



Investigación

CBR-Investigación Grupo Lazarus

Referencia del informe:	CBR-INV05
Clasificación de la información:	RESTRINGIDA

Tabla de contenido

1	Control de versiones	4
2	Introducción	4
3	Distribución de TTPs	5
3.1	Reconnaissance	5
3.2	Resource Development	5
3.3	Initial Access	6
3.4	Execution	6
3.5	Persistence	7
3.6	Privilege Escalation	8
3.7	Defense Evasion	8
3.8	Credential Access	10
3.9	Discovery	10
3.10	Lateral Movement	12
3.11	Collection	12
3.12	Command and Control	12
3.13	Exfiltration	13
3.14	Impact	14
4	Historia de sus ataques	14
4.1	2009 – Operation Troy (Operación Troya)	14
4.2	2011 - Diez Días de Lluvia	15
4.3	2013 – Más ataques en Corea del Sur	15
4.4	2014 – Ataque a Sony	15
4.5	2015 – Industria de fabricación en Corea del Sur atacada	16
4.6	2016 – Ataques en la red SWIFT	16
4.7	2017 – Bancos atacados nuevamente	16
4.8	2017 – Incidente de WannaCry	16
4.8.1	Resumen de las similitudes	17

5	El Grupo Lazarus hace uso de ingeniería social	17
6	Ransomware Lazarus	21
7	IOC's.....	23
7.1	IP's maliciosas	23
7.2	Dominios maliciosos	23
7.3	Servidores C2	24
7.4	Archivos maliciosos	24
8	Matriz del MITRE ATT&CK pintada	28
9	Reglas YARA	29
10	Referencias.....	31

1 Control de versiones


N.º Versión	Fecha	Cambio	Autor
1.0	10/08/2022	Creación	Rosa García López

2 Introducción

El Grupo Lazarus (también conocido como **HIDDEN COBRA** o **Whois Team**) es un conjunto de ciberdelincuentes norcoreano financiada por el gobierno. Se trata de una amenaza persistente avanzada (APT) debido a su nivel de amenaza y los múltiples métodos que utilizan para llevar a cabo una operación.

Llevan operando desde 2009 y han participado en numerosos ataques, varios de ellos enfocados en Corea del Sur, hasta el famoso ataque de WannaCry en 2017. El último ataque conocido que se atribuye a este grupo es un intento de phishing por correo a la plataforma cripto deBridge Finance.


Los hackers se forman en Shenyang, China, donde reciben un entrenamiento para desplegar malware de todo tipo en ordenadores, redes informáticas y servidores. Tal es la amenaza de este grupo que el FBI ha publicado una orden de búsqueda a uno de sus miembros.



WANTED BY THE FBI

PARK JIN HYOK

Conspiracy to Commit Wire Fraud; Conspiracy to Commit Computer-Related Fraud
(Computer Intrusion)



DESCRIPTION

Aliases: Pak Jin Hek, Jin Hyok Park	
Place of Birth: Democratic People's Republic of Korea (North Korea)	Hair: Black
Eyes: Brown	Sex: Male
Race: Asian	Languages: English, Korean

REMARKS

Park attended the Kim Chaek University of Technology in Pyongyang, North Korea. He is a North Korean citizen last known to be in North Korea. Park has traveled to China in the past and conducted legitimate IT work under the front company "Chosun Expo" or the Korean Expo Joint Venture in addition to activities conducted on behalf of North Korea's Reconnaissance General Bureau.

CAUTION

Park Jin Hyok is allegedly a North Korean computer programmer who is part of a state-sponsored hacking organization responsible for some of the costliest computer intrusions in history, including the cyber attack on Sony Pictures Entertainment, a series of attacks targeting banks across the world that collectively attempted to steal more than one billion dollars, and the WannaCry ransomware attack that affected tens of thousands of computer systems across the globe.

Park was alleged to be a participant in a wide-ranging criminal conspiracy undertaken by a group of hackers employed by a company that was operated by the North Korean government. The front company - Chosun Expo Joint Venture, also known as Korea Expo joint Venture - was affiliated with Lab 110, one of the North Korean government's hacking organizations. That hacking group is what some private cybersecurity researchers have labeled the "Lazarus Group." On June 8, 2018, a federal arrest warrant was issued for Park Jin Hyok in the United States District Court, Central District of California, after he was charged with one count of conspiracy to commit wire fraud and one count of conspiracy to commit computer-related fraud (computer intrusion).

If you have any information concerning this person, please contact your local FBI office or the nearest American Embassy or Consulate.

Field Office: Los Angeles

Ilustración 1 - Miembro de Lazarus buscado por el FBI

3 Distribución de TTPs

3.1 Reconnaissance

El reconocimiento consiste en técnicas que involucran a los atacantes activa o pasivamente recogiendo información que puede ser utilizada para operaciones futuras.

Las técnicas que utiliza, o ha utilizado, Lazarus de esta táctica son:

- **T1589.002 – Gather Victim Identity Information: Email Addresses:** El grupo ha recogido direcciones de email pertenecientes a varios departamentos de la organización elegida que han sido usados en campañas de phishing.
- **T1591 – Gather Victim Org Information:** Lazarus ha estudiado información pública sobre la organización elegida para mejorar las posibilidades de que funcione el spearphishing.
- **T1591.004 – Gather Victim Org Information: Identify Roles:** El grupo se ha dirigido a individuos específicos, pertenecientes a una organización, ofreciendo puestos de trabajo falsos.
- **T1593.001 – Search Open Websites/Domains: Social Media:** Lazarus ha hecho uso de LinkedIn para identificar y dirigirse a empleados específicos de la organización elegida.

3.2 Resource Development

El desarrollo de recursos consiste en técnicas que usan los atacantes para crear, comprar o comprometer/robar recursos para apoyar sus operaciones.

Las técnicas que utiliza, o ha utilizado, Lazarus de esta táctica son:

- **T1583.001 – Acquire Infrastructure: Domains:** El grupo ha obtenido dominios relacionados con sus campañas para actuar como puntos de distribución y canales C2.
- **T1583.004 – Acquire Infrastructure: Server:** Lazarus ha adquirido servidores para alojar sus herramientas maliciosas.
- **T1583.006 – Acquire Infrastructure: Web Services:** Lazarus ha alojado descargas maliciosas en Github y Dropbox.
- **T1584.001 – Compromise Infrastructure: Domains:** Han comprometido dominios legítimos, incluyendo los que están alojados en EE.UU. e Italia, para C&C.
- **T1584.001 – Compromise Infrastructure: Server:** Lazarus ha comprometido servidores para manipular herramientas maliciosas.
- **T1587.001 – Develop Capabilities: Malware:** El grupo ha desarrollado su propio malware para utilizarlo en sus operaciones.
- **T1585.001 – Establish Accounts: Social Media Accounts:** Lazarus se ha creado cuentas nuevas en LinkedIn y Twitter para llevar a cabo ingeniería social contra víctimas potenciales.
- **T1585.002 – Establish Accounts: Email Accounts:** Se han creado nuevas cuentas de email para operaciones de spearphishing.
- **T1588.002 – Obtain Capabilities: Tool:** Lazarus ha obtenido una variedad de herramientas para sus operaciones, incluyendo [Responder](#), PuTTY, PSCP, Wake-On-Lan, ChromePass y dbxcli.

- **T1588.003 – Obtain Capabilities: Code Signing Certificates:** También ha usado certificados de firmado de código, emitidos por Sectigo RSA, para algunos de sus malware y herramientas.
- **T1588.004 – Obtain Capabilities: Digital Certificates:** El grupo ha obtenido certificados SSL para sus dominios de C2.
- **T1608.001 – Stage Capabilities: Upload Malware:** Lazarus ha alojado archivos maliciosos tanto en servidores comprometidos como en los controlados por el propio grupo.
- **T1608.002 – Stage Capabilities: Upload Tool:** Han alojado herramientas personalizadas y de código abierto en servidores comprometidos y en los suyos.

3.3 Initial Access

El acceso inicial consiste en técnicas que usan varios vectores de entrada para obtener su acceso inicial dentro de la red.

Las técnicas que utiliza, o ha utilizado, Lazarus de esta táctica son:

- **T1189 – Drive-by Compromise:** El grupo Lazarus ha distribuido [RATANKBA](#) y otro código malicioso a las víctimas a través de páginas web legítimas comprometidas.
- **T1566.001 – Phishing: Spearphishing Attachment:** Lazarus ha mandado a individuos específicos emails conteniendo documentos de Microsoft Word maliciosos.
- **T1566.002 – Phishing: Spearphishing Link:** El grupo ha enviado enlaces maliciosos a las víctimas a través de correos.
- **T1566.003 – Phishing: Spearphishing via Service:** También han utilizado las redes sociales, incluyendo LinkedIn y Twitter, para mandar mensajes de spearphishing.

3.4 Execution

Consiste en técnicas que resultan en código controlado por el atacante que es ejecutado en un sistema local o remoto.

