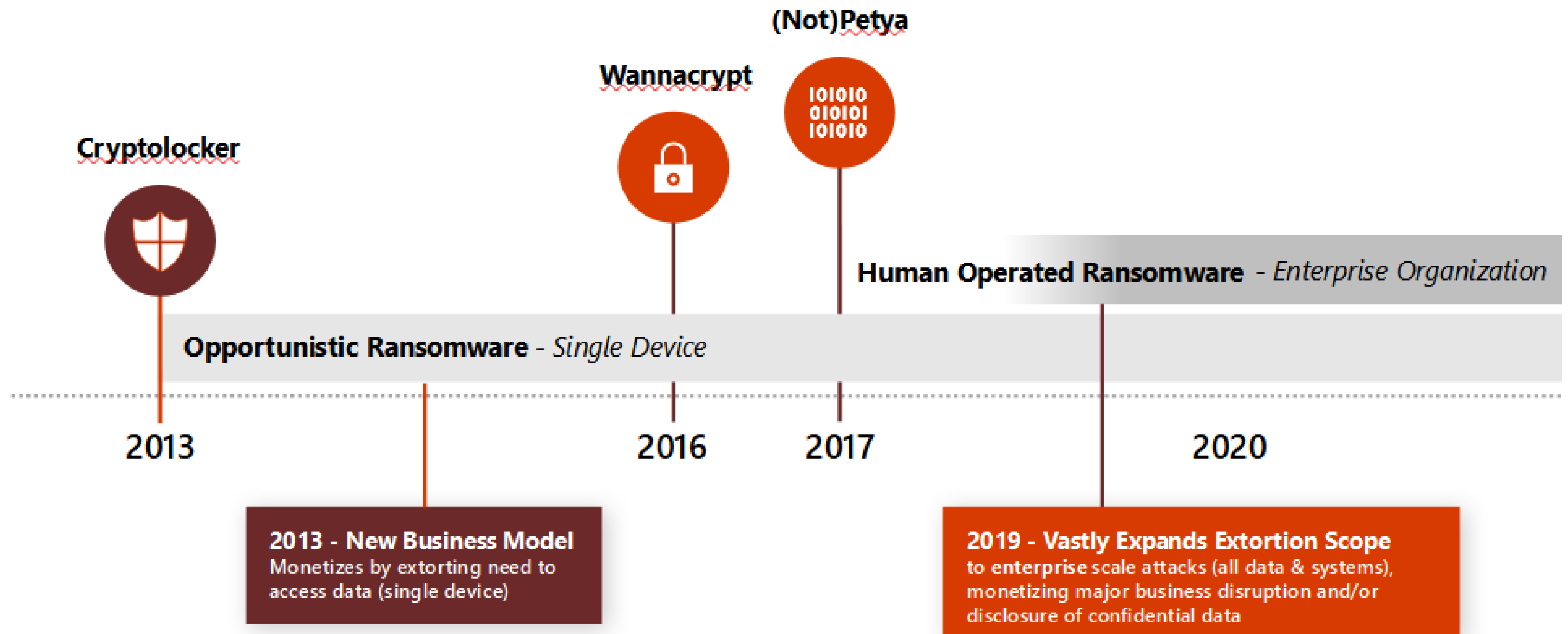


# Human Operated Ransomware





# Evolution of ransomware models



# Evolución de ataques de ransomware

## Human Operated Ransomware - Alto Impacto & Auge

### Cual es la Relación?



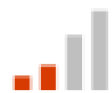
#### Alto impacto en el negocio

La extorsión debe interrumpir las operaciones comerciales para motivar el pago



