New Formbook Campaign Delivered Through Phishing Emails

By Gustavo Palazolo

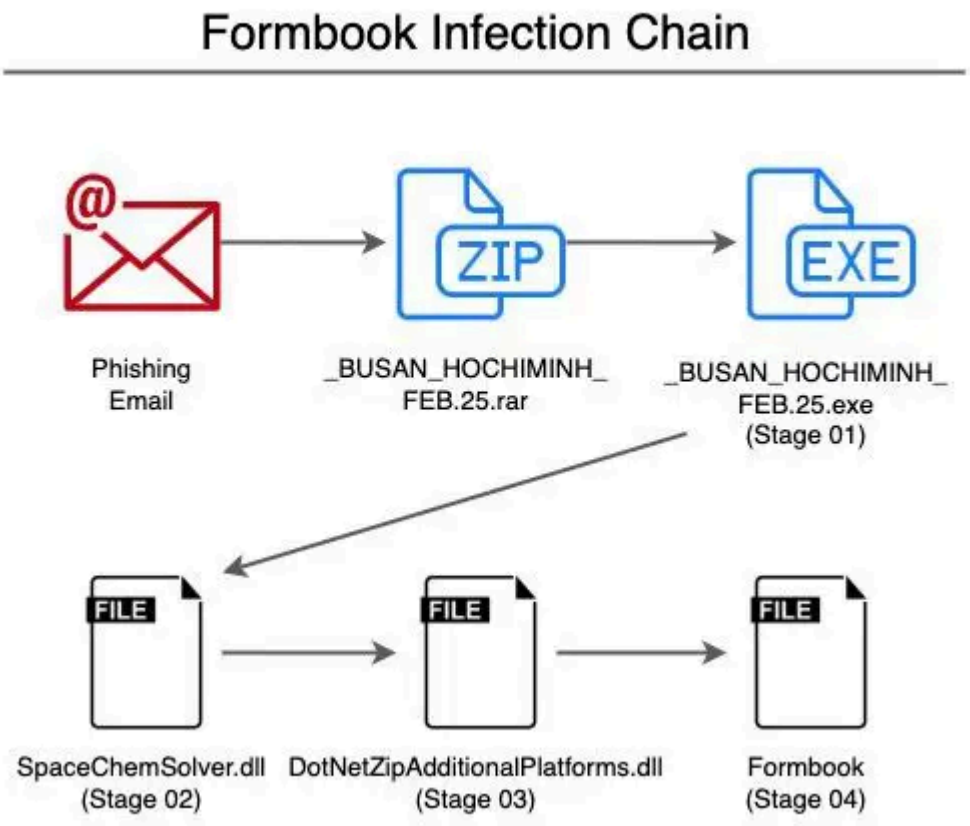
Published: 2022-03-11 · Archived: 2026-04-06 01:31:24 UTC

Summary

Since the beginning of 2022, the unfolding geopolitical conflict between Russia and Ukraine has resulted in the discovery of new malware families and related cyberattacks. In January 2022, a new malware named WhisperGate was found corrupting disks and wiping files in Ukrainian organizations. In February 2022, another destructive malware was found in hundreds of computers in Ukraine, named HermeticWiper, along with IsaacWiper and HermeticWizard.

Aside from new malware families and novel attacks, previously known malware families continue to be used against organizations in Ukraine and throughout the world. Recently, Netskope Threat Labs came across an interesting phishing email addressed to high-ranking government officials in Ukraine containing Formbook (a.k.a. XLoader), which is a well-known malware operating in the MaaS (Malware-as-a-Service) model. This malware provides full control over infected machines, offering many functionalities such as stealing passwords, grabbing screenshots, downloading, and executing additional malware, among others.

The email seems to be part of a new spam campaign, since there were multiple emails with the same subject and body addressed to other recipients. Most of them contain an infected spreadsheet encrypted with the "VelvetSweatshop" password, which is a known Formbook behavior. The infected spreadsheet delivers the threat through vulnerability described under CVE-2017-11882 and CVE-2018-0798. However, the email addressed to government officials in Ukraine contains a .NET executable, responsible for loading Formbook in a multi-stage chain:



In this blog post, we will analyze all the layers from the email attachment to the last Formbook payload.

Phishing Email

The infection flow starts with a generic phishing email that uses a common technique, tricking the victim into downloading the payload by pretending to be a shipping invoice.

Phishing email containing a malicious attachment.

The attachment is a compressed file containing the first Formbook stage.

Email attachment carrying Formbook.

