Primera Entrega Alan Bono

# **Dato fuente de la información**

Fueron analizadas las siguientes fuentes de información para la elaboración del informe:

* AnyRun
* VirusTotal

# **Análisis de Malware**

La noche del 20 al 23 de junio de 2021, LexCorp fue víctima de un ataque que afectó a sus servidores (Windows Server 2003/2012) y equipos de usuario (Windows 7/Windows 10) de toda la infraestructura. El área de soporte técnico guardó una muestra del malware para poder ser analizado.

Como resultado del análisis del malware, se ha identificado lo siguiente:

* No se detecta de donde proviene el archivo, sin embargo, es un archivo de tipo .ZIP que contiene un ejecutable. Es altamente probable que el mismo haya sido descargado de algún enlace adjunto a un mail sospechoso después de haber analizado las amenazas del malware. Ya que también dentro del análisis, se menciona la amenaza Stealer que suele estar involucrada con el phishing.
* El .ZIP fue extraído y una vez dentro, se ejecutó el archivo .EXE, lo cual desencadenó en un proceso de encriptación de archivos.
* No solamente se encriptaron los archivos de la pc donde se ejecutó el ransomware, si no que también sucedió con otros equipos de usuario y servidores, por lo cual se presume que el ataque se expandió a través de la misma red que estaban conectados todos estos equipos afectados.
* El ejecutable encripta y luego borra los archivos, luego solicita un rescate por cierto monto de dinero en moneda Bitcoin.

# **Muestra analizada con AnyRun**

|  |  |
| --- | --- |
| **Nombre de la muestra** | **Proforma Invoice and Bank swift-REG.PI-0086547654.exe** |
| **Fecha del análisis** | **24/09/2021 17:10** |
| **OS utilizado para análisis** | **Windows 7 Professional Service Pack 1 (32 bit)** |
| **MD5** | **D69DC6569B385C0467185D002E252D89** |

# **Información estática**

## 

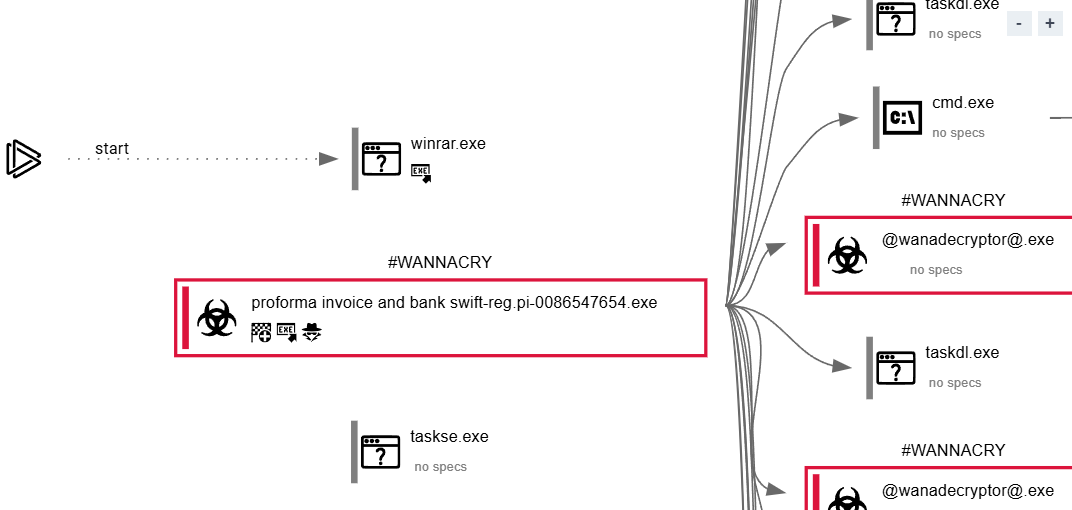
# **Screenshot de comportamiento**



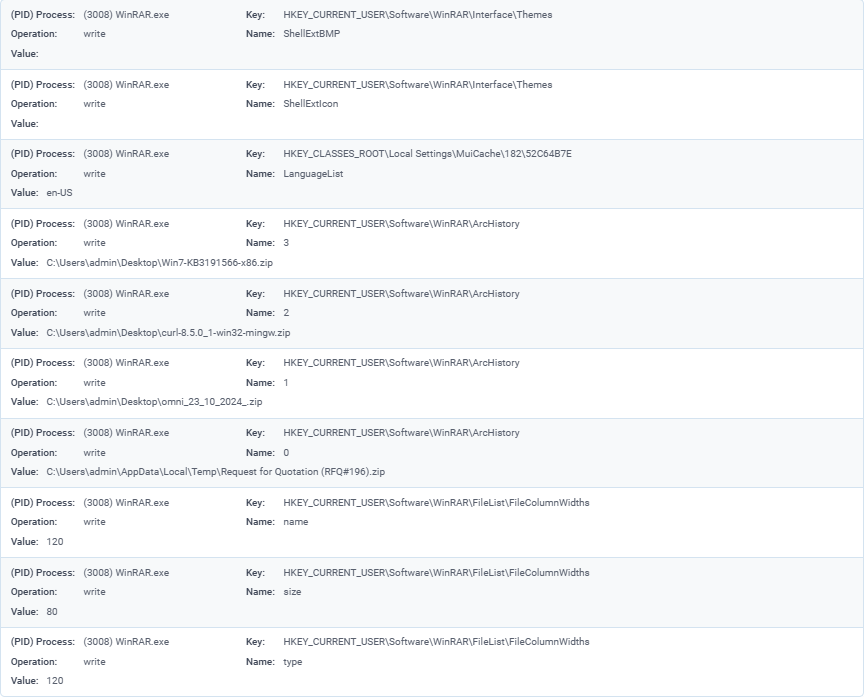
# **Screenshot de simulación**

# screenshot

# **Diagrama de procesos de comportamiento**



# **Eventos asociados**



# **HTTP Requests**

No hay.

