Documento Complementario al Informe Pericial – Contenido no incluido

1. Actividad sospechosa en la configuración de red

Durante el análisis se identificó la presencia del archivo **rasphone.pbk** en la ruta C:\Users\informant\AppData\Roaming\Microsoft\Network\Connections\Pbk_hiddenPbk\rasphone.pbk.

Este archivo, correspondiente a configuraciones de acceso remoto (RAS o VPN), fue creado, accedido y modificado el 22 de marzo de 2015 a las 15:35:09 (CET), coincidiendo con el inicio de la presunta fuga de información.

El archivo se encuentra dentro de una carpeta oculta (**_hiddenPbk**), lo que puede interpretarse como un intento de ocultar configuraciones de red. No obstante, el archivo presenta un tamaño de 0 KB y no contiene información útil sobre posibles conexiones remotas configuradas.

Por tanto, aunque la evidencia demuestra que el usuario accedió a la configuración de conexiones remotas, aún no se puede afirmar que se haya establecido o intentado establecer una conexión VPN o RAS basándonos exclusivamente en esta evidencia.

Pero reforzando la hipótesis anterior, durante el análisis del contenido no asignado del volumen, se identificó un fragmento del archivo **NETAVPNT.INF** localizado en la ruta:

```
/System Volume Information/{9b365807-d2ef-11e4-b734-000c29ff2429}{3808876b-c176-4e48-b7ae-04046e6cc752}-slack
```

Este archivo corresponde al protocolo de transporte **Agile VPN**, utilizado por los sistemas Windows para establecer conexiones de red privadas y cifradas.

La fecha de modificación registrada es el **25 de marzo de 2015 a las 15:57:27 (CET)**, momento que coincide con otros indicios de actividad sospechosa detectados en el sistema, relacionados con transferencia y ocultamiento de información.

El hallazgo se produjo en el espacio "Slack", lo que indica que el archivo fue eliminado posteriormente, pero su contenido residual permanece en el sistema, lo cual refuerza la hipótesis de manipulación de configuraciones de red y posible uso de VPN para exfiltración de datos.

Relevancia: Estos elementos sugieren que el usuario **pudo haber preparado canales seguros de salida**, aunque no se ha confirmado conexión efectiva. No se incluyó en el informe principal por falta de datos concluyentes de conexión activa.

2. Indicios de Uso de Conexiones Remotas

Durante el análisis forense de la imagen del disco, se han detectado múltiples evidencias relacionadas con el uso o la preparación de conexiones remotas (Remote Desktop y similares) por parte del usuario "informant" en fechas coincidentes con los eventos sospechosos de exfiltración de información.

1. Presencia de Remote Desktop Connection configurado en el sistema

- **Archivo:** Windows/System32/config/DEFAULT
- **Contenido clave:** corder.exe,-100<<Remote Desktop<<Connection
- **Última modificación:** 25/03/2015 a las 16:31:05 CET
- **Interpretación:** Se refiere al recurso del sistema asociado al acceso remoto, indicando configuración o interacción reciente con esta función.

---

2. Evidencia en Logs de Seguridad (Security.evtx)

- **Términos detectados:** Microsoft-Windows-Security-Auditing, Remote Desktop Users, Builtin, 37L4247F27-25$
- **Descripción:** Se observa que el equipo tenía configurado el grupo de usuarios de escritorio remoto, vinculado al nombre 37L4247F27-25$ en el entorno WORKGROUP.
- **Interpretación:** La inclusión en el grupo de Escritorio Remoto indica que el equipo estaba configurado para permitir este tipo de conexiones. No necesariamente

implica que se haya establecido una sesión, pero sí que era viable hacerlo.

---

3. Evidencia en NTUSER.DAT (registro de usuario)

- **Keyword Preview:** "exe& REMOTE~1.LNK<<Remote Desktop<<Connection.lnk@"
- **Fecha:** 25/03/2015 a las 16:30 CET
- **Interpretación:** Existencia de accesos o accesos directos configurados por el propio usuario al cliente de Escritorio Remoto, corroborando intencionalidad de uso.

