Proyecto Final:Primera Entrega

(PRIMERAENTREGA_FLORENCIA SOLANO)

Fecha del ataque: 20 al 23 de junio de 2021

Descripción del incidente:

Durante el periodo del 20 al 23 de junio de 2021, se produjo un ataque cibernético que afectó las redes informáticas de la organización LexCorp.
El 23 de junio como medida se produjo el apagado de todas las computadoras afectadas,el nivel de compromiso fue significante lo que resultó una gran pérdida de datos debido a la falta de copias de seguridad adecuadas, destacando que esas copias de seguridad ya están infectadas.
El incidente afectó a sistemas operativos Windows7 y 10 en la infraestructura de la organización.
El 19 de septiembre de 2021, se restauraron los sistemas afectados al estado correspondiente antes del ataque.Sin embargo, debido a la gravedad del incidente , el 24 de septiembre se solicitó la intervención de un analista de ciberseguridad para realizar un análisis exhaustivo y proporcionar recomendaciones para fortalecer la postura de ciberseguridad de la organización
Se observó que solo el 10% de las computadoras afectadas tenían copias de seguridad, lo que exacerbó la pérdida de datos.

Análisis del problema

La falta de copias de seguridad adecuadas, dejó a las computadoras vulnerables al ataque al no contar con parches de seguridad necesarios para protegerse contra las últimas amenazas.Además, la instalación de software no autorizado por parte de los empleados proveniente de fuentes no confiables pudo haber aumentado el riesgo de infección.

Paso en mostrar un Análisis con varias herramientas
Comenzando por los detalles de la muestra, su nombre: 2.bin , fue analizado el dia 04/12/2023 a las 23.15hs, OS utilizado:Windows 7 Professional Service Pack 1 (build:7601,32bit) y MD5.:0511a0c819ade47392a2f3a51eaf1f0b

Tenemos información estática:
Es un ejecutable para windows,

TRiD
.exe | Win32 Executable generic (52.9)
.exe | Generic Win DOS/ Executable (23.5)
.exe | Executable Generic (23.5)

EXIF:

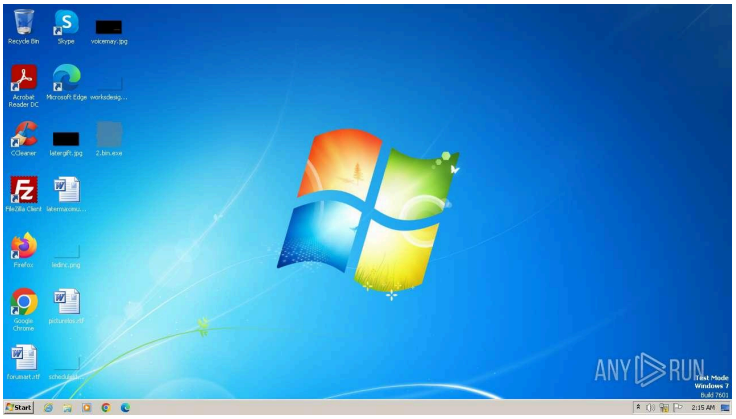
Version: 2.8.47.63
Nombre: Hdfgodifjg
Nombre de archivo original:Hugidfgy.exe
Nombre Interno:Astronomy.exe
Versión del archivo:64.5.34.31
Idioma del código:Unknown(0294)
Sistema Operativo del archivo: Windows NT 32-bit
Tipo de Máquina: Intel 386 or later, and compatibles

