Technical Analysis of SmokeLoader Version 2025 | ThreatLabz

By ThreatLabz

Published: 2025-09-15 · Archived: 2026-04-06 01:27:48 UTC

In this section, we will analyze the two latest versions of SmokeLoader: version 2025 alpha and version 2025. Note that version 2025 alpha identifies itself as version 2022 when communicating with the C2 server. However, the compilation timestamps for these samples date back to around February 2025. SmokeLoader consists of two main components: a stager and a main module. The stager has two main purposes: hinder analysis, detect virtual environments (and terminate if present), and inject the SmokeLoader main module into explorer.exe. The main module performs the bulk of the malicious functionality including establishing persistence, beaconing to the C2 server, and executing tasks and plugins.

SmokeLoader stager

In a previous blog, ThreatLabz identified significant bugs in SmokeLoader versions 2018 through 2022 that caused performance degradation on an infected system. This was caused by several factors including a scheduled task (used for persistence) that executed SmokeLoader's stager every 10 minutes. Since SmokeLoader's stager did not check whether the main module was already running (via a mutex), the stager would allocate memory in explorer.exe and inject a new copy of SmokeLoader's main module every 10 minutes. In addition, the main module created two threads to identify and disable analysis tools before checking whether SmokeLoader was already running. As a result, two new threads in explorer.exe were also created every 10 minutes.

Bug fixes

In order to address these performance issues, the SmokeLoader developer added a new mutex check into the stager's code starting with version 2025 alpha. Thus, the newer SmokeLoader stagers will first verify whether the machine specific SmokeLoader mutex name exists. If the mutex already exists, the stager will terminate immediately and will not inject the SmokeLoader main module into explorer.exe. The SmokeLoader mutex name format was also modified, which was previously identical to the bot ID consisting of 40 uppercase hexadecimal characters. Starting with version 2025 alpha, the mutex name has a variable length that consists of lowercase alphabetic letters. The mutex name and length are now determined by a pseudo random number generator that is seeded with the first 4 bytes of the SmokeLoader bot ID. The following Python code replicates the algorithm that is used to generate SmokeLoader's mutex name and length for versions 2025 alpha and 2025.

```
def generate_mutex(bot_id: bytes) -> str:
  def uint32(val: int) -> int:
      return val & 0xffffffff
  def rand(mod: int) -> int:
      nonlocal seed
      seed = uint32(uint32(0x41c64e6d * seed) + 0x33bd)
      return seed % mod
```

```
    seed = int.from_bytes(bot_id[:4], "little")
    mutex_len = rand(20) + 20
    print("mutex len:", mutex_len)
    mutex = bytearray()
    for i in range(mutex_len):
        val = rand(26)
        mutex.append(val + ord('a'))
    return mutex.decode()
```

Another bug that was fixed is the creation of the two anti-analysis threads (that terminate malware analysis tools) now occurs after the mutex check. Therefore, if the mutex check fails, those two threads will no longer be created. These SmokeLoader bug fixes are illustrated in the diagram below.