Also, as we mentioned previously, we found similar emails delivering malicious spreadsheets, so we believe that this is part of a new spam campaign delivering multiple threats.

Similar phishing email with a malicious attachment.

Analysis – Summary

Before executing the last file (Formbook), the malware is divided into multiple stages, which we have summarized below.

1. **Stage 01** is a loader, responsible for decoding and executing the next stage;
2. **Stage 02** is another loader, responsible for obtaining the encrypted bytes of **Stage 03** from the resources of **Stage 01**, decrypting and executing it;
3. **Stage 03** is a known packer/loader named CyaX-Sharp, responsible for decrypting and executing the last stage;
4. **Stage 04** is the Formbook payload, which injects itself into other processes, as described later in this analysis.

Summary of Formbook loading process

Analysis – Stage 01

The first stage is a .NET executable likely compiled on February 21, 2022. This file is a loader, responsible for decoding and executing the next stage.

Binary details of the first stage.

Once we decompile the file, we can see that the real executable name is "**VarArgMet.exe**". This stage doesn't contain any code obfuscation but does contain an obfuscated string and an encrypted resource which we will discuss later.

First stage decompiled.

Also, this file seems to be an infected version of a public .NET project named PlaylistPanda, created in 2009. Looking at the entry point, we can see the same code that is published in the PlaylistPanda public repository, where the **MainForm** function is called, followed by **InitializeComponent.**

Entry point of the first stage.

In this malicious version, the **InitializeComponent** function contains the main code of the first stage. Once running, the code reads an obfuscated and base64 encoded string stored in a variable named **x121312x121312**, which contains the next stage. Once it's deobfuscated and decoded, the file is passed as an argument to the function **Springfield.**

Furthermore, this loader contains a lot of junk code that will never be executed, possibly to confuse analysts and slow down analysis.

Loader’s main code, decoding and executing the next stage.

The **Springfield** function then loads the second stage as a .NET assembly, which is saved in a variable named **DebuggerVisualizer**.

Second stage being loaded as a .NET assembly.

The **DebuggerVisualizer** variable is then passed as an argument to the **EraInfo** function, which executes the second stage by calling the **CreateInstance** function with the payload and three strings as arguments:

- 5A6F6E654964656E746974795065726D697373696F6E417474726962 (ZoneIdentityPermissionAttrib)
- 6F513037 (oQ07)
- PlaylistPanda

Second stage being executed.

Analysis – Stage 02

The second stage is a .NET DLL, likely compiled on February 16, 2022. This file is another loader responsible for executing the third stage, which is stored in the resources of the first stage.

Binary details of the second stage.

Once we decompile the file, we can see that the real name is "**SpaceChemSolver.dll**". This file doesn't have any sort of code obfuscation or protection. The entry point of this stage is the **RunCore** function, which is called within **SharpStructures.Main.**

Second stage’s name.

This code is responsible for loading and executing the third stage, which is encrypted and stored as a resource named **ZoneIdentityPermissionAttrib** in the first stage (**PlaylistPanda**), masqueraded as a bitmap image.

Third stage execution flow.

After loading the fake image from the first stage resources, the function **ConstructionResponse** is responsible for decrypting the binary using XOR operations with the string **“oQ07”**.

Function that decrypts the third stage.

Once decrypted, the second stage loads the third stage as a .NET assembly, like we saw previously, executing a function named **yjO9HynvmD**.

Third stage being loaded.

Analysis – Stage 03 (CyaX-Sharp)

The third stage is yet another .NET file, but this time it's protected with .NET Reactor. The compilation date is also near the other files, on February 21, 2022. This file is a known loader/packer named CyaX-Sharp, which is commonly used to deliver malware like AgentTesla and Warzone RAT.

Binary details of the third stage.

Before executing the payload, this packer offers many functionalities such as Virtual Machine and Sandbox detection. These features can be enabled or disabled through configuration, which is stored in a string within the binary.

CyaX-Sharp configuration string.

Once it’s running, it starts by parsing the configuration string and then calling the functions related to the features for which the option is enabled.

CyaX-Sharp main function.

The malware checks if there's another instance running through a Mutex object named "**WuhpBQuQigdPUFFvzgV**".

Mutex created by the third stage.

Then, the malware checks if the process is running with administrative privileges, and it adds the path of the executable to the exclusion list of Microsoft Defender.

Simple Windows Defender bypass.

In this specific file, the Virtual Machine and Sandbox verification are disabled. However, just to demonstrate how it works, this malware is able to detect virtualized environments by checking the presence of specific values in the Windows Registry, used by software like VirtualBox and VMware.

