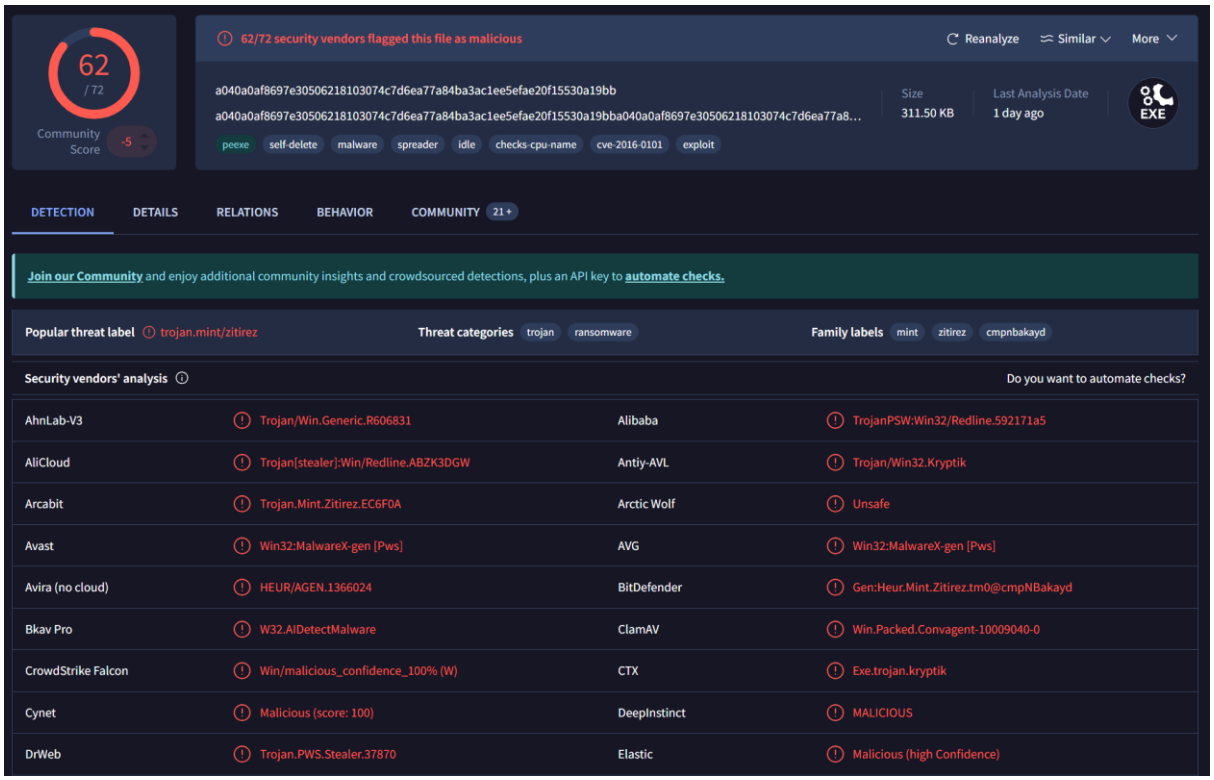
Contexto

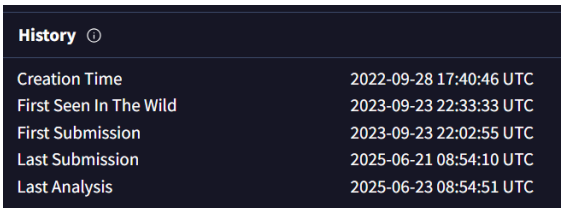
El contable de la empresa recibió a última hora de la tarde un correo electrónico titulado «Nuevo pedido urgente» de un cliente. Cuando intentó acceder a la factura adjunta, descubrió que contenía información falsa sobre el pedido. Posteriormente, la solución SIEM generó una alerta sobre la descarga de un archivo potencialmente malicioso. Tras una investigación inicial, se descubrió que el archivo PPT podría ser el responsable de esta descarga. ¿Podría realizar un examen detallado de este archivo?

Contamos con el hash del fichero **12C1842C3CCAFE7408C23EBF292EE3D9**, el análisis en Any Run y el sandbox report.

