Hive Pro

THREAT ADVISORY

Ukraine government entities targeted by a destructive malware “Whispergate”	TA2022011

Threat Level	RED	Publish Date – Jan 17, 2022

A malware attack was carried out on Ukraine government, non-profit, and IT entities with a wiper disguised as ransomware. The threat actor, DEV-0586 targeted government bodies that provide critical executive branch or emergency response functions.

The attack using the malware “Whispergate” was preformed in two stages:
Stage 1: The malware overwrites the Master Boot Record to display a faked ransom note that requests the payment of a $10,000 ransomware in bitcoin.
Stage 2: Stage2.exe is a downloader for second stage malware that corrupts files and is hosted on a Discord channel. After that, the corrupter virus searches for files with hundreds of various extensions, overwrites their contents with a predetermined quantity of 0xCC bytes, and renames each file with an apparently random four-byte extension.
This attack is intended to be destructive and designed to render targeted devices inoperable rather than to obtain a ransom.

Previously on 13th of January an attack by UNC1151 targeted at least 15 websites belonging to various Ukrainian public institutions were compromised, defaced, and subsequently taken offline. The attackers carried out a supply chain attack by using the vulnerability CVE-2021-32648 in October CMS which is a free content management system. Exploiting this vulnerability the hackers could send a password reset request for an account in this system and then gain access to it.

The attacks are not linked currently but there is a huge possibility that they are carried simultaneously. To mitigate the risk organizations are advised to update October CMS to the latest version and also to monitor the hashes in their system.

Actor Details

Name	Origin	Target Locations	Target sectors
DEV-0586	Russia (alleged)	Ukraine	government, non-profit, and IT entities
UNC1151	Belarus		

Vulnerability details

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE ID
CVE-2021-32648	OctoberCMS versions from 1.0.471 and 1.1.1 to 1.1.4	ccpe:2.3:a:octobercms:october:1.0.471:*:*:*:*:*:*:* cpe:2.3:a:octobercms:october:1.1.1:*:*:*:*:*:*:* cpe:2.3:a:octobercms:october:1.1.2:*:*:*:*:*:*:* cpe:2.3:a:octobercms:october:1.1.3:*:*:*:*:*:*:* cpe:2.3:a:octobercms:october:1.1.4:*:*:*:*:*:*:*	OctoberCMS security bypass	CWE-640

Indicators of Compromise (IoCs)

Type	Value
SHA-256	dcbbae5a1c61dbbbb7dcd6dc5dd1eb1169f5329958d38b58c3fd9384081c9b78, a196c6b8ffcb97ffb276d04f354696e2391311db3841ae16c8c9f56f36a38e92

Patch Link

https://github.com/octobercms/october/security/advisories/GHSA-mxr5-mc97-63rc

References

https://cert.gov.ua/article/17899
https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/
https://securityaffairs.co/wordpress/126782/apt/destructive-malware-campaign-targets-ukraine.html?utm_source=rss&utm_medium=rss&utm_campaign=destructive-malware-campaign-targets-ukraine
https://ain.ua/en/2022/01/14/hackers-attack-some-ukrainian-government-websites/