CODERHOUSE

PROYECTO FINAL: PROPUESTA DE MEJORA PARA LEXCORP

Realizado por: Candela Anahi Ocampo

Contexto del Caso

La noche del 20 al 23 de Junio de 2021, LexCorp fue víctima de un malware (ataque) que afectó a sus servidores (Windows Server 2003/2012) y equipos de usuario (Windows7/Windows10) de toda la infraestructura.
Tras identificar todos los dispositivos infectados, el área de soporte técnico tomó las siguientes acciones:

- Guardaron una muestra del malware.
- Apagaron, el mismo día 23 de Septiembre, las máquinas que se habían identificado como afectadas durante el incidente.
- En las máquinas que disponían de copia de seguridad (back-up), restauraron al estado correspondiente al día 19 de septiembre (fecha de último backup disponible previo al ataque). Solo un 10% del Parque contaba con backup.
- El 24 de septiembre, LexCorp solicita los servicios de un analista de ciberseguridad para analizar una muestra y emitir recomendaciones para su infraestructura de red y mejorar su postura de ciberseguridad.
- LexCorp solicita la elaboración de un informe de análisis del ataque, que tipo de malware es y el vector de ataque para aportar más detalles sobre el incidente y el nivel de compromiso derivado del mismo.

01

INFORME DE ANÁLISIS

El presente informe responde a la necesidad de conocer el alcance del incidente de seguridad de la noche del 20 al 23 de junio de 2021, provocado por un malware que afectó a sus servidores y equipos de usuarios de toda la infraestructura.

A continuación, se presenta un análisis con un cuadro justificativo de las acciones llevadas a cabo por Área de Soporte Técnico luego del ataque del malware:

ACCIÓN	JUSTIFICACIÓN
Guardaron muestra el malware.	Es *correcto*, esto permitirá analizar el malware.
Apagan todas las maquinas.	*Incorrecto*, esta acción permite que se pierda información de la memoria volátil lo cual es contradictorio ya que se pierde información importante para llevar a cabo el análisis.
Restauraron estado de máquinas con back-up.	*Correcto*, es mejor reinstalar o restaurar en el mejor de los casos.

HIPÓTESIS DEL CASO

- Un usuario abrió un correo e hizo click a un mail con link malicioso que descargo la muestra del malware.
- Descargado el archivo, ejecuto el .zip explotando el archivo que de inmediato inicio el proceso de encriptación.
- El archivo ejecutó algunos mecanismo de persistencia, utilizables por el atacante para acceder al sistema.
- Las acciones del atacante se centraron en robo de credenciales por navegadores web, cambiar nombre de archivos, cargar ejecutables eliminadas o reescritas y la ejecución de otras aplicaciones y acciones de robo de datos personales.

INFORMACIÓN DEL MALWARE

Nombre de la Muestra	2.bin
Fecha de Análisis	September 24, 2023 at 08:52:51
OS utilizado para el análisis	Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)
MD5	0511A0C819ADE47392A2F3A51EAF1F0B
Información del Archivo	PE32 executable (GUI) Intel 80386, for MS Windows.

Otros nombres del malware:

- 2.bin
- FA08.exe
- 2.exe
- 1c57.exe
- A674.exe

COMPORTAMIENTO

MALICIOSO

Se detecta parada
- 2.bin.exe (PID: 348)
- 2.bin.exe (PID: 3244)

La solicitud fue eliminada o reescrita desde otro proceso
- build2.exe (PID: 1468)
- build2.exe (PID: 912)
- build3.exe (PID: 2020)
- mstsca.exe (PID: 3196)

Utiliza el Programador de tareas para ejecutar otras aplicaciones
- build3.exe (PID: 2020)
- mstsca.exe (PID: 3196)

ARKEI detectado por volcados de memoria
- build2.exe (PID: 912)

Se conecta al servidor CnC
- build2.exe (PID: 912)

ARKEI fue detectado
- build2.exe (PID: 912)

Roba credenciales de navegadores web
- build2.exe (PID: 912)

RACCOONCLIPPER detectado por volcados de memoria
- mstsca.exe (PID: 3196)

roba credenciales
- build2.exe (PID: 912)

