SORINTSEC

THREAT HUNTING

LAB

BlueHammer windows Zero-Day

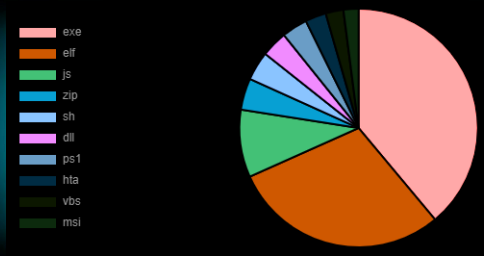
PUBLIC

Index

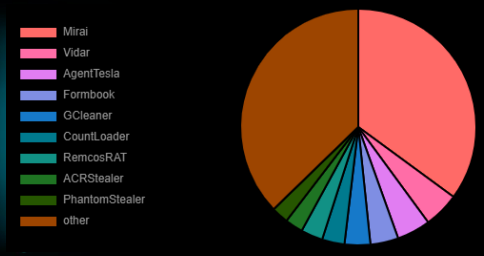
Global Weekly Threat Overview

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.

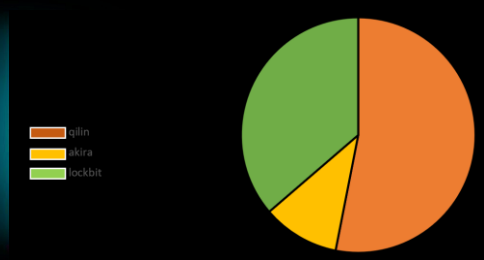
Top 10 file types



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.