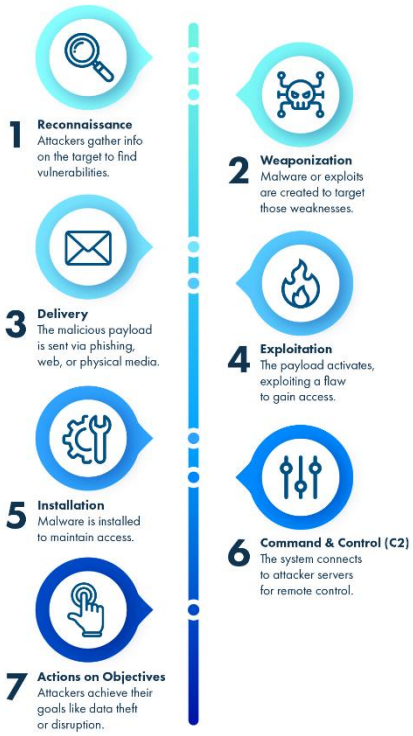
Investigación

Primeramente, se realiza un análisis del hash en la base de datos reputacional. Vemos que se encuentra altamente reportado por actividad maliciosa, mayoritariamente como troyano. En los detalles del archivo vemos que ha sido creado el día **28 de septiembre de 2022 a las 17:40**.





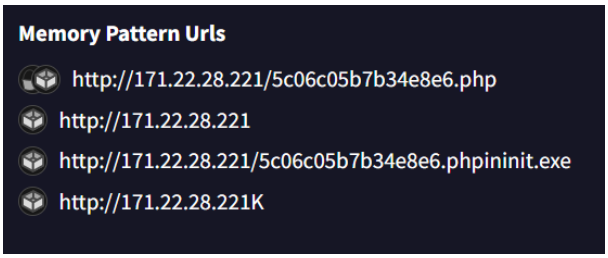
Una de las tareas más importantes es **identificar el servidor de Comando y Control (C2)**. Este es el servidor remoto con el que el malware se comunica para recibir órdenes o exfiltrar información.



En la Cyber Kill Chain de Lockheed Martin, la fase de Command and Control (C2) es la sexta etapa del ciclo de un ataque cibernético. Ocurre después de que el atacante ha conseguido ejecutar código malicioso en la máquina víctima, como en este caso cuando el usuario abre el archivo PPT.

El C2 es el **canal de comunicación entre el malware y el atacante**. A través de este canal, el atacante puede enviar órdenes, descargar cargas adicionales (payloads) y exfiltrar información. Es importante identificar este canal ya que, si se bloquea la comunicación, se puede **interrumpir el ataque antes de que cause daño real**.

Para encontrar esta información, en Virus Total tenemos la sección de Behavior donde aparecen detalles específicos del su comportamiento. Como estamos buscando las conexiones salientes establecidas por el archivo malicioso, debemos centrarnos en el apartado **"Network Communication"**, donde se listan los dominios, IPs y URLs con los que el archivo intenta comunicarse.



Una vez que el malware logra ejecutarse, es fundamental observar **cuáles son sus primeras acciones**, ya que estas pueden revelar su propósito o el tipo de ataque que intenta llevar a cabo. Analizar las **primeras bibliotecas (DLLs) que carga** tras la infección permite entender qué funciones del sistema está utilizando, lo que

puede apuntar a actividades como recolección de información, persistencia o conexión con un servidor externo.

El hecho de que sqlite3.dll aparezca en la sección **Files Dropped** significa que el propio archivo malicioso descarga o deja esta biblioteca en el sistema al ejecutarse. Esto sugiere que el malware usa una base de datos local (**SQLite**) para guardar información, como configuraciones o datos que recolecta.

En lugar de depender de que SQLite ya esté instalado, incluye su propia copia para asegurarse de que puede funcionar en cualquier equipo. Esto también le permite guardar datos sin necesidad de conectarse todo el tiempo a Internet, lo que lo hace más discreto.

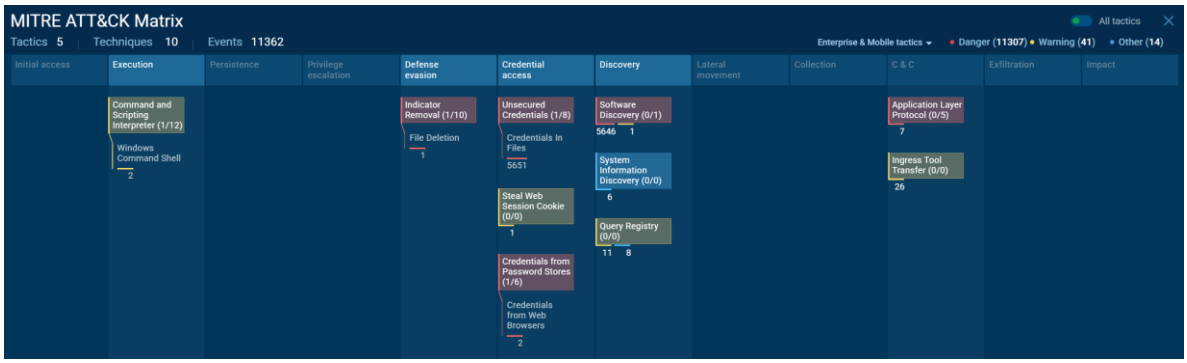
El malware utiliza la clave **532951462144124797572074900 9** para descifrar su cadena codificada en base64 mediante el algoritmo **RC4**.