#### Rentable para las atacantes

Incentivo económico para seguir creciendo



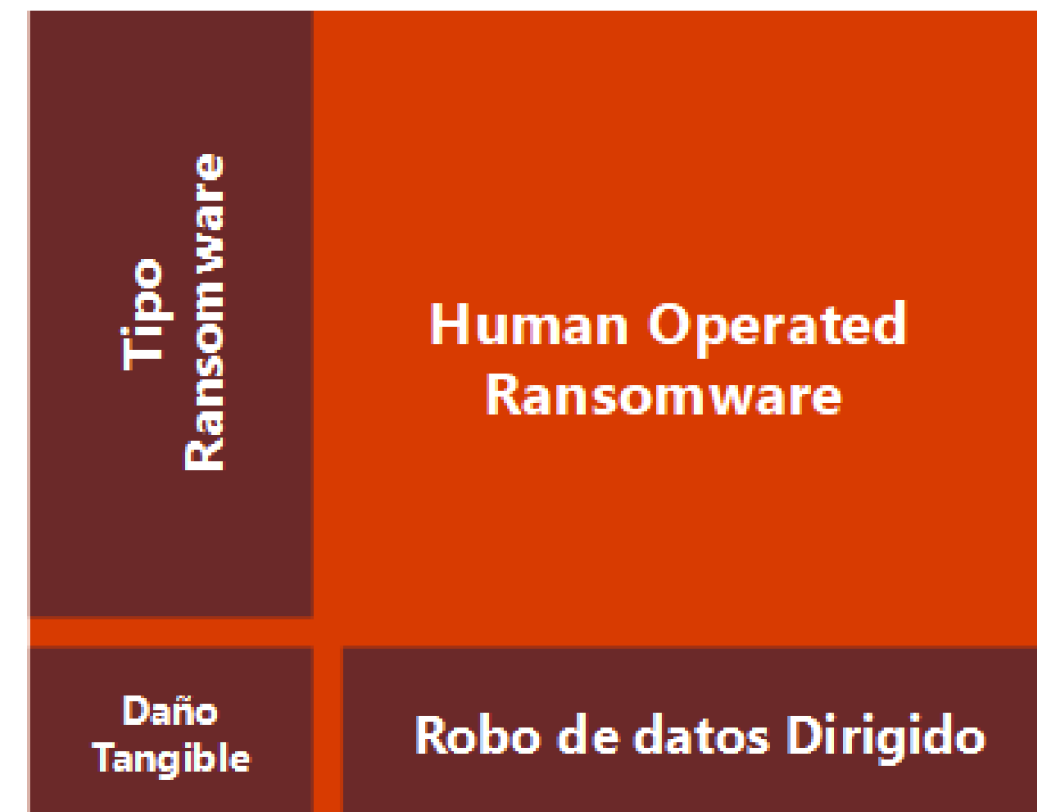
#### Motivos para crecer

Los atacantes pueden monetizar las brechas de mantenimiento de la seguridad en la mayoría de las empresas:

- **Aplicar actualizaciones de seguridad**
- **Configure de forma segura todos los recursos y dispositivos**
- **Mitigar el robo de credenciales**