Las técnicas que utiliza, o ha utilizado, Lazarus de esta táctica son:

- **T1059.001 – Command and Scripting Interpreter: PowerShell:** El grupo Lazarus ha usado PowerShell para ejecutar comandos y código malicioso.
- **T1059.003 – Command and Scripting Interpreter: Windows Command Shell:** La interfaz de comandos de Windows (cmd) puede ser usada para controlar casi todos los aspectos del sistema. El malware de Lazarus utiliza cmd.exe para ejecutar comandos en la máquina comprometida.
- **T1059.005 – Command and Scripting Interpreter: Visual Basic:** El grupo ha usado VBA y macros incrustados en documentos Word para ejecutar código malicioso.
- **T1203 – Exploitation for Client Execution:** Lazarus ha explotado la vulnerabilidad CVE-2018-4878 de Adobe Flash para la ejecución.
- **T1106 – Native API:** Las API nativas proporcionan un medio controlado para llamar a los servicios del sistema operativo de bajo nivel dentro del kernel. Lazarus ha utilizado la API

de Windows **"ObtainUserAgentString"** para obtener el usuario-agente del equipo comprometido para conectarse a un servidor C&C.

- **T1204.001 – User Execution: Malicious Link:** El grupo Lazarus ha enviado emails en campañas de spearphishing con la intención de que el usuario entrara en el enlace malicioso.
- **T1204.002 – User Execution: Malicious File:** Los miembros de Lazarus han intentado que los usuarios lancen un documento Word malicioso entregado a través de un email en campañas de spearphishing.
- **T1047 – Windows Management Instrumentation:** Lazarus ha utilizado WMIC para la táctica de descubrimiento y, también, para ejecutar payloads y obtener persistencia y moverse lateralmente en la red.

3.5 Persistence

Consiste en técnicas usadas por los atacantes para mantener acceso al sistema, aunque este sea reiniciado, cambien las credenciales, o se produzcan otras interrupciones que puedan finalizar su acceso.

Las técnicas que utiliza, o ha utilizado, Lazarus de esta táctica son:

- **T1098 – Account Manipulation:** La manipulación de cuentas incluye cambiar las contraseñas de cuentas comprometidas, añadir cuentas a grupos con más permisos, modificar las políticas de contraseñas y cualquier acción que preserve el acceso del atacante a la cuenta. El malware *WhiskeyDelta-Two* de Lazarus contiene una función que intenta renombrar la cuenta del administrador.
- **T1547.001 – Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder:** El grupo ha mantenido persistencia cargando código malicioso en un directorio de arranque o añadiendo una clave Registry Run.
- **T1547.009 – Boot or Logon Autostart Execution: Shortcut Modification:** El malware de Lazarus ha mantenido persistencia en el sistema creando un acceso directo de LNK en la carpeta de arranque del usuario.
- **T1543.003 – Create or Modify System Process: Windows Service:** Varias familias de los malware de Lazarus se instalan a sí mismos como servicios nuevos.
- **T1574.002 – Hijack Execution Flow: DLL Side-Loading:** Lazarus ha reemplazado "win_fw.dll", un componente interno que es ejecutado durante la instalación de IDA Pro, con un DLL malicioso para descargar y ejecutar un payload.
- **T1547.013 – Hijack Execution Flow: KernelCallbackTable:** El grupo ha abusado de "KernelCallbackTable" para secuestrar el flujo del control de procesos y ejecutar shellcode.

- **T1542.003 – Pre-OS Boot: Bootkit:** El malware “WhiskeyAlfa-Three” de Lazarus modifica el sector 0 de Master Boot Record (MBR) para asegurarse de que el malware persistirá incluso si la máquina se apaga.
- **T1053.005 – Scheduled Task/Job: Scheduled Task:** Los atacantes abusan del programador de tareas de Windows para programar tareas de ejecución inicial o recurrente de código malicioso. Lazarus ha usado *schtasks* para persistir, incluyendo la ejecución periódica de un script XSL remoto o un payload VBS.

3.6 Privilege Escalation

Consiste en técnicas que usan los adversarios para ganar permisos de mayor nivel en un sistema o red.

La técnica que utiliza, o ha utilizado, Conti de esta táctica es:

- **T1078 – Valid Accounts:** El grupo ha utilizado credenciales de administrador para obtener acceso a partes restringidas de la red.

3.7 Defense Evasion

Consiste en técnicas usadas por los atacantes para evitar ser detectados tras comprometer a la víctima.

Las técnicas que utiliza, o ha utilizado, Lazarus de esta táctica son:

- **T1134.002 – Access Token Manipulation: Create Process with Token:** El keylogger “KiloAlfa” de Lazarus obtiene tokens de usuario de las sesiones interactivas para ejecutarse con la llamada de API “CreateProcessAsUserA” bajo el contexto del usuario.
- **T1140 – Deobfuscate/Decode Files or Information:** Los atacantes pueden usar archivos ofuscados o información para esconder los artefactos usados en una intrusión de un análisis. Lazarus ha utilizado shellcode con macros para descifrar y mapear manualmente DLLs y el shellcode en memoria en tiempo de ejecución.
- **T1564.001 – Hide Artifacts: Hidden Files and Directories:** El grupo ha usado un Macro VBA para poner sus atributos de archivo como System y Hidden. También ha nombrado archivos con un punto como prefijo para ocultarlas de la aplicación Finder.
- **T1562.001 – Impair Defenses: Disable or Modify Tools:** El malware de Lazarus “TangoDelta” intenta terminar varios procesos asociados con McAfee. Además, su malware “SHARPKNOT” desactiva los servicios de notificación y alerta del sistema de Windows.
- **T1562.004 – Impair Defenses: Disable or Modify System Firewall:** Varios malware de Lazarus modifican el cortafuegos de Windows para permitir conexiones entrantes o lo desactivan con *netsh*.
- **T1070 – Indicator Removal on Host:** El grupo Lazarus ha restaurado el código malicioso [KernelCallbackTable](#) a su estado original tras haber tomado control del flujo de control de procesos.

- **T1140.003 – Indicator Removal on Host: Clear Command History:** Lazarus ha eliminado los logs en un router comprometido, incluyendo la eliminación automática a través de la utilidad *logrotate*.
- **T1140.004 – Indicator Removal on Host: File Deletion:** El malware de este grupo ha eliminado archivos de varias formas, entre ellas se incluyen los llamados “suicide scripts” para eliminar los binarios del propio malware.
- **T1140.006 – Indicator Removal on Host: Timestomp:** Varias familias malware de Lazarus editan la marca del tiempo. Pueden modificar la hora de la última escritura de un registro clave a una fecha aleatoria y también copiar la fecha de archivos .exe legítimos para sus propios ejecutables.
- **T1202 – Indirect Command Execution:** Los mecanismos de persistencia de Lazarus han usado “forfiles.exe” para ejecutar archivos .htm.
- **T1140 – Deobfuscate/Decode Files or Information:**
- **T1070.004 – Indicator Removal on Host: File Deletion:** LAZARUS genera el siguiente archivo batch que sirve para eliminar su muestra y, después, ese mismo archivo batch:
- **T1036 – Masquerading:** Los atacantes intentan manipular las características de sus herramientas para hacerlas parecer legítimas o benignas. Lazarus ha ocultado archivos maliciosos haciéndolos pasar por JPEG para evitar su detección.
- **T1036.003 – Masquerading: Rename System Utilities:** Lazarus ha renombrado utilidades del sistema, como *wscrip.exe* and *mshta.exe*.
- **T1036.004 – Masquerading: Masquerade Task or Service:** El grupo ha utilizado la tarea programada *SRCheck* para enmascarar la ejecución de una .dll maliciosa.
- **T1036.005 – Masquerading: Match Legitimate Name or Location:** Los integrantes han renombrado código malicioso para ocultarlo como un narrador de Microsoft y otros archivos legítimos.
- **T1027 – Obfuscated Files or Information:** El grupo ha usado múltiples tipos de encriptación y codificación para sus payloads, incluyendo AES, Caracachs, RC4, XOR, Base64 y otros trucos.
- **T1027.002 – Obfuscated Files or Information: Software Packing:** Hacen uso de “Themida” para empaquetar DLLs maliciosos y otros archivos.
- **T1055.001 – Process Injection: Dynamic-link Library Injection:** Una muestra de su malware realiza inyección de DLL reflectiva.
- **T1620 – Reflective Code Loading:** El grupo Lazarus ha cambiado los permisos de protección de la memoria para después sobrescribir en memoria código de la función DLL con shellcode. Esta función se ejecuta más tarde con *KernelCallbackTable*.
- **T1553.002 – Subvert Trust Controls: Code Signing:** Lazarus ha firmado digitalmente malware y otras utilidades para no ser detectado.
- **T1218 – System Binary Proxy Execution:** Los atacantes pueden sobrepasar las defensas basadas en procesos y/o firmas mediante la delegación de ejecución de su contenido malicioso en archivos binarios firmados o confiables. Algunos archivos de Lazarus que se han usado para la persistencia abusan el cliente de actualización de Windows para ejecutar un DLL malicioso.

