

# ANY.RUN Releases Expert Malware Analysis on AZORult

DUBAI, DUBAI, UNITED ARAB EMIRATES, September 4, 2024 /EINPresswire.com/ -- [ANY.RUN](#), a leading provider of interactive malware analysis solutions, presents an insightful guest post by malware reverse engineer and threat intelligence analyst, Mostafa ElSheimy. In this comprehensive analysis, Mostafa examines the main functionalities of AZORult, a sophisticated credential and payment card information stealer.

████████████████████ ████████████ █  
██████████' ██████████████ ███  
██████████

ElSheimy provides an in-depth look into the evolution of AZORult, tracing its origins from its early development in Delphi to its transition into C++ and the introduction of .bit domain support.

The key findings include:

- Execution of hidden PowerShell commands: AZORult uses PowerShell scripts to execute malicious commands undetected.
- Registry manipulation: AZORult modifies and deletes Windows registry keys, further securing its persistence within the system.
- File dropping: The malware deploys additional payloads, such as Declinometer235.exe, to enhance its functionality and ensure broader system compromise.