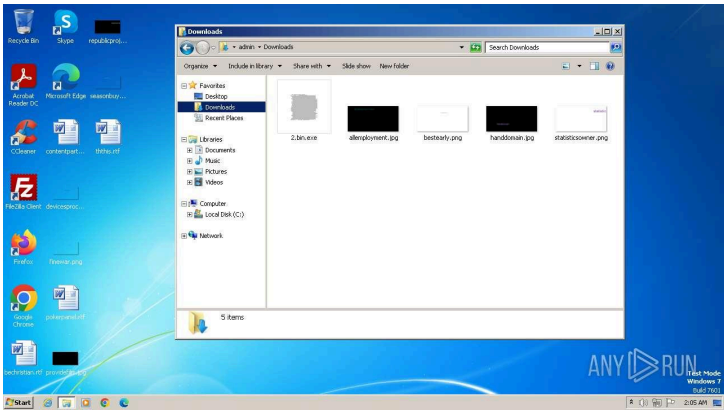
Hora de creación: 2022-10-28 23:17:51 UTC
primera presentación: 2023-09-24 08:46:05 UTC
última presentación: 2023-12-04 20:39:35 UTC
ultimo analisis:2024-01-30 23:49:40 UTC

conexiones:

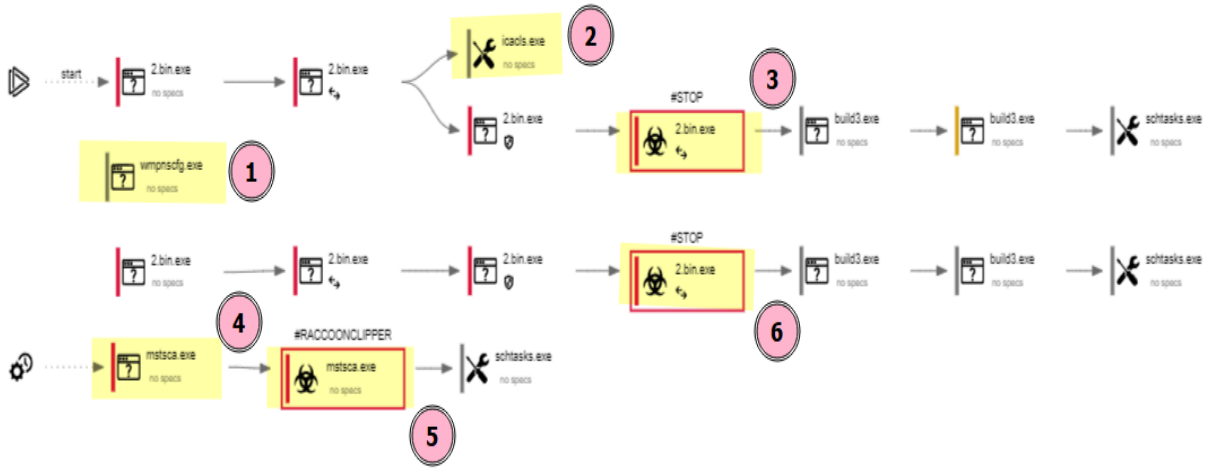
Observamos que se utilizan los puertos 5355,443 y 80 como peligrosos.
Resumidamente uno es de mDNS y se utiliza para descubrir y resolver nombres de host en redes locales por dispositivos y servicios que admiten la funcionalidad de descubrimiento automático en redes locales.
Con esto pudieron escanear la red de LexCorp en busca de dispositivos vulnerables o servicios expuestos.
Otro es HTTPS, cifra comunicaciones entre cliente y servidor se utiliza para la comunicación segura a través de internet,transferir datos sensibles .
Así pudo ser que se comprometieron los sistemas de LexCorp,especialmente si los empleados accedieron a servicios en línea sensibles sin la protección adecuada.
y el último es HTTP que es el protocolo básico para la navegación web y se utiliza para enviar y recibir datos no cifrados entre cliente y servidor web.
Pueden redirigir a usuarios a sitios web falsos,interceptar el tráfico de red o ataques de suplantación de identidad.Ataques de man in the middle para interceptar y modificar comunicaciones sensibles.
Esto podría haber sido una forma en que el malware inicial se introdujo en la red de LexCorp,infectando a las computadoras afectadas.
Y también puede distribuir malware a través de descargas de archivos ejecutables o scripts maliciosos.

