The New APT Group DarkCasino and the Global Surge in WinRAR 0-Day Exploits

nsfocusglobal.com/the-new-apt-group-darkcasino-and-the-global-surge-in-winrar-0-day-exploits/

November 10, 2023

Overview

In 2022, NSFOCUS Research Labs revealed a large-scale APT attack campaign called DarkCasino and identified an active and dangerous aggressive threat actor. By continuously tracking and in-depth study of the attacker's activities, NSFOCUS Research Labs has ruled out its link with known APT groups, confirmed its high-level persistent threat nature, and following the operational name, named this APT group **DarkCasino**.

In August 2023, security vendor Group-IB followed up and disclosed a DarkCasino activity against cryptocurrency forum users, and captured a WinRAR 0-day vulnerability CVE-2023-38831 used by the APT threat actor DarkCasino in this attack.

NSFOCUS Research Labs analyzed the APT group DarkCasino's attack activities in WinRAR vulnerability exploitation and confirmed its techniques and tactics; At the same time, NSFOCUS Research Labs also found a large number of attacks by known APT organizations and unconfirmed attackers when tracking the exploitation of WinRAR vulnerabilities. Most of these attacks targeted national governments or multinational organizations.

This report will analyze the APT group DarkCasino and its detailed attacks launched recently, disclose the exploitation of WinRAR vulnerabilities by multiple known APT attackers and new threat actors, and predict the development trend of this threat.

About APT Group DarkCasino

DarkCasino is an economically motivated APT group that was first discovered by NSFOCUS Research Labs in 2021.

Figure 2.1 Impression of DarkCasino created by DALL-E

Name	DarkCasino
Affiliation	Unknown
Motivation	Economic benefits
Target industries	Cryptocurrency trading platforms, online casinos and network banks worldwide
Target victims	Staff and users of online trading platforms
Main attack vectors	Watering hole phishing, spear phishing
Representative attack tools	Trojan DarkMe, Vulnerability CVE-2023-38831

Table 2.1 DarkCasino Information

The name of DarkCasino comes from a large-scale APT attack of the same name captured by NSFOCUS Research Labs in 2022. the APT group DarkCasino mainly targets various online trading platforms in Europe, Asia, the Middle East and other regions, covering industries such as cryptocurrencies, online casinos, network banks and online credit platforms. DarkCasino is good at obtaining assets deposited by victims in online accounts by stealing passwords from target hosts.

Attacks launched by the APT group DarkCasino are very frequent, demonstrating a strong desire to steal online property. In the early days, DarkCasino mainly operated in countries around the Mediterranean and other Asian countries using online financial services; more recently, with the change of phishing methods, its attacks have reached users of cryptocurrencies worldwide, even including non-English-speaking Asian countries such as South Korea and Vietnam.

DarkCasino is an APT threat actor with strong technical and learning ability, who is good at integrating various popular APT attack technologies into its attack process. In the early days, the APT group DarkCasino mainly drew on the attack idea of an APT attacker named Evilnum and used malicious shortcuts, image steganography and other technologies to realize phishing attacks. The overall process design was also similar to that of Evilnum, so NSFOCUS Research Labs once attributed this organization to Evilnum; after H2 2022, DarkCasino gradually abandoned the attack idea borrowed from Evilnum and developed a set of multi-level loading patterns based on several Visual Basic components, thus implementing many larger-scale network attacks.

In 2021, the APT group DarkCasino developed a Visual Basic-based Trojan Horse program called DarkMe and constantly refined the details of the attack process around it to improve its functions, countermeasures and delivery methods, thus enhancing the stability and efficiency of attacks. For a detailed analysis of this attack tool, please also refer to the published analysis report of NSFOCUS Research Labs.

At present, there is not enough evidence to prove the origin of DarkCasino.

About CVE-2023-38831

CVE-2023-38831 is an arbitrary execution vulnerability in WinRAR software that was first exploited by DarkCasino in April 2023 and fixed in a new version of WinRAR v6.23 in August 2023.

The implementation of CVE-2023-38831 is based on the file running mechanism of WinRAR software. By constructing a decoy file, a folder with the same name as the decoy file, and a malicious file with the same name with a space at the end of the folder, it spoofs the API function ShellExecuteExW called by WinRAR, so that it can mistakenly release the malicious file and execute when the decoy file should have been opened.

NSFOCUS Research Labs found that CVE-2023-38831 can be integrated into common email or watering hole phishing attacks, replacing malicious package attachments commonly found in phishing emails to make it more deceptive. It is difficult for untrained WinRAR users to identify and defend against such exploit attacks; Some CVE-2023-38831 vulnerability exploitation variants also have a certain anti-virus capability, which can bypass the endpoint protection software in the target device to achieve attack effects.

Due to the large installed capacity, blocked update channels and difficult maintenance of WinRAR software, CVE-2023-38831 has a great impact and attack power. It is expected that this vulnerability will become an important weapon for attackers to break through target defense for a period of time.

Recent Activities of DarkCasino

Overview

NSFOCUS Research Labs observed that DarkCasino has been active for more than a year since they first launched large-scale cyberattacks using the Trojan DarkMe in 2022. Attacks against online trading platforms launched by DarkCasino can be spotted in each quarter.

In April 2023, DarkCasino developed a new attack pattern and launched a new round of attacks against online trading forums.

DarkCasino exploited a WinRAR zero-day vulnerability (later identified by security researchers and assigned number CVE-2023-38831) in this new attack pattern, placing malicious programs into specially crafted vulnerability zip files for phishing attacks against forum users through online trading forum posts.

In general, DarkCasino constructed various post contents such as money-making tips and investment suggestions, and lured forum users into opening malicious files attached or pointed to the posts.

DarkCasino put a large number of vulnerability files in various trading forums. As of October, some posts with malicious links or files remained uncleaned, as shown below.

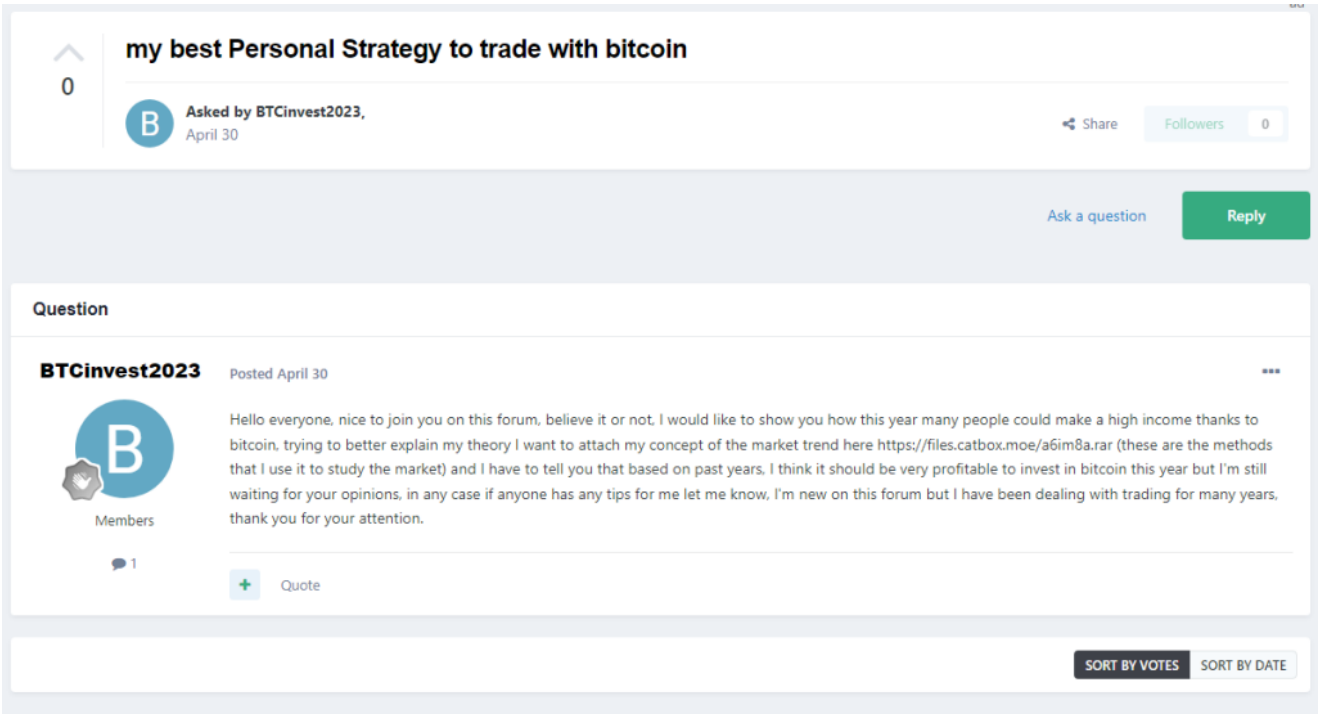


Figure 4.1 Phishing Posts from DarkCasino

Attack Process Analysis

NSFOCUS Research Labs found that DarkCasino implemented two attack processes by compressing files through these vulnerabilities. The main logic of these two attack processes is relatively similar, and the main difference lies in the storage form of the Trojan data.

