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

- 8d73718f7c4578ad7418e7ae088e6094
- 02ec875269791c1b039f15b727aa5034
- 04115098a78d042a3c7f0ed0ad8f2453
- 77227c54d8f83996610ff7306213f5ea
- 026f201bd4845bbda65327d214d75a3f
- 3285c170a13fc651fe71ec308982e17d
- 701c1f49568f70851d15750742a6169a
- 9cd599d658049708fe88c0fc63256216
- 58e1d6f601041b7bafc0f3b0a0bd3beb
- 2e2657f1615a3b3e85bbb08810712f95
- 572d05fe0dc0546103f1aecdbda3e7ce
- 4a29481bcff7afa8eba55c66ea729833
- e7141cadb71a36b0dcddb0ef7a67caec

SHA-256

- 6e8b50ce0fb3831a5afff633fccf423434b203a604ba3b08a79f32bb03cf4561
- 1ffd54f85a1a6c44f0d508c3bad9dbbce827dd3d4910636f93f47307dc0e2884
- 19a9ec9da618f09710fd8e6e1daec72377e05e78bd7469f33e203a9529d712fd
- 5b14b4ddf320a2a364744e6286fe8cf20d037ef53d72ff2a5ff1cdccb3753596
- 298d3c150bbee5312da015cd6448e7dc47eddcda5a6ddd215072102b6ba9e9e3
- c7b09601e132a1d10735f89dbec1fa98c2271b102d9a07b8bb41858775172312
- d640fe3968dbefc28ce7ae480b3e01578c6a1232087d7d17f96fbe35d89c19ae
- f0b819044a3bd7d24e2adfcf4fbed1f6ba6ca0a93fe29b6abf5f6dfe5279b8c7
- 494cf04c6406ba864ce890869984fa9e779751b0ad76c0e55ab28ec898d088b9
- 401a430936fe880e531de6c2476df50ed9be9e5bc9c8ea5149657b16b4a1eb84
- b0b3a059f434681f3f6cee2e2fcea6e91894255d7b63b0116d897b3e83b69e1a
- b4e446102081c3dda96a91145270f8a13ce318b708bea3921bc286e4c6fcc2a2
- 222ad93c9537bc72a00d01aaeab70acaea61210fb0de3967d671920848c87b04

SHA-1

- 37523bbc29985c9fb9c745c9ddfe6c68fe365d70
- c3337c257fdc957f4f84b56d9c6068519b5205ca
- 9f4df411d69f826863dadeb56ce2bb86061336a6
- 7e09d4048da0ec7a4574c569573b8e9223a878a0
- 7a4bfe6ce9f74c9897fa8037206ef1373d0378a7
- 05eaa0ed8484eb99dcd7f522ae2157fe5ecb4050
- b1b4256b1c91b916220039c3c803316ac818779b
- d4244ada046ba85cefa8972956b5f3ea2da4361d
- 882e839bfcf62cceae76a0bd42e60bf5f9a45870
- 8c1bbb96eb044f2933623909fc46d653b9ebd3ee
- 0e18210674716c41b201f978791eda3ad0125b29
- f1b04f09e2cd41d4a7763b7579404a792bbc0806
- f5728686a673d6c47416dfb9a0842702a7494c80

Remediation

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