


# New Rugmi Malware Loader Surges with Hundreds of Daily Detections

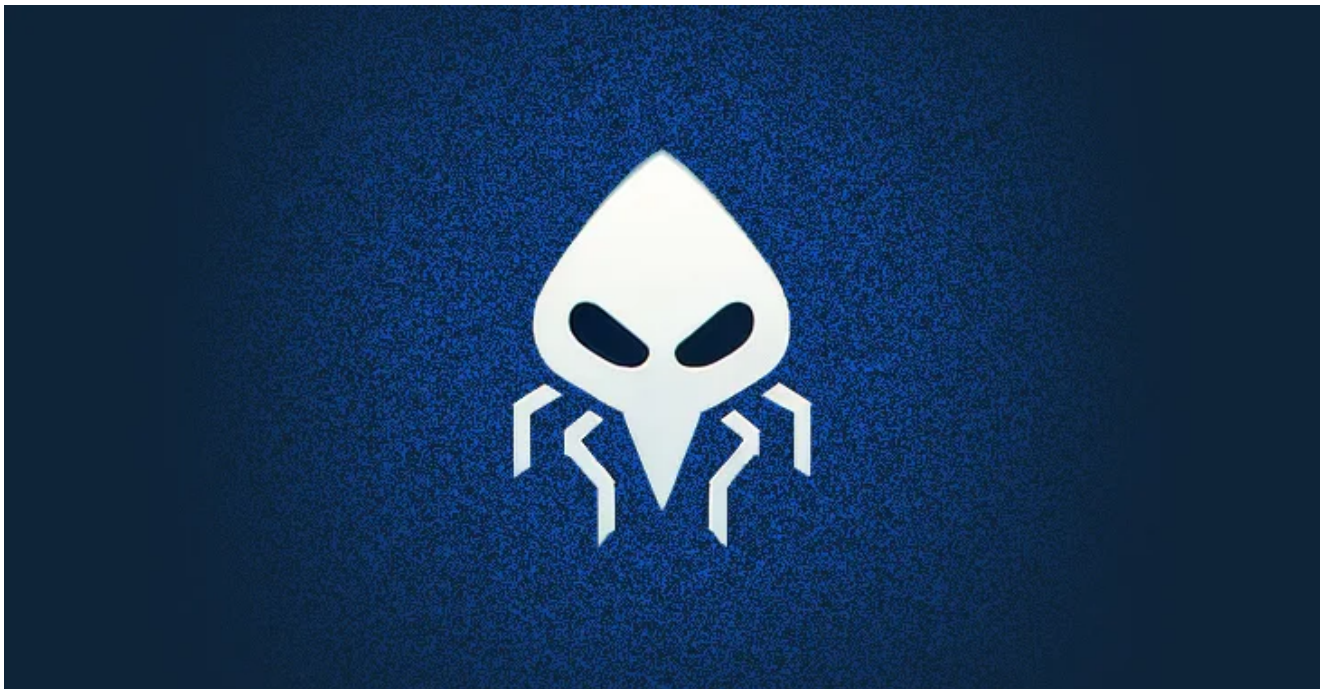
thehackernews.com/2023/12/new-rugmi-malware-loader-surges-with.html

December 28, 2023



WIZ+ Keep your cloud-native apps safe

Download now



A new malware loader is being used by threat actors to deliver a wide range of information stealers such as Lumma Stealer (aka LummaC2), Vidar, RecordBreaker (aka Raccoon Stealer V2), and Rescoms.

Cybersecurity firm ESET is tracking the trojan under the name **Win/TrojanDownloader.Rugmi**.

