SORINT.SEC

THREAT HUNTING

LAB

WEEK 06/10/2025 – 10/10/2025

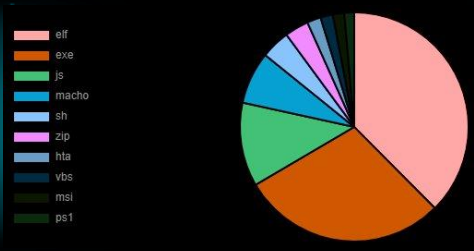
PUBLIC

Index

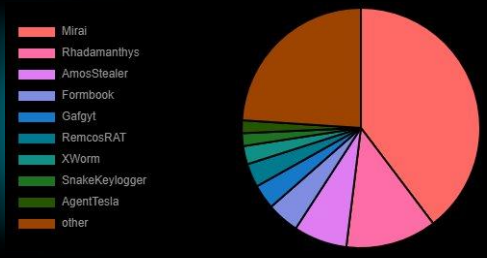
Global Weekly Threat Overview

Cybersecurity researchers have disclosed details of a new Rust-based backdoor called ChaosBot that can allow operators to conduct reconnaissance and execute arbitrary commands on compromised hosts. ChaosBot is noteworthy for its abuse of Discord for command-and-control (C2). It gets its name from a Discord profile maintained by the threat actor behind it. The payload is a malicious DLL ("msedge_elf.dll") that's sideloaded using the Microsoft Edge binary called "identity_helper.exe“ after which it performs system reconnaissance and downloads a fast reverse proxy (FRP) to open a reverse proxy into the network and maintain persistent access to the compromised network.

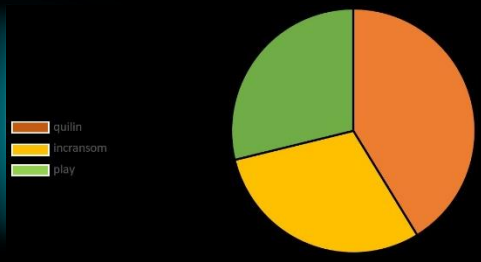
Top 10 file types



Top 10 malware family



Top 3 Ransomware Group



Threat actors are actively exploiting a critical security flaw impacting the Service Finder WordPress theme that makes it possible to gain unauthorized access to any account, including administrators, and take control of susceptible sites. The authentication bypass vulnerability, tracked as CVE-2025-5947 (CVSS score: 9.8), affects the Service Finder Bookings, a WordPress plugin bundled with the Service Finder theme. This vulnerability makes it possible for an unauthenticated attacker to gain access to any account on a site, including accounts with the 'administrator' role.

Global Weekly Notable One

Boot or Logon Autostart Execution: **Persistence**

WinRAR is one of the most popular file compression tools globally, known for its ability to efficiently compress, package, and exchange files. Its seamless integration into everyday computer workflows makes it an essential utility for users and organizations alike.
In 2025, a critical security vulnerability designated CVE-2025-8088 was discovered in the Windows version of WinRAR, a widely used file compression and archiving utility. This vulnerability is classified as a path traversal flaw with the specific exploitation mechanism involving Windows NTFS Alternate Data Streams. At its core, the flaw arises from WinRAR's failure to properly validate and canonicalize file paths within specially crafted RAR archive headers during extraction. Attackers exploit the improper handling of relative and absolute path components to bypass intended extraction directories and write files to arbitrary, locations on the victim's file system.

The vulnerability is rooted in the RARReadHeader and RARProcessFile routines, which are responsible for interpreting file metadata and managing file extraction. Due to lack of normalization and bounds-checking of relative directory segments in filenames, WinRAR allows malicious archive entries to traverse upward and laterally through the file system hierarchy. By embedding multiple ADSes within a single archive entry, attackers can further conceal malicious payloads, such as DLLs or Windows shortcut (.lnk) files, that appear innocuous within the archive but result in stealthy system infections when extracted.