# **Conexiones**



# **DNS requests**



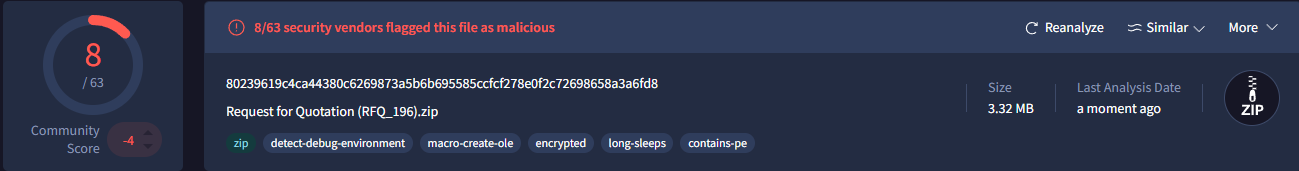
# **Amenazas**

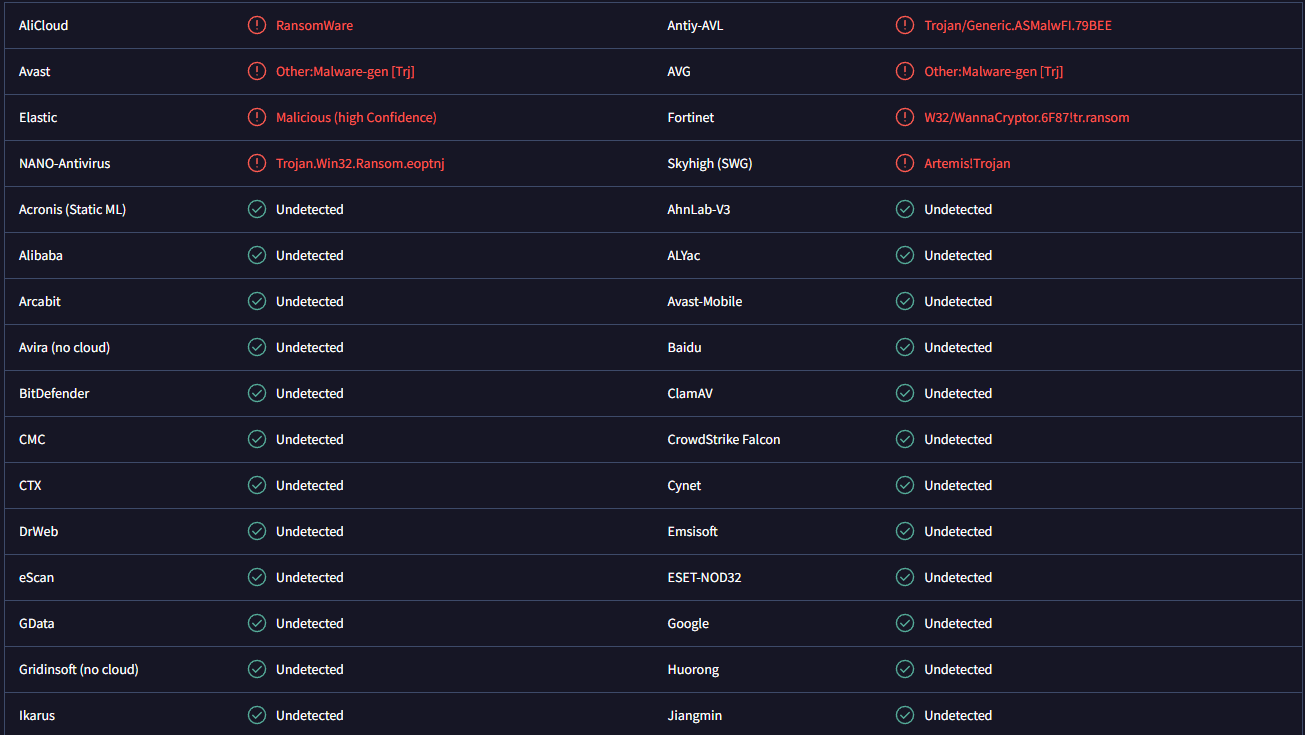


# **Muestra analizada con VirusTotal**

Sólo 7 de 64 vectores de seguridad detectaron como malicioso en el primer análisis del ransomware. Para el análisis se utilizo el mismo MD5 utilizado en AnyRun.

Se realizó un segundo análisis y dio como resultado 8 de 63.





# **Conclusión**

**Comportamiento del malware:** Loader / Evasion / Stealer

**Nombre general:** WannaCry

**Investigación del malware:** Ransomware WannaCry

**Tipo de malware:** Ransomware

## **Stealer:**

Es un grupo de software malicioso que intenta obtener acceso a la información del usuario sin la autorización del mismo. Este tipo de malware es distribuído a través de phishing.

## **WannaCry:**

Es un ransomware conocido por infectar al menos 200000 computadoras alrededor del mundo. El mismo continúa estando activo y siendo una peligrosa amenaza.