Global Weekly Notable One

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

SORINTSEC

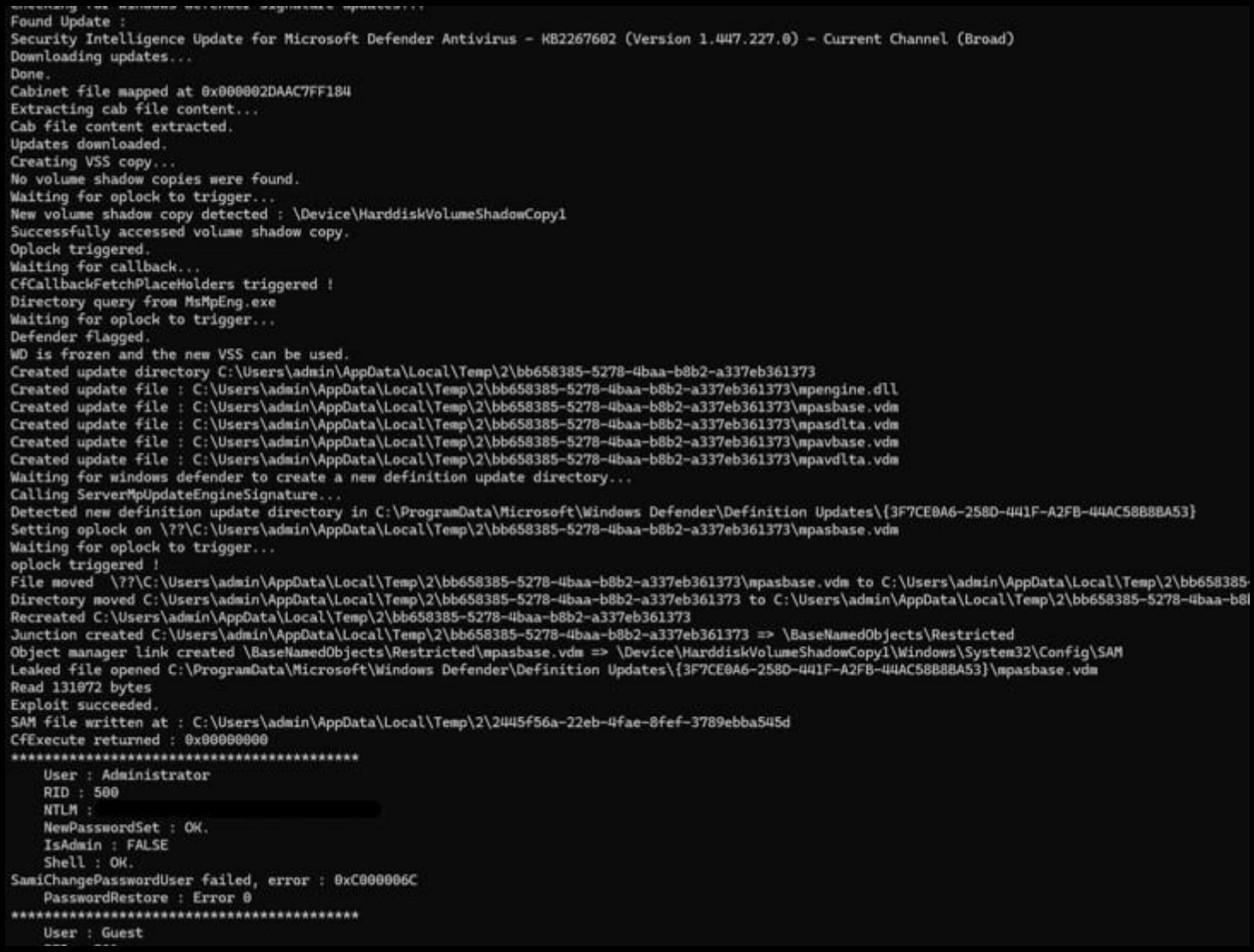
TACTIC Privilege Escalation

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.

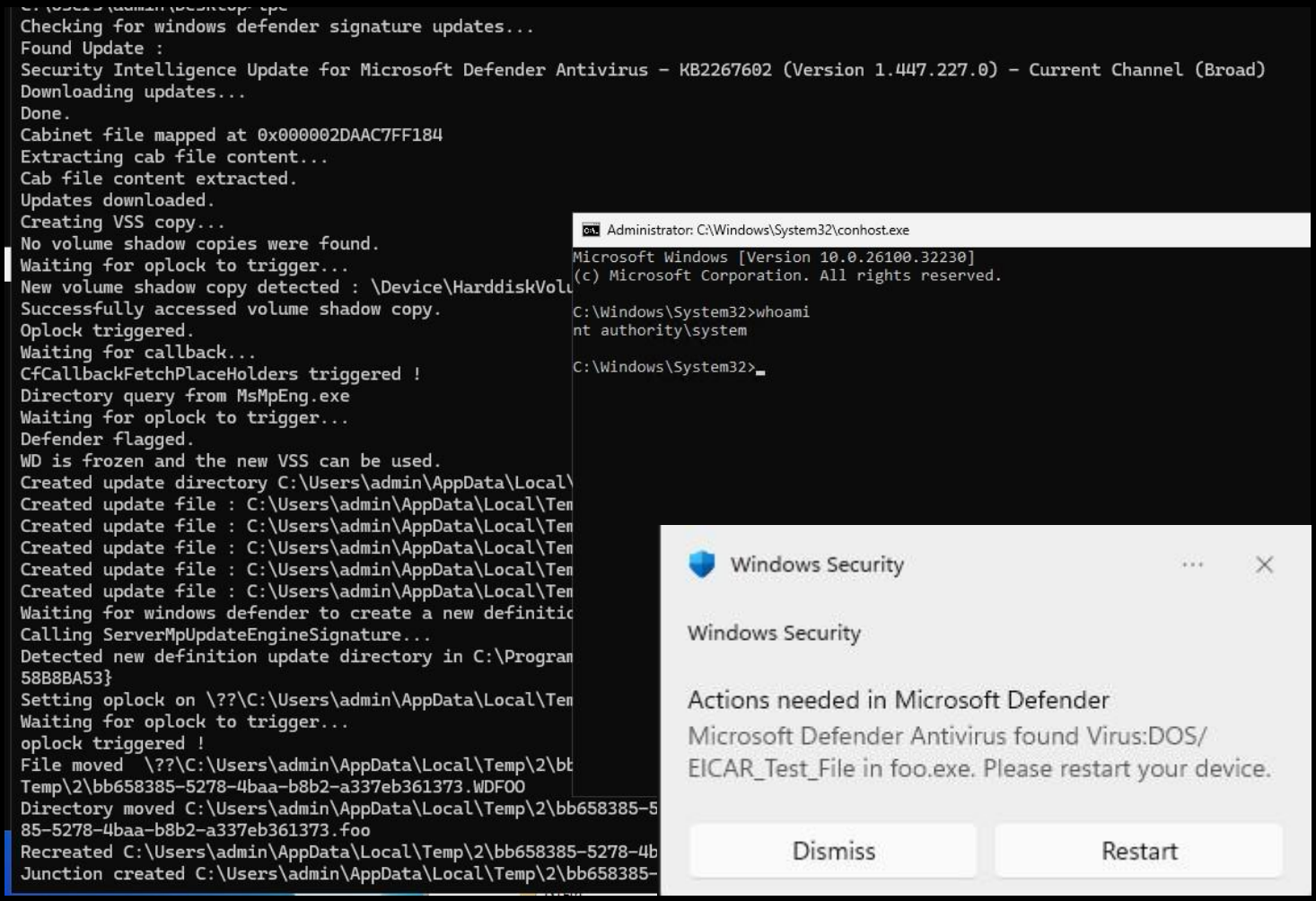
Threat Hunting Activity

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.



