Severity

Medium

Analysis Summary

HawkEye, primarily an infostealer, has additional capabilities such as bypassing of AV systems and keylogging. A spear-phishing campaign is detected using malicious RTF documents sent via corona-themed emails to distribute the HawkEye keylogger. While most malicious RTF documents use exploits to trigger Object Linking and Embedding (OLE) calls, in this case, the documents use the \objupdate switch. A victim would need to enable macros for the infection process to begin. The embedded OLE objects, five of them in this case, appear to be macro-enabled Excel sheets. PowerShell is used to execute .NET code which downloads and executes the Hawkeye payload.

Impact

- Information Theft
- Credential Theft
- Antivirus Bypass

Indicators of Compromise

MD5

- 985c6bfc24f5d4607865af8333611f0d
- b2af3b332d92fc09b79c4bf85263fd22

SHA-256

- c761c0aa331df2f68dcbe3e08f0f1ceda586a04c8ff79463cd44201777d6c80f
- b9dd8dfdb9a3fd61b2acffe0018cdf99b02c97025ae0d41a7aac7c9d76647b58

SHA-1

- 733ec0cd86c0e1e0e4ec0116fd11191f40c95025
- cbb3c3a4b17ba2888cfd0b96f59a5bc454d4ef32

Remediation

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