Functionality to detect virtualized environments.

For sandbox detection, the malware searches for common file names, loaded modules, and windows titles.

Functionality to detect sandboxes.

CyaX-Sharp also offers a feature to download and execute additional payloads, which is also disabled in this sample.

Functionality to download and execute additional payloads.

It then copies itself to AppData, as "**YtGUemuxgzC.exe**".

Malware copying itself to AppData.

The permission of this file is then changed to avoid anyone from deleting it.

Changing recently copied AppData permission.

To execute this copy, a very simple persistence technique is implemented via Windows scheduled tasks.

Malware’s persistence.

The final stage is then loaded from a resource named “fVkXSK7E”, which contains the encrypted bytes of Formbook.

CyaX-Sharp loading the final stage.

Before decrypting the payload, CyaX-Sharp builds the path string of the executable that will be used to inject Formbook. In this case, the malware is configured to use "**vbc.exe**".

Formbook is then decrypted through bitwise operations using the bytes of the string "**SUASbkTWociWWQ**".

CyaX-Sharp decrypting Formbook.

Formbook is injected into "**vbc.exe**" via Process Hollowing, which we have already explained in more detail in this analysis. All the APIs are loaded dynamically via GetProcAddress and LoadLibraryA APIs.

APIs related to Process Hollowing.

We can find Formbook fully decrypted by inspecting the "**vbc.exe**" process memory, or by dumping the bytes once it's decrypted in the third stage.

Formbook injected into “vbc.exe”

Analysis – Stage 04 (Formbook)

The last stage is Formbook, which is an infostealer sold as a service (MaaS) on hacking-related forums since 2016. This malware provides many functionalities, such as:

1. Grabbing keystrokes (Keylogger);
2. Grabbing screenshots;
3. Grabbing HTTP(s) forms from network requests;
4. Stealing data from the clipboard;
5. Stealing data from common software, such as browsers, email, and ftp clients;
6. Shutdown/Reboot the OS;
7. Download and execute additional files;
8. Remotely execute commands;
9. Encrypted C2 communication;

The malware is written in ASM/C, and the compilation timestamp seems to be altered, as it indicates it was created in 2003.

Binary details of Formbook payload.

The primary entry point of Formbook is straightforward. Once running, it calls the main function which is named "**InjectMaliciousPayload**" in this IDA database. Most of the strings are obfuscated using the "Stack Strings" technique, which can be defeated with FLOSS. A list of decoded strings for this sample can be found in our GitHub repository.

Formbook’s primary entry point.

It then executes a sequence of functions to assess the environment and determine whether it’s going to run, by verifying the presence of blacklisted processes and usernames, for example.

Formbook anti-analysis mechanisms.

After the anti-analysis mechanisms, Formbook proceeds by creating and injecting itself into a randomly chosen process from Windows directory. In this case, it is injected into "**svchost.exe**".

Formbook injecting itself into another process.

Also, another instance is injected into “**explorer.exe**”, responsible for the C2 communication. We found 65 different domains in this sample, where 64 are only used as decoys.

Formbook trying to connect to domains.

The real C2 of this sample is “www.biohackingz[.]one”.

Formbook C2 communication.

This domain was first seen on February 21, 2022 on VirusTotal.

Analysis of the C2 domain.

Once the communication is established, Formbook parses the data to determine the action that needs to be taken.

Part of the function that parses the C2 response.

Conclusions

Formbook is an infostealer, available via the Malware-as-a-Service model since 2016, often used by non-experienced people as it's sold as a service at a reasonable price. Although it's a simple threat, it contains many layers and techniques to slow down analysis and bypass detection engines. Regardless of the cheap price, Formbook can be quite dangerous as it provides full access to infected systems. Netskope Threat Labs will keep monitoring this new campaign as well as others that may emerge.

Protection

Netskope Threat Labs is actively monitoring this campaign and has ensured coverage for all known threat indicators and payloads.

- **Netskope Threat Protection**
  - Win32.Trojan.FormBook
  - Win32.Spyware.Noon
  - Win32.Malware.Heuristic
  - ByteCode-MSIL.Malware.Heuristic

- **Netskope Advanced Threat Protection** provides proactive coverage against this threat.
    - Gen.Malware.Detect.By.StHeur indicates a sample that was detected using static analysis
    - Gen.Malware.Detect.By.Sandbox indicates a sample that was detected by our cloud sandbox

IOCs

All the IOCs related to this campaign and the Yara rules can be found in our GitHub repository.
