APT Group DarkPink Exploits WinRAR 0-Day to Target Multiple Entities in Vietnam and Malaysia

10/13/2023

Overview

NSFOCUS Security Labs has been continuously monitoring the newly discovered WinRAR 0-day vulnerability, CVE-2023-38831. It has come to our attention that the advanced persistent threat group known as DarkPink has recently begun exploiting this vulnerability to target government entities in Vietnam and Malaysia.

In this round of attack activities, DarkPink attackers have incorporated the CVE-2023-38831 vulnerability into their existing attack processes, making several enhancements to their attack tactics, which has significantly increased their success rate.

This report will analyze DarkPink's enhanced attack process and tactics.

Introduction to DarkPink

DarkPink, also known as Saaiwc, is a newly identified APT group confirmed in January 2023. The organization initially became active in mid-2021 and primarily targets entities in the Asia-Pacific region. Their main targets include diplomatic, military, and various industries in countries such as Cambodia, Indonesia, Malaysia, the Philippines, Vietnam, Bosnia and Herzegovina, and others. DarkPink's primary method of attack involves spear-phishing, delivering their homemade Trojan programs, TelePowerBot and KamiKakaBot, through email to conduct network espionage activities.

Baits Used by DarkPink

In this recent cyberattack campaign, DarkPink employed various baits, all in the form of PDF files, which were placed within WinRAR vulnerability files to entice users to open and view them. One of these baits is named "VanBanGoc_2023.07.10. TT 03 FINAL", a legal document bearing the letterhead of the Vietnamese Ministry of Foreign Affairs, as shown in the figure below:

BỘ NGOẠI GIAO

Số: 03 /2023/TT-BNG

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM

Độc lập - Tự do - Hạnh phúc

Hà Nội, ngày 27 tháng 7 năm 2023

THÔNG TƯ

Về việc tổ chức giải quyết công tác lãnh sự

Căn cứ Luật Cơ quan đại diện nước Cộng hòa xã hội chủ nghĩa Việt Nam ở nước ngoài số 33/2009/QH12 ngày 18/6/2009;

Căn cứ Luật sửa đổi, bổ sung một số điều của Luật Cơ quan đại diện nước Cộng hòa xã hội chủ nghĩa Việt Nam ở nước ngoài số 19/2017/QH14 ngày 21/11/2017;

Căn cứ Luật Ban hành văn bản quy phạm pháp luật số 80/2015/QH13 ngày 22/6/2015; Luật sửa đổi, bổ sung một số điều của Luật Ban hành văn bản quy phạm pháp luật số 63/2020/QH14 ngày 18/6/2020;

Căn cứ Nghị định số 81/2022/NĐ-CP ngày 14/10/2022 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Ngoại giao;

Theo đề nghị của Cục trưởng Cục Lãnh sự,

Bộ trưởng Bộ Ngoại giao ban hành Thông tư hướng dẫn việc tổ chức giải quyết công tác lãnh sự.

