## Severity

High

## Analysis Summary

Cobalt Strike first appeared in 2012 in response to alleged flaws in the Metasploit Framework, an existing red team (penetration testing) tool. Cobalt Strike 3.0 was released in 2015 as a stand-alone opponent emulation platform. However, researchers began observing threat actors using Cobalt Strike by 2016. Cobalt Strike's use in hostile activities was previously connected with huge cybercriminal operations like TA3546 and APT40. Cobalt Strike is a legitimate Pen test (penetration testing) toolkit that deploys "beacons" on infected devices to perform malicious behaviors. It is commonly used in ransomware attacks.

Cobalt Strike allows the attacker to install a Beacon agent on the victim's PC, which gives them access to a variety of tools, including command execution, file transfer, keylogging, mimikatz, port scanning, and privilege escalation. Cobalt Strike includes a toolkit called Artifact Kit that is used to create shellcode loaders.

Ukraine is under attack using the Cobal Strike Beacon malware. Emails with the topic "Urgent!" are being circulated and If you open a document and activate a macro, the macro will download, create on disk and run the file "pe.dll". Other filenames are:

- spisok.exe
- Military on Azovstal.xls
- shellcode.bin.packed.dll
- notevil.dll

## Impact

- Information Theft and Espionage
- Exposure of Sensitive Data

## Indicators of Compromise

### Domain Name

- agreminj[.]com

### IP

- 84[.]32[.]188[.]29
- 138[.]68[.]229[.]0
- 139[.]60[.]161[.]74
- 139[.]60[.]161[.]225

### MD5

- 877f834e8788d05b625ba639b9318512
- e28ac0f94df75519a60ecc860475e6b3

### SHA-256

- ea9dae45f81fe3527c62ad7b84b03d19629014b1a0e346b6aa933e52b0929d8a
- 9990fe0d8aac0b4a6040d5979afd822c2212d9aec2b90e5d10c0b15dee8d61b1

### SHA-1

- 96bde83f4d3f29fb2801cd357c1abea827487e37

- 34bd51533865fe03756e7dc00f21e1d5f477db6f

**URL**

- http[:]//138[.]68[.]229[.]0/pe[.]dll
- https[:]//dezword[.]com/apiv8/getStatus
- https[:]//dezword[.]com/apiv8/updateConfig

# Remediation

- Prohibit office programs (EXCEL.EXE, WINWORD.EXE, etc.) from creating dangerous processes (for example, rundll32.exe, wscript.exe, etc.).
- Exercise caution when receiving messages from unknown senders.
- Block all threat indicators at your respective controls.
- Keep your software updated to the latest patches.
- Search for IOCs in your environment.