- **T1218.005 – System Binary Proxy Execution: Mshta:** El grupo ha usado *mshta.exe* para ejecutar páginas HTML descargadas por documentos de acceso inicial.
- **T1218.010 – System Binary Proxy Execution: Regsvr32:** Lazarus ha utilizado *rgsvr32* para ejecutar su malware.
- **T1218.011 – System Binary Proxy Execution: Rundll32:** También ha utilizado *rundll32* para ejecutar payloads maliciosas en el dispositivo comprometido.
- **T1221 – Template Injection:** El grupo ha usado archivos DOCX para recuperar una plantilla/DOTM.
- **T1220 – XSL Script Processing:** Como se ha visto antes, el grupo hace uso de WMIC para ejecutar un script XSL remoto y obtener persistencia.

3.8 Credential Access

Consiste en técnicas para robar credenciales como nombres de cuentas y contraseñas.

Las técnicas que utiliza, o ha utilizado, Lazarus de esta táctica son:

- **T1557.001 – Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay:** El grupo ha ejecutado Responder con el comando:

```
[Responder file path] -i [IP address] -rPv
```

Para obtener credenciales y moverse lateralmente.

- **T1110 – Brute Force:** Los atacantes pueden usar técnicas de fuerza bruta para obtener acceso a cuentas cuando no conocen la contraseña o han obtenido los hashes de las contraseñas. Lazarus ha realizado ataques de fuerza bruta a cuentas de administradores.
- **T1110 – Brute Force: Password Spraying:** El malware de Lazarus intenta conectarse a carpetas compartidas de Windows para moverse lateralmente. Utilizan una lista generada de nombres de usuario y contraseñas débiles.
- **T1056.001 – Input Capture: Keylogging:** Su malware “KiloAlfa” contiene funcionalidad de keylogging.

3.9 Discovery

Consiste en técnicas que permiten al atacante obtener conocimiento sobre nuestro sistema y red interna.

Las técnicas que utiliza, o ha utilizado, Lazarus de esta táctica son:

- **T1087.002 – Account Discovery: Domain Account:** Los atacantes tratan de obtener un listado de cuentas en un sistema o entorno.

Lazarus ha consultado un servidor de directorio activo para obtener una lista de cuentas, incluidas cuentas de administrador.

- **T1010 – Application Window Discovery:** El malware “IndiaIndia” del grupo obtiene y envía a su servidor C2 el título de la ventana de cada proceso activo. El keylogger “KiloAlfa” también tiene esta funcionalidad.
- **T1083 – File and Directory Discovery:** Se trata de una técnica que implica enumerar archivos y directorios. El grupo Lazarus ha buscado palabras en máquinas comprometidas para identificar archivos específicos de interés.
- **T1046 - Network Service Discovery:** Lazarus ha usado *nmap* desde un router de VM para escanear puertos en los sistemas pertenecientes a la red de la empresa.
- **T1057 – Process Discovery:** Varios de los malware de este grupo obtienen una lista de procesos activos en el sistema de la víctima y la envían a su servidor C2.
- **T1012 – Query Registry:** El malware “IndiaIndia” de Lazarus revisa las claves de registro dentro de HKCU y HKLM para determinar si ciertas aplicaciones están presentes; incluyendo SecureCRT, Terminal Services, RealVNC, TightVNC, UltraVNC, Radmin, mRemote, TeamViewer, FileZilla, pcAnyware y Remote Desktop. Otro de su malware comprueba la presencia de la siguiente clave de registro:

```
HKEY_CURRENT_USER\Software\Bitcoin\Bitcoin-Qt
```

- **T1082 – System Information Discovery:** Algunos malware de Lazarus recogen información del tipo y versión del SO perteneciente a la víctima, además de el nombre del ordenador e información de la CPU.
- **T1614.001 – System Location Discovery: System Language Discovery:** Lazarus ha desplegado malware diseñado para no correr en ordenadores con el lenguaje de Windows en: coreano, japonés o chino.
- **T1016 – System Network Configuration Discovery:** Su malware “IndiaIndia” obtiene y envía a su servidor C2 información sobre la configuración de la primera tarjeta de interfaz de red, incluyendo la dirección IP, puertas de enlace, máscara de subred, información de DHCP y si WINS está disponible.
- **T1049 – System Network Connections Discovery:** Para ganar acceso al sistema, los atacantes normalmente buscan conexiones activas en el sistema. Lazarus ha utilizado el siguiente comando para identificar y establecer una conexión con el anfitrión remoto:

```
net use
```

- **T1033 – System Owner/User Discovery:** Varios malware de Lazarus enumeran a los usuarios que tienen la sesión iniciada.
- **T1124 – System Time Discovery:** Un implante similar a Destover, utilizado por el grupo, puede obtener el tiempo real del sistema y enviarlo al servidor C2.
- **T1497.001 – Virtualization/Sandbox Evasion: System Checks:** Lazarus utiliza herramientas para detectar servicios de sandbox o VMware. Esto lo hace identificando la presencia de un debugger o servicios relacionados.

3.10 Lateral Movement

Consiste en técnicas que utilizan los atacantes para entrar y controlar sistemas remotos en una red.

Las técnicas que utiliza, o ha utilizado, Lazarus de esta táctica son:

- **T1534 – Internal Spearphishing:** El grupo ha llevado a cabo spearphishing interno desde dentro de una organización comprometida.
- **T1021.001 – Remote Services: Remote Desktop Protocol:** El malware “SierraCharlie” de Lazarus utiliza RDP para propagarse.
- **T1021.002 – Remote Services: SMB/Windows Admin Shares:** Otro de sus malware, “SierraAlfa”, accede la carpeta compartida *ADMIN\$* a través de SMB para moverse lateralmente.
- **T1021.004 – Remote Services: SSH:** El grupo utiliza SSH y la utilidad PSCP de PuTTY para ganar acceso a un segmento restringido de la red comprometida.

3.11 Collection

Consiste en técnicas para recolectar información y las fuentes de las que se recoge esa información que son relevantes para que los atacantes lleven sus objetivos a cabo.

Las técnicas que utiliza, o ha utilizado, Lazarus de esta táctica son:

- **T1560 – Archive Collected Data:** El grupo ha comprimido los datos robados con RAR y ha utilizado el malware “RomeoDelta” para archivar directorios específicos en formato .zip, encriptar el archivo .zip y subirlo al servidor C2.
- **T1560.002 – Archive Collected Data: Archive via Library:** Su malware “IndiaIndia” guarda la información recogida de la víctima en un archivo que es comprimido con Zlib, encriptado y subido al servidor C2.
- **T1560.003 – Archive Collected Data: Archive via Custom Method:** Una muestra de sus malware encripta datos utilizando una simple operación XOR basada en bytes antes de la exfiltración.
- **T1005 – Data from Local System:** El grupo ha recopilado datos y archivos de las redes comprometidas.
- **T1074.001 – Data Staged: Local Data Staging:** El malware “IndiaIndia” guarda el archivo con la información recogida sobre la víctima en el directorio *%TEMP%*, después es comprimido, encriptado y subido al servidor C2.

3.12 Command and Control

Consiste en técnicas que usan los atacantes para comunicarse con sistemas bajo su control dentro de la red de la víctima.

La técnica que utiliza, o ha utilizado, Lazarus de esta táctica son:

- **T1071.001 – Application Layer Protocol: Web Protocols:** Lazarus ha llevado a cabo C2 sobre HTTP y HTTPS.

- **T1132.001 – Data Encoding: Standard Encoding:** Un malware de Lazarus codifica datos con base64.
- **T1001.003 – Data Obfuscation: Protocol Impersonation:** El malware de Lazarus también usa una forma única de encriptación de comunicaciones conocida como FakeTLS, que imita a TLS, pero con un método de encriptación diferente que potencialmente evade la inspección del tráfico SSL.
- **T1573.001 – Encrypted Channel: Symmetric Cryptography:** Varios malware de Lazarus encriptan el tráfico C2 con código propio que utiliza XOR con una operación ADD y XOR con una operación SUB. Otro malware utiliza la encriptación Caracachs para encriptar payloads de C2.
- **T1008 – Fallback Channels:** Su malware “SierraAlfa” envía datos a uno de los servidores C2 harcodeados aleatoriamente, si la transmisión falla, escoge otro servidor para volver a intentar la transmisión.
- **T1105 – Ingress Tool Transfer:** El grupo Lazarus ha descargado en la máquina comprometida archivos, malware y herramientas de su servidor C2.
- **T1104 – Multi-Stage Channels:** Lazarus ha utilizado componentes de malware de varias etapas para inyectar etapas más tardías en procesos separados.
- **T1571 – Non-Standard Port:** Algunos malware de Lazarus utilizan una lista ordenada de números de puerto para el tráfico de C2, creando discrepancias en el protocolo del puerto.
- **T1090.001 – Proxy: Internal Proxy:** El grupo ha usado un router comprometido para servir como un proxy entre la red corporativa de la víctima y los segmentos restringidos.
- **T1090.002 – Proxy: External Proxy:** El grupo Lazarus ha utilizado múltiples proxys para ofuscar el tráfico de red de las víctimas.
- **T1102.002 – Web Service: Bidirectional Communication:** Los miembros han usado GitHub como C2, extrayendo payloads de imágenes alojadas y luego enviando la salida de ejecución de los comandos a archivos en directorios específicos.