CHƯƠNG I

CÁC QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh và đối tượng áp dụng

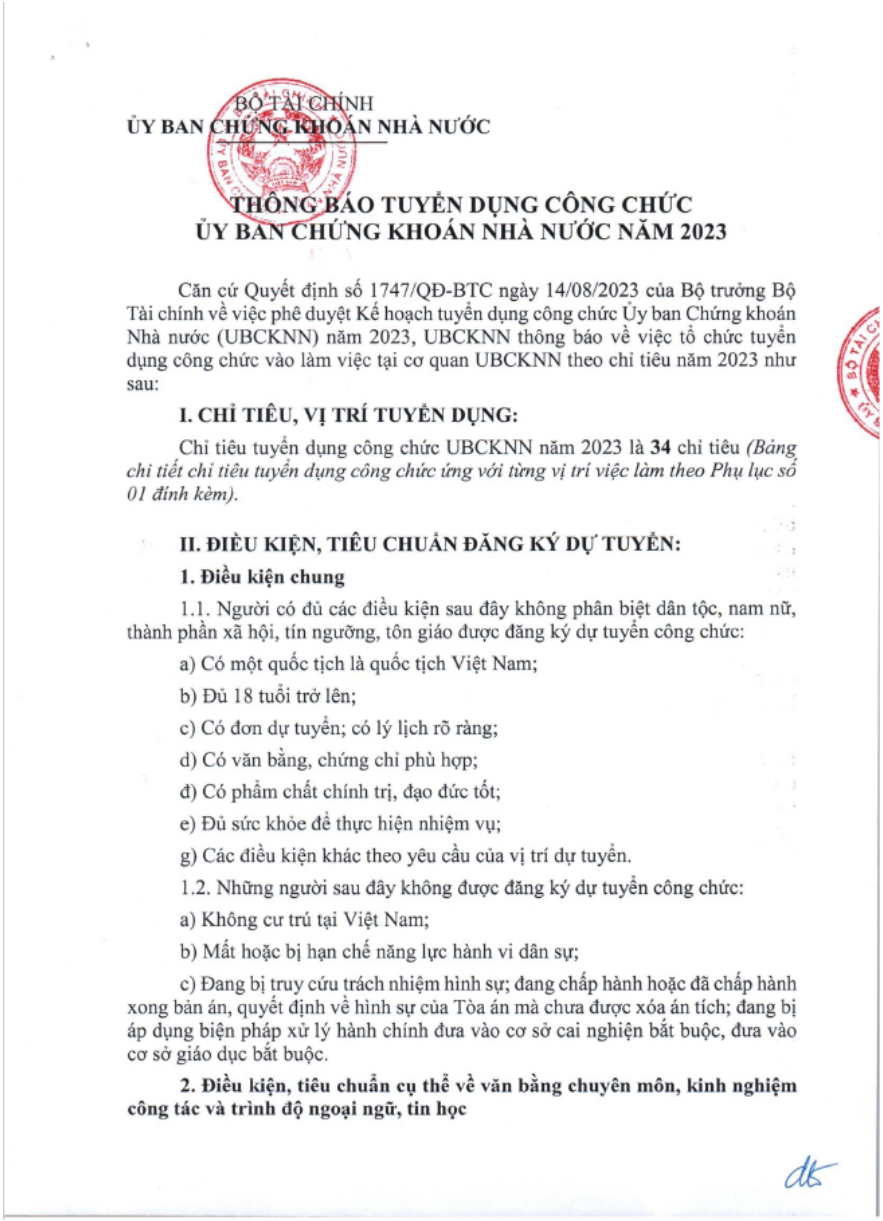
1. Thông tư này quy định việc tổ chức giải quyết công tác lãnh sự tại Cục Lãnh sự, Sở Ngoại vụ Thành phố Hồ Chí Minh, Văn phòng Bộ và các Cơ quan đại diện ngoại giao, cơ quan đại diện lãnh sự, cơ quan khác được uỷ quyền thực hiện chức năng lãnh sự của Việt Nam ở nước ngoài (sau đây gọi là Cơ quan đại diện).

2. Thông tư này áp dụng đối với đơn vị, cá nhân thực hiện công tác lãnh sự tại Bộ Ngoại giao và tại Cơ quan đại diện.

1

Figure 3.1 The bait file “VanBanGoc_2023.07.10. TT 03 FINAL”

Another bait is named “Ủy ban Chứng khoán Nhà nước thông báo tuyển dụng công chức năm 2023” (Announcement from the State Securities Commission for the recruitment of civil servants in 2023). This file originates from the State Securities Commission of Vietnam, as shown in the figure below:



BỘ TÀI CHÍNH
ỦY BAN CHỨNG KHOÁN NHÀ NƯỚC

THÔNG BÁO TUYỂN DỤNG CÔNG CHỨC
ỦY BAN CHỨNG KHOÁN NHÀ NƯỚC NĂM 2023

Căn cứ Quyết định số 1747/QĐ-BTC ngày 14/08/2023 của Bộ trưởng Bộ Tài chính về việc phê duyệt Kế hoạch tuyển dụng công chức Ủy ban Chứng khoán Nhà nước (UBCKNN) năm 2023, UBCKNN thông báo về việc tổ chức tuyển dụng công chức vào làm việc tại cơ quan UBCKNN theo chỉ tiêu năm 2023 như sau:

I. CHỈ TIÊU, VỊ TRÍ TUYỂN DỤNG:

Chỉ tiêu tuyển dụng công chức UBCKNN năm 2023 là **34** chỉ tiêu *(Bảng chi tiết chỉ tiêu tuyển dụng công chức ứng với từng vị trí việc làm theo Phụ lục số 01 đính kèm).*

II. ĐIỀU KIỆN, TIÊU CHUẨN ĐĂNG KÝ DỰ TUYỂN:

1. Điều kiện chung

1.1. Người có đủ các điều kiện sau đây không phân biệt dân tộc, nam nữ, thành phần xã hội, tín ngưỡng, tôn giáo được đăng ký dự tuyển công chức:

a) Có một quốc tịch là quốc tịch Việt Nam;

b) Đủ 18 tuổi trở lên;

c) Có đơn dự tuyển; có lý lịch rõ ràng;

d) Có văn bằng, chứng chỉ phù hợp;

đ) Có phẩm chất chính trị, đạo đức tốt;

e) Đủ sức khỏe để thực hiện nhiệm vụ;

g) Các điều kiện khác theo yêu cầu của vị trí dự tuyển.

1.2. Những người sau đây không được đăng ký dự tuyển công chức:

a) Không cư trú tại Việt Nam;

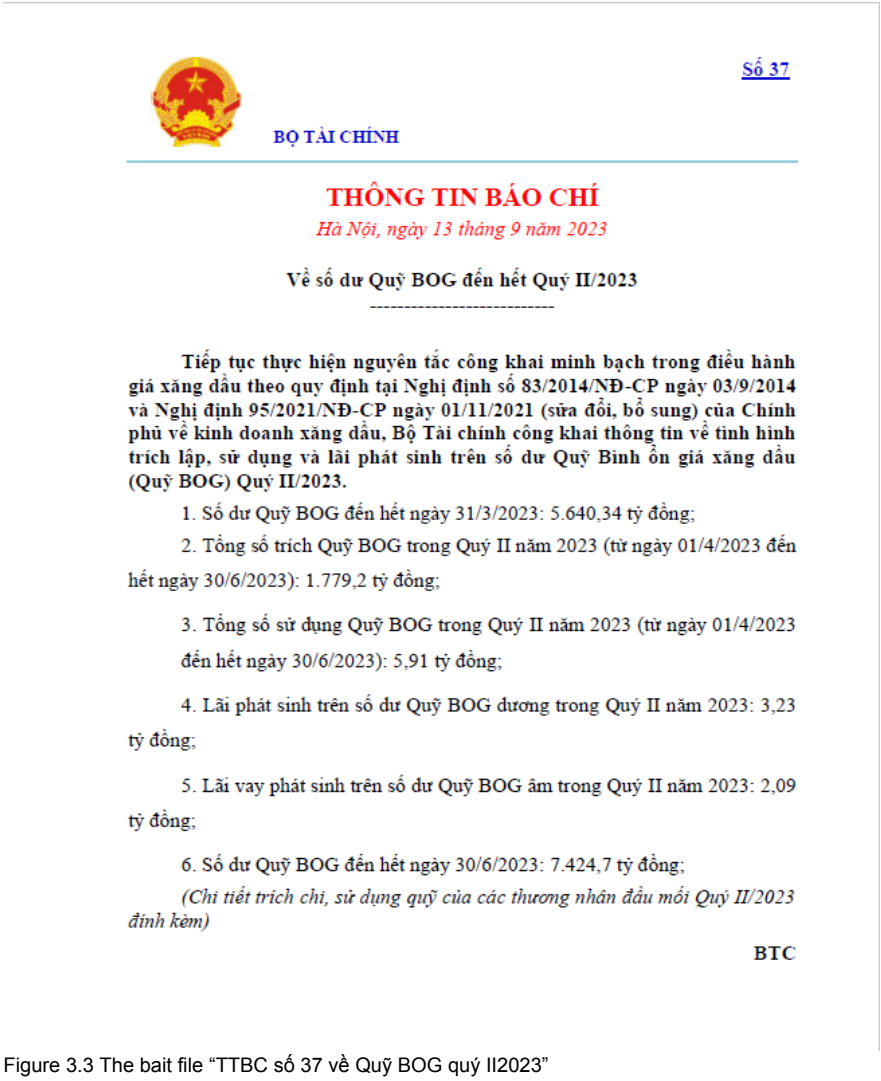
b) Mất hoặc bị hạn chế năng lực hành vi dân sự;

c) Đang bị truy cứu trách nhiệm hình sự; đang chấp hành hoặc đã chấp hành xong bản án, quyết định về hình sự của Tòa án mà chưa được xóa án tích; đang bị áp dụng biện pháp xử lý hành chính đưa vào cơ sở cai nghiện bắt buộc, đưa vào cơ sở giáo dục bắt buộc.

