

## Static Analysis

### 1. Virus Total Analysis

#### Hash Analysis

- File Hash: [Insert MD5, SHA-1, SHA-256 hash value]
  - MD5: a07ea73aaebe8be23dee196bde83e083
    - Verified on detect-it-easy
  - SHA-1: 0309273eb6bf0909143c656e286c05e40497fff8
    - Verified on detect-it-easy
  - SHA-256: f5158ada735739aee5bc2b07a92368f2817da2a3e16c1fce0ba365bedf54e6d0
    - Verified on detect-it-easy
- Method of hash acquisition: [Describe process]
  - Found on VirusTotal, verified by detect-it-easy
- [Link to VirusTotal results]
  - <https://www.virustotal.com/gui/file/f5158ada735739aee5bc2b07a92368f2817da2a3e16c1fce0ba365bedf54e6d0/details>

#### Vendor Analysis

- Number of vendors flagging as malicious: [38/73]
- Analysis of vendor results:
  - [Discuss patterns in detection]
    - Most major antivirus vendors flagged the file as a trojan, with many associating it with Cobalt Strike (CobaltSC) and Wacatac/Wacapew malware families. These names suggest the sample is likely linked to penetration testing tools turned malicious (Cobalt Strike beacons) or generic trojan droppers. **I identified the type / family of malware.**
    - Several vendors also highlighted persistence mechanisms, privilege escalation, and defense evasion techniques, aligning with MITRE ATT&CK tactics TA0003, TA0004, and TA0005.
  - [Common malware names identified]
    - CobaltSC / Cobalt Strike (Alibaba, CTX, Ikarus, Lionix, Kaspersky)
    - Win32/Wacatac (Microsoft)
    - Wacapew (AliCloud, Antiy-AVL)
    - Trojan.GenericKD.76104529 (BitDefender, Emsisoft, GData, Trellix)
    - Trojan.Win32.BSOD.cwr (Kaspersky)
    - Artemis!A07EA73AAEBE (Trellix ENS)
    - ML.Attribute.HighConfidence (Symantec)
  - [Notable vendor disagreements]
    - Undetected by 30+ vendors: A significant number of antivirus, including SentinelOne, Palo Alto Networks, Malwarebytes, CrowdStrike, and ClamAV, did not detect this sample.
    - Alibaba flagged the file as a Cobalt Strike Trojan, AliCloud classified it as Wacapew, Microsoft

classified it as Wacatac.B!ml, Kaspersky identified it as BSOD.cwr, Elastic assigned a moderate confidence rating, Cylance outright flagged it as unsafe

#### File History

- First Submission Date: [Date]
  - First Submission: 2025-03-19 22:23:01 UTC
- File Creation Date from Windows: [Date]
  - Creation Time: 2025-03-17 20:08:13 UTC
- Analysis of submission timeline:
  - [Discussion of file age]
    - It was released 2 days after it was created, and it was only created last week
  - [Notable resubmissions or changes]
    - It was submitted under 3 different names: Week8.exe, week8.exe, malware\_fun.exe
    - This short window suggests that the file was either quickly flagged as suspicious by a security system or intentionally submitted soon after its development. Given that the file was created less than a week ago, it is likely a recently developed or modified sample.

#### Community Score

- [Link to your VirusTotal community contribution]
  - <https://www.virustotal.com/gui/file/f5158ada735739aee5bc2b07a92368f2817da2a3e16c1fce0ba365bedf54e6d0/community>
  - I created a Virus Total comment and provided a username.
- Summary of initial findings posted to the community:

##### Comments (6) ⓘ



sshinn

a moment ago



Week8.exe is a Trojan that creates malware\_fun.exe and hello\_STUDENTS\_41.454 modifying system settings to change the desktop wallpaper and ensure persistence via a registry key. The malware modifies registry key (HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run) to ensure it runs on startup. It blocks access to VirusTotal. The malware is linked to Cobalt Strike activity.