El comportamiento fue el siguiente primera imagen como estaba y como terminó:





El comportamiento que tuvo en general fue el siguiente:



Paso a explicar algunos comandos más relevantes:

1)wmpnscfg.exe:
Este proceso fue ejecutado manualmente por un usuario, con el proceso principal siendo “Explorer.EXE”. El programa está ubicado en el directorio de Windows Media Player se puede utilizar “wmpnscfg.exe” para configurar ajustes de red o realizar otras tareas relacionadas con la reproducción de medios como también leer el nombre del equipo y verificar los idiomas admitidos como parte de su funcionamiento normal.
Sin embargo, se puede abusar de esto y realizar acciones no autorizadas en un sistema.Por ejemplo:Podría usarse para recopilar información sobre el sistema a leer, el nombre del equipo y ejecutar código o comandos maliciosos en el sistema.

2)icacls.exe:
Los datos JSON muestran un proceso donde se está utilizando la utilidad icacls.exe para denegar permisos en un directorio específico ubicado en
"C:\Users\admin\AppData\Local\b87e7799-e98a-4643-baae-f0b447150a6f"
para el usuario.El comando es ejecutado por el proceso padre “ICACLS.EXE”.
Esta herramienta permite a los administradores controlar quién puede acceder,modificar o eliminar recursos específicos,asegurando la seguridad y la integridad de los datos del s.o
Puede ser utilizada para restringir el acceso a archivos o directorios críticos del sistema,lo que dificulta que las herramientas de seguridad o los administradores detecten y eliminen componentes maliciosos.
En este caso,se están denegando permisos al identificador de seguridad especificado *S-1-1-0 para el directorio
"C:\Users\admin\AppData\Local\b87e7799-e98a-4643-baae-f0b447150a6f".

3)2.bin.exe:
Fue ejecutado con los argumentos de línea de comandos “Admin IsNotAutoStart IsNotTask” y fue generado por otra instancia de 2.bin.exe con los mismos argumentos.El proceso también creó archivos o carpetas en el directorio del usuario,solicitó binarios o scripts desde Internet y dejo caer un archivo ejecutable inmediatamente después de comenzar.
Estos pueden leer configuraciones de registro,como idiomas,nombre de equipo,configuración de internet,seguridad y certificados del sistema, para configurarse a sí mismo o proporcionar experiencias personalizadas para los usuarios, como configuraciones de seguridad e información del servidor proxy,con fines de reconocimiento.

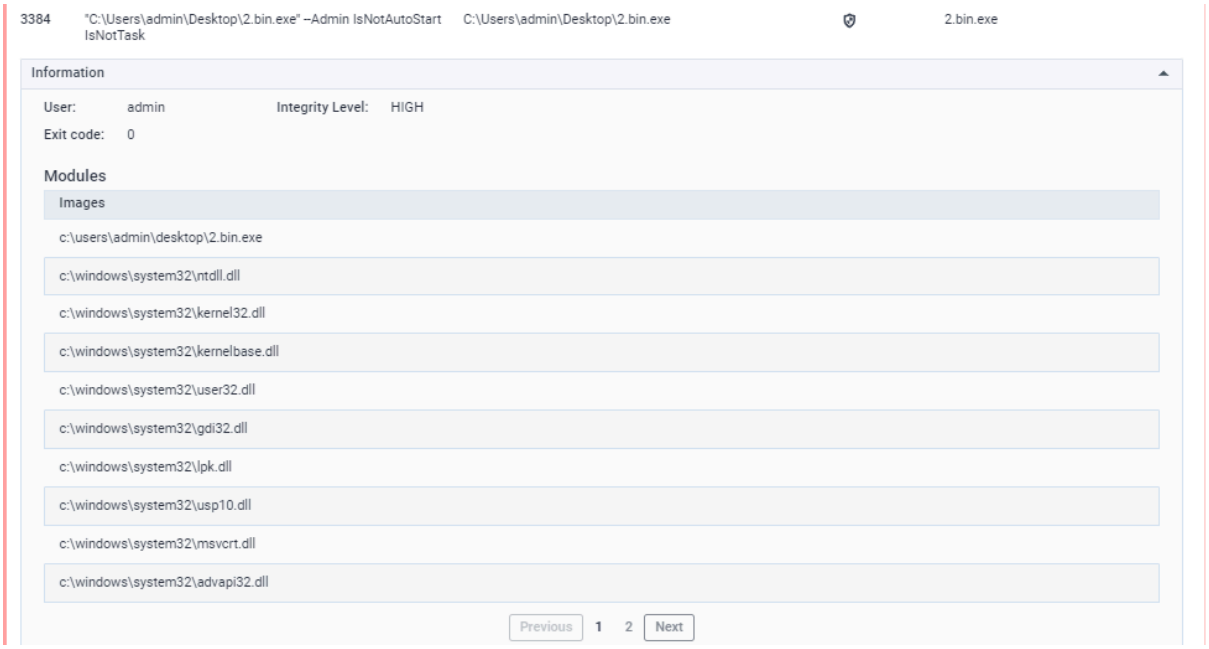
4)mstsca.exe:
Los datos JSON muestran que el proceso está siendo ejecutado a través del programador de tareas,siendo el proceso padre taskeng.exe . Además el proceso verifica los idiomas admitidos en el registro y se ejecuta así mismo,lo que indica cierto comportamiento de auto recopilación

