

Interactivity is now available in beta. Submit or resubmit a file or URL and select 'Live interaction' to explore feature.

Sandbox Report

File: pplnk.exe

[Resubmit](#)
[Print](#)
[Download options](#)

SHA-256
73fe4fef701bf731...30fb81e433240736

Submitted by
prashant.deshmukh@fisglobal.com

Discovered

Detonation environment
Windows 10 64, Professional, 10.0 (build 16299)

Network settings
Default network connectivity

Timestamp
Jan. 9, 2024 17:43:48

Threat level ⓘ
Suspicious

Threat score ⓘ
39/100

- Static analysis
- Dynamic analysis
- Intelligence
- MITRE ATT&CK

Tactics and Techniques observed

Click on a technique to see additional details.

Collection 3	Execution 1	Privilege Escalation 1	Defense Evasion 6	Credential Access 2	Discovery
Screen Capture	Native API	Process Injection 2 ^	Debugger Evasion	Input Capture 1 ^	Debugger Evasion
Email Collection		Thread Execution Hijacking	Deobfuscate/Decode Files or Information	Keylogging	Network Sniffing
Input Capture 1 ^		Extra Window Memory Injection	Impair Defenses 1 ^	Network Sniffing	Process Discovery
Keylogging					Query Registry