H E A D Q U A R T E R S
ARMED FORCES OF THE PHILIPPINES CYBER COMMAND
Camp General Emilio Aguinaldo, Quezon City

CYBERSECURITY BULLETIN 2025-05

PupkinStealer Malware Target Windows Systems

Overview

Cybersecurity researchers have identified a new malware threat named PupkinStealer, first observed in April 2025, which is actively targeting Windows systems. Written in C# using the .NET framework. This lightweight 6.21MB executable is designed to steal login credentials, session tokens, and files from compromised machines.

Delivery methods of this malware are likely via email phishing, cracked software, or malware-as-a-service campaigns. Its stolen data includes: browser-stored credentials and cookies, telegram and discord session data, desktop files, active desktop screenshot and metadata such as username and IP address. Stolen data are compressed into a zip archive and sent via Telegram bots.

PupkinStealer does not establish long-term system persistence, enabling fast and stealthy data-theft operation. Exfiltration of stolen data via Telegram allows the malware to evade traditional detection methods by blending with legitimate traffic which makes it harder to detect.

Recommendations:

Following are the recommended actions to reduce exposure to the said malware:

1. **Block Telegram Bot API Communications**

Restrict access to suspicious Telegram-related traffic on organization's networks.

2. **Apply Multi-Factor Authentication (MFA)**

Implement MFA especially on critical applications and messaging platforms.

3. **Conduct Security Awareness Training**

Educate personnel on avoiding malware-laced attachments and phishing sites.

4. **Audit Access to Messaging Platforms**

Review permission and third-party access to messaging apps such as Telegram and Discord.

5. **Monitor for large ZIP Uploads**

Consider configuring Data Loss Prevention tools to alert or block the transmission of these archives particularly if they include metadata.

Conclusion

PupkinStealer exemplifies a growing trend of low-complexity, high-impact malware using legitimate platforms to avoid detection. Though lacking sophisticated evasion, its effectiveness in stealing high-value data particularly credentials and sensitive information makes it a serious threat for organizations using digital communication.

Stay alert. Stay protected.

Reference: https://cybersecuritynews.com/pupkinstealer-attacks-windows-system/