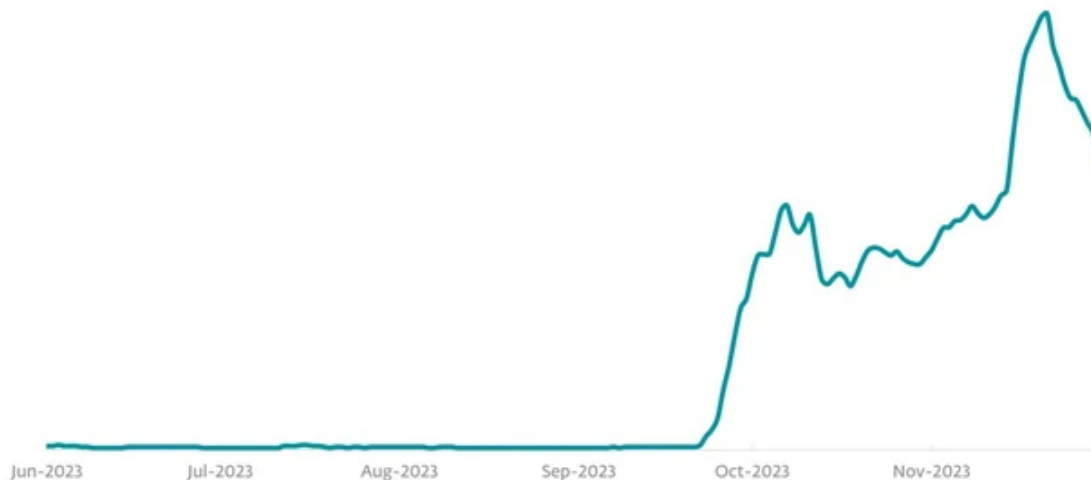
"This malware is a loader with three types of components: a downloader that downloads an encrypted payload, a loader that runs the payload from internal resources, and another loader that runs the payload from an external file on the disk," the company said in its Threat Report H2 2023.

Telemetry data gathered by the company shows that detections for the Rugmi loader spiked in October and November 2023, surging from single digit daily numbers to hundreds per day.

Stealer malware is typically sold under a malware-as-a-service (MaaS) model to other threat actors on a subscription basis. Lumma Stealer, for instance, is advertised in underground forums for \$250 a month. The most expensive plan costs \$20,000, but it also gives the customers access to the source code and the right to sell it.

There is evidence to suggest that the codebase associated with Mars, Arkei, and Vidar stealers has been repurposed to create Lumma.

Besides continuously adapting its tactics to evade detection, the off-the-shelf tool is distributed through a variety of methods ranging from malvertising to fake browser updates to cracked installations of popular software such as VLC media player and OpenAI ChatGPT.



### **Win/TrojanDownloader.Rugmi detection trend** in H2 2023, seven-day moving average

Another technique concerns the use of Discord's content delivery network (CDN) to host and propagate the malware, as revealed by Trend Micro in October 2023.

This entails leveraging a combination of random and compromised Discord accounts to send direct messages to prospective targets, offering them \$10 or a Discord Nitro subscription in exchange for their assistance on a project.

Users who agree to the offer are then urged to download an executable file hosted on Discord CDN that masquerades as iMagic Inventory but, in reality, contains the Lumma Stealer payload.

"Ready-made malware solutions contribute to the proliferation of malicious campaigns because they make the malware available even to potentially less technically skilled threat actors," ESET said.



"Offering a broader range of functions then serves to render Lumma Stealer even more attractive as a product."

The disclosures come as McAfee Labs disclosed a new variant of NetSupport RAT, which emerged from its legitimate progenitor NetSupport Manager and has since been put to use by initial access brokers to gather information and perform additional actions on victims of interest.

"The infection begins with obfuscated JavaScript files, serving as the initial point of entry for the malware," McAfee said, adding it highlights the "evolving tactics employed by cybercriminals."

The execution of the JavaScript file advances the attack chain by running PowerShell commands to retrieve the remote control and stealer malware from an actor-controlled server. The campaign's primary targets include the U.S. and Canada.

Found this article interesting? Follow us on Twitter and LinkedIn to read more exclusive content we post.

SHARE \_ \_ \_ \_

SHARE

Cybercriminal, cybersecurity, Discord, Malware Loader, Malware-as-a-Service, source code