

SHA256 31a7e70deb8af07d7b76b5dea8cbf90ec63bea24bffd5ebac6f223c02f55753

This analysis was an attempt to blindly try to analyze an unknown pulled from MalwareBazaar for practice.

Analysis

High entropy shown in Figure 1. indicates that it is packed. There is also a suspicious section labeled as .text which also happens to be the entrypoint highlighted on PESTudio seen in Figure 2.

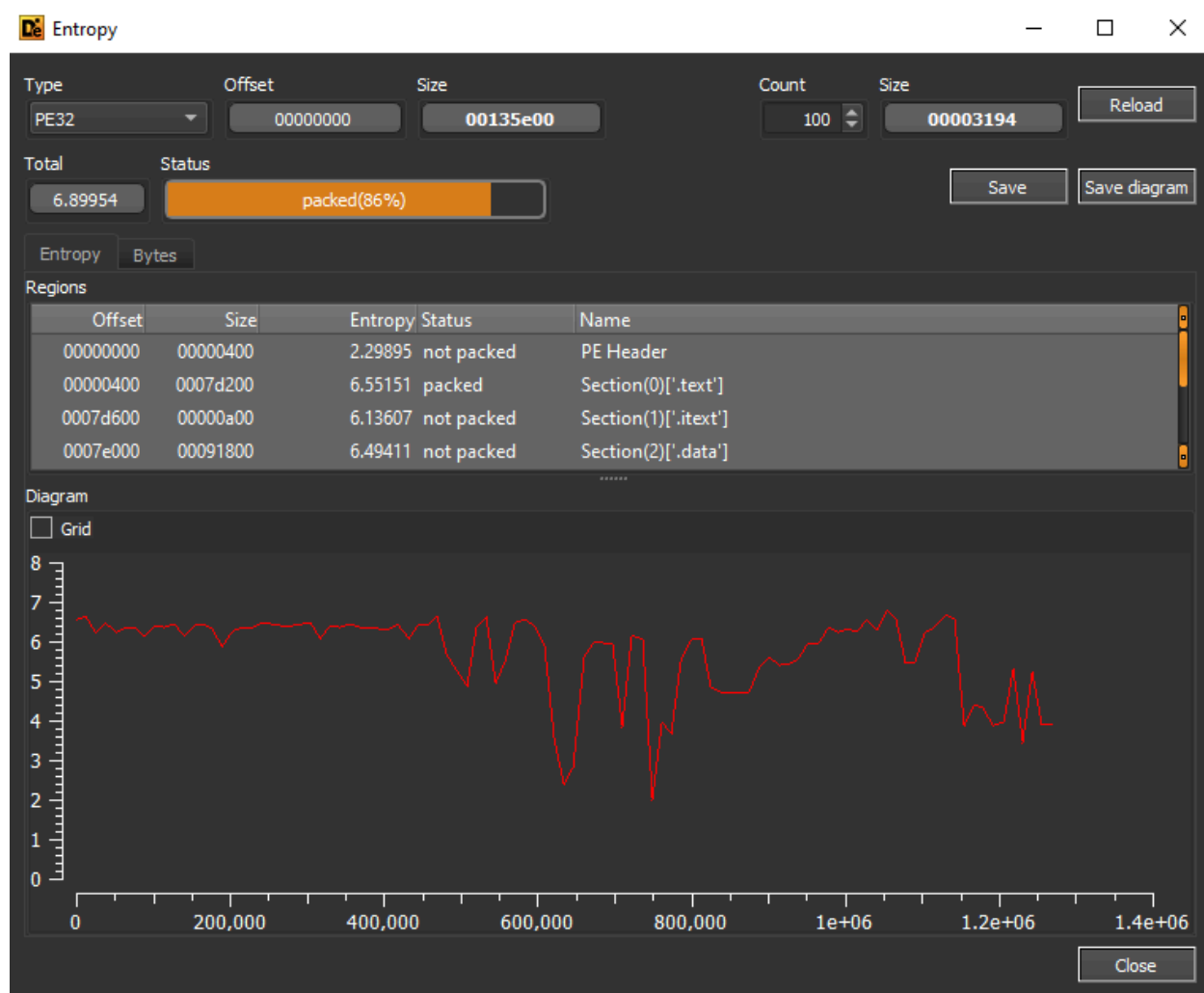


Figure 1. Entropy from DiE

From Figure 2. Below, it can be seen that the entry point of the executable is on the custom section .itext