---

4. Registros en Memoria Virtual (Pagefile.sys)

- **Contenido encontrado:**
  "The Windows Installer does not permit installation from a Remote Desktop Connection."
- **Interpretación:** Confirma que existió al menos un intento de realizar acciones administrativas o de instalación durante una sesión remota, lo que suele ocurrir al usar RDP.
- **Fecha**: 25/03/2015, con horas de creación, acceso y modificación entre las 11:15:19h y las 14:05:36 CET.

---

5. Evidencias en Hibernación del Sistema (hiberfil.sys)

- **Contenido:** "Chrome Remote Desktop Viewer This plugin allows you to securely access other computers that have been shared with you."
- **Hora registrada:** 25/03/2015 a las 14:05 CET
- **Interpretación:** Sugiere que estaba instalado y potencialmente en uso el complemento de acceso remoto de Google Chrome, lo que ampliaría las vías de conexión externa al equipo.

---

6. Archivo de Configuración de Menú Inicio (desktop.ini)

- **Ruta:** ProgramData/Microsoft/Windows/Start Menu/Programs/Accessories/Desktop.ini
- **Contenido:** "Remote Desktop Connection.lnk=@%SystemRoot%\system32\mstsc.exe,-4000"
- **Hora:** 25/03/2015 a las 11:18:12 CET
- **Interpretación:** El acceso directo a RDP estaba disponible en el menú de inicio, facilitando el acceso recurrente al mismo.

---

7. Controladores y Servicios RDP en el Sistema

- **Archivo:** rdpbus.PNF
- **Contenido:** "Remote Desktop Device Redirector Bus Driver"
- **Interpretación:** Confirma que el sistema tenía habilitados los servicios y controladores necesarios para las sesiones remotas.
- **Fecha**: última modificación 25/03/2015 a las 11:18:10 CET.

---

8. Evidencias en Navegador Chrome

- **Archivo en Cache:** f_000123
- **Contenido:** "Remote Desktop"
- **Archivo DLL:** chrome_child.dll
- **Contenido:** "Remote Desktop Services is currently busy."
- **Interpretación:** El navegador disponía de extensiones o plugins relacionados con el control remoto, complementando las vías de acceso detectadas.

---

9. Ccleaner con Referencias a Remote Desktop

- **Archivo:** Ccleaner.exe
- **Contenido:** "Viewer\Recent File List [<<Remote Desktop<<]".
- **Acceso:** 25/03/2015 a las 15:58:35 CET
- **Interpretación:** Ccleaner podría haber sido utilizado para eliminar rastros, lo que encaja con un intento de ocultar la actividad remota previa.

Relevancia: El conjunto de evidencias presentadas sugiere de forma consistente que el usuario tenía configurado, accesible y en uso el servicio de Escritorio Remoto, tanto mediante las herramientas nativas de Windows como a través del complemento de Google Chrome. La presencia de accesos directos, artefactos en memoria, controladores activos y referencias en herramientas de limpieza como CCleaner indica un patrón claro de uso intencionado y posiblemente reiterado de conexiones remotas al sistema. Estos indicios adquieren especial valor pericial por su concentración en el día 25 de marzo de 2015, dentro de la ventana temporal crítica del caso, y refuerzan la hipótesis de que parte de las acciones sensibles pudieron realizarse mediante sesiones remotas o preparadas para ser gestionadas a distancia.
Aunque algunas de estas evidencias se incluyeron en el informe principal de forma resumida, este apartado expone la **extensión y profundidad** del uso de Escritorio Remoto. Su volumen excedía el espacio disponible en el cuerpo principal del informe.

