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

Filename

- conferma d’ordine 46574[.]uue

MD5

- d019ae37773b21b29495a24b49b648c2

SHA-256

- df156dd5a1af82e5bd243f38362e615302b469b08d8c50d0db931c48d1bb559a

SHA-1

- e531c46d451ce2505f4592a5d0769e48bf055787

Remediation

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