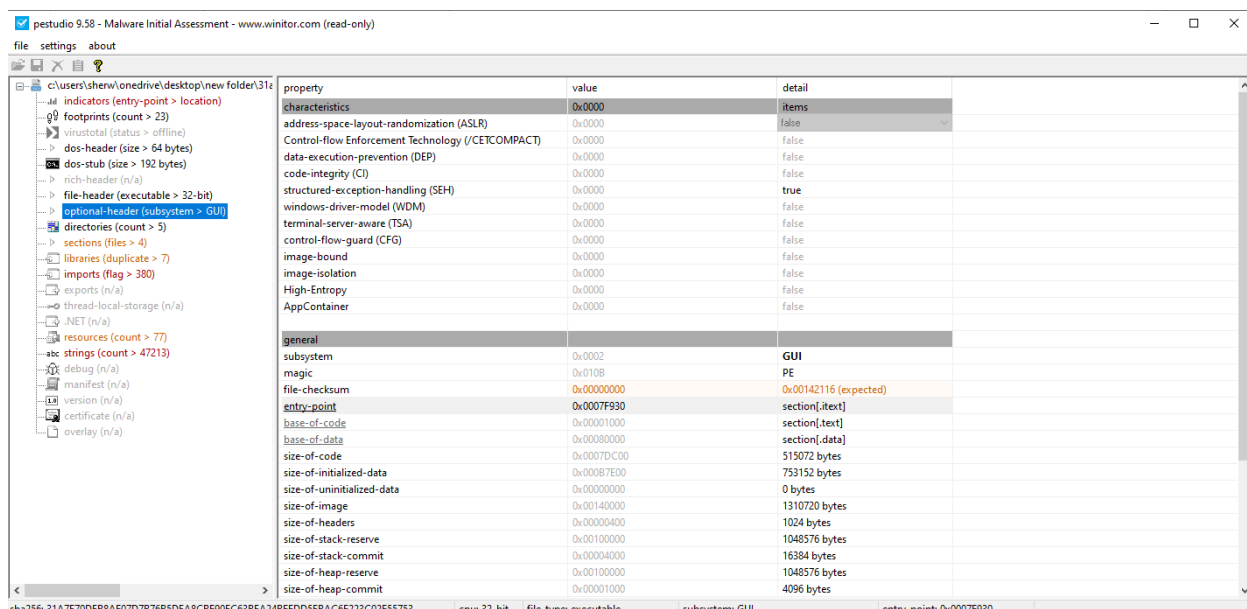


Figure 2. Suspicious Entry Point

The breakpoints I used.

Type	Address	Module/Label/Exception	State	Disassembly	Hits	Summary
Software	76D788E0	<kernel32.dll.CreateProcessW>	Enabled	mov edi,edi	0	
	76D7F660	<kernel32.dll.VirtualAlloc>	Enabled	mov edi,edi	0	
	76D80760	<kernel32.dll.VirtualProtect>	Enabled	mov edi,edi	0	
	76D82370	<kernel32.dll.IsDebuggerPresent>	Enabled	jmp dword ptr ds:[<IsDebuggerPresent>]	0	
	76D92DF0	<kernel32.dll.CreateProcessInternal>	Enabled	mov edi,edi	0	
	76D95220	<kernel32.dll.WriteProcessMemory>	Enabled	mov edi,edi	0	
	772E30B0	<ntdll.dll.NtResumeThread>	Enabled	mov eax,70052	0	

Figure 3. Breakpoints Set

After setting the breakpoints, the executable is then ran. The first breakpoint that was hit is VirtualAlloc. After hitting VirtualAlloc, I run until the return, then follow EAX in dump to see what is allocated in the region of memory.