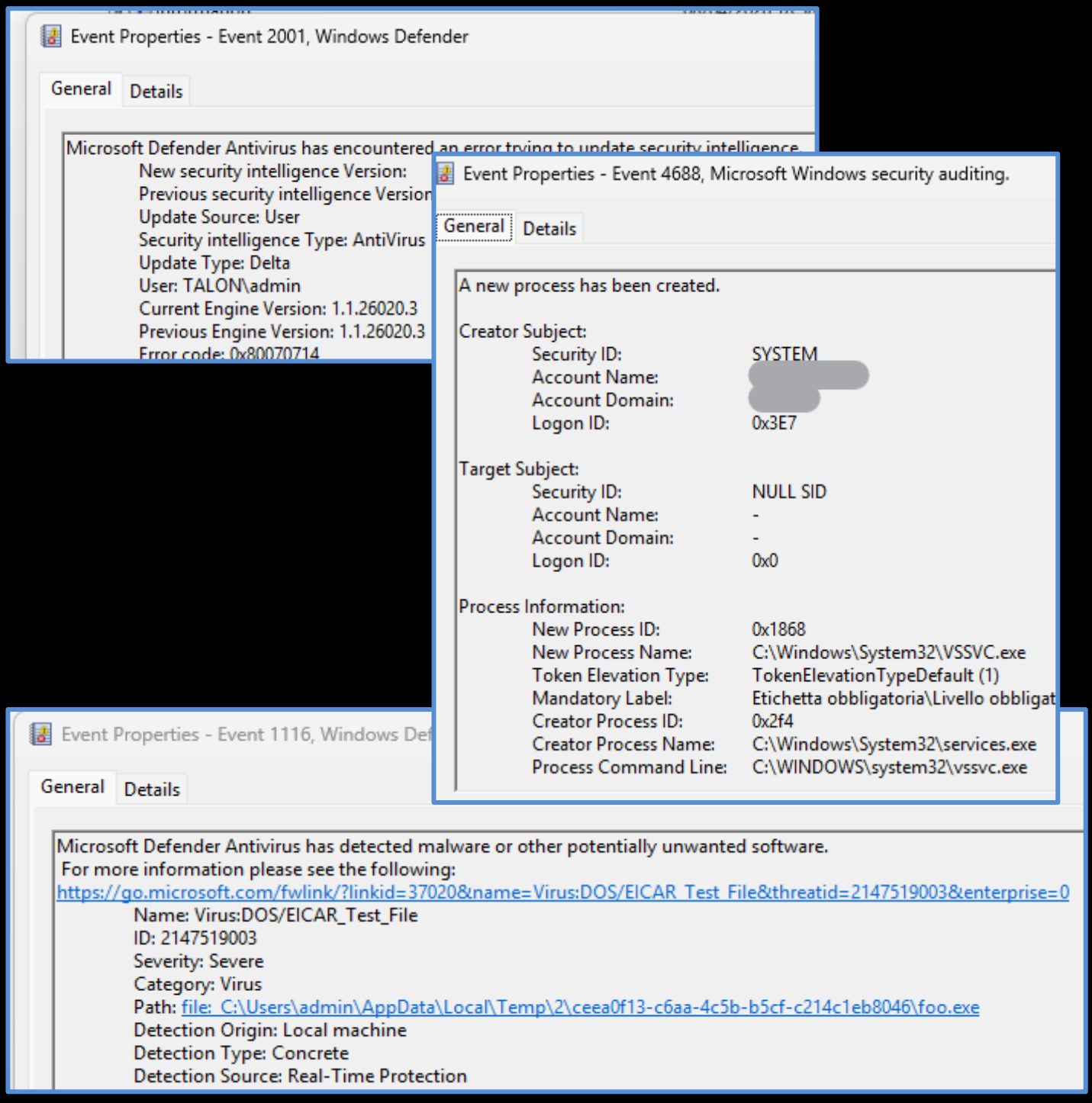
Threat Hunting Activity

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



Threat Hunting Activity

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




THREAT
HUNTING
SORINT SEC
PUBLIC