Cargas ejecutables eliminadas o reescritas
- build2.exe (PID: 912)

VIDAR fue detectado
- build2.exe (PID: 912)

Cambia el nombre de archivos como ransomware
- 2.bin.exe (PID: 3244)

Las acciones parecen robo de datos personales.
- build2.exe (PID: 912)

SOSPECHOSO

Lee la configuración de seguridad de Internet Explorer
- 2.bin.exe (PID: 1888)
- build2.exe (PID: 912)

La aplicación se lanzó sola
- 2.bin.exe (PID: 3564)
- 2.bin.exe (PID: 1888)
- 2.bin.exe (PID: 876)
- build2.exe (PID: 1468)
- 2.bin.exe (PID: 3200)

Comprueba la configuración de confianza de Windows
- 2.bin.exe (PID: 1888)
- build2.exe (PID: 912)

Lee la configuración de Internet
- 2.bin.exe (PID: 1888)
- 2.bin.exe (PID: 348)
- build2.exe (PID: 912)
- 2.bin.exe (PID: 3244)

Lee la configuración de los certificados del sistema
- 2.bin.exe (PID: 1888)
- build2.exe (PID: 912)

Utiliza ICACLS.EXE para modificar listas de control de acceso
- 2.bin.exe (PID: 1888)

Agrega/modifica certificados de Windows
- 2.bin.exe (PID: 3564)

Procesar solicitudes binarias o script desde Internet
- 2.bin.exe (PID: 348)

El proceso se ejecuta a través del Programador de tareas.
- 2.bin.exe (PID: 3200)
- mstsca.exe (PID: 3196)

El proceso se comunica con Telegram (posiblemente usándolo como servidor C2 de un atacante)
- build2.exe (PID: 912)

Lee las cookies del navegador
- build2.exe (PID: 912)

Se conecta al servidor sin un nombre de host
- build2.exe (PID: 912)

Busca software instalado
- build2.exe (PID: 912)

INFORMACIÓN

Comprueba los idiomas admitidos
- 2.bin.exe (PID: 1888)
- 2.bin.exe (PID: 3564)
- 2.bin.exe (PID: 348)
- 2.bin.exe (PID: 876)
- build2.exe (PID: 1468)
- build3.exe (PID: 2020)
- build2.exe (PID: 912)
- 2.bin.exe (PID: 3200)
- 2.bin.exe (PID: 3244)
- mstsca.exe (PID: 3196)

Lee el GUID de la máquina desde el registro.
- 2.bin.exe (PID: 1888)
- 2.bin.exe (PID: 348)
- build2.exe (PID: 912)
- 2.bin.exe (PID: 3244)

Lee el nombre de la computadora
- 2.bin.exe (PID: 1888)
- 2.bin.exe (PID: 348)
- build2.exe (PID: 912)
- 2.bin.exe (PID: 3244)

Comprueba la información del servidor proxy
- 2.bin.exe (PID: 1888)
- 2.bin.exe (PID: 348)
- build2.exe (PID: 912)
- 2.bin.exe (PID: 3244)

Crea archivos o carpetas en el directorio de usuarios.
- 2.bin.exe (PID: 1888)
- 2.bin.exe (PID: 348)
- build3.exe (PID: 2020)
- build2.exe (PID: 912)
- 2.bin.exe (PID: 3244)

Ejecución manual por parte de un usuario.
- mmc.exe (PID: 2880)
- mmc.exe (PID: 3316)
- explorer.exe (PID: 916)
- notepad.exe (PID: 2996)

Crea archivos en el directorio del programa.
- build2.exe (PID: 912)

Lee el nombre del producto
- build2.exe (PID: 912)

Lee los valores del entorno
- build2.exe (PID: 912)

Lee información de la CPU
- build2.exe (PID: 912)

