

# GuLoader Downloaded: A Look at the Latest Iteration

By Adi Bleih

Published: 2024-03-11 · Archived: 2026-04-05 15:35:28 UTC

## What is GuLoader?

GuLoader stands out as a prominent downloader founded on shellcode that has been used in many attacks aimed at spreading a diverse array of highly sought-after malware strains.

For over three years, GuLoader has maintained its activity and is continuously evolving through ongoing development efforts. The latest iteration introduces novel anti-analysis techniques, making its analysis extremely difficult. The recent GuLoader samples consistently receive zero detections on VirusTotal, concealing its malevolent payloads.

GuLoader adopts a strategy of complete encryption, including PE headers, for its payload. This tactical approach enables threat actors to stockpile payloads on widely recognized public cloud services. This circumvents the safeguards of antivirus solutions, and preserves the availability of these payloads for extended periods.

In its earlier manifestations, GuLoader took the form of VB6 applications that contained encrypted shellcode. Now, the prevalent versions predominantly use VBScript and the NSIS installer. The VBScript variant stores the shellcode on a remote server as part of its configuration.

## GuLoader Delivery Methods

GuLoader is written in encrypted shellcode wrapped in a Visual Basic 6 (VB6) executable. Notably, it stores second-stage payloads in cloud drive services. Usually, in Google Drive or Microsoft OneDrive. This way, it can establish a connection and download the executable without raising any red flags. The payload is usually encrypted, allowing it to slip past the cloud host's security measures.

The distribution method of GuLoader is very typical. The loader is usually delivered as an Office document attachment in spam email campaigns. When downloaded, it uses a macro to install the malicious program. Sometimes it is also delivered as an executable in a .rar archive.

During the pandemic, many campaigns exploited the fear surrounding Covid-19 by mentioning the virus. More recently, attackers have been using fake payment invoices. They will impersonate a bank and use social engineering to trick the victim into downloading an infected file to check "payment details."

## The Impact of GuLoader

GuLoader is available as a service for a relatively low price, can be easily found in the clearnet, and comes with easy-to-follow instructions. No wonder, then, that creators claim they already have over 5000 clients. Thanks to the combination of advanced anti-evasion tricks and ease of use, we expect its popularity to continue to grow.

The contribution made by malware loaders, often referred to as “crypters,” is of great significance in the propagation of Remote Administration Tools (RATs) and data-stealing malwares that target individual user information. The pilfered Personal Identifiable Information (PII) sourced from compromised endpoints is predominantly gathered and directed towards various underground data marketplaces for sale. This phenomenon has a cascading impact on enterprises, as critical authentication-related data is leaked from users’ personal devices, consequently granting unauthorized access to corporate networks.

GuLoader is extensively utilized within large-scale malware campaigns to infiltrate users’ systems with prevalent data-stealing malwares like Raccoon, Vidar, and Redline. Additionally, these campaign activities are also responsible for disseminating commodity RATs like Remcos.

---

Source: <https://cyberint.com/blog/other/guloader-downloaded-a-look-at-the-latest-iteration/>