

Case of Malware Distribution Exploiting LogMeIn and PDQ Connect

[A asec.ahnlab.com/en/90968](https://asec.ahnlab.com/en/90968)

ATCP

November 9, 2025



Download



AhnLab SEcurity intelligence Center (ASEC) recently identified cases of attacks exploiting the RMM (Remote Monitoring and Management) tools LogMeIn Resolve (GoTo Resolve) and PDQ Connect. While the initial distribution method is unknown, the attacks involve a legitimate-looking website that disguises the malware as a normal program. When a user downloads and installs the program, an additional malware strain with data exfiltration capabilities is also installed.

1. Distribution Method

The initial distribution method of LogMeIn is unknown, but it is presumed to have been distributed disguised as a legitimate program. The following are the various names under which LogMeIn, which was used in the attack, was installed.

The.exe
Microsoft.exe
chatgpt.exe
OpenAI.exe
notepad++.exe
7-zip.exe
winrar.exe
Videolan.exe
divine.exe
module_required.exe
windows12_installer.exe

The user seems to have accessed the website through an unknown path and installed LogMeIn Resolve from the following download page. These websites disguise themselves as the download page of free utilities such as Notepad++ and 7-Zip, but actually download the threat actor's LogMeIn Resolve.



Figure 1. Download page of Digestive Utility

2. LogMeIn

LogMeIn is an RMM tool that supports remote support, patch management, and monitoring. It is a tool that can remotely control systems that are installed for legitimate purposes and are not malware such as backdoors or RATs, so it is being exploited by various threat actors. This is an intentional attempt to bypass security products' detection. Unlike typical malware, security products such as firewalls and antivirus software have limitations in simply detecting and blocking these tools.

For LogMeIn Resolve, the internal configuration file contains the information of the administrator or threat actor. Typically, the "CompanyId" field is the ID of the administrator or threat actor who created the LogMeIn Resolve installation file, allowing the threat actor to be identified. [\[1\]](#)

```
017531E0 7B 22 70 75 62 6C 69 63 6B 65 79 22 3A 22 36 34 {"publickey":"64
```

Figure 2. Configuration data of LogMeIn Resolve

In the attack campaigns exploiting LogMeIn Resolve identified in Korea, three different “CompanyId” values were used.

- Threat Actor’s CompanyId – 1: 8347338797131280000
- Threat Actor’s CompanyId – 2: 1995653637248070000
- Threat Actor’s CompanyId – 3: 4586548334491120000




If a user installs LogMeIn disguised as a legitimate utility, it can be registered in LogMeIn’s infrastructure and seized by the threat actor. The threat actor exploited LogMeIn to execute PowerShell commands and install PatoRAT, a backdoor malware.

Target Type	File Name	File Size	File Path ⓘ
-------------	-----------	-----------	-------------

Figure 3. Malware installation log using LogMeIn Resolve

3. PDQ Connect

Additionally, PatoRAT has been installed by PDQ Connect as well as LogMeIn Resolve. PDQ Connect is an RMM tool that provides features such as software package distribution, patch management, inventory, and remote control, similar to LogMeIn Resolve. Threat actors abused PDQ Connect like LogMeIn Resolve to execute PowerShell commands and install PatoRAT.

Target Type	File Name	File Size	File Path ⓘ
Target	 webview.exe	8.41 MB	%SystemDrive%\users\%ASD%\edgeupdate\webview.exe
Current	 powershell.exe	444 KB	%SystemRoot%\system32\windowspowershell\v1.0\powershell.exe
Parent	 pdq-connect-agent.exe	8.98 MB	%ProgramFiles%\pdq\pdqconnectagent\pdq-connect-agent.exe




Process	Module	Target	Behavior	Data
 powershell.exe	N/A	N/A	Creates executable file	 webview.exe
 powershell.exe	N/A	N/A	A suspicious process created a file.	N/A

