SmokeLoader Rises From the Ashes

ThreatLabz ⋮ ⋮ 9/14/2025

Security Research

THREATLABZ

September 15, 2025 - 9 min read

Introduction

Active since 2011, SmokeLoader (aka Smoke or Dofoil) is a popular malware loader that is designed to deliver second-stage payloads such as trojans, ransomware, and information stealers. Over the years, SmokeLoader has been updated and enhanced to evade detection and optimize payload delivery. SmokeLoader's capabilities have also been expanded through a modular plugin framework that is capable of credential harvesting, browser hijacking, cryptocurrency mining, and more.

In May 2024, Operation Endgame, an international collaboration between law enforcement and private industry (which included Zscaler ThreatLabz) dismantled numerous instances of SmokeLoader and remotely removed the malware from infected systems. These actions suppressed SmokeLoader activity following the takedown. However, in early 2025, ThreatLabz identified a new version of SmokeLoader that included bug fixes and other improvements. We refer to this new variant as version 2025 alpha. Several months later, in

July 2025, the author of SmokeLoader advertised a new version on a cybercriminal forum. Shortly thereafter, ThreatLabz identified an additional variant with more changes and a slightly modified network protocol that breaks compatibility with prior versions. We will refer to this variant as version 2025, which is consistent with the version number that it reports in beacons to the command-and-control (C2) server.

Key Takeaways

- SmokeLoader is a modular malware family that was first advertised on criminal forums in 2011.
- Smoke's primary function is to download and execute second stage malware. SmokeLoader may also utilize optional plugins to perform tasks such as stealing data, launching distributed denial of service attacks, and mining cryptocurrency.
- ThreatLabz has identified two new SmokeLoader versions that are being used by multiple threat groups.
- These versions, which we refer to as version 2025 alpha and version 2025, fix significant bugs that previously caused significant performance degradation on an infected system.
- In addition, various SmokeLoader artifacts have been updated to evade static and behavior based detection.

Technical Analysis

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.