3.13 Exfiltration

Consiste en técnicas cuya finalidad es robar datos de tu red.

Las técnicas que utiliza, o ha utilizado, Lazarus de esta táctica son:

- **T1048.003 – Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted Non-C2 Protocol:** Su malware “SierraBravoTwo” genera un correo a través de SMTP que contiene información sobre nuevas víctimas infectadas.
- **T1041 – Exfiltration Over C2 Channel:** Lazarus ha realizado el envío de datos y archivos exfiltrados sobre un canal C2, a través de sus herramientas y malware.
- **T1567.002 – Exfiltration Over Web Service: Exfiltration to Cloud Storage:** El grupo ha exfiltrado datos robados a Dropbox usando una versión personalizada de dbxcli.

3.14 Impact

Consiste en técnicas que alteran la disponibilidad o comprometan la integridad mediante la manipulación de los procesos comerciales y operacionales.

Las técnicas que utiliza, o ha utilizado, Lazarus de esta táctica son:

- **T1485 – Data Destruction:** Lazarus ha utilizado una función personalizada y segura para sobrescribir los contenidos de un archivo con datos de la memoria.
- **T1491.001 – Defacement: Internal Defacement:** El grupo ha reemplazado el fondo de pantalla de los sistemas con una imagen amenazante después de hacer que el sistema no se pueda iniciar con un borrado de estructura del disco.
- **T1561.001 – Disk Wipe: Disk Content Wipe:** Lazarus ha utilizado malware como “WhiskeyAlfa” para sobrescribir los primeros 64 MB de todos los discos por una mezcla de buffers estáticos y aleatorios. Luego, un proceso similar es usado para borrar el contenido en discos lógicos y, finalmente, intentar borrar todos los bytes de todos los sectores en todos los discos.
- **T1561.002 – Disk Wipe: Disk Structure Wipe:** Su malware “SHARPKNOT” sobrescribe y elimina el Master Boot Record (MBR) de la máquina de la víctima y ha poseído malware MBR wiper desde 2009.
- **T1489 – Service Stop:** El grupo ha detenido el servicio MExchangeIS para hacer que los contenidos de Exchange sean inaccesibles para los usuarios.
- **T1529 – System Shutdown/Reboot:** Lazarus ha reiniciado sistemas tras destruir archivos y borrar el MBR.

4 Historia de sus ataques

4.1 2009 – Operation Troy (Operación Troya)

Aunque el grupo lleva activo desde 2007, La primera actividad que llamó la atención sucedió en 2009 cuando una serie de ataques; comenzando el 4 de julio de ese año, afectaron a sitios web gubernamentales, financieros y mediáticos en Estados Unidos y Corea del Sur. Los ataques comenzaron en E.E.U.U en su día de la independencia, dirigidos a varias instituciones incluyendo la Casa Blanca y el Pentágono.

El tipo de ataques era una serie de denegación de servicio distribuido (DDoS). Los atacantes usaron el malware *Mydoom* y *Dozer*, un troyano, para llevar a cabo esos ataques. Colocó en los sitios web el texto “Memoria del día de la Independencia” en el registro de arranque maestro (MBR). Los ataques eran relativamente poco sofisticados, pero a lo largo de los años Lazarus ha refinado sus métodos para llevar a cabo ataques más sofisticados. Sin embargo, como se ha visto en el incidente de WannaCry al que ha sido vinculado el grupo, también pueden ser propensos al descuido.

4.2 2011 - Diez Días de Lluvia

En este ataque de tipo DDoS tuvieron como objetivo organizaciones en Corea del Sur. Similar al ataque de 2009, fueron atacados los sitios web privados y del gobierno, utilizando una herramienta llamada *Trojan.Koredos*. El modo de operar fue inusual para un ataque de DDoS, ya que no utilizaron un servidor C&C sino que los comandos estaban ocultos dentro de la propia amenaza. El uso de esta táctica mostraba una mejora en términos de sofisticación en los ataques.

También se encontró que si no se eliminaba este troyano de los dispositivos infectados el registro de arranque maestro (MBR) de algunos sería destruido en 10 días.

4.3 2013 – Más ataques en Corea del Sur

Este año, se reportó un ataque destructivo contra bancos y compañías de transmisión locales en Corea del Sur. El ataque anuló el sitio web de un ISP coreano y también paralizó los servidores de varias organizaciones. Los sitios web de las compañías afectadas se cayeron, y en algunas se les borró el contenido de muchos de sus discos. El malware utilizado en este ataque es conocido como *Jokra*, por el cual un grupo llamado “Whois” reclamó crédito en un mensaje publicado en los ordenadores. Sin embargo, los investigadores de seguridad apuntan a que Lazarus está tras este ataque.

Además, el mismo año, investigadores encontraron indicios del malware *Castov*, atacando a instituciones financieras, y sus clientes, de Corea del Sur. En este ataque, también atribuido a Lazarus, *Castov* fue usado para robar contraseñas, detalles de cuentas y certificados digitales de los ordenadores infectados.

4.4 2014 – Ataque a Sony

Este ataque es uno de los que más impacto ha tenido a nivel mediático. El ataque se hizo público el 24 de noviembre de 2014, cuando los empleados de Sony encendieron sus ordenadores para ver un esqueleto rojo y la frase “Hacked by GOP”, abreviación de “Guardians of the Peace”. El mensaje también amenazaba con publicar información más tarde ese mismo día si no completaban una solicitud. En las siguientes semanas, se publicaron grandes cantidades de los datos robados a Sony, incluyendo: información personal de sus empleados y familias; mensajes de correos entre los empleados de la compañía; información sobre los salarios, películas sin estrenar y más información.

Mucha de la información filtrada, particularmente algunos mensajes de correo entre los ejecutivos recibieron mucha atención de los medios de comunicación y causaron vergüenza a la compañía.

Además de filtrar grandes cantidades de información, los atacantes también destruyeron varios ordenadores en la organización utilizando el malware *Backdoor.Destover*. Este es un malware particularmente destructivo que puede eliminar completamente el sistema infectado. Es posible configurar *Destover* para que tenga como objetivos solamente los ordenadores de una organización específica, que seguramente haya sido el caso en este ataque.

4.5 2015 – Industria de fabricación en Corea del Sur atacada

En octubre de 2015, Symantec encontró evidencia de que organizaciones en Corea del Sur estaban siendo atacadas con varias herramientas maliciosas, incluyendo *Backdoor.Duuzer*, *W32.Brambul*, y *Backdoor.Joanap*. Estas amenazas aparentemente tienen origen en el mismo grupo. El objetivo de estos ataques parecía ser el de robar datos e información; ciberespionaje.

4.6 2016 – Ataques en la red SWIFT

Un ciberataque en febrero de 2016 resultó en el robo de 81 millones de dólares robados al Banco Central de Bangladesh, que con la vigilancia de empleados bancarios frenaron el fraude antes de que se robara más dinero.

El dinero fue robado a través de transacciones SWIFT fraudulentas, el sistema SWIFT en sí no fue comprometido, y el malware *Trojan.BanSwift* fue usado para cubrir el rastro del ataque. Investigaciones posteriores de Symantec determinaron que los mismos atacantes estaban detrás de ataques similares en otros bancos de Asia, como el Tien Phong Bank de Vietnam, que dijo que había interceptado una transferencia fraudulenta de más de 1 millón de dólares en el cuarto trimestre de 2015.

El hecho de que el troyano *BanSwift* y *Backdoor.Contopee* compartieran código, que previamente había usado Lazarus, conllevó que los investigadores determinaran que Lazarus estaba detrás de estos ataques.

4.7 2017 – Bancos atacados nuevamente

En febrero de 2017, Symantec publicó una investigación de ataques “watering hole” que intentaron infectar más de 100 organizaciones en 31 países diferentes con un malware que era desconocido llamado *Downloader.Ratabanka*. Estos ataques se dirigieron mayormente a bancos, un número pequeño de telecomunicaciones y firmas de internet. Sin embargo, no hay pruebas de que se robara dinero a ninguno de los bancos.

Los investigadores de Symantec fueron capaces de establecer enlaces entre *Ratabanka* y herramientas asociadas previamente con Lazarus, llevándoles a concluir que Lazarus estaba detrás de estos ataques.

4.8 2017 – Incidente de WannaCry

Los ataques del ransomware WannaCry recibieron una gran atención mediática desde que un ataque generalizado el 12 de mayo causó que los sistemas de muchas organizaciones grandes de todo el mundo, incluido el NHS en Reino Unido, se detuvieran de golpe.

Symantec descubrió pruebas de que una versión anterior de WannaCry fue usada en ataques dirigidos a empresas en febrero, marzo y abril; pero el filtrado del exploit para EternalBlue por Shadow Brokers en abril aparentemente fue un hecho fortuito para los atacantes, que les permitió difundir el ransomware a más sitios.

