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

- 5610722bbbb7a687e139cf4d31f93b24
- fd9fc09a487c9eef61292e37fa9076c4
- 0d88d2be2e529e2e17b6fd66848e2f05
- e43e767f6896bbaabc50333542ad4ab8
- 2011fb1821d54f71cf61e3f1ceb32c78
- ac5b584f655fe8280f459f224cc7fdfb
- 3c3ccd42e1c0d72f84f08526bde81784
- 133beb9db3b71264188fa096cf119361
- d34a0f1dadcac29699e31b3903b7048c
- 7f7077faeb5eab7418f6cd5aa2f1928b
- f84851f7c66cefb93e0dc3d937323736
- 6c9bc8e528a6f60fd4a323fc518cc416
- 377eee86fc7eb8f94e79983f87e4bbd1

SHA-256

- dd1ed5209c967dd24b1a861d3eb959a0d52a3ed54a9e0e39685ec5269760f91a
- a75eaf347aeba5dccb918f638a30c5bceb7f2b2dd78a6cd496a258840fdfb1f1
- 0a32b76a81539d7c1e0c822755c8c138651238a227bab3df7bf2c29090337866
- 48b206d08e4a1e1a224947e8704cbaa02ff62060c6ba400e3a69c86c9c96d2a9
- e9232d005ebacceddcf4a8734969c04a57a8370d15d22c546661b54fd8f8df83
- 790d6dc689fab0f9bde9560c06f27fcfa6a146c87bc4ffd412847b0723b0c276
- 15a868a30e5cb8f5d81b67556ed9e45f819b275c77994caaa20dd149ed2671db
- 44db94e19afff7b161917ec4d3d2dd2a1e30fd766aec9f8ddfff070370f0688e
- 54768d1d7b75617da85033549e8087754e6079477827d12a5635afab20510cc5c
- 95fe8a4baed016cdc06c1c4cd0aca99b9f35b84e87f17bc06c50f05e51b4c874
- c1b9506eabf8d9ff95961ca89f65677bb298fc6105197d28942cc8ac8ca714f2
- c6335645313d55821bf05b78a4a036eb02bd3fbd6185f6bbd6aef66857c07d09
- 3cc46b047dce85c4ddf9f39894a6c67e42fe985e9835303e35f204a12b09c512

SHA-1

- dbc6a8c6fce7bb891d3cd8965da935eea647b3b3
- 4432e8481ece4c6631d99f43ec6e4fde15d9e359
- 5aa020b3b4b826ec80b8593785e2462d9c98ebf7
- f87dc382116b66d455324ec71bdbe2c21f73b5db
- 600c08baae604fd43bd4da9858c3c2b041d1a72c
- 1dac4ae2817ab4bd5c3f55b158e2c12ce9790b3d
- e96239c02e6ddcf63d9588389c2a8067cdff2a88
- 68348e8af9c7d055082778c7356af3af81b99ae1
- 073d69c6532755179ee1de736d00e2f8f8bc2791
- 023b5d5c33f4d58cc1badc9840b128ccdac548a5
- 299740de83dbb9f1dc08252c4a2480446d1af558
- 55a1ab1356d69116d82f16a3877b2bff2d923d7f
- 20585418c8a1041cdf503d39e607e53a3ad60698

Remediation

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