This report takes the attack flow using encrypted .txt files as an example to introduce the process design ideas and changes of DarkCasino in this round of operations.

The main composition of this attack process is shown in the following figure, which consists of the CVE-2023-38831 vulnerability exploitation file, Cabinet archive file, registry file and ActiveX control file. It is divided into three stages: vulnerability exploitation, load release and Trojan execution.

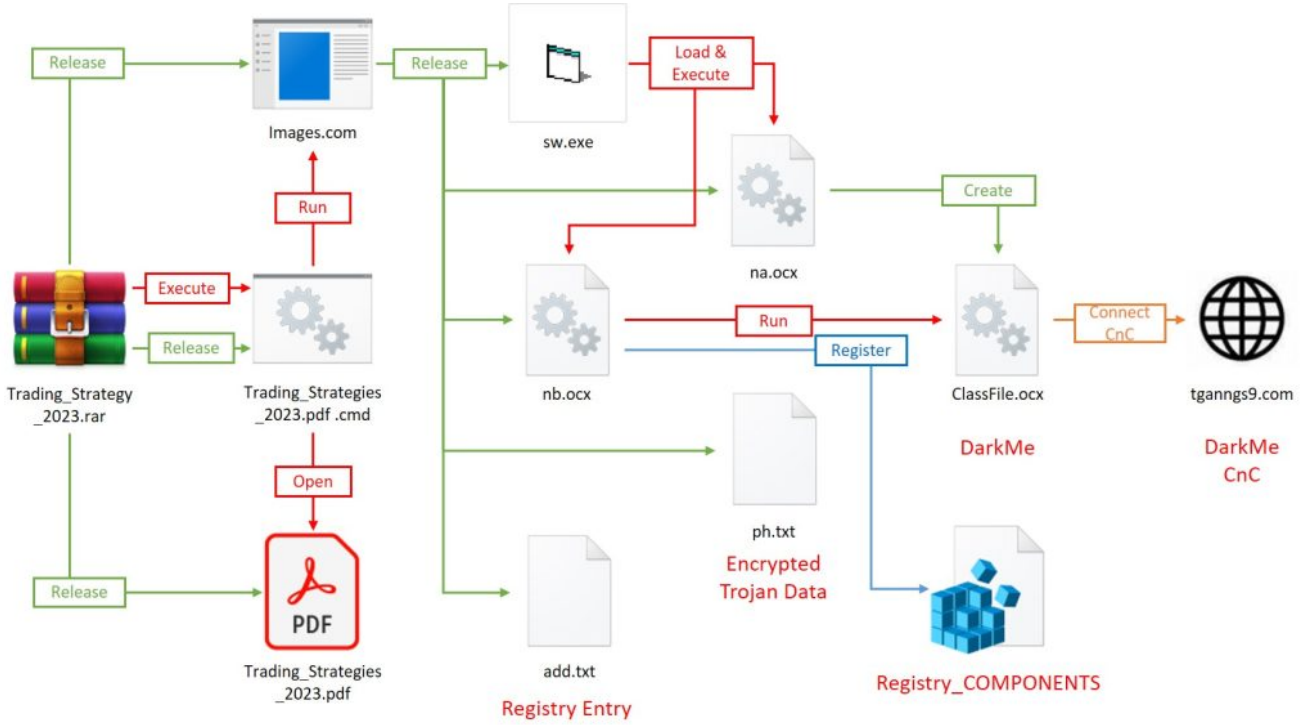


Figure 4.2 Main Attack Process of DarkCasino

In another attack flow, DarkCasino replaces the medium storing encrypted Trojan data with a steganographic image.

Vulnerability Exploitation Stage

When the victim opens a file named “Trading_strategy_2023.rar”, the following file structure will be displayed in WinRAR:

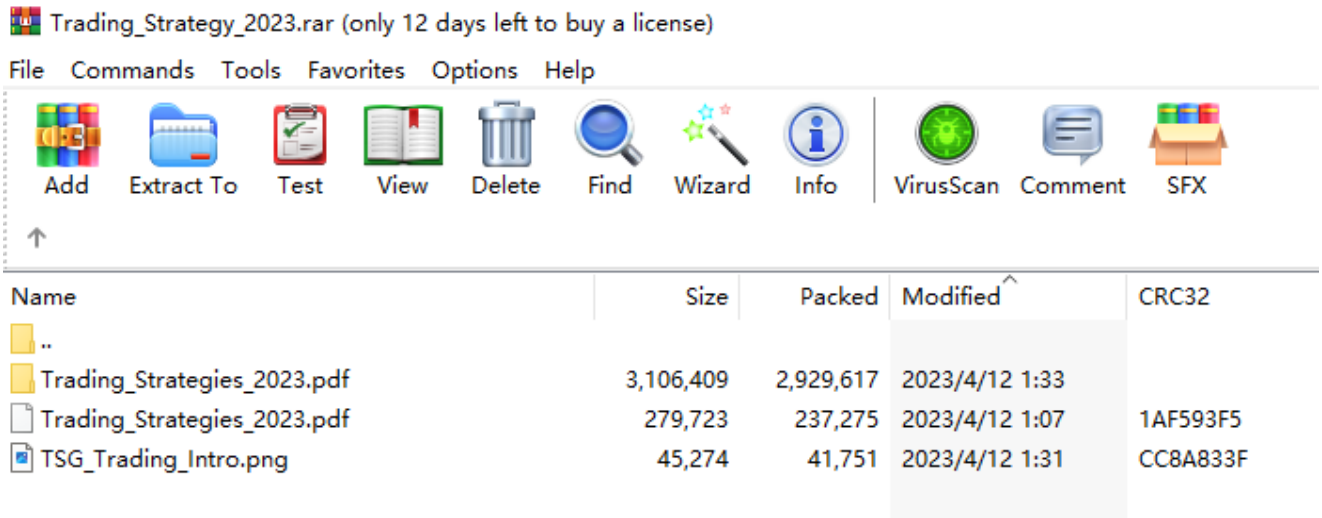


Figure 4.3 DarkCasino Vulnerability File Structure A

This is a typical build pattern for CVE-2023-38831 vulnerabilities. When the user tries to double-click to open the pdf file in the zip package, it actually executes a batch file named “Trading_Strategies_2023.pdf .cmd” under the same name folder.

