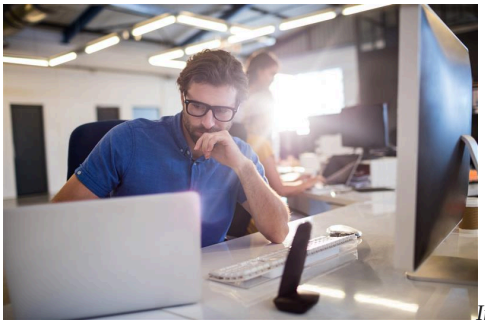
Loki Info Stealer Propagates through LZH Files

Archived: 2026-04-05 20:28:38 UTC



Insights and analysis by Miguel Ang

LZH files, more commonly used in Japan for compressing files, have also been used to deliver other malware such as Negasteal and Ave Maria.

The malicious LZH file attachment comes from an email posing as a payment confirmation advice from a bank. The attachment is named “payment confirmation.lzh”.

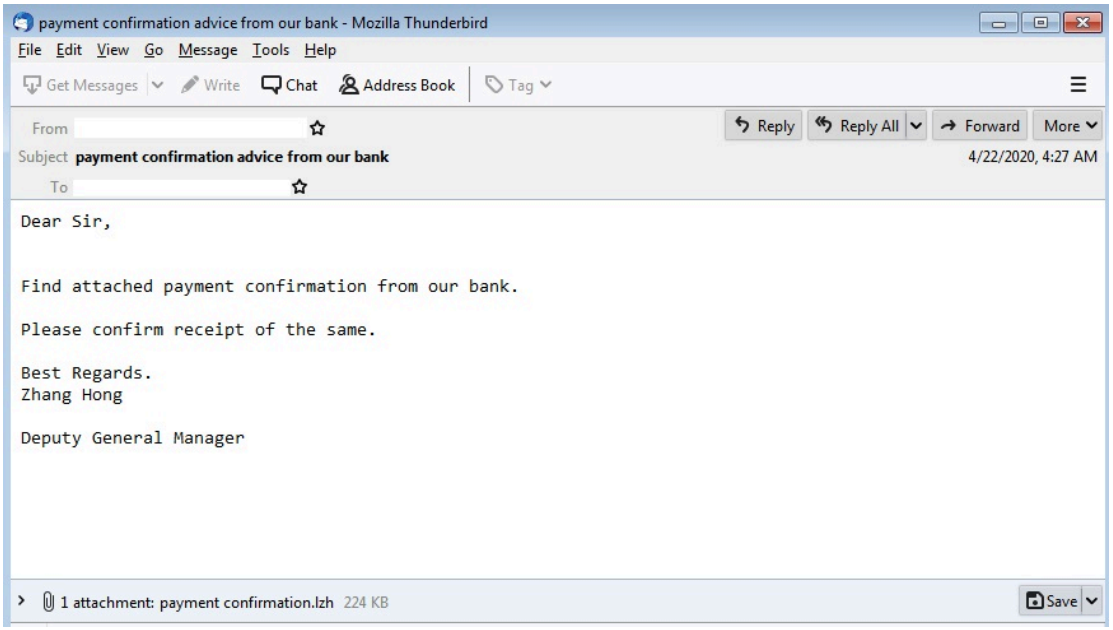


Figure 1. Sample email delivering Loki through LZH attachment

The LZH archive attachment contained the Loki dropper named bFbnF2vovw15SVM.exe. It also has a folder named “crypted_files,” which contains an empty folder named “myself_crypted” inside. This was either the result of an error in archiving the sample or was meant to be used to contain additional components or payloads.

