BLACKSWAN CYBERSECURITY

THREAT ADVISORY

RedSun Zero-Day (Windows Defender)

April 17, 2026

Severity: High
CVSS Score: Not yet assigned (0-day local privilege escalation)
Affected Systems: Windows 10, Windows 11, and Windows Server 2019+ with Microsoft Defender Antivirus real-time protection enabled (remains exploitable on systems with the April 2026 Patch Tuesday updates applied)
Exploited in the Wild: Yes (confirmed by Huntress and other MDR providers as of April 16, 2026)

Summary

A publicly disclosed proof-of-concept (PoC) for a vulnerability nicknamed **"RedSun"** was published on April 15, 2026, in the GitHub repository **Nightmare-Eclipse/RedSun**. The flaw stems from a logic error in Microsoft Defender's handling of files marked with a **cloud tag** (via the Windows Cloud Files API). Instead of quarantining or deleting a detected malicious file, Defender can rewrite/restore the file to its original location with elevated privileges. Attackers abuse this behavior, combined with NTFS directory junctions (reparse points), opportunistic locks (oplocks), and Cloud Files API tricks, to redirect Defender's privileged write operation and overwrite protected system files.

(most commonly C:\Windows\System32\TieringEngineService.exe)

This results in **local privilege escalation to SYSTEM** when the Cloud Files Infrastructure service executes the attacker-controlled binary.

This is the second Defender-related LPE PoC released by the same researcher (following BlueHammer/CVE-2026-33825, patched April 14, 2026), apparently in protest of Microsoft's vulnerability disclosure practices. A companion tool called **UnDefend** can disable or starve Defender of signature updates. The RedSun repository contains the full C++ source (RedSun.cpp), though the author noted they intentionally avoided a "simple drop" because "it's way too funny".

Vulnerability Details

- **Root Cause**: Defender's remediation logic for cloud-tagged files performs an unvalidated rewrite/restore to the original path instead of safe deletion or quarantine.
- **Exploit Chain** (high-level, per independent verification):
    1. Create a crafted file containing an EICAR test string (or equivalent) and mark it with a cloud tag via the Cloud Files API.
    2. Use oplocks to win a race condition against Defender's volume shadow copy scanning.
    3. Swap a directory junction/reparse point to redirect Defender's privileged write operation.

4. Defender "helpfully" rewrites the malicious payload into a protected system location (e.g., C:\Windows\System32\TieringEngineService.exe).
5. The Cloud Files Infrastructure service executes the overwritten binary as **SYSTEM**.

- **Impact**: Any low-privileged local user can achieve full SYSTEM access without kernel exploits, admin rights, or network connectivity. This enables persistence, credential dumping, ransomware deployment, lateral movement, or complete host takeover.
- **Requirements**: Microsoft Defender real-time protection must be enabled and cldapi.dll present (standard on all supported Windows versions). No other privileges needed.

The PoC is reliable **(~100% success rate on fully patched systems)** and has been independently validated by security researchers.

Observed Exploitation

Threat actors began actively weaponizing RedSun (often paired with BlueHammer and UnDefend) in real incidents as of April 16, 2026. Observed tactics include:

- Dropping renamed exploit binaries into user-writable folders such as **Pictures** or **Downloads**.
- Using the exploit to gain SYSTEM after initial access (e.g., via hijacked SSL VPN accounts).
- Combining with UnDefend to prevent Defender updates and maintain persistence.

Indicators of Compromise (IOCs)

Confirmed / Available IOCs (from vendor reporting and PoC analysis):

- **File Names** (dropped/renamed variants commonly observed):
  - RedSun.exe
  - FunnyApp.exe (or similar short/obfuscated names)
  - Other generic names placed in %USERPROFILE%\Pictures\ or %USERPROFILE%\Downloads\
- **Embedded Strings**: EICAR test file signature (or encrypted/obfuscated variants) inside the exploit binary.
- **Target File Modification**: Unexpected overwrite or replacement of C:\Windows\System32\TieringEngineService.exe (or other protected System32 binaries).
- **Behavioral Signs**:
  - Defender alerts involving cloud-tagged files or EICAR-like detections followed by file restoration.
  - Creation of NTFS junctions/reparse points or oplock activity in user directories.
  - Anomalous execution of binaries originating from user-writable locations under the Cloud Files Infrastructure service (running as SYSTEM).

THREAT ADVISORY

RedSun Zero-Day (Windows Defender)

April 17, 2026

Assumed / High-Confidence IOCs (based on exploit mechanics and early sightings):

- Presence of RedSun.cpp-derived binaries (check VirusTotal hashes for known variants; some are already detected as Program:Win32/Wacapew.C!ml).
- Process creation logs showing SYSTEM-level execution tied to Cloud Files API calls from untrusted parent processes.
- File system events showing directory junctions pointing to System32 paths from user context.

No official file hashes have been broadly published yet, but security teams should scan for the above patterns and monitor VirusTotal for new RedSun-related samples.

