EvilExtractor – All-in-One Stealer

fortinet.com/blog/threat-research/evil-extractor-all-in-one-stealer

April 20, 2023

FortiGuard Labs Threat Research

By Cara Lin | April 20, 2023

Affected platforms: Windows
Impacted parties: Any organization
Impact: Controls victim's device and collects sensitive information
Severity level: Critical

EvilExtractor (sometimes spelled Evil Extractor) is an attack tool designed to target Windows operating systems and extract data and files from endpoint devices. It includes several modules that all work via an FTP service. It was developed by a company named Kodex, which claims it is an educational tool. However, research conducted by FortiGuard Labs shows cybercriminals are actively using it as an info stealer.

Based on our traffic source data to the host, evilextractor[.]com, malicious activity increased significantly in March 2023. FortiGuard Labs observed this malware in a phishing email campaign on 30 March, which we traced back to the samples included in this blog. It usually pretends to be a legitimate file, such as an Adobe PDF or Dropbox file, but once loaded, it begins to leverage PowerShell malicious activities. It also contains environment checking and Anti-VM functions. Its primary purpose seems to be to steal browser data and information from compromised endpoints and then upload it to the attacker's FTP server.

We recently reviewed a version of the malware that was injected into a victim's system and, as part of that analysis, identified that most of its victims are located in Europe and America. The developer released its project in October 2022 (Figure 1) and has kept updating it to increase its stability and strengthen its module.

This article will examine the initial attack method used to deliver EvilExtractor and its functions.

Figure 1. EvilExtractor for sale on the web

Initial Access

The phishing email with the malicious attachment is shown in Figure 2. It is disguised as an account confirmation request. The attacker also tricks the victim by using an Adobe PDF icon for the decompressed file. The PE header is shown in Figure 3.

Figure 2. The phishing email

Figure 3. File header of "Account_Info.exe"

The execution file is a Python program packaged by PyInstaller. We extracted it with pyinstxtractor and found that the "PYARMOR" string in its main code file "contain.pyc", shown in Figure 4, is an obfuscating tool for Python script that makes the malware harder to be analyzed and detected. We extracted the key and iv from _pytransform.dll and decrypted the "contain.pyc" using AES-GCM.

Figure 4. Code in "contain.pyc"

In addition to the Python program, we observed a .NET loader that can extract EvilExtractor. Figure 5 is part of the code. It contains Base64-encoded data, which is a PowerShell script. This execution file is generated from the tool "PS2EXE-GUI", which can convert PowerShell scripts to EXE Files.

Figure 5. .Net Code for EvilExtractor

EvilExtractor

After decrypting the pyc file, we get the primary code of EvilExtractor. It is a PowerShell script that contains the following modules:

- Date time checking
- Anti-Sandbox
- Anti-VM
- Anti-Scanner
- FTP server setting
- Steal data
- Upload Stolen data
- Clear log

It first checks whether the system's date is between 2022-11-09 and 2023-04-12. If not, it uses the following command to delete the data in PSReadline and terminate:

```
DEL \"$env:APPDATA\Microsoft\Windows\PowerShell\PSReadline\*\" -Force –Recurse
```

It then compares the product model to see if it matches any of the following: VirtualBox, VMWare, Hyper-V, Parallels, Oracle VM VirtualBox, Citrix Hypervisor, QEMU, KVM, Proxmox VE, or Docker, as shown in Figure 6. It also checks the victim's hostname against 187 names from VirusTotal machines or other scanner/virtual machines, as shown in Figure 7.

Figure 6. EvilExtractor comparing product model for match

Figure 7. Virtual environment and scanner/virtual machine checking

After passing the environment check, EvilExtractor downloads three components from http://193[.]42[.]33[.]232 used for stealing data. These files are also Python programs that are obfuscated using PyArmor. The first is "KK2023.zip", which is used for stealing browser data and saving it in the folder "IMP_Data". It can extract cookies from Google Chrome, Microsoft Edge, Opera, and Firefox. It also collects browser history and passwords from the following browsers:

The second file is "Confirm.zip". It is a key logger that saves data in the "KeyLogs" folder. The last file, "MnMs.zip", is a webcam extractor. Its corresponding code is shown in Figure 8.

