Case: Malicious ISO Attachment / GuLoader Loader

1. Executive Summary

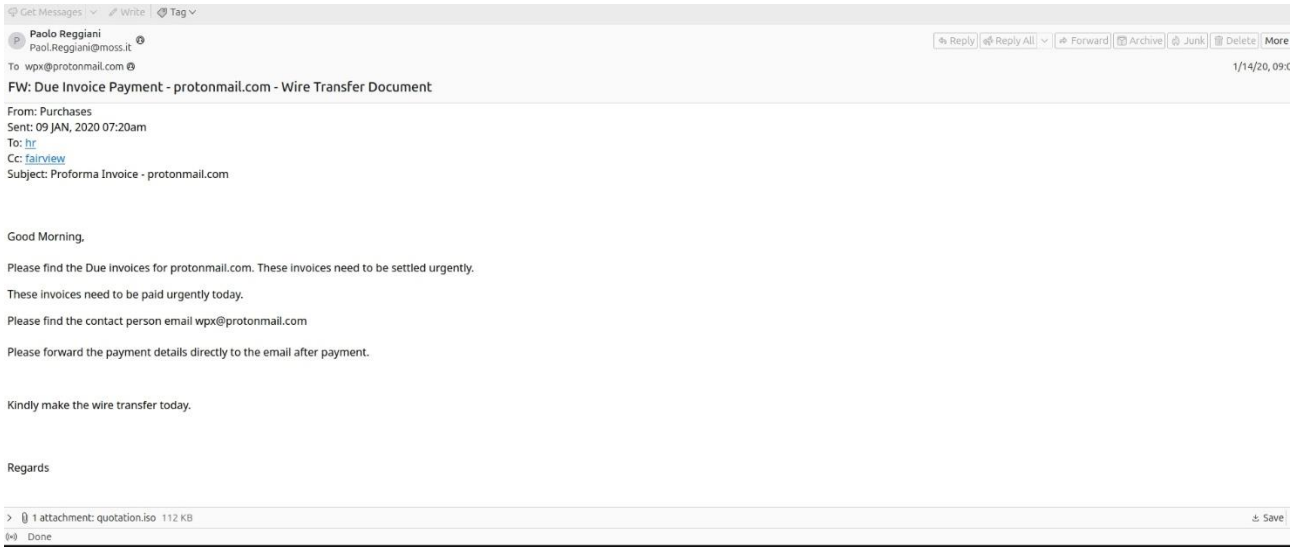
This report analyzes a suspicious email containing an ISO file attachment, which was found to be part of a targeted malware campaign delivering a loader known as GuLoader. The malicious payload was confirmed by multiple antivirus platforms.
Key investigation steps including analysis of the email, attachment, and threat intelligence have been documented.

2. Case Overview

- The analysis date is October 27, 2025.
- The threat type is a targeted malware campaign using a loader disguised as an ISO attachment.
- The attacker aims to steal funds or credentials by tricking the user into running the malicious ISO

3. Email Visual Appearance

When the email was opened in the user's mailbox client, it presented as a financial business request with a sense of urgency to transfer funds. The ISO file was presented as a legitimate financial document named "quotation.iso."

