OneNote | ThreatLabz

By Meghraj Nandanwar, Shatak Jain

Published: 2023-03-01 · Archived: 2026-04-05 16:36:05 UTC

Case Study-1: RAT

Starting in December 2022, attackers have been using OneNote files to distribute Remote Access Trojans (RAT) such as AsyncRAT, Quasar RAT, NetWire, and Xworm. These RATs use complex obfuscation techniques with OneNote files in order to evade detection by security software.

During the course of the investigation, researchers found the file containing the malicious payload disguised under the misleading name "**PaymentAdv.one**".

Fig.2 - OneNote phishing document

After analyzing the file with OneNoteAnalyzer, researchers uncovered that the attack was carried out by dropping and executing a batch file called "**zoo1.bat**".

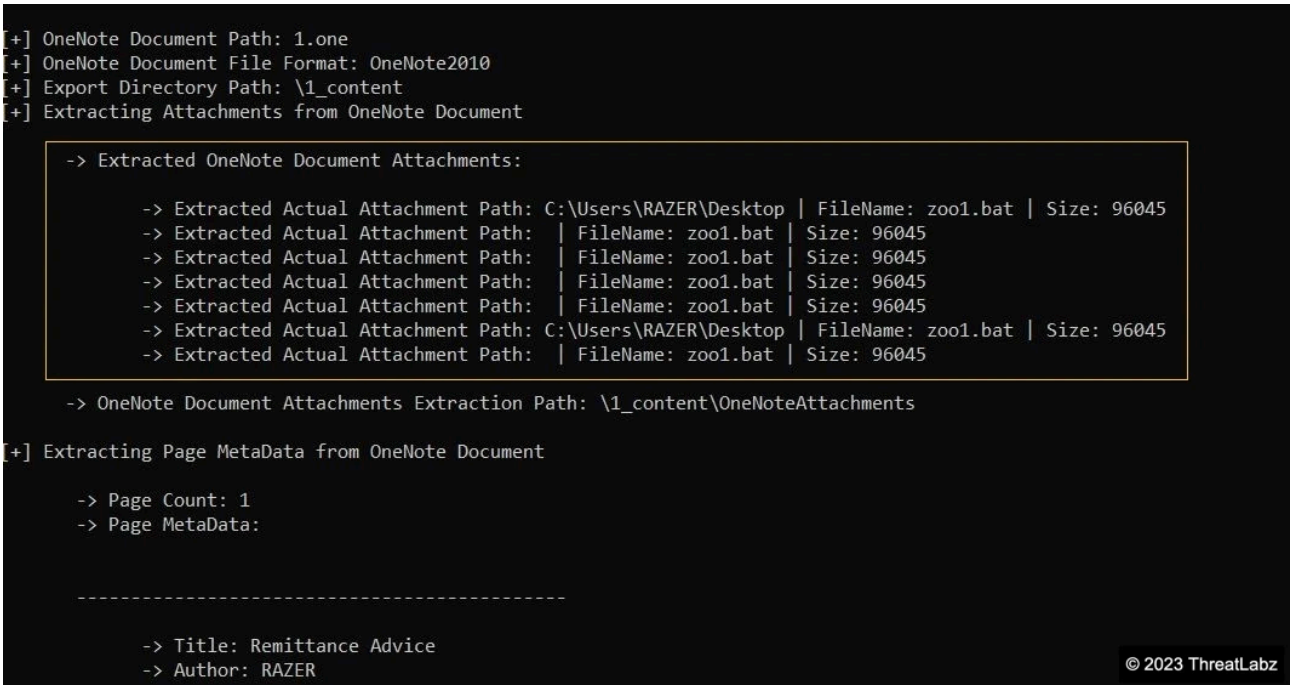

Fig.3 - Malicious files extracted from OneNote document

The batch file was obfuscated and contained an encrypted blob at the start, followed by heavily obfuscated PowerShell code.

Fig.4 - Obfuscated batch file

By removing the "**@echo off**" line and adding "**echo**" to the start of each line in the batch file, researchers were able to decode the file's activities and log the output as shown in the screenshot below.

*Fig.5 - Commands executed by "**zoo1.bat.exe**"*

The log indicated that the batch file had copied and disguised the malicious program as "**zoo1.bat.exe**" in an attempt to hide its activities.

The Powershell code associated with it was obfuscated and difficult to comprehend, so researchers manually pretty print to deobfuscate and reformat the file, making it more readable as demonstrated in the screenshot below.

