## Incident handler's journal

**Date:** 2024-08-08  
**Entry:** 1  
**Description:** This incident involves a ransomware attack on a healthcare clinic in the U.S., triggered by a phishing email containing a malicious attachment. The ransomware encrypted critical files and left a ransom note.  
**The 5 W's:**

* **Who caused the incident?** An organized group of unethical hackers targeting healthcare organizations.
* **What happened?** Ransomware encrypted essential files at the clinic and demanded payment for decryption.
* **When did the incident occur?** Tuesday at 9:00 a.m.
* **Where did the incident happen?** At a small healthcare clinic in the United States.
* **Why did the incident happen?** Due to a malicious attachment from a phishing email downloaded by clinic employees.  
  **Tools Used:**
* No specific tools were utilized in this entry as it focused on the incident documentation.  
  **Reflections/Notes:**
* This incident highlights the critical need for robust security training to mitigate phishing threats.
* Implementing effective email filtering solutions can prevent similar attacks.
* A thorough evaluation of the clinic's incident response procedures is essential for improving future responses.
* Continuous monitoring and updating of security measures are necessary to address evolving threats.

**Date:** 2024-08-09  
**Entry:** 2  
**Description:** While investigating a suspicious file hash, it was found to be associated with known malware. The file was collected and analyzed to determine its impact and origin.  
**The 5 W's:**

* **Who caused the incident?** The malware was traced back to a known threat actor group.
* **What happened?** The file was identified as malware that could compromise system security.
* **When did the incident occur?** The suspicious file was detected on August 9, 2024.
* **Where did the incident happen?** On a workstation within the corporate network.
* **Why did the incident happen?** The file was downloaded from a malicious email attachment.  
  **Tools Used:**
* **Hash Analysis Tool:** Used to determine the nature of the file and compare it against known malware databases.
* **Antivirus Software:** Scanned the file for malicious behavior and confirmed its threat level.  
  **Reflections/Notes:**
* It's important to regularly update antivirus definitions to catch new threats.
* Ensuring employees are aware of the dangers of unsolicited attachments can reduce risk.
* Implementing automated tools for file analysis can speed up the incident response process.
* Continuous improvement in threat detection capabilities is crucial.

**Date:** 2024-08-10  
**Entry:** 3  
**Description:** During the analysis of Suricata rules, a custom rule was created to detect unauthorized HTTP methods. The rule was designed to monitor traffic for specific patterns indicating potential threats.  
**The 5 W's:**

* **Who caused the incident?** Not applicable; the focus was on creating a preventive rule.
* **What happened?** A custom Suricata rule was implemented to enhance traffic monitoring.
* **When did the incident occur?** Rule creation occurred on August 10, 2024.
* **Where did the incident happen?** On the network monitoring system.
* **Why did the incident happen?** To improve detection of suspicious HTTP traffic patterns.  
  **Tools Used:**
* **Suricata:** A network intrusion detection system used to create and deploy custom rules.
* **Rule Editor:** Used to configure the rule syntax and parameters for HTTP method detection.  
  **Reflections/Notes:**
* Regular updates to Suricata rules are necessary to stay ahead of new threats.
* Proper testing of rules ensures they do not generate false positives.
* The effectiveness of network monitoring tools can significantly improve incident response times.
* Ongoing training on tool usage can enhance overall security posture.

**Date:** 2024-08-11  
**Entry:** 4  
**Description:** Analyzing network traffic with Wireshark revealed unusual patterns indicative of a potential data exfiltration attempt. Detailed inspection of the packets was carried out to confirm the threat.  
**The 5 W's:**

* **Who caused the incident?** Potentially an insider threat or external attacker.
* **What happened?** Unusual network traffic patterns suggested data exfiltration.
* **When did the incident occur?** Analysis was conducted on August 11, 2024.
* **Where did the incident happen?** Within the organization's network.
* **Why did the incident happen?** Suspicious behavior was detected in the network traffic.  
  **Tools Used:**
* **Wireshark:** Utilized to capture and analyze network packets for abnormal patterns.
* **Network Analyzer:** Helped in identifying specific traffic anomalies and potential data leaks.  
  **Reflections/Notes:**
* Continuous network monitoring is crucial for detecting and mitigating data exfiltration threats.
* Regular analysis of network traffic can help identify early signs of compromise.
* Ensuring proper network segmentation can reduce the impact of a potential breach.
* Training staff on recognizing and responding to anomalies can enhance security measures.

## Diario de Gestión de Incidentes (spanish)

**Fecha:** 2024-08-08  
**Entrada:** 1  
**Descripción:** Este incidente involucra un ataque de ransomware a una clínica de atención médica en EE.UU., desencadenado por un correo electrónico de phishing que contenía un archivo malicioso. El ransomware cifró archivos críticos y dejó una nota de rescate.  
**Las 5 W:**

* **¿Quién causó el incidente?** Un grupo organizado de hackers poco éticos que se especializa en atacar organizaciones en los sectores de salud y transporte.
* **¿Qué ocurrió?** El ransomware cifró archivos importantes en la clínica y exigió un pago para proporcionar la clave de descifrado.
* **¿Cuándo ocurrió el incidente?** El incidente ocurrió el martes a las 9:00 a.m.
* **¿Dónde ocurrió el incidente?** En una clínica de atención médica en los Estados Unidos.
* **¿Por qué ocurrió el incidente?** El ataque fue provocado por la descarga de un archivo malicioso adjunto a un correo electrónico de phishing enviado a los empleados de la clínica.  
  **Herramientas Utilizadas:**
* No se utilizaron herramientas específicas en esta entrada ya que se enfocó en la documentación del incidente.  
  **Reflexiones/Notas:**
* Este incidente resalta la necesidad crítica de mejorar la capacitación en seguridad para mitigar amenazas de phishing.
* Implementar soluciones efectivas de filtrado de correos electrónicos puede prevenir ataques similares.
* Es esencial evaluar los procedimientos de respuesta a incidentes de la clínica para mejorar futuras respuestas.
* La monitorización continua y la actualización de las medidas de seguridad son necesarias para enfrentar amenazas en evolución.

