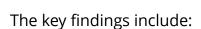


## ANY.RUN Releases Expert Malware Analysis on AZORult

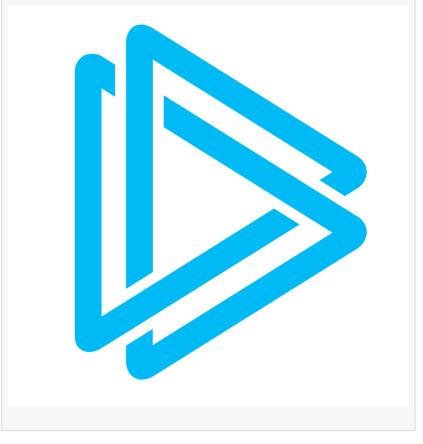
DUBAI, DUBAI, UNITED ARAB EMIRATES, September 4, 2024 /EINPresswire.com/ -- ANY.RUN, a leading provider of interactive malware analysis solutions, presents an insightful guest post by malware reverse engineer and threat intelligence analyst, Mostafa ElSheimy. In this comprehensive analysis, Mostafa examines 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.



- 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.



• Anti-debugging techniques: It employs techniques such as GetTickCount to detect if it's running in a virtualized environment, helping it avoid detection.

## 

For cybersecurity experts, this report serves as a practical guide to understanding malware's strategies and methods, which can be vital for developing countermeasures against this type of threat.

Learn more on ANY.RUN's blog

## 00000 000.000

ANY.RUN assists over 400,000 cybersecurity professionals worldwide with its interactive sandbox solutions, simplifying the analysis of malware targeting both Windows and Linux systems. Our advanced threat intelligence tools, including TI Lookup, YARA Search, and Feeds, help organizations quickly gather Indicators of Compromise (IOCs), understand active threats, and respond faster to incidents.

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

Χ

This press release can be viewed online at: https://www.einpresswire.com/article/740665218 EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information. © 1995-2024 Newsmatics Inc. All Right Reserved.