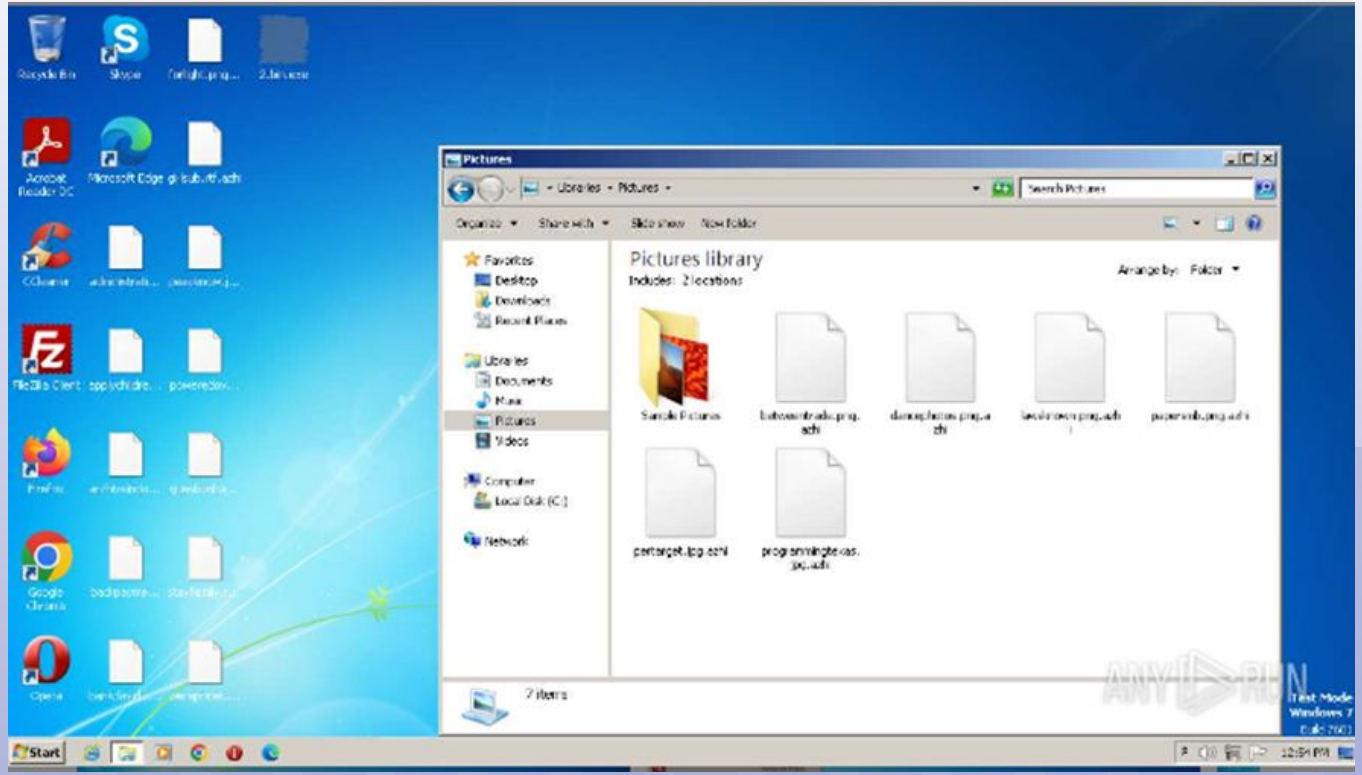
INFORMACIÓN ESTÁTICA ENCONTRADA

EXE

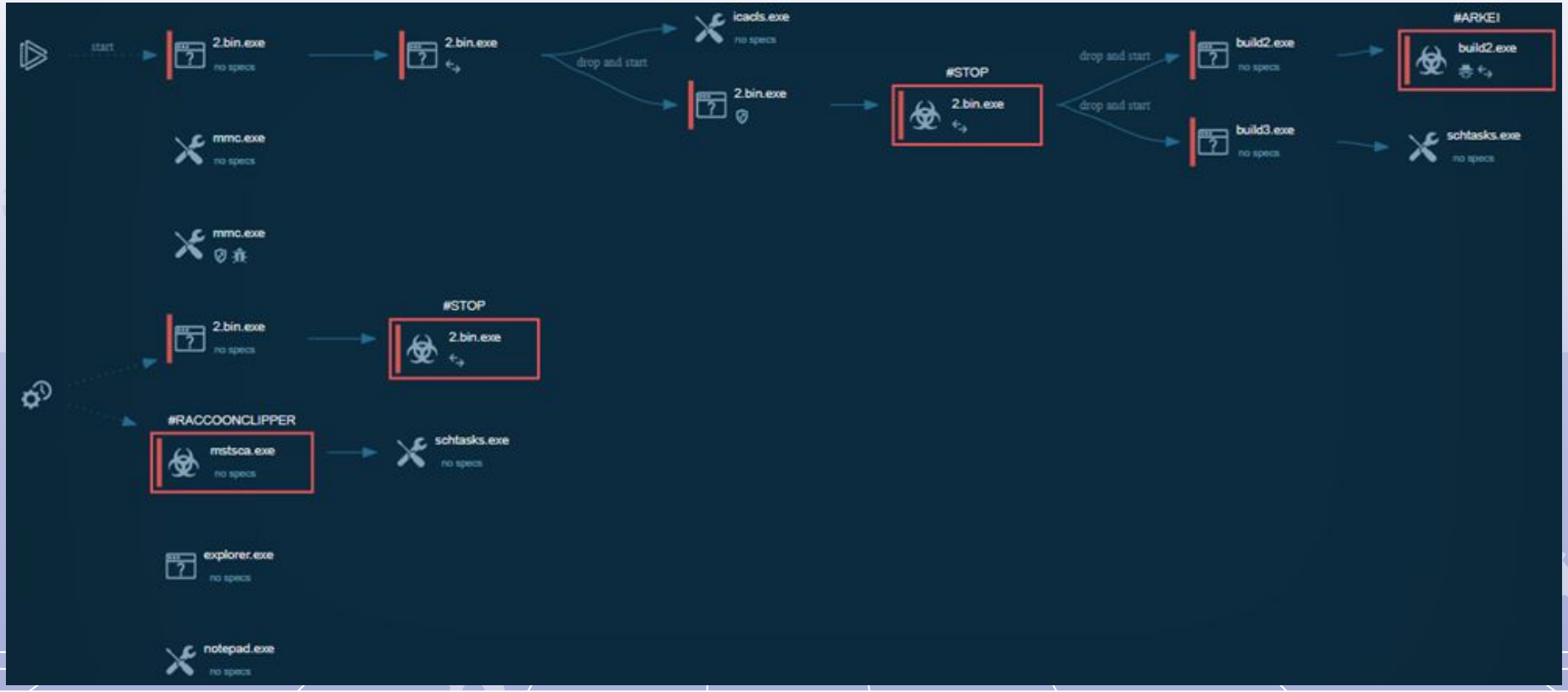
MachineType: Intel 386 or later, and compatibles
PEType: PE32
CodeSize: 760320
UninitializedDataSize: -
OSVersion: 5.1
SubsystemVersion: 5.1
FileVersionNumber: 91.0.0.0
FileFlagsMask: 0x003f
FileOS: Windows NT 32-bit
FileSubtype: -
CharacterSet: Unknown (85B3)
InternalName: Astronomy.exe
ProductName: Hdfgodifjg

TimeStamp: 2022:10:28 23:17:51+00:00
LinkerVersion: 10
InitializedDataSize: 35047424
EntryPoint: 0x54bd
ImageVersion: -
Subsystem: Windows GUI
ProductVersionNumber: 98.0.0.0
FileFlags: (none)
ObjectFileType: Executable application
LanguageCode: Unknown (0294)
FileVersions: 64.5.34.31
OriginalFileName: Hugidfgy.exe
ProductVersion: 2.8.47.63

SCREENSHOT DE SIMULACIÓN



PROCESOS DE COMPORTAMIENTO



EVENTOS CRITICOS ASOCIADOS

Actividad registral

Eventos totales	Leer eventos	Escribir eventos	Eliminar eventos
12 990	12 851	134	5

(PID) Process: (1888) 2.bin.exe
Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{FCC67766-6201-4AD1-A6B8-2F4553C93D47}
Operation: write
Name: WpadDecision
Value: 0