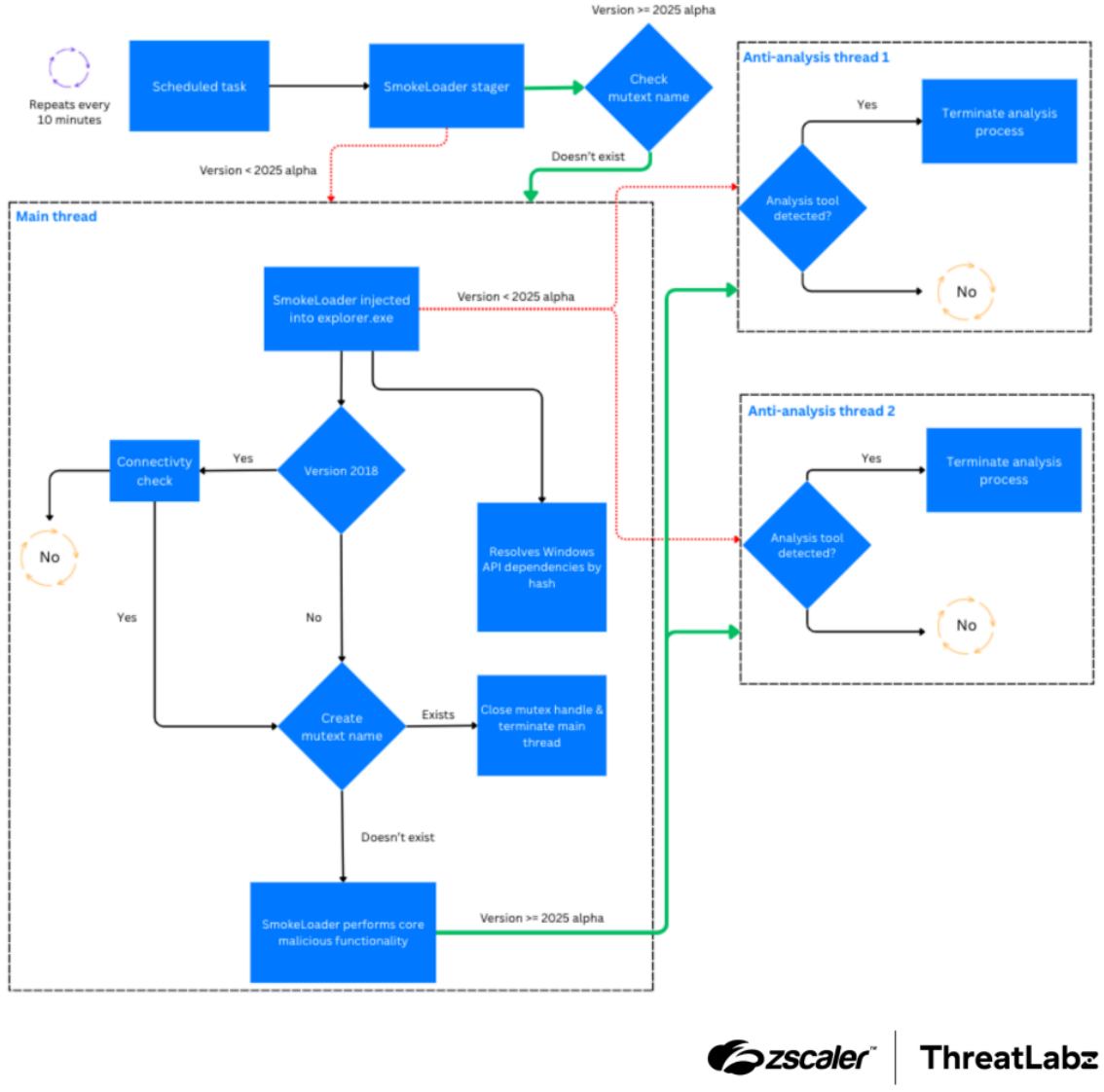

Figure 1: SmokeLoader execution process control flow comparison with versions before (red) and after (green) 2025 alpha.

SmokeLoader 2025 stager changes

Although the stager for version 2025 alpha fixed the bug of injecting SmokeLoader continuously into the explorer.exe process, the remaining parts of the code were largely unchanged. However, in SmokeLoader's version 2025 stager, additional changes were introduced including the following:

- Implemented a new function to decrypt code blocks by adding a hardcoded value to each byte before execution.
- Dynamically calculates RVAs (by performing an XOR operation with a constant) when decrypting code.
- Added new 64-bit shellcode to inject the main module into explorer.exe

The green lines illustrate these new updates to SmokeLoader starting in version 2025 alpha. For comparison, the dotted red lines indicate the process control flow for versions prior to 2025 alpha.

Main module

The main module of SmokeLoader has received a number of updates in both version 2025 alpha and 2025 with significant overlap between the two versions. Since the mutex generation algorithm was moved to the stager, the mutex string is passed to the main module, where the mutex is created if it does not already exist. If the mutex name exists (which in theory should never happen due to the check in the stager), SmokeLoader terminates.

In both versions, various constants are obfuscated using a simple function that performs an XOR operation with a hardcoded value (that changes per sample). In version 2025, constants are obfuscated such as the value 0xF001F (`SECTION_ALL_ACCESS`) that is passed to the function NtCreateSection. However, in version 2025 alpha, different constants are obfuscated including the SmokeLoader version number as shown below.

