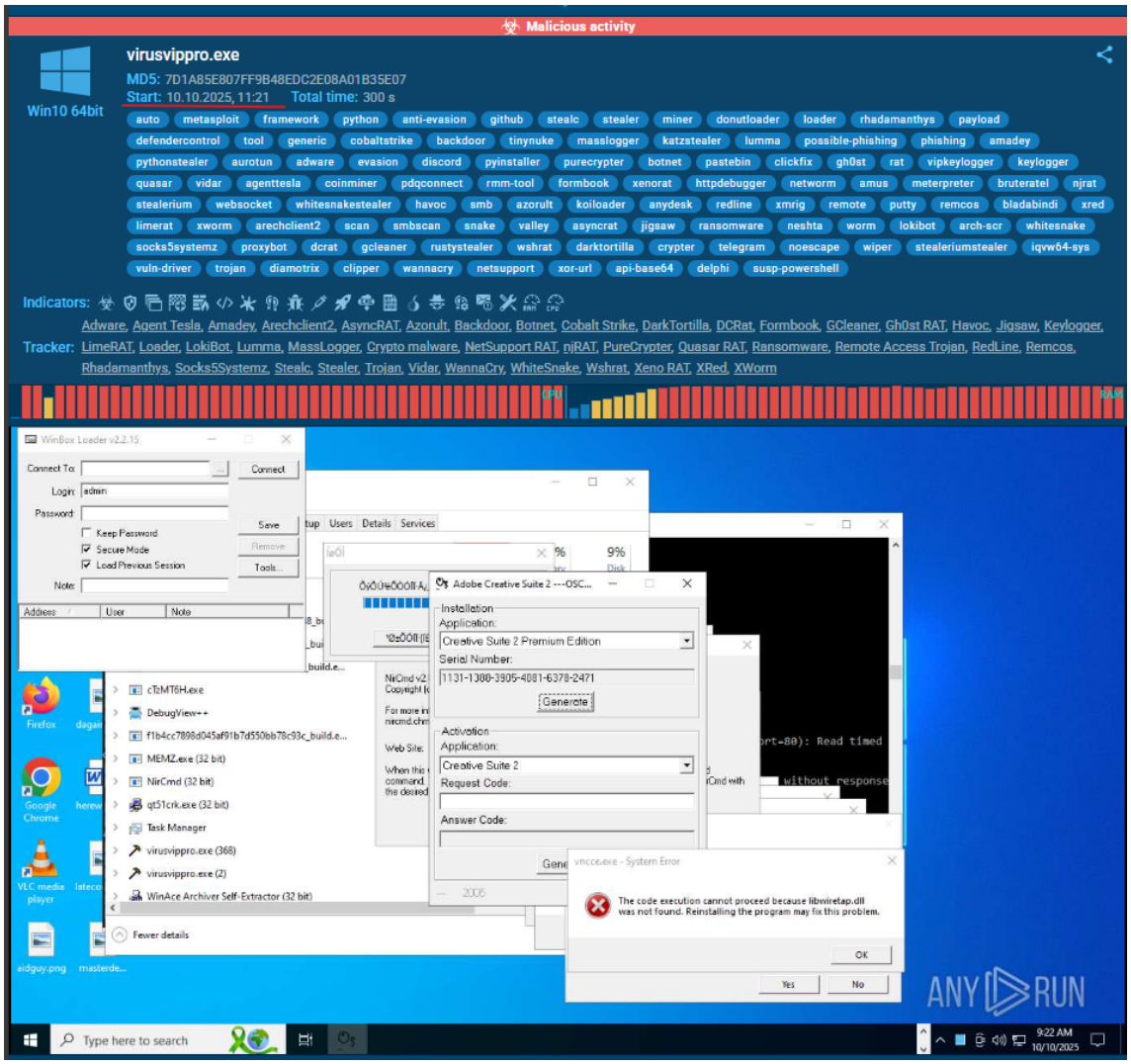
Daniel Pérez y Sergio Pernas

Inteligencia y recopilación de un Malware

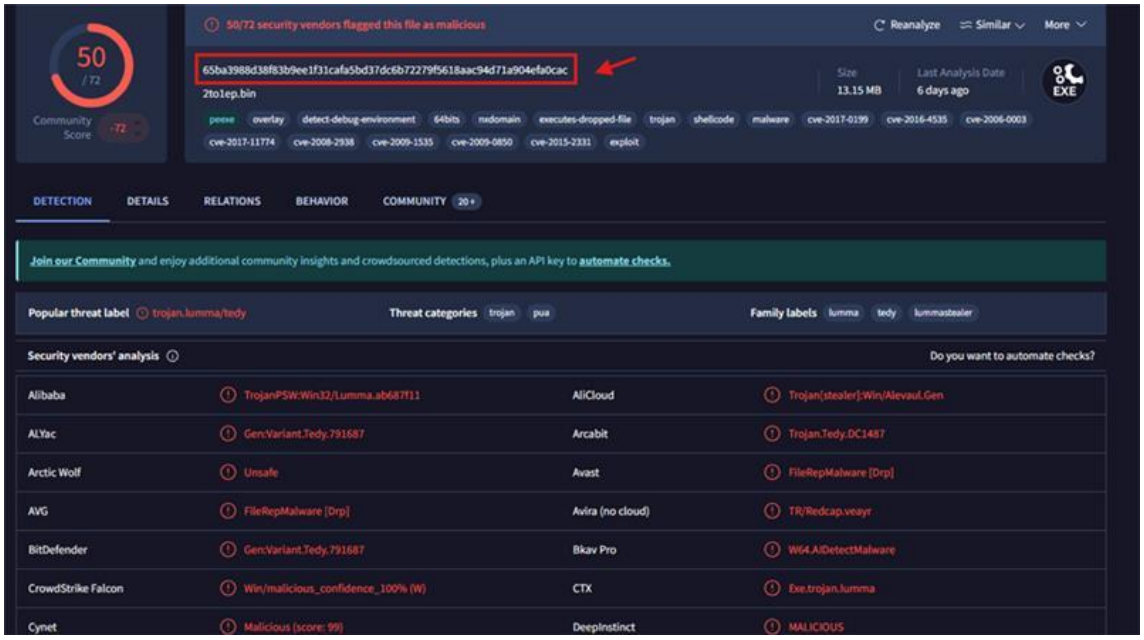
Para esta tarea vamos a analizar un malware reciente, llamado **virusvippro.exe**.

El análisis de AnyRun que estamos viendo es bastante reciente, de la mañana de hoy 10 de Octubre del 2025, y podemos ver que es un virus bastante completo con múltiples tags (autorun, botnet, remote, rat, etc)

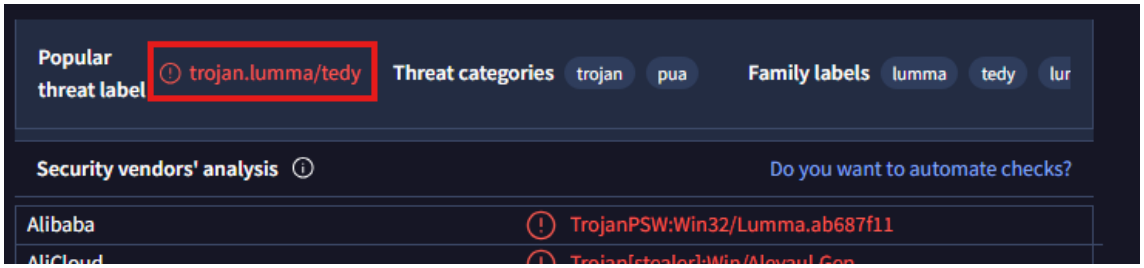


A falta de una cuenta empresarial en Any.run, lo cual nos impide la descarga del Malware, vamos a copiar el Hash MD5 del malware y lo vamos a pegar en VirusTotal

Procedemos a pegarlo en VirusTotal y nos analiza el Malware, y como podemos ver hay múltiples antivirus que ya lo han clasificado como peligroso, pese a ser tan reciente



Podemos ver que tiene una etiqueta de troyano de **Lumma**



Ejecución de un malware en un entorno controlado

En un entorno controlado (una máquina virtual sin acceso a la red y sin ninguna carpeta compartida con la máquina anfitriona) hemos grabado la ejecución de un Malware, concretamente un Ransomware, el WannaCry, que infectó miles de dispositivos en el 2017 aprovechando una backdoor, y Microsoft tuvo que lanzar una actualización con un parche para proteger a los equipos de futuras infecciones mediante el MS17_10. No obstante, años después, sigue siendo posible ejecutar el Ransomware desactivado los antivirus del ordenador, incluyendo el Microsoft Defender.

Desde este enlace a Google Drive, puede verse el proceso de infección y cómo encripta el equipo.

¿Cómo funciona el malware virusvippro.exe?

Informe Técnico (extraído de any.run y virustotal):

Nombre:

- 2to1ep.bin
- 2to1ep.exe
- virusvippro.exe.bin

Tipo: Win64 Executable

Tamaño: 13.15 MB

Detecciones 50/72 Motores AV en VirusTotal

Campaña maliciosa observada

La muestra se encuentra relacionada con una campaña de malware activa, donde se unitilizan muchos servidores para descargar payloads, ejecutar scripts y comunicarse con infraestructura de comando y control (C2), se observo uso de exploits antiguos como CVE-2017-0199 que es un remote code execution, luego el CVE-2016-4535 que permite a los atacantes remotos provocar denegación de servicios. Y el CVE-2017-11774 que incibe lo llama “Microsoft Outlook Security Feature Bypass Vulnerability”.