2. Điều kiện, tiêu chuẩn cụ thể về văn bằng chuyên môn, kinh nghiệm công tác và trình độ ngoại ngữ, tin học

Figure 3.2 The bait file “Ủy ban Chứng khoán Nhà nước thông báo tuyển dụng công chức năm 2023”

Another bait is named “TTBC số 37 về Quỹ BOG quý II2023” (Document No. 37 regarding the BOG Fund in the second quarter of 2023). This document is news information released by the Ministry of Finance of Vietnam regarding the Petroleum Price Stabilization Fund (BOG), as shown below:



Số 37

BỘ TÀI CHÍNH

THÔNG TIN BÁO CHÍ

Hà Nội, ngày 13 tháng 9 năm 2023

Về số dư Quỹ BOG đến hết Quý II/2023

Tiếp tục thực hiện nguyên tắc công khai minh bạch trong điều hành giá xăng dầu theo quy định tại Nghị định số 83/2014/NĐ-CP ngày 03/9/2014 và Nghị định 95/2021/NĐ-CP ngày 01/11/2021 (sửa đổi, bổ sung) của Chính phủ về kinh doanh xăng dầu, Bộ Tài chính công khai thông tin về tình hình trích lập, sử dụng và lãi phát sinh trên số dư Quỹ Bình ổn giá xăng dầu (Quỹ BOG) Quý II/2023.

1. Số dư Quỹ BOG đến hết ngày 31/3/2023: 5.640,34 tỷ đồng;

2. Tổng số trích Quỹ BOG trong Quý II năm 2023 (từ ngày 01/4/2023 đến hết ngày 30/6/2023): 1.779,2 tỷ đồng;

3. Tổng số sử dụng Quỹ BOG trong Quý II năm 2023 (từ ngày 01/4/2023 đến hết ngày 30/6/2023): 5,91 tỷ đồng;

4. Lãi phát sinh trên số dư Quỹ BOG dương trong Quý II năm 2023: 3,23 tỷ đồng;

5. Lãi vay phát sinh trên số dư Quỹ BOG âm trong Quý II năm 2023: 2,09 tỷ đồng;

6. Số dư Quỹ BOG đến hết ngày 30/6/2023: 7.424,7 tỷ đồng;

(Chi tiết trích chi, sử dụng quỹ của các thương nhân đầu mối Quý II/2023 đính kèm)

BTC

Figure 3.3 The bait file “TTBC số 37 về Quỹ BOG quý II2023”

There is another bait file named ‘Keputusan Permohonan Mendapatkan Perkhidmatan Penceramah Luar Untuk Program Anjuran Kementerian Pertahanan’ (Decision on the Application to Obtain External Speaker Services for the Ministry of Defence’s Organized Program). This is also a government document with the letterhead of the Department of Strategic Planning and Policy of the Malaysian Ministry of Defence, as shown in the figure below:

MEMO
BAHAGIAN DASAR DAN PERANCANGAN STRATEGIK
KEMENTERIAN PERTAHANAN

Ruj. Kami: MOD.500-6/1/2 JLD.62 (32) Tarikh : 1 Jun 2023
Ruj. Tuan: Tel. : 03-40125010

TAJUK	**KEPUTUSAN PERMOHONAN MENDAPATKAN PERKHIDMATAN PENCERAMAH LUAR UNTUK PROGRAM ANJURAN KEMENTERIAN PERTAHANAN** **BILANGAN 6 TAHUN 2023**	
DARIPADA	**KPSU (P)**	Salinan: Fail
KEPADA	**Seperti Senarai Edaran**	

Dengan hormatnya saya diarah merujuk perkara tersebut di atas.

