SORINT.SEC

THREAT HUNTING

LAB

Deep Dive into Snow Flurry campaign:
Edgecution Persistence and the "Headless Process Clean Up"

PUBLIC

Index

Global Weekly Threat Overview

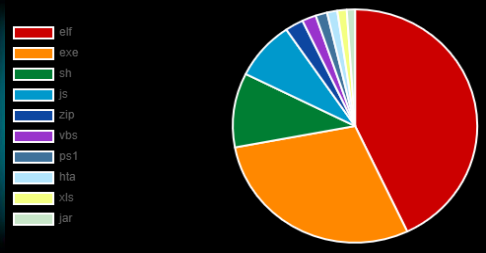
Global Weekly Notable One

Threat Hunting Activity

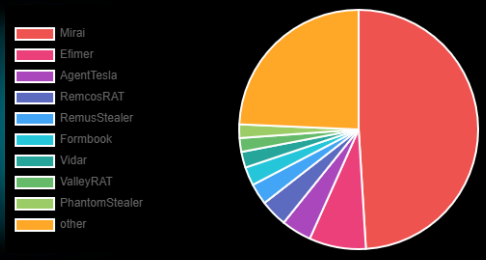
Global Weekly Threat Overview

North Korean hackers have been exploiting a Windows zero-day vulnerability (CVE-2026-68820) to target defense-sector companies as part of the Operation Dream Job campaign. Microsoft addressed the flaw in this month's Patch Tuesday security updates, marking it as actively exploited in the wild. Researchers found that the Lazarus threat group has been leveraging it since early July. Microsoft says that the vulnerability is a "use-after-free in Windows Ancillary Function Driver for WinSock (AFD.sys)" that allows an attacker to increase their local privileges. The tech giant added that a locally authenticated user could run a specially crafted application on an affected system to trigger a race condition, eventually gaining SYSTEM privileges without any user interaction.

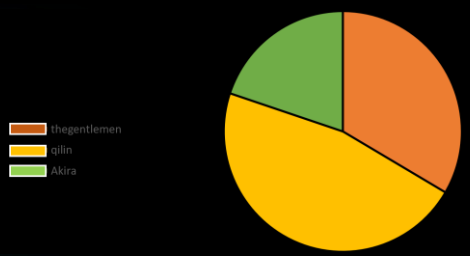
Top 10 file types



Top 10 malware family



Top 3 Ransomware Group



A financially motivated threat actor previously associated with the Medusa ransomware operation is now deploying a new ransomware strain called StormEncryptor. Storm-1175 is believed to be a China-based threat actor. It was previously linked to Medusa ransomware, targeting systems via zero-day and n-day flaws in various products. StormEncryptor is a C++ malware that appends encrypted files with the ".encrypted" filename extension and drops a ransom note named '!!!README_FIRST!!!.txt' into every scanned directory. After gaining access to the target network, the attacker used AnyDesk or SimpleHelp for remote management, Advanced IP Scanner for network discovery, and the Mimikatz tool to dump credentials from the Local Security Authority Subsystem Service (LSASS) process.

Global Weekly Notable One

Discovery: Process Discovery

UNC6692, or "Snow Flurries," conducts sophisticated multistage intrusions beginning with email bombing to distract victims. They impersonate IT support via Microsoft Teams, directing users to Amazon S3-hosted phishing sites that employ a "double-entry" trick-rejecting initial password attempts to ensure the attacker captures credentials twice.

The campaign utilizes the SNOW ecosystem, primarily featuring Edgecution (SNOWBELT), a malicious browser extension. Once inside, the actors perform internal reconnaissance, harvest credentials from LSASS memory, and move laterally to Domain Controllers. The operation concludes by exfiltrating the NTDS.dit Active Directory database and registry hives via LimeWire.

