|  |
| --- |
| \*\*Logo\*\* |
| Cyber Malware Analysis Report Template V 1 |
|  |
|  |
| **Cyber Security Incident Response Team: [Analyst Name]** |
| **4/28/2021** |

|  |
| --- |
| *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** |

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

|  |  |
| --- | --- |
| Date |  |
| Analyst |  |

Sample information

|  |  |
| --- | --- |
| File name |  |
| File size |  |
| File type |  |
| MD5 |  |
| SHA1 |  |
| SHA256 |  |
| Packer / compiler info |  |
| Compile time |  |

|  |
| --- |
| **Case Specific Requirements** |
| * Request?   1. Details * Where was the sample found?   1. Details * Why is this sample interesting?   1. Details   **Standing Information Requirements** |

* What functionality does the malware provide the attacker once it installed successfully?
  1. Details
* Is this known malware affecting multiple organizations, malware targeting the Sofware Health Industry or are there indicators of a tailored attack against Benefitfocus?
  1. Details
* What indicators of compromise are associated with this malware?
  1. Network related (IP Addresses, URLs, email addresses, unique traffic patterns)
  2. Running processes / RAM artifacts
  3. Registry keys of interest
  4. File created
* Does the malware maintain persistence on the victim system? If so, how?
  1. Details
* Which application, service or other vulnerability does this malware exploit?
  1. Is it related to an existing CVE?
     1. If yes, list all related CVE numbers
     2. If no, could it be an unknown 0-day vulnerability?
  2. Does a patch exist?
  3. Does Endpoint Protection protect against this attack?
* What remediation options are available to effectively remove the malware and return the system to a secure state?
  1. Details

|  |
| --- |
| **Additional Information / Examiner Notes** |
| * Any additional information supporting this report   **IOCs** |
| * Extracted IOCs, usable for other teams to detect the sample in the environment   **Attachments** |

* List any attachments that should accompany this report