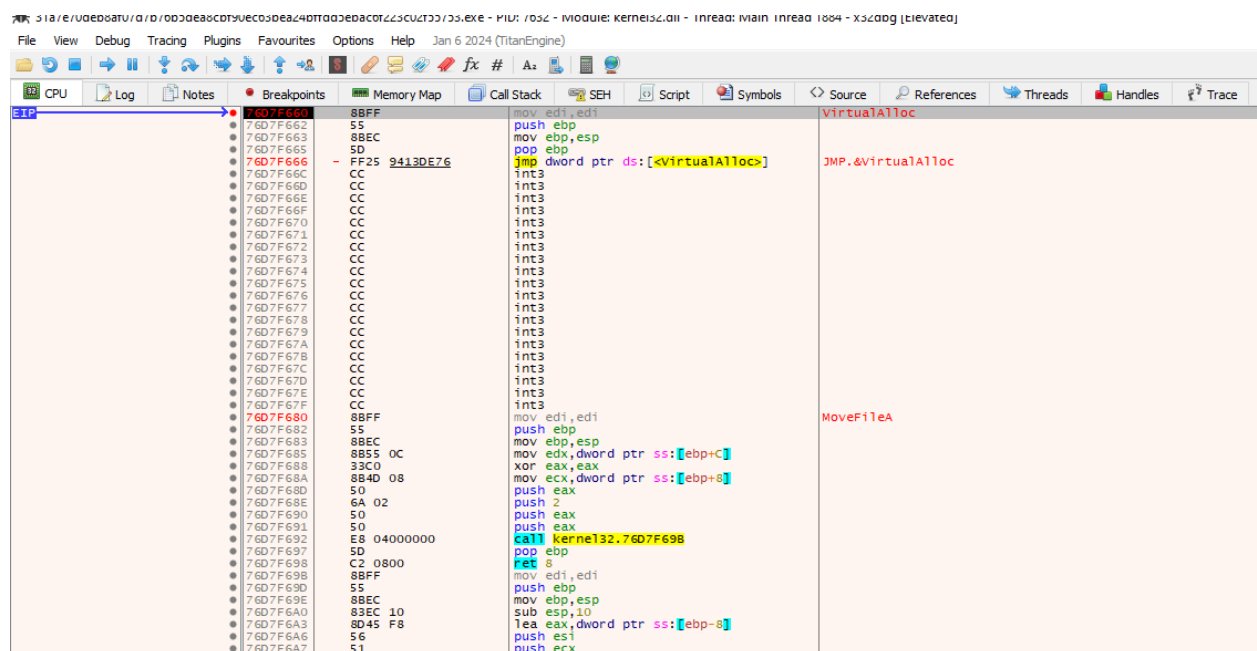


Figure 4. Repeated Hits in VirtualAlloc

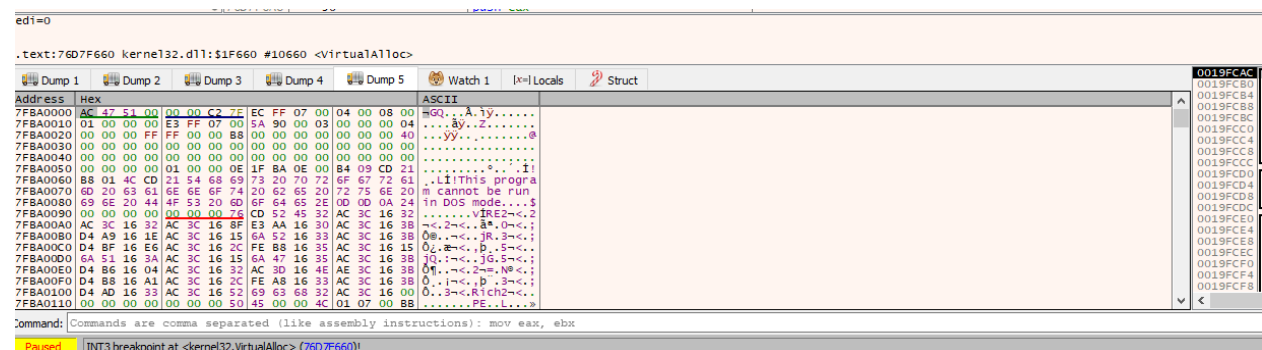
During my debugging process; VirtualProtect has been hit for more than 40 times already and it is unlikely that this is the right API call to hook so in the next steps, I have removed this breakpoint instead to let the executable continue to run. Figure 5. Shows the current breakpoint hits but is not the total yet.