Detection Rules

Sigma Rules (for SIEM / EDR platforms supporting Sigma)

1. RedSun Exploit Binary Drop (File Creation)

```
YAML
title: RedSun Defender LPE Exploit Binary Dropped
id: 8f3a9b2c-4d5e-4f6a-9b2c-1d3e4f5a6b7c
status: experimental
description: Detects creation of known RedSun exploit binaries in user-writable
directories
author: Grok Threat Intel
date: 2026-04-17
logsource:
  category: file_event
  product: windows
detection:
  selection:
    TargetFilename|contains:
      - '\Pictures\RedSun.exe'
      - '\Pictures\FunnyApp.exe'
      - '\Downloads\RedSun.exe'
      - '\Downloads\FunnyApp.exe'
      - '\Downloads\z.exe'
    Image|endswith: '\explorer.exe'  # or other user processes
  condition: selection
level: high
tags:
  - attack.privilege_escalation
  - attack.t1068
```

2. Anomalous Modification of Protected System File by Defender

```
YAML
title: RedSun Defender Rewrite to System32
id: 9a4b5c6d-7e8f-9g0h-1i2j-3k4l5m6n7o8p
status: experimental
description: Detects unexpected writes to TieringEngineService.exe (common RedSun
target)
author: Grok Threat Intel
date: 2026-04-17
logsource:
  category: file_event
  product: windows
detection:
  selection:
    TargetFilename: 'C:\Windows\System32\TieringEngineService.exe'
    Image|contains: 'MsMpEng.exe'  # Defender engine performing the write
  condition: selection
level: critical
tags:
  - attack.privilege_escalation
  - attack.t1574
```

3. NTFS Junction / Reparse Point Abuse from User Context

```
YAML
title: RedSun NTFS Junction Creation for Privilege Escalation
id: a1b2c3d4-e5f6-g7h8-i9j0-k1l2m3n4o5p6
status: experimental
description: Detects junction point creation pointing toward System32 from user
processes
author: Grok Threat Intel
date: 2026-04-17
logsource:
  category: process_creation
  product: windows
detection:
  selection:
    CommandLine|contains:
      - 'mklink /J'
      - 'New-Item -ItemType Junction'
    CommandLine|contains: 'System32'
    User|contains: 'Users\\'  # executed from standard user context
  condition: selection
```

level: high

YARA Rules (for static file scanning)

1. RedSun Exploit Binary (Basic String-Based)

```
yara
rule RedSun_Exploit_Binary
{
   meta:
      description = "Detects RedSun Defender LPE exploit binary (RedSun.exe / FunnyApp.exe)"
      author = "Grok Threat Intel"
      date = "2026-04-17"
      reference = "https://github.com/Nightmare-Eclipse/RedSun"
   strings:
      $s1 = "RedSun" ascii fullword
      $s2 = "FunnyApp" ascii fullword
      $s3 = "cloud tag" ascii nocase
      $s4 = "cldapi.dll" ascii
      $s5 = "TieringEngineService" ascii
      $eicar = "X5O!P%@AP[4\\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*" ascii
   condition:
      uint16(0) == 0x5A4D and  // MZ header
      filesize < 2MB and
      (2 of ($s*)) or $eicar
}
```

2. RedSun Cloud File / Junction Helper Strings

```
yara
rule RedSun_CloudFile_Abuse_Strings
{
   meta:
      description = "Detects strings related to RedSun Cloud Files API and junction abuse"
      author = "Grok Threat Intel"
      date = "2026-04-17"
   strings:
      $a1 = "Cloud Files API" ascii nocase
      $a2 = "oplock" ascii nocase
      $a3 = "reparse point" ascii nocase
      $a4 = "CreateFileW" ascii
      $a5 = "SetFileInformationByHandle" ascii
```

```
    condition:
        uint16(0) == 0x5A4D and
        3 of them
}
```

Notes on Rules:

- These are **experimental** and should be tested in your environment to reduce false positives.
- Tune paths and add known-good exclusions (e.g., legitimate admin tools using junctions).
- For best coverage, combine with behavioral EDR rules monitoring Defender remediation events and Cloud Files API calls from non-OneDrive processes.

Recommendations

Immediate Actions:

- **Hunt for IOCs**: Scan user directories (especially Pictures/Downloads) for suspicious .exe files and monitor for modifications to TieringEngineService.exe. Review Defender event logs for cloud-file remediation or EICAR detections.
- **Behavioral Detection**: Enable or tune EDR/XDR rules to alert on:
    - Anomalous Defender writes to protected paths.
    - NTFS junction/oplock abuse from user processes.
    - Cloud Files API activity originating outside legitimate OneDrive/sync processes.

Mitigation Steps:

- Apply all Windows updates immediately (monitor MSRC for an emergency RedSun-specific patch. None released as of April 17, 2026).
- Supplement Defender with a secondary EDR solution (e.g., Huntress) capable of detecting Defender bypasses.
- Run Defender in passive mode (with alternative real-time protection) in high-risk or internet-facing environments.
- Enforce strict least-privilege access and block unnecessary Cloud Files API usage where possible.
- Enable Microsoft Defender tamper protection and audit Event Logs for privileged service executions from user-writable paths.
- Consider temporary network-level blocks on the GitHub repository (though compiled variants are already circulating widely).

Detection Opportunities:

- **Windows Security Event Logs**: Look for Defender events (e.g., file restoration) and process creation under SYSTEM from unexpected sources.

- **File integrity monitoring** on System32.
- **Behavioral analytics** for junction point creation and Cloud Files API calls.

References

- GitHub Repository (including full source and author notes): https://github.com/Nightmare-Eclipse/RedSun
- Related Tools: BlueHammer (prior LPE) and UnDefend (Defender DoS)
- Vendor Reporting: Huntress Labs, BleepingComputer, The Hacker News, and independent validation by Will Dormann

Contact Blackswan Cybersecurity at 855-BLK-SWAN or Contact@Blackswancybersecurity.com