Informe Pericial Informático sobre el Ataque de Ransomware a la Empresa "Finanzas S.L."

Identificación:

- **Código de Identificación**: Informe Pericial Nº 001/2024
- **Órgano destinatario**: Juzgado de Instrucción Nº1 de Madrid
- **Número de expediente**: 12345
- **Perito**: Sergio Carretero Otero
  - Número de colegiado: 12345
  - Asociación Nacional de Peritos Informáticos (ANPI)
  - Contacto: sergiocarretero@peritos.com / Tel: +34 600 123 456
- **Solicitante**: Finanzas S.L.
  - Dirección: Calle Mayor, Nº 23, 28013 Madrid
- **Abogado**: Ana López García (Colegiado Nº54321)
- **Procurador**: Carlos Martín Rodríguez
- **Fecha de emisión del informe**: 25 de septiembre de 2024
- **Firma del perito**:

  Sergio Carretero Otero
  Perito Informático

Declaración de Tachas:

"Yo, Sergio Carretero Otero, manifiesto mi imparcialidad en la elaboración del presente informe pericial, y aseguro que no me encuentro en ninguna de las situaciones descritas en el artículo 343 de la Ley de Enjuiciamiento Civil."

Requisito de Veracidad:

"De conformidad con lo dispuesto en el artículo 335.2 de la Ley de Enjuiciamiento Civil, me comprometo a decir la verdad en la elaboración de este informe, actuando de buena fe y con imparcialidad. Reconozco las consecuencias legales del incumplimiento de mis obligaciones como experto."

Índice General:

1. Objeto del Informe:

Este informe tiene como objeto determinar los sistemas comprometidos durante el ataque de ransomware sufrido por *Finanzas S.L.* y evaluar si los datos fueron cifrados o exfiltrados, además de verificar el impacto en la privacidad de los datos de los clientes.

2. Alcance:

El análisis abarca los equipos comprometidos por el ransomware, los datos cifrados y las comunicaciones de los atacantes, con el fin de ofrecer una evaluación forense completa.

3. Antecedentes:

El 15 de septiembre de 2024, la empresa *Finanzas S.L.* reportó un ataque de ransomware que afectó varios de sus sistemas. Los atacantes exigieron un rescate en criptomonedas. La empresa solicitó este informe pericial para evaluar el daño.

4. Consideraciones Preliminares:

Se revisaron los servidores y estaciones de trabajo clave de *Finanzas S.L.*, preservando la integridad de las pruebas con herramientas como FTK Imager. Los logs de actividad de red fueron analizados para detectar tráfico relacionado con los servidores de comando y control (C&C) de los atacantes. También se evaluaron las notas de rescate encontradas en los sistemas.

5. Documentos de Referencia:

- Reglamento General de Protección de Datos (RGPD)

- Ley de Enjuiciamiento Civil
- Normativa UNE 197001:2019

6. Terminología y Abreviaturas:

- **C&C**: Command and Control
- **AES**: Advanced Encryption Standard
- **FTK Imager**: Herramienta de imagen forense

7. Desarrollo del Estudio:

Los equipos comprometidos fueron identificados, y se preservaron las evidencias digitales. Los logs de red mostraron conexiones sospechosas con el servidor 45.77.169.12, que está relacionado con la actividad del ransomware. Los archivos en el servidor Servidor01 fueron cifrados con el algoritmo AES-256.