Type	Address	Module/Label/Exception	State	Disassembly	Hits	Summary
Software	76D788E0	<kernel32.dll.CreateProcessW>	Enabled	mov edi,edi	0	
	76D7F660	<kernel32.dll.VirtualAlloc>	Enabled	mov edi,edi	4	
	76D80760	<kernel32.dll.VirtualProtect>	Enabled	mov edi,edi	41	
	76D82370	<kernel32.dll.IsDebuggerPresent>	Enabled	jmp dword ptr ds:[<IsDebuggerPresent>]	0	
	76D92DF0	<kernel32.dll.CreateProcessInternal>	Enabled	mov edi,edi	0	
	76D95220	<kernel32.dll.WriteProcessMemory>	Enabled	mov edi,edi	0	
	772E30B0	<ntdll.dll.NtResumeThread>	Enabled	mov eax,70052	0	

Figure 5. Breakpoint Hits

[illegible]

The next VirtualAlloc call clears the memory and allocates something that starts to look like an executable payload. The GQ characters appear in most of the virtualalloc calls and might be useful in the future.



Repeating the process eventually shows the MZ magic bytes. Interestingly the data does not start at the MZ but instead it looks like it starts at the GO bytes instead.

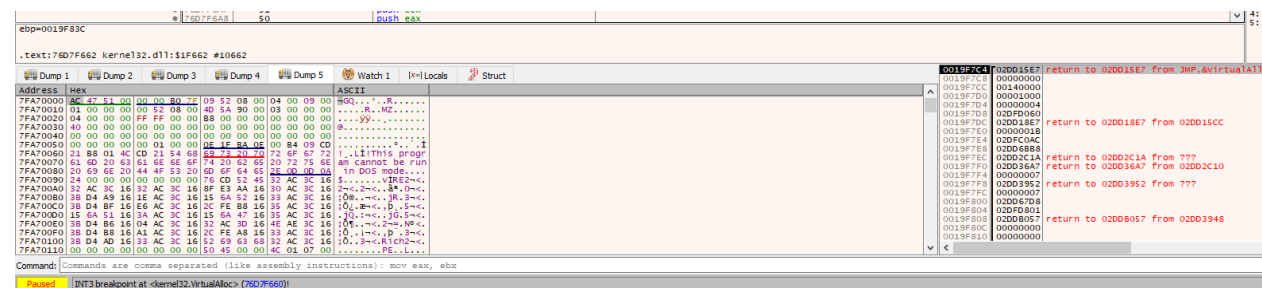
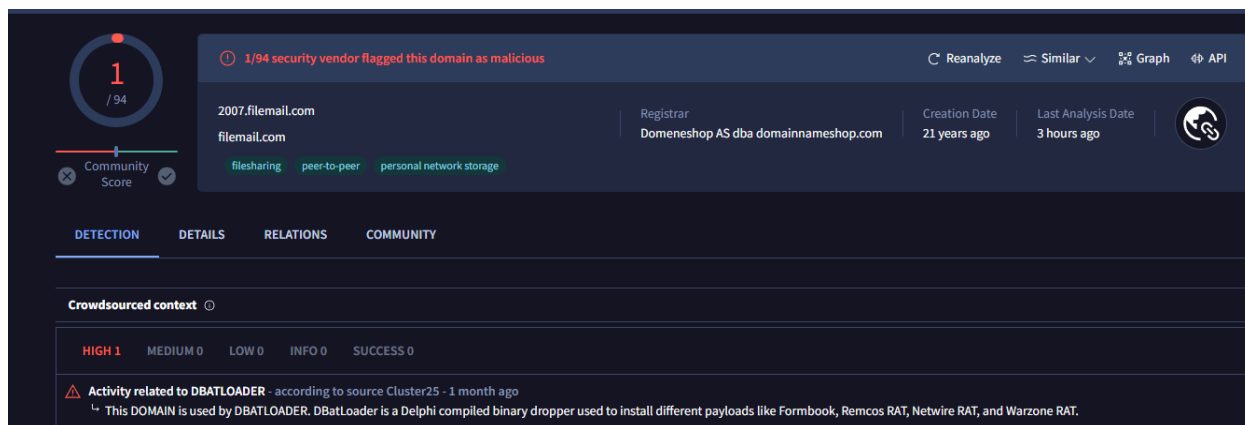


