Emansrepo Stealer: Multi-Vector Attack Chains

fortinet.com/blog/threat-research/emansrepo-stealer-multi-vector-attack-chains

September 3, 2024

Article Contents

By Pei Han Liao | September 03, 2024

Affected Platforms: Microsoft Windows
Impacted Users: Microsoft Windows
Impact: The stolen information can be used for future attack
Severity Level: High

In August 2024, FortiGuard Labs observed a python infostealer we call Emansrepo that is distributed via emails that include fake purchase orders and invoices. Emansrepo compresses data from the victim's browsers and files in specific paths into a zip file and sends it to the attacker's email. According to our research, this campaign has been ongoing since November 2023.

The attacker sent a phishing mail containing an HTML file, which was redirected to the download link for Emansrepo. This variant is packaged by PyInstaller so it can run on a computer without Python.

Figure 1: Attack flow in November 2023

Figure 2: The download link for Emansrepo is embedded in RTGS Invoices.html.
As time goes by, the attack flow has become increasingly complex. Below are the attack flows we found in July and August 2024:

Figure 3: Attack flow in August and July 2024
Various stages are being added to the attack flow before downloading Emansrepo, and multiple mailboxes are used to receive different kinds of stolen data. This article will provide a detailed analysis of each attack chain and its behavior. We will then provide a quick summary of the next campaign.

Attack Flow

Chain 1

Figure 4: The phishing mail in chain 1 contains a fake download page
The attachment is a dropper that mimics a download page. It creates a link element that points to the data of Purchase-Order.7z and uses the click() method to "download" Purchase-Order.7z. Six seconds later, it redirects to a completely unrelated website.

Figure 5: Source code of the attachment
Purchase-Order.exe, the file embedded in Purchase-Order.7z, is an AutoIt-compiled executable. It doesn't include any files, and the AutoIt script determines its behavior. The script has many unused functions, frustrating its analysis. The only meaningful code downloads preoffice.zip to the Temp folder and unzips it into % TEMP%\PythonTemp. The zip archive contains necessary Python modules and tester.py, the malicious script for information stealing.

Figure 6: The AutoIt script downloads the Python infostealer
Chain 2

Figure 7: The phishing mail in chain 2
The innermost file in P.O.7z is an HTA file. Its source file is a JavaScript file that shows a hidden window named PowerShell Script Runner and downloads the PowerShell script, script.ps1, with VBScript for the next stage.

Figure 8: The decryption algorithm of the JavaScript file and the result
The behavior of script.ps1 is similar to the AutoIt script in chain 1. It downloads preoffice.zip to the Temp folder and unzips it to %TEMP%\PythonTemp, but it executes Emansrepo using run.bat.

Figure 9: script.ps1 executes run.bat to run the infostealer
Chain 3

Figure 10: The phishing mail in chain 3
The 7z file from the link in the phishing mail contains a batch file obfuscated by BatchShield.

Figure 11: The obfuscated batch file
After deobfuscation, we can see that it is not as complicated as it first seems. It simply downloads and executes script.ps1 using PowerShell.

Figure 12: The deobfuscated batch file

Python Infostealer

According to the email receiving the data, the infostealer behavior can be divided into three parts. It creates folders to temporarily store the stolen data for each part and deletes them after sending the data to the attacker. The stolen data is attached to the email sent to the attacker.

Part 1 – User information and text files

In part 1, the Python stealer collects login data, credit card information, web history, download history, autofill, and text files (less than 0.2 MB) from the Desktop, Document, and Downloads folders.

Sender	minesmtp8714@maternamedical[.]top
Receiver	minestealer8412@maternamedical[.]top
Target	**Browsers** amigo, torch, kometa, orbitum, cent-browser, 7star, sputnik, vivaldi, google-chrome-sxs, google-chrome, epic-privacy-browser, microsoft-edge, uran, yandex, brave, iridium
Folder and files	**%TEMP%\Browsers:** Text files (less than 0.2 MB) copied from Desktop, Document, Downloads **%TEMP%\Browsers\{browser name}:** Saved_Passwords.txt, Saved_Credit_Cards.txt, Browser_History.txt, Download_History.txt, Autofill_Data.txt
Attachment	Zip file of **%TEMP%\Browsers** folder

Part 1 includes the initial features of Emansrepo since there is only code for part 1 in the November 2023 variant (e346f6b36569d7b8c52a55403a6b78ae0ed15c0aaae4011490404bdb04ff28e5). It’s worth noting that *emans841 report* has been used as the divider in Saved_Passwords.txt since the December 2023 variant (ae2a5a02d0ef173b1d38a26c5a88b796f4ee2e8f36ee00931c468cd496fb2b5a). Because of this, we call it Emansrepo.

