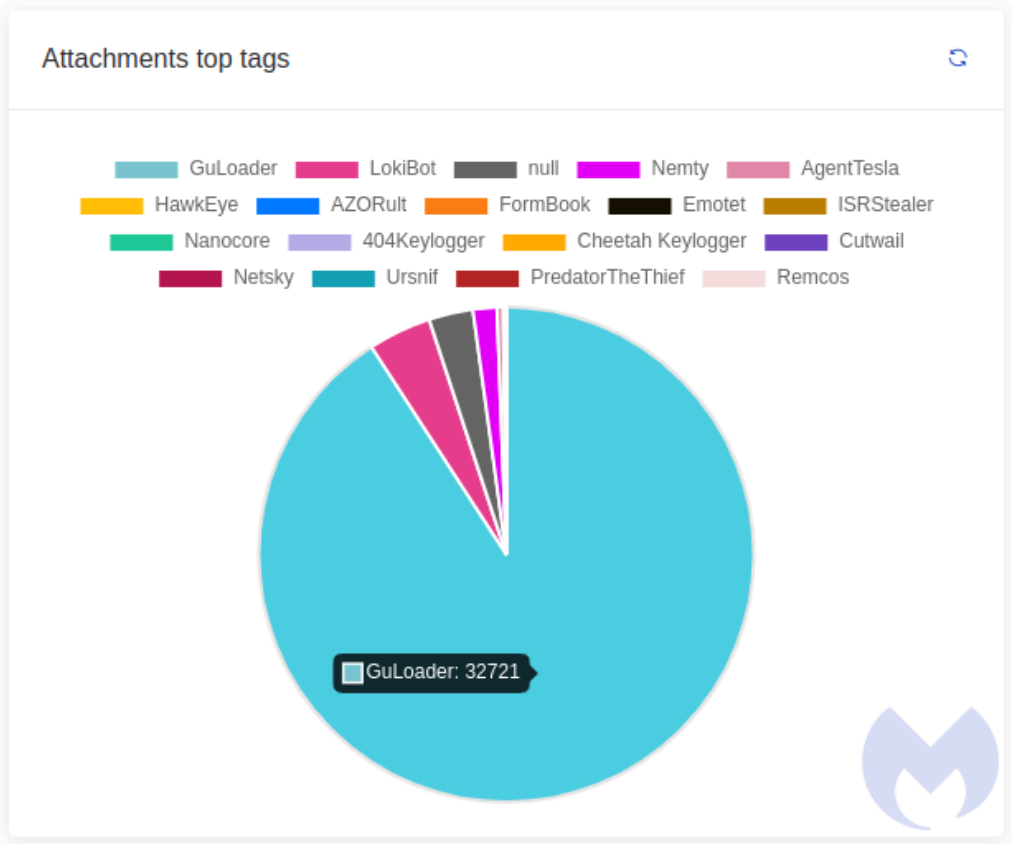
GuLoader returns with a rotten shipment

By Christopher Boyd

Published: 2023-04-24 · Archived: 2026-04-05 20:03:18 UTC

GuLoader, a perennial favourite of email-based malware campaigns since 2019, has been seen in the wild once again. GuLoader is a downloader with a chequered history, dating back to somewhere around 2011 in various forms. Two years ago it was one of our most seen malspam attachments.