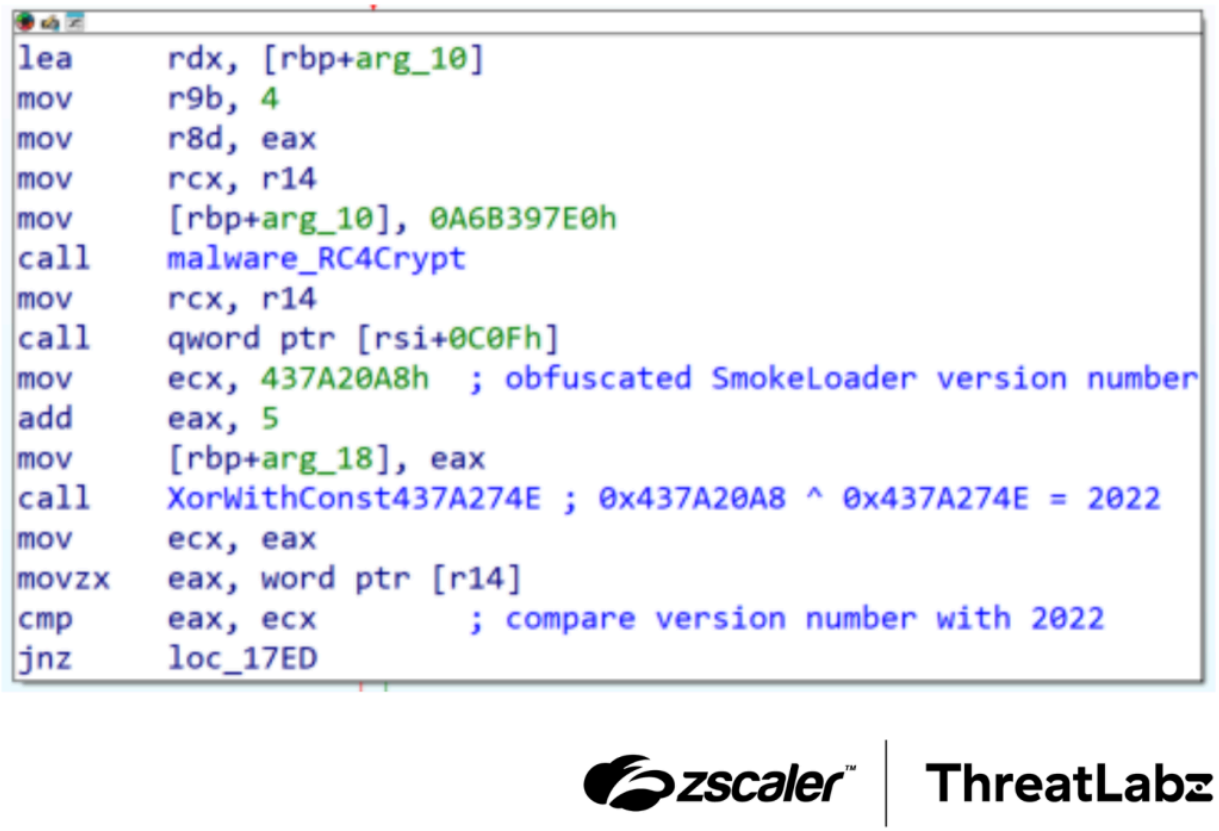

Figure 2: Example of SmokeLoader version 2025 alpha constant obfuscation

In version 2025, there is an additional language check that compares whether the victim's keyboard layout is Russian (and not Ukrainian). If a Russian keyboard layout is detected, SmokeLoader terminates itself. Interestingly, a very similar check is already present in SmokeLoader's stager, so this code is somewhat redundant.

Another change in the main module, in versions prior to 2025, is the file mapping name consisted of the bot ID appended with "FF" characters. In version 2025, the file mapping name is now the hash of the bot ID (as a string) converted to uppercase hexadecimal characters (without "FF" characters appended).

Scheduled task name

Previous versions of SmokeLoader used the format string `Firefox Default Browser Agent %hs` for the scheduled task that established persistence. Starting with version 2025 alpha, SmokeLoader now uses the format string `MicrosoftEdgeUpdateTaskMachine%hs`. In both cases, the `%hs` format string of the task name is the first 16 characters of the victim bot ID. Interestingly, the SmokeLoader developer removed the space between the fake browser string prefix and the bot ID, which is likely an oversight.

Version 2025 network protocol

While the 2025 alpha variant utilizes the same network protocol as version 2022, there were modest adjustments made in version 2025. For example, the two byte version number now reports the value 2025 (0x7e9) instead of

2022 (0x7e6). Version 2025 also updated the request to include a four byte CRC32 value at byte offset 2. The CRC32 checksum is computed on the bytes following offset 6 (that start with the bot ID) as shown in the figure below.

2 bytes	4 bytes	41 bytes	16 bytes	6 bytes	1 byte	1 byte	1 byte	2 bytes	4 bytes	4 bytes	N bytes
Version	CRC32 checksum	Bot ID	Computer name	Affiliate ID	Windows version	Windows architecture	System privileges	Command type	Command options	Command result	Data

Figure 3: SmokeLoader version 2025 beacon format

The response format in version 2025 was also slightly modified. Previously, the first 4 bytes of the C2 response contained the length of the command. This length value is now obfuscated via an XOR operation with the samples RC4 encryption key.

Source: https://www.zscaler.com/blogs/security-research/smokeloader-rises-ashes