*Detener Operaciones del Negocio*

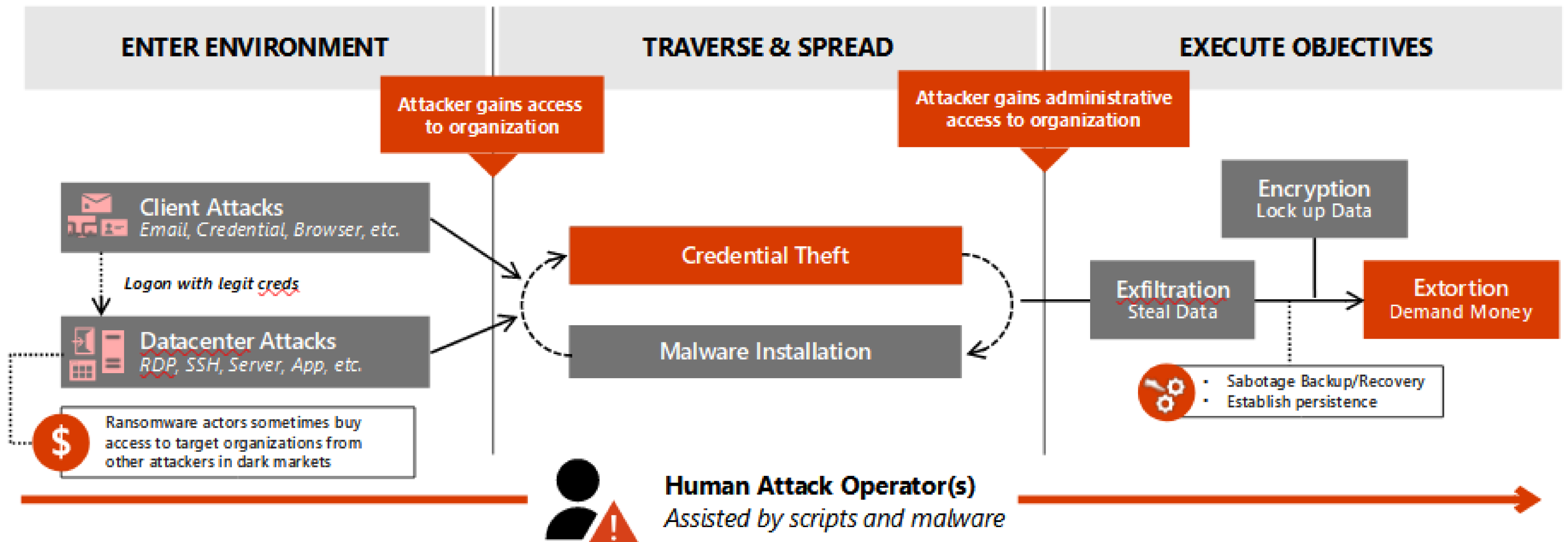
*Impacto Inmediato Limitado*



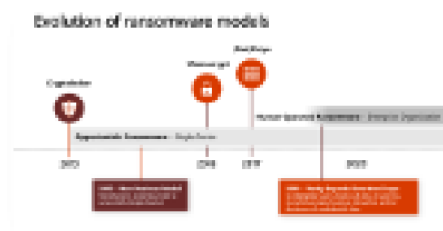
*Por PC*

*Toda La Empresa*

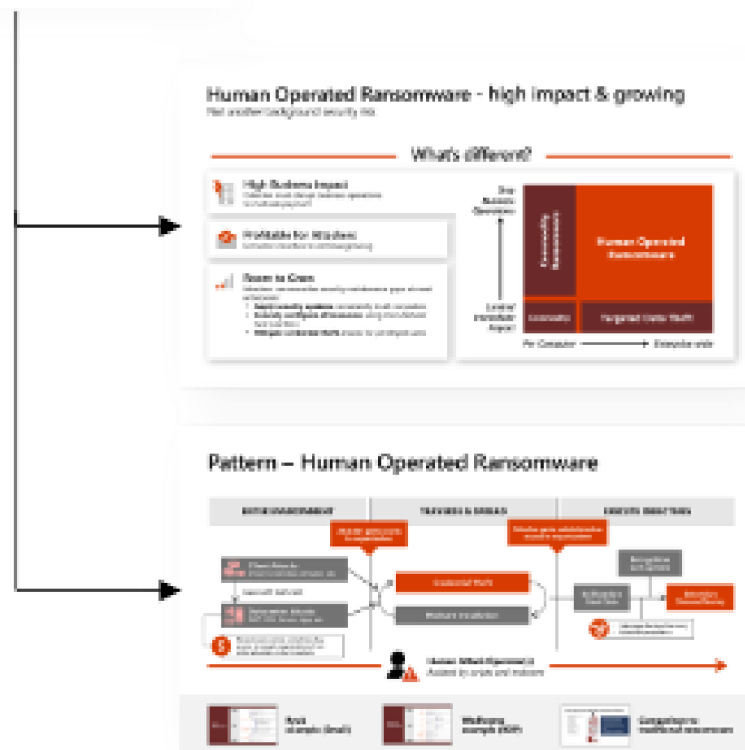
# Pattern – Human Operated Ransomware



# Puntos Claves



**El Esquema ha cambiado con la evolución de la amenaza** Este modelo de esquema cambia el impacto y la probabilidad de los ataques



**Amenaza Continua** – potencial trayectoria de crecimiento por:

- *Rentabilidad para el atacante*
- *Escaza o poca capacidad de persecución por parte de la autoridad competente*