El análisis, hecho por Symantec, de los primeros ataques de WannaCry reveló similitudes sustanciales en las herramientas, técnicas e infraestructura entre las utilizadas por los atacantes y

las previamente vistas en ataques de Lazarus, por lo que es muy probable que Lazarus también estuviera detrás de la propagación de WannaCry.

Si bien causó atención, ciertos errores en la forma en la que se implementó WannaCry indican un grado de descuido que pudo haber reducido su efectividad. Por ejemplo, aunque el ransomware tenía código para proporcionar direcciones de Bitcoin únicas para cada víctima, elegía las que se encontraban harcodeadas por defecto, como resultado de un error de condición de carrera. Esto significaba que WannaCry no podía usar direcciones Bitcoin únicas por el error y no podían seguir el rastro de las transacciones. Los atacantes publicaron una variante 13 horas después del desarrollo inicial de WannaCry con el error arreglado, pero la mayoría de las infecciones que ocurrieron tenían este error.

Aún existe mucho misterio en el ataque de WannaCry y en el grupo Lazarus. Pero dado por hecho que ha estado activo por casi una década, es poco probable que este ataque ransomware sea el último que veamos de este grupo.

4.8.1 Resumen de las similitudes

- En el primer ataque de WannaCry en febrero, se encontraron tres evidencias de malware en la red de la víctima vinculadas a Lazarus: *Trojan.Volgmer* y dos variantes de *Backdoor.Destover*, la herramienta para borrar discos utilizada en los ataques a Sony.
- *Trojan.Alphanc*, que fue utilizado para propagar WannaCry en los ataques de marzo y abril, es una versión modificada de *Backdoor.Duuzer*; que ha sido previamente relacionada con Lazarus.
- *Trojan.Bravonc* utilizaba las mismas direcciones IP por C&C que *Backdoor.Duuzer* y *Backdoor.Destover*, ambos han sido relacionados con Lazarus.
- *Backdoor.Bravonc* tiene un código de ofuscación similar al de WannaCry e *Infostealer.Fakepude*, el cual tiene conexión con Lazarus.
- Existe código compartido entre WannaCry y *Backdoor.Contopee*, previamente relacionado con el grupo.

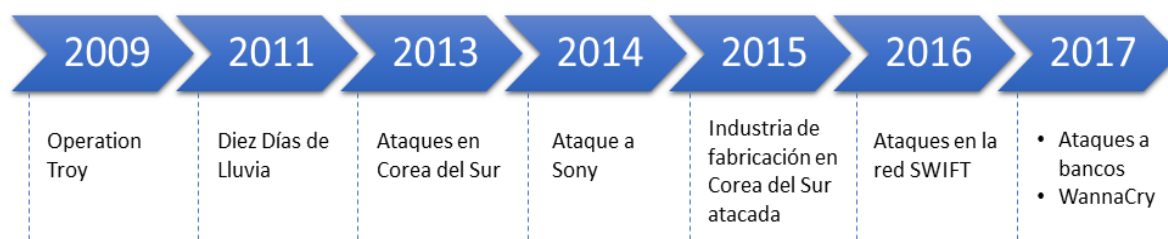


Ilustración 2 - Resumen de ataques más importantes de Lazarus

5 El Grupo Lazarus hace uso de ingeniería social

En varias ocasiones, y actualmente, los miembros de Lazarus han intentado hacerse pasar por alguna persona perteneciente a empresas relacionadas con criptomonedas.

En agosto de 2020, el grupo utilizó **LinkedIn** para enviar una oferta de trabajo falsa y relacionada con una compañía de blockchain. En estos casos el atacante necesita convencer a la víctima para que active los macros del documento que esconde el código malicioso. En esta campaña, el documento de Microsoft Word decía estar protegido bajo el Reglamento general de protección de datos (RGPD) de la Unión Europea y el contenido solo podría ser mostrado si se activaban los macros.

Una vez se habilitan los macros, estos crean un archivo .LNK diseñado para ejecutar un archivo llamado “mshta.exe” y llamar a un enlace *bit.ly* conectado a un script de Visual Basic. Este script hace comprobaciones del sistema y envía información operacional a un servidor C2.

Se pueden ver ejemplos de una campaña en 2021, en la que el señuelo era una oferta de trabajo en Crumpton Group LLC.

