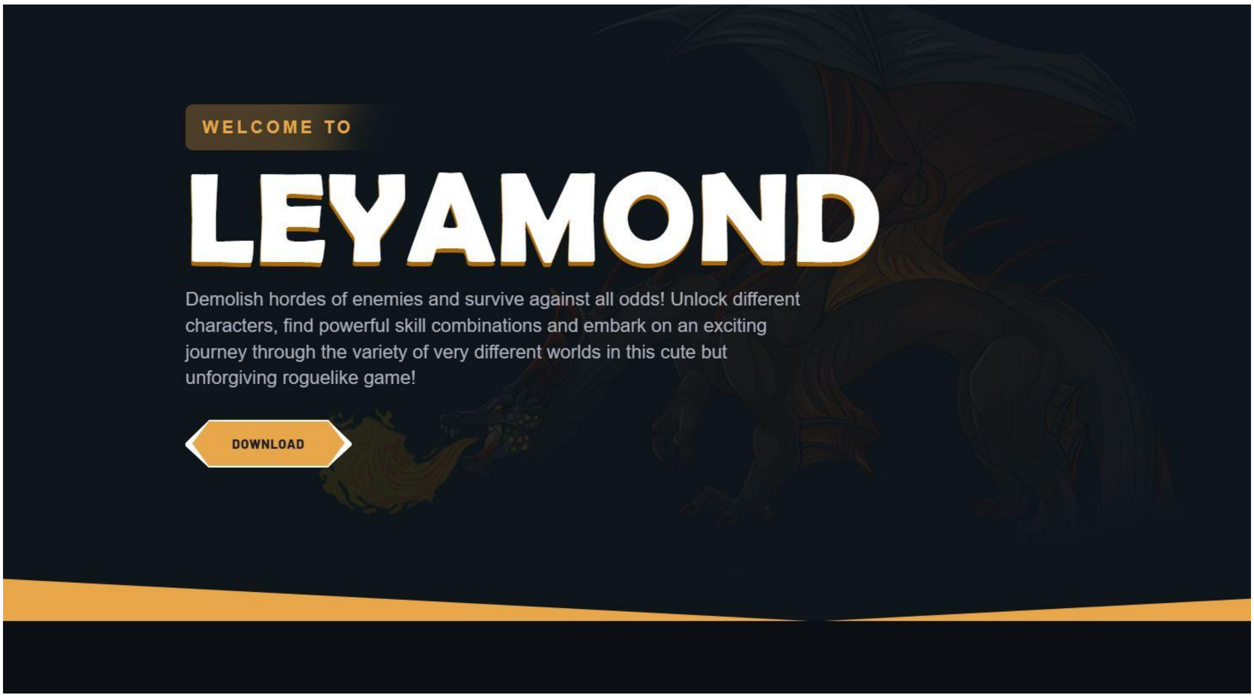
*January 06, 2025*

# Discord Phishing Scam: Trojan Distribution Under the Guise of Game Beta Testing

**Overview:** A malicious phishing campaign is making its rounds across multiple platforms, primarily targeting Discord users but also spreading through email and text messages. Victims receive messages from alleged game developers offering a chance to beta-test a new video game, often accompanied by a download link and a password for the installer archive. Unfortunately, the files being offered are not game installers, but information-stealing Trojans like Nova Stealer, Ageo Stealer, and Hexon Stealer. These Trojans can steal sensitive information such as Discord tokens, session cookies, saved passwords, credit card details, and even cryptocurrency wallet information. The goal of these attacks is primarily financial, using stolen credentials and trust to expand the network of compromised accounts for further scams and malware distribution.

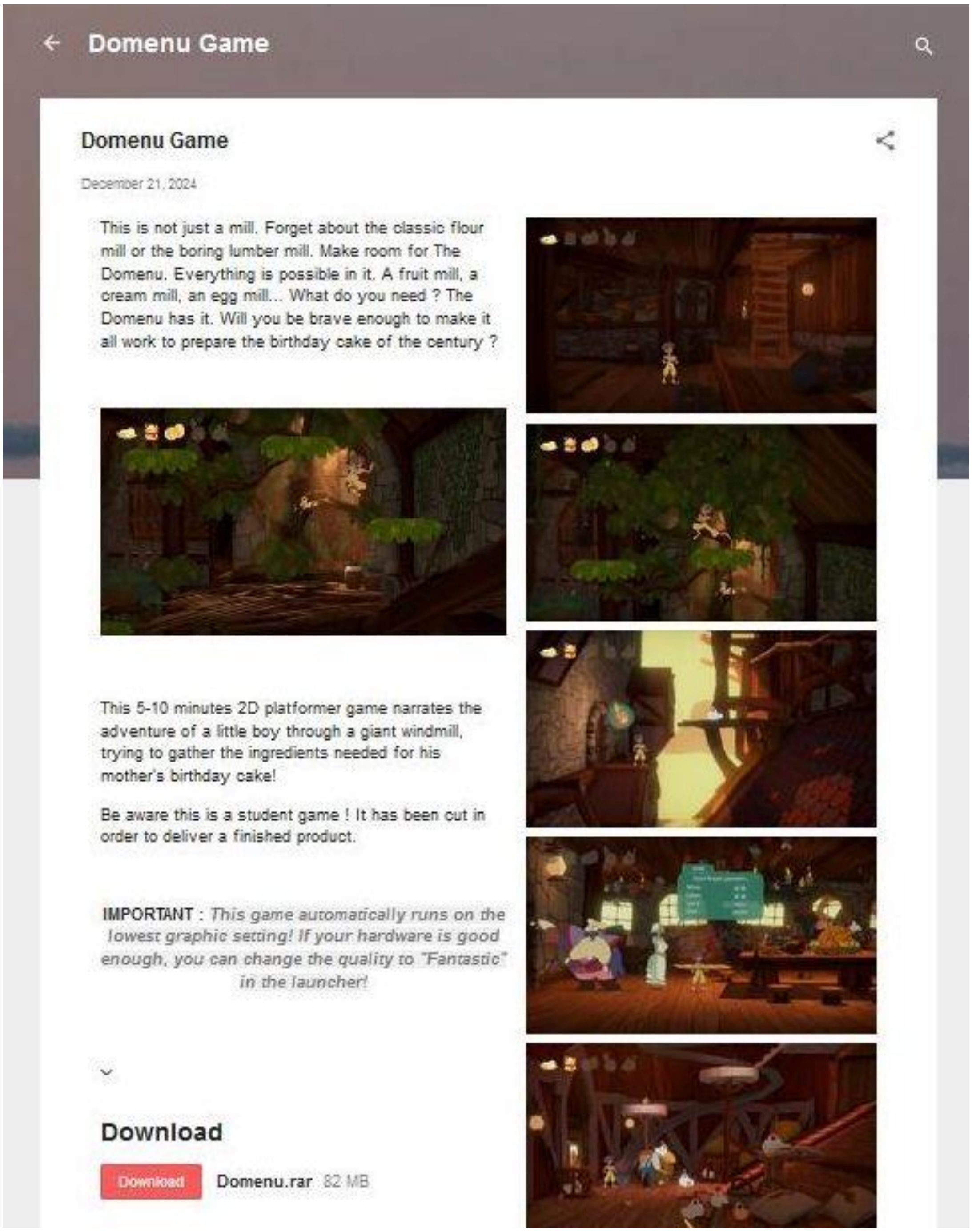
**CTI Analysis:** This attack leverages social engineering tactics, such as the promise of exclusive access to a beta game, which appeals to the target's curiosity and enthusiasm. The malicious files are distributed through platforms like Dropbox, compromised Discord accounts, and even Blogspot, lending legitimacy to the scam.



