Severity

Medium

Analysis Summary

CaddyWiper is another destructive data wiper suspected to be targeting Ukraine. The wiper, which erases user data and information from associated drives, was discovered on several systems in a limited number of companies. By overwriting the data with a NULL value, CaddyWiper removes all files under C:\Users as well as all files under accessible discs from D: to Z:. If the size of the target file exceeds 0xA00000 bytes (10MB), it only wipes the first 0xA00000 bytes. CaddyWiper shares no code similarities with HermeticWiper or IsaacWiper, the other two new data wipes that have infected Ukrainian organizations. However, this wiper has a tactical overlap with HermeticWiper as it was deployed via the Windows domain controller, implying that the attackers had gained control of the Active Directory server.

Impact

- Data Exfiltration
- Credential Theft
- Financial Loss

Indicators of Compromise

Filename

- zrada[.]exe
- peremoga[.]exe
- vatt[.]exe
- pa[.]pay
- caddywiper[.]bin

IP

- 91[.]245[.]255[.]243
- 195[.]230[.]23[.]19

MD5

- 9ec8468dd4a81b0b35c499b31e67375e
- 1938380a81a23b8b1100de8403b583a7
- b63b9929b8f214c4e8dcff7956c87277

SHA-256

- cda9310715b7a12f47b7c134260d5ff9200c147fc1d05f030e507e57e3582327
- 1724a0a3c9c73f4d8891f988b5035effce8d897ed42336a92e2c9bc7d9ee7f5a
- fc0e6f2effbfa287217b8930ab55b7a77bb86dbd923c0e8150551627138c9caa

SHA-1

- 6fa04992c0624c7aa3ca80da6a30e6de91226a16
- 9ce1491ce69809f92ae1fe8d4c0783bd1d11fbe7
- 13aa2b7c1dad663462efc0a88d64770d2bc5dc4d

Remediation

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