Global Weekly Notable One

Boot or Logon Autostart Execution: **Persistence**

A prominent cybercriminal group known as RemCom (also called Tropical Scorpion) has been leveraging CVE-2025-8088 in their latest campaigns. Tropical Scorpion is a Russian-aligned advanced persistent threat group that has gained notoriety for its focused cyber espionage and cybercrime activities. While the group's exact origins are not fully disclosed, their operations are strongly linked to Russian cybercriminal underground, often targeting political, governmental, and critical infrastructure sectors in Eastern Europe, particularly Ukraine and Poland. Starting from mid-2025, RemCom weaponized this WinRAR flaw to deliver malware payloads via malicious RAR archives, often disguised as job application documents.

This method exploits the vulnerability to gain initial access to target systems, enabling subsequent deployment of advanced malware and persistent threats.

Threat Hunting Activity

SORINTsec

TACTIC

Persistence

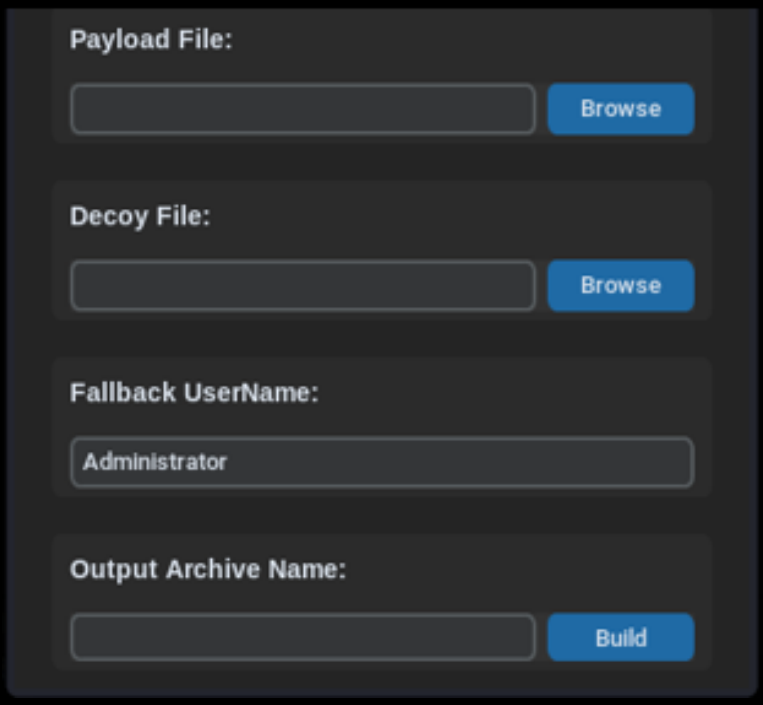
TECHNIQUES

T1547 – Boot or Logon Autostart Execution

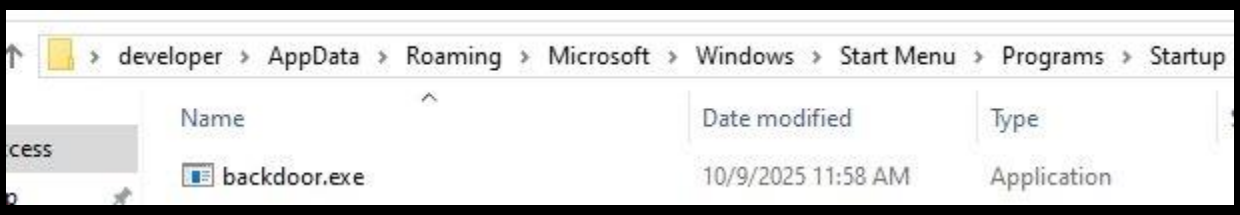
Adversaries may configure system settings to automatically execute a program during system boot or logon to maintain persistence or gain higher-level privileges on compromised systems. Operating systems may have mechanisms for automatically running a program on system boot or account logon. These mechanisms may include automatically executing programs that are placed in specially designated directories or are referenced by repositories that store configuration information, such as the Windows Registry. An adversary may achieve the same goal by modifying or extending features of the kernel.

Threat Hunting Activity

Several script and POC are now available allowing easy creation of malicious rar archives even through gui interface.



Once delivered and extracted a payload is placed



Threat Hunting Activity

Detection can be made monitoring suspicious file creation in the startup folder

PUBLIC