Severity

High

Analysis Summary

In the year 2018, the threat actor WIRTE APT Subgroup was discovered for the first time. Spear-phishing emails are used to encourage victims to open a malicious Microsoft Excel/Word document. All of the Excel droppers found were using a technique that leverages formulae in hidden spreadsheets or cells to execute macro 4.0 commands named as Excel 4.0 macros. It is used to drop malware called Ferocious droppers. The payload was downloaded using conventional VBA macros by the Word droppers. The actor customized the counterfeit contents to the targeted victims, including logos and themes that were relevant to the targeted company or current events in their location. However, in some circumstances a bogus 'Kaspersky Update Agent' executable worked as a dropper for the VBS implant. The threat actor appears to have targeted a range of sectors, including diplomatic and financial institutions, government, law firms, military groups, and technological enterprises. Armenia, Cyprus, Egypt, Jordan, Lebanon, Palestine, Syria, and Turkey are among the countries affected. WIRTE is a suspected part of the Gaza Cybergang that is an Arabic politically motivated cyber criminal group. WIRTE APT Subgroup changed their toolkit and how they operate in order to be inconspicuous for longer. They use simple but successful tactics to compromise its victims and outperformed its suspected peers in terms of OpSec by using interpreted language malwares like VBS and PowerShell scripts.

Impact

- Information Theft and Espionage

Indicators of Compromise

MD5

- a65ad679989b3a403eca8d3e7ba442e9
- 49e67a8382d10a764591b84f7e5aaf0e
- 314c947e3cf6a8d7b96152dcd8e8f9a7

SHA-256

- d767e2ba31b75714aeb1cc3995de9191a53bd184e213780987e51e315ec2e4c5
- aca9e602caefd598a3c5991d68937bc1624cdc8f1d602f8bc0a3b9c0078a1d28
- a49eabce7f084e16753ac08abf2f7cd54052a9d20f68ecb34cf2b88d9a05d34d

SHA-1

- a6ace9deb2b2febd9815b4f4da0e6e1929ed6f5a
- 2ef520b4149869b184165e4f3300b2a04e376e9e
- 205a5668445d0c9810d418488effe8fd4d2557f

Remediation

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