

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

**Source** Hybrid Analysis Technology

**Relevance** 3/10

**MITRE ATT&CK** [Screen Capture](#) T1113

**Details**

```

System.Drawing.Graphics::CopyFromScreen(System.Drawing.Point,System.Drawing.Point,System.Drawing.Size) at
f10e8ffc8be006eacb4c276c92634063-60000e1-FormCollection~IC_MouseMove
System.Drawing.Graphics::CopyFromScreen(System.Drawing.Point,System.Drawing.Point,System.Drawing.Size) at
f10e8ffc8be006eacb4c276c92634063-6000104-FormCollection~tiSlide_Tick
System.Drawing.Graphics::CopyFromScreen(System.Drawing.Point,System.Drawing.Point,System.Drawing.Size) at
f10e8ffc8be006eacb4c276c92634063-60000db-FormCollection~IC_Stroke
System.Drawing.Graphics::CopyFromScreen(System.Int32,System.Int32,System.Int32,System.Int32,System.Drawing.Size) at
f10e8ffc8be006eacb4c276c92634063-6000087-FormDisplay~SnapShot

```

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

 Suspicious

22 ^

Found a potential E-Mail address in binary/memory ^

**Source** File/Memory

**Relevance** 3/10


**MITRE ATT&CK** [Email Collection](#) T1114

**Details** Pattern match: "t@l.f" 

PE file with no import directory ^

**Source** Static Parser

**Relevance** 5/10

**Details** "ppInk.exe" has no "IMAGE\_DIRECTORY\_ENTRY\_IMPORT" 

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

**Source** File/Memory

**Relevance** 10/10

**MITRE ATT&CK** [Native API](#) T1106

**Details** Found string "memcpy" (Source: ppInk.exe, API is part of module: VCRUNTIME140\_CLR0400.DLL) 

Monitors specific registry key for changes ^




**Source** API Call

**Relevance** 4/10

**MITRE ATT&CK** [Query Registry](#) T1012

**Details** "ppInk.exe" monitors "HKLM\SOFTWARE\Microsoft\Ole" (Filter: 268435457; Subtree: 0) "ppInk.exe" monitors "\REGISTRY\USER\S-1-5-21-735145574-3570218355-1207367261-1001\_Classes\Local Settings\Software\Microsoft" (Filter: 268435457; Subtree: 1) "ppInk.exe" monitors "\REGISTRY\USER\S-1-5-21-735145574-3570218355-1207367261-1001\_Classes" (Filter: 268435461; Subtree: 1) 

Opens a handle to the specified process ^

**Source** API Call**Relevance** 3/10**MITRE ATT&CK** [Process Discovery](#) T1057**Details** "ppInk.exe" opens a process "C:\ppInk.exe" (UID: 00000000-00007268) Found a string that may be used as part of an injection method **Source** File/Memory**Relevance** 4/10**MITRE ATT&CK** [Extra Window Memory Injection](#) T1055.011**Details** "Shell\_TrayWnd" (Taskbar window class may be used to inject into explorer with the SetWindowLong method) in Source: 00000000-00007268.00000000.69301.B5AA0000.00000002.mdmp "!Progman" (Program manager) in Source: 00000000-00007268.00000000.69301.B5AA0000.00000002.mdmp Contains ability to modify thread functionality - possible hijack (API string) **Source** File/Memory**Relevance** 1/10**MITRE ATT&CK** [Thread Execution Hijacking](#) T1055.003**Details** Found reference to API "SuspendThread" (Indicator: "SuspendThread"; File: "ppInk.exe") Found reference to API "ResumeThread" (Indicator: "ResumeThread"; File: "ppInk.exe") Found reference to API "SuspendThread" (Indicator: "SuspendThread"; Source: "00000000-00007268.00000000.69301.B2FC2000.00000002.mdmp") Found reference to API "ResumeThread" (Indicator: "ResumeThread"; Source: "00000000-00007268.00000000.69301.B2FC2000.00000002.mdmp") Queries process information **Source** API Call**Relevance** 4/10**MITRE ATT&CK** [Process Discovery](#) T1057**Details** "ppInk.exe" queried SystemProcessInformation at 00000000-00007268-00000C13-58772322 [PID: 7268] "ppInk.exe" queried SystemProcessInformation at 00000000-00007268-00000C13-58773761 [PID: 7268] "ppInk.exe" queried SystemProcessInformation at 00000000-00007268-00000C13-61497699 [PID: 7268] "ppInk.exe" queried SystemProcessInformation at 00000000-00007268-00000C13-61499382 [PID: 7268] "ppInk.exe" queried SystemProcessInformation at 00000000-00007268-00000C13-61506218 [PID: 7268] "ppInk.exe" queried 