(PID) Process: (1888) 2.bin.exe
Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{FCC67766-6201-4AD1-A6B8-2F4553C93D47}
Operation: write
Name: WpadNetworkName
Value: Network 3

(PID) Process: (1888) 2.bin.exe
Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff
Operation: write
Name: WpadDecisionTime
Value: 10C951AADDEED901

(PID) Process: (912) build2.exe
Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections
Operation: write
Name: SavedLegacySettings
Value: 460000005101000009000000000000000000000000000000004000000000000000C0E333BBEAB1D3010000000000000000000000000100000002000000C0A864B7000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000

(PID) Process: (912) build2.exe
Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write
Name: ProxyBypass
Value: 1

(PID) Process: (912) build2.exe
Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write
Name: IntranetName
Value: 1

(PID) Process: (348) 2.bin.exe
Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{FCC67766-6201-4AD1-A6B8-2F4553C93D47}
Operation: write
Name: WpadDecision
Value: 0

(PID) Process: (348) 2.bin.exe
Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{FCC67766-6201-4AD1-A6B8-2F4553C93D47}
Operation: write
Name: WpadNetworkName
Value: Network 3

(PID) Process: (348) 2.bin.exe
Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff
Operation: write
Name: WpadDecisionTime
Value: AADE29B4DDEED901

SOLICITUDES HTTP

Detallamos las solicitudes HTTP de reputación “desconocida”.

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
912	build2.exe	GET	200	168.119.168.251:80	http://168.119.168.251/data.zip	unknown	compressed	2.56 Mb	unknown
348	2.bin.exe	GET	200	201.119.80.5:80	http://zexeq.com/raud/get.php?pid=6E3AAB7CB29BC9495DFDE01272C66F39&first=true	unknown	binary	563 b	unknown
912	build2.exe	POST	200	168.119.168.251:80	http://168.119.168.251/	unknown	text	2 b	unknown

CONEXIONES

Se presentan aquellas conexiones “desconocidas” que realiza el malware.

PID	Process	IP	Domain	ASN	CN	Reputation
1888	2.bin.exe	162.0.217.254:443	api.2ip.ua	NAMECHEAP-NET	NL	unknown
1888	2.bin.exe	67.26.83.254:80	ctldl.windowsupdate.com	LEVEL3	US	unknown
1888	2.bin.exe	104.18.14.101:80	ocsp.comodoca.com	CLOUDFLARENET	–	unknown
1888	2.bin.exe	104.18.15.101:80	ocsp.comodoca.com	CLOUDFLARENET	–	unknown
348	2.bin.exe	162.0.217.254:443	api.2ip.ua	NAMECHEAP-NET	NL	unknown
348	2.bin.exe	211.40.39.251:80	colisumy.com	LG DACOM Corporation	KR	unknown
348	2.bin.exe	201.119.80.5:80	zexeq.com	Uninet S.A. de C.V.	MX	unknown
912	build2.exe	149.154.167.99:443	t.me	Telegram Messenger Inc	GB	unknown

SOLICITUDES DNS

Domain	IP	Reputation
colisumy.com	211.40.39.251 115.88.24.200 211.171.233.129 211.119.84.111 123.213.233.131 95.86.30.3 123.140.161.243 51.211.69.92 175.120.254.9 196.188.169.138	unknown
zexeq.com	201.119.80.5 211.59.14.90 187.170.26.222 180.94.156.61 211.119.84.112 211.119.84.111 211.168.53.110 210.182.29.70 211.171.233.126 175.120.254.9	unknown