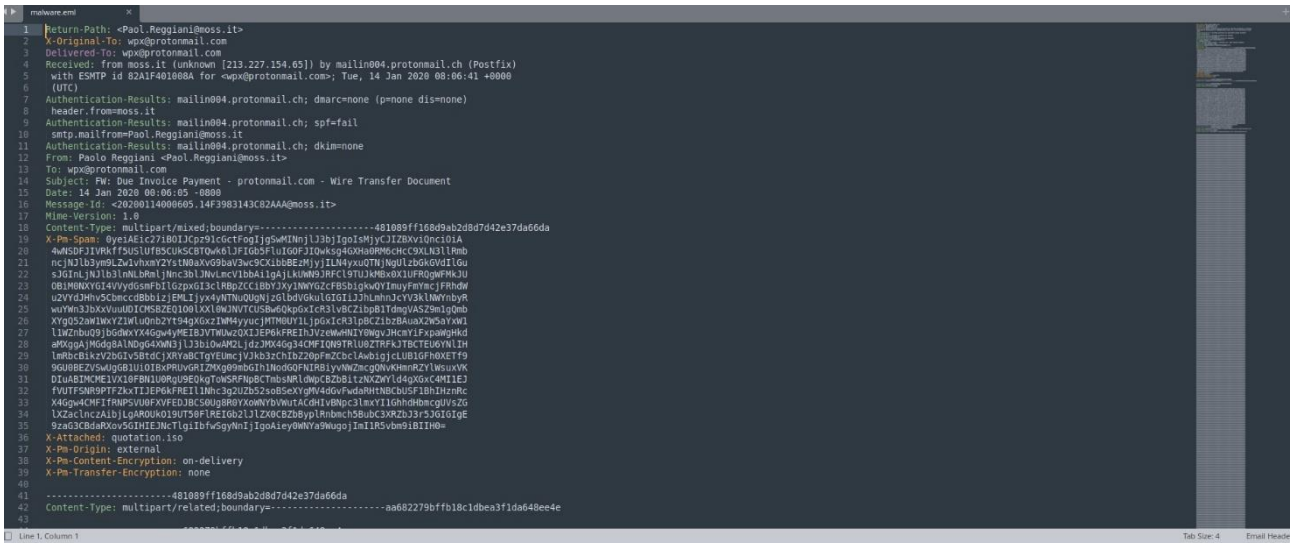


The email used professional tone and references typical in business wire transfer requests, increasing the chance the recipient would trust it.

4. Email Header and Technical Analysis

A detailed review of the raw headers showed:

- The sender was "Paolo Reggiani" with the spoofed email address Paol.Reggiani@moss.it.
- The recipient was wpx@protonmail.com.
- The Return-Path value matched the 'From' address, so no anomaly was detected here. However, other authentication checks (SPF, DKIM, DMARC) failed, confirming spoofing and suspicious origins.