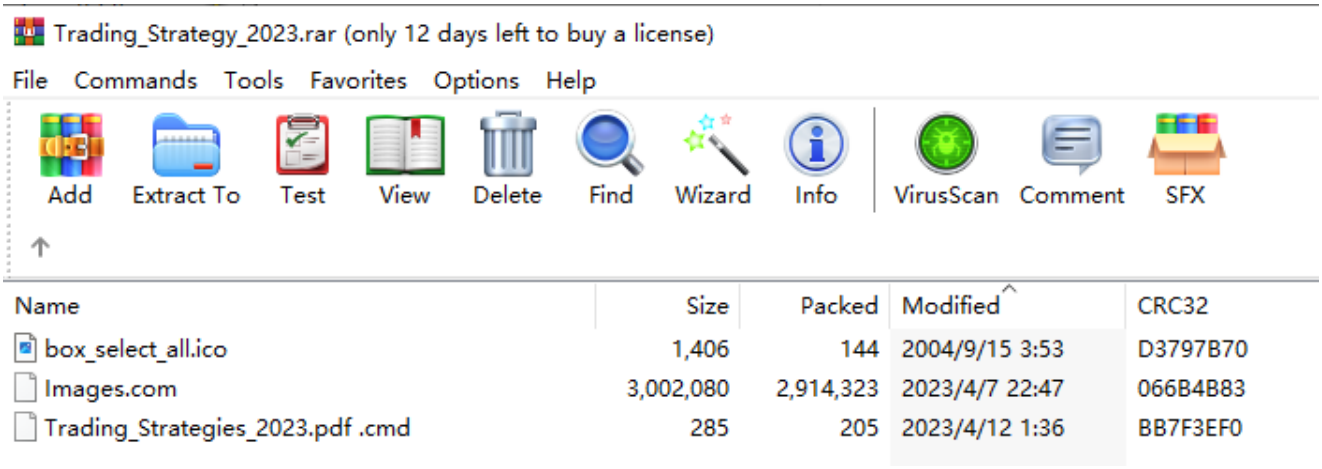
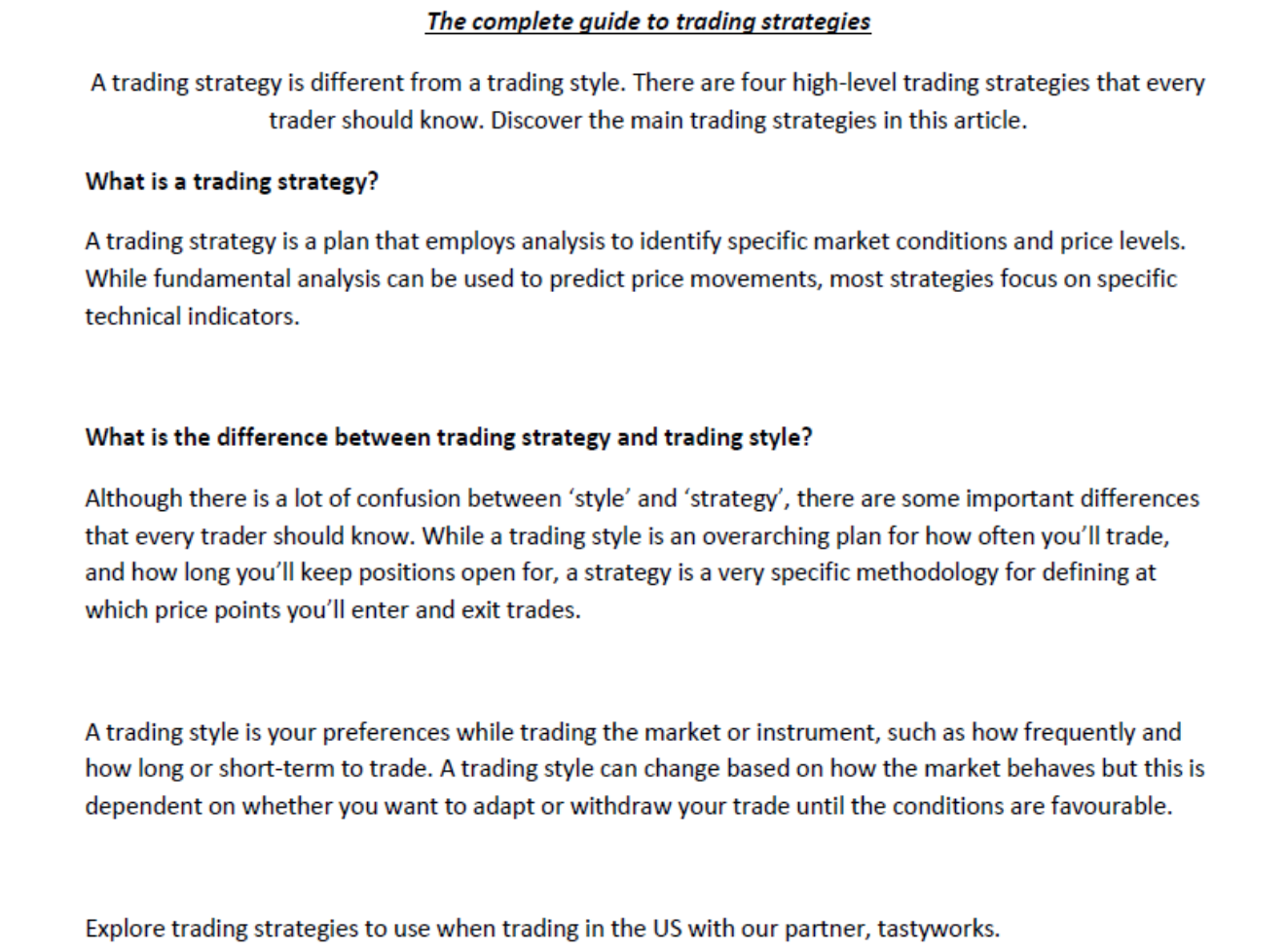


Figure 4.4 DarkCasino Vulnerability File Structure B

This batch will open the original decoy pdf file as well as a malicious file named Images.com.

The contents of the original decoy pdf file in this example process are shown below.



The complete guide to trading strategies

A trading strategy is different from a trading style. There are four high-level trading strategies that every trader should know. Discover the main trading strategies in this article.

What is a trading strategy?

A trading strategy is a plan that employs analysis to identify specific market conditions and price levels. While fundamental analysis can be used to predict price movements, most strategies focus on specific technical indicators.

What is the difference between trading strategy and trading style?

Although there is a lot of confusion between 'style' and 'strategy', there are some important differences that every trader should know. While a trading style is an overarching plan for how often you'll trade, and how long you'll keep positions open for, a strategy is a very specific methodology for defining at which price points you'll enter and exit trades.

A trading style is your preferences while trading the market or instrument, such as how frequently and how long or short-term to trade. A trading style can change based on how the market behaves but this is dependent on whether you want to adapt or withdraw your trade until the conditions are favourable.

Explore trading strategies to use when trading in the US with our partner, tastyworks.

Figure 4.5 Decoys used by DarkCasino

Load Release Stage

The Images.com file, which was exploited to execute batch files within the file, is a loader-type Trojan designed by DarkCasino. The program is actually a cabinet archive file disguised as a .com file, including sw.exe, na.ocx, nb.ocx, ph.txt and add.txt five components.

After the loader Trojan releases the above five components to the TEMP directory, it will run the sw.exe program to start the subsequent loading execution process.

Sw.exe itself does not contain malicious functions and is mainly used to load na.ocx and nb.ocx library files.

na.ocx will read and decrypt the ph.txt file, save the decrypted content in %APPDATA%\RarDir\ClassFile.ocx, and also transfer add.txt to this directory.

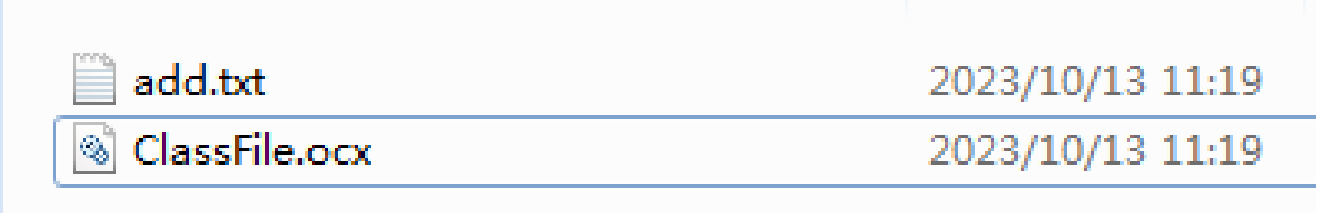


Figure 4.6 Malicious files generated by DarkCasino in APPDATA
The nb.ocx file mainly runs the following cmd commands:

cmd /c cd APPDATA\RarDir&&cmd /c timeout 1&&cmd /c reg.exe import add.txt

cmd /c cd APPDATA\RarDir&&cmd /c timeout 1&&cmd /c rundll32.exe /sta {EA6FC2FF-7AE6-4534-9495-F688FEC7858C} Mouse_Keyboard

These cmd commands register a com component by writing to the host registry and then running it.

The registered com component is the above decrypted and saved ClassFile.ocx file.

Trojan Execution Stage

The com component ClassFile.ocx running in the above process is the final payload Trojan of this attack flow.

The Trojan horse used by DarkCasino in this round of operations is DarkMe, which is commonly used by the group.

The Trojan DarkMe appeared in this round of attacks is basically the same as that previously used by DarkCasino in terms of functions. The main difference is that DarkCasino has added more obfuscation codes to the new Trojan, expanding the whole program file to over 20MB. This strategy can effectively reduce the risk of being detected.

DarkMe is a Visual Basic spy Trojan. Its initial version appeared on September 25, 2021. Currently, it supports host information collection, screenshot, file manipulation, registry manipulation, cmd command execution, self-update, persistence and other functions.

For a detailed analysis of the Trojan DarkMe, refer to NSFOCUS Research Labs' published report on Operation DarkCasino.

