Gelsemium: When threat actors go gardening

welivesecurity.com/2021/06/09/gelsemium-when-threat-actors-go-gardening/

June 9, 2021

ESET researchers shed light on new campaigns from the quiet Gelsemium group

In mid-2020, ESET researchers started to analyze multiple campaigns, later attributed to the Gelsemium group, and tracked down the earliest version of the malware going back to 2014. Victims of these campaigns are located in East Asia as well as the Middle East and include governments, religious organizations, electronics manufacturers and universities.

Key points in this report:

- ESET researchers believe that Gelsemium is behind the supply-chain attack against BigNox that was previously reported as *Operation NightScout*
- ESET researchers found a new version of Gelsemium, complex and modular malware, later referred to as Gelsemine, Gelsenicine and Gelsevirine
- New targets were discovered that include governments, universities, electronics manufacturers and religious organizations in East Asia and the Middle East
- Gelsemium is a cyberespionage group active since 2014

Gelsemium

Download Research Paper

The geographical distribution of Gelsemium's targets can be seen in Figure 1.

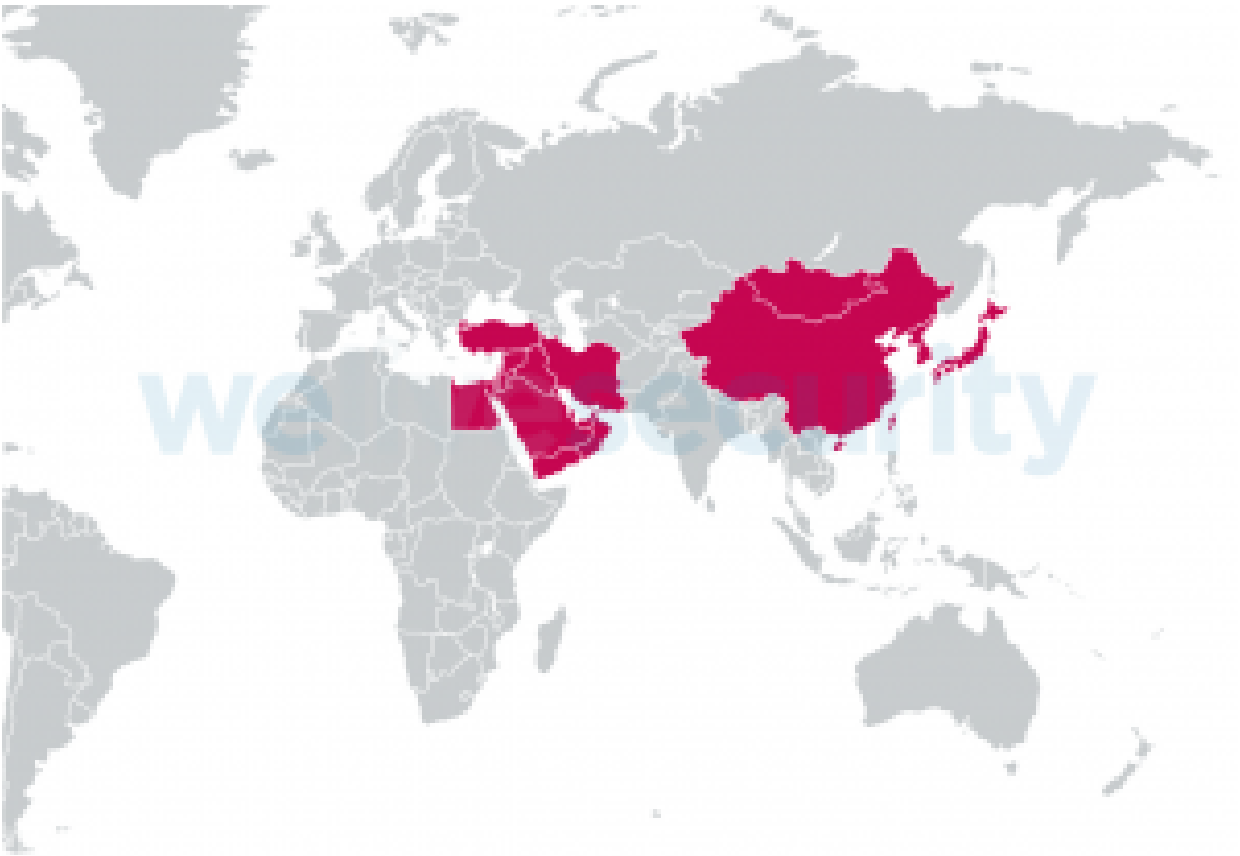

Figure 1. Targets' locations

Gelsemium components

Gelsemium's whole chain might appear simple at first sight, but the exhaustive configurations, implanted at each stage, modify on-the-fly settings for the final payload, making it harder to understand. Behaviors analyzed below are tied to the configuration; as a result, filenames and paths may be different in other samples. Most of the campaigns we observed follow what we describe here.

