Unusual "ZPAQ" Archive Format Delivers Malware

By Anna Lvova

Published: 2023-11-20 · Archived: 2026-04-05 15:18:29 UTC

11/20/2023

New "Agent Tesla" Variant: Unusual "ZPAQ" Archive Format Delivers Malware

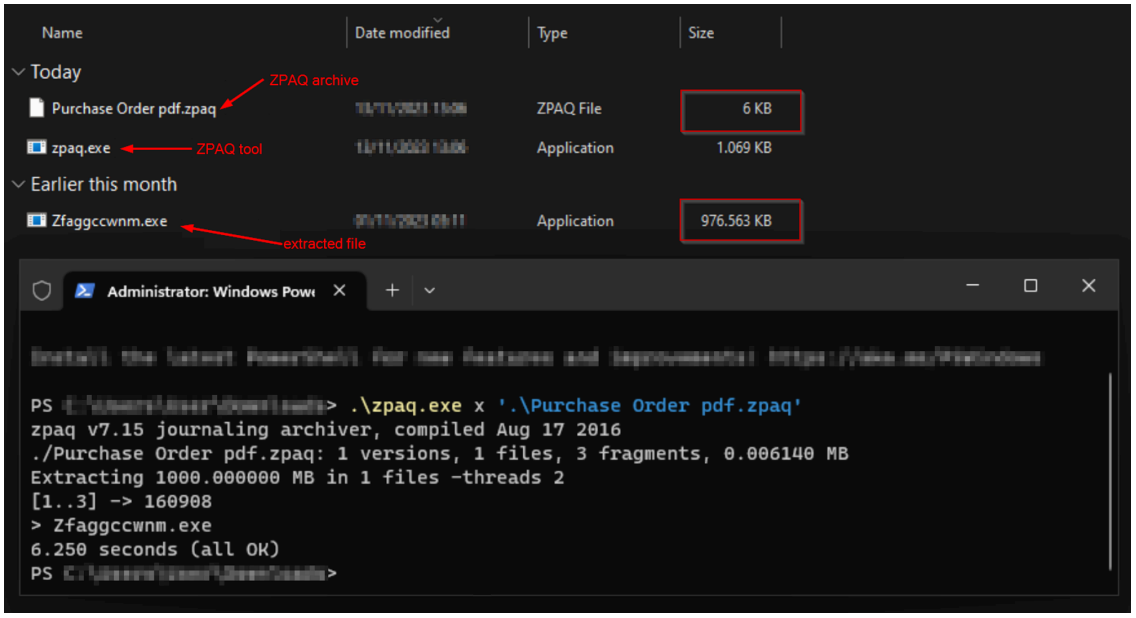
Reading time: 4 min (1143 words)

A new variant of Agent Tesla uses the uncommon compression format ZPAQ to steal information from approximately 40 web browsers and various email clients. But what exactly is this file compression format? What advantage does it provide to threat actors? And why it is assumed that the version of Agent Tesla is “new”?

ZPAQ compression format and what it hides

On November 1, 2023, researcher Xavier Mertens reported a phishing attempt on one of his honeypots. What's noteworthy is that a threat actor used the ZPAQ archive and .wav file extension to infect the system with Agent Tesla.

ZPAQ is a file compression format that offers a better compression ratio and journaling function compared to widely used formats like ZIP and RAR. That means that ZPAQ archives can be smaller, saving storage space and bandwidth when transferring files. However, ZPAQ has the biggest disadvantage: limited software support. There are GUI unpackers that support this format, for example, Peazip, but ZPAQ can be extracted primarily with a command-line tool that does not make it easy to work with, especially for users without technical expertise.



Extraction of the .NET executable with ZPAQ cmd tool and comparison of size.

The initial file was found in an email called "Purchase Order pdf.zpaq". As you can see from the file name, the threat actor is attempting to deceive us into believing that the archive contains a PDF file with important information. After using the command-line extraction tool ZPAQ it turns out that the 6KB archive suddenly "weighed" 1GB after extraction. After a deep look into the executable, it turned out that the file is a .NET executable with async methods and that is bloated with zero bytes. One of the indicators is 0 entropy in the overlay section. The analysis of the executable in a hex editor proved that 90% of the sample is filled with zero bytes.