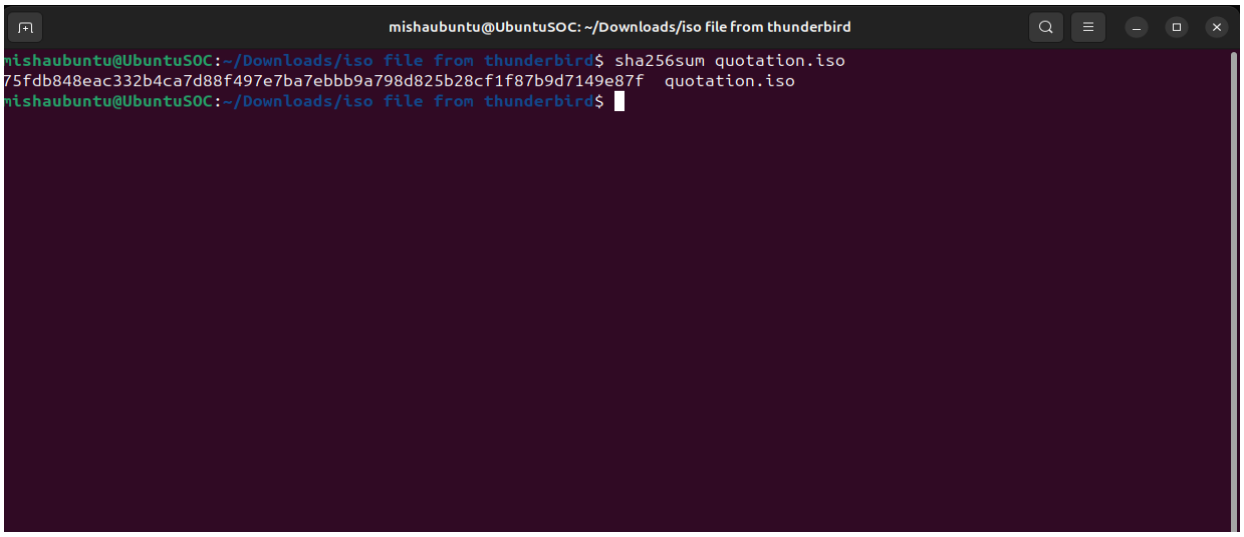
```
malware.eml
Return-Path: <Paol.Reggiani@moss.it>
X-Original-To: wpx@protonmail.com
Delivered-To: wpx@protonmail.com
Received: from moss.it (unknown [213.227.154.65]) by mailin004.protonmail.ch (Postfix)
 with ESMTP id 82A1F401008A for <wpx@protonmail.com>; Tue, 14 Jan 2020 08:06:41 +0000
 (UTC)
Authentication-Results: mailin004.protonmail.ch; dmarc=none (p=none dis=none)
 header.from=moss.it
Authentication-Results: mailin004.protonmail.ch; spf=fail
 smtp.mailfrom=Paol.Reggiani@moss.it
Authentication-Results: mailin004.protonmail.ch; dkim=none
From: Paolo Reggiani <Paol.Reggiani@moss.it>
To: wpx@protonmail.com
Subject: FW: Due Invoice Payment - protonmail.com - Wire Transfer Document
Date: 14 Jan 2020 00:06:05 -0800
Message-Id: <20200114000605.14F3983143C82AAA@moss.it>
Mime-Version: 1.0
Content-Type: multipart/mixed;boundary="--------------------481089ff168d9ab2d8d7d42e37da66da
X-Pm-Spam: 0yeiAEic27iBOIJCpz91cGctFoqIjg5wMINnjlJ3bjIgoIsMjyCJIZBXviQnciOiA
 4wNSDFJIVRkff5USlUfB5CUkSCBTQwK6lJFIGb5FluIGOFJIQwksg4GXHa0RM6cHcC9XLN3llRmb
 ncjNJlb3ym9LZw1vhxmY2YstN0aXvG9baV3wc9CXibbBEzMjyjILN4yxuQTNjNgUlzbGkGVdIlGu
 sJGInLjNJlb3lnNLbRmljNnc3blJNvLmcV1bbAilgAjLkUWN9JRFcl9TUJkMBx0X1UFRQgWFMkJU
 OBlM0NXYGI4VVydGsmFbIlGzpxGI3clRbpZCCi8bYJXylNNYGZcf05bigkwQYImuyFmYmcjFRhdW
 uZVYdJHhv5CbmccdBbbizjEMLIjyx4yNTNuQUqNjzGlbdVGkulGIGIiJhLmhnJcYV3kliNWYnbyR
 wuYWn3JbXxVuuUDICMSBZEQ1O0lXXl8WJNVTCUSBw6QkpGxIcR3lvBCZibpBlTdmqVASZ9m1gQmb
 XYgO52aW1WxYZ1WluQnb2Yt94gXGxzIWM4yyucjMTM0UY1LjpGxIcR3lpBCZibzBAuaX2W5aYxW1
 l1WZnbuQ9jbGdWxYX4Ggw4yMEIBJVTWUwzQXIJEP6kFREIhJVzeWwHNIY0WgvJHcmYiFxpaWgHkd
 aMXgqAjMGdg8AlNDgG4XWN3jlJ3biOwAM2LjdzJMX4Gg34CMFIQN9TRlU0ZTRFkJTBCTEU6YNlIH
 lmRbcBikzV2bGIv5BtdCjXRYaBCTgYEUmcjVJkb3zChIbZ2OpFmZCbclAwbigjcLUBlGFh0XETf9
 9GU0BEZV5WdgGB1Ui0IBxPRUvGRIZMXg09mbGIhlNodGQFNIRBiyxNWZmcgONvKHmRZYlWsuxYK
 DIuABIMCME1VX10FBN1U0RgU9E0kgToWSRFNpBCTmbsNRldWpCBZbBitzNXZWYld4gX6xC4MI1EJ
 fVUTFSNR9PTFZkxTIJEP6kFREIl1Nhc3q2UZb52soBSeXYgMV4dGvFwdaRHtNBCbU5F1BhIHznRc
 X4Ggw4CMFIfRNPSVU0FXVFEDJBCS0Ug8R0YXoWNYbVWutACdHIvBNpc3lmxYI1GhhdHbmcgUVsZG
 lXZaclnczAibjLgARO0Uk0I9UT50FlREIGb2lJlZX0CBZbByplRnbmch5BubC3XRZbJ3r5JGIGIgE
 9zaG3CBdaRXov5GIHIEJNcTlgiIbfw5gyNnIjIgoAiey0WNYa9WugojImIlR5vbm9iBIIH0=
X-Attached: quotation.iso
X-Pm-Origin: external
X-Pm-Content-Encryption: on-delivery
X-Pm-Transfer-Encryption: none

--------------------481089ff168d9ab2d8d7d42e37da66da
Content-Type: multipart/related;boundary="--------------------aa682279bffb18c1dbea3f1da648ee4e
```