Esta línea de comandos se utiliza para ejecutar el archivo “mca.exe” ubicado en el directorio `":\\Users\\admin\\AppData\\Roaming\\Microsoft\\Network\\".`
Los programas pueden usar líneas de comandos similares para ejecutar archivos ejecutables almacenados en directorios específicos para diversas tareas del sistema o de la aplicación, por ejemplo:herramientas de mantenimiento del sistema o actualizaciones de software pueden usar comandos similares para ejecutar procesos necesarios.
Los actores maliciosos a menudo colocan archivos ejecutables maliciosos en directorios para evadir la detección y ejecutar actividades dañinas en el sistema.En este caso, la línea de comandos podría usarse para ejecutar un ejecutable malicioso que puede realizar acciones como robo de datos , compromiso del sistema o instalaciones de malware adicional en el sistema

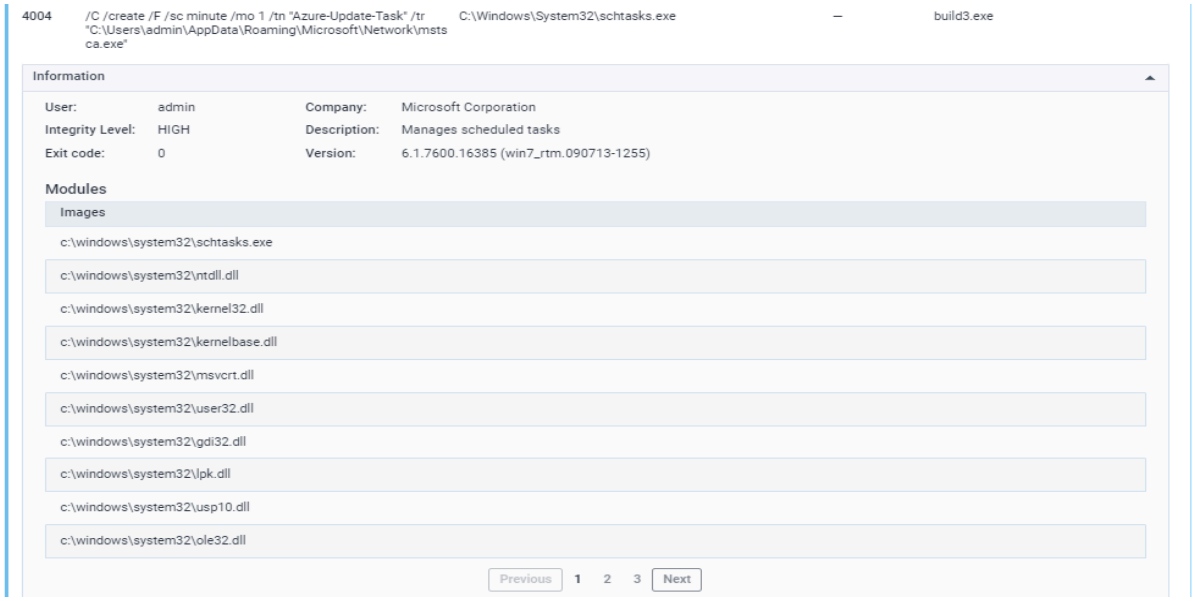
5)mstsca.exe:
Este comportamiento sugiere que el proceso está programando tareas para ejecutar.Al utilizarlo en momentos predeterminados sin intervención del usuario, mejora la eficiencia y productividad del sistema.Además podría indicar un intento de persistir en el sistema programando la ejecución de cargas útiles o actividades maliciosas.Este comportamiento permite que el malware mantenga una presencia en el sistema infectado.Además la presencia de RACCOONCLIPPER,una amenaza conocida detectada por YARA sugiere que el proceso podría estar involucrado en la exfiltración de datos y otras actividades maliciosas.