## 2. Detect It Easy (DIE) Analysis

#### File information

- File type: [PE64]
- Architecture: [AMD64]
- Compiler: [Compiler information]
  - Compiler: MinGW(GCC: (x86\_64-posix-seh-rev0, Built by MinGW-W64 project) 8.1.0)
- Additional relevant information:
  - [List notable file characteristics]
    - Language: C
    - Operation system: Windows(Server 2003)
    - Size: 4345856(4.14 MB)
    - (Heur)Packer: Compressed or packed data[High entropy + Section 9 (".rsrc") compressed]

- [Unusual headers or structures]
  - Overlay: Binary[Offset=0x0041d340,Size=0xc0]
  - .pdata
  - .xdata
  - .bss
  - .idata
  - .CRT
  - .tls

#### Memory Map Analysis

- Section breakdown:
  - .text
    - Size: 00002600
    - Permissions: RE
    - Info: (Compiler) Code Section
  - .data
    - Size:00000200
    - Permissions: RW
    - Info: (Compiler) Data Section
  - .rdata
    - Size: 00000c00
    - Permissions:R
    - Info: (Compiler) Read-only initialized Data Section (MS and Borland)
  - .pdata
    - Size: 00000400
    - Permissions: R
    - Info: (Compiler) Exception Handling Functions Section (PDATA records)
  - .xdata
    - Size:00000400
    - Permissions:R
    - info:(Compiler) Exception Information Section
  - .bss
    - Size:00000000
    - Permissions:RW
    - info:(Compiler) Uninitialized Data Section
  - .idata
    - Size:00000c00
    - Permissions:RW
    - info:(Compiler) Initialized Data Section (Borland) | (Compiler) mingw/cygwin
  - .CRT
    - Size:00000200
    - Permissions:RW
    - info:(Compiler) Initialized Data Section (C RunTime) | (Compiler) mingw/cygwin
  - .tls
    - Size:00000200
    - Permissions:RW
    - info:(Compiler) Thread Local Storage Section

- .rsrc
  - Size:00418340
  - Permissions:RW
  - info:(Compiler) Resource section
- Notable findings:
  - [Unusual section permissions]
    - The .rsrc section is usually read-only (R) because it contains embedded resources such as icons, manifests, and version information. The presence of write (W) permissions could be a sign of malware behavior.
    - .idata and .CRT having write permissions could be an indicator of malicious behavior, because they could make runtime modifications
  - [Section size anomalies]
    - .rsrc size = 0x418340 (4 MB+) This is unusually large for a typical resource section
  - I conducted a file analysis and identified what was unique or suspicions of this file.

#### String Analysis

- Notable strings discovered:
  - [URLs/IPs]
    - 127.0.0.1 virustotal.com (This is the hosts file blocking access to VirusTotal)
  - [File paths]
    - %s\hello\_STUDENTS\_%d.454
    - %s\warning.jpg
    - %s\malware\_fun.exe
    - C:\Windows\System32\drivers\etc\hosts
  - [Command lines]
    - None observed
  - [API calls]
    - RtlAdjustPrivilege - Attempts to escalate privileges.
    - NtRaiseHardError - Can be used to cause system crashes or bypass security mechanisms.
    - TerminateProcess - Can be used to kill security-related processes.
    - RegOpenKeyExA - Opens registry keys, often used for persistence.
    - RegSetValueExA - Modifies registry values, possibly for auto-starting malware.
    - SHGetFolderPathA - Retrieves system folder paths, which can be used to drop malicious files in startup locations.
    - CopyFileA - Could be used to spread the malware or copy itself to a different location.
    - GetModuleHandleA - Resolves module handles, possibly for function hooking.
    - GetProcAddress - Dynamically resolves API functions, often seen in malware using indirect system calls.
    - GetTickCount - Can be used for timing-based sandbox