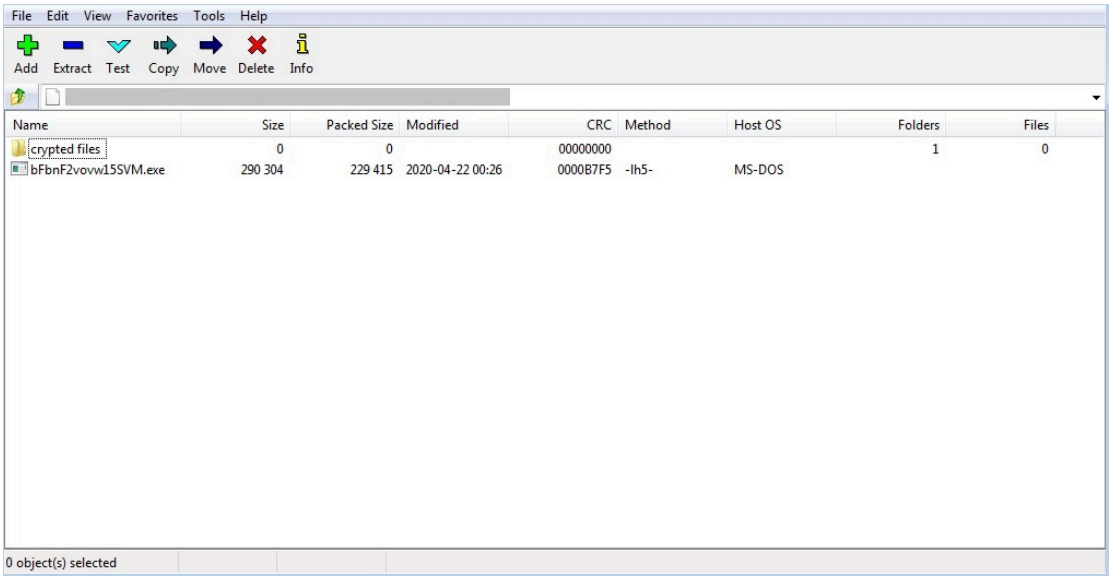


Figure 2. Attachment contents

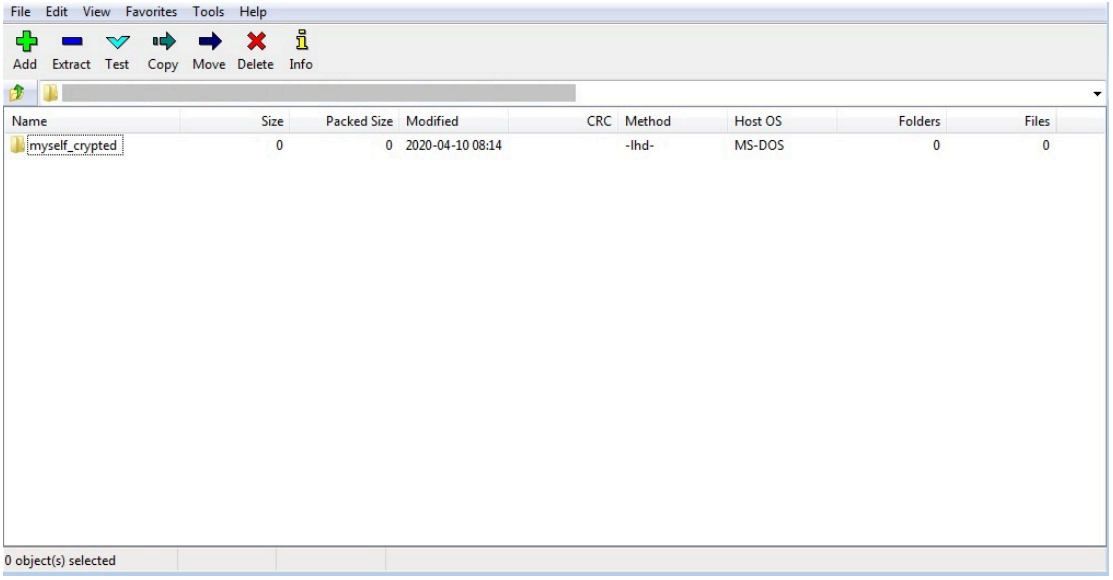


Figure 3. Contents of the “crypted files” folder

The Loki dropper uses .NET compiled binaries to add multiple layers of obfuscation. It eventually uses process hollowing to load and execute the main Loki payload. This method is reminiscent of the campaign that propagates Loki through CAB file attachmentsnews- cybercrime-and-digital-threats. The main Loki payload that it drops also has the same hash as the variant concealed through CAB files, indicating that both samples are under the same ongoing campaign.