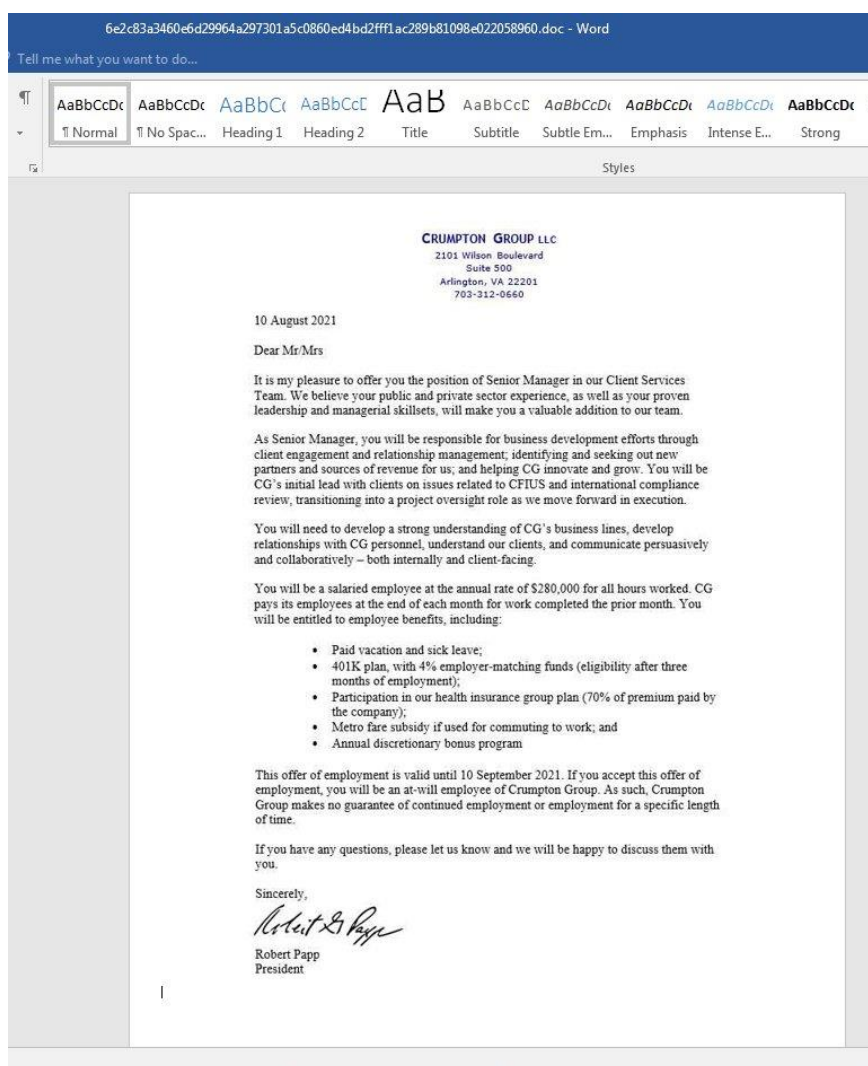


Ilustración 3 - Oferta de trabajo falsa

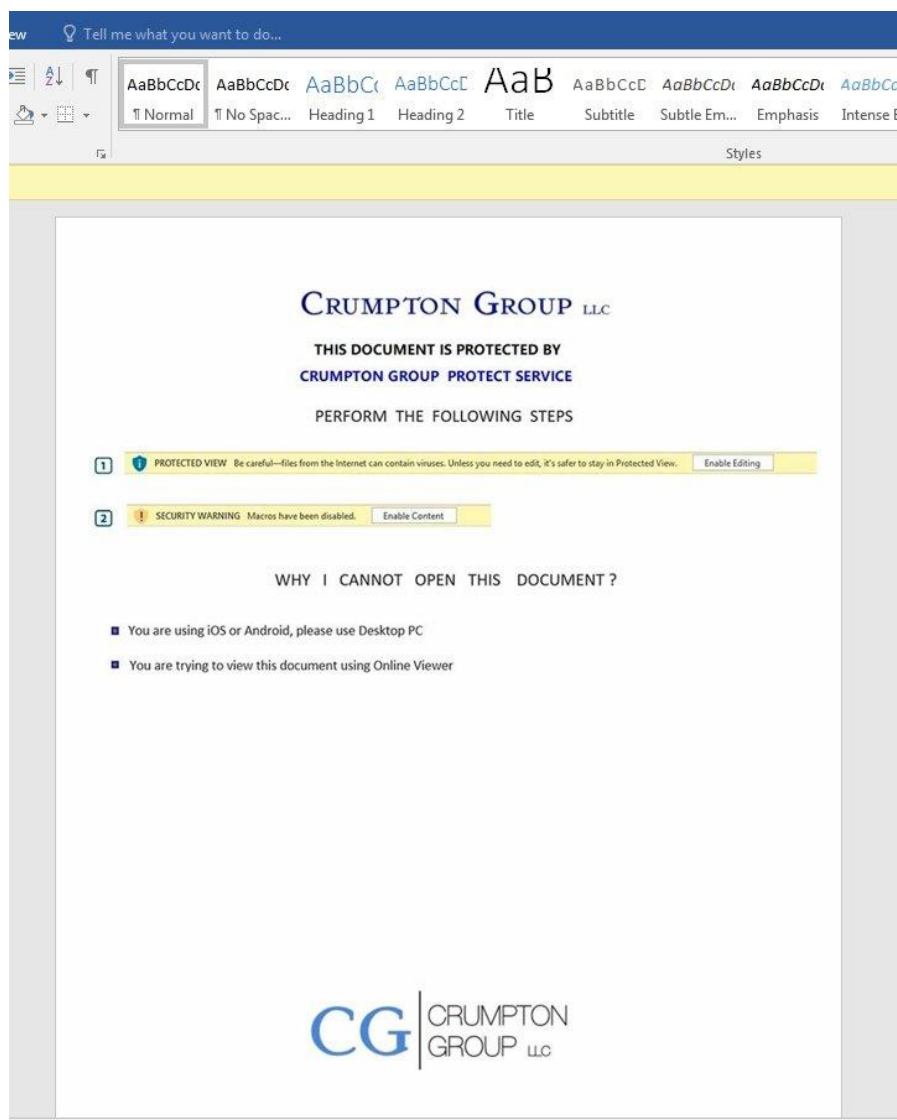


Ilustración 5 - Pasos para que la víctima habilite los macros

En otras ocasiones también han utilizado Telegram como una vía para que la víctima se conecte a un servidor C2:

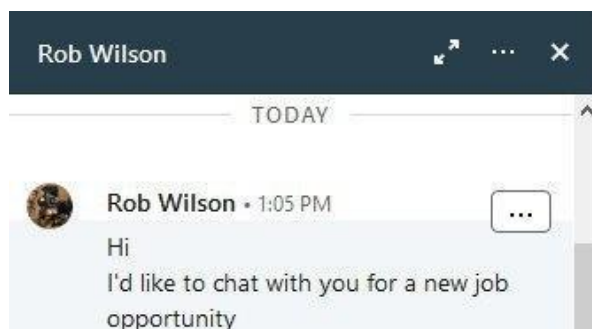


Ilustración 4 - Mensaje phishing en LinkedIn

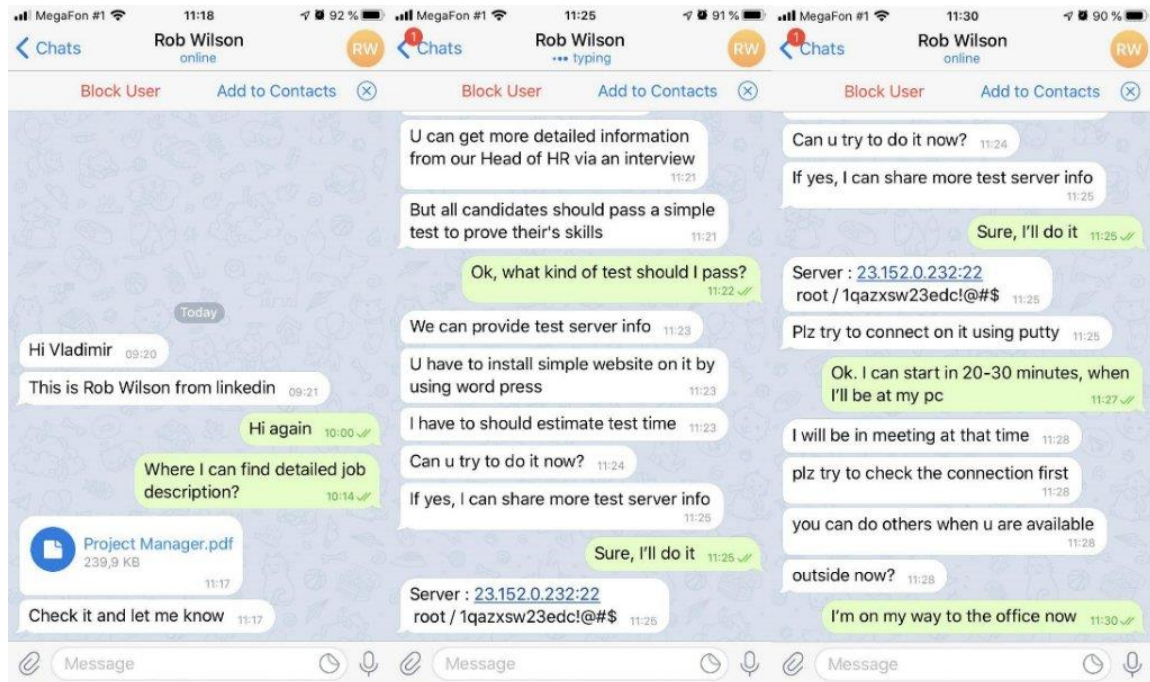


Ilustración 6 - Conversación de Telegram

El 8 de febrero de este año, se atribuye a Lazarus otra campaña similar a las anteriores. En este caso utilizó el nombre de la empresa “Lockheed Martin” para ofrecer ofertas de trabajo falsas. Los documentos, llamados “Lockheed_Martin_JobOpportunities.doc” y “Salary_Lockheed_Martin_job_opportunities_confidential.doc”, contienen macros maliciosos que activan shellcode para interceptar el flujo de control, recuperar los documentos señuelo y crear tareas programadas como forma de persistencia.

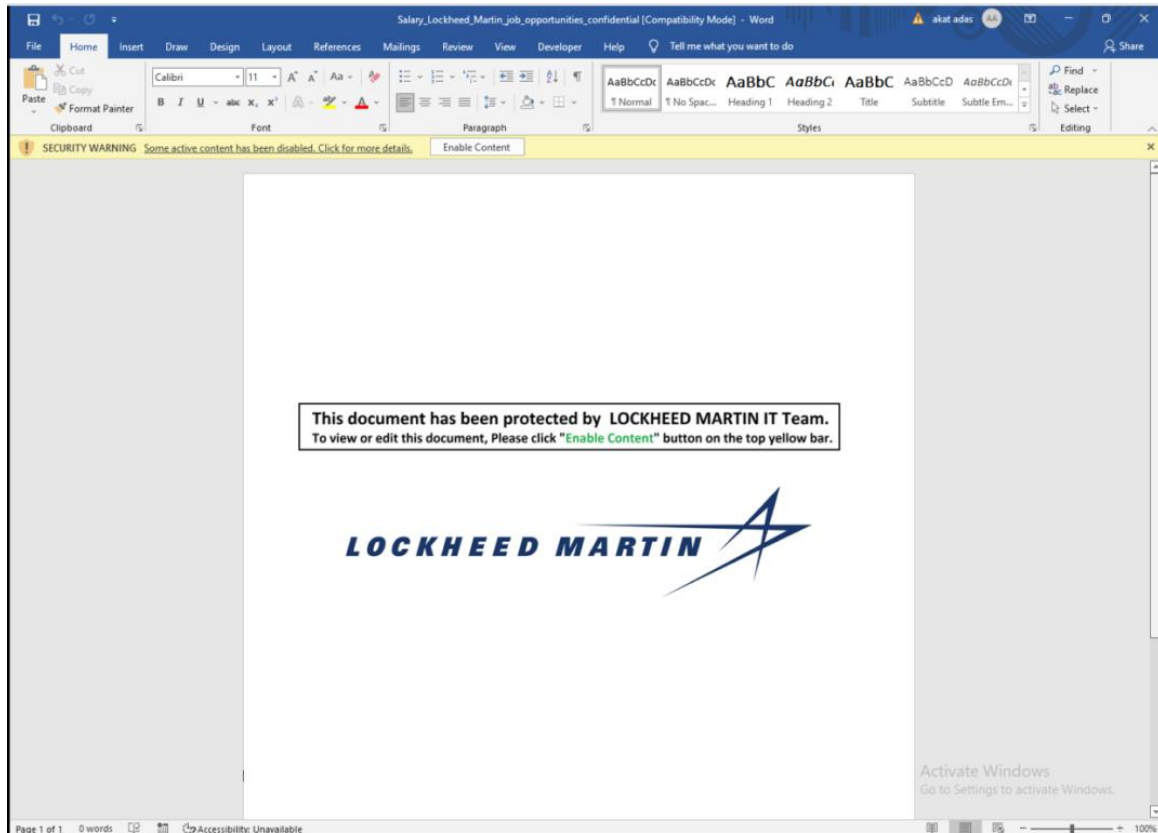


Ilustración 7 - Documento con la oferta de trabajo falsa

6 Ransomware Lazarus

Existe un ransomware con el nombre de Lazarus, este procede de King Ouroboros, otro programa de tipo ransomware. Como los demás programas de este tipo, Lazarus cifra los archivos y los atacantes piden un pago a cambio de que sean descifrados. Lazarus añade al nombre de los archivos cifrados una cadena que contiene a dirección de e-mail, ID de víctima y la extensión ".Lazarus". Por ejemplo, el archivo "test.txt" podría convertirse en: "test.txt.[ID=L34xIF62Ac][Mail=ejemplo@gmail.com].Lazarus". Además, crea un archivo de texto llamado "Read-Me-Now.txt" y muestra una ventana emergente.