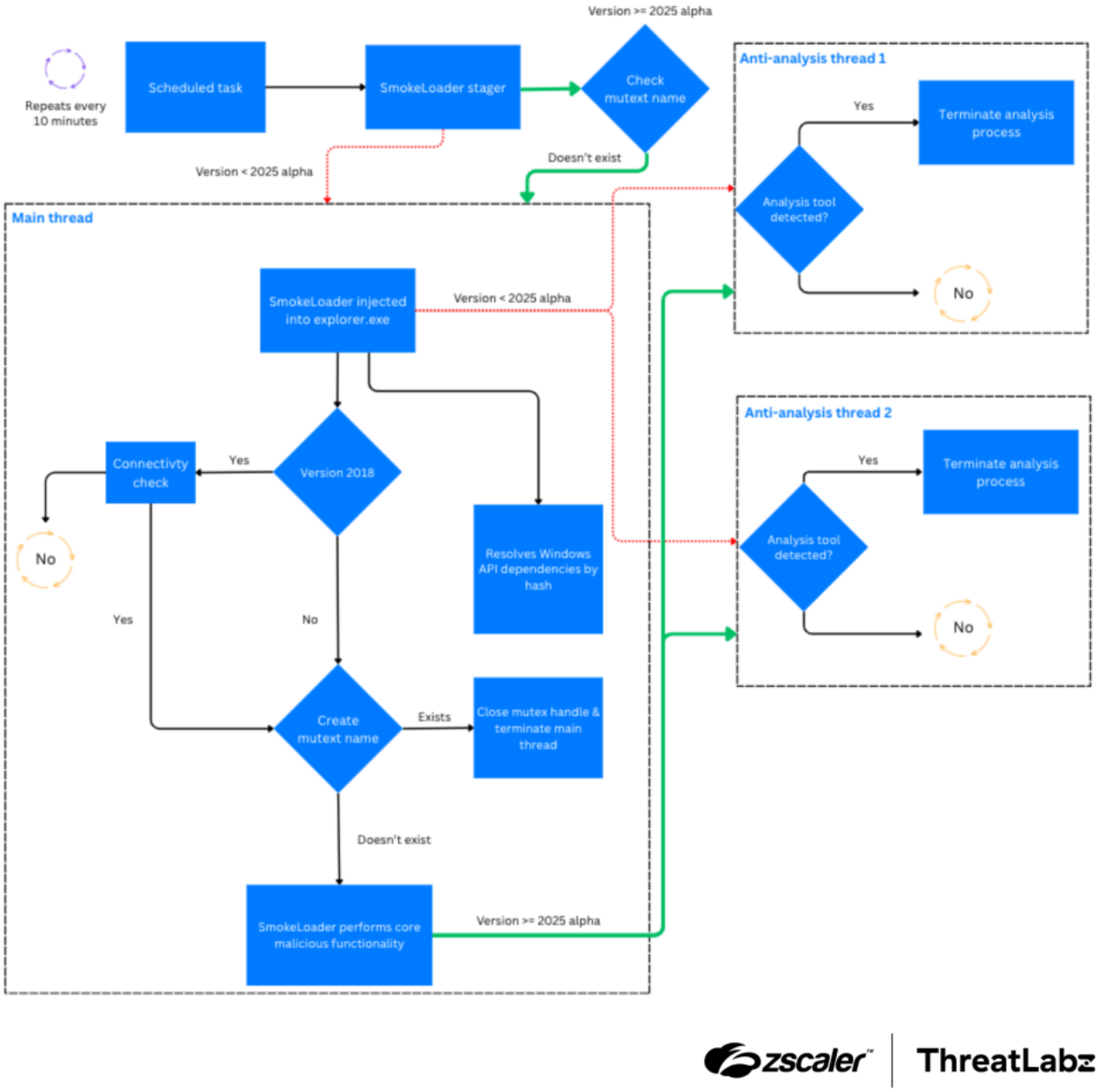

Figure 1: SmokeLoader execution process control flow comparison with versions before (red) and after (green) 2025 alpha.

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.

```
lea     rdx, [rbp+arg_10]
mov     r9b, 4
mov     r8d, eax
mov     rcx, r14
mov     [rbp+arg_10], 0A6B397E0h
call    malware_RC4Crypt
mov     rcx, r14
call    qword ptr [rsi+0C0Fh]
mov     ecx, 437A20A8h  ; obfuscated SmokeLoader version number
add     eax, 5
mov     [rbp+arg_18], eax
call    XorWithConst437A274E ; 0x437A20A8 ^ 0x437A274E = 2022
mov     ecx, eax
movzx   eax, word ptr [r14]
cmp     eax, ecx        ; compare version number with 2022
jnz     loc_17ED
```

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.

SmokeLoader Version Comparison

The table below provides a comparison of the most significant changes for the last three versions of SmokeLoader.

	Version 2022	Version 2025 alpha	Version 2025
Obfuscated constants	No	Yes	Yes
Scheduled task name	Firefox Default Browser Agent %hs	MicrosoftEdgeUpdateTaskMachine%hs	MicrosoftEdgeUpdateTaskMachine%hs
Mutex check	Main module	Stager + main module	Stager + main module
Network protocol version	2022	2022	2025
Keyboard layout check	Stager	Stager	Stager + main module
File mapping name	Bot ID + “FF"	Bot ID + “FF"	MD5(Bot ID)

Table 1: High-level comparison of the last three SmokeLoader variants

SmokeBuster Updates

ThreatLabz has released a free tool that we named SmokeBuster, which can be used to identify, manipulate, and clean an infected system. The tool has been updated to support all the latest variants of SmokeLoader including version 2025 alpha and version 2025 as shown in the figure below.

