SORINT SEC

# THREAT HUNTING

## LAB

WEEK 17/11/2025 – 21/11/2025

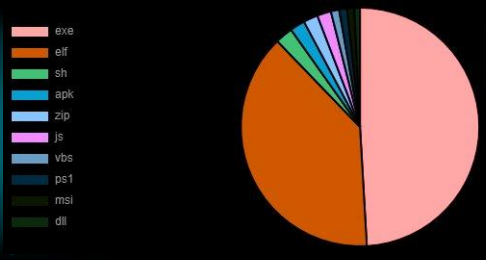
PUBLIC

# Index

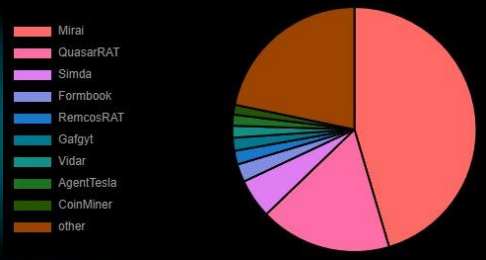
# Global Weekly Threat Overview

Thousands of credentials, authentication keys, and configuration data impacting organizations in sensitive sectors have been sitting in publicly accessible JSON snippets submitted to the JSONFormatter and CodeBeautify online tools that format and structure code. Researchers discovered more than 80,000 user pastes totaling over 5GB exposed through a feature called Recent Links provided by both services, which is freely accessible to anyone. Some of the companies and organizations with sensitive data leaked this way are in high-risk sectors like government, critical infrastructure, banking, insurance, aerospace, healthcare, education, cybersecurity, and telecommunications.

Top 10 file types




Top 10 malware family




Top 3 Ransomware Group


ClickFix attack variants have been observed where threat actors trick users with a realistic looking Windows Update animation in a full screen browser page and hide the malicious code inside images. ClickFix is a social engineering attack where users are convinced to paste and execute in Windows Command Prompt code or commands that lead to running malware on the system. The attack has been widely adopted by cybercriminals across all tiers due to its high effectiveness and has continually evolved, with increasingly advanced and deceptive lures.

# Global Weekly Notable One

## Boot or Logon Autostart Execution: **Persistence**

Recently we observed a campaign that involves a malicious Latrodectus MSI malware variant, often deployed via a multi-stage process involving obfuscated PowerShell.
The malware significantly abuses the legitimate Advanced Installer framework to repackage payloads and establish persistence, sometimes attempting to bypass UAC prompts. In this campaign It masquerades as SentinelOne security software, using also signed files to succeed while remaining unnoticed.

The final payload exhibited zero initial antivirus detections, demonstrating strong evasion. Latrodectus performs system reconnaissance, collecting unique identifiers like the MachineGuid and enumerating trusted certificates. The complexity highlights why behavioral detection is critical.

# Threat Hunting Activity

SORINTSEC

## TACTIC

Persistence

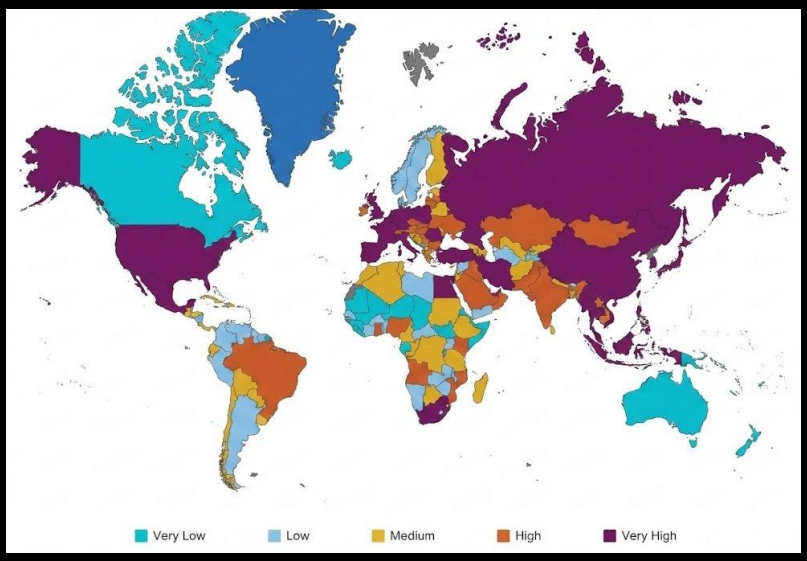
## TECHNIQUES

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.

# Threat Hunting Activity

Latrodectus is a sophisticated malware loader that has emerged as a major threat in the cybercrime landscape since its first detection in late 2023. It is also known by aliases such as BlackWidow, IceNova, Lotus, or Unidentified 111. Latrodectus is primarily used as a downloader and backdoor, allowing attackers to execute remote commands, deploy additional payloads, and maintain persistence on compromised systems.