CVE-2023-38831 Exploitation in the Wild

When NSFOCUS Research Labs analyzed the impact surface of vulnerability CVE-2023-38831, it found that since this vulnerability was revealed in August 2023, multiple APT organizations and unconfirmed attackers have used this vulnerability for phishing attacks, most of which target important government agencies in various countries.

NSFOCUS Research Labs also captured a large number of exploitation files produced and disseminated by phishing email hackers worldwide, indicating that the vulnerability has been exploited on a large scale.

Attacks by known APT groups

It has been observed that APT group DarkPink in Southeast Asia, APT group Konni in East Asia and APT group GhostWriter in Eastern Europe use CVE-2023-38831 vulnerabilities to carry out cyberattack activities.

DarkPink-linked attacks on the governments of Vietnam and Malaysia

The APT group DarkPink has used the vulnerability CVE-2023-38831 to attack government targets in Vietnam and Malaysia.

DarkPink attackers used this vulnerability in this round of attacks to upgrade their existing attack processes and make multiple improvements to attack techniques and tactics, significantly improving the success rate of attacks.

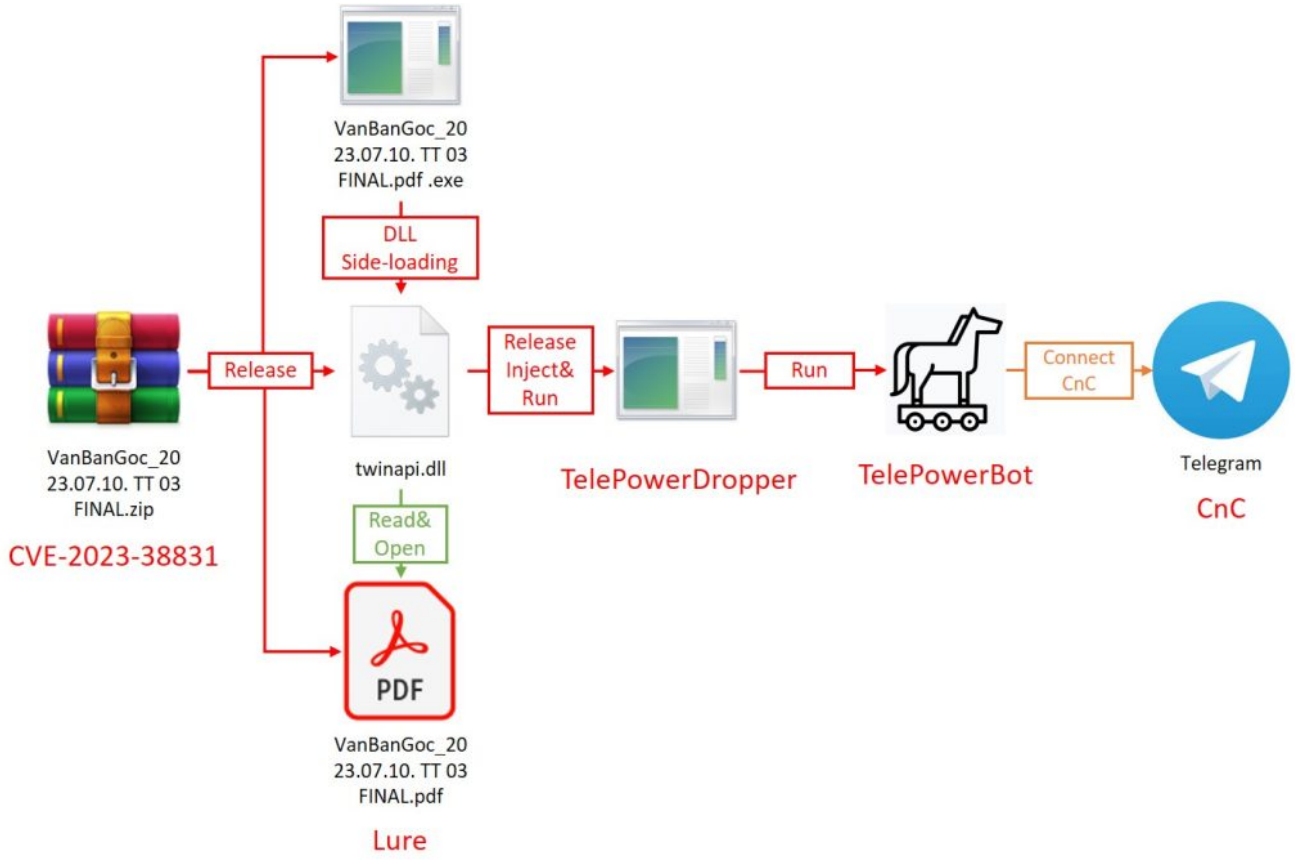


Figure 5.1 Main Attack Process of DarkPink

Known targets of the DarkPink attack include Vietnam's Ministry of Foreign Affairs, Ministry of Finance, Vietnam's State Securities Regulatory Commission and Malaysia's government sectors like Ministry of Defense and Strategic Planning.

DarkPink still uses its main Trojan programs, TelePowerDropper and TelePowerBot, to steal information during this round of attacks.

A detailed analysis of the DarkPink campaign can be found in reports published by NSFOCUS Research Labs.

Konni-linked attacks on cryptocurrency industry in South Korea

Konni, an APT group from North Korea, also quickly used the vulnerability CVE-2023-38831 to launch attacks on South Korea's cryptocurrency industry after it was made public. Relevant attacks were first disclosed by Knownsec.

Interestingly, the attack process built by Konni using this vulnerability is somewhat similar to that originally used by DarkCasino. It consists of components such as batch files, Trojan horse programs disguised as images, and binaries storing encrypted information.

The decoy used by Konni in this attack is a web file named "Screenshot_2023_09_06_Qbao_Network.html", which contains the cryptographic mnemonic of a cryptocurrency wallet application.

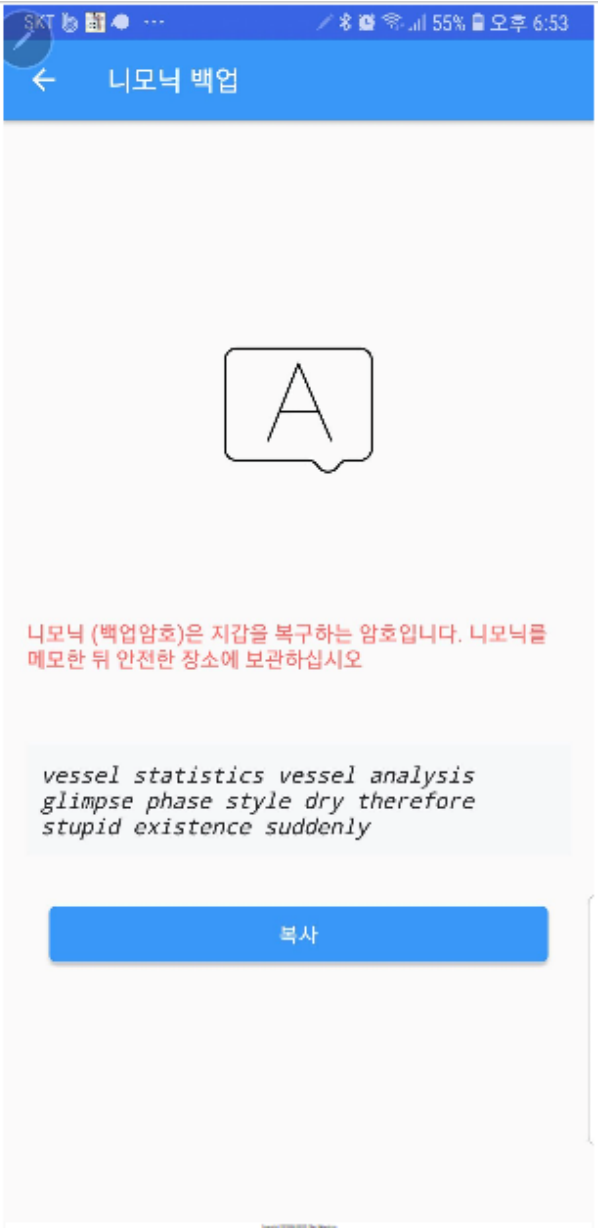


Figure 5.2 Decoys used by Konni

The final payload delivered by Konni in this attack is its representative Trojan KonniRAT, which can take long-term control of the victim host and obtain important contents.

GhostWriter-linked attacks on defense and educational institutions in Ukraine

Also at the end of August when the vulnerability was revealed, GhostWriter (UAC-0057, UNC1151), an APT group suspected of coming from Belarus, also began to exploit this vulnerability to launch attacks against Ukraine.