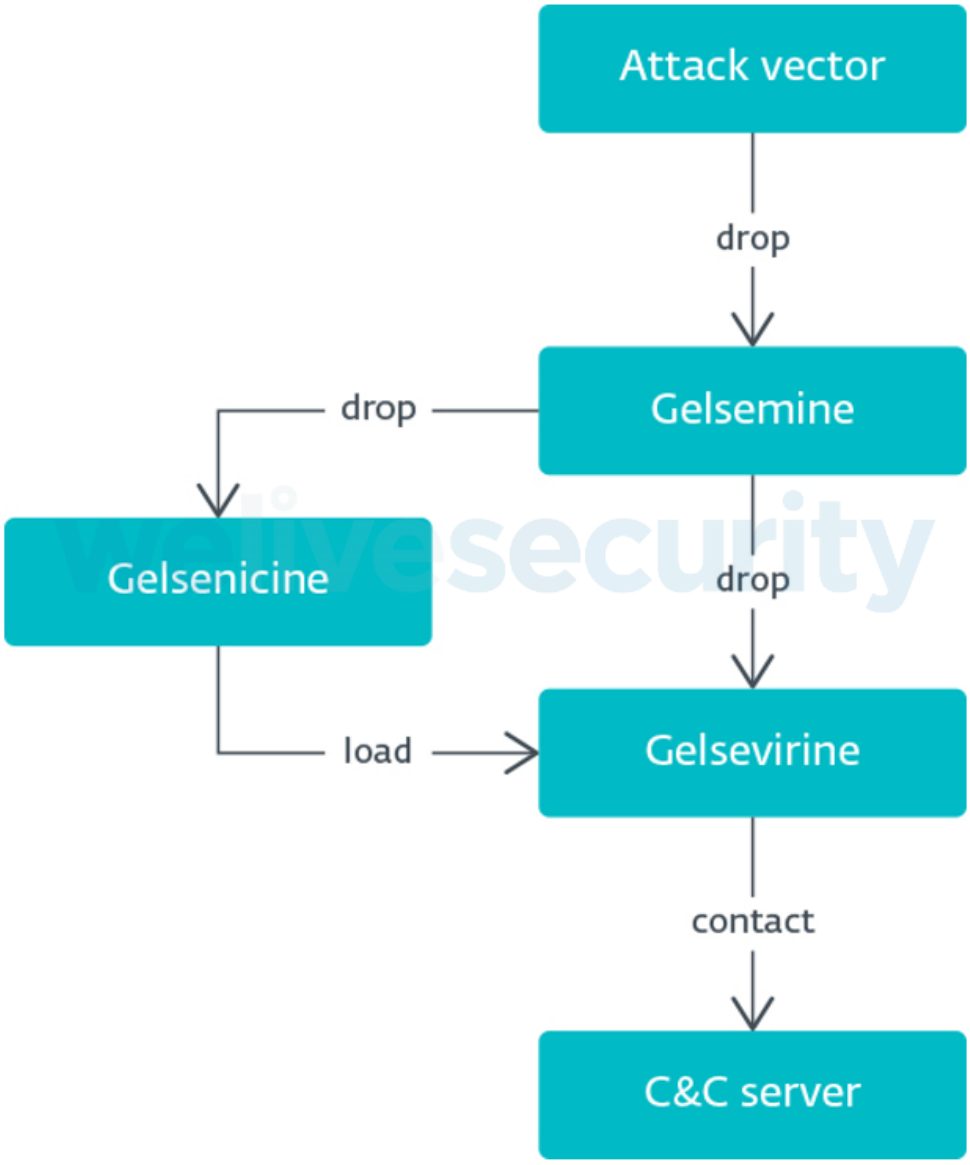

Figure 2. Overview of the three components' workflow

Gelsemine: The dropper

Gelsemium's first stage is a large dropper written in C++ using the Microsoft Foundation Class library (MFC). This stage contains multiple further stages' binaries. Dropper sizes range from about 400 kB to 700 kB, which is unusual and would be even larger if the eight embedded executables were not compressed. The developers use the zlib library, statically linked, to greatly reduce the overall size. Behind this oversized executable is hidden a complex yet flexible mechanism that is able to drop different stages according to the characteristics of the victim computer, such as bitness (32-bit vs. 64-bit) or privilege (standard user vs. administrator). Almost all stages are compressed, located in the resource section of the PE and mapped into the same component's memory address space. Figure 3 illustrates all stages in the Gelsemine component.