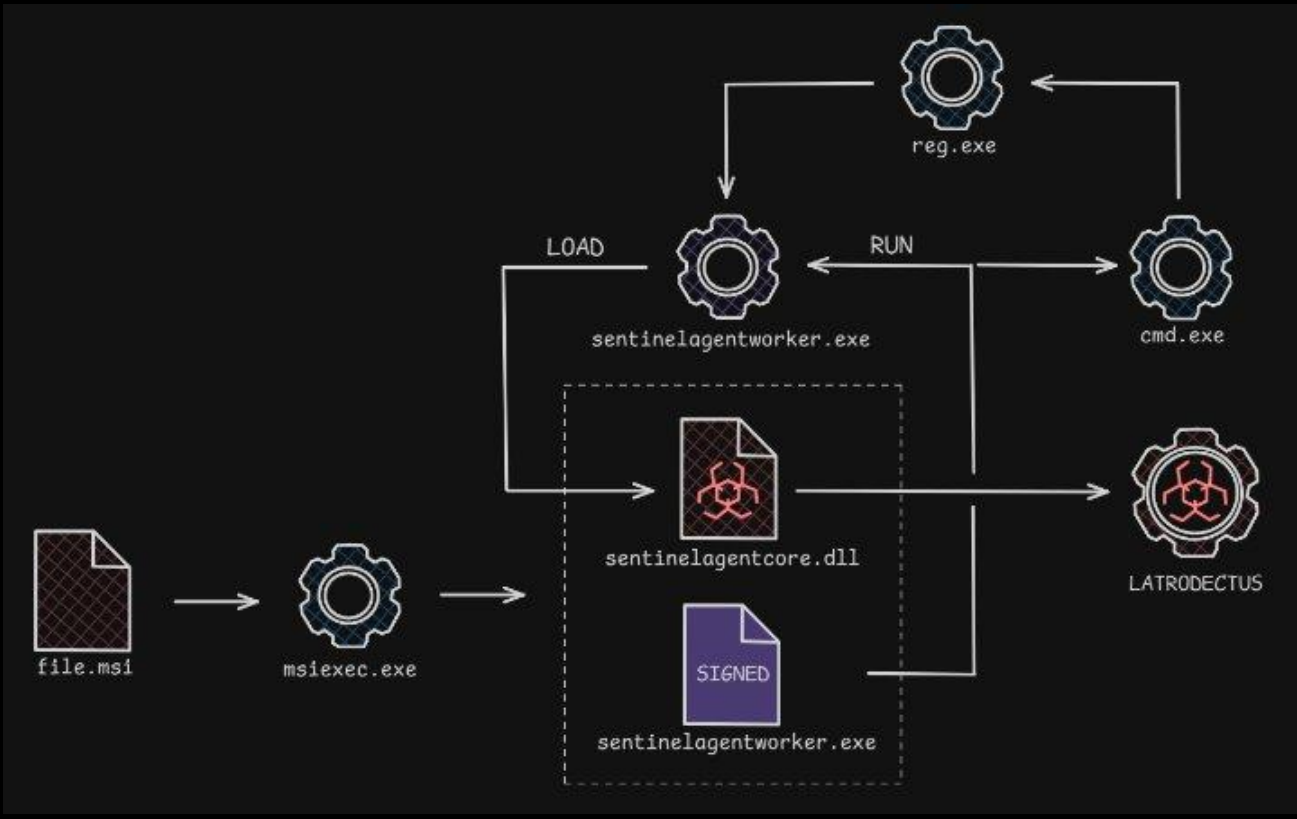



Last year malware impact

Latrodectus typically spreads through phishing campaigns, once executed, Latrodectus employs various evasion techniques, including: Dynamic resolution of Windows API functions, anti-debugging and sandbox detection and persistence mechanisms such as AutoRun registry keys and scheduled tasks. Focusing on the last one, this campaing use a persistence technique pretty simple and known: It adds an entry into the registry key "\Software\Microsoft\Windows\CurrentVersion\Run" that it is known Windows startup location used to automatically launch programs when a user logs on.

# Threat Hunting Activity

The malware achieves performing a registry Write operation to create the key entry “sentinelsscheduler” in the “\Software\Microsoft\Windows\CurrentVersion\Run” key. This ensures the signed executable, SentinelAgentWorker.exe, is automatically launched every time the user logs in.

