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

- 6c0cd8a71a4a79e96334c2b7605039ed

SHA-256

- c51f1844a27c74adbaf675d364dc637a1b48340a97ff608226d95f249314519a

SHA-1

- a7b05e47424e399853f2df25875196941566d252

Remediation

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