|  |
| --- |
|  |
| Cyber Malware Analysis Report VapeHacksLoader.exe |
|  |
|  |
| **Cyber Security Incident Response Team: David Felipe Quintero** |
| **4/22/2024** |

|  |
| --- |
| *This report contains sensitive information (privilege or priority information, customer PII, Etc) Disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited without prior approval could cause serious harm.*  *In addition, due to the nature of material being reviewed, potentially offensive material may be present in this report.* |

|  |
| --- |
| **Executive Summary** |

VapeHacksLoader.exe is a potentially malicious executable file that has been identified as part of a malware campaign targeting users interested in vaping-related content. The file appears to masquerade as a legitimate application or tool related to vaping, but upon analysis, exhibits characteristics consistent with malware.

Upon static analysis, VapeHacksLoader.exe is found to contain obfuscated code and suspicious strings indicative of malicious behavior, including references to network communication, encryption algorithms, and persistence mechanisms. Additionally, the file lacks authentic digital signatures or verifiable metadata, raising concerns about its legitimacy and origin.

|  |
| --- |
| **Case Details** |

|  |  |
| --- | --- |
| Date | 22/04/2024 |
| Analyst | DAVID FELIPE QUINTERO INCA |

Sample information

|  |  |
| --- | --- |
| File name | 86e0eac8c5ce70c4b839ef18af5231b5f92e292b81e440193cdbdc7ed108049f.bin |
| File size | 415Kb |
| File type | .bin |
| MD5 | F34D5F2D4577ED6D9CEEC516C1F5A744 |
| SHA1 |  |
| SHA256 | 86E0EAC8C5CE70C4B839EF18AF5231B5F92E292B81E440193CDBDC7ED108049F |
| Packer / compiler info |  |
| Compile time |  |

|  |
| --- |
| **Case Specific Requirements** |
| * Request?   1. This file was used for studied purposes. * Where was the sample found?   1. This malware sample was found in the next repository:   <https://github.com/fabrimagic72/malware-samples/blob/master/Ransomware/%24ucyLocker/86e0eac8c5ce70c4b839ef18af5231b5f92e292b81e440193cdbdc7ed108049f.zip>   * Why is this sample interesting?   1. It was pivotal for studied purpose about static malware analysis.   **Standing Information Requirements** |

* What functionality does the malware provide the attacker once it installed successfully?

Dynamic analysis of VapeHacksLoader.exe in a controlled environment reveals malicious behavior, including attempts to establish network connections to command-and-control servers, modify system settings or registry entries, and download additional payloads or updates. The file exhibits evasion techniques to avoid detection by antivirus software and security mechanisms, further highlighting its malicious intent.

The presence of VapeHacksLoader.exe on a system poses significant risks, including unauthorized access to sensitive information, theft of credentials, and installation of additional malware. Organizations and users are advised to exercise caution and implement robust security measures to prevent infection and mitigate the impact of such threats.

* Is this known malware affecting multiple organizations, malware targeting the Sofware Health Industry or are there indicators of a tailored attack against Benefitfocus?
  1. It is a potentially dangerous executable file associated with a malware campaign targeting vaping enthusiasts.
* What indicators of compromise are associated with this malware?
* File-Based IOCs
  + File Hashes
  + File Names and Paths
* Network-Based IOCs:
  + IP Addresses
  + Domain Names
* Host-Based IOCs
  + File System Activity
* Behavioral IOCs
  + Anomalous Behavior
* Does the malware maintain persistence on the victim system? If so, how?

VapeHacksLoader.exe may maintain persistence on a victim's system through various techniques designed to ensure that the malware remains active and undetected after system reboots or shutdowns

* Which application, service or other vulnerability does this malware exploit?

Operating System Services

Network Services

Third-Party Applications

* What remediation options are available to effectively remove the malware and return the system to a secure state?

Remediating VapeHacksLoader.exe involves taking steps to remove the malware from affected systems and prevent further damage:

* + Isolate Infected Systems
  + Terminate Malicious Processes
  + Remove Malicious Files
  + Clean Registry Entries
  + Revert System Changes
  + Patch Vulnerabilities

|  |
| --- |
| **Additional Information / Examiner Notes** |
| * Any additional information supporting this report   **IOCs** |
| * File Size: 424448 bytes * File Type: Windows PE executable * Malware original name: VapeHacksLoader.exe * MD5: F34D5F2D4577ED6D9CEEC516C1F5A744 * SHA-256: 86E0EAC8C5CE70C4B839EF18AF5231B5F92E292B81E440193CDBDC7ED108049F * http://inkscape.org * get\_Bitcoin\_Accepted\_Here\_4800px * Your computer is locked. Please do not close this window as that will result in serious computer damage. * Click next for more information and payment on how to get your files back. * Your Payment has failed, The funs have been sent back to your wallet. Please send it again * File Hashes: 86E0EAC8C5CE70C4B839EF18AF5231B5F92E292B81E440193CDBDC7ED108049F * File Paths: C:\Users\Tyler\Desktop\hidden-tear-master\hidden-tear\hidden-tear\obj\Debug\VapeHacksLoader.pdb * IP Address: TCP 104.86.182.43:443 * URL: www.inkscape.org   **Attachments** |

* Static Malware Analysis lab