AMENAZAS CRITICAS

PID	Process	Class	Message
–	–	Device Retrieving External IP Address Detected	ET POLICY External IP Address Lookup DNS Query (2ip .ua)
1888	2.bin.exe	Potentially Bad Traffic	ET INFO Observed External IP Lookup Domain (api .2ip .ua in TLS SNI)
348	2.bin.exe	A Network Trojan was detected	ET USER_AGENTS Suspicious User Agent (Microsoft Internet Explorer)
348	2.bin.exe	A Network Trojan was detected	ET MALWARE Win32/Filecoder.STOP Variant Request for Public Key
348	2.bin.exe	A Network Trojan was detected	ET MALWARE Win32/Filecoder.STOP Variant Public Key Download
348	2.bin.exe	A Network Trojan was detected	ET USER_AGENTS Suspicious User Agent (Microsoft Internet Explorer)
348	2.bin.exe	A Network Trojan was detected	ET MALWARE Potential Dridex.Maldoc Minimal Executable Request
348	2.bin.exe	A Network Trojan was detected	ET MALWARE Win32/Vodkagats Loader Requesting Payload
348	2.bin.exe	Potential Corporate Privacy Violation	ET POLICY PE EXE or DLL Windows file download HTTP
348	2.bin.exe	A Network Trojan was detected	ET MALWARE Potential Dridex.Maldoc Minimal Executable Request
348	2.bin.exe	A Network Trojan was detected	ET MALWARE Win32/Vodkagats Loader Requesting Payload
348	2.bin.exe	Potential Corporate Privacy Violation	ET POLICY PE EXE or DLL Windows file download HTTP
912	build2.exe	A Network Trojan was detected	STEALER [ANY.RUN] Arkei
912	build2.exe	Potentially Bad Traffic	ET INFO Dotted Quad Host ZIP Request

02

CONCLUSIONES

Comportamiento del Malware: Evasion/Stealers
Nombre General: 2.bin
Investigación del Malware: Troyano 2.bin
Tipo de Malware: Troyano

Información sobre 2.bin:
El malware .bin infringe daños en las organizaciones a través de los siguientes troyanos: Arkei, Raccoon stealer y Vidar.
Comienza haciendo una entrada a través de la ejecución de usuario provocando que el programador de tareas ejecuta varias aplicaciones.
Una vez ejecutado las aplicaciones evade la defensa del sistema provocando una que se realice una modificación de permisos de archivos y directorios (a través de ICACLS.EXE para modificar listas de control de acceso) y a su vez subvertir los controles de confianza, es decir, agrega/modifica certificados del SO: Windows.
Luego, comienza con el robo de credenciales a través de navegadores web y de acciones que parecen robos de datos personales, incluso encripta archivos como imágenes, databases, documentos y otros para usarlos ante una demanda por cierta cantidad de dinero para el rescate de los archivos encriptados a través de un software.
Por último, se conecta al servidor CnC evitando la detección/filtrado de red al mezclarse con el tráfico existente y además se sabe que cambia el nombre de archivos como ransomware.

INFORMACIÓN ADICIONAL

- **¿Qué es un troyano?**

  Tipo de software malicioso o malware que se presenta como un programa aparentemente legítimo o inofensivo, pero que en realidad realiza funciones no autorizadas y dañinas en un sistema informático. Una vez que un usuario ejecuta el programa troyano, éste puede llevar a cabo diversas acciones maliciosas, como robar información confidencial, obtener acceso no autorizado al sistema, instalar otros malware, o incluso controlar de manera remota el sistema comprometido.

- **¿Qué es Arkei?**

  Es un tipo de malware, específicamente un troyano bancario. Los troyanos bancarios son programas maliciosos diseñados para robar información financiera y credenciales de acceso a cuentas bancarias. Arkei ha sido conocido por dirigirse a usuarios de servicios bancarios en línea, capturando información confidencial como nombres de usuario, contraseñas y datos de tarjetas de crédito.

INFORMACIÓN ADICIONAL

- **¿Qué es Raccon stealer?**

  Es un tipo de malware de robo de información. Se clasifica como un ”stealer” porque su principal función es robar datos sensibles almacenados en las computadoras de las víctimas. Este malware ha sido utilizado para recopilar información como credenciales de inicio de sesión, detalles de tarjetas de crédito y otra información personal.

- **¿Qué es Vidar?**

  Vidar es un tipo de malware diseñado para robar información sensible de los sistemas infectados. Es conocido como un troyano de robo de datos, y su función principal es recopilar datos confidenciales almacenados en las computadoras de las víctimas.

03

PROPUESTA DE MEJORA

Para poder asegurar el perímetro de la empresa LexCorp presentamos las siguientes implementaciones de Firewall, Sistemas de Prevención (IPS), Honeypots y Sistema de detección de Intrusos (IDS).

