# ANY.RUN Shows How Cyber Criminals Abuse WebDAV to Launch Malware Attacks

DUBAI, DUBAI, UNITED ARAB EMIRATES, April 8, 2024 /EINPresswire.com/ -- ANY.RUN, the leading provider of an interactive malware analysis sandbox, has published a study on cyber attacks that leverage WebDAV, URLs, and LNK files to deliver malicious payloads. The article provides a detailed analysis of the attack execution and offers actionable information to detect and prevent such attacks.

□□□ □□□□□ □□ □ □□□□□□ □□□□□□
WebDAV (Web Distributed Authoring and Versioning) is a file transfer protocol built on HTTP. Attackers often exploit this technology to host malicious payloads, which are then downloaded and executed on victims' computers using scripts or other methods.

An attack using a WebDAV server targeting a PC follows four main steps:

1. The attacker creates a shortcut (LNK) file that contains malicious commands.
2. The LNK file is then uploaded to the attacker's WebDAV server, ready to be downloaded and executed by the victim's computer.
3. The attacker creates a URL pointing to a file containing the link to the attacking WebDAV server hosting the LNK. This URL file is what the victim will run.
4. When the victim runs the URL file, it triggers the download and execution of the LNK file. This leads to the device getting infected with malware such as AsyncRat, Purelogs, or others.

□□□□□□□□ □□□ □□□□□□□□□
The researchers introduce several methods to identify and counter such attacks. These include:

• YARA, Suricata, and SIGMA Rules to detect malicious URL/LNK files, command line indicators, and network connections to WebDAV servers.
• Blocking URL Execution: The experts suggest blocking the execution of URL files in Windows settings as a mitigation strategy. This prevents the automatic execution of malicious files.
Make sure to take into consideration the growing threat of WebDAV attacks and introduce proper security measures to protect your infrastructure.

Read more on ANY.RUN's blog.

□□□□□ □□□.□□□
ANY.RUN is a cybersecurity company specializing in interactive malware analysis. Its flagship product, an interactive malware sandbox, enables security teams to analyze threats efficiently and accurately. ANY.RUN is dedicated to helping businesses strengthen their cybersecurity posture.

Veronika Trifonova
ANYRUN FZCO
+1 657-366-5050
email us here
Visit us on social media:
Twitter
YouTube