The vulnerability exploitation file constructed by GhostWriter is named ” Збірник_тез_НУОУ_23″ (National Defense University of Ukraine Digest 23), and its structure is shown in the following figure, consisting of decoy pdf file, cmd batch file and lnk shortcut file:

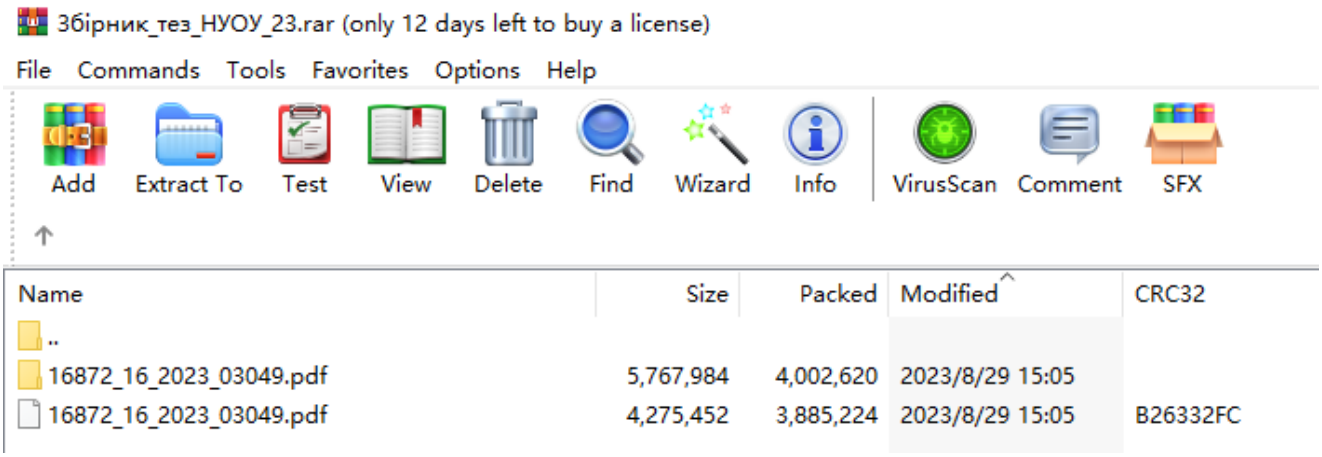


Figure 5.3 Vulnerability File Structure A Built by GhostWriter

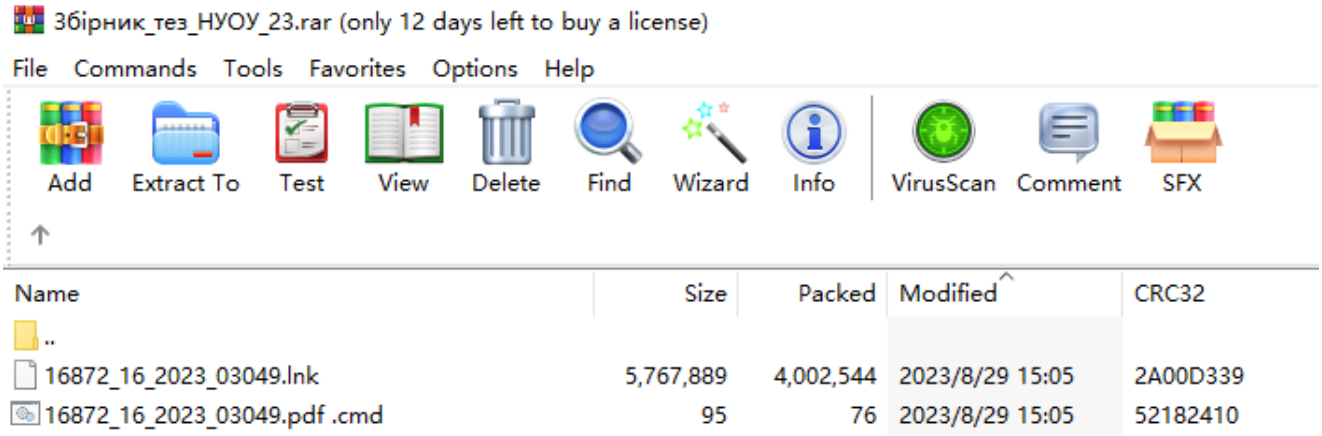


Figure 5.4 Vulnerability File Structure B Built by GhostWriter

After the vulnerability is triggered, the actually executed cmd batch file will run an lnk shortcut to release the decoy .pdf file and GhostWriter's iconic Trojan PicassoLoader.

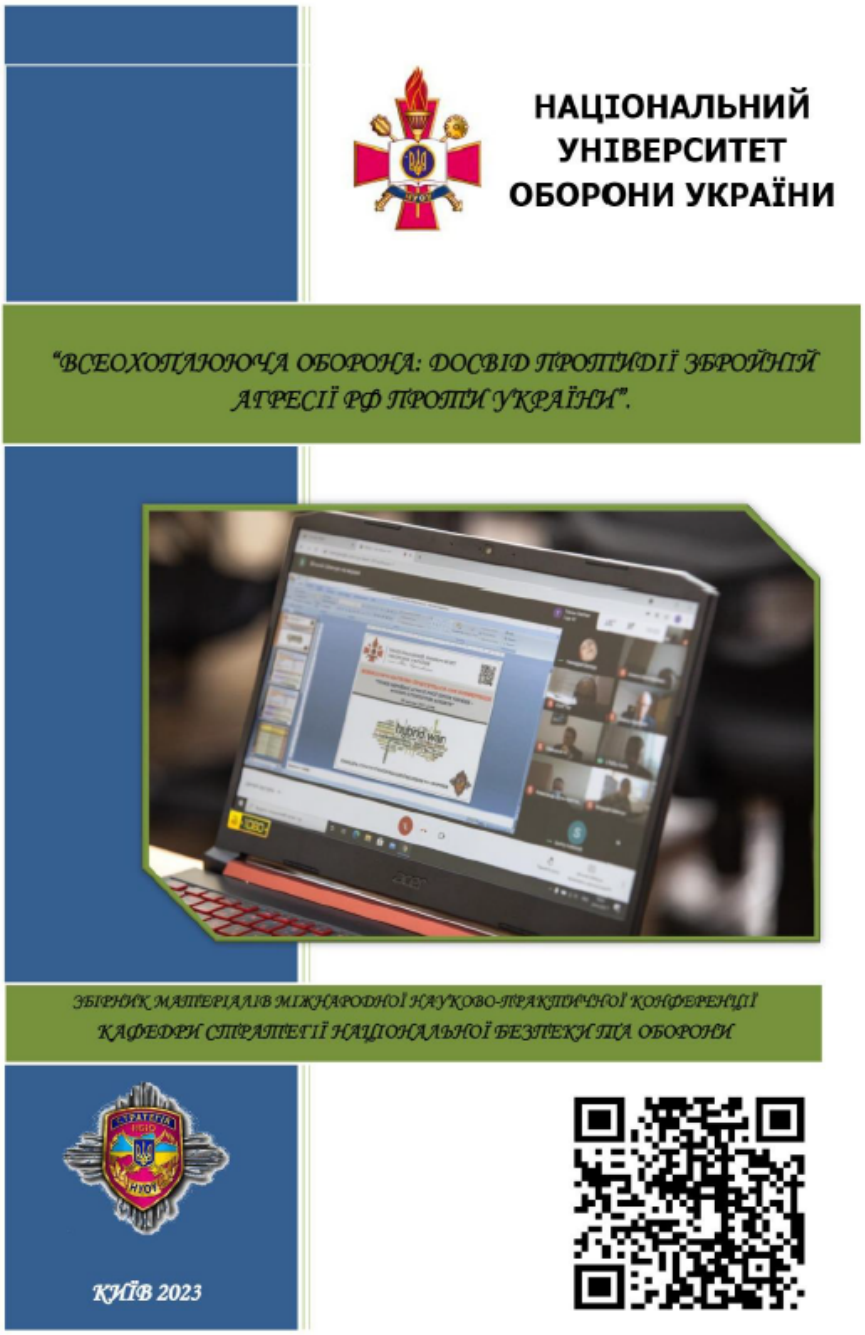


Figure 5.5

Decoys Used by GhostWriter

The PicassoLoader is a variant Trojan written with JavaScript. Its main function is to download and decrypt a piece of data, obtain and load the Trojan CobaltStrike Beacon, and control the victim's host.