SystemProcessInformation at 00000000-00007268-00000C13-62246651 [PID: 7268] "ppInk.exe" queried SystemProcessInformation at 00000000-00007268-00000C13-62247997 [PID: 7268] "ppInk.exe" queried SystemProcessInformation at 00000000-00007268-00000C13-62910639 [PID: 7268] "ppInk.exe" queried SystemProcessInformation at 00000000-00007268-00000C13-62912010 [PID: 7268]

Uses a .NET obfuscator to hide its code ^

**Source** File/Memory

**Relevance** 2/10

**MITRE ATT&CK** [Deobfuscate/Decode Files or Information](#) T1140

**Details** "<CompressionMethod>k\_\_BackingField" is a hint for the obfuscator "MPRESS" "get\_CompressionMethod" is a hint for the obfuscator "MPRESS" "set\_CompressionMethod" is a hint for the obfuscator "MPRESS" 📄

PE file has unusual entropy sections ^

**Source** Static Parser

**Relevance** 3/10

**MITRE ATT&CK** [Software Packing](#) T1027.002

**Details** .text with unusual entropies 7.2504577231 📄

Creates guarded memory regions (anti-debugging trick to avoid memory dumping) ^

**Source** API Call

**Relevance** 10/10

**MITRE ATT&CK** [Disable or Modify Tools](#) T1562.001

**Details** "ppInk.exe" is allocating memory with PAGE\_GUARD access rights (Handle: 4294967295); (PID: 7268) 📄

Tries to detect debugger using ProcessDebugPort ^

**Source** API Call

**Relevance** 5/10

**MITRE ATT&CK** [Debugger Evasion](#) T1622

**Details** "ppInk.exe queries ProcessDebugPort (UID: 7268) 📄

Contains ability to retrieve keyboard strokes



**Source** Hybrid Analysis Technology

**Relevance** 8/10

**MITRE ATT&CK** [Keylogging](#) T1056.001

**Details** gInk.FormCollection::GetAsyncKeyState(System.Int32) at f10e8ffc8be006eacb4c276c92634063-60000e1-FormCollection~IC\_MouseMove  
 gInk.FormCollection::GetKeyState(System.Int32) at f10e8ffc8be006eacb4c276c92634063-6000104-FormCollection~tiSlide\_Tick  
 gInk.FormCollection::GetAsyncKeyState(System.Int32) at f10e8ffc8be006eacb4c276c92634063-60000df-FormCollection~IC\_CursorDown  
 gInk.FormCollection::GetKeyState(System.Int32) at f10e8ffc8be006eacb4c276c92634063-60000c3-FormCollection~AltKeyPressed  
 gInk.FormCollection::GetAsyncKeyState(System.Int32) at f10e8ffc8be006eacb4c276c92634063-60000db-FormCollection~IC\_Stroke  
 gInk.FormCollection::GetAsyncKeyState(System.Int32) at f10e8ffc8be006eacb4c276c92634063-6000103-FormCollection~KeyCodeState  
 gInk.FormCollection::GetAsyncKeyState(System.Int32) at f10e8ffc8be006eacb4c276c92634063-60000e0-FormCollection~IC\_MouseDown  
 gInk.FormCollection::GetKeyState(System.Int32) at f10e8ffc8be006eacb4c276c92634063-60000c2-FormCollection~IC\_MouseWheel  
 gInk.CallForm::GetAsyncKeyState(System.Int32) at f10e8ffc8be006eacb4c276c92634063-6000003-CallForm~timer1\_Tick  
 gInk.FormCollection::GetKeyState(System.Int32) at f10e8ffc8be006eacb4c276c92634063-600012b-FormCollection~FormCollection\_FormClosing



