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
- Crediential Thedt
- Keystroke Logging

Indicators of Compromise

MD5

- f0eeda90c1a4d6099adfac6afafae743
- 9c38b509da7dc648e86ced26c86e38e4
- 4aa4a7730fe37b2168430203cb8fd0a4
- c4244a4b3c4b9f010952f650f741debd
- ed1690f3a3da74f266cac843187bf6c2
- 246d350f4698af2681c794a9203a96e5
- 0cfd52eb6025907beaf2f7f1ddde97de
- eeb1c2b12fdac0811cb143b179f16ba2
- ad41031b3648dea03db051ad6bebaacc
- 4665816f4565fe8486cebe90d442fac3
- c9b0f6ff056961a3988621a9bafd0440
- 49177c2be832b6c3cfff56411dfbbc5a

SHA-256

- 158fd8dc086132451bb06cb6f9f4db855bcff4fcf87ab86b1986dcc9e7e5e6ed
- 760d9ff24fa09df7e0ac02e7bd6f8715988043bafff70279b950c2d599be04ca
- 101159b2df3d82639b34a56f1b72524504492b91c80543689484a6e4ead0848c
- 81f4e3b64cd382fe241f3ce5f0f31eafca0fc82c77c91b751d03f8eb41511b3e
- d1324ad6746ac4d0022a3501ea81785bb78304512b4041ac0eb1f3dc19a68769
- 06413191f73628949b030b8a40c9db6a65487beed5d1d3c8e7e70af666ae538d
- fb638437a279bd91fc892b1c565ef4b308ff366fb56a2a1bd4dc1dab954eb535
- 045b2713fa49b215c38ab96d39f3f46b056c46391cec1c4772e3e15b6dd2005a
- af0ad92c81842deb70edc599988a44950e79a146fa014e36077b139e6bc82e8a
- 2273d198e458cede0e587d1c4d253a1853dee5e267659691f1758d2a87e50d77
- 3334df75a0322177f15a06b1ac65a73ebbf035af063c98cb582dfd2e7938221b
- 842a75ab92773e52741160c011f7265b489d57d82bdb8e1e6a5582b8852d8f3d

SHA-1

- 61e41f18da40cc21382d79807a71a35adc5e7b04
- ddb2360fd9afb687bb2b6f37cf9074d6f03352e0

- 44545b50c15de1a3cb67f5cbc02db712fa32b088
- 22da99fe11024705d53b2013d03f4bede12b2dbd
- 92a6553ae2295adc7ac5861f61817e7f36959120
- 81aaa39a424fac5016e0b08faa97875e06b6d305
- e351c1d0ab14b8750c3872ea02e1e7c136e6c483
- 3050341fd02dbf75426d12f761f860b2ec0ebad8
- 1096faa4a6449678cfee04c90f12626d9b60bf89
- 7f35fa7d52f7de5831b7c67b6252eb89bdf9ae13
- 8079af8820a29a2b84a3c1bc33f4b9433ad151c9
- e92dd8ede12b7c550d98304245d7924b82bff0dc

Remediation

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