- detection.
  - QueryPerformanceCounter - Often used to detect debugging environments.
  - VirtualProtect - Modifies memory protection, often used in code injection or shellcode execution.
  - VirtualQuery - Can be used to scan memory for security software or hooks.:
  - SystemParametersInfoA - Can be used to modify system settings, such as changing the wallpaper as indicated in the malware strings.
  - SetUnhandledExceptionFilter - Can be abused to handle or suppress exceptions, sometimes used for anti-debugging.
- Analysis of string findings:
  - [Potential functionality indicated]
    - Persistence:
      - Registry: RegOpenKeyExA, RegSetValueExA
      - Startup Folder: SHGetFolderPathA, CopyFileA
        - malware may copy itself to the Startup folder to ensure execution on reboot.
    - RtlAdjustPrivilege
      - Attempts to escalate privileges
    - System Crash/BYPASS Mechanism: NtRaiseHardError
      - Could be used to crash the system
    - TerminateProcess
      - the malware might kill security processes (e.g., antivirus, system monitoring tools)
    - VirtualProtect
      - for executing shellcode or injecting malicious code.
    - VirtualQuery
    - GetModuleHandleA, GetProcAddress
    - Wallpaper Manipulation: SystemParametersInfoA
      - the malware may change the desktop wallpaper
    - Network:
      - C:\Windows\System32\drivers\etc\hosts modification (127.0.0.1 virustotal.com)
  - [Suspicious patterns]
    - %s\malware\_fun.exe
    - Use of TerminateProcess combined with file deletion messages like [INFO] Boom. File deleted: %s suggests the malware may delete itself
    - Strings such as "I hope you are not scared of the dark, I put a little surprise inside for you this week!" and "Here goes another little fun thing for you today!"

#### Entropy Analysis

- Overall entropy score: [Score]
  - 7.76286, 97% packed
- Section-specific entropy:

- [List sections with unusual entropy]
  - All sections besides .rsrc section are unpacked
  - The .rsrc section is packed, it has entropy of 7.76982
- Packing analysis:
  - [Packed/Unpacked determination]
    - It has a packed .rsrc section
  - [Packer identified (if applicable)]
    - The packer is not identified
  - [Unpacking methodology (if attempted)]
    - I inspected the .rsrc section using ResourceHacker and found 9 sec
  - [Alternative unpacking approaches (if needed)]
    - I tried using UnPac.Me, it did not work
    - I used Resource Hacker to unpack the .rsrc section and found the following information
      - I found 9 icons of different and increasing sizes
      - I found the following file information:

VALUE "CompanyName", "University of Arizona"

VALUE "FileDescription", "Spring 2025 Week 8 Malware Analysis"

VALUE "FileVersion", "1.0.0.0"

VALUE "InternalName", "week8.exe"

VALUE "LegalCopyright", "\xA9 2025 Michael Galde. All rights reserved."

VALUE "OriginalFilename", "week8.exe"

VALUE "ProductName", "Week8"

VALUE "ProductVersion", "1.0.0"

#### 4. Disassembly Analysis

- Found entrypoint
- Identified a suspicious function
- clues:
  - "SuspiciousEntry\_004052f6
  - What\_are\_you\_looking\_for?
  - [->ADVAPI32.DLL::RegSetValueExA]
  - [->ADVAPI32.DLL::RegCloseKey]
  - "[INFO] Registry clue added: HKEY\_CURRENT\_USER\\%s\\%s\n"
  - SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Registry changes for persistence!

Disassembly clues point to registry changes:

ADVAPI32.DLL::RegSetValueExA. This function is responsible for writing values into the Windows Registry. The registry path being modified (SOFTWARE\Microsoft\Windows\CurrentVersion\Run) is an autostart location where programs can be configured to run automatically upon user login, which is a persistence tactic. ADVAPI32.DLL::RegCloseKey. After modifying the registry, the malware closes the key handle. "Registry clue added: HKEY\_CURRENT\_USER\\%s\\%s\n". The use of HKEY\_CURRENT\_USER (HKCU) rather than HKEY\_LOCAL\_MACHINE (HKLM) suggests it doesn't require administrator privileges—it targets the current user instead.

