New ValleyRAT Malware Campaign Identified, Using Advanced Techniques

DUBAI, DUBAI, UNITED ARAB EMIRATES, August 20, 2024 /EINPresswire.com/ -- A new, highly sophisticated malware campaign targeting Chinese-speaking users has been identified, ANY.RUN researchers say, involving the distribution of a multi-stage malware known as ValleyRAT.

This campaign was first originally reported in June 2024 and has since evolved to include advanced techniques for persistence, privilege escalation, and evasion.

ValleyRAT is a versatile backdoor malware that enables attackers to remotely control compromised systems, deploy additional malicious plugins, and monitor victim activities. The malware primarily spreads through email messages containing URLs that lead to compressed executables, designed to appear as legitimate applications such as Microsoft Office files.

Once executed, ValleyRAT initiates a multi-stage attack sequence. The first-stage loader drops a decoy document and executes shellcode that advances the attack, establishing communication with a command-and-control (C2) server. The malware then downloads additional components, including RuntimeBroker and RemoteShellcode, which are responsible for maintaining persistence on the host, escalating privileges, and bypassing security controls.

One notable characteristic of ValleyRAT is its ability to evade detection by executing its components directly in memory, reducing its traceable footprint on the infected system. Additionally, the malware has been observed scanning the Windows Registry for keys related to popular Chinese applications, reinforcing the assessment that this campaign specifically targets

Chinese-speaking users.

The ValleyRAT malware has been successfully analyzed using the ANY.RUN interactive sandbox, which provides detailed insights into the malware's behavior. The analysis revealed the use of legitimate processes such as MSBuild.exe to disguise malicious activities, making detection more challenging.

For more information on ValleyRAT and to explore the full capabilities of ANY.RUN, please visit ANY.RUN's official blog.

The ANY.RUN team
ANYRUN FZCO
+ +1 657-366-5050
email us here
Visit us on social media:
X
YouTube

This press release can be viewed online at: https://www.einpresswire.com/article/736823945