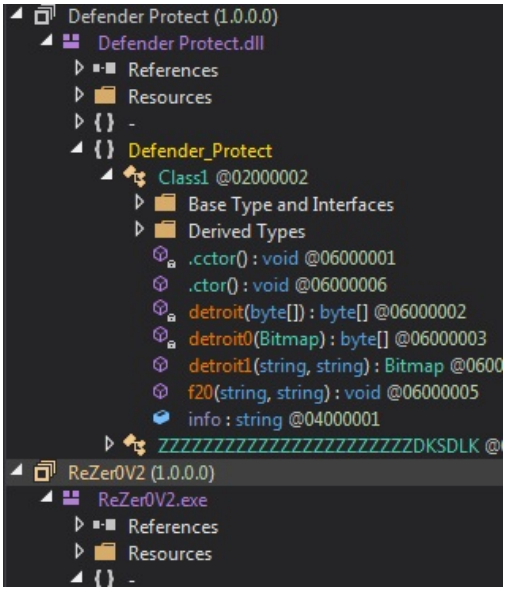


Figure 4. Obfuscated compiled binaries

Detachment from malicious files

Cybercriminals can use a variety of file attachments to spread malware, ranging from more common file types like Word Document or PDF, to less familiar ones like CAB or LZH files. Regardless of the file type used to conceal it, the fact remains that malware can compromise systems, disrupt device performance, or steal data. The following best practicesnews-cybercrime-and-digital-threats can help prevent malware infections:

- Do not download attachments or click links on emails from unknown sources. This may lead to the installation of malware. Users may check where the embedded links lead to by hovering the pointer over the link.
- Read emails carefully to gauge the credibility of its contents. Some giveaway signs of spam are bad grammar, misspelled words, and unfamiliar or spoofed email addresses.
- Avoid sharing contact details and other sensitive information on public web forums or social media.

For a more proactive defense against threats that use emails as entry points, the following solutions are recommended:

- Trend Micro™ Deep Discovery™ Email Inspectorproducts – Stops email-based threats including spam, ransomware, and targeted attacks through advanced analysis and custom sandboxing.
- Trend Micro™ Email Securityproducts – Employs sandbox for unknown files and URL, email sender analysis and authentication, and checking of email header and content for signs of compromise.
- Trend Micro™ Cloud App Securityproducts – Protects file sharing from malware and controls sensitive data usage.

Indicators of Compromise

URL

hxxp://retrak.co[.]ke/psy/five/fre.php

File Name	SHA-256	Trend Micro Pattern Detection
bFbnF2vovw15SVM.exe	e6adc1df97033110cdf1bd9e9763559fe17811e2234013e4d57fa23b6ddbb207	TrojanSpy.Win32.LOKI.TI
payment confirmation.lzh	fb37c52635a47cacba754f811ec64937aa6da3c0ced0162c201748b38952e164	TrojanSpy.Win32.LOKI.TI

HIDE

Like it? Add this infographic to your site:

1. Click on the box below. 2. Press Ctrl+A to select all. 3. Press Ctrl+C to copy. 4. Paste the code into your page (Ctrl+V).

Image will appear the same size as you see above.

We Recommend

-
-
-
-

- The Industrialization of Botnets: Automation and Scale as a New Threat Infrastructurenews article
- Complexity and Visibility Gaps in Power Automatenews article
- Cracking the Isolation: Novel Docker Desktop VM Escape Techniques Under WSL2news article
- Azure Control Plane Threat Detection With TrendAI Vision One™news article
- The AI-fication of Cyberthreats: Trend Micro Security Predictions for 2026predictions
- Ransomware Spotlight: DragonForcenews article
- Stay Ahead of AI Threats: Secure LLM Applications With Trend Vision Onenews article
- The Road to Agentic AI: Navigating Architecture, Threats, and Solutionsnews article

---

Source: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/loki-info-stealer-propagates-through-lzh-files