6)2.bin.exe:
Este proceso fue observado ejecutándose con los argumentos de linea de comandos “AdminIsNotAutoStartIsNotTask” y su proceso padre tambien fue 2.bin.exe con los mismos argumentos.El proceso fue ejecutado desde el escritorio del usuario.Los programas maliciosos a menudo exhiben comportamientos como leer información sensible del registro, verificar vulnerabilidades de seguridad, dejar caer archivos ejecutables para persistencia y comunicarse con servidores externos para descargar cargas útiles adicionales o recibir comandos. En este caso, el proceso fue señalado por crear archivos en el directorio del usuario, detener un proceso y realizar solicitudes de red a una entidad sospechosa llamada "VODKAGATS".

A modo de ejemplo, muestro algunos eventos asociados:



El proceso se encuentra en el escritorio del usuario “admin”.Se ejecuta con los argumentos de linea de comandos “Admin IsNotAutoStartIsNotTask”.Este proceso se inicia asi mismo.El proceso se ejecuta con privilegios elevados ya que el nivel de integridad es ALTO.La salida muestra un valor de 0 que sugiere que el proceso se ejecuta sin errores y termina correctamente



Este evento utiliza el comando “schtasks.exe” en Windows para crear una nueva tarea llamada AzureUpdate-Task.Se configura para ejecutarse cada un minuto,y utiliza el ejecutable “mstsca.exe” .También podemos observar que la tarea fue ejecutada por el

usuario “admin” y pertenece a la compañía Microsoft Corporation.La salida del proceso muestra un código de salida 0 lo que indica que la tarea se ejecutó exitosamente y muestra la versión del s.o en la que se ejecutó.

Observando los http request

Tenemos URL que se utilizan para descargar un archivo CAB,podrían haber sido utilizadas por los atacantes para infiltrarse en los sistemas y descargar certificados raíz maliciosos.Esto habría comprometido la integridad de las actualizaciones de Windows y permitido la comunicación maliciosa con servidores falsificados
También tenemos otras URL que se utiliza para una solicitud HTTP GET, se puede verificar el estado de revocación de certificados digitales.El dominio ocsp.pki.goog se utiliza para las solicitudes del Protocolo de Estado de Certificación en Línea(OCSP) se puede utilizar para verificar el estado del certificado.
Otros obtienen datos o recursos del servidor zexeq.com para operaciones normales,instalaciones de software o actualizaciones.
Tenemos 2 URL maliciosas que se aprovechan para descargar y ejecutar archivos ejecutables maliciosos,como ransomware desde un servidor remoto para actividades maliciosas como robo de datos o compromiso del sistema o descargas binarias lo que conduce a actividades maliciosas como la exfiltración de datos o el compromiso del sistema de la empresa.

