

# ANY.RUN Unveils Detailed Analysis of PSLoramyra: A Fileless Malware Loader

DUBAI, DUBAI, UNITED ARAB EMIRATES, December 2, 2024

/EINPresswire.com/ -- The cybersecurity team at [ANY.RUN](#) has shared an in-depth look at PSLoramyra, an advanced fileless malware loader that uses PowerShell, VBS, and BAT scripts to break into systems, run malicious code directly in memory, and stay hidden. This in-depth analysis demonstrates the behavior of the loader step by step, showing how it evades traditional detection, bypasses security and maintains control.

□□ □□□□□□□□ □□ □□□□□□□□□□□  
□□□□□□□□ □□□□□□ □□□□□□□□□□



The analysis by ANY.RUN reveals how PSLoramyra, a sophisticated fileless malware loader, uses PowerShell, VBS, and BAT scripts to deliver and execute payloads like Quasar RAT directly in memory, bypassing traditional detection methods.

□□□ □□□□□□□□ □□□□ □□ □□□□□□□□□□ □□□□□□□□

The research breaks down its infection chain, showing how it creates scheduled tasks for persistence and uses obfuscation techniques to stay hidden, giving cybersecurity professionals a closer look at how to tackle this type of threat:

- □□□□□□□□ □□□□□□□□□□: PSLoramyra operates entirely in memory, leveraging PowerShell to execute malicious payloads, leaving minimal traces on the disk and evading traditional detection methods.

- **Script Execution:** The malware uses a combination of VBS, BAT, and PowerShell scripts, working together to deliver and execute payloads such as the Quasar RAT.
- **Task Scheduler:** It ensures long-term access by creating a Task Scheduler task that runs every two minutes, executing its scripts without user awareness.
- **Obfuscation:** Obfuscates payloads using hex-encoded strings and custom delimiters, making static analysis and detection more challenging for security tools.
- **Script Names and Domains:** Unique script names (roox.vbs, roox.bat, roox.ps1), command lines, and malicious domains provide valuable clues for identifying and mitigating the threat.

To dive deeper into the details of PSLoramyra's techniques, visit [ANY.RUN's blog](#).

ANY.RUN

ANY.RUN provides interactive malware analysis tools trusted by over 500,000 cybersecurity professionals worldwide. With powerful features for real-time behavioral analysis, ANY.RUN helps identify threats, reduce investigation time, and provide actionable insights for incident response.

The ANY.RUN team

ANYRUN FZCO

+1 657-366-5050

[email us here](#)

Visit us on social media:

[X](#)

[LinkedIn](#)

---

This press release can be viewed online at: <https://www.einpresswire.com/article/765430523>

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.