Analysis of Backdoor.WIN32.Buterat

Lat61 Threat Intelligence Team ⋮ ⋮ 9/9/2025

Introduction:

Backdoor malware is a covert type of malicious software designed to bypass standard authentication mechanisms and provide persistent, unauthorized access to compromised systems. Unlike conventional malware that prioritizes immediate damage or data theft, backdoors focus on stealth and longevity, enabling attackers to control infected endpoints remotely, deploy additional payloads, exfiltrate sensitive information, and move laterally across networks with minimal detection.

The Buterat backdoor is a notable example of this threat class, known for its sophisticated persistence techniques and adaptive communication methods with remote command-and-control (C2) servers. First identified in targeted attacks against enterprise and government networks, Buterat commonly spreads through phishing campaigns, malicious attachments, or trojanized software downloads. Once executed, it disguises its processes under legitimate system tasks, modifies registry keys for persistence, and uses encrypted or obfuscated communication channels to avoid network-based detection.

Preliminary Information About Sample:

MD5: 5d73aad06259533c238f0cdb3280d5a8

SHA-1: 6a1c418664fe5214c8e3d2f8f5020e1cb4311584

SHA-256: f50ec4cf0d0472a3e40ff8b9d713fb0995e648ecedf15082a88b6e6f1789cdab

Imphash: 3a1c6ade174e0b7afaa15737bba99cab

Compiler: Borland Delphi

Static Analysis:

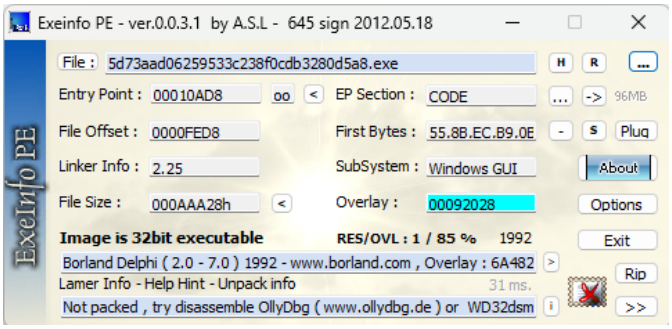

Figure 1: Static Analysis using ExeInfo PE tool

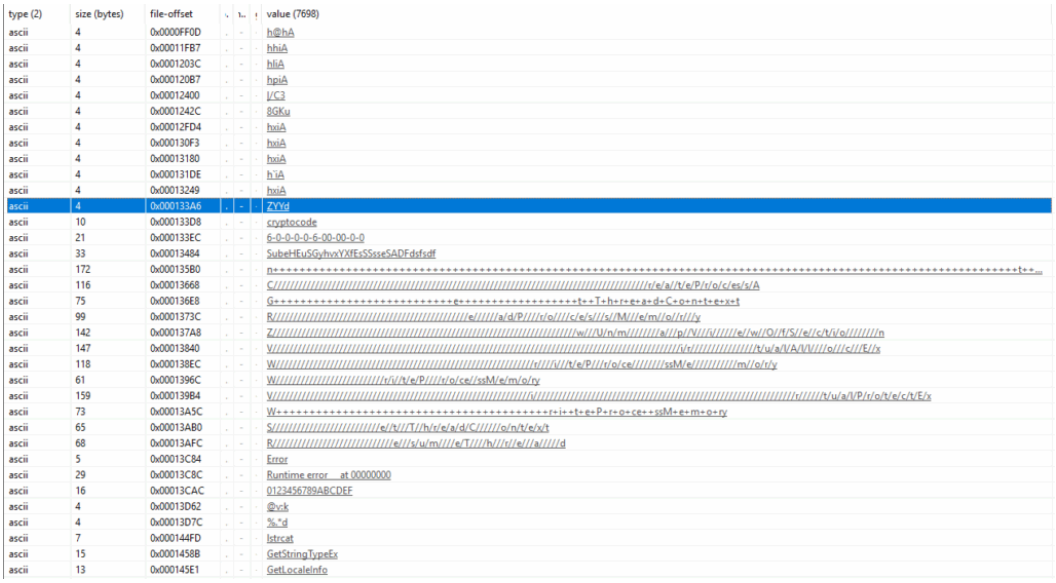

Figure 2: Encrypted and Obfuscated strings

A preliminary static analysis reveals that the sample contains some strings which are encrypted or obfuscated to hide the execution flow. These hidden strings may contain API calls for executing or downloading malicious files on the infected PC.