IOCs identificados

Url maliciosas contactadas.

Estas URLs fueron accedidas por el malware para descargar otros ejecutables o scripts maliciosos.

http://8.218.112.112:8880/02.08.2022.exe 200 ok

Url	Estado	Archivo descargado
http://8.218.112.112:8880/02.08.2022.exe	200 OK	.exe
http://118.89.58.108:MpUXSrv.exe	200 OK	.exe
http://43.134.189.185:8007/beacon_x64.ps1	200 OK	PowerShell
http://162.248.53.119:8000/svhost.exe	200 OK	.exe
http://46.8.120.153:8080/ServerBB.exe	200 OK	.exe
http://213.209.150.18:8080/agodee2.exe	200 OK	.exe
http://101.43.156.141:2323/winlicen.exe	200 OK	.exe

En total, la muestra contactó con más de 30 URLs durante su actividad. Además, se observaron los siguientes dominios maliciosos:

Dominio	Detecciones	Comentario
l4yaa.com	9 / 95	Infraestructura sospechosa desde 2012
3a9.net	6 / 65	Relacionado a campañas anteriores
securecloudsanbox.com	2 / 95	Posible señuelo o simulación
dcrat0106.duckdns.org	14 / 95	C2 relacionado a **DCRat**
cegelecinfo.fr	6 / 95	Usado para servir payload

Y por último, tuvo contacto con múltiples direcciones IP maliciosas durante la ejecución del malware, descargando archivos de dichas direcciones:

IP	País	Actividad
8.218.112.112	China	Servidor de descarga
43.134.189.185	China	Script PowerShell

43.6.120.153	Rusia	Payload EXE
101.43.156.141	China	Archivo winlicen.exe
213.209.150.18	Rusia	Varios ejecutables
1.94.184.17	China	sun32.exe
192.140.225.33	EEUU	Múltiples archivos en phpMyAdmin/

Se han identificado más de **400 IPs contactadas**, muchas de ellas en **ASN de alto riesgo**

Cadena (Kill chain / ATT&CK)

1. **Acceso Inicial**

T1190 – Exploit Public-Facing Application

Evidencia: aparecen etiquetas (cve-2017-0199, cve-2016-4535, cve-2017-11774, exploit).

2. **Ejecución**

T1059.001 – Command and Scripting Interpreter: PowerShell

Evidencia: http://43.134.189.185:88077/beacon_x64.ps1 (PowerShell script listado entre contacted URLs); ademas aparecen rev-shell.ps1

T1106 – Native Api

Evidencia; importa listadas incluyen CreateProcessW

T1055 – Process Injection (Shellcode execution)

Evidencia; etiqueta textual en output “shellcode”

(Ejectures-dropped-file - > ejecución de archivos droppeados)

Evidencia: etiqueta textual executes-dropped-file en tu output

3. **Persistencia**

No hay evidencia explícita de casos de persistencia como Runkeys, servicios ni nada.

4. **Evasión de Defensa**

T1027 – Obfuscated Files or Information

Evidencia: overlay + alta entropía y tag peexe/overlay en el output

5. **Credenciales de Acceso**

(no hay evidencia textual de Credential Access

6. **Movimiento Lateral**

T1021.005 – Remote Services: VNC

Evidencia: vnc.exe , aparece en la lista de dropped files.

7. **Recopilación de información**

T1113 – Screen Capture

Evidencia: Screnshoter , aparece en la lista.

8. **Command and Control (C2)**

T1071.001 – Aplication Layer Protocol: Web Protocols (HTTP/S)

Evidencia: En contacted Urls aparecen 460 urls, ejemplos textuales con respuestas 200:

- http://8.218.112.112:8880/02.08.2022.exe
- http://118.89.58.108:9999/MpUXSrv.exe
- http://43.134.189.185:8007/beacon_x64.ps1
- http://162.248.53.119:80007svhost.exe

T11105 - Ingress Tool Transfer

Evidencia: Multiples entradas de URLs que devuelven estado 200 para .exe y .ps1

9. **ExFiltration**

T1041 – ExFiltration Over C2 Channel

Evidencia: El output muestra abudante actividad de C2/HTTP Y dropped files, la tenica se incluye porque hay Contacte URLs y C2 HTTP litados.

No hay ransomware claro aunque en el tag de any.run lo indique, ya que no hay encriptación de datos ni archivos, Es más bien un troyano, según virustotal actúa como un backdoor que infecta el equipo y después descarga y ejecuta más archivos, ejecuta scripts, abre canales remotos C2 y deja artefactos como VNC / screenshoters.