\*\*\*My dynamic analysis confirms that this malware achieves persistence through a registry Run key labeled "SuspiciousEntry"

I used a disassembler and used my dynamic analysis findings to aid disassembler review of the malicious analysis.

```

Listing: Week8.exe

LAB_004014d2
004014d2 0f 1f 40 00    NOP             dword ptr [RAX]
004014d6 66 2e 0f      NOP             word ptr CS:[RAX + RAX*0x1]
1f 84 00
00 00 00 00

*****
*                               FUNCTION
*****
undefined entry()
AL:1 <RETURN>
entry
XREF[3]: Entry Point(*), 0040603c(*)

004014e0 48 83 ec 28    SUB            RSP,0x28
004014e4 48 8b 05      MOV            RAX,qword ptr [PTR_DAT_004059c0]
d5 44 00 00
004014eb c7 00 00      MOV            dword ptr [RAX]>=DAT_00408610,0x0
00 00 00
004014f1 e8 aa 08      CALL           FUN_00401da0
00 00
004014f6 e8 85 fc      CALL           FUN_00401180
ff ff
004014fb 90            NOP
004014fc 90            NOP
004014fd 48 83 c4 28    ADD            RSP,0x28

```

```

Listing: Week8.exe

s_[ERROR]_Failed_to_copy_EXE_to_St_00405298 XREF[1]: FUN_00401a30:00401aaa(*)
00405298 5b 45 52      ds             "[ERROR] Failed to copy EXE to Startup folder."
52 4f 52
5d 20 46 ...

004052c6 00            ??            00h
004052c7 00            ??            00h

s_SOFTWARE\Microsoft\Windows\Curre_004052c8 XREF[2]: FUN_00401b00:00401b14(*)
                                                FUN_00401b00:00401b70(*)
004052c8 53 4f 46      ds             "SOFTWARE\Microsoft\Windows\CurrentVersion\...
54 57 41
52 45 5c ...

s_SuspiciousEntry_004052f6 XREF[2]: FUN_00401b00:00401b44(*)
                                                FUN_00401b00:00401b69(*)
004052f6 53 75 73      ds             "SuspiciousEntry"
70 69 63
69 6f 75 ...

s_What_are_you_looking_for?_00405306 XREF[2]: FUN_00401b00:00401b2f(*)
                                                FUN_00401b00:00401b53(*)
00405306 57 68 61      ds             "What are you looking for?"
74 20 61
72 65 20 ...

s_[INFO]_Registry_clue_added:_HKEY_00405320 XREF[1]: FUN_00401b00:00401b77(*)
00405320 5b 49 4e      ds             "[INFO] Registry clue added: HKEY_CURRENT_USER...
46 4f 5d
20 52 65 ...

```

## Static Analysis Summary

- Key findings from static analysis:
  - [Major indicators of malicious behavior]
    - The file is flagged as a trojan by 38 out of 73 antivirus vendors on VirusTotal. It is associated with Cobalt Strike (penetration testing tool abused by attackers) and Wacatac/Wacapew malware families.
    - Packed .rsrc section: Unusually large .rsrc section (4MB) with high entropy (7.76), indicating packing or obfuscation.
  - [Potential functionality]
    - Potential self-deletion
    - The malware modifies registry keys (HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run) to ensure it runs on startup. Registry modifications ensure execution at login.
    - Uses RtlAdjustPrivilege (to escalate privileges), VirtualProtect (potential code injection), VirtualQuery (anti-analysis technique), and TerminateProcess (likely to kill security processes).
    - Privilege escalation
    - SystemParametersInfoA could change the desktop wallpaper
  - [Risk indicators]
    - Operates under HKEY\_CURRENT\_USER, meaning it doesn't need elevated permissions to persist.
    - Network manipulation: It modifies the Windows hosts file to block access to VirusTotal.
  - I provided an overall analysis for my static analysis and provided my steps and methodology.

## Dynamic Analysis

### 1. Analysis Environment

#### Environment Setup

- Virtual Machine specifications:
  - [OS version] Windows 10 Home
  - [Memory allocation] 8 GB
  - [Network configuration] not connected to internet
- Monitoring tools deployed:
  - [Process monitoring]
    - I am using RegShot, Process Monitor, Process Explorer
  - [Network monitoring]
    - I am using Wireshark
  - [File system monitoring]
  - I used ANYRUN
- Safety measures implemented:
  - [Network isolation]



- Not connected to the internet
- [Snapshot configuration]
  - I can reset the virtual machine
- [Additional protections]
  - I am using a virtual machine that is not connected to the internet and that can be reverted to a snapshot