Threat Hunting Activity

TACTIC

Discovery

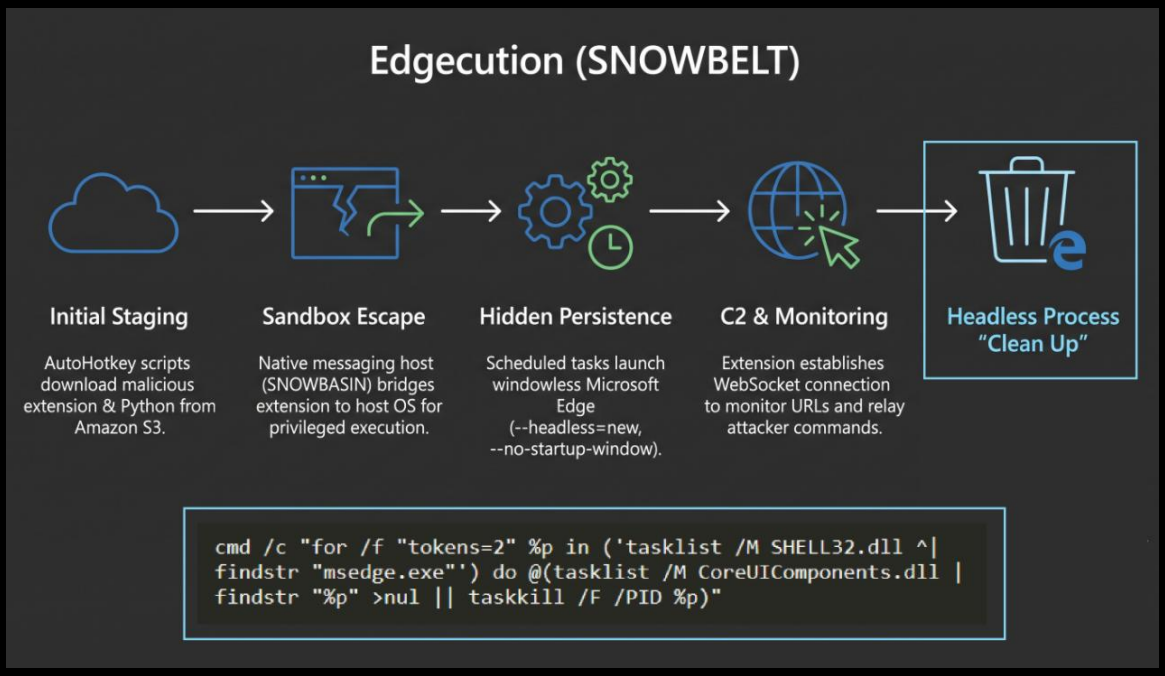
TECHNIQUES

T1057 – Process Discovery

Adversaries may attempt to get information about running processes on a system. Information obtained could be used to gain an understanding of common software/applications running on systems within the network. Adversaries may use the information from Process Discovery during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

Threat Hunting Activity

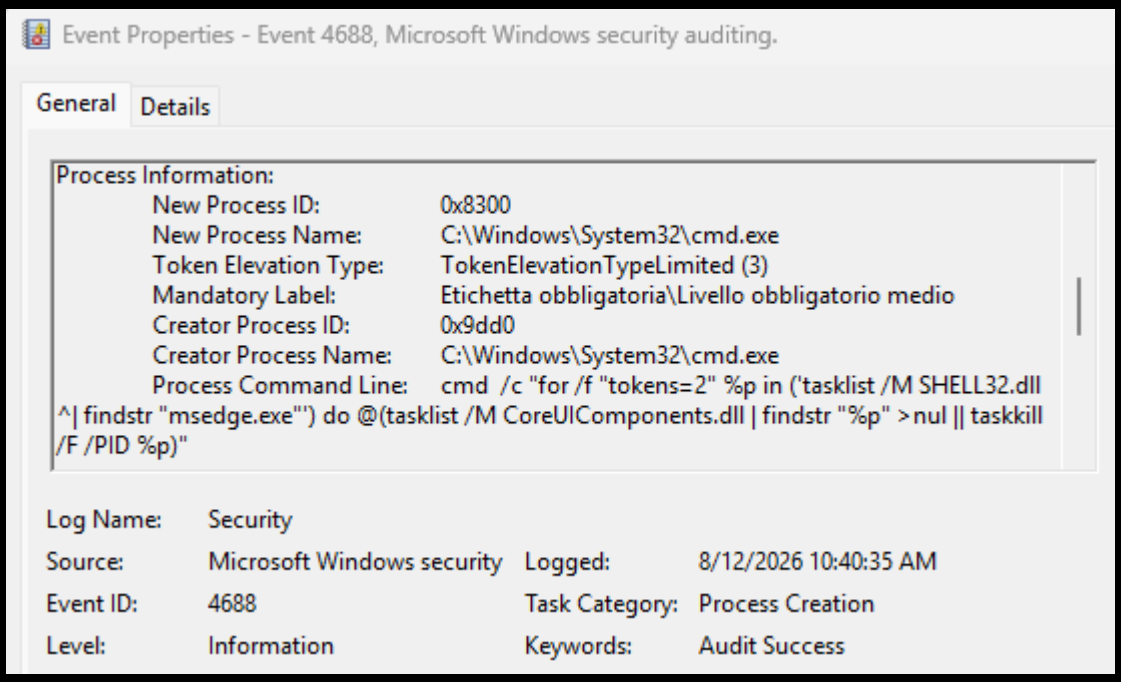
The Edgecution (SNOWBELT) attack chain begins with an AutoHotkey stager downloading the malicious extension and Python components from Amazon S3. To escape the browser sandbox, it utilizes a native messaging host, granting it privileged access to the host OS for command execution and monitoring. Persistence is secured through scheduled tasks that launch windowless Microsoft Edge instances using --headless=new or --no-startup-window flags, ensuring the activity remains invisible.



A central feature of this chain is the Headless Process 'Clean Up' mechanism.
The threat actor deploys a specialized scheduled task designed to manage these background instances. Because Microsoft Edge processes lacking CoreUIComponents.dll are typically headless, the actor uses the absence of this DLL to identify malicious background processes. By executing a command string involving tasklist and findstr, the malware detects these instances and forcefully terminates them via taskkill. This automated routine allows the actor to "clean up" or cycle the hidden processes executing their malware, preventing resource bloat while maintaining a stealthy, persistent foothold.

Threat Hunting Activity

Detection can be made monitoring process execution event logs, identify the actor's automated maintenance by monitoring for msedge.exe process enumeration via tasklist (checking for SHELL32.dll and CoreUIComponents.dll) followed shortly by a taskkill /F /PID command. This behavior, initiated by malware components like native_host.py or scheduled tasks, signals the cycling of headless Edge instances used to host the group's malicious browser extensions.



PUBLIC