2. Dimaklumkan bahawa, keputusan permohonan mendapatkan perkhidmatan penceramah luar yang dikemukakan oleh pihak tuan/puan adalah seperti di **Lampiran A**.

3. Sehubungan itu, kerjasama pihak tuan/puan adalah dipohon untuk:

i. Memaklumkan kepada penceramah bahawa sesi ceramah mereka akan dirakam; dan
ii. Rakaman sesi ceramah akan digunakan untuk ulangan/pembelajaran kendiri/secara atas talian.

Sekian, terima kasih.

"MALAYSIA MADANI"
"BERKHIDMAT UNTUK NEGARA"
"PERTAHANAN NEGARA TANGGUNGJAWAB BERSAMA"

Saya yang menjalankan amanah,

b/p

(EDDY SAHRIZAN BIN RUSLI)

Figure 3.4 The bait file "Keputusan Permohonan Mendapatkan Perkhidmatan Penceramah Luar Untuk Program Anjuran Kementerian Pertahanan"

It's evident that the primary targets of DarkPink's current attack campaign are the governments of Vietnam and Malaysia. The bait files used in this campaign follow the group's consistent approach of using genuine-looking government documents to enhance the deception of the baits. Coupled with the newly used WinRAR vulnerability exploitation, this makes it difficult for victims to detect that they have fallen victim to an attack.

Attack Process of DarkPink in this Campaign

In this campaign, DarkPink employed an enhanced process that combines their classic attack methodology with the exploitation of the CVE-2023-38831 vulnerability, as shown below:

Figure 4,1 Main attack process of DarkPink in this campaign

Vulnerability Exploitation Phase

The CVE-2023-38831 vulnerability exploitation file constructed by DarkPink is as follows, including a PDF bait file and a folder with the same name:

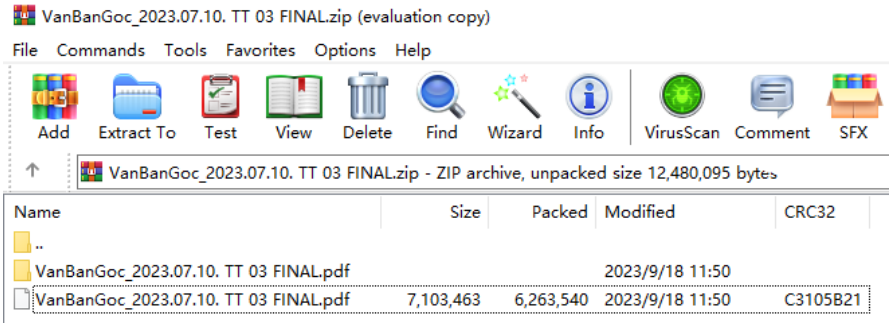


Figure 4.2 Vulnerability exploitation file constructed by DarkPink

Inside the folder, there are two files: one is an exe program with the same name as the PDF bait file, and the other is a library file named 'twinapi.dll':

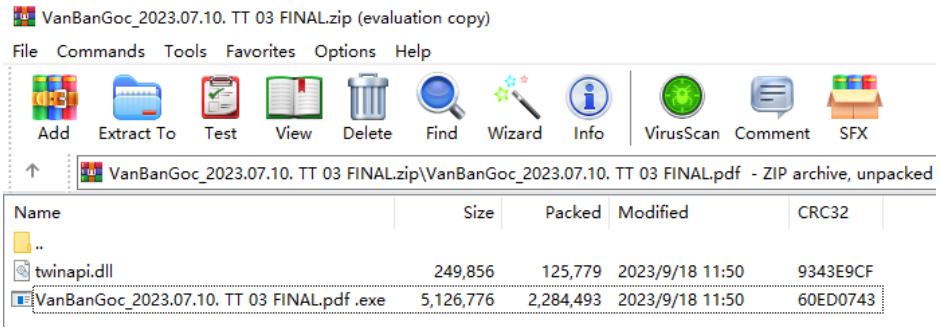


Figure 4.3 Contents of the folder within the vulnerability exploitation file

When a user attempts to open the PDF bait file in a lower version of WinRAR, the CVE-2023-38831 vulnerability exploitation is triggered, leading to the execution of the exe program within the folder.

