INFORME FORENSE

Investigación del robo de información al centro universitario ACME University

María Andrea Ugarte Valencia y Marcos Villar Avión

Contenido

INFORMACIÓN DECLARATIVA

Declaración de Abstención y Tachas

Dña. María Andrea Ugarte Valencia y D. Marcos Villar Avión, con carnets profesionales Nº 274 y Nº 297 de la Asociación Nacional de Tasadores y Peritos Judiciales Informáticos (ANTPJI), miembros de la Asociación Profesional de Peritos Judiciales Aparejadores y Arquitectos Técnicos de Galicia Colegiado Nº 123 con Titulación Académica-Profesional de Experto en Ciberseguridad y Peritaje Informático Judicial, por la ANTPJI desde el año 2019, con Título de Máster en Ciberseguridad por la Universidad de Coruña e Ingeniería Informática con más de 4 años de experiencia en el sector de las tecnologías de la información y la seguridad informática, colaborador con varias empresas informáticas y consultoras de formación. Han sido designados para realizar el Informe pericial forense correspondiente a la investigación, informe sobre el robo de información de una materia por parte de un alumno de la Universidad ACME University.

Los peritos declaran:

Los firmantes del presente informe o dictamen, en lo concerniente a los temas y alcance tratados, así como las partes y terceros involucrados o afectadas por el mismo y conocidos hasta este momento, en base a los expresados en el art. 105 de la Ley de Enjuiciamiento Civil y el art. 219 De la Ley Orgánica del Poder Judicial,

DECLARAN,

a priori y en la fecha de elaboración del informe, desconocer causa o motivo alguno por la que deba de abstenerse de la realización del presente informe. Y en base al art. 343 de la Ley de Enjuiciamiento Civil,

DECLARAN,

a priori y en la fecha de elaboración del informe, desconocer causa o motivo alguno por el cual el perito pueda ser tachado por Tercero interesado o Parte en un proceso judicial derivado de las acciones posteriores llevadas a cabo con el presente informe o dictamen judicial.

Declaración o Juramento de Promesa

Los peritos firmantes del presente informe o dictamen, en lo concerniente a los temas y el alcance tratados en el mismo, y en base a lo expresado en art. 335 de la Ley de Enjuiciamiento Civil,

DECLARAN,

Decir la verdad y haber actuado con la mayor objetividad e imparcialidad posible tomando en consideración tanto lo que pueda favorecer como lo que sea susceptible de causar perjuicio a tercero o parte solicitante del informe y conoce las responsabilidades civiles, penales, disciplinarias y asociativas que comporta la aceptación de la elaboración de un informe o dictamen judicial. Asimismo, bajo su única responsabilidad,

DECLARAN,

que lo expresado y reflejado en el presente informe o dictamen pericial está basado en los hechos, información y circunstancias que se han podido constatar, por medio de los conocimientos propios y la experiencia adquirida a lo largo de la trayectoria profesional, quedando las conclusiones siempre sujetas y abiertas a la consideración de nuevas informaciones, exámenes y aportaciones o de un mejor criterio u opinión que pudiese ser aportado.

Declaración de imparcialidad

Los peritos MARÍA ANDREA UGARTE VALENCIA y MARCOS VILLAR AVIÓN declaran no tener intereses el resultado de la investigación. Asimismo, en cumplimiento del artículo 335.2. de la LEC, los peritos firmantes, responsables del contenido del dictamen, manifiesta, bajo juramento, que ha actuado y, en su caso, actuará, con la mayor objetividad posible, siendo conocedor de las sanciones penales en las que podría incurrir si incumpliese su deber como peritos.

Declaración de Confidencialidad

Los peritos MARÍA ANDREA UGARTE VALENCIA y MARCOS VILLAR AVIÓN, con carnet profesional Nº 276 y Nº 297 de la Asociación Nacional de Tasadores y Peritos Judiciales Informáticos (ANTPJI), se comprometen de manera expresa y asumen que el compromiso es mutuo por parte de los peticionarios del Informe/Dictamen, tanto durante la vigencia del encargo, como después de su extinción, sin límite de tiempo, a no difundir, transmitir o revelar a terceras personas cualquier información proporcionada por el peticionario o por el objeto del Informe/Dictamen

a la que tenga acceso como consecuencia de la actividad laboral, ni a utilizar tal información en interés propio o de terceros vinculados con el mismo.

