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

- Credential theft
- Keystroke logging
- Data Theft

Indicators of Compromise

MD5

- 4e6628e5f18ab15aac6fd96ef95b656d
- e21f324f15efde144c8a0e4107197d26
- 25b6e2d44ee8a077ca3b033ef76f30a4
- 2864cc846d8612ff5acb11545320efd9
- 7ced3b500e08cc17a580314471648b7b
- 0a3506bbf74aae38a9c80792d5df650d
- a7f2993548d91d5622b39c85f7e170b6
- 3193ca4b197f1745d3723cae02895d1d
- 0cc70bc96ebddba9730044db57a55579

SHA-256

- 87937d8e251601ab750fc53c6fed7e34f1f4400cad227e5083aae26ac09daf4a
- c7722c79d6e32511e879743467112fe5cebdc063e1938cfe59de4e1766c8a379
- bdea3bc64a4a9bf19ef37bfab2c993a422a37264d9e6c973c0842bb19d8deac1
- 200c93fd40e6be4f45726919ea9d7fc3850dd07e76acc180820964d5f8a5f48a
- 6fdd9a50a2d96e6516d38fc90084cca38559705db75350d22e2abd31a8806b83
- b8eaea107d52393bc327b1f69696169cee58ee72037fbbff1cf89019f872fe9f
- b67c56bafb316958f7f38463825bbc1daf462fe91a871cd37bdabdfd3c1630b5
- a7ed3c97d06221fa9d93b5089220f2686c635e87ac0fe890ee081e8b1d19468e
- 6ad48235e555a700a7322f5834311a3bd60c450a74f5354abf2cc139ffce0b18

SHA-1

- 71414122a1f431f62087841084e200955e2b20b8
- 6ef1f5d8e6fda633aca810aa59f10e47e6ed0563
- e19fdd202c0e12d2a98e33b2c33e30a5a3aa4072
- 3d901551c6227f9f2aa501ab70f42db98dba43ae
- b2522615cd8a6decba3f488d18a458d08724ae47
- e9eabe5c466a741fe5b49c96cd14390511a3cfc9
- 234ac5d2541757a5f57674d9312a03bc21afa821
- c2934d548086d540357f1afa0218a4367f991144

- 837f1d9ee067dcb5f35b2b74a1588a3876ac0ba7

Remediation

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