

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

Behavioral threat indicators

Malicious

Contains ability to capture the screen

1

Suspicious

Found a potential E-Mail address in binary/memory

22


PE file with no import directory

Input file contains API references not part of its Import Address Table (IAT)

Monitors specific registry key for changes

Opens a handle to the specified process

- Behavioral threat indicators
- Process details
- Screenshots
- Network activity
- Memory analysis
- Discovered URL analysis
- Extracted strings
- Extracted files

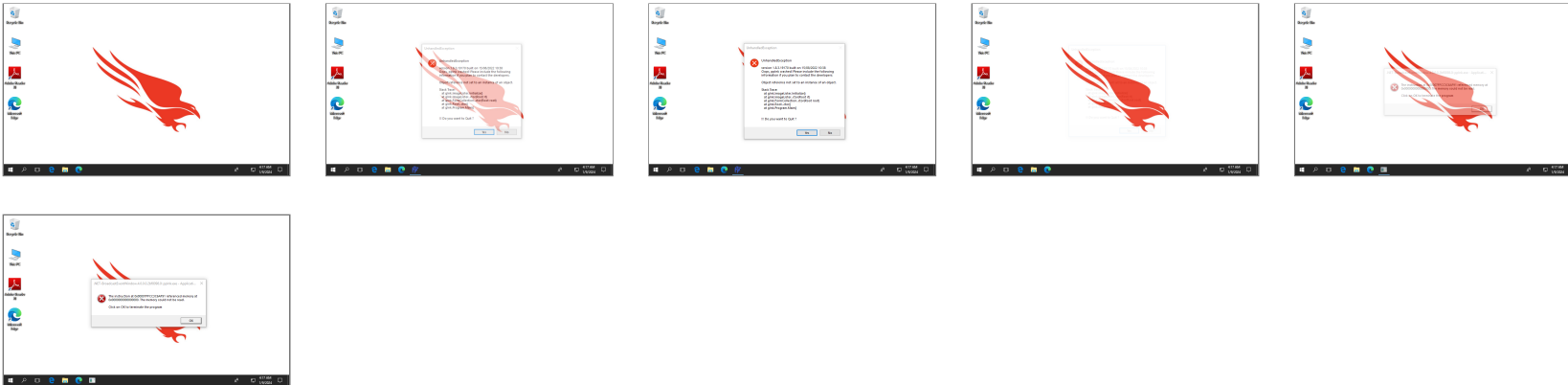
Found a string that may be used as part of an injection method	∨
Contains ability to modify thread functionality - possible hijack (API string)	∨
Queries process information	∨
Uses a .NET obfuscator to hide its code	∨
PE file has unusual entropy sections	∨
Creates guarded memory regions (anti-debugging trick to avoid memory dumping)	∨
Tries to detect debugger using ProcessDebugPort	∨
Contains ability to retrieve keyboard strokes	∨
Contains ability to enumerate processes/modules/threads	∨
Contains ability to listen for incoming connections	∨
Contains ability to open a port and listen for incoming connection	∨
Calls an API typically used to acquire handle to a key container within a CSP	∨
Calls an API typically to import asymmetric cryptographic keys into a CSP	∨
Contains ability to use Microsoft's Enhanced Cryptographic Provider	∨
Calls an API typically to import cryptographic keys into a CSP	∨
Writes registry keys	∨
Contains indicators of bot communication commands	∨
 Informative	94 ∨

Process details



- [pplnk.exe](#) PID 7268
- [WerFault.exe](#) PID 7532
- [WerFault.exe](#) PID 2980
- [WerFault.exe](#) PID 7480

Screenshots



Network activity



Memory network forensics

String	Process name	PID	Context	Stream UID
freepik.com	pplnk.exe	7268	Domain/IP reference	f10e8ffc8be006eacb4c276c...
https://github.com/pubpub-...	pplnk.exe	7268	Domain/IP reference	f10e8ffc8be006eacb4c276c...

2 results (1-2 shown)

Items per page

5

Page 1 of 1

Memory analysis



Download memory dumps

pplnk.exe

1

Discovered URL analysis



No verdict

1

Extracted strings



Download extracted strings

pplnk.exe	1176	∨
WerFault.exe	1	∨
crash.txt	9	∨
screen_5.png	3	∨

Extracted files



 No verdict	1	∨
--	---	---