## 2. Runtime Observations

### Initial Execution

- [Immediate system changes]
  - Command window opened, it said "I hope you are not scared of the dark, I put a little surprise inside for you this week"
  - Wallpaper changed successfully!
  - Executable added to startup
  - Registry clue added
  - Try running the program as Administrator
  - Window Self Destruct Activated
  - The wallpaper was changed to a dragon
- [Process creation]
  - Week8.exe
  - conhost.exe
  - SppExtComObj.exe
  - slui.exe
  - PLUGScheduler.exe
  - malware\_fun.exe
- [Registry creation]
  - HKEY\_CURRENT\_USER\Microsoft\Windows...
- [Network activity]
  - SearchApp.exe
  - desktop-jglljld
  - 224.0.0.251
- [File system changes]
  - hello\_STUDENTS\_41.454 is created on Desktop
  - I took a screenshot of the contents of the file in Notepad

### Continued Monitoring

- [Persistent changes]
  - Malware is persistent, stays running on system whenever I close and then open up the virtual machine and restarts itself on startup
- [Scheduled tasks]
  - It reruns itself every time I turn on the system, a command prompt opens with the messages shown in my screenshot
- [Registry modifications]
  - Registry clue added: HKEY\_CURRENT\_USER\\%s\\%s\n"
- [Additional payloads]
- I provided dynamic analysis using tools to aid in the identify activity.

## 3. Post-Execution Analysis

- System state changes:

- [Permanent modifications]
  - The wallpaper was changed to an image of a dragon.
  - A new file hello\_STUDENTS\_41.454 was created on the Desktop.
  - A new executable malware\_fun.exe was added to the startup folder.
  - Registry modifications were made to establish persistence.
  - A scheduled task was created to rerun the malware on system startup.
- [Persistence mechanisms]
  - The malware added an entry to HKEY\_CURRENT\_USER\Microsoft\Windows\...\Startup to execute on boot.
  - The malware set up a scheduled task to execute itself when the system restarts.
  - malware\_fun.exe was added to the Windows startup folder, ensuring it launches at boot.
- [Data exfiltration evidence]
  - The process SearchApp.exe initiated a network request.
  - A connection was attempted to 224.0.0.251, a multicast address, which may indicate C2 communication
- Network activity summary:
  - The malware attempted outbound connections using SearchApp.exe.
  - It contacted 224.0.0.251
  - desktop-jglljld may be an infected system or a local host communicating with the malware.
  - I identified identified Network-Based Indicator which are Indicators associated with a network communication, such as an IP address or domain name

Analysis Week8.exe (MD5: A07E73AAEBE8BE23DEE1968DE83E083)

app.any.run/tasks/22ccb0bd-4af4-4964-9d2d-6e0d3f647377

Tools Social Media and O... Recon Additional Recon Email Search Dev OSINT GLTR (glitter) v0.5

Win10 64bit

Week8.exe  
MD5: A07E73AAEBE8BE23DEE1968DE83E083  
Start: 24.03.2025, 05:11

02:22

CPU 59% RAM 34%

Processes Filter by PID or name Only Important

Reboots Initial 1

3668	SCH	PLUGScheduler.exe	0	0	25

HTTP Requests 6 Connections 26 DNS Requests 17 Threats 0

Timeshift	Status	Rep	Domain	IP
BEFORE	Responded	✓	settings-win.data.microsoft.com	4.231.128.59
BEFORE	Responded	✓	cr1.microsoft.com	23.216.77.18
BEFORE	Responded	✓	google.com	216.58.206.78

Analysis Week8.exe (MD5: A07E73AAEBE8BE23DEE1968DE83E083)

app.any.run/tasks/22ccb0bd-4af4-4964-9d2d-6e0d3f647377

Tools Social Media and O... Recon Additional Recon Email Search Dev OSINT GLTR (glitter) v0.5

Win10 64bit

Week8.exe  
MD5: A07E73AAEBE8BE23DEE1968DE83E083  
Start: 24.03.2025, 05:11

02:04

CPU 0% RAM 36%

Processes Filter by PID or name Only Important

Reboots Initial 1

3668	SCH	PLUGScheduler.exe	470	30	25

5960	malware_fun.exe	PE	114	19	25

6760	conhost.exe	0xffffffff-ForceV1	582	32	36

HTTP Requests 6 Connections 38 DNS Requests 21 Threats 0

Timeshift	Status	Rep	Domain	IP
BEFORE	Responded	✓	settings-win.data.microsoft.com	4.231.128.59
BEFORE	Responded	✓	cr1.microsoft.com	23.216.77.18
BEFORE	Responded	✓	google.com	216.58.206.78