El contenido del archivo sería el que muestra la siguiente imagen:

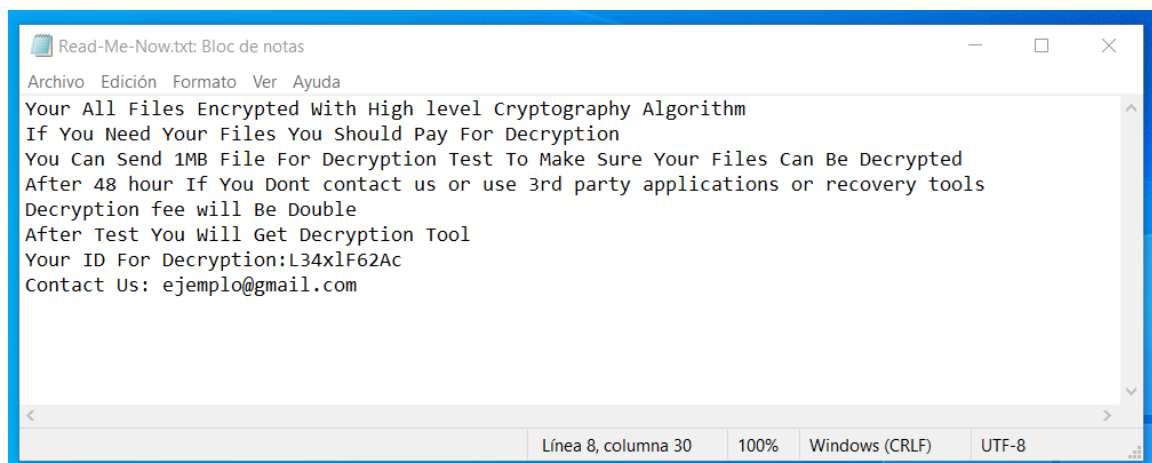


Ilustración 8 - Nota de rescate del ransomware

El contenido de la ventana emergente es el siguiente:

Your Files Has Been Encrypted
How To Recover:
Your Data Has Been Encrypted Due The Security Problem
If You Want To Restore Your Files Send Email to Us
Before Paying You Can Send 1MB file For Decryption Test to guarantee that your Files Can Be Restored
Test File Should Not Contain Valuable Data (Databases Large Excels , Backups)
Do Not Rename Files or Do Not Try Decrypt Files With 3rd Party Softwares , It May Damage Your Files
And Increase Decryption Price

Your ID: -
Our Email: mr.teslabrain@gmail.com

How To Buy Bitcoin:
Payment Should Be With Bitcoin
You Can learn how To Buy Bitcoin From This Links:
 [hxxps://localbitcoins.com/buy_bitcoins](https://localbitcoins.com/buy_bitcoins)
 [hxxps://www.coindesk.com/information/how-can-i-buy-bitcoins](https://www.coindesk.com/information/how-can-i-buy-bitcoins)

El precio que piden los atacantes para descifrar los archivos varía; sin embargo, si no han recibido noticias en 48 horas tras el cifrado se duplicará la cantidad que ha sido pedida.

Como con los demás ransomware, no se recomienda cooperar con los atacantes ni pagar lo pedido. Lo mejor sería tener una o más copias de seguridad para poder recuperar los archivos sin problema.

7 IOC's

7.1 IP's maliciosas

- 139.60.161.228
- 45.14.227[.]5
- 199.188.103[.]115
- 82.102.31.14
- 108.170.55[.]202
- 104.168.98[.]156
- 38.132.124[.]161
- 89.45.4[.]151
- 182.48.49[.]233
- 150.60.192[.]67
- 54.64.30[.]175
- 164.46.106[.]43
- 118.128.190[.]191
- 160.153.142[.]0
- 198.133.183[.]67
- 166.62.39[.]82
- 23.152.0[.]232
- 162.241.219[.]119
- 92.249.45[.]182
- 104.168.167.16
- 23.254.217.53
- 185.243.115.17
- 104.168.218.42
- 95.213.232.170
- 108.174.195.134
- 185.228.83.32
- 172.81.135.194

7.2 Dominios maliciosos

- tokenais[.]com
- dafom[.]dev
- cryptais[.]com
- alticgo[.]com
- esilet[.]com
- creaideck[.]com
- aideck[.]net

- goldllama4.sakura[.]ne.jp
- propro[.]jp
- vega.mh-tec[.]jp
- hospitality-partners[.]co.jp
- apars-surgery[.]org
- akramportal[.]org
- bootcamp-coders.cnm[.]edu
- clicktocareers[.]com
- forecareer[.]com
- gbflatinamerica[.]com
- inovecommerce[.]com.br
- www.wb-bot.org
- www.jmttrading.org
- cyptian.com
- beastgoc.com
- www.private-kurier.com
- www.wb-invest.net
- wfcwallet.com
- chainfun365.com
- www.buckfast-zucht.de
- invesuccess.com
- private-kurier.com
- aeroplans.info
- mydealoman.com
- unioncrypto.vip

7.3 Servidores C2

- hxxp://emsystec[.]com/include/inc[.]asp
- hxxp://www[.]gyro3d[.]com/common/faq[.]asp
- hxxp://www[.]newbusantour[.]co[.]kr/gallery/left[.]asp
- hxxp://ilovesvc[.]com/HomePage1/Inquiry/privacy[.]asp
- hxxp://www[.]syadplus[.]com/search/search_00[.]asp
- hxxp://bn-cosmo[.]com/customer/board_replay[.]asp
- hxxp://softapp[.]co[.]kr/sub/cscenter/privacy[.]asp
- hxxp://gyro3d[.]com/mypage/faq[.]asp
- https://bodyshoppechiropractic.com
- https://ecombox.store
- http://trade.publicvm.com/images/top_bar.gif

7.4 Archivos maliciosos

MD5	SHA256
-----	--------

21307227ECE129B1E12797ECC2C9B6D9	8A4D2BAA8CF519C7A9B91F414A0A9D8BA2B 9E96D21D9E77DA7B34ED849830A36
6F0338AF379659A5155B3D2A4F1A1E92	CA8DC152DC93EC526E505CF2A173A635562F FBF55507E3980F7DC6D508F0F258
0489978ffa3b864ede646d0470500336	2A99BCB5D21588E0A43F56AADA4E2F38679 1E0F757126B2773D943D7CBF47195
a1ffca7ba257b4eca7fe7d1e78bac623	3C86FC0A93299A0D0843C7D7FF1A137A9E79 9F8F2858D3D30F964E3C12C28C9E
f27cf59b00dacdd266ad7894a1df0894	92b0f4517fb22535d262a7f17d19f7c21820a0 11bfe1f72a2ec9fbffbd7e3e0
a1ffca7ba257b4eca7fe7d1e78bac623	3C86FC0A93299A0D0843C7D7FF1A137A9E79 9F8F2858D3D30F964E3C12C28C9E
511778c279b76cac40d5d695c56db4f5	91146EE63782A2061701DB3229320C161352 EE2BC4059CCC3123A33114774D66
f774c0588da59a944abc78d5910be407	A7EA1852D7E73EF91EFB5EC9E26B4C482CA6 42D7BC2BDB6F36AB72B2691BA05A
8386379a88a7c9893a62a67ea3073742	7F8166589023CD62AE55A59F5FCA60705090 D17562B7F526359A3753EB74EA2F
3bc855bfadfea71a445080ba72b26c1c	043E0D0D8B8CDA56851F5B853F244F677BD 1FD50F869075EF7BA1110771F70C2
F27CF59B00DACDD266AD7894A1DF0894	92B0F4517FB22535D262A7F17D19F7C21820 A011BFE1F72A2EC9FBFFBDC7E3E0
E8C6ACC1EB7256DB728C0F3FED5D23D7	524F8F0F8C31A89DF46A77C7A30AF5D2A1D C7525B08BFAFBED98748C3D8A3F1C
1D4EC831292B611F1FF8983EBD1DB5D4	41E9D6C3374FD0E78853E945B567F9309446 084E05FD013805C70A6A8205CD70
D0CE651A344979C8CD11B8019F8E4D7E	436195BD6786BAAE8980BDFED1D7D7DBCCC B7D5085E79EBDCC43E22D8BAE08A8
9A5FA5C5F3915B2297A1C379BE9979F0	9F177A6FB4EA5AF876EF8A0BF954E3754491 7D9AABA04680A29303F24CA5C72C
86759CE27D0FE0B203AAA19D4390A416	AE8E9FF2DC0EC82B6BAE7C4D978E3FEAC933 53CB3CD903E15873D31E30749150
FCF3702E52AE32C995A36F7516C662B7	FC079CEFA19378A0F186E3E3BF90BDEA19AB 717B61A88BF20A70D357BF1DB6B8