Trojan Deployment Phase

In fact, the exe program executed when triggered by CVE-2023-38831 is the Windows system application explorer.exe. During its execution, it attempts to load the twinapi.dll file located in the same directory, creating a side-loading exploitation attack pattern.

The twinapi.dll is a loader-type Trojan specially developed by DarkPink for this campaign. The main function of this Trojan is to extract a portion of data from the PDF bait file, decrypt one of the embedded PE files, and inject it into the parent process.

```
*(_QWORD *)((char *)vkey + 7) = 0x88059BA565346124ui64;// 4d 1d 15 24 12 0d 8c 24 61 34 65 a5 9b 05 88
*vkey = 0x248C0D1224151D4Di64;
v26 = 1i64;
for ( i = 0i64; i != 0x5C200; i += 2i64 )
{
  *((_BYTE *)vbuf + i) ^= *((_BYTE *)vkey + 0xFFFFFFF1 * (i / 0xF) + i);
  *((_BYTE *)vbuf + i + 1) ^= *((_BYTE *)vkey + 0xFFFFFFF1 * (v26 / 0xF) + i + 1);
  v26 += 2i64;
}
```

Figure 4.4 XOR Decryption Logic in the Loader Trojan

The loaded PE file is DarkPink's typical loader-type Trojan program, TelePowerDropper, which ultimately implants the remote control Trojan program, TelePowerBot, on the victim's host.

Analysis of Techniques and Tactics Used by DarkPink

Given that in this campaign DarkPink has continued to employ its previously used attack approach, this report will focus on the techniques and tactics that have been newly added or modified by the APT group this time.

Execution – User Execution – Malicious File

CVE-2023-38831 Exploitation

In this attack campaign, the most significant change in DarkPink's tactics and techniques is the transformation of the initial malicious file into a CVE-2023-38831 vulnerability exploitation file.

In previous attack campaigns, DarkPink attackers used ISO files as the initial bait, hoping that victims would directly run the executable file with a disguised filename after opening the ISO file, thereby triggering the entire execution process. A typical bait used by DarkPink in previous attack campaigns is shown in the figure below:

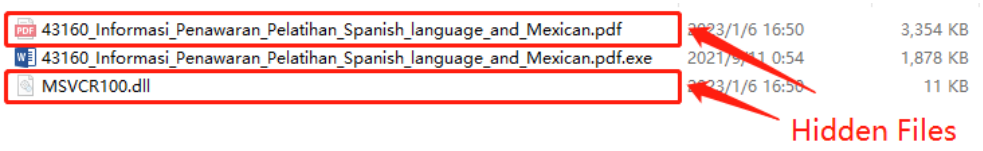


Figure 5.1 Typical bait file used by DarkPink in previous attack campaigns

This is a classic method of disguised execution, but its drawback lies in exposing the executable file extension, making it challenging to deceive vigilant victims.

In this attack campaign, the CVE-2023-38831 vulnerability significantly enhances the deception of the initial malicious file. Victims trigger the attack process when viewing the malicious file with WinRAR software, as shown in the figure below.

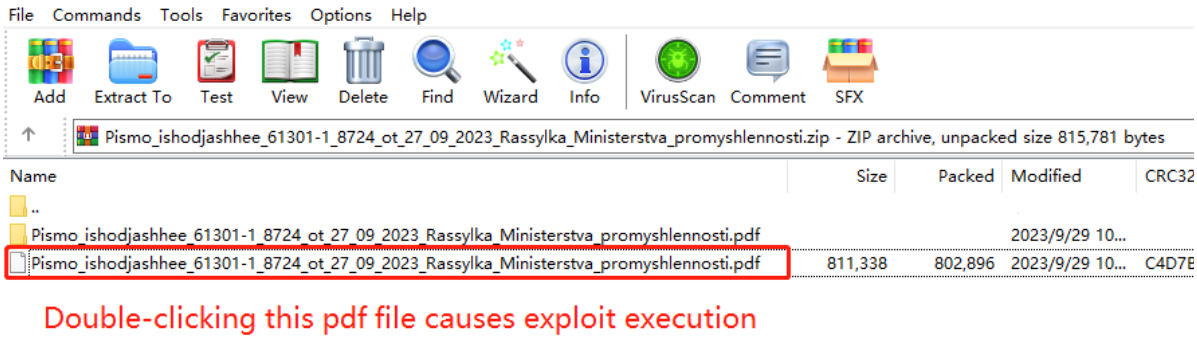


Figure 5.2 Vulnerability exploitation bait used by DarkPink in this campaign

Unless they have a certain understanding of this vulnerability, victims have almost no defense against this attack method, greatly increasing DarkPink's success rate in this campaign.