DNS request

Dominios:
api.2ip.ua IP ->

- 188.114.97.3
- 188.114.96.3

Reputación:Shared

ctldl.windowsupdate.com IP->

- 93.184.221.240

Reputación:whitelisted indicando que es confiable

ocsp.pki.goog IP->

- 142.250.186.131

Reputación:whitelisted indicando que es confiable

colisumy.com IP->

- -

Reputación:unknown

zexeq.com IP->

- 211.168.53.110
- 201.119.20.32
- 190.219.136.87
- 211.119.84.112
- 109.175.29.39
- 181.168.176.36
- 91.104.83.7
- 123.213.233.131
- 14.33.209.147
- 211.53.230.67

Reputación:unknown

amenazas:

explicando brevemente como afecto cada uno :

1080	svchost.exe	Device Retrieving External IP Address Detected	ET POLICY External IP Address Lookup DNS Query (2ip .ua)
1864	2.bin.exe	Potentially Bad Traffic	ET INFO Observed External IP Lookup Domain (api .2ip .ua in TLS SNI)
2996	2.bin.exe	Potentially Bad Traffic	ET INFO Observed External IP Lookup Domain (api .2ip .ua in TLS SNI)
2996	2.bin.exe	A Network Trojan was detected	ET USER_AGENTS Suspicious User Agent (Microsoft Internet Explorer)
2996	2.bin.exe	A Network Trojan was detected	ET MALWARE Win32/Filecoder.STOP Variant Request for Public Key
2996	2.bin.exe	A Network Trojan was detected	ET MALWARE Win32/Filecoder.STOP Variant Public Key Download
4088	2.bin.exe	Potentially Bad Traffic	ET INFO Observed External IP Lookup Domain (api .2ip .ua in TLS SNI)
2996	2.bin.exe	A Network Trojan was detected	ET USER_AGENTS Suspicious User Agent (Microsoft Internet Explorer)
2996	2.bin.exe	A Network Trojan was detected	ET MALWARE Win32/Vodkagats Loader Requesting Payload
2996	2.bin.exe	A Network Trojan was detected	ET MALWARE Potential Dridex.Maldoc Minimal Executable Request

3588 2bin.exe ET MALWARE Win32/Vodkagats Loader ….

3588 2bin.exe ET POLICY PE EXE or DLL Windows file ……

Voy a hablar de algunos de ellos en orden:

1080:El evento está relacionado con el incidente de seguridad en la organización LexCorp. Este tipo de alerta sugiere que hubo actividad sospechosa relacionada con la comunicación de dispositivos de la red con servidores externos.
1864:El evento muestra una alerta de tráfico malicioso.
2996:Tráfico potencialmente malicioso
2996:Detección de Troyano de red con un usuario sospechoso
2996:Detección de Troyano de red indicando una solicitud de una clave pública
2996:Detección de Troyano de red relacionado con la descarga de la clave pública
4088:Alerta de tráfico potencialmente malo activada
2996:Detección de Troyano de red con agente de usuario sospechoso
2996:Detección de Troyano de red intentando solicitar una carga útil
2996:Detección de solicitud potencial de malware desencadenada por un troyano de red
3588:Detección de posible actividad de malware
3588:Posible violacion de la privacidad corporativa donde se descargo un archivo ejecutable

Conclusión:
El impacto sobre la empresa fue significativo, ya que la pérdida de información de los componentes afectados, afectó directamente a las operaciones y continuidad de la empresa LexCorp.Hubo defectos que fueron factores críticos que contribuyeron al éxito del ataque lo que resultó una pérdida irreversible de información importante para la organización.
Podemos concluir que el malware involucrado fue un ransomware con características de loader y troyano.
Ya que por ejemplo, se cifró los archivos de los equipos, la presencia de loader y troyano puede entenderse el cómo se propagó y persistió el ransomware en la red de LexCorp.Cabe destacar que loader es un componente del malware que se utiliza para la carga y ejecutar otros archivos maliciosos en el sistema comprometido y por otro lado el troyano permite el acceso remoto y el control de las computadoras infectadas por parte de los atacantes,lo que permite moverse lateralmente dentro de la red.