Latrodectus Rapid Evolution Continues With Latest New Payload Features

By Leandro Fróes

Published: 2024-08-29 · Archived: 2026-04-05 15:03:36 UTC

Summary

Latrodectus is a downloader first discovered by Walmart back in October of 2023. The malware became very famous due to its similarities with the famous IcedID malware, not only in the code itself but also the infrastructure, as previously reported by Proofpoint and Team Cymru S2.

The malware is usually delivered via email spam campaigns conducted by two specific threat actors: TA577 and TA578. Among the several features it contains is the ability to download and execute additional payloads, collect and send system information to the C2, terminate processes, and more. In July of 2024 Latrodectus was also observed being delivered by a BRC4 badger.

During the Threat Labs hunting activities we discovered a new version of the Latrodectus payload, version 1.4. The malware updates include a different string deobfuscation approach, a new C2 endpoint, two new backdoor commands, and more.

In this blog, we will focus on the features added/updated in this new version.

JavaScript file analysis

The first payload of the infection chain is a JavaScript file obfuscated using a similar approach used by other Latrodectus campaigns. The obfuscation technique is employed by adding several comments into the file, making it more difficult to be analyzed as well as increasing the file size considerably.

The relevant code is present in between the junk comments and once removed from the file we can see the code that would be executed.

The malware searches for lines starting with the “/////” string, puts them into a buffer and executes them as a JS function. The executed function then downloads an MSI file from a remote server and executes/installs it.

MSI file analysis

Once executed/installed, the MSI file uses the rundll32.exe Windows tool to load a DLL named “nvidia.dll” and calls a function named “AnselEnableCheck” exported by this DLL. The malicious DLL is stored inside a CAB file named “disk1”, present in the MSI file itself:

Crypter analysis

As an attempt to obfuscate the main payload, the “nvidia.dll” file uses a crypter named Dave. This crypter has been around for a long time and was used in the past by other malware such as Emotet, BlackBasta, and previous versions of Latrodectus.

The crypter stores the payload to be executed either in a resource or in a section. In the analyzed sample, the payload is stored in a section named “V+N”.

The steps used to deobfuscate, load, and execute the final payload are rather simple. The malware moves a key into the stack and resolves the Windows API functions VirtualAlloc, LoadLibrary, and GetProcAddress.

It then allocates memory using the VirtualAlloc function and performs a multi-byte XOR operation against the data in the mentioned section using the previously set key and the result of the operation is the final payload. The next steps involve aligning the payload in memory and calling its main function.

Since the crypter first copies the original payload to the allocated memory before the other steps are performed, one could simply dump the content of the first allocated memory and obtain the final payload. A script to statically unpack/deobfuscate Latrodectus payloads using Dave crypter can be found here.

The final payload is a DLL and its DllMain function is called by the crypter code. The next step is the execution of the “AnselEnableCheck” exported function, which is responsible for the execution of the final payload.

When looking at the final payload we notice it has multiple exported functions, though since all of them have the same RVA it doesn’t matter which one is called.

Latrodectus DLL analysis

Since the general features of the main payload were already described in the past by other researchers, the following sections will focus on the updates employed by the new Latrodectus version.

String obfuscation

Unlike the previous versions that used an XOR operation to deobfuscate its strings, the updated version uses AES256 in CTR mode. The AES key is hardcoded in the deobfuscation function itself and the IV changes for each string to be decrypted. The key used in the analyzed samples is "d623b8ef6226cec3e24c55127de873e7839c776bb1a93b57b25fdbea0db68ea2".

The deobfuscation function receives two parameters. The first one is a chunk of data and the second an output buffer. The chunk of data is used to store information used to decrypt the string and follows the format below:

- String length: 2 bytes
- IV: 16 bytes
- Encrypted string: Size specified in the first field

One thing to notice is that sometimes there will be extra bytes after the encrypted string content. The following image is an example of this data chunk:

Campaign ID

In the current malware version, the campaign ID generation function continues to use the same approach where an input string is hashed using the FNV algorithm. However, a new input string “Wiski” was used, resulting in the hash 0x24e7ce9e as the campaign ID.

C2 communication

For its initial communication with the C2 server, Latrodectus collects a lot of information from the infected system such as the username, OS version and the MAC address. The information is formatted using a specific pattern, encrypted using the RC4 algorithm, encoded using base64 and sent to the C2.

The RC4 keys found in the analyzed samples were “2sDbsEUXvhgLOO4Irt8AF6el3jJ0M1MowXyao00Nn6ZUjtjXwb” and “kcyBA7IbADOhw5ztcv09vmF8GYmR38eu7OGdfD7pyRelTPKH1G”.

During the data formatting we are able to flag the version number 1.4 being set.

The information is sent in the HTTP body via an HTTP POST request. The endpoint used in the new variants is “/test” instead of “/live” as observed in previous versions. Although a very weak indicator the usage of this specific endpoint might indicate that this is a test version of the malware.

Commands

In version 1.4 Latrodectus has introduced two new commands to its payload: command ID 22 and 25.

Command 0x16

In this command the malware downloads a shellcode from the specified server and executes it via a new thread.

The difference between this command and command 14 is that a function that performs base64 encoding is passed as a parameter to the shellcode itself. The address of the base64 function is stored in a mapped file view named “12345”.

Command 0x19

In this command, the malware receives a file name and a remote location to download the file from. The file name is then appended to %AppData%, the file is downloaded and its content written to the mentioned path.

Considering these additions, below is a table of the updated commands supported by the malware:

Command ID	Description
2	Collect a list of desktop file names
3	Collect info about the running processes
4	Collect system information
12	Download and execute a regular executable
13	Download and execute a DLL via rundll32
14	Download and execute a shellcode
15	Self update
17	Terminate itself

Command ID	Description
18	Download and execute the IcedID payload
19	Increase sleep timeout
20	Reset request counter
21	Download and execute the stealer module
22	Download and execute a shellcode passing the base64 encoding function as a parameter
25	Download a file to %AppData% directory

Netskope Detection

- Netskope Threat Protection
  - Gen:Variant.Ulise.493872
  - Trojan.Generic.36724146
- Netskope Advanced Threat Protection provides proactive coverage against this threat.
  - Win64.Trojan.ShellCoExec

Conclusions

Latrodectus has been evolving pretty fast, adding new features to its payload. The understanding of the updates applied to its payload allow defenders to keep automated pipelines properly set as well as use the information for further hunting for new variants. Netskope Threat Labs will continue to track how the Latrodectus evolves and its TTP.

IOCs

All the IOCs and scripts related to this malware can be found in our GitHub repository.