Figure 13: The content of Saved_Passwords.txt
The variant used in November 2023 uses *Prysmax Premium* as the divider.

By comparing the variant in November 2023 with the first edition of the Prysmax stealer shared on GitHub, we find they contain many similar functions, though the Emansrepo stealer had fewer features. However, as parts 2 and 3 were added to Emansrepo, it has become quite different from the Prysmax stealer.

Figure 14: Left: Variant in November 2023. Right: First edition of Prysmax Stealer on GitHub

Part2 – PDF files, extensions, crypto wallets, and game platform

Part 2 copies PDF files (less than 0.1 MB) from the Desktop, Document, Downloads, and Recents folders and compresses folders of browser extensions, crypto wallets, and game platforms into zip files.

Sender	extensionsmtp@maternamedical[.]top
Receiver	filelogs@maternamedical[.]top
Target	**Browsers** Opera, Chrome, Brave, Vivaldi, Yandex, Edge **Crypto wallet** Atomic Wallet, Guarda, Zcash, Armory, Bytecoin, Exodus, Binance, Electrum, Coinomi, jaxx **Game platform** Steam, Riot Games **Browser extension** MetaMask, BNB Chain Wallet, Coinbase Wallet, Ronin Wallet, Trust Wallet, Venom Wallet, Sui Wallet, Martian Aptos & Sui Wallet, TronLink, Petra Aptos Wallet, Pontem Crypto Wallet, Fewcha Move Wallet, Math Wallet, Coin98 Wallet, Authenticator, Exodus Web3 Wallet, Phantom, Core | Crypto Wallet & NFT, TokenPocket - Web3 & Nostr Wallet, SafePal Extension Wallet, Solflare Wallet, Kaikas, iWallet, Yoroi, Guarda, Jaxx Liberty, Wombat, Oxygen - Atomic Crypto Wallet, MEW CX, GuildWallet, Saturn Wallet, Station Wallet, Harmony, EVER Wallet, KardiaChain Wallet, Pali Wallet, BOLT X, Liquality Wallet, XDEFI Wallet, Nami, MultiversX Wallet, Temple - Tezos Wallet, XMR.PT
Folder and files in temp folder	**%TEMP%\pdf_temps:** • PDF files (less than 0.1 MB) copied from Desktop, Document, Downloads and Recents folder • {extension ID}.zip • {data folder}.zip
Attachment	All files in pdf_temp

Part 3 – Cookies

Part 3 copies cookie files and zips it into {process_name}_cookies.zip.

Sender	cookiesmtp@maternamedical[.]top
Receiver	cooklielogs@maternamedical[.]top
Target	**Browsers** Chrome, msedge, brave, opera, 360se, 360browser, yandex, UCBrowser, QQBrowser
Folder and files in temp folder	**%TEMP%\cookies_data:** {process_name}_cookies.zip
Zip file	Zip files in cookies_data

New Campaign

We recently found another attack campaign using the Remcos malware, which we believe is related to the same attacker because of the phishing email.

Figure 15: Left: the email for the Python infostealer. Right: The email for Remcos.
As the above screenshot shows, these attacks have the same content but use different methods to distribute malware. The attack flow for Remcos is much simpler. The attacker just sends phishing emails with a malicious attachment. The attachment is a DBatLoader, which downloads and decrypts data for the payload. The payload is a Remcos protected by a packer.

Figure 16: Attack flow of new Remcos campaign

Conclusion

Emansrepo has been active since at least last November, and the attack method is continuously evolving. The attack vectors and malware are ever-changing and pervasive, so it’s vital for organizations to maintain cybersecurity awareness. FortiGuard will continue monitoring these attack campaigns and providing appropriate protections as required.

Fortinet Protections

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

W32/Kryptik.EB!tr
JS/Agent.FEI!tr
BAT/Downloader.2C22!tr

FortiGate, FortiMail, FortiClient, and FortiEDR support the FortiGuard AntiVirus service. The FortiGuard AntiVirus engine is part of each solution. As a result, customers who have these products with up-to-date protections are already protected.

