Hive Pro

THREAT ADVISORY

Destructive data wipers and worm targeting Ukrainian organizations	TA2022045
Threat Level RED	**Published Date –** Mar 2, 2022 **Updated Date –** Mar 15,2022

Cybersecurity & Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) have jointly released an advisory and warned of an ongoing cyber attack using destructive malware targeting organizations in Ukraine that allows attackers to take complete access of the systems and make them inoperable.

Several cybersecurity researchers reported from across the globe and disclosed a highly catastrophic malware known as HermeticWiper which was targeting several organizations in Ukraine. The malware targets Windows devices' master boot record and manipulates to cause the boot failure. To infiltrate the network, lateral movement, and malware distribution, attackers used tools like Impacket and RemCom as remote access software. Microsoft tracks this malware as Foxblade wiper.

A worm HermeticWizard uses WMI and SMB to spread through network and deploy wiper to local computer. Successful exploitation may directly impact the daily operations of any organization and cause the unavailability of critical assets and data. Another wiper named Isaacwiper is now targeting the organizations which are not affected by Hermeticwiper. On the other hand, they do not have the same code. Along with the wiper, a ransomware HermeticRansom was also used potentially to hide the wiper's action.

A fourth wiper dubbed as CaddyWiper is targeting Ukraine as of March second week. The wiper is deployed using Group Policy Objects and further avoids deleting data on domain controllers in order to keep access to the target organization while yet disrupting operations. In addition to this, it determines whether a device is a domain controller by calling the DsRoleGetPrimaryDomainInformation() method. This is most likely a method employed by attackers to keep access to the infiltrated networks of the businesses they target while causing significant disruption to operations by deleting other vital devices.

The Mitre TTPs used by the malwares in the current attack are:
TA0001: Initial Access
TA0007: Discovery
TA0040: Impact
TA0042: Resource Development
TA0002: Execution
TA0008: Lateral Movement
T1588: Obtain Capabilities
T1588.002: Obtain Capabilities: Tool
T1588.003: Obtain Capabilities: Code Signing Certificates
T1078: Valid Accounts
T1078.002: Valid Accounts: Domain Accounts
T1059: Command and Scripting Interpreter
T1059.003: Command and Scripting Interpreter: Windows Command Shell
T1106: Native API
T1569: System Services

T1569.002: System Services: Service Execution
T1047: Windows Management Instrumentation
T1018: Remote System Discovery
T1021: Remote Services
T1021.002: Remote Services: SMB/Windows Admin Shares
T1021.003: Remote Services: Distributed Component Object Model
T1561: Disk Wipe
T1561.002: Disk Wipe: Disk Structure Wipe
T1561.001: Disk Wipe: Disk Content Wipe
T1485: Data Destruction
T1499.002: Endpoint Denial of Service
T1499.002: Endpoint Denial of Service: Service Exhaustion Flood

Indicators of Compromise (IoCs)

Type	Value
SHA-1	912342F1C840A42F6B74132F8A7C4FFE7D40FB77, 61B25D11392172E587D8DA3045812A66C3385451, 3C54C9A49A8DDCA02189FE15FEA52FE24F41A86F, F32D791EC9E6385A91B45942C230F52AFF1626DF, AD602039C6F0237D4A997D5640E92CE5E2B3BBA3, 736A4CFAD1ED83A6A0B75B0474D5E01A3A36F950, E9B96E9B86FAD28D950CA428879168E0894D854F, 98b3fb74b3e8b3f9b05a82473551c5a77b576d54
MD5	a952e288a1ead66490b3275a807f52e5, 231b3385ac17e41c5bb1b1fcb59599c4, 095a1678021b034903c85dd5acb447ad, eb845b7a16ed82bd248e395d9852f467
SHA-256	a294620543334a721a2ae8eaaf9680a0786f4b9a216d75b55cfd28f39e9430ea

References

https://www.cisa.gov/uscert/ncas/alerts/aa22-057a
https://www.welivesecurity.com/2022/03/01/isaacwiper-hermeticwizard-wiper-worm-targeting-ukraine/
https://www.bleepingcomputer.com/news/security/new-caddywiper-data-wiping-malware-hits-ukrainian-networks/