Su importancia se extiende a todas las empresas a nivel mundial que emplean recursos cibernéticos, ya que todos estamos expuestos a posibles ataques en el entorno digital. Estos componentes juegan un papel vital en la defensa contra las amenazas que podrían comprometer la seguridad de la información y la operatividad de las organizaciones.

- **Firewall de filtrado de paquetes estáticos:**
  Configurar firewalls para filtrar el tráfico de red y bloquear cualquier conexión no autorizada. Esto ayudará a prevenir que el malware .bin se conecte al servidor CnC y se mezcle con el tráfico existente ya que los firewalls son una práctica que nos sirve para limitar el acceso no autorizado y bloquear aquellas conexiones maliciosas.

- **Sistema de Prevención de Instrucciones (IPS):** los IPS no solamente detectan una amenaza sino que también bloquean las actividades maliciosas como la modificación de permisos.
  Beneficio: puede evitar que los ataques tengan éxitos, de esta forma minimiza los daños.

- **Honeypots:** la configuración de los honeypots servirán para detectar la presencia de troyanos y malware como Arkei, Raccon Stealer y Vidar, lo que permitiría a los equipos identificar su presencia y tomar medidas antes de que se expanda por la red principal.
  Algunos beneficios podrían ser:
  Recopilar Información.
  Desviar a los Atacantes.

- **Sistema de Detección de Intrusos (IDS):** el IDS detecta las actividades inusuales como la modificación de archivos y directorios a través de ICACLS.EXE (fue por donde el malware modificó las listas de control de acceso) , esto ayudaría a evitar daños adicionales como por ejemplo la modificación de archivos que hizo el malware o la encriptación de estos mismos.
  La utilización de esta herramienta debe ser hablada y pactada con LexCorp para poder configurar los sistemas en base a sus necesidades.

04

TECNICAS DE DEFENSA DE PERIMETRO

MEDIDAS DE SEGURIDAD PARA TROYANOS

- **Filtrado de Correos Electrónicos:**
  Esta estrategia evitaría un ataque al bloquear aquellos correos maliciosos que podrían contener enlaces y/o archivos infectados con troyanos.

- **Actualizar el Sistema:**
  Aplicar parches de seguridad y mantener actualizado el sistema operativo como también el software de aplicaciones para cerrar aquellas vulnerabilidades que los troyanos podrían explotar.

- **Establecer Políticas de Acceso y Privilegios:**
  Implementar aquellas políticas que regulen el acceso y los privilegios, de esta forma se restringe los permisos a lo esencial para reducir la capacidad de que los troyanos se propaguen y causen daño.

- **Plan de Acciones:**
  Establecer un plan de acción para manejar aquellos incidentes que incluya pasos específicos para la identificación, contención y eliminación de troyanos.
  Sugerencia: realizar simulacros.

- **Capacitación a Usuarios:**
  Desarrollar programas de capacitación que permita a los usuarios sensibilizar sobre las amenazas asociadas a los troyanos, enfocándose en prácticas seguras al navegar por internet y descargar archivos.

- **Software de Seguridad:**
  Asegurarse de los programas de seguridad como antivirus y antimalware se encuentren actualizados para poder detectar un ataque como troyanos y eliminarlo.
  Sugerencia: realizar un análisis semanal en los dispositivos.

MEDIDAS DE SEGURIDAD PARA ARKEI

- **Actualizar Software:**
  Mantener el sistema operativo y el software de seguridad de forma regular actualizados para no tener vulnerabilidades.

- **Monitoreo de Tráfico de Red:**
  Implementar sistemas de monitoreo de red para detectar patrones de tráfico inusual que puedan indicar una infección de malware.
  Advertencia: en caso de identificar, se debe aislar rápidamente sistemas comprometidos.

- **Soluciones Antivirus y Antimalware:**
  Emplear software antivirus y antimalware de calidad, actualizado y con análisis periódicos para detectar y eliminar el malware Arkei.

- **Soluciones Antivirus y Antimalware:**
  Emplear software antivirus y antimalware de calidad, actualizado y con análisis periódicos para detectar y eliminar el malware Arkei.