Threat actors may prefer to use bloated executable files due to their significant advantage: the inability to upload such files to automatic scanning systems, Virus Total, sandboxes, etc. This technique allows them to bypass traditional security measures and increase the effectiveness of their attack.

Sounds like stolen data

ILSpy. Link to download malicious component and the string that is responsible for decryption (Click to enlarge)

The main function of the unarchived .NET executable is to download a file with .wav extension and decrypt it (3DES algorithm).

Waveform Audio File Format (shortened as .wav) is a popular audio file format standard. However, in that case, it is unrelated to audio, and the threat actor simply used this file extension to hide the presence of malicious content. One possible reason is covert communication: using commonly used file extensions disguises the traffic as normal, making it more difficult for network security solutions to detect and prevent malicious activity.

Another Agent Tesla

```
        // Token: 0x0400000F RID: 15
        public static bool EnableKeylogger = Convert.ToBoolean("false");

        // Token: 0x04000010 RID: 16
        public static bool EnableScreenLogger = Convert.ToBoolean("false");

        // Token: 0x04000011 RID: 17
        public static bool EnableClipboardLogger = Convert.ToBoolean("false");

        // Token: 0x04000012 RID: 18
        public static bool EnableTorPanel = Convert.ToBoolean("false");

        // Token: 0x04000013 RID: 19
        public static bool EnableCookies = Convert.ToBoolean("false");

        // Token: 0x04000014 RID: 20
        public static bool DeleteBackspace = Convert.ToBoolean("false");

        // Token: 0x04000015 RID: 21
        public static int TorPid = 0;

        // Token: 0x04000016 RID: 22
        public static int KeyloggerInterval = Convert.ToInt32("20");

        // Token: 0x04000017 RID: 23
        public static int ScreenInterval = Convert.ToInt32("20");

        // Token: 0x04000018 RID: 24
        public static int LogType = Convert.ToInt32("3");

        // Token: 0x04000019 RID: 25
        public static string TelegramApi = "https://api.telegram.org/bot[redacted]";

        // Token: 0x0400001A RID: 26
        public static string ChatId = "5[redacted]351";

        // Token: 0x0400001B RID: 27
        public static bool AppAddStartup = Convert.ToBoolean("false");

        // Token: 0x0400001C RID: 28
        public static bool HideFileStartup = Convert.ToBoolean("false");

        // Token: 0x0400001D RID: 29
        public static string AppStartupFullPath = "";

        // Token: 0x0400001E RID: 30
        public static string StartupDirectoryPath = "";

        // Token: 0x0400001F RID: 31
        public static string StartupEnvName = "appdata";

        // Token: 0x04000020 RID: 32
        public static string StartupDirectoryName = "MYZPTk";

        // Token: 0x04000021 RID: 33
        public static string StartupInstallationName = "MYZPTk.exe";

        // Token: 0x04000022 RID: 34
        public static string StartupRegName = "MYZPTk";
    }
}
```

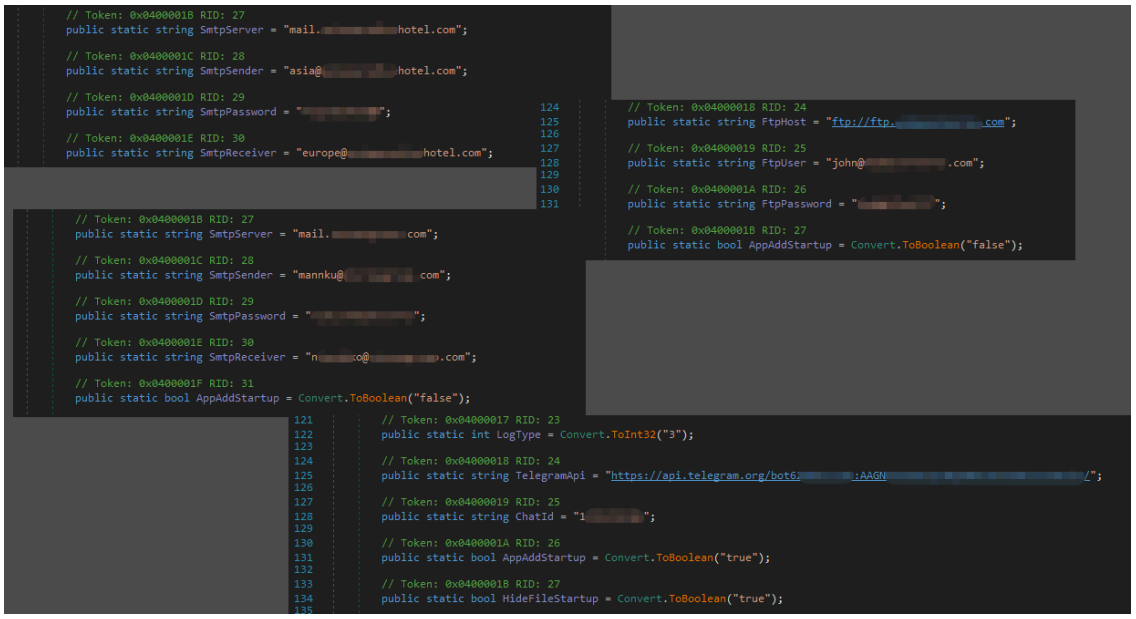
Configuration data (click to enlarge)