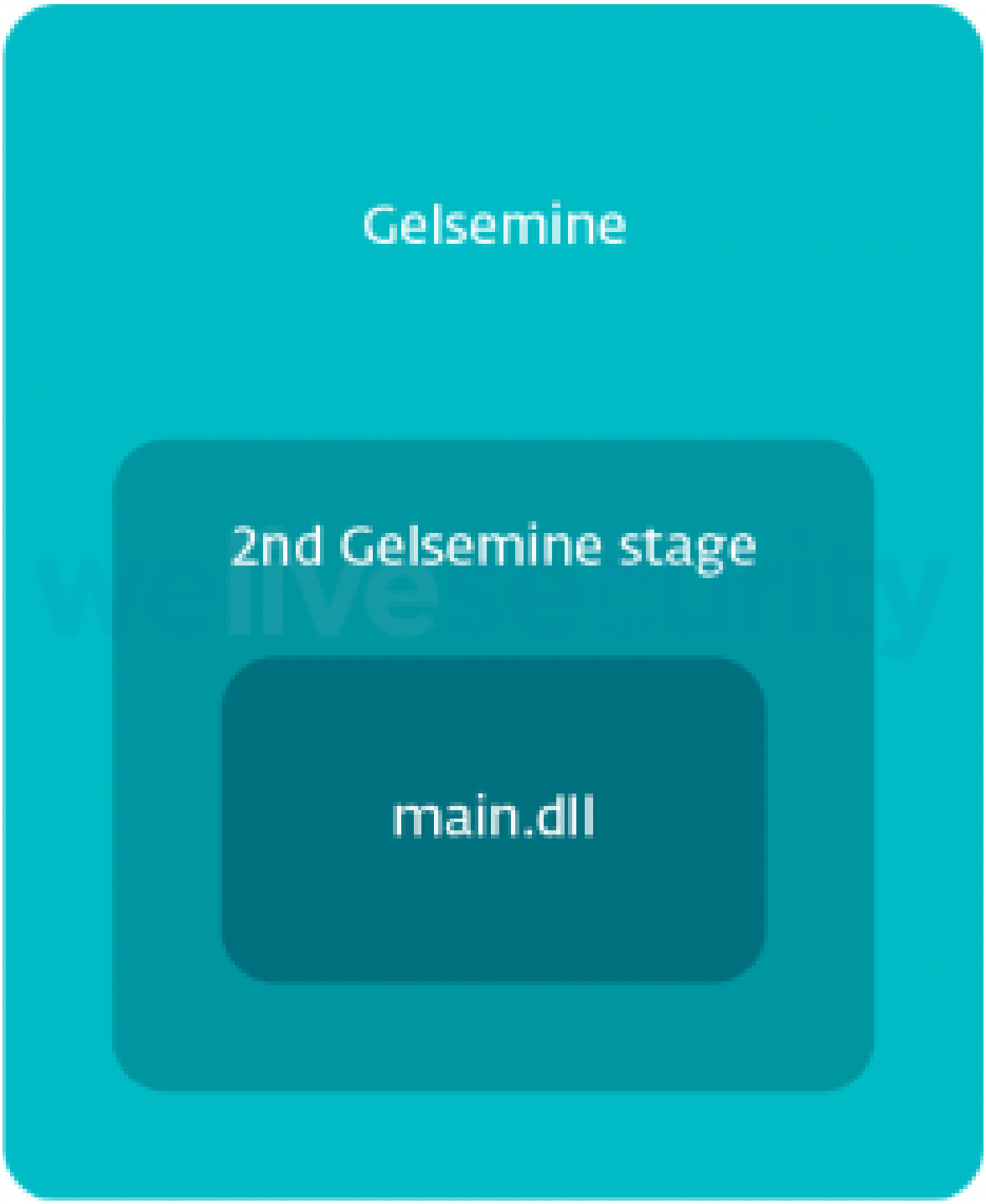

Figure 3. Gelsemine address space overview

Gelsenicine: The loader

Gelsenicine is a loader that retrieves Gelsevirine and executes it. There are two different versions of the loader – both of them are DLLs; however, they differ in the context where Gelsemine is executed.