Contains ability to enumerate processes/modules/threads



**Source** Hybrid Analysis Technology

**Relevance** 5/10

**MITRE ATT&CK** [Process Discovery](#) T1057

**Details** System.Diagnostics.Process::GetProcessById(System.Int32) at f10e8ffc8be006eacb4c276c92634063-6000141-FormCollection~GetCaptionOfActiveWindow



Contains ability to listen for incoming connections



**Source** Hybrid Analysis Technology

**Relevance** 5/10

**MITRE ATT&CK** [Network Sniffing](#) T1040

**Details** System.Net.HttpListener::GetContextAsync() at f10e8ffc8be006eacb4c276c92634063-600038a-APIRestHandleIncomingConnectionsd\_\_10~MoveNext System.Net.HttpListener::Close() at f10e8ffc8be006eacb4c276c92634063-600000e-APIRest~Close System.Net.HttpListener::Stop() at f10e8ffc8be006eacb4c276c92634063-6000013-APIRest~Stop  
 System.Net.HttpListener::get\_Prefixes() at f10e8ffc8be006eacb4c276c92634063-6000010-APIRest~GetAddress gInk.APIRest::IsListening() at f10e8ffc8be006eacb4c276c92634063-6000184-FormOptions~FormOptions\_Load System.Net.HttpListener::get\_IsListening() at



f10e8ffc8be006eacb4c276c92634063-6000011-APIRest~IsListening System.Net.HttpListener::StartO at f10e8ffc8be006eacb4c276c92634063-6000012-APIRest~Start System.Net.HttpListener::StopO at f10e8ffc8be006eacb4c276c92634063-600000f-APIRest~ChangeAddress

Contains ability to open a port and listen for incoming connection ^

**Source** Hybrid Analysis Technology

**Relevance** 5/10

**MITRE ATT&CK** [Non-Standard Port](#) T1571

**Details** System.Net.WebSockets.WebSocket::get\_StateO at f10e8ffc8be006eacb4c276c92634063-6000396-FormCollectionReceiveObsMesgsd\_\_267~MoveNext System.Net.HttpListener::GetContextAsyncO at f10e8ffc8be006eacb4c276c92634063-600038a-APIRestHandleIncomingConnectionsd\_\_10~MoveNext System.Net.HttpListener::CloseO at f10e8ffc8be006eacb4c276c92634063-600000e-APIRest~Close System.Windows.Forms.Control::set\_TabIndex(System.Int32) at f10e8ffc8be006eacb4c276c92634063-6000154-FormCollection~InitializeComponent System.Net.HttpListener::StopO at f10e8ffc8be006eacb4c276c92634063-6000013-APIRest~Stop gInk.FormCollection::SendInWs(System.Net.WebSockets.ClientWebSocket,System.String,System.Threading.CancellationToken,System.String) at f10e8ffc8be006eacb4c276c92634063-60003a0-FormCollectionc\_\_DisplayClass270\_0~ObsStopRecordingb\_\_0 System.Type::GetFields(System.Reflection.BindingFlags) at f10e8ffc8be006eacb4c276c92634063-6000028-JSONParser~ParseObject System.Windows.Forms.Control::set\_TabIndex(System.Int32) at f10e8ffc8be006eacb4c276c92634063-60001ec-FormOptions~InitializeComponent System.Net.WebSockets.WebSocket::get\_StateO at f10e8ffc8be006eacb4c276c92634063-60003a6-FormCollectionSendInWsd\_\_273~MoveNext System.Windows.Forms.Control::set\_TabIndex(System.Int32) at f10e8ffc8be006eacb4c276c92634063-600005a-FormInput~InitializeComponent