Figure 8. Download components for the Keylogger and Webcam Snapshot functions

EvilExtractor also collects system information by PowerShell script, shown in Figure 9. Figure 10 shows the concatenated data in a text file called "Credentials.txt".

Figure 9. PowerShell script for collecting system information

Figure 10. Content of “Credentials.txt”

EvilExtractor downloads files with specific extensions from the Desktop and Download folders, including jpg, png, jpeg, mp4, mpeg, mp3, avi, txt, rtf, xlsx, docx, pptx, pdf, rar, zip, 7z, csv, xml, and html. It also uses the command “CopyFromScreen” to capture a screenshot. The code is shown in Figure 11.

Figure 11. Downloading files and getting a screenshot

After EvilExtractor extracts all the data from the compromised endpoint, it uploads it to the attacker’s FTP server, shown in Figure 12. The developer of EvilExtractor also provides an FTP server for those who purchase its malware.

Figure 12. Upload file to attacker’s FTP server

Kodex Ransomware

EvilExtractor also has a ransomware function. It is called “Kodex Ransomware”, as shown in Figure 13. We extracted this PowerShell script from the .Net loader mentioned in the previous section, and the script for its ransomware is similar to the one for its stealer.

Figure 13. Introduction form evilextracom[.]com

It downloads “zzyy.zip” from evilextractor[.]com. Details of the unzipped file, a 7-zip standalone console, are shown in Figure 14. Figure 15 shows it leverages “7za.exe” to encrypt files with the parameter “-p”, which means zipping files with a password. It also generates a ransom-demanding message saved in “KodexRansom”, shown in Figure 16.

Figure 14. File in "zzyy.zip"

Figure 15. PowerShell script for Kodex Ransomware

Figure 16. Kodex ransomware's note

Conclusion

EvilExtractor is being used as a comprehensive info stealer with multiple malicious features, including ransomware. Its PowerShell script can elude detection in a .NET loader or PyArmor. Within a very short time, its developer has updated several functions and increased its stability. This blog explains how threat actors launch an attack via phishing mail and what files are leveraged to extract the EvilExtracrtor PowerShell script. We also detailed what functions are included, what data can be collected by EvilExtractor, and how the Kodex Ransomware works. Users should be aware of this new info stealer and continue to be cautious about suspicious mail.

Figure 17. Attack Chain

Fortinet Protections

The malware described in this report are detected and blocked by FortiGuard Antivirus as:

W32/EvilExtractor.A!tr
W32/Infostealer.A!tr
W32/Keylogger.A!tr

The FortiGuard AntiVirus service is supported by FortiGate, FortiMail, FortiClient, and FortiEDR, and the Fortinet AntiVirus engine is a part of each of those solutions. Customers running current AntiVirus updates are protected.

The FortiGuard Web Filtering Service blocks the malicious URL and IP address.

If you think this or any other cybersecurity threat has impacted your organization, contact our Global FortiGuard Incident Response Team.

IOCs

IP Address:

45[.]87[.]81[.]184
193[.]42[.]33[.]232

Files:

352efd1645982b8d23a841107007c8b4b024eb6bb5d6b312e5783ce4aa62b685
023548a5ce0de9f8b748a2fd8c4d1ae6c924c40acbde32e9599c868115d11f4e
75688c32a3c1f04df0fc02491180c8079d7fdc0babed981f5860f22f5e118a5e
826c7c112dd1ae80469ef81f5066003d7691a349e6234c8f8ca9637b0984fc45
b1ef1654839b73f03b73c4ef4e20ce4ecdef2236ec6e1ca36881438bc1758dcd
17672795fb0c8df81ab33f5403e0e8ed15f4b2ac1e8ac9fef1fec4928387a36d

Related Posts