La prohibición establecida en el párrafo anterior se extiende a la reproducción, en cualquier soporte, de la información del peticionario, cliente o asunto a la que tenga acceso y así como información relativa a clientes, procedimientos y sistemas de organización, programas informáticos o cualquier otro tipo de información interna, salvo que tal información sea estrictamente necesaria publicitarla para el desarrollo del contenido inherente de su labor.

Asimismo, los peritos MARÍA ANDREA UGARTE VALENCIA y MARCOS VILLAR AVIÓN quedan exentos de dicho compromiso cuando la información sea requerida en los supuestos legalmente contemplados por la ley y en aquellos casos en los que se esté colaborando con los Cuerpos de Seguridad o con los Órganos de Justicia, o implique riesgos para la integridad de las personas o se evidencie clara e inequívocamente la comisión de delito, en cuyo caso se informará a las Autoridades competentes.

Uso no Autorizado

Queda expresamente prohibido el uso, copia y/o divulgación de la información parcial o total redactada y liberada en este informe, sin la autorización expresa del autor del mismo y firma original del informe, en tanto en cuanto no se haya completado la relación y los compromisos contractuales del encargo, entre ellos, el devengo total de las minutas, gastos y los honorarios estipulados para la realización de dicho encargo, incluidos los impuestos aplicables correspondientes.

Manifiesto

En el momento de emitir este informe se considera que es completo y adecuado. Este informe únicamente se actualizará a solicitud de los tribunales competentes, por lo que no se asume ninguna responsabilidad sobre aspectos ocurridos o conocidos con posterioridad a la emisión del mismo y que pudieran modificar las conclusiones del perito.

Asimismo, los peritos MARÍA ANDREA UGARTE VALENCIA y MARCOS VILLAR AVIÓN declaran que el informe se presenta manuscrito, firmado y que, de encontrarse epígrafes manuscritos, no serán responsabilidad de los peritos.

INFORMACIÓN DESCRIPTIVA

De un lado, el cliente José Manuel Vázquez Naya, en representación de la universidad ACME University requiere los servicios de los peritos María Andrea Ugarte Valencia y Marcos Villar Avión para que emitan un contra Informe/Dictamen pericial con la finalidad de investigar y realizar un informe pericial acerca de una investigación por robo de información a la universidad.

ANTECEDENTES DEL ASUNTO

Se establece que un estudiante de la ACME University ha sido objeto de acusaciones por el presunto robo de información relacionada con una materia específica. Se ha alegado que el individuo logró acceder a la red de la universidad mediante una conexión VPN y comprometió uno de sus sistemas. Como parte de la investigación en curso, se procedió a la incautación de los dispositivos del estudiante, incluyendo su equipo personal, del cual se extrajo un volcado de memoria, así como se realizó un clonado de su disco duro. Además, se llevó a cabo el clonado de un pendrive en posesión del individuo con fines forenses.

ALCANCE

El alcance ha sido definido y pactado con la universidad ACME University bajo el amparo y marco legal de las leyes actuales, a día 10 de Mayo de 2024, procediendo a coordinar el acto de investigación hoy día viernes 10 de Mayo de 2024 a las 17:00 horas hasta el día 13 de mayo de 2024.

El análisis se centrará en la investigación del robo de la información de la materia buscando en los datos entregados.

CONSIDERACIONES

- Consideraciones limitativas y/o restrictivas
- Cualquier dato o actividad que no esté en el alcance de esta pericial queda excluida de su análisis, auditoría o peritaje.

GARANTÍA DE LA CADENA DE CUSTODIA

Acordado el alcance de la pericial, el día y la hora a realizar y e informados los agentes implicados se comunica que todo el proceso de la actuación del perito informático se realizara siempre con la obtención del Hash de cada archivo para las investigaciones resultantes.