The FortiGuard CDR (content disarm and reconstruction) service can disarm the embedded link object inside the Excel document.

To stay informed of new and emerging threats, you can sign up to receive future alerts.

We also suggest our readers go through the free Fortinet Cybersecurity Fundamentals (FCF) training, a module on Internet threats designed to help end users learn how to identify and protect themselves from phishing attacks.

FortiGuard IP Reputation and Anti-Botnet Security Service proactively block these attacks by aggregating malicious source IP data from the Fortinet distributed network of threat sensors, CERTs, MITRE, cooperative competitors, and other global sources that collaborate to provide up-to-date threat intelligence about hostile sources.

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

IOCs

Address

hxxps://bafybeigm3wrvmyw5de667rzdgdnct2fvwumyf6zyzybzh3tqvv5jhlx2ta[.]ipfs[.]dweb[.]link/wetrankfr[.]zip
hxxps://bafybeifhhbimsau6a6x4m2ghdmzer5c3ixfztpocqqudlo4oyzer224q4y[.]ipfs[.]w3s[.]link/myscr649612[.]js
https://estanciaferreira[.]com[.]br/wp-includes/TIANJIN-DOC-05082024-xls[.]7z
hxxps://dasmake[.]top/reader/timer[.]php
hxxps://hedam[.]shop/simple/Enquiry.7z
191[.]101[.]130[.]185
192[.]236[.]232[.]35

Email address

stealsmtp@dasmake[.]xyz
hanbox@dasmake[.]xyz
publicsmtp@dasmake[.]xyz
publicbox@dasmake[.]xyz
minesmtp8714@dasmake[.]xyz
minestealer8412@dasmake.xyz
minesmtp8714@maternamedical[.]top
minestealer8412@maternamedical[.]top
extensionsmtp@maternamedical[.]top
filelogs@maternamedical[.]top
cookiesmtp@maternamedical[.]top
cooklielogs@maternamedical[.]top

Phishing mail

a6c2df5df1253f50bd49e7083fef6cdac544d97db4a6c9c30d7852c4fd651921
9e5580d7c3c22e37b589ec8eea2dae423c8e63f8f666c83edabecf70a0948b99
9bd3b8d9ac6ad680b0d0e39b82a439feedd87b9af580f37fa3d80d2c252fef8c
915bad0e2dbe0a18423c046f84d0ff7232fff4e5ba255cc710783f6e4929ab32

64e5c9e7b8dfb8ca8ca73895aa51e585fa7e5414f0e1d10659d3a83b9f770333

b343cce5381b8633b3fd3da56698f60db70c75422e120235a00517d519e37d8d

32bcbce53bfee33112b447340e7114d6d46be4ccf1a5391ad685431afdc8fb86

Delivery

bee8da411e71547ac765a5e63e177b59582df438432cc3b540b57a6f1a56dd16

70ba3d67b476e98419ecbbbb5d81efcb5a07f55a92c96e7b9207176746e3b7a6

a2fa6790035c7af64146158f1ed20cb54f4589783e1f260a5d8e4f30b81df70d

4cd8c9fa7f5e2484b73ed9c7be55aa859969c3f21ca2834610102231d337841d

6670e5c7521966e82d091e7adff4e16335f03f2e2740b653adcc9bfe35c7bf9b

dd656953a6844dd9585f05545a513c4e8c2ded13e06cdb67a0e58eda7575a7a4

9866934dd2b4e411cdabaa7a96a63f153921a6489f01b0b40d7febed48b02c22

Malware

e346f6b36569d7b8c52a55403a6b78ae0ed15c0aaae4011490404bdb04ff28e5

8e43c97e5bc62211b3673dee13e376a1f5026502ebe9fd9f7f455dc17c253b7f

ae2a5a02d0ef173b1d38a26c5a88b796f4ee2e8f36ee00931c468cd496fb2b5a

7a9826be22b6d977d6a0e5179f84d8e88b279fe6d9df8f6c93ebc40a6ba70f06

18459be33cd4f59081098435a0fbaa649f301f985647a75d21b7fc337378e59b

6e7313b6aa37a00b602e620a25a0b71a74503ea967f1814c6c7b8b192535a043

222dd76c461e70c3cb330bacfcf465751b07331c4f8a4415c09f4cd7c4e6fcd9

6e7313b6aa37a00b602e620a25a0b71a74503ea967f1814c6c7b8b192535a043