For victims with administrator privileges, Gelsemine drops Gelsenicine at C:\Windows\System32\spool\prtprocs\x64\winprint.dll (user-mode DLL for print processor) that is then automatically loaded by the spoolsv Windows service. To write a file under the %WINDIR%/system32 directory, administrator privileges are mandatory; hence the requirement previously mentioned.

Users with standard privileges compromised by Gelsemine drop Gelsenicine under a different directory that does not require administrator privileges. The DLL chrome_elf.dll is dropped under %CommonAppData%/Google/Chrome/Application/Library/.

Gelsevirine: The main plug-in

Gelsevirine is the last stage of the chain and it is called MainPlugin by its developers, according to the DLL name and also PDB path found in old samples (Z:\z_code\Q1\Client\Win32\Release\MainPlugin.pdb). It's also worth mentioning that if defenders manage to obtain this last stage alone, it won't run flawlessly since it requires its arguments to have been set up by Gelsenicine.

The config used by Gelsenicine contains a field named controller_version that we believe is the versioning used by the operators for this main plug-in. Figure 4 provides a timeline of the different versions we have observed in the wild; the dates are approximate.

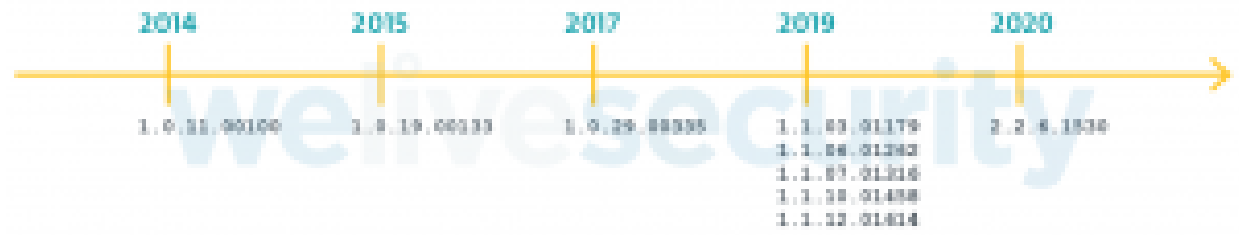

Figure 4. Gelsevirine version timeline

Additional links/tools

During our investigation we encountered some interesting malware described in the following sections.

- **Operation NightScout (BigNox)**: In January 2021, another ESET researcher analyzed and wrote an article about Operation NightScout; a supply-chain attack compromising the update mechanism of NoxPlayer, an Android emulator for PCs and Macs, and part of BigNox's product range with over 150 million users worldwide. The investigation uncovered some overlap between this supply-chain attack and the Gelsemium group. Victims originally compromised by that supply-chain attack were later being compromised by Gelsemine. Among the different variants examined, "variant 2" from that article shows similarities with Gelsemium malware.

- **OwlProxy**: This module also comes in two variants – 32- and 64-bit versions – and as a result it contains a function to test the Windows version the same as in the Gelsemium components.
- **Chrommme**: Chrommme is a backdoor we found during our adventures in the Gelsemium ecosystem. Code similarities with Gelsemium components are almost nonexistent but small indicators were found during the analysis that lead us to believe that it's somehow related to the group. The same C&C server was found in both Gelsevirine and Chrommme, both are using two C&C servers. Chrommme was found on an organization's machine also compromised by Gelsemium group.

Conclusion

The Gelsemium biome is very interesting: it shows few victims (according to our telemetry) with a vast number of adaptable components. The plug-in system shows that its developers have deep C++ knowledge. Small similarities with known malware tools shed light on interesting, possible overlaps with other groups and past activities. We hope that this research will drive other researchers to publish about the group and reveal more roots related to this malware biosphere.

A full and comprehensive list of Indicators of Compromise (IoCs) and samples can be found in the full white paper and in our GitHub repository.

For any inquiries, or to make sample submissions related to the subject, contact us at threatintel@eset.com.

To learn more about how threat intelligence services can enhance the cybersecurity posture of your organization, visit the ESET Threat Intelligence page.

9 Jun 2021 - 02:00PM

Sign up to receive an email update whenever a new article is published in our Ukraine Crisis – Digital Security Resource Center

Newsletter

Discussion