5. Attachment Details and Hashing Process

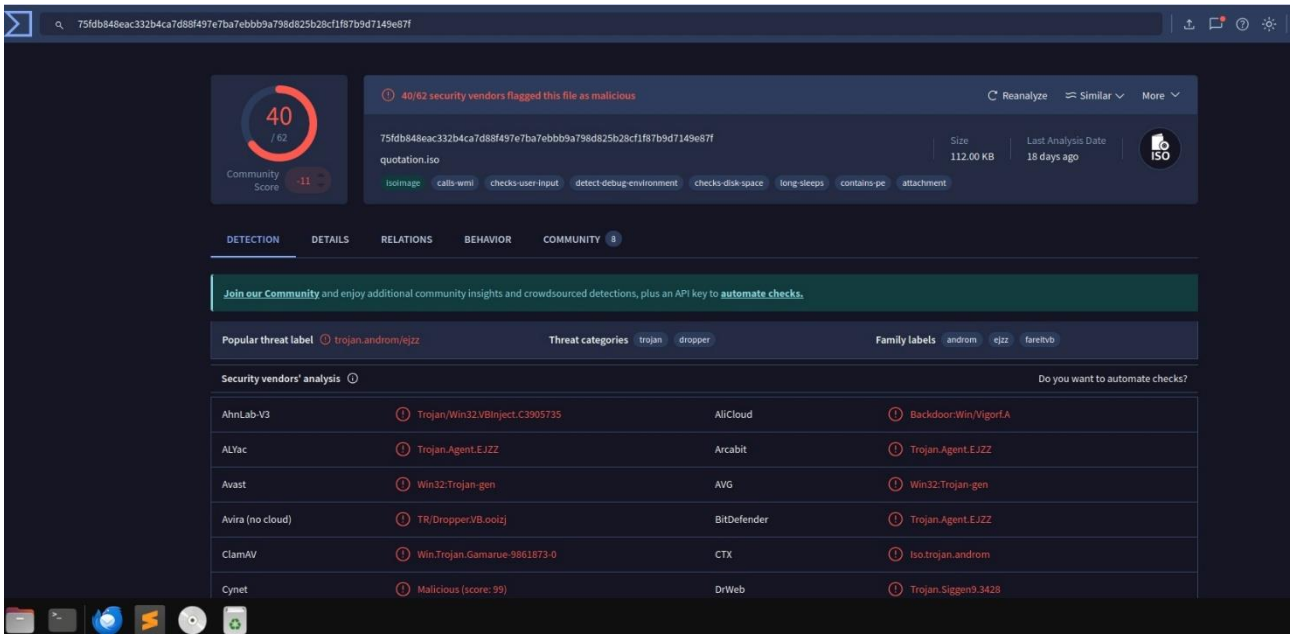
The attachment named "quotation.iso" was identified as an ISO CD-ROM image with a size of 112 KB.

