Severity

High

Analysis Summary

MetaStealer – a newly developed data-stealing malware spreads via a vast spam campaign. The spam campaign starts with an attachment in an email (a malicious MS Excel file). The creator of this malware attaches a malicious Microsoft Excel document called transfer “info2460.xls” (name may differ) to an email disguised as a letter about an approved transaction. After that, this malicious document infects a machine with MetaStealer after enabling macros commands. This type of malware harvests login information, credit card details, and other sensitive information. Their goal is to hijack online accounts and make unauthorized transactions and purchases.

Impact

- Credential theft
- Unauthorized Access

Indicators of Compromise

MD5

- 878801c8603b4087824fb0a5089ff5f9
- 7cc941628c333a1f6f6f519cabefdae6
- e74116c5efc7492fa74334a39e22afe8
- 187e468a41562814758d3fb231dda20b
- 117a0c218785e3dbd0d71bf99fccbe3f
- c54040cb03e3952b39f4f4961b8eb001
- b284363026bd2eef844085d6826d63ed

SHA-256

- 981247f5f23421e9ed736dd462801919fea2b60594a6ca0b6400ded463723a5e
- 81e77fb911c38ae18c268178492224fab7855dd6f78728ffedfff6b62d1279dc
- f644bef519fc0243633d13f18c97c96d76b95b6f2cbad2a2507fb8177b7e4d1d
- 7641ae596b53c5de724101bd6df35c999c9616d93503bce0ffd30b1c0d041e3b
- fba945b78715297f922b585445c74a4d7663ea2436b8c32bcb0f4e24324d3b8b
- bf3b78329eccd049e04e248dd82417ce9a2bcaca021cda858affd04e513abe87
- 71e54b829631b93adc102824a4d3f99c804581ead8058b684df25f1c9039b738

SHA-1

- e145f985ff965cb94d74de8d0e068a63044705e1
- 42a5768e490d89761c214c4cea4c07de65689615
- 393e81a3d525e8b582355d855d2c367047e4e0b0
- 5999138d62a0b94f65ee7e199058f758a4f05f5f
- de27feaf9d5ab451737c1daaf8ea49da5ceec2c7
- be82ad6a6c536ef36ace526e65974fbc05dafd7f
- 94143d6470da270fc2a623c264ea1b939fa0ad58

Remediation

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