Agent Tesla is a .NET-based information stealer that emerged around 2014. Over time, it has undergone multiple updates, evolving in terms of both capabilities and evasion techniques. In this specific case, Agent Tesla was obfuscated with the .NET Reactor (my colleague Karsten has done an in depth analysis of this in a video - the link will open in a new window), and several rounds of de-obfuscation were necessary to make the code clearer. The analysis revealed that it possesses the following functions:

- targetting sensitive data of around 40 different web browsers
- stealing credentials from popular email clients

- screen logging
- keylogging
- gathering system information
- capturing sensitive data of VPN tools

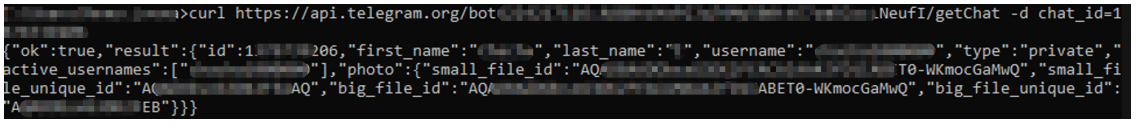
From a capabilities standpoint, it doesn't offer anything significantly new. However, after analysis of similar samples, all of them have a similar .NET class with configuration data. The way to submit the stolen data, persistence variables, keylogger variable and etc. are kept in this class. Other samples had the same structure, but just different methods to deliver information to the threat actor



Communication ways in similar samples. (Click to enlarge)

The way to submit the stolen data, persistence variables, keylogger variable and etc. are kept in this class. Other samples had the same structure, but just different methods to deliver information to the threat actor. It was noticed that besides Telegram, the threat actor uses FTP and SMTP. And the list can be much bigger, because since 30.09.2023 more than 700 versions of this variant were observed on VirusTotal. As is customary in casses like this, the data being used is associated with compromised websites, the accerss credentials to which were likely acquired through an access broker who specializes in selling those types of accounts..

One of the TelegramAPIs from the oldest observed sample is still active. Here the information that was found about this communication channel:



Active Telegram API from the oldest observed file (as of September 30, 2023)

Takeaways

The usage of the ZPAQ compression format raises more questions than answers. The assumptions here are that either threat actors target a specific group of people who have technical knowledge or use less widely known

archive tools, or they are testing other techniques to spread malware faster and bypass security software. However, it is definitely a good example that even very specific archive formats or widely spread file extensions like .wav can be used for malicious purposes.

Like any other stealer, Agent Tesla can harm not only private individuals but also organizations. It has gained popularity among cybercriminals for many reasons including ease of use, versatility, affordability on the Dark Web, and so on. It is worth mentioning that cybersecurity professionals and organizations are constantly working on developing countermeasures and detection techniques to minimize its effects. To protect your devices, it is essential to have malware protection, maintain a high level of security awareness, and regularly update software.

Information for fellow researchers

ZPAQ archive:
1c33eef0d22dc54bb2a41af485070612cd4579529e31b63be2141c4be9183eb6 - Archive.Trojan-Downloader.AgentTesla.LG5F9Z

.wav file:
c2c466e178b39577912c9ce989cf8a975c574d5febe15ae11a91bbb985ca8d2e - MSIL.Malware.Injector.L8JTF6

Agent Tesla:
45dc4518fbf43bf4611446159f72cdbc37641707bb924bd2a52644a3af5bab76 - MSIL.Trojan-Stealer.AgentTesla.B

Share Article

Content
