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

- 237bf3f32d40fefc5a67bb40b0d4a90d
- 5d4e98f42dc389a7a4b3d7ebb9aba83c
- 1042bda94adb7262d5a401d78c905524
- bd929543f251601313e4792f143419bc
- 976a815660086ec01d659eb30ad53288
- 57ba8f73725ba9eaa988eec85adcaf69
- f7174a65ad4de72292ebd45bad53c014
- aac47b26622b7b112abb2cf4545409b4
- ee9e1252b05b8f0ad34d0eb5f6d87365

SHA-256

- 59513c88f8f80d7a7c871c8f31f7bdf3e96d9831ec74ee9563845c202957a9cf
- 9f3d95b9160149fcdfd2d59114d87917abd2a8b903e1e3f5ccbdae11b1c28d68
- b01c10020580708d2d28cd94e8ec15fba89d16794a788d0a09928fb2af068117
- 6a4dcd405fe4ec854fd0bfa69f852b2a53e4cfa8bed45c7affeb4f86e963cb08
- dd60e55c229563801df128c29f52b21bc1cf22625c8b4b9442b2d7839c9175a4
- 5c8cdc3745711d1054704b8663828b005aa7a66535b0004c0364bc5cff832ddc
- 5d63cb62e9c2099fa70b843c45883c69237a557d5d7198499c37a95789f00bd4
- f46d6d7bf1c9f466498c2a11c9c96fcc594c3490db04e763f81e7552f7ae6764
- 24b22264a9954fe9763f2a35d92088be412600ae1e0e6fc8586925a18216c967

SHA-1

- dd62b8c971b610479ad5f04d3fb3d4f1f77a3ab9
- 44984db3396741017132afabf47a44d42030bcbe
- add94df8371d823578177fddf8fc47896b275b1f
- 4898a5c0ab8f310868c55e50a15e1e770c216ece
- cf7fad3596ddac9e7becc7da2726a08aae29b383
- 243a88cc0d31b588dd15ef583e08d569b80b1684
- 16848b5fe34886a7d5b24ba316381eb973d6d85c
- a1878da3ea31f946527897a759ffb1c9393fe426

- bac19e4a702d886d4739e45c0c310e62c93eea7d

Remediation

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