Unconfirmed Threat Actors

NSFOCUS Research Labs also captured many field exploit files that could not be attributed to known APT attackers. Since most of these exploit files are aimed at targets such as government agencies and multinational organizations, NSFOCUS Research Labs has marked these attackers and assigned temporary names for tracking.

Actor230830: Attack targeting the European Parliament

The attacker marked as Actor230830 organized attacks on relevant personnel of the European Parliament immediately after the vulnerability became public.

The attack flow built by Actor230830 is relatively simple. After the vulnerability is triggered, a cmd batch file will be executed, which will access the following two addresses through an edge browser:

http://89.96.196[.]150:8080/

https://www.europarl.europa[.]eu/pdfs/news/expert/agenda_week_by_day/35-2023/35-2023_en.pdf

The link to the .pdf file is used to display a decoy that is used to confuse victims, while the link to the IP address is used to help attackers carry out attacks

Agenda

28 August - 03 September 2023
20230823APR04240

European Parliament

The Week Ahead 28 August – 03 September 2023

Committee and political group meetings, Brussels

Commissioner Wojciechowski on the Black Sea grain deal. Members of the Committee on Agriculture and Rural Development will quiz Commissioner Wojciechowski on the Black Sea grain deal and market situation. (*Thursday*)

Establishing theUkraine Facility. The Commission's proposal for a €50 billion initiative to support Ukraine's recovery, reconstruction and modernisation from 2024 to 2027 will be discussed by members of the committees on Budgets and Foreign Affairs. (*Wednesday*)

Mid-term revision of the EU's long-term budget. The package to boost the EU's Multiannual Financial Framework (MFF) in order to be able to face urgent challenges will be the focus of a debate in the Committee on Budgets, during which the rapporteurs will present their draft report on the revision. (*Wednesday*)

Announcement of LUX Award Finalists. The five films shortlisted for the 2024 LUX European Audience film award will be unveiled at the Venice film festival. (*Friday*)

President's agenda. Roberta Metsola, President of the European Parliament, will meet with the Prime Minister of Romania Ion-Marcel Ciolacu on Friday 14:00.

EP press contacts

Figure 5.6 Decoys used by Actor230830

The researchers were unable to confirm the attacker's actual attack pattern because service on port 8080 of the above-mentioned remote server had been withdrawn when this attack was discovered.

In the existing sandbox records, access to this IP port triggered the NTLM authentication mechanism of Windows. Therefore, it can be speculated that the attacker may use the vulnerability of NTLM protocol to try to steal the password of the victim's host domain.

Known victims of this attack are located in Portugal and the United Kingdom.

Actor231003: Attack targeting Serbia

Another unknown attacker, Actor231003, exploited the vulnerability CVE-2023-38831 in early October to launch a cyberattack targeting Serbia.

The decoy built by the attacker in this activity is called “NATONSPAFinalInviteList.zip”, and its construction uses the common pattern of .pdf decoys matching cmd batch files, as shown below.

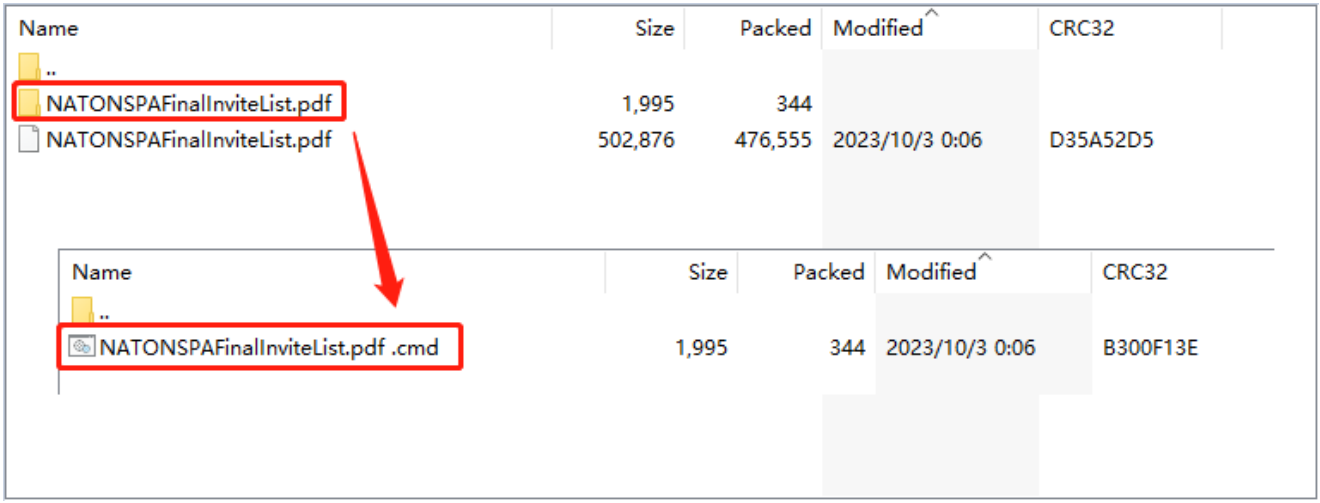


Figure 5.7 Vulnerability File Structure Built by Actor231003

The contents of NATO Public Diplomacy Programmes are documented in the decoy file called “NATONSPAFinalInviteList.pdf” as shown below.

Figure 5.8 Decoys used by Actor231003

The vulnerability file was uploaded to Serbia, so it can be inferred that the attackers were targeting pro-NATO forces in non-NATO countries.

After the vulnerability is triggered, subsequent Trojan programs will be downloaded from the specified location https://allnato[.]net/news/uploads/chrmap.exe to realize attacks.

The Trojan released by Actor231003 in this event is the well-known remote-controlled Trojan Remcos. It can achieve full control of the victim's host.

Actor231004: Attack targeting government departments of New Zealand

NSFOCUS Research Labs also uncovered another suspected cyber-attack against governmental sectors of New Zealand. The attacker we labeled as Actor231004 used a report from the Ministry of Foreign Affairs and Trade of New Zealand as bait and exploited vulnerabilities in CVE-2023-38831 to release a well-known commercial spyware Bumblebee.

Figure 5.9

Decoys used by Actor231004

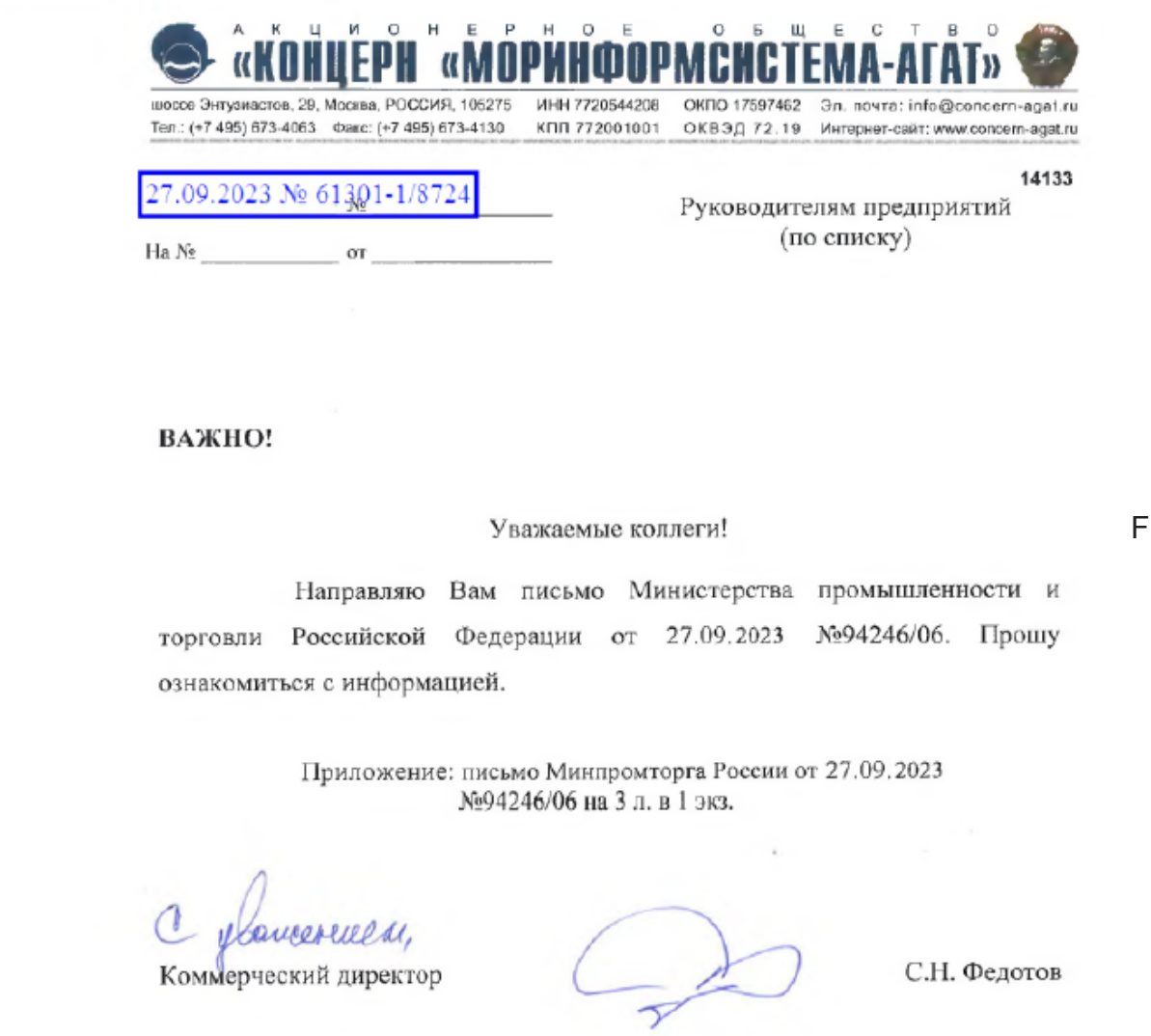
Bumblebee is a loader-type Trojan. With that, an attacker can deliver subsequent attack components to steal secrets or take over the operations of remote hosts.