**Fecha:** 2024-08-09  
**Entrada:** 2  
**Descripción:** Durante la investigación de un hash de archivo sospechoso, se descubrió que estaba asociado con malware conocido. El archivo fue recopilado y analizado para determinar su impacto y origen.  
**Las 5 W:**

* **¿Quién causó el incidente?** El malware se rastreó hasta un grupo de actores de amenazas conocido.
* **¿Qué ocurrió?** El archivo se identificó como malware que podría comprometer la seguridad del sistema.
* **¿Cuándo ocurrió el incidente?** El archivo sospechoso fue detectado el 9 de agosto de 2024.
* **¿Dónde ocurrió el incidente?** En una estación de trabajo dentro de la red corporativa.
* **¿Por qué ocurrió el incidente?** El archivo fue descargado a partir de un archivo adjunto en un correo electrónico malicioso.  
  **Herramientas Utilizadas:**
* **Herramienta de Análisis de Hash:** Utilizada para determinar la naturaleza del archivo y compararlo con bases de datos de malware conocidas.
* **Software Antivirus:** Escaneó el archivo en busca de comportamientos maliciosos y confirmó su nivel de amenaza.  
  **Reflexiones/Notas:**
* Es importante actualizar regularmente las definiciones de antivirus para capturar nuevas amenazas.
* Asegurar que los empleados conozcan los peligros de los archivos adjuntos no solicitados puede reducir el riesgo.
* Implementar herramientas automatizadas para el análisis de archivos puede acelerar el proceso de respuesta a incidentes.
* La mejora continua en las capacidades de detección de amenazas es crucial.

**Fecha:** 2024-08-10  
**Entrada:** 3  
**Descripción:** Durante el análisis de reglas en Suricata, se creó una regla personalizada para detectar métodos HTTP no autorizados. La regla se diseñó para monitorear el tráfico en busca de patrones específicos que indiquen posibles amenazas.  
**Las 5 W:**

* **¿Quién causó el incidente?** No aplicable; el enfoque fue en la creación de una regla preventiva.
* **¿Qué ocurrió?** Se implementó una regla personalizada en Suricata para mejorar la monitorización del tráfico.
* **¿Cuándo ocurrió el incidente?** La creación de la regla se realizó el 10 de agosto de 2024.
* **¿Dónde ocurrió el incidente?** En el sistema de monitoreo de red.
* **¿Por qué ocurrió el incidente?** Para mejorar la detección de patrones de tráfico HTTP sospechosos.  
  **Herramientas Utilizadas:**
* **Suricata:** Un sistema de detección de intrusiones en la red utilizado para crear y desplegar reglas personalizadas.
* **Editor de Reglas:** Utilizado para configurar la sintaxis y los parámetros de la regla para la detección de métodos HTTP.  
  **Reflexiones/Notas:**
* Las actualizaciones regulares de las reglas de Suricata son necesarias para mantenerse al día con nuevas amenazas.
* La prueba adecuada de las reglas garantiza que no generen falsos positivos.
* La eficacia de las herramientas de monitoreo de red puede mejorar significativamente los tiempos de respuesta a incidentes.
* La capacitación continua en el uso de herramientas puede mejorar la postura de seguridad general.

**Fecha:** 2024-08-11  
**Entrada:** 4  
**Descripción:** Al analizar el tráfico de red con Wireshark, se revelaron patrones inusuales indicativos de un intento potencial de exfiltración de datos. Se realizó una inspección detallada de los paquetes para confirmar la amenaza.  
**Las 5 W:**

* **¿Quién causó el incidente?** Posiblemente una amenaza interna o un atacante externo.
* **¿Qué ocurrió?** Los patrones de tráfico de red inusuales sugirieron una posible exfiltración de datos.
* **¿Cuándo ocurrió el incidente?** El análisis se realizó el 11 de agosto de 2024.
* **¿Dónde ocurrió el incidente?** Dentro de la red de la organización.
* **¿Por qué ocurrió el incidente?** Se detectaron comportamientos sospechosos en el tráfico de red.  
  **Herramientas Utilizadas:**
* **Wireshark:** Utilizado para capturar y analizar paquetes de red en busca de patrones anómalos.
* **Analizador de Red:** Ayudó a identificar anomalías específicas en el tráfico y posibles fugas de datos.  
  **Reflexiones/Notas:**
* La monitorización continua de la red es crucial para detectar y mitigar amenazas de exfiltración de datos.
* El análisis regular del tráfico de red puede ayudar a identificar señales tempranas de compromiso.
* Asegurar una segmentación adecuada de la red puede reducir el impacto de una posible brecha.
* La capacitación del personal en la identificación y respuesta a anomalías puede mejorar las medidas de seguridad.