- **Capacitacion de Usuarios:**
  Educar a los usuarios mediante capacitaciones sobre las amenazas de malware, especialmente el phishing mediante programas de concienciación de seguridad.

- **Restringir Privilegios:**
  Aplicar el principio de menor privilegio, limitando los permisos de usuarios y programas para reducir el impacto potencial del malware en caso de compromiso.

MEDIDAS DE SEGURIDAD PARA RACCON STEALER

- **Conexión Segura:**
  Utilizar una red privada virtual (VPN) para cifrar el tráfico.

- **Control de Dispositivos:**
  Implementa controles para limitar el uso de dispositivos de almacenamiento extraíbles y otros medios que podrían introducir malware en la red.

- **Gestionar Actualizaciones:**
  Implementar un sistema centralizado para gestionar y aplicar actualizaciones de software en todos los dispositivos de la empresa, incluyendo sistemas operativos y programas de seguridad.

- **Política de Contraseñas Robustas:**
  Establecer y hacer cumplir una política de contraseñas robustas, con cambios periódicos, y considerar el uso de autenticación de múltiples factores para una capa adicional de seguridad.

- **Monitoreo de Red:**
  Establecer soluciones de monitoreo de red que puedan identificar patrones de tráfico inusual, lo que podría indicar actividades maliciosas, y establecer alertar para una respuesta rápida y automática.

05

IMPLEMENTAR PROGRAMA

SNORT

PASOS DE IMPLEMENTACIÓN

SNORT: es un sistema de detección de intrusiones (IDS), es una herramienta de código abierto que es utilizada ampliamente.

1 INSTALACIÓN

Descarga e instala Snort en el servidor que actuará como el nodo central de monitoreo

2 CONFIGURACIÓN DE REGLAS

Configurar las reglas de Snort para definir qué tipo de tráfico se considerará normal y cuál podría ser malicioso.

3 CONFIGURACIÓN DE INTERFACES DE RED

Definir las interfaces de red que Snort debe monitorear. Esto implica especificar las interfaces de red donde esperas detectar el tráfico malicioso.

4 CONFIGURACIÓN DE ALERTAS

Configura las alertas para que Snort te notifique inmediatamente si detecta algún patrón de tráfico sospechoso. Puedes configurar alertas por correo electrónico, mensajes de registro, o incluso integrar Snort con otros sistemas de gestión de eventos e información de seguridad (SIEM).

PASOS DE IMPLEMENTACIÓN

IMPLEMENTACIÓN EN MODO INLINE(IPS)

5

Si deseas que Snort también tome medidas activas contra tráfico malicioso, puedes configurarlo en modo Inclinar para que funcione como un Sistema de Prevención de Intrusiones (IPS).

ACTUALIZACIONES Y MANTENIMIENTO

7

Mantener actualizado Snort descargando regularmente las últimas reglas de detección de amenazas y actualizaciones del programa para estar al tanto de nuevas vulnerabilidades y amenazas.

MONITOREO CONTINUO

6

Iniciar Snort y monitorear continuamente las alertas y registros generados. Asegurar de ajustar y mejorar las reglas según sea necesario, para optimizar la detección de amenazas específicas.

INTEGRACIÓN CON OTROS SISTEMAS

8

Si es posible, integrar Snort con otros sistemas de seguridad como firewalls, antivirus etc, para mejorar la capacidad de respuesta y la coordinación en caso de un ataque.

CONCLUSIÓN DE LAS PROPUESTAS DE MEJORA

La combinación estratégica de tecnologías como honeypots, IPS, IDS y firewalls proporciona una defensa sólida para el sistema. Al seguir estas prácticas, podemos disminuir el riesgo de impactos significativos en la empresa, lo que podría llevar a una reducción en la prestación de servicios.

Como complemento a estas medidas, la implementación de herramientas especializadas como Snort, un sistema de detección de intrusiones de código abierto, fortalece aún más la postura de seguridad de la empresa. Snort puede ser una pieza integral en la detección proactiva de amenazas, contribuyendo así a la construcción de una defensa completa y eficiente contra posibles ataques cibernéticos.

¡MUCHAS GRACIAS!