Cyber National Mission Force discloses IOCs from Ukrainian networks

cybercom.mil/Media/News/Article/3098856/cyber-national-mission-force-discloses-iocs-from-ukrainian-networks/

July 20, 2022

FORT GEORGE E. MEADE, Md.-- In close coordination with the Security Service of Ukraine, USCYBERCOM's Cyber National Mission Force is disclosing these indicators of compromise. In the last few months, the Security Service of Ukraine discovered several types of malware in their country, and have analyzed the samples and identified IOCs. The IOCs included 20 novel indicators in various formats.

We are publically uploading these IOCs to highlight the potential compromises and provide additional context to our industry counterparts.

Our Ukrainian partners are actively sharing malicious activity they find with us to bolster collective cyber security, just as we are sharing with them. We continue to have a strong partnership in cybersecurity between our two nations.

Why IOCs matter: IOCs are evidence of possible intrusions on a host system or network, and act as digital forensics for network defenders of a potential breach. IOCs implementation enables users to search and identify malware within that host system or network. Malware has a specific behavior that can be identified with the implementation of IOCs. Additionally, the file hash is a quick way to look for the malware, because if the file is the same as the malware, it will have the same hash.

https://www.virustotal.com/gui/file/6662ef0cfe92fe4a61663ce89306a481c2d605591faaa7e1b03be7e0d9d4a1b6/details

https://github.com/CYBERCOM-Malware-Alert/IOCs/blob/main/Ukraine%20Network%20IOCs%20July%2020%202022.xlsx

https://pastebin.com/PCK97yjc

IOC	Related Signature
195.154.255 [.] 211	

a8yq99tadibixcolmcy8eiyfncvafk7iqcnarcqxaaaaaaaaaaaaaaaaalaaiaa.aaaaaaaaaaaa e.mx 1[.]be	
a8yk66yshlbixcolmcy8eiyfncvafk7iqcnarcqxaaaaaaaaaaaaaaaaalaaiaa.aaaaaaaaaaaa ae.mx 1[.]be	
a8y1a442fibixcolmcy8eiyfncvafk7iqcnarcqxaaaaaaaaaaaaaaaaalaaiaa.aaaaaaaaaaaa e.153 [.]re	
9cf2ee018a565c00e811897e6056a5a2	
8fc42ee971ab296f921bb05633f6b4a6	
Зброя НОВ.zip	2fd2a110eb2f0b1c15381a4727b2e312
Zbroia.lnk	e8c1cd480ecee79077472800be06b3e7
zbroia/1.jpg	117a4913ca14a74a0264352a4b8a2bb6
zbroia/2.jpg	c17c26bef5917fb914e0f32e24b4071a
zbroia/зброя нов.xsls	14a89a87f6209515745fbcfe8976287c
"план евакуації (затверджений сбу 28.02.2022 наказом № 009363677833).rar_pass_123.zip	cd8834da2cfb0285fa75decf6c67d049
a236cb7f2b0e34619039788de7f7760b	
wisw.exe	9ad4a2dfd4cb49ef55f2acd320659b83
java-sdk.exe	c8bf23864162121212901517570e96fae7
oracle-java.exe	4f11abdb96be36e3806bada5b8b2b8f8
microsoft-cortana.exe	9ea3aaaeb15a074cd617ee1dfdda2c26
tmp.php	e5e91ec7f8ee8e87a5c349b239bbb47e
up.php	21cc2e276dc88edbbfd7afc45f664534
BC9DF288FB11693DD1C7CE96A9B9DFB3	