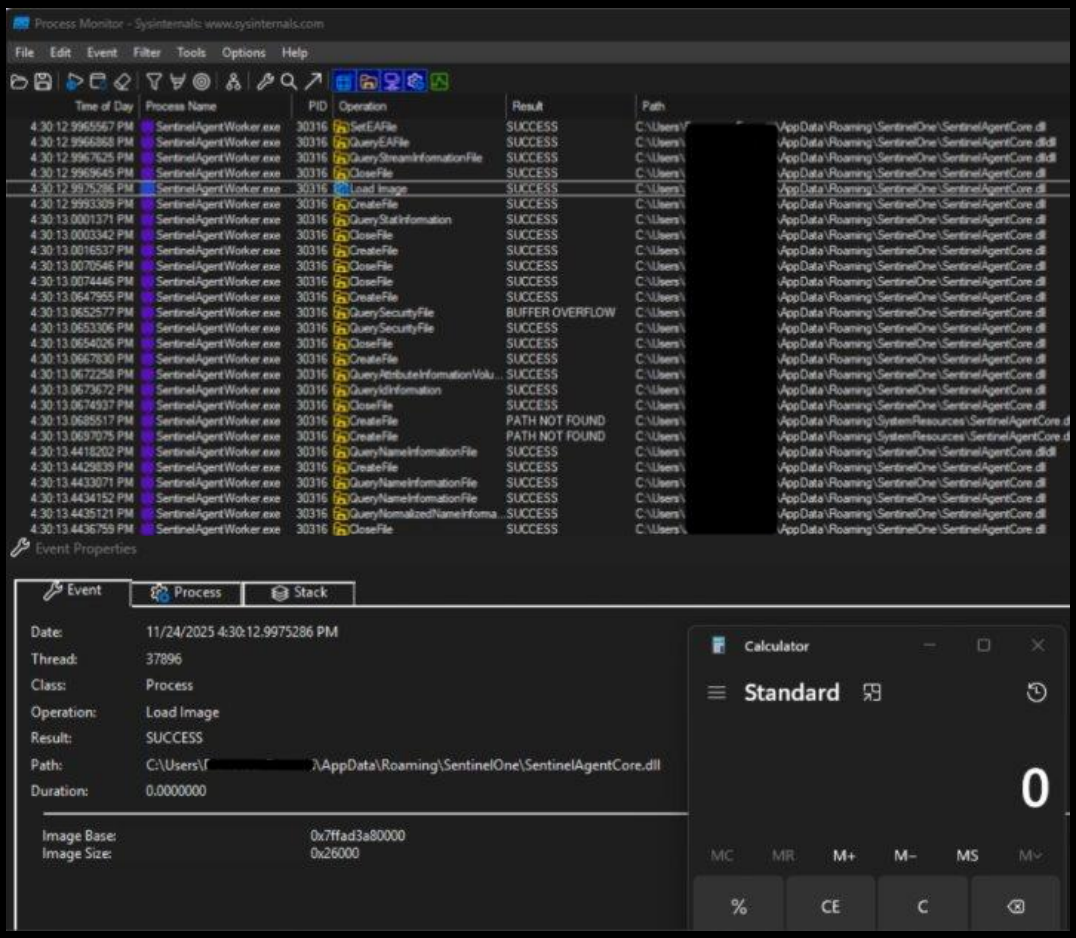



Persistence side-load

Hijacking library search order, malicious dll is then loaded and then Latrodectus too.

# Threat Hunting Activity

By emulating the tests in the laboratory after sanitizing the infected DLL, we reproduced the side-loading test by running SentinelOne's signed software.

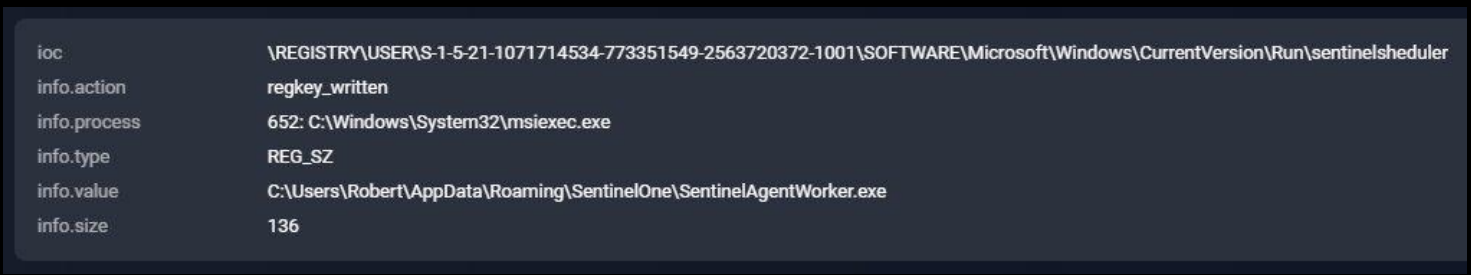



Side-load emulation with sanitized dll

The result was as expected: the DLL was successfully loaded because it was stored in the same folder as the executable and the dll search order was respected and exploited.

# Threat Hunting Activity

Detection can be made monitoring new entry in this specific registry key path. This path is usually closely monitored by EDRs and correlation rules in a SOC, but unlike “more default” tactics, the executable included in the entry is lecit and signed. Such registry changes may be deprioritized or complicate detection by security teams. For this reason, we believe it is necessary to pay greater attention to this campaign, as a timely detection would significantly raise the bar of criticality by not allowing a legitimate binary to go unnoticed, thus drawing due attention to the observed campaign.




Registry key written

This will allow us to critically assess and contextualize any alerts relating to this campaign, thereby identifying potential DLLs that will be involved in sideloading.


PUBLIC