Demolish hordes of enemies and survive against all odds! Unlock different characters, find powerful skill combinations and embark on an exciting journey through the variety of very different worlds in this cute but unforgiving roguelike game!

*Figure 1: Example of the templated fake website*

These fake game sites are often hosted by companies that are unresponsive to takedown requests and are usually protected by Cloudflare, making it more difficult for researchers to shut them down. However, once a site is taken down, attackers can easily set up a new one. Additionally, Blogspot-hosted sites have a distinct design but still adhere to the same template strategy, making them another point of concern for unsuspecting users.



Domenu Game

This is not just a mill. Forget about the classic flour mill or the boring lumber mill. Make room for The Domenu. Everything is possible in it. A fruit mill, a cream mill, an egg mill... What do you need ? The Domenu has it. Will you be brave enough to make it all work to prepare the birthday cake of the century ?

This 5-10 minutes 2D platformer game narrates the adventure of a little boy through a giant windmill, trying to gather the ingredients needed for his mother's birthday cake!

Be aware this is a student game ! It has been cut in order to deliver a finished product.

**IMPORTANT** : *This game automatically runs on the lowest graphic setting! If your hardware is good enough, you can change the quality to "Fantastic" in the launcher!*

Download

*Figure 2: Blogpost template*

Attackers use these tactics to distribute information-stealing Trojans like Nova Stealer, Ageo Stealer, and Hexon Stealer, which exfiltrate sensitive data, including Discord credentials, session cookies, and cryptocurrency wallet details. The malware's infrastructure, such as Discord webhooks, allows attackers to monitor compromised accounts and receive instant alerts when new data is obtained, aiding in the expansion of their malicious network.

**Impact Analysis:** The impact of this scam is multifaceted. Initially, victims face the theft of personal data, including login credentials for various platforms. With a primary focus on Discord accounts, attackers gain access to an increasing number of compromised accounts, which can be leveraged to further spread the attack. These compromised accounts help scammers impersonate trusted friends or contacts, convincing other users to download malicious files or fall for phishing attempts. The long-term effect can also involve financial losses, especially in cases where sensitive data, such as cryptocurrency wallet details and credit card information, is stolen and misused. The rapid spread of this campaign across platforms like Discord and other commonly used file-sharing services increases the number of potential victims.

**Mitigations:**

- Always verify invitations to download files, especially from friends, through another communication channel (e.g., direct text or a different social media platform).
- Keep your anti-malware solution up to date and running, and scan for any unusual behavior or files.
- Avoid interacting with unsolicited messages that prompt you to download or install software.
- Be cautious when visiting websites that offer beta games, especially those with templated designs or hosted on suspicious platforms like Blogspot.
- Use two-factor authentication (2FA) on your accounts to minimize the risk of unauthorized access.

**Conclusion:** This growing phishing campaign highlights the importance of staying vigilant and cautious when interacting with unsolicited messages, especially those that seem to promise exclusive access to enticing opportunities. By recognizing suspicious patterns and using proper mitigation strategies, users can protect themselves from falling victim to these malicious Trojan campaigns. Always prioritize security, verify requests from trusted contacts, and keep software up to date to mitigate the risk of compromising personal and financial information.

**Source:**

https://www.infostealers.com/article/can-you-try-a-game-i-made-fake-game-sites-lead-to-information-stealers/

https://www.hendryadrian.com/web/?url=https://www.hendryadrian.com/can-you-try-a-game-i-made-fake-game-sites-lead-to-information-stealers/

https://www.malwarebytes.com/blog/news/2025/01/can-you-try-a-game-i-made-fake-game-sites-lead-to-information-stealers