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

- db1ede692838491be776d080ab2c890f
- a65ed177dfdf72e59f4a0d7a067cbcd5
- fa8a527f359a0815951dc38c4f95fe48
- d73792cdd4d135dc64d02e0cbbbbef52
- 6195cb2c622af75cc1689db47dea72ed

SHA-256

- 6dcffbbad26aa764fbcad76e0d821ba525acd18ccb25d688a239321ec07b7152
- 8b5fc481cee1804819aa3d6194fee9fbed93773f1b031760608bf1429704d36a
- 447530717de1dafdc9ac2145ce099b5adfa634d5e7fb30c14fc3852f22f2f9c3
- 0d9614aa395c74185c00f93c5b32a94e53d0458aa52cd1b496a1ecc4167a9282
- 858d8d49de1ad4ff735cf7fc2540587dc2efa86ccb5a8384134413f96742c655

SHA-1

- 2db0a30695e921c6fb35ab3a287a0d21c68fe01c
- 76e946c3a4404f223fa93db59494231eefd60784
- 9ef29b6f54321352d117f1af90c58213e4547625
- f0b61087d8fd166bb752ca666fca17302ffe844f
- 9fd47b44692f9514979254246af45196b6efb51a

Remediation

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