Dynamic Analysis:

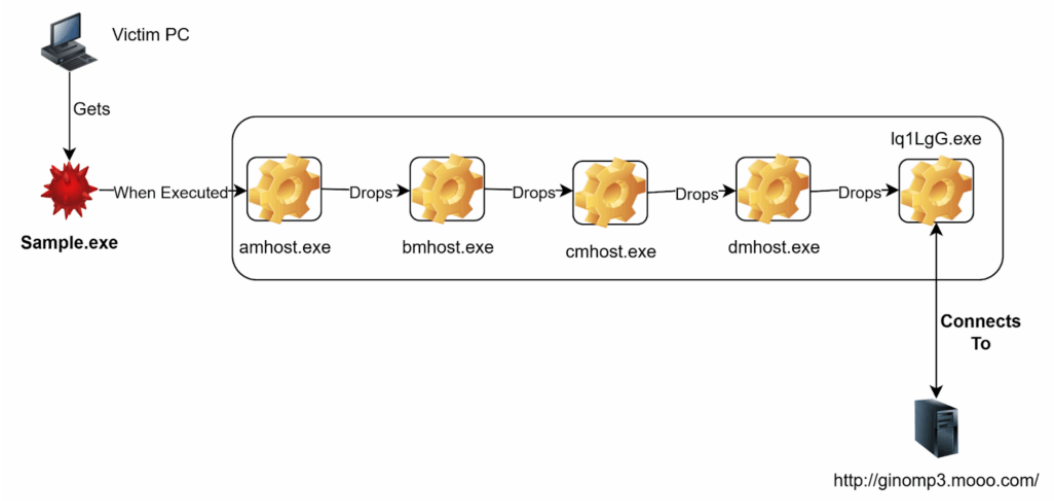

Figure 3: Execution Flow diagram

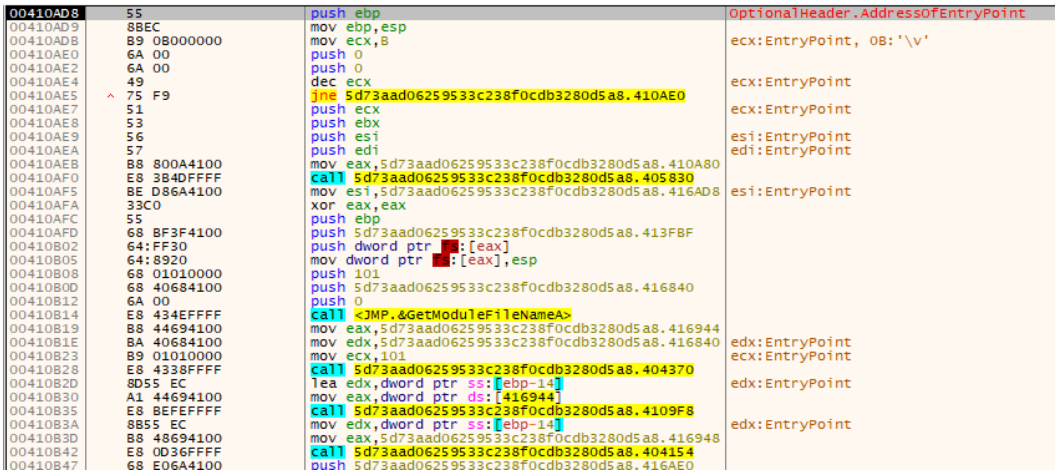

Figure 4: Address of Entry Point

Entry point for the sample is at 0x00410AD8. So the user code execution starts at this address as shown in the above figure.

Figure 5: Obfuscated API calls

Some Obfuscated API calls:

- SetThreadContext

This API provides attackers with precise control over thread execution, enabling them to hijack existing threads without creating new ones or altering the process entry point. Such capabilities make it a preferred choice for stealthy payload delivery, thread injection, and evasion of lightweight behavioural detection mechanisms.

