

A large, detailed illustration of a bee, rendered in a dark blue and black color scheme. The bee's body and wings are overlaid with glowing blue circuit board patterns, symbolizing technology and security. The bee is positioned centrally, with its head facing left and its legs extending downwards.

THREAT HUNTING

LAB

WEEK 11/08/2025 - 15/08/2025

Global Weekly Threat Overview

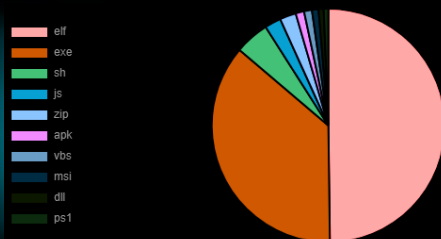
Global Weekly Notable One

Threat Hunting Activity

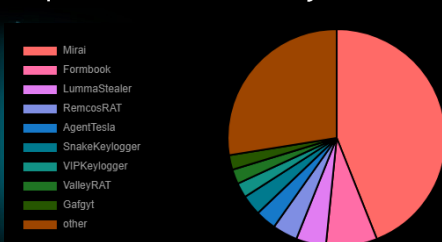
Global Weekly Threat Overview

Cisco has released security updates to address a maximum-severity security flaw in Secure Firewall Management Center (FMC) Software that could allow an attacker to execute arbitrary code on affected systems. The vulnerability, assigned the CVE identifier CVE-2025-20265 (CVSS score: 10.0), affects the RADIUS subsystem implementation that could permit an unauthenticated, remote attacker to inject arbitrary shell commands that are executed by the device. For this vulnerability to be exploited, Cisco Secure FMC Software must be configured for RADIUS authentication for the web-based management interface, SSH management, or both.

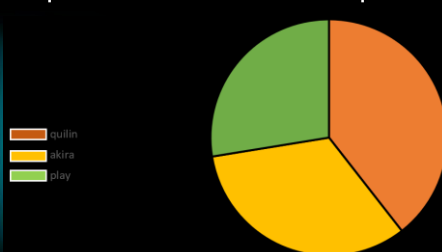
Top 10 file types



Top 10 malware family



Top 3 Ransomware Group



Financial institutions like trading and brokerage firms are the target of a new campaign that delivers a previously unreported remote access trojan called GodRAT. The malicious activity involves the distribution of malicious .SCR files disguised as financial documents. The attacks, which have been active as recently as August 12, 2025, employ a technique called steganography to conceal within image files shellcode used to download the malware from a command-and-control (C2) server. The screen saver artifacts have been detected since September 9, 2024, targeting countries and territories like Hong Kong, the United Arab Emirates, Lebanon, Malaysia, and Jordan.

Global Weekly Notable One



OS Credential Dumping: Credential Access

In a recent SEO poisoning campaign, attackers returned to using Bumblebee malware to gain initial access. SEO Poisoning is an attack technique where threat actors manipulate search engine optimization algorithms to rank malicious websites high in search results. The goal is to attract users actively searching for legitimate software or information, luring them into downloading trojan applications.

The application downloaded sideloaded a version of the Bumblebee malware. Bumblebee is a modular, highly stealthy malware loader linked to ransomware group. It is designed to evade antivirus detection and maintain persistence within compromised networks. EDR and security system usually detect this tools once they trigger suspicious actions like credentials dump. Abusing legit windows tools allow evasion of this kind of telemetry. For this task attackers, once on domain controller, abuse legitimate tools like wbadm. Wbadm's native administrative trust and command-line accessibility make it an ideal tool for attackers post-compromise.

Threat Hunting Activity

TACTIC

Credential Access

TECHNIQUES

T1003

OS Credential Dumping

Adversaries may attempt to dump credentials to obtain account login and credential material, normally in the form of a hash or a clear text password. Credentials can be obtained from OS caches, memory, or structures. Credentials can then be used to perform Lateral Movement and access restricted information.