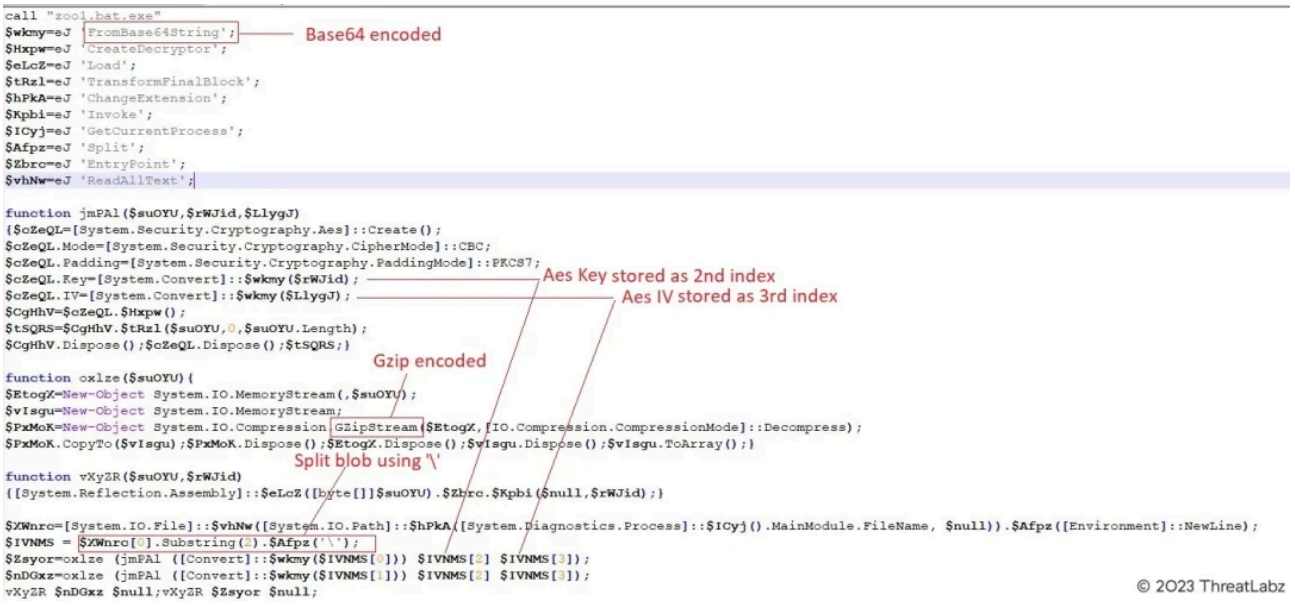

Fig.6 - Obfuscated Powershell code in readable format

After deobfuscation, researchers discovered that the script used base64 encoding to split the encrypted blob seen in the initial batch file into its actual data, AES key, and index using the backslash character. With these values, the script was able to decrypt the data and decode it using gzip encoding to reveal the final executable.

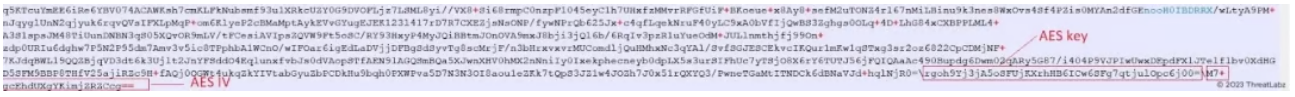

Fig.7 - AES Key and IV identified in the blob

Now lets the cook the above recipe using Cyberchef and check what does it results:

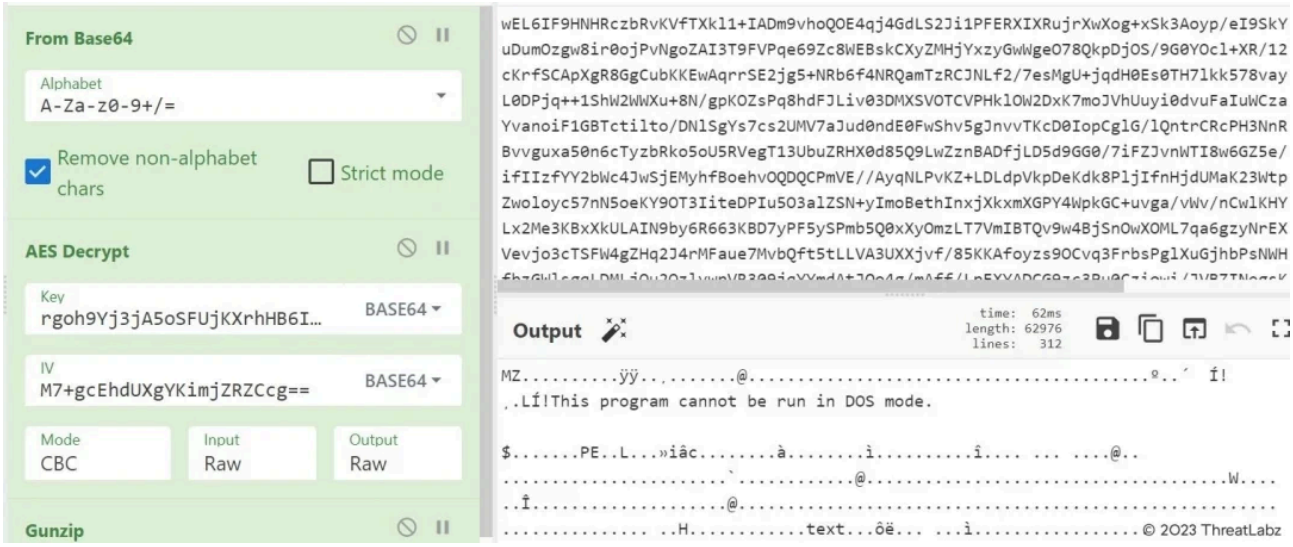

Fig.8 - Decrypted payload extracted using CyberChef

Similarly we can decode the second blob which will also result in a Portable Executable (PE) file.

Fig.9 - AgileDotNet Packed AsyncRAT Payload

The resulting file is a .NET File packed with AgileDotNet, which was revealed to contain a malicious AsyncRAT payload after deobfuscating and unpacking with the .NET Kali Linux tool known as de4dot.

Explore more Zscaler blogs

Source: https://www.zscaler.com/blogs/security-research/onenote-growing-threat-malware-distribution