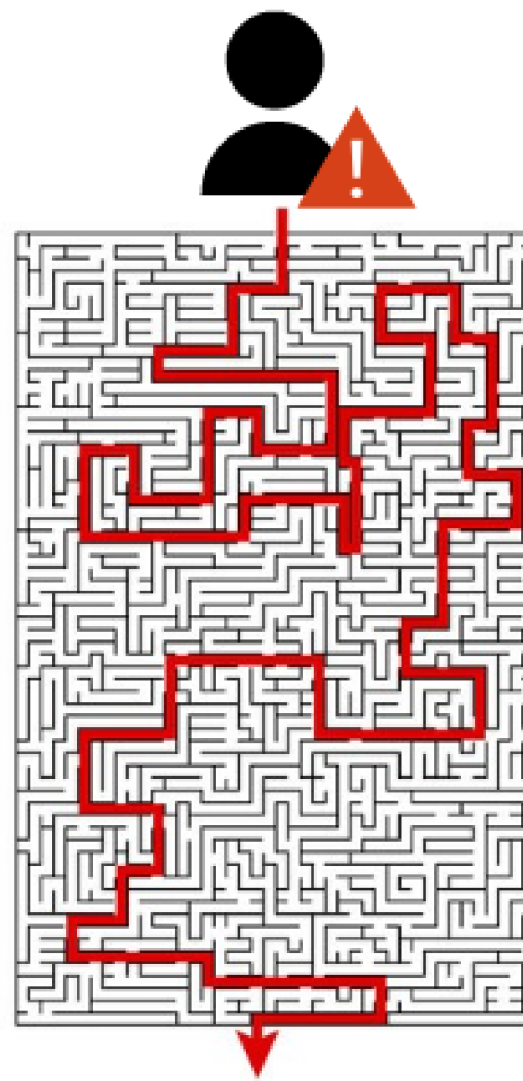
**Los Ataques aprovechan vulnerabilidades** – la extorsión eficiente se basa en:

- *Ganar acceso al activo* – rápidamente con privilegios administrativos
- *Denegando la recuperación* – via backups and recovery processes

# Que vuelve a *human operated* ransomware diferente?

## → Human Operated Ransomware

- Trojano Bancario
- AV Deshabilitado
- Robo de Credenciales
- Cobalt Strike
- Reconocimiento de red
- Compuesto por backdoors
- Borran los log/registros
- Exfiltran datos
- Secuestran dispositivos