Persistence – Event Triggered Execution – Changing Default File Association

Malicious code triggered by amv files

In this attack campaign, DarkPink attackers gained the ability to run malicious cmd commands stably on the victim's host by modifying the default opening method for specific files. The specific implementation of this technique involves two steps.

First, DarkPink's TelePowerDropper Trojan creates the following set of registry entries:

REG_openkey	HKEY_CURRENT_USER
REG_openkey	HKEY_CURRENT_USER\Environment
REG_setval	HKEY_CURRENT_USER\Environment\TKS
REG_setval	HKEY_CURRENT_USER\Environment\IDS
REG_mkkey	HKEY_CURRENT_USER\Software\Classes\.amv
REG_mkkey	HKEY_CURRENT_USER\Software\Classes\.amv
REG_setval	HKEY_CURRENT_USER\Software\Classes\.amv\
REG_mkkey	HKEY_CURRENT_USER\Software\Classes\amvfile\shell\open\command
REG_mkkey	HKEY_CURRENT_USER\Software\Classes\amvfile\shell\open\command
REG_mkkey	HKEY_CURRENT_USER\SOFTWARE
REG_mkkey	HKEY_CURRENT_USER\Software\Classes
REG_mkkey	HKEY_CURRENT_USER\Software\Classes\amvfile
REG_mkkey	HKEY_CURRENT_USER\Software\Classes\amvfile\shell
REG_mkkey	HKEY_CURRENT_USER\Software\Classes\amvfile\shell\open
REG_mkkey	HKEY_CURRENT_USER\Software\Classes\amvfile\shell\open\command
REG_setval	HKEY_CURRENT_USER\Software\Classes\amvfile\shell\open\command\
REG_setval	HKEY_CURRENT_USER\Software\Classes\amvfile\shell\open\command\amv
REG_setval	HKEY_CURRENT_USER\Software\Classes\amvfile\shell\open\command\DelegateExecute

Figure 5.3 Registry entries created by TelePowerDropper

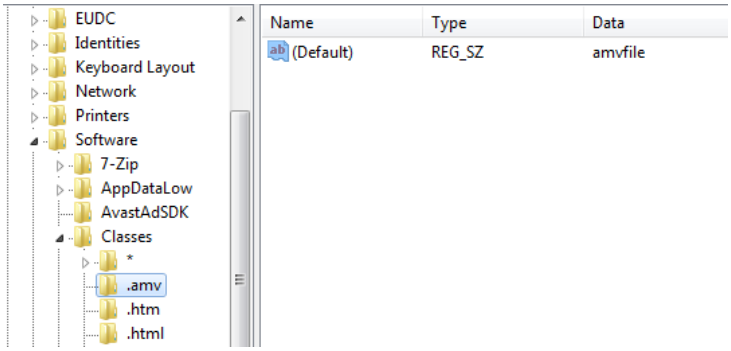


Figure 5.4 Figure 1.1 Registry key values set by TelePowerDropper (A)

With this configuration, when Windows attempts to open .amv files, it triggers the malicious code in the registry entries (See the abuse of DelegateExecute in the next section for the triggering method).

In the second step, the TelePowerDropper Trojan creates an empty file named 'Tsys.amv' in the system's Startup directory. This way, when the system starts up, it attempts to open this .amv file, triggering the subsequent execution process of the TelePowerBot Trojan.

