IMPORTANT CYBERSECURITY NEWS: FAKE BOOKING WEBSITES USED TO SPREAD LUMMASTEALER MALWARE

Vairav Cyber Security News Report

Date: March 05, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

EXECUTIVE SUMMARY

A new malvertising campaign has been discovered leveraging fraudulent booking websites to distribute LummaStealer, an info-stealer malware operating under the Malware-as-a-Service (MaaS) model. Researchers at G DATA identified this global campaign using fake travel itinerary pages and deceptive CAPTCHA prompts to infect unsuspecting users. Attackers trick victims into executing PowerShell commands, enabling LummaStealer to steal credentials, banking information, and cryptocurrency wallets. This evolving malware now incorporates advanced evasion techniques, making detection more challenging.

INCIDENT ANALYSIS

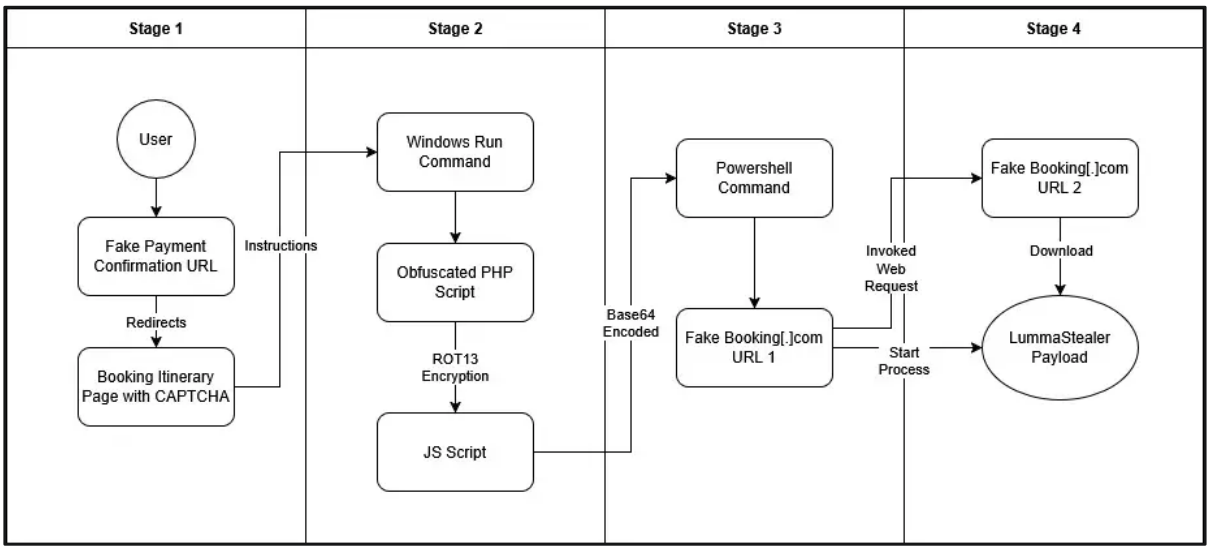

Figure 1: Lumma stealer infection chain

Threat actors have shifted their delivery tactics from traditional platforms like GitHub and Telegram to fake online booking confirmations. Victims searching for travel accommodation are lured into malicious sites that display CAPTCHA verification prompts. Instead of validating the user, these prompts initiate a PowerShell command that downloads LummaStealer.

Key Observations:

1. Global Targeting – Initial infections were observed in Palawan, Philippines, before shifting to Munich, Germany, indicating a worldwide campaign.
2. Increased Malware Complexity – The latest version of LummaStealer has grown by 350% (from 2MB to 9MB), likely due to new evasion features.
3. Advanced Obfuscation Techniques:

- Binary Padding – Inflating file size to bypass antivirus detection thresholds.
- Indirect Control Flow Obfuscation – Using Dispatcher Blocks to alter execution paths dynamically, complicating analysis.

LummaStealer's rapid evolution suggests it may soon mimic malware families like Emotet, known for their adaptive attack methods and widespread impact. The weaponization of fake booking platforms to distribute LummaStealer marks a shift in cybercriminal tactics. As threat actors refine their evasion techniques, organizations and users must adopt enhanced security measures to prevent malware infections. Travel-related scams are expected to rise, reinforcing the need for vigilance against phishing and malvertising campaigns.

RECOMMENDED ACTIONS

- Always book travel through official websites, avoiding unknown third-party platforms.
- If a travel website asks you to run a command or download a file, do not proceed.
- Disable PowerShell for non-administrative users to prevent script-based infections.
- Use behavior-based antivirus solutions to detect obfuscation techniques used by LummaStealer.
- Regularly update security tools with Indicators of Compromise (IoCs) related to LummaStealer's infrastructure.

RESOURCES

https://securityonline.info/lummastealer-expands-attack-surface-with-fake-booking-sites-and-captcha-tricks/

https://www.gdatasoftware.com/blog/2025/03/38154-lummastealer-fake-recaptcha

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com