8. Conclusiones:

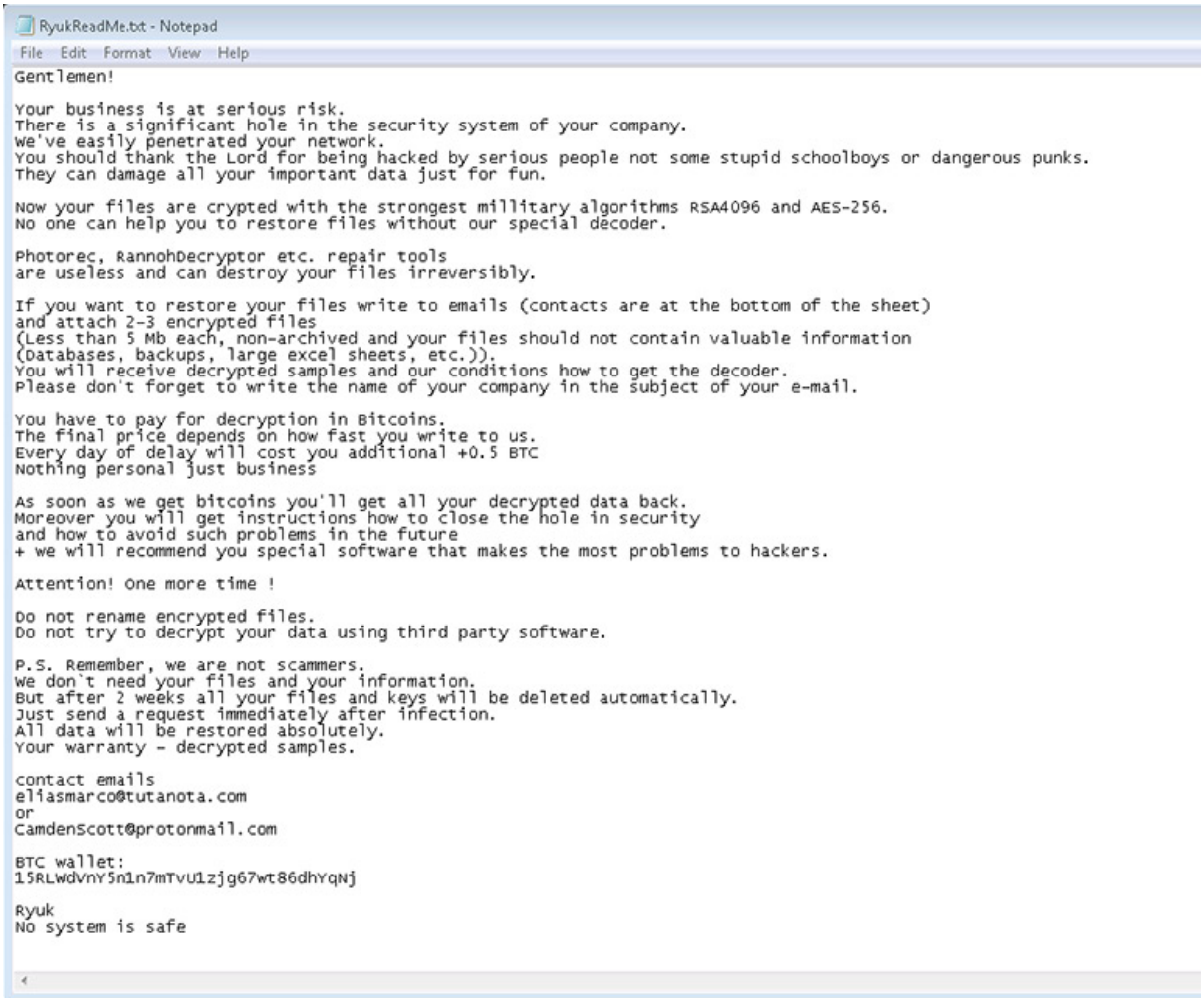
El análisis confirmó que los atacantes cifraron una porción significativa de los archivos y solicitaron un rescate. Aunque no se pudo verificar la exfiltración de datos, existe un alto riesgo de que la información confidencial haya sido comprometida.

Anejos:

- **Anexo 1**: Logs de eventos de red (pág. 6)

Time	Source IP	Destination IP	Protocol	Length	Info
14:12:10.342	192.168.10.15	45.77.169.12	HTTP	320	GET /decrypt_files.html HTTP/1.1
14:12:12.655	192.168.10.15	8.8.8.8	DNS	64	Standard query A commandserver.com
14:12:15.789	192.168.10.15	192.168.1.1	TCP	78	SYN Sent
14:12:17.456	45.77.169.12	192.168.10.15	TCP	66	SYN ACK
14:12:20.123	192.168.10.15	45.77.169.12	TCP	350	POST /upload.php HTTP/1.1
14:12:25.567	192.168.10.15	10.0.0.1	TCP	74	Client Hello

- **Anexo 2**: Capturas de pantalla del ransomware (pág. 7)



RyukReadMe.txt - Notepad

File Edit Format View Help

```
Gentlemen!

Your business is at serious risk.
There is a significant hole in the security system of your company.
We've easily penetrated your network.
You should thank the Lord for being hacked by serious people not some stupid schoolboys or dangerous punks.
They can damage all your important data just for fun.

Now your files are crypted with the strongest millitary algorithms RSA4096 and AES-256.
No one can help you to restore files without our special decoder.

Photorec, RannohDecryptor etc. repair tools
are useless and can destroy your files irreversibly.

If you want to restore your files write to emails (contacts are at the bottom of the sheet)
and attach 2-3 encrypted files
(Less than 5 Mb each, non-archived and your files should not contain valuable information
(Databases, backups, large excel sheets, etc.)).
You will receive decrypted samples and our conditions how to get the decoder.
Please don't forget to write the name of your company in the subject of your e-mail.

You have to pay for decryption in Bitcoins.
The final price depends on how fast you write to us.
Every day of delay will cost you additional +0.5 BTC
Nothing personal just business

As soon as we get bitcoins you'll get all your decrypted data back.
Moreover you will get instructions how to close the hole in security
and how to avoid such problems in the future
+ we will recommend you special software that makes the most problems to hackers.

Attention! One more time !

Do not rename encrypted files.
Do not try to decrypt your data using third party software.

P.S. Remember, we are not scammers.
We don't need your files and your information.
But after 2 weeks all your files and keys will be deleted automatically.
Just send a request immediately after infection.
All data will be restored absolutely.
Your warranty - decrypted samples.

contact emails
eliasmarco@tutanota.com
or
CamdenScott@protonmail.com

BTC wallet:
15RLWdVnY5n1n7mTvU1zjg67wt86dhYqNj

Ryuk
No system is safe
```

Referencias

de Posgrado, I. E. (s/f). *Análisis Forense: El Informe Pericial*. https://campusvirtual.iep.edu.es/recursos/biblioteca/pdf/IEP-CB-AF/clase4_pdf1.pdf

Informe pericial informático. (s/f). Indalics Peritos Informáticos. Recuperado el 25 de septiembre de 2024, de https://indalics.com/informe-pericial-informatico

Ryuk Ransomware Screenshot. (s/f). https://hyphenet.com/wp-content/uploads/2019/12/ryuk-ransomware.jpg

(S/f). Codepen.io. Recuperado el 25 de septiembre de 2024, de https://codepen.io/TheRealAlan/pen/PwbExG