There are many known attacker organizations related to the Trojan Bumblebee, including GOLD CABIN, TA578 and TA579.

Actor231010: Attack targeting Russia and Belarus

Another attacker Actor231010 (aka SkeletonWolf) by NSFOCUS Research Labs used this vulnerability to launch phishing attacks against Russia and Belarus.

The vulnerability file constructed by this attacker also consists of a decoy .pdf file and a batch file used for the attack. The decoy name is Pismo_ishodjashhee_61301-1_8724_ot_27_09_2023_Rassylka_Ministerstva_promyshlennosti.pdf (Ministry of Industry mail 61301-1 8724 dated September 27, 2023). The document is a letter from the Federal Ministry of Industry and Trade of Russia, so it can be presumed that Actor231010's target in this attack is the people who had dealings with the Ministry of Industry of the Government of Russia.



АКЦИОНЕРНОЕ ОБЩЕСТВО
«КОНЦЕРН «МОРИНФОРМСИСТЕМА-АГАТ»

шоссе Энтузиастов, 29, Москва, РОССИЯ, 105275 ИНН 7720544208 ОКПО 17597462 Эл. почта: info@concern-agat.ru
Тел.: (+7 495) 673-4063 Факс: (+7 495) 673-4130 КПП 772001001 ОКВЭД 72.19 Интернет-сайт: www.concern-agat.ru

27.09.2023 № 61301-1/8724

14133

На № _____ от _____

Руководителям предприятий
(по списку)

ВАЖНО!

Уважаемые коллеги!

Направляю Вам письмо Министерства промышленности и торговли Российской Федерации от 27.09.2023 №94246/06. Прошу ознакомиться с информацией.

Приложение: письмо Минпромторга России от 27.09.2023 №94246/06 на 3 л. в 1 экз.

С уважением,
Коммерческий директор С.Н. Федотов

Figure

5.10 Decoy A used by Actor231010

Another decoy document, disguised as a Belarus State Military Committee document, requires that property received by military units from the Ministry of Defense be reported in accordance with the form attached to the document. The decoy was suspected of targeting military units in Belarus.

ДЗЯРЖАЎНЫ
ВАЕННА-ПРАМЫСЛОВЫ КАМІТЭТ
РЭСПУБЛІКІ БЕЛАРУСЬ
(ДЗЯРЖКАМВАЕНПРАМ)

пр-т Незалежнасці, д. 115, 220114, г. Мінск
тэл. (017) 272 29 82, тэл/факс (017) 373 90 81
E-mail: mail@vpk.gov.by

ГОСУДАРСТВЕННЫЙ
ВОЕННО-ПРОМЫШЛЕННЫЙ КОМИТЕТ
РЕСПУБЛИКИ БЕЛАРУСЬ
(ГОСКОМВОЕНПРОМ)

пр-т Независимости, д. 115, 220114, г. Минск
тел. (017) 272 29 82, тел/факс (017) 373 90 81
E-mail: mail@vpk.gov.by

15.09.2023 № 05-09/1997-ви
на № _____ от _____

Руководителям организаций
(по списку)

О проверке целевого использования имущества военного назначения

В соответствии с Положением о контроле за целевым использованием организациями Республики Беларусь приобретенного имущества, отнесенного к продукции военного назначения, утвержденным постановлением Государственного военно-промышленного комитета Республики Беларусь от 24 января 2008 г. № 3, направляется копия графика проверок целевого использования имущества военного назначения, приобретенного организациями Республики Беларусь.

Проверка целевого использования указанного имущества будет осуществлена комиссией, назначенной приказом Госкомвоенпрома от 15 января 2009 г. № 7 (состав комиссии прилагается).

Проверке подлежит имущество военного назначения, приобретенное у Министерства обороны организациями Республики Беларусь в 2022 – 2023 годах, а также находящееся (состоящее на учете) в организации на момент предыдущей проверки.

Прошу до 30 марта 2024 г. направить информацию в Госкомвоенпром о сотруднике организации (Ф.И.О., занимаемая должность, контактный телефон) для включения в состав комиссии при проведении проверки в данной организации.

До начала проверки:

подготовить в печатном и электронном виде (в формате Microsoft Excel 97 – 2003) сведения о движении имущества военного назначения, приобретенного у Минобороны организацией, по прилагаемой форме (с даты проведения прошлой проверки);

подготовить копии документов, подтверждающих получение, постановку на учет и использование приобретенного имущества в заявленных целях (за исключением документов, вошедших в акт предыдущей проверки Госкомвоенпрома).

В ходе проведения проверки:

Figure

5.11 Decoy B used by Actor231010

The batch file portion of these vulnerability files contains an obfuscated powershell directive to download a malicious file from a specified remote location, which is an open source remote control Trojan called AthenaAgent that uses the discord channel as the CnC server.

It is worth noting that the detection rate of exploit files built by Actor231010 was very low, and only 6 samples were detected in VirusTotal.