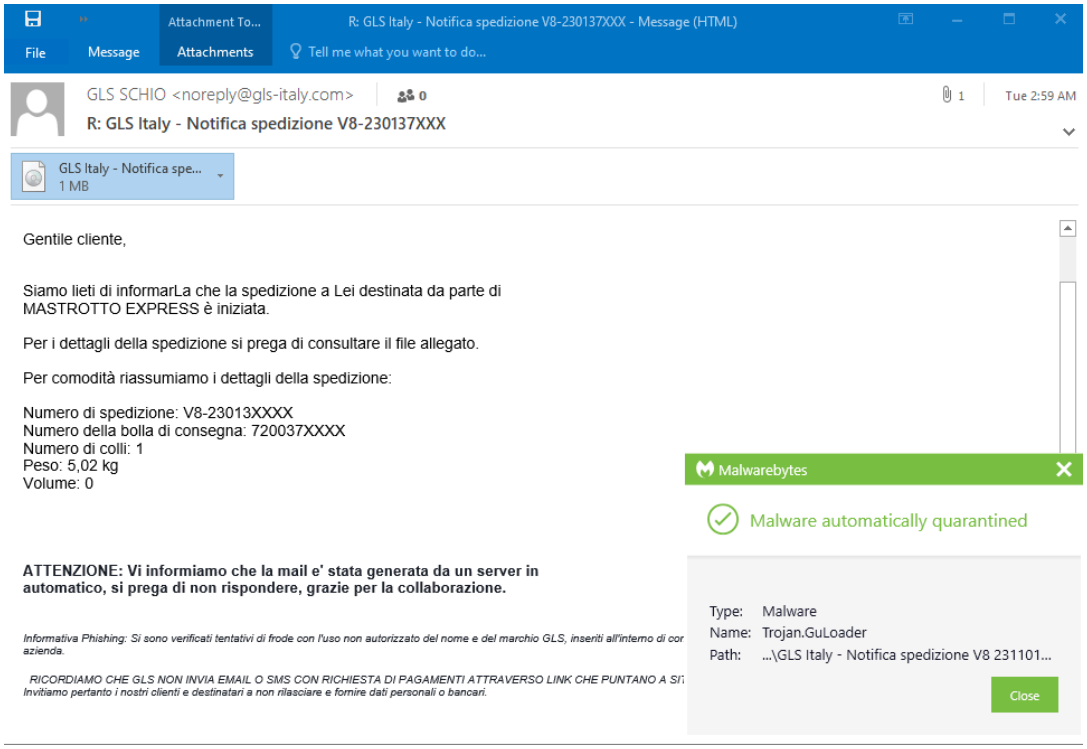


Most popular attachments by tags in Malwarebytes email telemetry

We also saw it during the pandemic, masquerading as a health e-book sent from the World Health Organisation.

GuLoader is typically used to load in the payload for the campaign in question. It often arrives in a ZIP file, and once opened and the file inside is executed the malicious activity begins. It may attempt to download data stealers, trojans, generic forms of malware…whatever is required. On top of this, GuLoader is designed to evade network detection and sneak past sandbox technology. For example, it may recognise being loaded up inside a virtual testing machine and refuse to load.

In this case, we have a bogus shipping notification written in Italian.