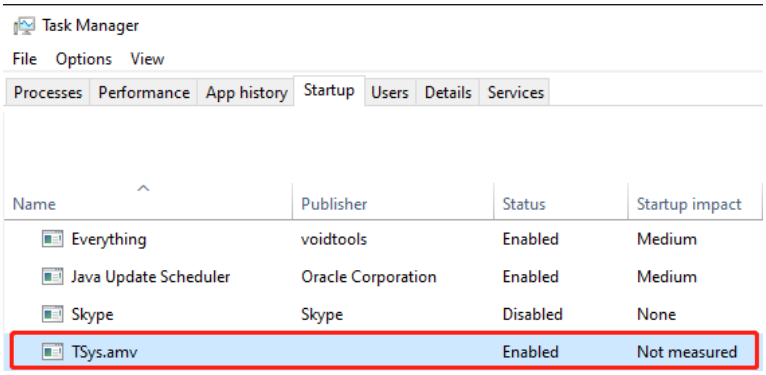


Figure 5.5 Startup items set by TelePowerDropper

Compared to previous attack processes, the enhancements in this campaign primarily focus on two key aspects.

Firstly, DarkPink changed the file type for the execution trigger from '.abcd' to '.amv,' reducing the likelihood of discovering DarkPink attack traces through a file extension search. Secondly, the improvement is seen in the specific triggering method, where DarkPink directly sets the startup file to trigger the execution instead of the previous method of writing cmd code in the registry's UserInitMprLogonScript entry. This change also reduces the likelihood of discovering DarkPink attack traces by searching specific registry entries.

The enhancements to this attack technique aim to remove the characteristics of the technique exposed previously.

Defense Evasion – File or Information Obfuscation – Command Obfuscation

Splitting Registry Key Values

Another improvement by DarkPink in this campaign involves UAC bypass and Windows Defender evasion through the use of the DelegateExecute logic in the registry.

The TelePowerDropper Trojan used by DarkPink in this campaign creates the following registry key values under "HKEY_CURRENT_USER\Software\Classes\amvfile\shell\open\command\".

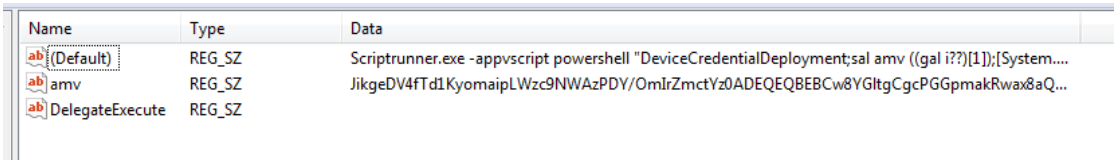


Figure 5.6 Registry key values set by TelePowerDropper (B)

The key difference in the key values written by the new TelePowerDropper Trojan in this campaign is the splitting of the malicious code that was originally all written into the Default value, and the use of Scriptrunner.exe as the launcher.

Additionally, the TelePowerDropper Trojan creates a key named 'DelegateExecute,' causing the Windows system to first check this key value when handling amv files before proceeding to execute the malicious command located under Default.

These changes make it more difficult to detect malicious code in the registry, and when combined with the CVE-2023-38831 vulnerability exploitation, they successfully bypass checks by Windows 10's UAC and Windows Defender in practice.

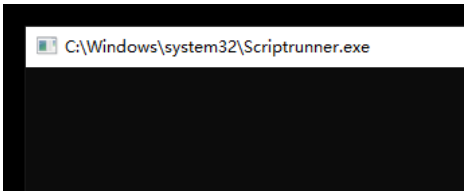


Figure 5.7 Actual execution result of this technique

Conclusion

The recent attack campaign launched by DarkPink shows that the WinRAR vulnerability CVE-2023-38831 has attracted great interest from APT groups. Since the disclosure of CVE-2023-38831, it has quickly become a favorite among various hacking groups, including APT groups. This was due to its one-click activation, compatibility with WinRAR software, ease of constructing the vulnerability, and effectiveness in facilitating phishing attacks. Using this vulnerability file as an attachment significantly increases the success rate of phishing attacks, and the difficulty in managing and updating WinRAR makes it challenging to eliminate the impact of this vulnerability exploitation.

Currently, the primary policy for defending against CVE-2023-38831 should focus on enhancing endpoint detection and response (EDR) capabilities. NSFOCUS Security Labs has observed various variants of CVE-2023-38831 vulnerability files, indicating that attackers are working on ways to reduce the detection rate of these files. It is expected the ongoing battle between cyberattacks and defense related to CVE-2023-38831 will persist.