Using Linux command line, the SHA256 hash of the file was calculated as: 75fdb848eac332b4ca7d88f497e7ba7ebbb9a798d825b28cf1f87b9d7149e87f



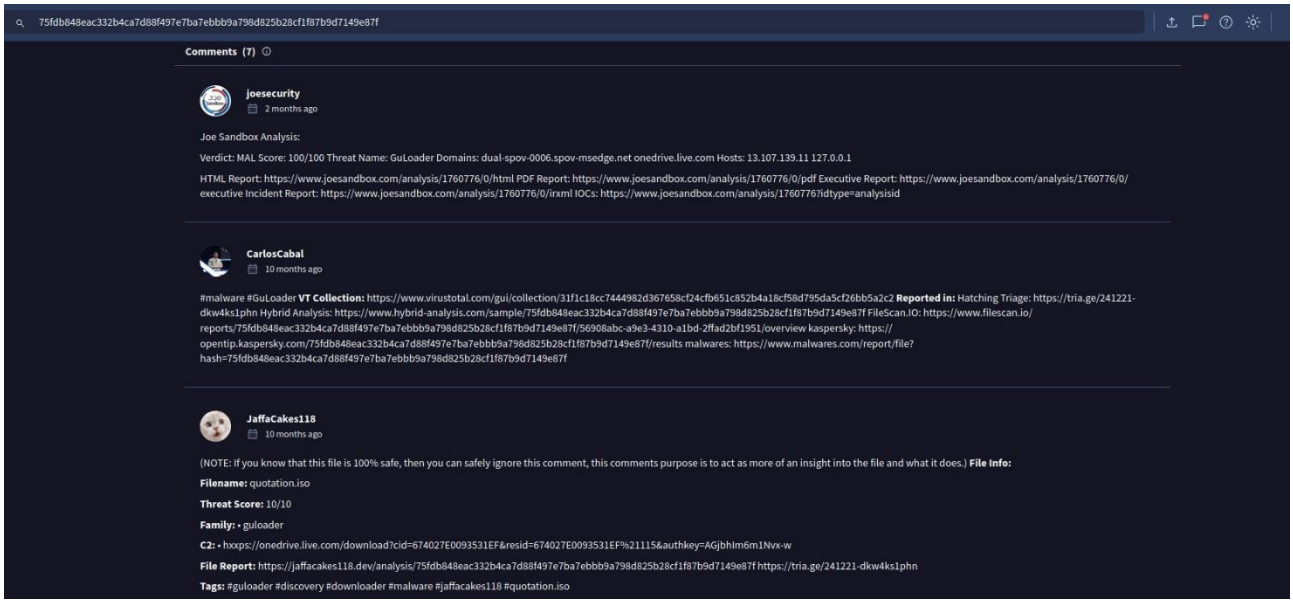
6. Malware Scanning and Threat Intelligence

VirusTotal results show that 40 out of 62 antivirus engines detected the file as malicious. Common detections included variant names such as Trojan.Agent.EJZZ, Trojan/Win32.VBInject, Backdoor:Win/Vigorf.A, and Iso.trajan.androm.