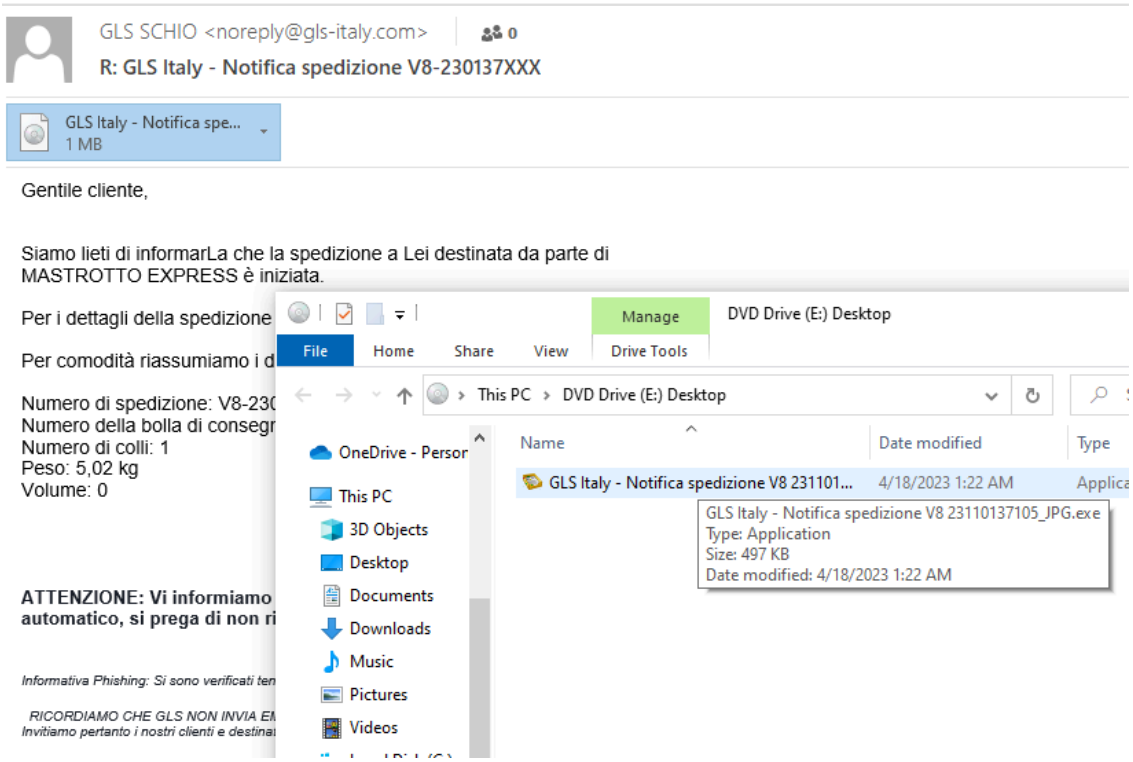
This is somewhat humorous given GuLoader's Italian origins. The mail, titled "Shipment Notification", reads as follows:

> Dear Customer,
>
> We are pleased to inform you that the shipment to you by Mastrotto Express has begun. For shipping details, please see the attached file. For convenience, we summarise the details of the shipment:
>
> Shipping number:
>
> Delivery note number:
>
> Number of packages:
>
> Weight:
>
> Volume:
>
> We inform you that the email was automatically generated by a server, please do not reply, thanks for your cooperation.

In this example, GuLoader is not hidden inside a Zip file. Instead, the attachment is an .ISO file. An .ISO is designed to be a copy of a DVD, a CD, and other related forms of media. If you ever spent some time backing up your CD collection to a computer, you probably have a lot of these in a folder somewhere.

The file (or image, as they're also sometimes called) would then be mounted as a virtual drive to gain access to the content. You could also just use a program like WinZip to open the files. However you do it, in this case the only thing waiting inside is GuLoader taking the form of a fake .JPG file. Note the .EXE (executable) extension in

the below screenshot. Pretending that an executable is an image by giving it a double extension is an incredibly old trick. On the other hand, it works!

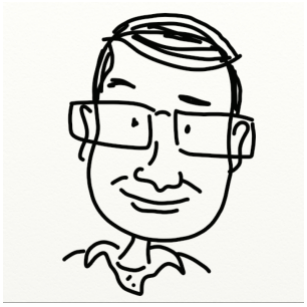


How to avoid fake parcel scams

- **Check your orders**. The email isn't going anywhere, and neither is your order. You have plenty of time to see if you recognise parcel details, and also the delivery network.
- **Avoid attachments**. So-called invoices or shipping details enclosed in a ZIP file should be treated with suspicion.
- **Watch out for a sense of urgency**. Be wary of anything applying pressure to make you perform a task. A missing payment and only 24 hours to make it? A time-sensitive refund? Mysterious shipping charges? All are designed to hurry you into making a decision.
- If in doubt, make contact with the company directly via official channels.

Thanks to Jerome for sending over.

About the author



Former Director of Research at FaceTime Security Labs. He has a very particular set of skills. Skills that make him a nightmare for threats like you.