Impact Analysis

## 1. User Impact Assessment

### Home Users

- [Potential impact]
  - The malware can change system wallpaper, create unexpected files, and modify registry settings for persistence
- [Risk level]
  - High. The malware demonstrates persistent behavior
- [Data compromise potential]
  - While there was no direct indication of data exfiltration, the network activity suggests potential for communication with a command and control server

### Business Users

- [Operational impact]
  - The malware's capacity to execute on startup and modify system settings may lead to business disruptions
- [Data security concerns]
  - The behavior of the malware rebooting and shutting down the machine could make it impossible to recover data on the infected machine
- [Financial implications]
  - Costs associated with cleanup, incident response, and potential data loss could be significant. Additionally, potential downtime could impact revenue

### Government Users

- [Security implications]
  - Government systems often hold sensitive data and critical operations. This malware could pose risks to national security
- [Data sensitivity concerns]
  - This malware is capable of transmitting confidential data over a network, and impacts the accessibility of data by shutting down and rebooting the system over and over
- [Operational disruption potential]
  - disruptions could affect critical infrastructure and services

## 2. Mitigation Strategy

### Immediate Response

- [Initial containment steps]
  - Disconnect the infected system from any network
- [System isolation procedures]
  - Create a forensic image of the current system state for analysis while isolating the infected machine from the network
- [Data preservation methods]
  - Backup critical files

### Long-term Prevention

- [Security control recommendations]
  - Regularly update security software
- [Policy modifications]

- Develop and enforce policies around software installation, restricting user privileges
- [Training requirements]
  - Provide security training for users about the dangers of unknown software, phishing, and recognizing signs of malware.

## Conclusion

### 1. Analysis Reflection

- [Summary of findings]
  - The file likely represents a trojan associated with CobaltStrike. The behaviors observed such as changing wallpaper, modifying registry for persistence, and attempting network connectivity suggest malicious intent
- [Unusual characteristics]
  - large .rsrc section with high entropy indicates packing.
- [Learning outcomes]
  - malicious software can exploit user-level permissions
- [Additional research needed]
- The static analysis identified characteristics of the malware, such as type, potential malicious behavior, persistence mechanisms, and indicators of compromise (such as high entropy in packed .rsrc section).
- The dynamic analysis, on the other hand, validated many of those static findings by observing the actual behavior of the malware. It captured the execution of the malware, such as system changes (changing wallpaper, creating new files), persistence through registry modifications, and potential network actions.
- I provided an analysis comparing the results from my static and dynamic analyses. I explained steps and my methodology

### 2. Evidence Documentation

- [Screenshot descriptions and relevance]
- [Tool output documentation]
- [Additional supporting materials]
- I identified Host-based IoC #1 which are indicators that suggest suspicious activity on a specific computer or system.
- IoC #1: 38/73 vendors flagged as malicious, with most of them saying that this malware is a trojan linked to CobaltStrike
- I identified Host-based IoC #2 which are indicators that suggest suspicious activity on a specific computer or system.
- IoC #2: Strings such as "I hope you are not scared of the dark, I put a little surprise inside for you this week!" and "Here goes another little fun thing for you today!" along with the string %s\malware\_fun.exe indicate that this file is suspicious
- Also, many suspicious api calls such as VirtualProtect - Modifies memory protection, often used in code injection or shellcode execution.
- I identified Host-based IoC #3 which are indicators that suggest suspicious activity on a specific computer or system.

IoC#3: Disassembly clues point to registry changes:  
ADVAPI32.DLL::RegSetValueExA. This function is responsible for writing values into the Windows Registry. The registry path being modified (SOFTWARE\Microsoft\Windows\CurrentVersion\Run) is an autostart location where programs can be configured to run automatically upon user login, which is a persistence tactic. ]