Calls an API typically used to acquire handle to a key container within a CSP ^

**Source** API Call

**Relevance** 1/10

**MITRE ATT&CK** [Obfuscated Files or Information](#) T1027

**Details** "ppInk.exe" called "CryptAcquireContextW" with parameters {"phProv": "102f30b529020000" "dwProvType": "1" "dwFlags": "4026531840"} "ppInk.exe" called "CryptAcquireContextW" with parameters {"phProv": "102e30b529020000" "szProvider": "Microsoft Enhanced RSA and AES Cryptographic Provider" "dwProvType": "24" "dwFlags": "4026531840"}

Calls an API typically to import asymmetric cryptographic keys into a CSP ^

**Source** API Call

**Relevance** 1/10

**MITRE ATT&CK** [Asymmetric Cryptography](#) T1573.002

**Details** "ppInk.exe" called "BCryptImportKeyPair" with parameters {"nAlgorithm": "B530Bf00" "pszBlobType": "RSAPUBLICBLOB" "phKey": "f07f31b529020000" "pbInput": "RSA1" "cbInput": "163" "dwFlags": "0"} "ppInk.exe" called "BCryptImportKeyPair" with parameters {"hAlgorithm": "b530bf00" "pszBlobType": "RSAPUBLICBLOB" "phKey": "c07f31b529020000" "pbInput": "RSA1" "cbInput": "163" "dwFlags": "0"} "ppInk.exe" called

```

"dwFlags": "0"} "ppInk.exe" called "BCryptImportKeyPair" with parameters {"hAlgorithm": "b530bf00" "pszBlobType": "RSAPUBLICBLOB" "phKey":
"007c31b529020000" "pbInput": "RSA1" "cbInput": "163" "dwFlags": "0"} "ppInk.exe" called "BCryptImportKeyPair" with parameters {"hAlgorithm":
"b530bf00" "pszBlobType": "RSAPUBLICBLOB" "phKey": "807731b529020000" "pbInput": "RSA1" "cbInput": "163" "dwFlags": "0"} "ppInk.exe" called
"BCryptImportKeyPair" with parameters {"hAlgorithm": "b530bf00" "pszBlobType": "RSAPUBLICBLOB" "phKey": "c07631b529020000" "pbInput":
"RSA1" "cbInput": "163" "dwFlags": "0"} "ppInk.exe" called "BCryptImportKeyPair" with parameters {"hAlgorithm": "b530bf00" "pszBlobType":
"RSAPUBLICBLOB" "phKey": "p~1" "pbInput": "RSA1" "cbInput": "163" "dwFlags": "0"} "ppInk.exe" called "BCryptImportKeyPair" with parameters
{"hAlgorithm": "b530bf00" "pszBlobType": "RSAPUBLICBLOB" "phKey": "@r1" "pbInput": "RSA1" "cbInput": "163" "dwFlags": "0"} "ppInk.exe" called

```

Contains ability to use Microsoft's Enhanced Cryptographic Provider

**Source** File/Memory

**Relevance** 2/10

**MITRE ATT&CK** [Encrypted Channel](#) T1573

**Details** Found api reference "CryptDecrypt" (Indicator: "CryptDecrypt"; Source: "00000000-00007268.00000000.69301.B5250000.00000004.mdmp")