Stealc

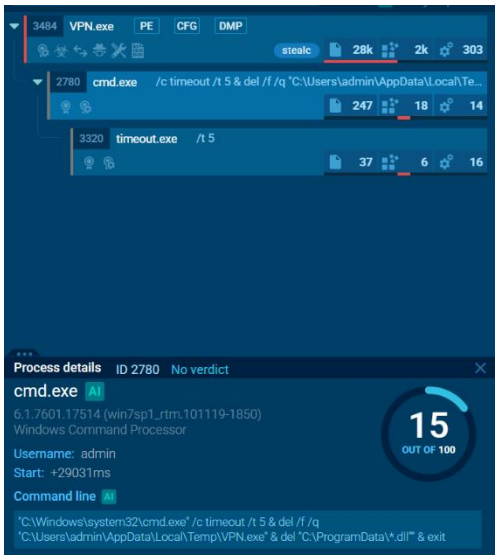
(PID) Process	(3484) VPN.exe
C2	http://171.22.28.221/5c06c05b7b34e8e6.php
Keys	
RC4	532951462144124797572074900 9
Strings (298)	" & del "C:\ProgramData*.dll"" & exit
	%08lX%04lX%lu
	%APPDATA%

RC4 es un algoritmo de cifrado simétrico que genera un flujo de claves para cifrar o descifrar datos. En este caso, el malware aplica RC4 para revelar información oculta dentro de la cadena base64.

Al analizar el reporte de la sandbox y mapear las técnicas en la matriz MITRE ATT&CK, se identifica la técnica principal **T1555**, que corresponde al robo de credenciales del usuario.



T1555	Credentials from Password Stores	Adversaries may search for common password storage locations to obtain user credentials. Passwords are stored in several places on a system, depending on the operating system or application holding the credentials. There are also specific applications and services that store passwords to make them easier for users to manage and maintain, such as password managers and cloud secrets vaults. Once credentials are obtained, they can be used to perform lateral movement and access restricted information.
.001	Keychain	Adversaries may acquire credentials from Keychain. Keychain (or Keychain Services) is the macOS credential management system that stores account names, passwords, private keys, certificates, sensitive application data, payment data, and secure notes. There are three types of Keychains: Login Keychain, System Keychain, and Local Items (iCloud) Keychain. The default Keychain is the Login Keychain, which stores user passwords and information. The System Keychain stores items accessed by the operating system, such as items shared among users on a host. The Local Items (iCloud) Keychain is used for items synced with Apple's iCloud service.
.002	Securityd Memory	An adversary with root access may gather credentials by reading `securityd`'s memory. `securityd` is a service/daemon responsible for implementing security protocols such as encryption and authorization. A privileged adversary may be able to scan through `securityd`'s memory to find the correct sequence of keys to decrypt the user's logon keychain. This may provide the adversary with various plaintext passwords, such as those for users, WiFi, mail, browsers, certificates, secure notes, etc.
.003	Credentials from Web Browsers	Adversaries may acquire credentials from web browsers by reading files specific to the target browser. Web browsers commonly save credentials such as website usernames and passwords so that they do not need to be entered manually in the future. Web browsers typically store the credentials in an encrypted format within a credential store; however, methods exist to extract plaintext credentials from web browsers.
.004	Windows Credential Manager	Adversaries may acquire credentials from the Windows Credential Manager. The Credential Manager stores credentials for signing into websites, applications, and/or devices that request authentication through NTLM or Kerberos in Credential Lockers (previously known as Windows Vaults).
.005	Password Managers	Adversaries may acquire user credentials from third-party password managers. Password managers are applications designed to store user credentials, normally in an encrypted database. Credentials are typically accessible after a user provides a master password that unlocks the database. After the database is unlocked, these credentials may be copied to memory. These databases can be stored as files on disk.
.006	Cloud Secrets Management Stores	Adversaries may acquire credentials from cloud-native secret management solutions such as AWS Secrets Manager, GCP Secret Manager, Azure Key Vault, and Terraform Vault.



El malware apunta al directorio **C:\ProgramData** para eliminar todos los archivos DLL, según se observa al examinar el árbol de procesos del reporte de la sandbox Any.run. Esto puede ser un intento de borrar rastros o eliminar componentes de seguridad instalados en esa ruta. Esta acción suele buscar evadir detección y dificultar la respuesta ante el incidente. Además, podemos ver que el tiempo que tarda en autodestruirse es de 5 segundos, tal y como se puede ver en el proceso **timeout.exe**.