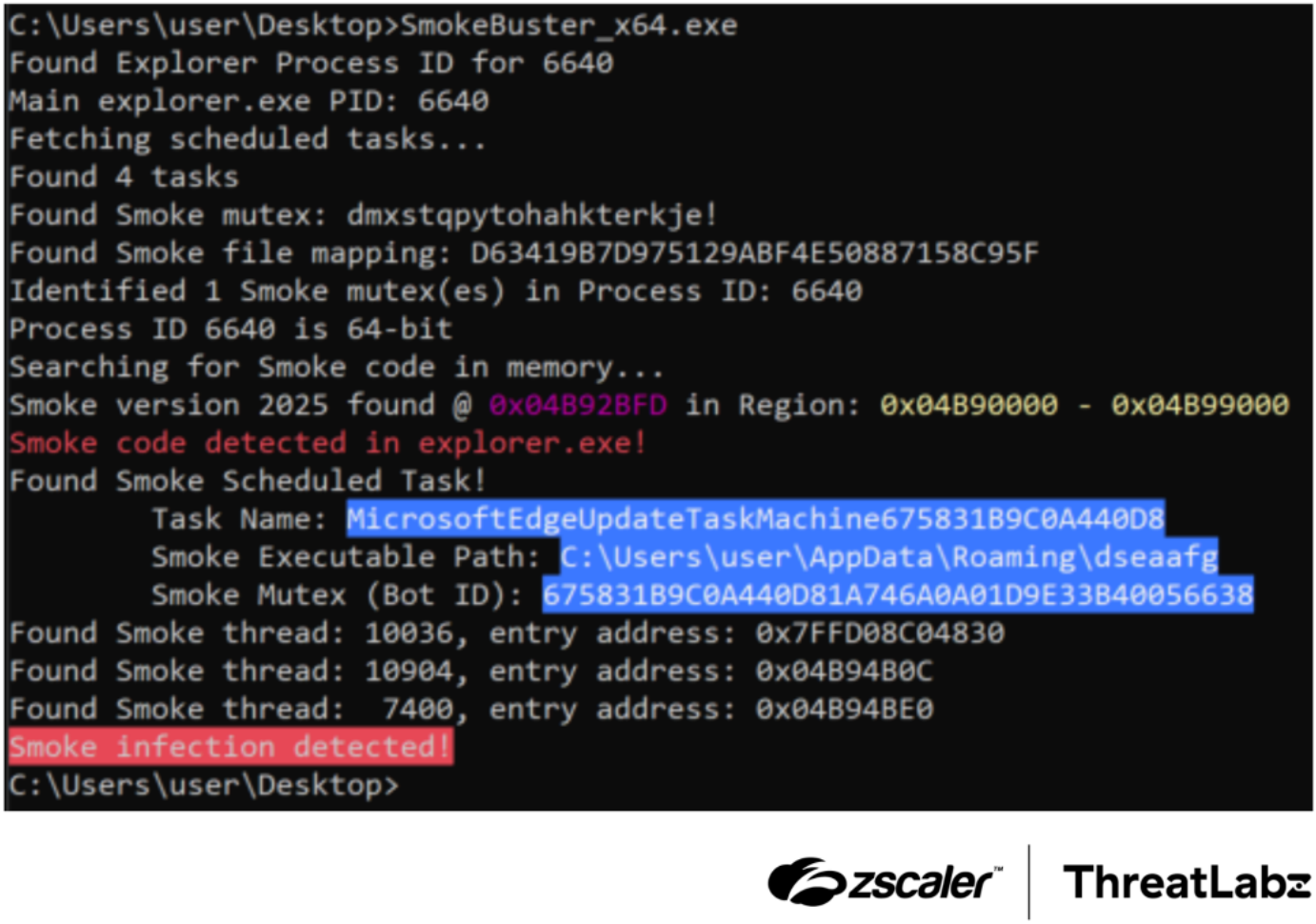

Figure 4: SmokeBuster example run for SmokeLoader version 2025

The tool is currently available in our GitHub repository here.

Conclusion

Despite Operation Endgame, SmokeLoader continues to be updated and used by multiple threat groups. The latest updates in SmokeLoader are relatively small, but fix important bugs, and are designed to hinder static-based detections. Currently, SmokeLoader version 2025 alpha is the most active version, which may be due to the fact that it is backward compatible with previous versions of the C2 panel. However, SmokeLoader version 2025 is likely to be adopted and deployed by more threat actors in the near future.

Zscaler Coverage

In addition to sandbox detections, Zscaler's multilayered cloud security platform detects indicators related to SmokeLoader at various levels with the following threat names:

- Win32.Downloader.Smokeloader

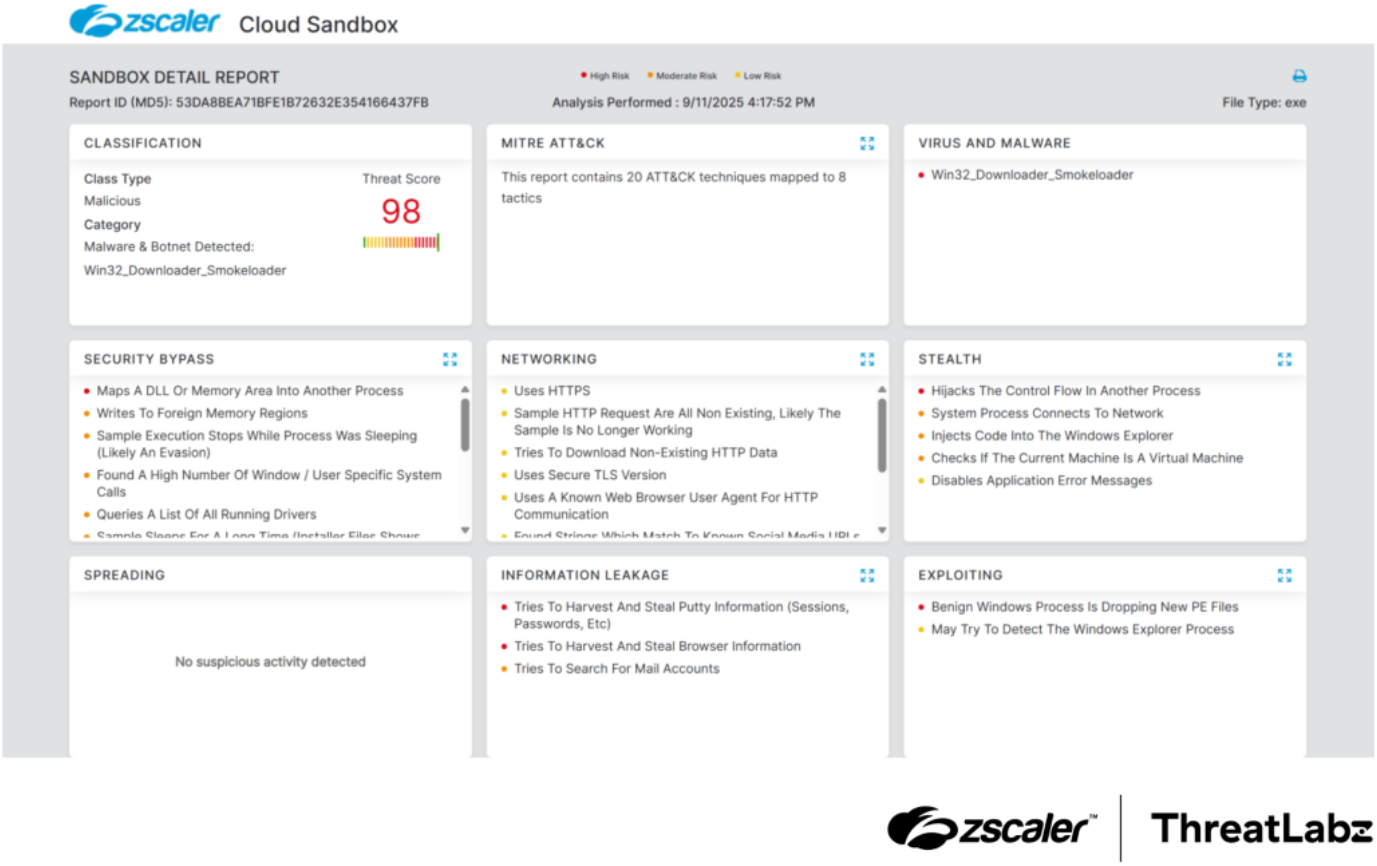

Figure 5: Zscaler Cloud Sandbox report

Indicators Of Compromise (IOCs)

Indicator	Description
fe18dba2d72ccf4a907d07674b18d1bc23e3ea10f66cbf2a79e73000df43b358	SmokeLoader version 2025 alpha
d5e20fc37dd77dd0360fd32446799978048a2c60e036dbfbf5e671333ebd81f1	SmokeLoader version 2025 alpha
413325dfeddf2287f86ca9998c1f6be2942145a647a14f1bfe1390e738adae61	SmokeLoader version 2025 alpha
d38f9ab81a054203e5b5940e6d34f3c8766f4f4104b14840e4695df511feaa30	SmokeLoader version 2025
0b06c6a25000addde175277b2d157d5bca4ab95cbfe3d984f1dba2ecefa3a4cd	SmokeLoader version 2025
http://ardt[.]info/tmp/	SmokeLoader C2
http://disciply[.]nl/tmp/	SmokeLoader C2
http://e-bonds[.]ru/tmp/	SmokeLoader C2
http://cobyrose[.]com/tmp/	SmokeLoader C2
http://dfbdw3tyge[.]info/tmp/	SmokeLoader C2
http://cusnick[.]com/tmp/	SmokeLoader C2
http://dfbdw3tyge[.]info/tmp	SmokeLoader C2

Indicator	Description
http://es-koerier[.]nl/tmp/	SmokeLoader C2
http://solanges[.]info/tmp/	SmokeLoader C2
http://udlg[.]nl/tmp/	SmokeLoader C2
http://ownmbaego[.]com/index.php	SmokeLoader C2
https://ownmbaego[.]com/index.php	SmokeLoader C2
http://176.46.152[.]46/	SmokeLoader C2
http://178.16.53[.]7/	SmokeLoader C2

Thank you for reading

Was this post useful?

Yes, very!

Not really

Explore more Zscaler blogs

SmokeBuster: Keeping Systems SmokeLoader Free

Read post

Operation Endgame: Up In Smoke

Read post

A Brief History of SmokeLoader, Part 1

Read post

Get the latest Zscaler blog updates in your inbox

By submitting the form, you are agreeing to our privacy policy.