GEOLOCALIZACIÓN

Ubicación física de la intervención

La intervención se realiza en la dirección de las oficinas de MMF S.L. con dirección en, Campus de Elviña s/n 15008, (A Coruña). Dicha ubicación tiene coordenadas de GPS (43° 19' 58.8'' N 8° 24' 33.948'' W)

ACTUACIONES

La actuación, se realiza siguiendo los protocolos de:

- Norma UNE_197001:2011 Criterios generales para la elaboración de informes y dictámenes periciales informáticos y telemáticos.
- UNE- EN ISO 9000. Sistemas de Gestión de calidad. Fundamentos y vocabulario (ISO 9000:2005)
- UNE 50132. Documentación. Numeración de las divisiones y subdivisiones en los documentos escritos.
- Código Deontológico de ANTPJI y Asociación Profesional de Peritos Judiciales Aparejadores y Arquitectos Técnicos de Galicia

Tanto en protocolo de investigación, volatilidad de las evidencias electrónicas (digitales y telemáticas), análisis de datos, procedimientos forenses, deontología y ética, así como en el proceso de preservación de datos y la cadena de custodia, y todas las evidencias tengan validez legal, se harán siempre obteniendo el hash y describiendo paso a paso, de modo que las acciones puedan ser reproducidas por cualquier perito.

Se utilizarán copias idénticas de la evidencia gracias a las clonaciones de datos o copias exactas e inequívocas, de las mismas se obtendrá un HASH, y quedarían a disposición del Perito, para realizar los estudios pertinentes, que aclaren, o formen la base argumental para un dictamen final. El “hash criptográfico”, es un cálculo matemático cuyo resultado es una combinación de números y letras con la peculiaridad que cualquier cambio en la información, por pequeño que sea, altera totalmente su “hash”, siendo imposible encontrar otra información que tenga como

resultado el mismo “hash”. Una vez establecida la cadena de custodia, el perito informático comienza el Análisis Forense.

INVESTIGACIÓN

El 22 de marzo de 2024, se recibió una serie de archivos relacionados con el incidente bajo investigación. Estos archivos incluyen un volcado de memoria denominado "memory.raw" con el hash SHA-256 BDE0C34E79A01BC5298D317D6DC7F440EBC968CF9920CF66111AD348857C18B5, una imagen de disco clonada llamada "disk.img" con el hash SHA-256 F7E5BA4BAF5E65FBBA58B13639A044440648F4C0CD4C86E948497C6C5CB3A9C0, y una imagen clonada de una unidad flash llamada "pendrive.img" con el hash SHA-256 9B1CD9FA66EA1555F587242D80B377EF17947224FD09E1B8D54B140E45110A1C. Estos archivos proporcionaron la base para llevar a cabo una investigación sobre el supuesto robo de información.

Se utilizó una combinación de herramientas forenses, incluyendo Volatility y Autopsy, para analizar los archivos recibidos. Según los resultados obtenidos, se determinó que el sistema operativo utilizado durante el incidente fue Windows 7 con Service Pack 1, con una arquitectura de 64 bits.

Se llevó a cabo una investigación para recuperar información sobre las actividades, archivos y demás información relacionada con el incidente. Entre los hallazgos significativos se encuentran:

- La se identificación de varios usuarios y contraseñas asociadas en el sistema comprometido. Estos incluyen:

  - Usuario "Administrador"

  - Usuario "Invitado"

  - Usuario "pentester" con contraseña "Pw:lnQL04,"

  - Usuario "kiddie" con contraseña "AnW9.s2NmwL!"

  - Usuario "anonymous" con contraseña "Ñ4p4:)"

- La aparición del nombre "Judith Santamaria Morales" en el sistema, obtenido de los metadatos de una fotografía encontrada en la ruta /img_disk.img/vol_vol3/Users/kiddie/Documents/linkedin.png de la imagen de disco. Esta fotografía tiene el hash SHA-256 401b0548ceb1ef2c35fcd6b9532adfc9f24850ac0fe9f91badf567ba0040e751.