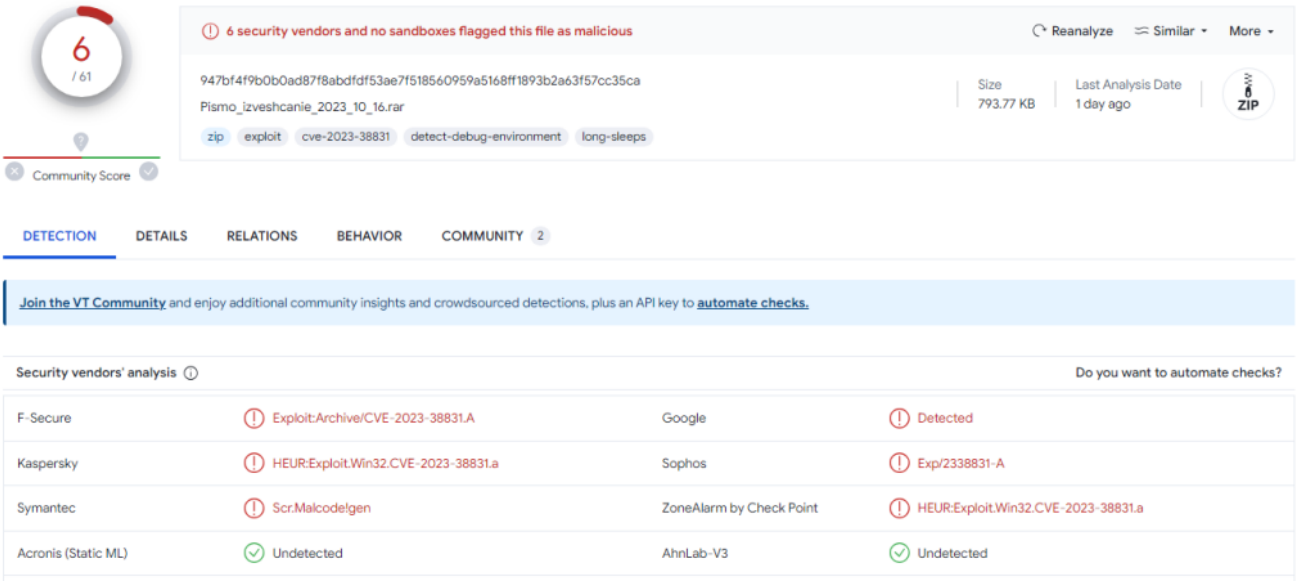
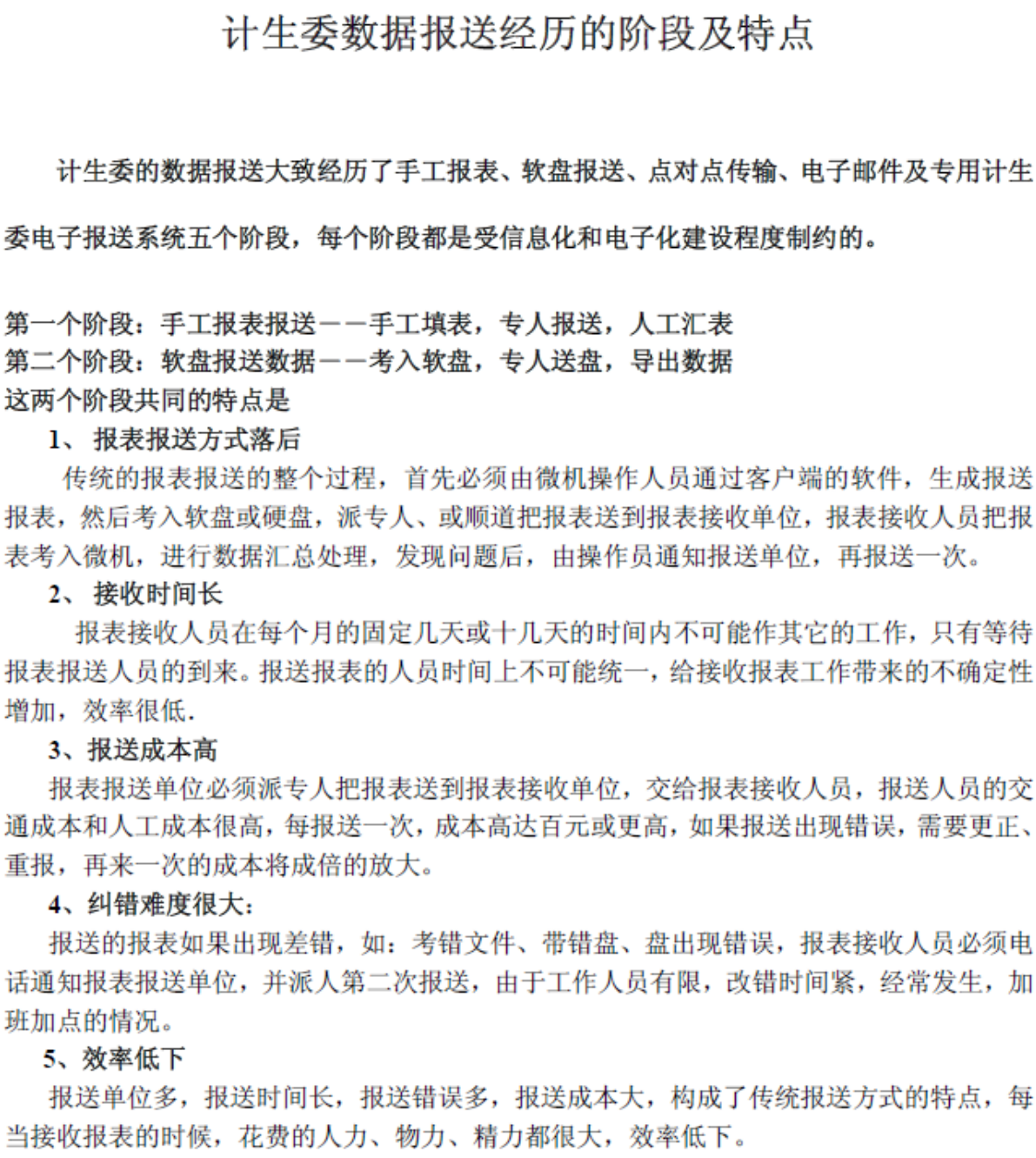


Figure 5.12 Detection of Actor231010 Vulnerability File

Actor231009: Attack targeting China

In addition, NSFOCUS Research Labs monitored a suspected correlated cyber-attack against China. An attacker labeled Actor231009 crafts a WinRAR exploit file that also contains the combination of .pdf and .cmd batch files.

The decoy file named “Doc57585894.pdf” opened and displayed a report related to the “Electronic Submission System of the Family Planning Commission”, indicating that the target of the attack may be the government or enterprises in China.



计生委数据报送经历的阶段及特点

计生委的数据报送大致经历了手工报表、软盘报送、点对点传输、电子邮件及专用计生委电子报送系统五个阶段，每个阶段都是受信息化和电子化建设程度制约的。

第一个阶段：手工报表报送——手工填表，专人报送，人工汇表
第二个阶段：软盘报送数据——考入软盘，专人送盘，导出数据
这两个阶段共同的特点是

1、 报表报送方式落后

传统的报表报送的整个过程，首先必须由微机操作人员通过客户端的软件，生成报送报表，然后考入软盘或硬盘，派专人、或顺道把报表送到报表接收单位，报表接收人员把报表考入微机，进行数据汇总处理，发现问题后，由操作员通知报送单位，再报送一次。

2、 接收时间长

报表接收人员在每个月的固定几天或十几天的时间内不可能作其它的工作，只有等待报表报送人员的到来。报送报表的人员时间上不可能统一，给接收报表工作带来的不确定性增加，效率很低.

3、报送成本高

报表报送单位必须派专人把报表送到报表接收单位，交给报表接收人员，报送人员的交通成本和人工成本很高，每报送一次，成本高达百元或更高，如果报送出现错误，需要更正、重报，再来一次的成本将成倍的放大。

4、纠错难度很大：

报送的报表如果出现差错，如：考错文件、带错盘、盘出现错误，报表接收人员必须电话通知报表报送单位，并派人第二次报送，由于工作人员有限，改错时间紧，经常发生，加班加点的情况。

5、效率低下

报送单位多，报送时间长，报送错误多，报送成本大，构成了传统报送方式的特点，每当接收报表的时候，花费的人力、物力、精力都很大，效率低下。

Figure 5.13 Decoys used by Actor231009

After a malicious batch file is triggered, the subsequent load Trojan will be downloaded from the designated remote location https://dnalnoomnus.ru/bx0/356x.exe. NSFOCUS Research Labs captured multiple different loads at this download address and found that the attacker mainly dropped the commercial Trojan Smokeloader. Attackers can use subsequent components of the Smokeloader program for operations like stealing files and records of information.

The operation of Actor231009 in this campaign indicates that the attacker may be in the exploring stage. NSFOCUS Research Labs will closely monitor potential follow-up activities of this attacker.

Conclusion

The WinRAR vulnerability CVE-2023-38831 brought by the APT group DarkCasino brings uncertainties to the APT attack situation in the second half of 2023. Many APT groups have taken advantage of the window period of this vulnerability to attack critical targets such as governments, hoping to bypass the protection system of the targets and achieve their purposes.

NSFOCUS Research Labs has also captured batch-generated vulnerability exploitation files decoyed by transaction bills. This phenomenon indicates that large phishing attack controllers have also incorporated this vulnerability into their phishing attack processes, which heralds more victims of WinRAR vulnerability exploitation in the future.

IoC

Hash	APT Group
dd9146bf793ac34de3825bdabcd9f0f3	DarkPink
5504799eb0e7c186afcb07f7f50775b2	DarkPink
c5331b30587dcaf94bfde94040d4fc89	DarkPink
ac28e93dbf337e8d1cc14a3e7352f061	DarkPink
fefe7fb2072d755b0bfdf74aa7c9013e	DarkPink
428a12518cea41ef7c57398c69458c52	Konni
7bb106966f6f8733bb4cc5bf2ab2bab4	GhostWriter
2b02523231105ff17ea07b0a7768f3fd	Actor230830
63085b0b7cc5bb00859aba105cbb40b1	Actor231003
7195be63a58eaad9fc87760c40e8d59d	Actor231004
129ccb333ff92269a8f3f0e95a0338ba	Actor231010
cd1f48df9712b984c6eee3056866209a	Actor231010
b05960a5e1c1a239b785f0a42178e1df	Actor231010
6b5d5e73926696a6671c73437cedd23c	Actor231009