| Nro. Alerta: | AL-2025-029 | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR<br>**ALERTAS DE SEGURIDAD** | ecucert<br>V 1.1 |
|---|---|---|---|
| TLP: | TLP:CLEAR | | |
| Fecha: | 9-jul-2025 | Malware Tedy.7918 | Pág.: **1** of **4** |

## I. DATOS GENERALES:

**Clase de alerta:** Informativo
**Tipo de Incidente:** Malware
**Nivel de riesgo:** Alta

## II. ALERTA

***Figura 1.-*** Malware Tedy.7918- figura referencial

Usuarios en el foro de la comunidad de FORTINET reportan la amenaza W32/Tedy.7918!tr en archivo ejecutable de actualización de Adobe Acrobat Reader (armsvc.exe).

## III. INTRODUCCIÓN

El malware Tedy.7918 (también identificado como Trojan: Win32/Tedy o Gen.Variant.Tedy), aunque no está ampliamente catalogado en las bases del Sitio Web de VirusTotal (https://www.virustotal.com/gui/home/upload) según reporte de más usuarios, múltiples EPP (Plataforma de Protección de Endpoint) lo han detectado en tiempo de ejecución con comportamiento sospechoso. La actividad sugiere un posible ataque a la cadena de suministro.

El presente informe documenta un posible incidente de seguridad identificado en varios entornos organizacionales, en el cual el archivo asociado al proceso de actualización de Adobe Reader, armsvc.exe estaría ejecutando código malicioso detectado como

Win32/Tedy.7918. Este troyano pertenece a la familia de malware que actúa como vector de ejecución remota, modificador de políticas de seguridad y canal de descarga de payloads adicionales.

## IV. VECTOR DE ATAQUE

El vector de ataque se presenta bajo la modalidad de suplantación o compromiso de un proceso legítimo, específicamente el servicio de actualización automática de Adobe Acrobat Reader. En este caso, el archivo armsvc.exe es ejecutado como parte de un flujo aparentemente normal de actualización, pero descarga o contiene un componente malicioso.

Algunos motores antivirus han detectado el comportamiento malicioso únicamente en tiempo de ejecución, lo que indica posibles técnicas de evasión o empaquetado.

## V. IMPACTO

- Sistemas Windows.
- Ejecución remota de código malicioso, con persistencia en el sistema.
- Alteración de políticas de seguridad locales, incluyendo desactivación o exclusión en Windows Defender.
- Posible comunicación con C2 (Command and Control) para descarga de payloads adicionales.
- Riesgo alto de escalamiento lateral y exfiltración, especialmente en redes no segmentadas.
- Compromiso de la cadena de suministro a través de software legítimo ampliamente utilizado.

## VI. INDICADORES DE COMPROMISO

| Hash Detectado |
|---|
| **MD5:** 798cd6d62ca995eb320059595efd0b03<br>8fb10da817e73f639d2e905c8b6b43f0 |
| **SHA256:** E730922F614E4DFFE70D229EC118CD3052A31E9CA4DAB274A1A15DF1CBFA5674<br>1942A8CC615E3CDCB06A336AA9F88358005D320F5FD9DF31264BACBCAEB9267 |

***Tabla 1.***-Hash - Malware Tedy.7918

| Nombre del malware en firmas AV: |
|---|
| W32/Tedy.7918 |
| Trojan Win32/Tedy |
| Gen.Variant.Tedy.* |

***Tabla 2.***- Nombres Identificativos - Malware Tedy.7918

| **Proceso sospechoso involucrado:** |
|---|
| C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe (posiblemente reemplazado o suplantado) |

***Tabla 3.-*** Proceso sospechoso - Malware Tedy.7918

| **Comportamientos observados:** |
|---|
| Inyección de comandos PowerShell para exclusión de antivirus |
| Conexiones salientes HTTP(s) no autorizadas |
| Persistencia en el sistema a través de AppData o Startup. |

***Tabla 4.-*** Tipos de comportamientos - Malware Tedy.7918

## VII. RECOMENDACIONES:

- Bloquear temporalmente las actualizaciones automáticas de Adobe Acrobat Reader (armsvc.exe) en endpoints hasta verificar integridad del archivo.
- Agregar el hash detectado a listas negras en EPP/EDR y Firewalls.
- Subir el archivo sospechoso a sandbox (Hybrid Analysis, Any.run) para análisis de comportamiento.
- Revisar logs de red y procesos para identificar conexiones sospechosas o ejecución no autorizada.
- Implementar monitoreo activo de procesos firmados pero ejecutados fuera de su ubicación esperada.
- Comunicar el hallazgo al proveedor (Adobe) y compartir IoCs con el CERT nacional o CSIRT sectorial.
- Al tratarse de una amenaza 0-day se recomienda seguir las actualizaciones del caso.

## VIII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

## IX. REFERENCIAS:

**FORTINET COMMUNITY (2025).** Adobe W32 Tedy.7918 tr found in armsvc.exe. https://community.fortinet.com/t5/Support-Forum/Adobe-W32-Tedy-7918-tr-found-in-armsvc-exe/td-p/400176

**TREND MICRO (2023). TROJAN.WIN64.TEDY.B.** https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/trojan.win64.tedy.b

**MICROSOFT SECURITY INTELLIGENCE (2023).** Trojan:Win32/Tedy!MTB. https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia description?Name=Trojan:Win32/Tedy!MTB

**MICROSOFT SECURITY INTELLIGENCE (2023).** Trojan:Win32/Tedy. https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia description?Name=Trojan:Win32/Tedy

**HYBRID ANALYSIS (2025).** Overview of sample e730922f614e4dffe70d229ec118cd3052a31e9ca4dab274a1a15df1cbfa5674. https://hybrid-analysis.com/sample/e730922f614e4dffe70d229ec118cd3052a31e9ca4dab274a1a15df1cbfa5674

**VIRUSTOTAL (2025).** VirusTotal – Threat analysis platform. https://www.virustotal.com/gui/home/search

Deluge Forum (2025). Foro técnico – Discusión sobre W32/Tedy detections. https://forum.deluge-torrent.org/viewtopic.php?t=57055