Severity

Medium

Analysis Summary

Since 2016, FormBook has been active as a data-stealing malware that affects 4% of enterprises in 2020. It tracks and monitors keystrokes, finds and accesses files, takes screenshots, harvests passwords from various browsers, drops files, downloads, and executes stealthier malware in response to orders from a command-and-control server (C2). The cybercriminals behind these email campaigns used a variety of distribution techniques to deliver this malware, including PDFs, Office Documents, ZIP, RAR, etc.

Impact

- Sensitive Information Theft
- Credential Theft
- Keystroke Logging

Indicators of Compromise

MD5

- ccbe9aabcefa40af1e346e51ccee2b06
- 17uoEtuihi6Lsg4hdedT7PUhF4FNgBPD2F
- caf6ee23c1c1323c357e346e22d3e96f
- 713389a8fe739719850f57db5bae0358
- 3PxkHEMPaNMPMyiiHpHEj6ZgWzShh54N65

SHA-256

- 37b917980a25374058247c7dc8f63393dcca983fc522bef8d2be422206d9b865
- ab16df3a8883b6049c041dfb010de4ca1ff8ef1ff598c46b9395833b52f78f83
- 7b25cfa3fd8510d716490999e1fb90d79330f8e852aa2d539060e4768ffcf058
- 2c9a7034a9d5463d3c4e91dd5b652c91e906864b1731933397b41662bf85d0d2
- c609759c0751aa3c1f102e116ad18284337695e5168d74137fb9eb03a6c6a8a1

SHA-1

- 2a891a2ce8fe1c5a3139f0841c1b15e4bcd6d8a5
- b8c864e4db81925c7e5dcc587ddee6bae7836fcd
- cd256284acd932dc7f226a1114ed3de3dbd31a54
- b2a990e7d8918864868c74e7d32de30b45be1ede
- 02c4aece2efa4b39de7e3daf8e0de0319a24c218

Remediation

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