

Traffic-Analysis.net - 2024-03-07: Latrodectus infection leads to Lumma Stealer

Archived: 2026-04-05 23:43:56 UTC

NOTES:

- Zip files are password-protected. Of note, this site has a new password scheme. For the password, see the "about" page of this website.

REFERENCES:

- https://www.linkedin.com/posts/unit42_latrodectus-lummastealer-unit42threatintel-activity-7172007697196810240-gBxT
- https://twitter.com/Unit42_Intel/status/1766242077585596520

ASSOCIATED FILES:

- [2024-03-07-IOCs-for-Latrodectus-and-Lumma-Stealer.txt.zip](#) 2.7 kB (2,699 bytes)
- [2024-03-07-Latrodectus-malspam-1800UTC.eml.zip](#) 3.9 kB (3,914 bytes)
- [2024-03-07-Latrodectus-infection-with-Lumma-Stealer.pcap.zip](#) 25.8 MB (25,762,724 bytes)
- [2024-03-07-Latrodectus-and-Lumma-Stealer-malware-and-artifacts.zip](#) 5.4 MB (5,369,328 bytes)
- [2024-03-07-traffic-to-horaot.org.pcap.zip](#) 23.6 kB (23,591 bytes)

[Click here](#) to return to the main page.

Source: <https://www.malware-traffic-analysis.net/2024/03/07/index.html>