

Malware Analysis:

In the attached VM, there is a sample named 'redline' in the Desktop/Samples directory. What is the md5sum of this sample?

```
redline 311 wannacry 2ms023p1nwc  
ubuntu@ip-10-10-40-51:~/Desktop/Samples$ md5sum redline  
ca2dc5a3f94c4f19334cc8b68f256259 redline  
ubuntu@ip-10-10-40-51:~/Desktop/Samples$
```

What is the creation time of this sample?

Search the Md5 hash value in Virustotal.com



The image shows the VirusTotal search interface. At the top is the VirusTotal logo and a description: "Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community." Below this is a navigation bar with "FILE", "URL", "SEARCH", and a settings icon. The "SEARCH" tab is active. In the center, there is a magnifying glass icon and the text: "Search for a hash, domain, IP address, URL or gain additional context and threat landscape visibility with OUR THREAT INTELLIGENCE OFFERING." Below this is a search input field containing the MD5 hash "ca2dc5a3f94c4f19334cc8b68f256259". Under the input field, there is a disclaimer: "By submitting data above, you are agreeing to our Terms of Service and Privacy Notice, and to the sharing of your Sample submission with the security community. Please do not submit any personal information; we are not responsible for the contents of your submission. Learn more." At the bottom, there is a link: "Want to automate submissions? Check our API, or access your API key."

Navigate to details, the creation date can be found there:

History	
Creation Time	2020-08-01 02:44:18 UTC
First Submission	2022-03-06 15:45:53 UTC
Last Submission	2024-11-17 19:26:06 UTC
Last Analysis	2024-11-27 12:54:13 UTC

Analyzing PE Headers:

In the attached VM, there is a sample named 'redline' in the directory Desktop/Samples. What is the entropy of the .text section of this sample?

```
jubuntu@ip-10-10-40-51:~/Desktop/Samples$ pecheck redline
PE check for 'redline':
Entropy: 7.999627 (Min=0.0, Max=8.0)
MD5 hash: ca2dc5a3f94c4f19334cc8b68f256259
SHA-1 hash: ce9943d9efc7d5f10cac4ab0b5aa48d62a063852
SHA-256 hash: e8ba49a75de083cb786e8ed84972affa11542dd913f1a07b0d44e1d45e5e22e9
SHA-512 hash: 8c774f64631342c2465d166cd4c374356c40c1cf6bae13b2e0b003ce6c85e397da799f111cbbed638d548029c555f31156c2633d531fa1b20160d7904fa17d75
.text entropy: 6.453919 (Min=0.0, Max=8.0)
.rdata entropy: 5.136718 (Min=0.0, Max=8.0)
.data entropy: 4.096809 (Min=0.0, Max=8.0)
.ndata entropy: 0.000000 (Min=0.0, Max=8.0)
.rsrc entropy: 4.209687 (Min=0.0, Max=8.0)
Dump Info:
-----DOS_HEADER-----
[IMAGE_DOS_HEADER]
0x0 0x0 e_magic: 0x5A4D
0x2 0x2 e_cblp: 0x90
0x4 0x4 e_cp: 0x3
0x6 0x6 e_cblp: 0x0
```

The sample named 'redline' has five sections. .text, .rdata, .data and .rsrc are four of them. What is the name of the fifth section?

Answer: .ndat

From which dll file does the sample named 'redline' import the RegOpenKeyExW function?

```
ADVAPI32.dll.RegCreateKeyExW Hint[466]
ADVAPI32.dll.RegEnumKeyW Hint[480]
ADVAPI32.dll.RegQueryValueExW Hint[504]
ADVAPI32.dll.RegSetValueExW Hint[517]
ADVAPI32.dll.RegCloseKey Hint[459]
ADVAPI32.dll.RegDeleteValueW Hint[473]
ADVAPI32.dll.RegDeleteKeyW Hint[471]
ADVAPI32.dll.AdjustTokenPrivileges Hint[28]
ADVAPI32.dll.LookupPrivilegeValueW Hint[336]
ADVAPI32.dll.OpenProcessToken Hint[428]
ADVAPI32.dll.SetFileSecurityW Hint[559]
ADVAPI32.dll.RegOpenKeyExW Hint[493]
ADVAPI32.dll.RegEnumValueW Hint[482]
```

Answer: ADVAPI32.dll

Basic Dynamic:

Check the hash of the sample 'redline' on Hybrid analysis and check out the hybrid analysis report. In the process tree, which is the first process launched when the sample is launched?