e117406e3c14ab8e98b27c3697aea0b6	2BA20E39FF90E36086044D02329D43A8F7AE 6A7663EB1198B91A95EA556CF563
a4873ef95e6d76856aa9a43d56f639a4	b5665832542286da685a020bbcb37508df453 12e81d4e4722fa6a644a11421bb
d35a9babbd9589694deb4e87db222606	fc5654ffc82ec3c7190122ba5fb06b0677744a1 8a702b439a0997fc828e04989
70bcafbb1939e45b841e68576a320603	f460692ea6c4e5dbb968def9567090335d5d7 188167c3e487d05c526d7201108
3f4cf1a8a16e48a866aebd5697ec107b	202cfbe37bcde2f5700fa43e5a4e08e6b2df63 22d9cdfa958d95ab598b47b6b3
b7092df99ece1cdb458259e0408983c7	4281854f27a755ab51e71d951016ad10ff30a0 3cd612ba1b14c4d89d9b4be212
8e302b5747ff1dcad301c136e9acb4b0	d178cced92bbce22d2214dbdd3db0491f1c35 2d21634fda9abd08d720faca84d
d90d267f81f108a89ad728b7ece38e70	96723f0282d2439bce61885e20a7a080fd1cc1 178d1371d1dd55274a2a84f4b7
47b73a47e26ba18f0dba217cb47c1e16	0e48382f001420abb7cedcc9f74f7c8348be4f9 668bb082629b0eaf533d4b715
77ff51bfce3f018821e343c04c698c0e	2254bc2a7e8e77dc968bb10bc2738ea56a004 e1dc81e99fbea015396d8644b42
c2ea5011a91cd59d0396eb4fa8da7d21	60b3cfe2ec3100caf4afde734cfd5147f78acf58 ab17d4480196831db4aa5f18
930f6f729e5c4d5fb52189338e549e5e	5b40b73934c1583144f41d8463e227529fa71 57e26e6012babd062e3fd7e0b03
4e5ebbecd22c939f0edf1d16d68e8490	f0e8c29e3349d030a97f4a8673387c2e21858c ccd1fb9ebbf9009b27743b2e5b
1c7d0ae1c4d2c0b70f75eab856327956	765a79d22330098884e0f7ce692d61c40dfcf2 88826342f33d976d8314cfd819
855b2f4c910602f895ee3c94118e979a	e3d98cc4539068ce335f1240deb1d72a0b57b 9ca5803254616ea4999b66703ad
9a6307362e3331459d350a201ad66cd9	8acd7c2708eb1119ba64699fd702ebd96c0d5 9a66cba5059f4e089f4b0914925
53d9af8829a9c7f6f177178885901c01	9ba02f8a985ec1a99ab7b78fa678f26c0273d9 1ae7cbe45b814e6775ec477598

1ca31319721740ecb79f4b9ee74cd9b0	9d9dda39af17a37d92b429b68f4a8fc0a76e93ff1bd03f06258c51b73eb40efa
9578c2be6437dcc8517e78a5de1fa975	dced1acbbee11db2b9e7ae44a617f3c12d6613a8188f6a1ece0451e4cd4205156
5d43baf1c9e9e3a939e5defd8f8fbd8d	867c8b49d29ae1f6e4a7cd31b6fe7e278753a1ba03d4be338ed11fd1efc7dd36
8397ea747d2ab50da4f876a36d673272	89b5e248c222ebf2cb3b525d3650259e01cf7d8fff5e4aa15ccd7512b1e63957
636f8bd214d092ae3feb547599b4935e	0f56ebca33efe0a2755d3b380167e1f5eab4e6180518c03b28d5cffd5b675d26
b484b0dff093f358897486b58266d069	f12db45c32bda3108adb8ae7363c342fdd5f10342945b115d830701f95c54fa9
c9ed87e9f99c631cda368f6f329ee27e	802efe9c41909354921009bd54be7dcf1ee14fcfaf62dacbcdaafbe051a711e3
2025d91c1cdd33db576b2c90ef4067c7	bed916831e8c9babfb6d08644058a61e3547d621f847c081309f616aed06c2fe
5cc28f3f32e7274f13378a724a5ec33a	18f0ad8c58558d6eb8129f32cbc2905d0b63822185506b7c3bca49d423d837c7
cd0a391331c1d4268bd622080ba68bce	7446efa798cfa7908e78e7fb2bf3ac57486be4d2edea8a798683c949d504dee6
12011c44955fd6631113f68a99447515	c92c158d7c37fea795114fa6491fe5f145ad2f8c08776b18ae79db811e8e36a3
6e815cacb43c9bc055399a4fd4922ebc	1174fd03271f80f5e2a6435c72bdd0272a6e3a37049f6190abf125b216a83471
8ed89d14dee005ea59634aade15dba97	9c906c2f3bfb24883a8784a92515e6337e1767314816d5d9738f9ec182beaf44
058542975392c636371b88a3f6142d7	75bf8feeac2b5b1690feab45155a6b97419d6d1b0d36083daccb061dc5dbdea8
e5ff537666b387c39a406cbbb359b2ed	e13888eed2466efaae729f16fc8e348fbabea8d7acd6db4e062f6c0930128f8f
994c02f8c721254a959ed9bc823ab94b	17f1c3dc3ad9e0e87e6a131bd93d12c074b443f365eea2e720b9d9939f9ce22e
bc731ade86b380e87eb6188b7f2b4255	c3a6e07ab16c8c887368ec65bed759f4690efcb539eb6a0904db005d1fe25427

24b3614d5c5e53e40b42b4e057001770	e3623c2440b692f6b557a862719dc95f41d2e 9ad7b560e837d3b59bfe4b8b774
629b9de3e4b84b4a0aa605a3e9471b31	01c13f825ec6366ac2b6dd80e5589568fa5c86 85cb4d924d1408e3d7c178902f
055829e7600dbdae9f381f83f8e4ff36	09625d6c73ba17a14cd927f5c6d90400efcaf9 21b42962c473c5de11a12d2cf1

8 Matriz del MITRE ATT&CK pintada

about

Lazarus Group

Tácticas y técnicas usadas por el grupo Lazarus.



Ilustración 9 – Matriz pintada con los TTPs de Lazarus

9 Reglas YARA

```
rule APT_Lazarus_Keylogger {
  meta:
    description = "Detects possible Lazarus Keylogger"
    author = "@VK_Intel"
    date = "2019-01-25"
  strings:
    $s0 = "%s%s" fullword ascii wide
    $s1 = "[ENTER]" fullword ascii wide
```

```
$s2 = "[EX]" fullword ascii wide
$s3 = "%02d:%02d" fullword ascii wide

$dll0 = "PSLogger.dll" fullword ascii wide
$dll1 = "capture_x64.dll" fullword ascii wide
$exe = "PSLogger.exe" fullword ascii wide

condition:
    uint16(0) == 0x5a4d and all of ($s*) and (1 of ($dll*) or $exe)
}
```

```
rule apt_possible_Lazarus_powerratankba_b {
    meta:
        description = "Detects possible Lazarus PowerRatankba.B from Redbanc"
        author = "@VK_Intel"
        date = "2019-01-15"
        hash1 = "db8163d054a35522d0dec35743cfd2c9872e0eb446467b573a79f84d61761471"
        strings:
            $f0 = "function EncryptDES" fullword ascii
            $s0 = "$ProID = Start-Process powershell.exe -PassThru -WindowStyle Hidden -ArgumentList" fullword ascii
            $s1 = "$respTxt = HttpRequestFunc_doprocess -szURI $szFullURL -szMethod $szMethod -contentData $contentData;" fullword ascii
            $s2 = "$cmdSchedule = 'schtasks /create /tn \"ProxyServerUpdater\"" ascii
            $s3 = "/tr \"powershell.exe -ep bypass -windowstyle hidden -file \" ascii
            $s4 = "C:\\\\Users\\\\Public\\\\Documents\\\\tmp' + -join " ascii
```

```
$s5 = "$cmdResult = cmd.exe /c $cmdInst | Out-String;" fullword  
ascii  
$s6 = "whoami /groups | findstr /c:\"S-1-5-32-544\" fullword ascii  
condition:  
filesize < 500KB and $f0 and 2 of ($s*)  
}
```

10 Referencias

<https://attack.mitre.org/groups/G0032/>

<https://www.bleepingcomputer.com/news/security/debridge-finance-crypto-platform-targeted-by-Lazarus-hackers/>

<https://www.fbi.gov/wanted/cyber/park-jin-hyok>

<https://medium.com/threat-intel/lazarus-attacks-wannacry-5fdeddee476c>

<https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=b2b00f1b-e553-47df-920d-f79281a80269&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments>

<https://www.pcrisk.es/guias-de-desinfeccion/9335-lazarus-ransomware>

<https://securelist.com/lazarus-trojanized-defi-app/106195/>

https://www.cisa.gov/uscert/sites/default/files/publications/AA22-108A-TraderTraitor-North_Korea_APT_Targets_Blockchain_Companies.pdf

<https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/lazarus-recruitment/>

<https://securelist.com/operation-applejeus-sequel/95596/>

<https://www.zdnet.com/article/lazarus-hackers-target-defense-industry-with-fake-lockheed-martin-job-offers/>