Figure 8. MZ Found

I am unable to unpack anything from this file; likely because I do not have an internet connection active on my virtual machine, but setting a breakpoint on CreateFileA shows something related to filemail[.]com which VT has a tag for being a domain used by DBATLoader



The image shows a VirusTotal scan result for the domain filemail.com. At the top, a red circle with the number 1 indicates that 1 out of 94 security vendors flagged the domain as malicious. A warning message states: "1/94 security vendor flagged this domain as malicious". The domain is listed as 2007.filemail.com, registered by Domeneshop AS dba domainnameshop.com, created 21 years ago, and last analyzed 3 hours ago. The domain is categorized as filesharing, peer-to-peer, and personal network storage. The DETECTION tab is active, showing a Crowdsourced context with a HIGH 1 rating. A warning icon indicates activity related to DBATLOADER, noting that the domain is used by DBATLOADER, a Delphi compiled binary dropper used to install different payloads like Formbook, Remcos RAT, Netwire RAT, and Warzone RAT.

1 / 94

1/94 security vendor flagged this domain as malicious

Reanalyze Similar Graph API

2007.filemail.com

filemail.com

filesharing peer-to-peer personal network storage

Registrar: Domeneshop AS dba domainnameshop.com

Creation Date: 21 years ago

Last Analysis Date: 3 hours ago

Community Score

DETECTION DETAILS RELATIONS COMMUNITY

Crowdsourced context

HIGH 1 MEDIUM 0 LOW 0 INFO 0 SUCCESS 0

Activity related to DBATLOADER - according to source Cluster25 - 1 month ago

This DOMAIN is used by DBATLOADER. DBATLoader is a Delphi compiled binary dropper used to install different payloads like Formbook, Remcos RAT, Netwire RAT, and Warzone RAT.

```
80] Host: ctldl.windowsupdate.com
80]
er] svchost.exe (2036) requested UDP 192.168.254.254:53
er] Received A request for domain '2007.filemail.com'.
er] 31a7e70deb8af07d7b76b5dea8cbf90ec63bea24bffd5ebac6f223c02f55753.exe (5216) requested TCP 192.0.2.123:443
er] svchost.exe (2036) requested UDP 192.168.254.254:53
er] Received A request for domain '2007.filemail.com'.
er] 31a7e70deb8af07d7b76b5dea8cbf90ec63bea24bffd5ebac6f223c02f55753.exe (5216) requested TCP 192.0.2.123:443
er] svchost.exe (2036) requested UDP 192.168.254.254:53
er] Received A request for domain 'ctldl.windowsupdate.com'.
er] 31a7e70deb8af07d7b76b5dea8cbf90ec63bea24bffd5ebac6f223c02f55753.exe (5216) requested TCP 192.0.2.123:80
80] GET /msdownload/update/v3/static/trustedr/en/authrootstl.cab?85a7e8f957c6b527 HTTP/1.1
80] Connection: Keep-Alive
80] Accept: */*
80] User-Agent: Microsoft-CryptoAPI/10.0
80] Host: ctldl.windowsupdate.com
80]
er] svchost.exe (2036) requested UDP 192.168.254.254:53
er] Received A request for domain 'watson.events.data.microsoft.com'.
er] program name unknown (924) requested TCP 192.0.2.123:443
er] svchost.exe (2036) requested UDP 192.168.254.254:53
er] Received A request for domain 'ctldl.windowsupdate.com'.
er] program name unknown (924) requested TCP 192.0.2.123:80
80] GET /msdownload/update/v3/static/trustedr/en/authrootstl.cab?17a3747ca5796ec0 HTTP/1.1
80] Connection: Keep-Alive
80] Accept: */*
80] User-Agent: Microsoft-CryptoAPI/10.0
80] Host: ctldl.windowsupdate.com
```