3. Actividad criptográfica sospechosa (CryptoAPI – RSA Private Keys)

Se han identificado dos archivos binarios en el directorio:

```
C:\Users\informant\AppData\Microsoft\Crypto\RSA\{GUID}
```

Titulados:

```
"13243-43e3a4a9826996aba5d7727553958fbf_482809d2-6993-4f93-aeb9-f2de273cca18
"
```

creado con la fecha de **23/03/2015 05:36h CET**

y además:

"13245-932a2db58c237abd381d22df4c63a04a_482809d2-6993-4f93-aeb9-f2de273cca18" creado con la fecha de **23/03/2015 11:10h CET.**

Ambos presentan contenido característico de claves privadas asociadas a mecanismos de cifrado o autenticación, como demuestran las cadenas extraídas de los binarios anteriores mediante la herramienta cat **(cat (GNU coreutils) 8.32)**:

```
"cryptoAPI private keyf"
"Microsoft Enhanced Cryptographic Provider v1.0"
```

La generación de estas claves horas antes del inicio comprobado de comunicaciones externas y la transferencia de información por medios cifrados (Google Drive, VPN) sugiere una planificación deliberada por parte del usuario para asegurar la exfiltración de información de manera encubierta.

Este texto anteriormente mencionado identifica el proveedor criptográfico utilizado por Windows para la generación y gestión de claves RSA. Su presencia refuerza que el archivo contiene una **clave privada real generada por el sistema**, probablemente asociada a operaciones de cifrado o autenticación realizadas por el usuario **informant.**
La presencia de estos archivos **horas antes del envío de enlaces de Google Drive** y otros correos clave, sugiere que el usuario **pudo haber cifrado documentos sensibles** o establecido canales seguros de salida de información.

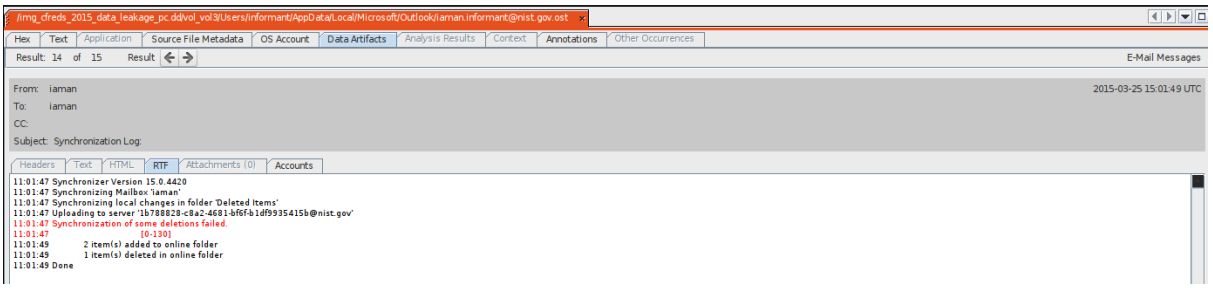
Relevancia: Apoya la hipótesis de que el usuario **pudo haber cifrado archivos sensibles** o protegido conexiones con autenticación fuerte. No se incluyó en el informe principal por no haberse podido vincular de forma directa con un canal de salida concreto (ej: VPN activa).

4. Análisis de registro de sincronización de correo electrónico

Se han proporcionado dos capturas de pantalla de un registro de sincronización de una cuenta de correo electrónico. El objetivo de este análisis es comprender el contenido de dichos registros.

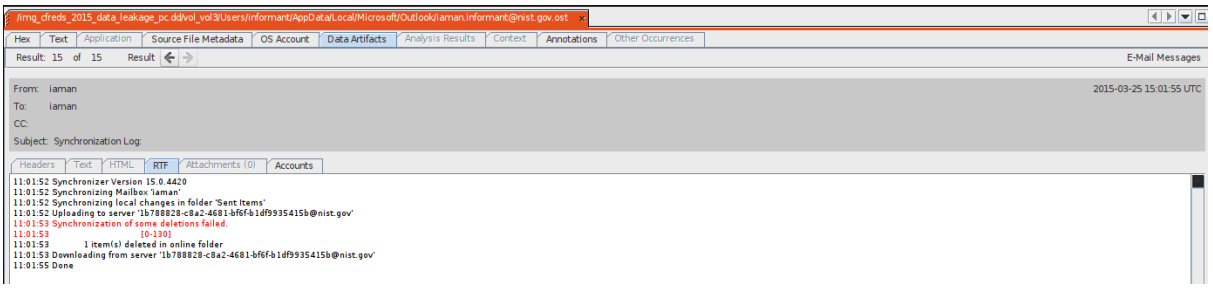
Las imágenes muestran los siguientes detalles:

1. **Captura de Autopsy nr. 1**:



- Fecha y hora: 25 de marzo de 2015, 15:01:49 UTC
- Remitente: iaman
- Asunto: Synchronization Log
- Acciones registradas:
  - Sincronización de la carpeta "Deleted Items" del buzón de "laman"
  - Carga de datos al servidor "1b788828-c8a2-4681-bf6f-b1df9935415b@nist.gov"
  - Fallo en la sincronización de algunas eliminaciones
  - Adición de 2 elementos a la carpeta en línea y eliminación de 1 elemento

2. **Captura de Autopsy nr. 2**:



- Fecha y hora: 25 de marzo de 2015, 15:01:52 UTC
- Remitente: iaman
- Asunto: Synchronization Log
- Acciones registradas:
  - Sincronización de la carpeta "Sent Items" del buzón de "laman"
  - Carga de datos al servidor "1b788828-c8a2-4681-bf6f-b1df9935415b@nist.gov"

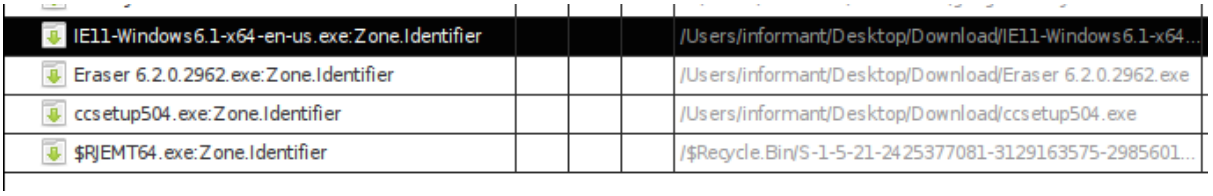
- Fallo en la sincronización de algunas eliminaciones
- Eliminación de 1 elemento de la carpeta en línea
- Descarga de datos del servidor "1b788828-c8a2-4681-bf6f-b1df9935415b@nist.gov"

Estos registros de sincronización proporcionan información sobre las actividades de gestión y sincronización de un buzón de correo electrónico, incluyendo la carga y descarga de datos, así como la adición y eliminación de elementos en las carpetas.

5. Configuración horaria del sistema:

Nombre del valor	Tipo	Valor hexadecimal	Significado
TimeZoneKeyName	REG_SZ	Eastern Standard Time	Nombre del huso horario configurado
Bias	REG_DWORD	0x0000012c (300)	Desfase base respecto a UTC (300 minutos = UTC-5)
ActiveTimeBias	REG_DWORD	0x000000f0 (240)	Desfase activo durante horario de verano (UTC-4)