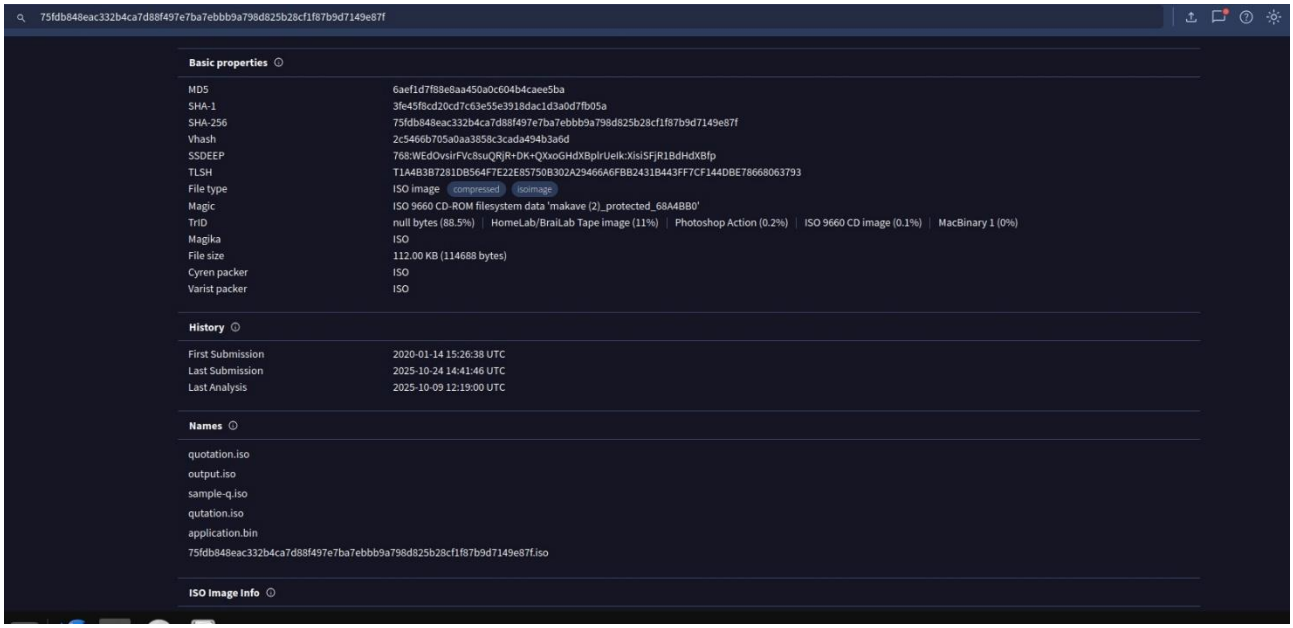
6.1 Community Threat Intelligence Insights

Analysis by the community confirms the file belongs to the GuLoader family, a well-known malware loader. Public sandbox links indicate connections to command-and-control infrastructure hosted on onedrive.live.com, demonstrating the file's capability for remote control and payload download.



7. File Properties and History

The file's metadata matches known characteristics of GuLoader samples, with consistent signatures, file size, and historical submissions on malware databases dating back to early 2020. The file has been reanalyzed as late as October 2025, confirming its ongoing use.



8. Attack Technique Explanation

Attackers use ISO attachments to bypass some antivirus email gateways that struggle to inspect ISO container files thoroughly. The social engineering element is strong, with spoofed senders, business-like language, and urgent financial requests to motivate opening the file, which triggers malware deployment.

9. Indicators of Compromise (IOCs)

The key IOCs for monitoring and blocking are:

- Spoofed email sender: Paol.Reggiani@moss.it
- Targeted recipient: wpx@protonmail.com
- Malicious file hash (SHA256): 75fdb848eac332b4ca7d88f497e7ba7ebbb9a798d825b28cf1f87b9d7149e87f
- Command and control domain: onedrive.live.com
- Related malicious domains and IPs referenced in VirusTotal community analysis

10. Conclusion and Recommendations

The email is a sophisticated threat delivering a GuLoader malware loader through an ISO file disguised as a financial quotation. This method relies on social engineering and attachment obfuscation to infect targets.

Actions recommended include:

- Never opening or mounting the ISO attachment.
- Blocking the known malicious hash on endpoint protection platforms.
- Alerting users to avoid similar suspicious attachments.
- Monitoring network traffic for connections to identified C2 domains.
- Expanding user training on recognizing such business-related phishing attempts.