- El descubrimiento de una fotografía tomada desde el aeropuerto de Coruña, ubicada en /img_disk.img/vol_vol3/Users/kiddie/Pictures/IMG-3405893082345.jpg en la imagen

de disco. Esta fotografía tiene el hash SHA-256 6a6adbe968e7f7dbab446354d21c4e6bbb4591ac05b59bf3d82c28416e2c1c23.

- El archivo "Examen.pdf", que contiene el examen de la asignatura "Investigaciones Forenses Avanzadas", junto con el archivo "Estudiantes.xlsx", que contiene un listado de 19 estudiantes de la asignatura. Estos archivos se encontraron en el volcado de memoria “memory.raw” en un archivo cifrado denominado “archivos-robados.7z”, en la dirección de memoria 0x000000011fafe9a0 y con hash 8DDFAD22E443A965335024E54EA26F938BB16794173C6863B28B97D7D3E942EC.

- La identificación de los individuos "Faustino Mateo Reina" y "Juan Antonio Cuadrado Domingo" asociados con los archivos "Examen.pdf" y "Estudiantes.xlsx", respectivamente. El nombre de “Faustino Mateo Reina” fue hallado en las propiedades del archivo “Examen.pdf” mientras que, el nombre de “Juan Antonio Cuadrado Domingo” se encontró en los metadatos del archivo “Estudiantes.xlsx”.

- Las direcciones IP 172.20.20.2 y 172.20.20.101, pertenecientes a la misma red. La IP 172.20.20.101 se trata de una dirección IP perteneciente al equipo encautado y la IP 172.20.20.2 es una dirección IP con la que el usuario del equipo ha interactuado. Esta información se ha obtenido a partir de la opción netscans de Volatility.

- Que el robo de la información comprometida ha sido efectuado mediante el aprovechamiento de la vulnerabilidad del servicio FTP del equipo víctima de la universidad ACME University.

- Además, se identificaron actividades sospechosas en el equipo comprometido, incluyendo el uso de herramientas como Nmap. También se encontró que el equipo contenía las siguientes herramientas instaladas: BurpSuite y Npcap. También se identificó la instalación de aplicaciones de comunicación como Zoom, Telegram y Windows Mail.

- Una billetera digital de la criptomoneda Monero en la ubicación /img_disk.img/vol_vol3/Windows/AppCompat/Monero GUI Wallet/monero-wallet-gui.exe.

Para recopilar la información relacionada con los usuarios y contraseñas, se han identificado las ubicaciones de los archivos correspondientes a diferentes partes del registro para localizar la tabla SAM y correlacionarla con el archivo SYSTEM. Las contraseñas del usuario “pentester” y “kiddie” se han conseguido con la herramienta Mimikatz para recuperar contraseñas almacenadas en sistemas Windows. En el caso de la contraseña del usuario "anonymous", fue necesario emplear técnicas de craqueo para descifrar su hash.

DICTAMEN Y CONCLUSIONES

Los Peritos Informáticos firmantes de este Dictamen Pericial. DECLARAN,

Las conclusiones expresadas son el resultado de la aplicación de los conocimientos y experiencias adquiridas por los Peritos Informáticos en su desempeño profesional y dentro de su leal saber y entender, quedando siempre abierto a considerar nuevas aportaciones de información, evidencias o mejor opinión.

CONCLUSIONES

A juicio de los peritos y, siempre a su juicio y dadas las evidencias electrónicas (digitales y telemáticas) de las pruebas analizados, afirma:

- Que el responsable del robo de la información a la universidad ACME University se trata de una persona que haya tenido contacto previo con el equipo substraído.

- Que los hechos han tenido lugar bajo el uso del usuario “kiddie”.

Por todo lo expuesto en este documento, resultado de las diversas investigaciones y peritajes realizados, los peritos informáticos pueden certificar que se ha encontrado información con relación a todas las solicitudes del cliente.

Para constancia a los efectos oportunos, se emite el presente informe en la ciudad de A Coruña, 10 de Mayo de 2024.

Dña. María Andrea Ugarte Valencia

Carnet Profesional Nº 276 Colegiado Nº 123

D. Marcos Villar Avión

Carnet Profesional Nº 297 Colegiado Nº 123