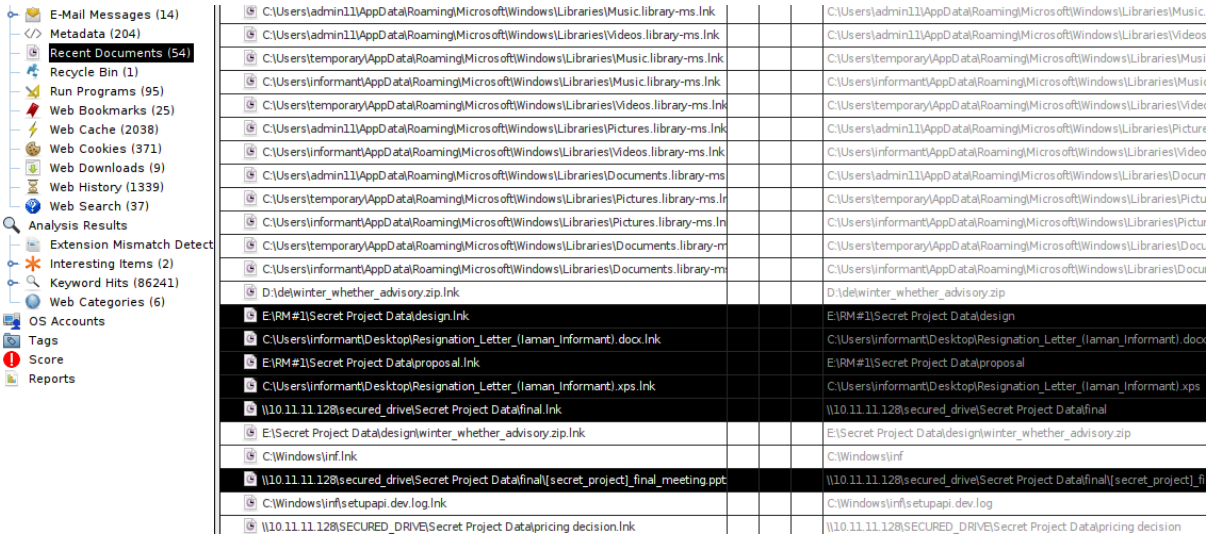
StandardBias	REG_DWORD	0x00000000 (0)	No hay ajuste adicional en horario estándar
DaylightBias	REG_DWORD	0xffffffc4 (-60)	Ajuste de horario de verano (-60 min)
DaylightStart	REG_BINARY	00 00 03 00 02 00 02 00 00 00 00 00 00 00 00 00	Primer domingo de marzo a las 02:00 h
StandardStart	REG_BINARY	00 00 0B 00 01 00 02 00 00 00 00 00 00 00 00 00	Primer domingo de noviembre a las 02:00 h
DynamicDaylightTimeDisabled	REG_DWORD	0x00000000 (0)	Horario de verano habilitado



6. Referencias a dispositivos externos, concretamente:

La nomenclatura **RM#1** sugiere que se trata de una memoria USB previamente conectada al sistema, utilizada para almacenar documentos clasificados dentro de una estructura de carpetas denominada "Secret Project Data".

```
E:\RM#1\Secret Project Data\design
```



Este hallazgo, unido al contenido de los correos interceptados refuerza la hipótesis de que el implicado empleó medios físicos externos para la exfiltración de datos.

7. Conceptos Técnicos Relacionados con el Certificado Digital Recuperado

Dentro de la evidencia, se identificaron rutas de distribución asociadas al certificado digital perteneciente a la infraestructura de autenticación y firma de NIST, que incluyen los siguientes servicios:

- **LDAP (Lightweight Directory Access Protocol):**
  Protocolo estándar para consultar directorios corporativos o gubernamentales.
  En este caso, permite consultar la validez y los detalles de certificados en tiempo real a través del servidor:
  ldap://sspdir.managed.entrust.com/...

Esto indica que el certificado se encuentra registrado y puede ser verificado contra el directorio de la entidad emisora.

- **CRL (Certificate Revocation List):**
  Lista de Revocación de Certificados, accesible en:
  http://sspweb.managed.entrust.com/CRLs/EMSSSPCA1.crl
  Permite comprobar si el certificado ha sido revocado antes de su fecha de expiración. En entornos de seguridad, los sistemas consultan esta lista para evitar el uso de credenciales comprometidas.

- **OCSP (Online Certificate Status Protocol):**
  Protocolo en tiempo real para verificar el estado de un certificado, accesible en:
  http://ocsp.managed.entrust.com/OCSP/EMSSSPCAResponder
  Es un mecanismo más ágil que la CRL, utilizado para confirmar en el momento si el certificado sigue siendo válido, sin necesidad de descargar listas completas.

La presencia de estos datos técnicos sugiere que el usuario investigado disponía de un certificado digital oficial emitido por la infraestructura gubernamental estadounidense, específicamente el Departamento de Comercio. Su utilización podría haber servido para:

- Firmar digitalmente documentos.
- Autenticarse en sistemas o servicios seguros.
- Cifrar información enviada, como los archivos detectados en la nube o las comunicaciones por correo.

La presencia de múltiples direcciones de correo institucional, en combinación con identificadores internos de Exchange y certificados emitidos por una Autoridad de Certificación del gobierno de EE.UU., indica que la identidad de **Galen Koepke** estuvo activamente involucrada en comunicaciones institucionales electrónicas.