Answer: setup_installer.exe

Start by searching the MD5 hash in hybrid-analysis.com:



File/URL File Collection Report Search YARA Search String Search

Search through 1.1B+ Indicators of Compromise (IOCs).

ca2dc5a3f94c4f19334cc8b68f256259 Search

or

Advanced Search

Maximum upload size is 100 MB.
Powered by **CrowdStrike Falcon® Sandbox**.
[Interested in a free trial?](#)

Releases & Updates

Introducing Community Score on Hybrid Analysis
October 24, 2024

Hybrid Analysis Integrates Criminal IP for Enhanced Threat Analysis
October 24, 2024

[See More!](#)

Hybrid Analysis

Tip: Click an analysed process below to view more details.

Analysed 17 processes in total.

- redline.exe** (PID: 1888) 62/70 Hash Seen Before
- setup_installer.exe** (PID: 3900) 41/70 Hash Seen Before
- cmd.exe** %WINDIR%\system32\cmd.exe /c powershell -inputformat none -outputformat none -Noninteractive -Command Add-MpPreference -ExclusionPath %TEMP%\ (PID: 2712) Hash Seen Before
- powershell.exe** powershell -inputformat none -outputformat none -Noninteractive -Command Add-MpPreference -ExclusionPath %TEMP%\ (PID: 7528) Hash Seen Before
- cmd.exe** %WINDIR%\system32\cmd.exe /c 62237fa25bdfc_Sat15d93b81243b.exe (PID: 8096) Hash Seen Before
- cmd.exe** %WINDIR%\system32\cmd.exe /c 62237fa38bcf4_Sat15f98352f48.exe (PID: 3364) Hash Seen Before
- cmd.exe** %WINDIR%\system32\cmd.exe /c 62237fa44c09c_Sat15f6e00f22a4.exe (PID: 3352) Hash Seen Before
- cmd.exe** %WINDIR%\system32\cmd.exe /c 62237fa56f568_Sat15e879a10c5.exe (PID: 2676) Hash Seen Before
- cmd.exe** %WINDIR%\system32\cmd.exe /c 62237fa63049c_Sat15e844a2af9.exe (PID: 2812) Hash Seen Before
- cmd.exe** %WINDIR%\system32\cmd.exe /c 62237fa8c3051_Sat155c8dc0cfb2.exe (PID: 2820) Hash Seen Before
- cmd.exe** %WINDIR%\system32\cmd.exe /c 62237fa9b2b38_Sat157d1e38e.exe (PID: 2836) Hash Seen Before
- cmd.exe** %WINDIR%\system32\cmd.exe /c 62237fab2cfab_Sat1500aa1ec1ab.exe (PID: 2880) Hash Seen Before
- cmd.exe** %WINDIR%\system32\cmd.exe /c 62237fad01b21_Sat15bb83952787.exe /mixtwo (PID: 3048) Hash Seen Before
- cmd.exe** %WINDIR%\system32\cmd.exe /c 62237fad2cc5_Sat151a15a05.exe (PID: 5908) Hash Seen Before
- cmd.exe** %WINDIR%\system32\cmd.exe /c 62237fafd9ca1_Sat1555ade0f.exe (PID: 7064) Hash Seen Before
- cmd.exe** %WINDIR%\system32\cmd.exe /c 62237fb0d0dd1_Sat159fc8bb76b4.exe (PID: 6580) Hash Seen Before

Logged Script Calls Logged Status Extracted Streams Memory Dumps

Reduced Monitoring Network Activity Network Error Multiscan Match

- Incident Response
- Related Sandbox Artifacts
- Indicators
- CrowdStrike AI
- File Details
- Screenshots (3)
- Hybrid Analysis (7)**
- Network Analysis
- Extracted Strings
- Extracted Files (22)
- Notifications
- Community (1)
- [Back to top](#)

In the process tree, there are two Windows utilities utilized by the malware to perform its activities. What are the names of the two utilities?

Answer: cmd.exe and powershell.exe