Severity

Medium

Analysis Summary

Guloader is currently being distributed via spam email campaigns with archived attachments that contain the malware. The majority of malware downloaded by GuLoader is commodity malware, with AgentTesla, FormBook, and NanoCore being the most predominant. This downloader typically stores its encrypted payloads on Google Drive. It has also downloaded its payloads from Microsoft OneDrive and also from compromised or attacker-controlled websites. By utilizing legitimate file-sharing websites, GuLoader can evade network-based detection, as these services are not generally filtered or inspected in corporate environments. Usually, the downloaded payloads are encrypted with a hard-coded XOR key embedded in the malware, making it difficult for file-sharing service providers to identify the payload as malicious. This time, the GuLoader Shellcode injector is being distributed via a file named “EXTERNAL RFPPAN India Epoxy/PU 2021”. The scope of this campaign so far seems to be global.

Impact

- Malware installation
- detection evation
- Information theft

Indicators of Compromise

MD5

- c033536c526b3f9a8a972c289fddd870
- 5bc069f8644f6e6ad5a1df00def3ae51
- 4a039ccf1c333214953856f96659e016
- 7aee1dcf19413b36960429382fb0785a
- f1ca0f5c7f519f4d07a73a9194d7a026

SHA-256

- f59fc580630ea8988b88d4fd4b854d4fbab0c7812ddaa6c849844e07a1002ae9
- 1a3ec21661224b7896a73c5ea2873d62c82750d1b1c8790d16b8a66fd9448247
- 29f965bf7b3c668eea93c555096dc628ed64bb78b5eeb610d16e5a146334787e
- 6cdf57af0be70c20aad11e8fa0e6b3ac98cfd628e7ee9f266fe53e1fa168fa27
- 7a065837ab9f1dbd91bc4337c97b4b2e1541b0fcc0c16e31cca04e451478d1a0

SHA-1

- f8384b0631744e6fa90196516573e1bee5526510
- fd3f96bfd7590534047d91848b5904d4e49308f3
- d366ff5ec70c4ee9329b2d0a7abad23fe3e4b97a
- 816cf3e95eba0ac12a0a08b0026f08712d9183e3
- 650dbf8511283e3b21b506486211ea820d02c4c9

Remediation

- Search for IOCs in your environment.
- Block all the threat indicators at your respective controls.