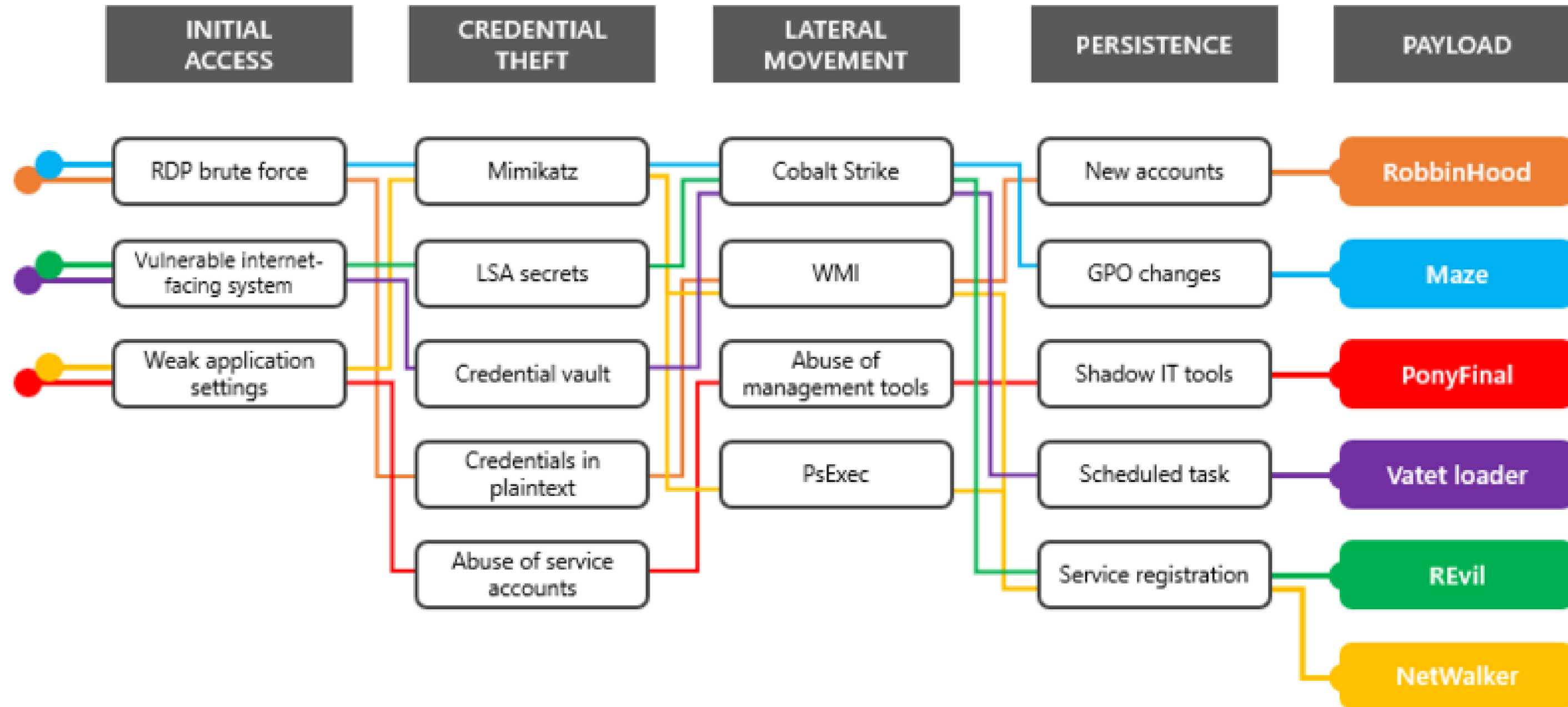
**Los ataques no están preprogramados. Los operadores de ataque se ajustan según sea necesario**