Threat Hunting Activity

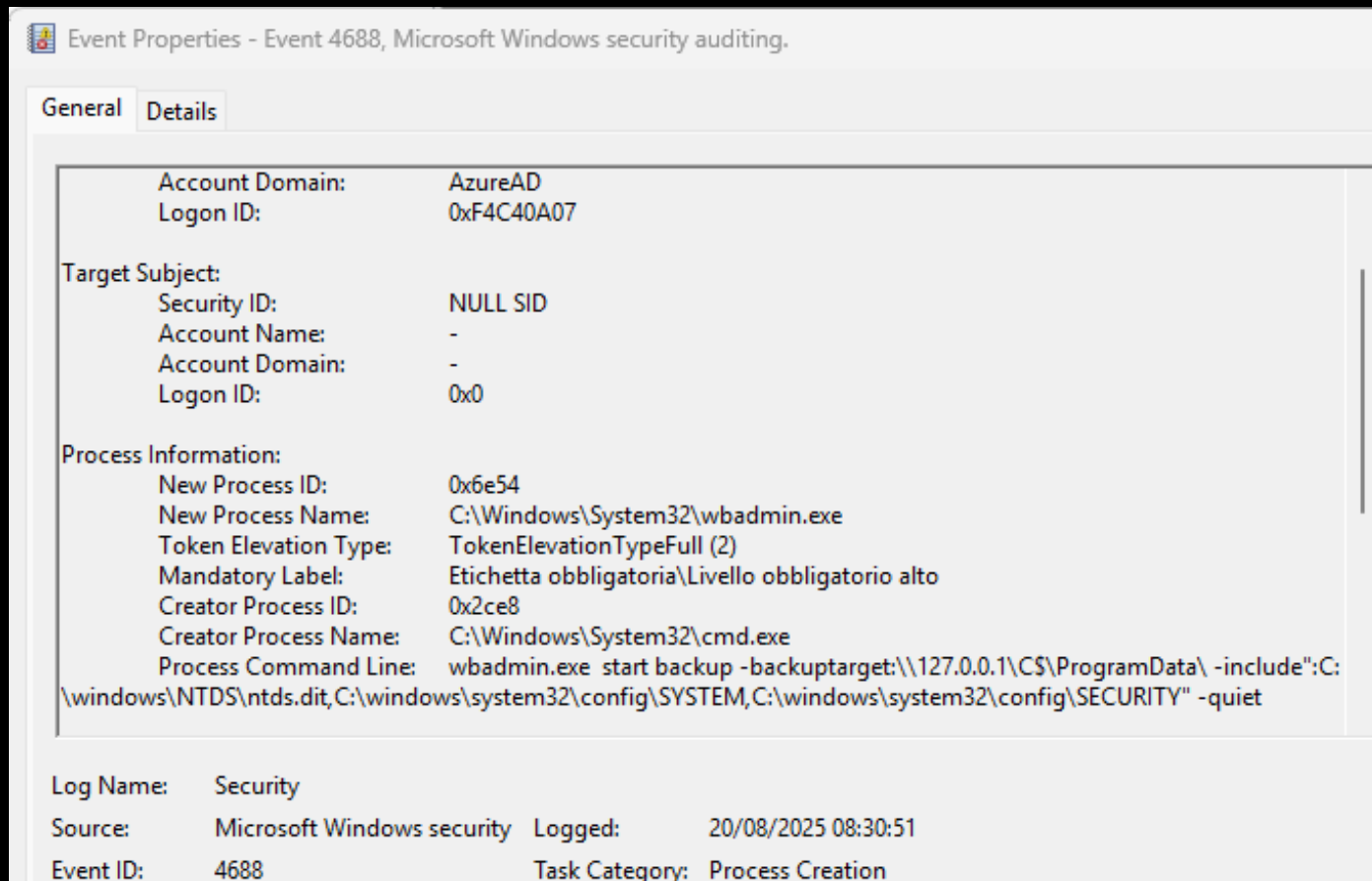
Normally used to perform backup tasks, Wbadmin is misused to dump credentials. In the case of a domain controller, it can be used to dump the entire active directory targeting for example the .dit file.

```
C:\Users\          \Desktop>wbadmin.exe start backup -backuptarget:\\127.0.0.1\C$\ProgramData\  
-include":C:\windows\NTDS\ntds.dit,C:\windows\system32\config\SYSTEM,C:\windows\system32\config\SEC  
URITY" -quiet  
wbadmin 1.0 - Backup command-line tool  
(C) Copyright Microsoft Corporation. All rights reserved.
```

Wbadmin execution

Threat Hunting Activity

Detection can be made on EID 4688 looking for suspicious wadmin process.



Event Properties - Event 4688, Microsoft Windows security auditing.

General Details

Account Domain:	AzureAD
Logon ID:	0xF4C40A07
Target Subject:	
Security ID:	NULL SID
Account Name:	-
Account Domain:	-
Logon ID:	0x0
Process Information:	
New Process ID:	0x6e54
New Process Name:	C:\Windows\System32\wadmin.exe
Token Elevation Type:	TokenElevationTypeFull (2)
Mandatory Label:	Etichetta obbligatoria\Livello obbligatorio alto
Creator Process ID:	0x2ce8
Creator Process Name:	C:\Windows\System32\cmd.exe
Process Command Line:	wadmin.exe start backup -backuptarget:\\127.0.0.1\CS\ProgramData\ -include":C:\windows\NTDS\ntds.dit,C:\windows\system32\config\SYSTEM,C:\windows\system32\config\SECURITY" -quiet

Log Name: Security

Source: Microsoft Windows security Logged: 20/08/2025 08:30:51

Event ID: 4688 Task Category: Process Creation

EID 4688



THREAT HUNTING

 SORINT_{SEC}