Calls an API typically to import cryptographic keys into a CSP

**Source** API Call

**Relevance** 1/10

**MITRE ATT&CK** [Data Encrypted for Impact](#) T1486


**Details** "ppInk.exe" called "CryptImportKey" with parameters {"hProv": "b5302f10" "pbData":  
"0602000000240000525341310004000001000100b5fc90e7027f67871e773a8fde8938c81dd402ba65b9201d60593e96c492651e889cc13f1415  
ebb53fac1131ae0bd333c5ee6021672d9718ea31a8aebd0da0072f25d87dba6fc90ffd598ed4da35e44c398c454307e8e33b8426143daec9f596836f97c  
8f74750e5975c64e2189f45def46b2a2b1247adc3652bf5c308055da9" "dwDataLen": "148" "dwFlags": "0" "phKey": "e0af2eb529020000"} "ppInk.exe"  
called "CryptImportKey" with parameters {"hProv": "b5302f10" "pbData":  
"0602000000240000525341310004000001000100b5fc90e7027f67871e773a8fde8938c81dd402ba65b9201d60593e96c492651e889cc13f1415ebb  
53fac1131ae0bd333c5ee6021672d9718ea31a8aebd0da0072f25d87dba6fc90ffd598ed4da35e44c398c454307e8e33b8426143daec9f596836f97c8f74  
750e5975c64e2189f45def46b2a2b1247adc3652bf5c308055da9" "dwDataLen": "148" "dwFlags": "0" "phKey": "30b12eb529020000"} "ppInk.exe"  
called "CryptImportKey" with parameters {"hProv": "b5302f10" "pbData":  
"0602000000240000525341310004000001000100b5fc90e7027f67871e773a8fde8938c81dd402ba65b9201d60593e96c492651e889cc13f1415ebb  
53fac1131ae0bd333c5ee6021672d9718ea31a8aebd0da0072f25d87dba6fc90ffd598ed4da35e44c398c454307e8e33b8426143daec9f596836f97c8f74

Writes registry keys

**Source** Registry Access

**Relevance** 3/10

**MITRE ATT&CK** [Modify Registry](#) T1112


**Details** "ppInk.exe" (Access type: "SETVAL"; Path: "HKLM\SYSTEM\CONTROLSET001\SERVICES\EVENTLOG\APPLICATION\UNHANDLEDEXCEPTION"; Key: "EVENTMESSAGEFILE"; Value: "%WINDIR%\Microsoft.NET\Framework64\v4.0.30319\EventLogMessages.dll") 

Contains indicators of bot communication commands 

**Source** File/Memory

**Relevance** 3/10


**MITRE ATT&CK** [Exfiltration Over C2 Channel](#) T1041




**Details** Found string "LbIFmpegCmd="Command Line"" (Indicator: "cmd="; Source: "00000000-00007268.00000000.69301.B2FC2000.00000002.mdmp") 

 **Informative** 94 

## Process details

 [ppInk.exe](#) PID 7268   

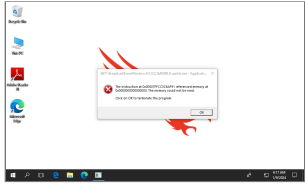
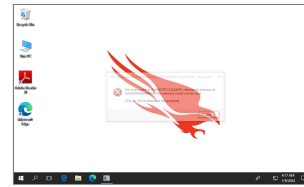
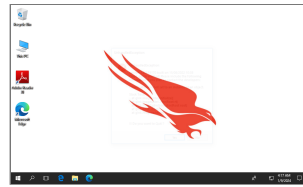
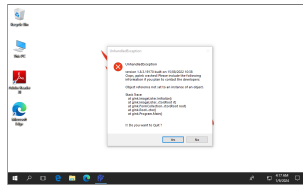
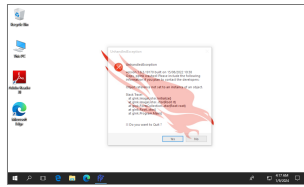
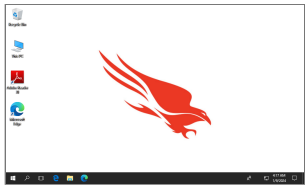
 [WerFault.exe](#) PID 7532  

 [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 ▾