- ResumeThread

Resumes a thread whose info has been edited and changed by an attacker.

Files dropped during infection:

- C:\Users\Admin\amhost.exe
- C:\Users\Admin\bmhost.exe
- C:\Users\Admin\cmhost.exe
- C:\Users\Admin\dmhost.exe
- C:\Users\Admin\lqL1gG.exe

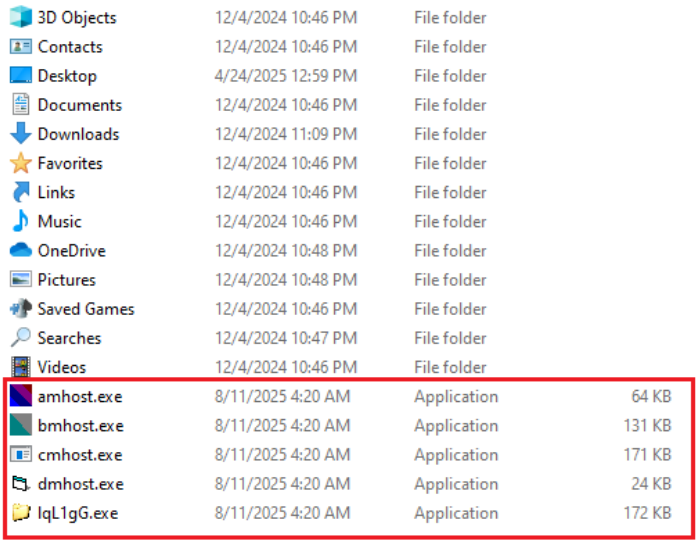

Figure 6: Files Dropped during infection

Network Activity:

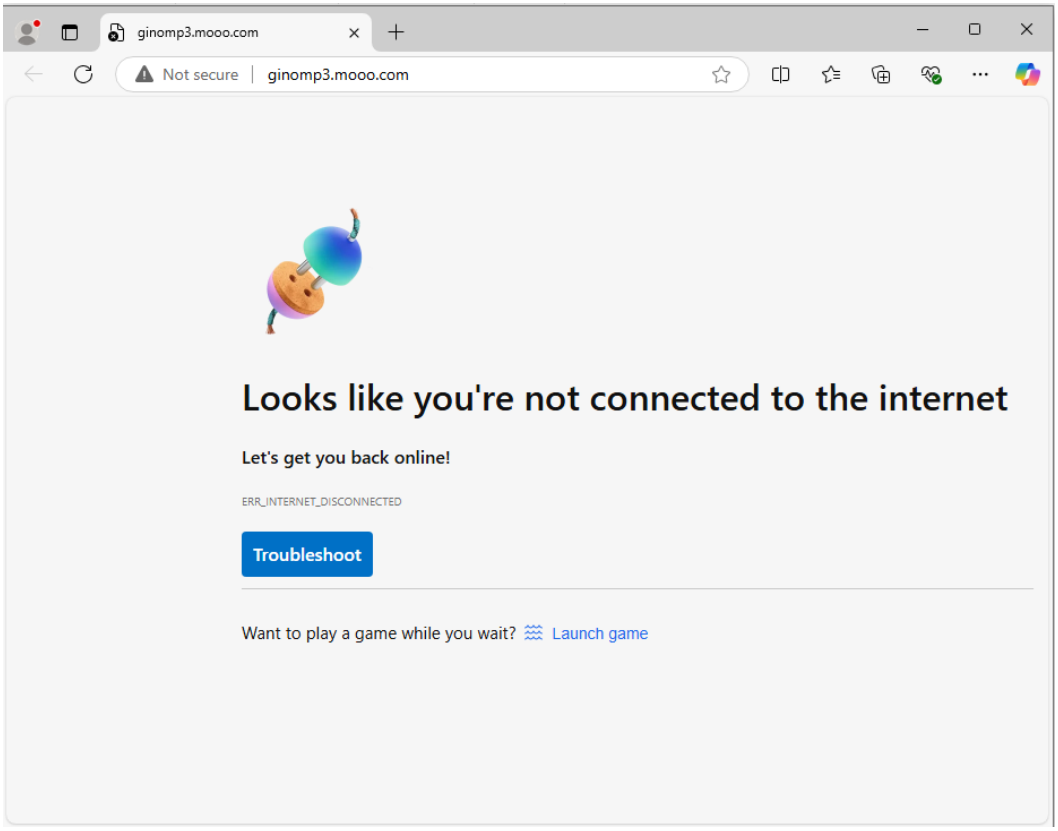

Figure 7: Sample trying to contact a suspicious link

Infection Prevention and Remediation:

What are the Technical Controls?

- Endpoint Protection:
  - Use up-to-date anti-malware and antivirus software to detect and remove threats like Backdoor.Buterat.
- Network Monitoring:
  - Implement tools and practices to monitor network traffic for suspicious connections. The malware connects to a remote C2 server at http://ginomp3.mooo.com/, which can be flagged as malicious activity.
- Firewall & IDS:

    - Configure your firewall to block unauthorized access and use an Intrusion Detection System (IDS) to monitor for suspicious network activity.
- System Integrity Monitoring:
    - Monitor for unexpected file creation or modifications, such as the dropping of amhost.exe, bmhost.exe, cmhost.exe, dmhost.exe, and lqL1gG.exe in the C:\Users\Admin directory.
- Application Control:
    - Employ application control or allowlisting to prevent the execution of unauthorized or suspicious executables. This can stop the dropped files from running and further infecting the system.
- Obfuscation & Encryption Detection:
    - Be aware that the malware uses encrypted or obfuscated communication channels and hides its processes under legitimate system tasks to avoid detection. Use security solutions with behavioural analysis to identify unusual activity that may indicate the presence of this malware, even if its files are not detected by signature-based methods.

Employee Training & Awareness:

- Phishing campaigns: The Buterat backdoor commonly spreads through phishing campaigns and malicious attachments. Educate employees on how to identify and avoid suspicious emails and attachments.
- Malicious Downloads: The malware can also spread through trojanized software downloads. Users should only download software from trusted, official sources.

Incorporating Point Wild Product Protection:

Point Wild has a platform called Lat61 that unifies its security solutions, providing a framework for defense against threats like Backdoor.Buterat. The Lat61 Threat Intelligence Team at Point Wild actively tracks malware, its methods, infrastructure, and motivations.

Conclusion:

The Backdoor.Win32.Buterat malware demonstrates a highly stealthy and persistent infection methodology designed to maintain long-term unauthorized access to compromised systems. By leveraging encrypted strings, obfuscated API calls like SetThreadContext, and sophisticated thread manipulation techniques, it effectively bypasses standard behavioural detection mechanisms. Its ability to drop multiple payloads and establish communication with remote command-and-control (C2) infrastructure further amplifies its threat potential, enabling attackers to execute arbitrary commands, exfiltrate data, and deploy additional malicious components.

Given its advanced persistence and evasion tactics, timely detection and remediation are critical to preventing prolonged compromise. Security teams should implement network monitoring for unusual outbound traffic, file integrity checks, and memory analysis to identify injected threads and unauthorized processes. Proactive threat hunting, combined with updated signatures and behavioural detection rules, is essential to minimize exposure to Buterat and similar backdoor threats.

What are the Indicators of Compromise (IOCs)?

Hashes:

f50ec4cf0d0472a3e40ff8b9d713fb0995e648ecedf15082a88b6e6f1789cdab

c5cdb87162f6e9162a92b461909a3624547e0ec8b9ffe36c2150ec5f78ce1164

6d57ce74d2af2192a533127c658cad041a75f3210c9c9c66c27f9822c0a0b091

2d72cf5e200110f5d75669441abe053be11d11768038f68860706dff54fc6be6

73999153156cf5707c2cb88bea6c577a7abdc7ba2b62369fdb03cdc26f42e963

86f5a5bb4153ae4b4b2129f112534638cb15527c28b0a771e4fd8ba8870daf77

Network:

Command and Control (C2) Server: http://ginomp3.mooo.com/