**Apuntar deliberadamente a activos críticos**

**Pagar el rescate no elimina al atacante**

**Los brotes de COVID-19 tuvieron como objetivo a sistemas críticos y trabajadores de primera línea**

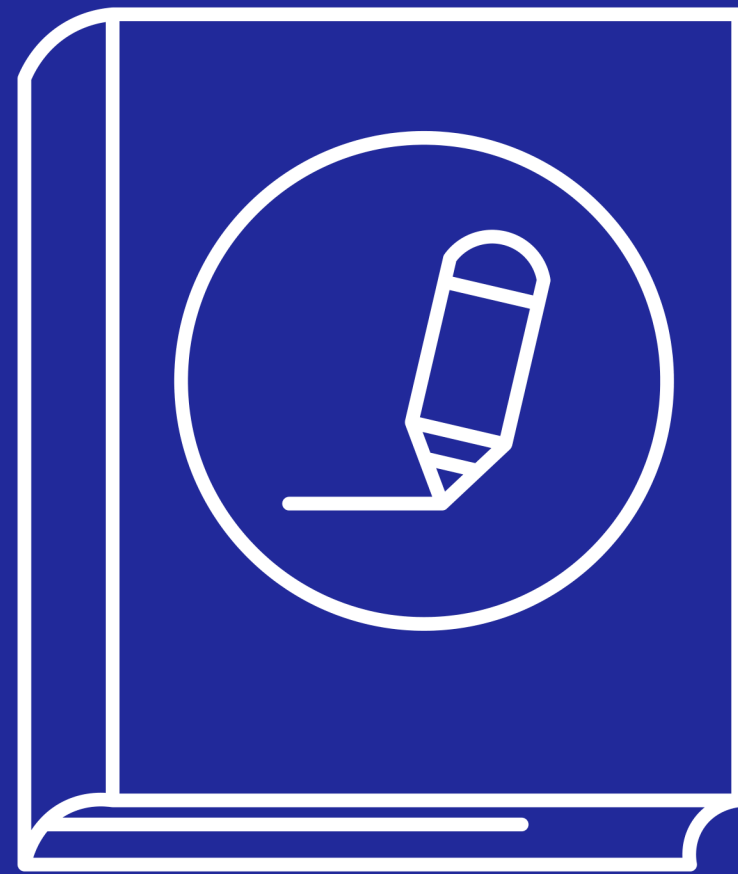
# Human Operated Ransomware



# Buenas prácticas

- Emplear autenticación multifactor (MFA) para todos los servicios en la medida de lo posible
- Aplicar el principio de privilegio mínimo a todos los sistemas/servicios
- Aprovechar las mejores prácticas para proteger los entornos en la nube
- Desarrollar y actualizar periódicamente el diagrama de red
- Emplear medios lógicos o físicos de segmentación de red
- Tener un enfoque integral de gestión de activos
- Restringir el uso de PowerShell, usando la Política de grupo
- Controladores de dominio hardenizados (DC)
- Conservar y asegurar adecuadamente los registros
- Monitoree y analice de la actividad de la red para determinar patrones de comportamiento
- Formación, ejercicios de phishing para concienciar
- Proteger y monitorear el protocolo de escritorio remoto (RDP)...
- Mantenga regularmente copias de seguridad fuera de línea de sus datos
- Reducir al área de ataques de cara a internet
- Adoptar un modelo Zero-Trust

# Lecciones Aprendidas





# Ransomware en Instituciones Paraguayas



**HiveV4**

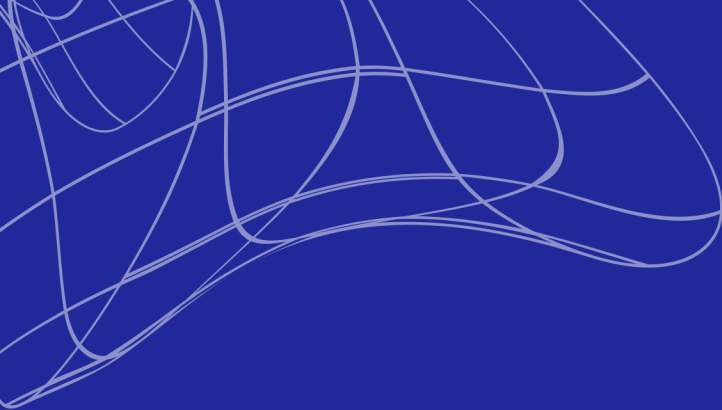
**Glob Imposter 2.0**

**Djavu**

**Dharma**

# Lecciones Aprendidas

- Si su organización sufre un evento de ransomware, y si no está seguro de que acciones tomar, NO TOQUE NADA!!! una acción equivocada puede derivar en la pérdida de información vital al momento de realizar el análisis de respuesta a incidente
- No borre, ni mueva ningún archivo de carpeta de los equipos infectados, sin antes realizar una copia
- No apague los equipos, dispositivos que hayan sido cifrados, desconéctelos de la red, nada más...
- Elaborar y mantener un inventario de activos(Hardware, Software, Aplicaciones), identificando la prioridad de cada activo en relación a su relevancia
- Realizar copias de seguridad de los activos de información y sistemas críticos (reinstalar un sistema operativo es una tarea de media dificultad, recuperar un archivo cifrado es una tarea bastante compleja, inclusive en algunos casos imposible)
- Adoptar una postura de ciberseguridad en la organización(CIS Controls, MGCTI, ISO-27001)
- Reducir al área de ataques de cara a internet
- Si sufre un incidente relacionado a un ransomware, comparta la información con el CERT-PY, inclusive de forma anónima si no está autorizado por su organización, usted puede ayudar a otros a través de su experiencia.. [abuse@cert.gov.py](mailto:abuse@cert.gov.py)



**“Tu adversario no espera a que termines de parchear”. - El arte de la guerra cibernética**

@SunTzuCyber



Muchas gracias por la  
atención!!

DESCARGUE  
LA  
PRESENTACIÓN