Figure 4. Malware installation log using PDQ Connect

4. PatoRAT

The ultimate malware installed by the threat actor using LogMeIn Resolve and PDQ Connect is PatoRAT. Developed in Delphi, PatoRAT is a backdoor that supports features such as remote control and information theft. Internal strings such as debug logs are written in Portuguese. The malware is classified as PatoRAT based on its ClientID.

```

push    dword ptr fs:[eax]
mov     fs:[eax], esp
mov     edx, offset aPacket_0 ; "Packet"
mov     eax, [ebp+var_3C]
call    sub_650628
mov     edx, offset aLocaltonet ; "localtonet"
call    sub_65245C
mov     edx, offset aStatus_2 ; "Status"
mov     eax, [ebp+var_3C]
call    sub_650628
mov     edx, offset aBaixandoEInsta ; "baixando e instalando o localtonet"
call    sub_65245C
mov     eax, [ebp+var_60]
mov     eax, [eax+0Ch]

```

Figure 5. Portuguese included in the binary

The configuration data is 1-byte XOR encrypted with the key value of 0xAA and stored in the RCDATA area of the resource under the item name "APPCONFIG". When decrypted, it contains the clientTag, mutex name, C&C server address list, and flag value.



Figure 6. Configuration data stored in the resource section

When PatoRAT is executed, it sends the following basic information about the system to the C&C server.

Item	Information
Packet identify id	Infected System ID (Combination of information such as CPU, environment variables, computer name, and volume serial number)
country	Locale Information
ComputerName	Computer Name
user	User Name
os	Operating System Information
version	1.6.1
performance Memoria	Memory Usage
activeWindow	Active Window
Screens MonitorsResolutions	Resolution
privileges	Permission to Execute Malware
clientTag	patolino" or "secondfloor
SDK	SDK Installation Status

Table 1. Information of the PatoRAT

Afterward, the following commands can be supported according to the commands of the C&C server.

Category	Command
Remote Control	Mouse control, Download and execute, Execute PowerShell commands, Manipulate clipboard, Update, Shutdown, Restart
Screen Control	HVNC, Remote desktop
Information Gathering	Keylogging, Screen capturing, Steal web browser credentials
Others	Install localtonet (Port forwarding is suspected), Scan QR code, Plugin support

Table 2. Supported commands

6. Conclusion

Recently, there have been cases of attacks installing backdoor malware using LogMeIn Resolve and PDQ Connect. LogMeIn Resolve is installed through a page disguised as a legitimate utility, and the threat actors used the RMM tool to install the PatoRAT backdoor malware. Users must check the official website when downloading utilities and verify the version information and certificate of the downloaded file to ensure that they are installing the intended file. They should also keep their operating systems and security products up to date to protect themselves from known threats.

MD5

04547ab017b84bc1934b39513fd8bad2

082823d138f9da9b085be91161c3cd04

17f1080ba64740c0b218e76b0bddb1e2

2638281ba875fce2fb2f595a7e8cf1fa

299b22f03a0affcb1ed74889c0c7e436

Additional IOCs are available on AhnLab TIP.

URL

[https://bithumb-19-10\[.\]netlify\[.\]app/%EB%B9%97%EC%8D%B8\[.\]exe](https://bithumb-19-10[.]netlify[.]app/%EB%B9%97%EC%8D%B8[.]exe)

[https://chatg31-10\[.\]netlify\[.\]app/chatgpt\[.\]exe](https://chatg31-10[.]netlify[.]app/chatgpt[.]exe)

[https://chatgpt-30-10\[.\]netlify\[.\]app/ChatGpt\[.\]exe](https://chatgpt-30-10[.]netlify[.]app/ChatGpt[.]exe)

[https://dazzling-genie-b16946\[.\]netlify\[.\]app/Browser%20Update\[.\]exe](https://dazzling-genie-b16946[.]netlify[.]app/Browser%20Update[.]exe)

[https://joyful-cajeta-](https://joyful-cajeta-66bmicro[.]netlify[.]app/%EB%A7%88%EC%9D%B4%ED%81%AC%EB%A1%9C%EC%86%8C%ED%94%84%ED%8A%B8[.]EXE)

[66bmicro\[.\]netlify\[.\]app/%EB%A7%88%EC%9D%B4%ED%81%AC%EB%A1%9C%EC%86%8C%ED%94%84%ED%8A%B8\[.\]EXE](https://joyful-cajeta-66bmicro[.]netlify[.]app/%EB%A7%88%EC%9D%B4%ED%81%AC%EB%A1%9C%EC%86%8C%ED%94%84%ED%8A%B8[.]EXE)

Additional IOCs are available on AhnLab TIP.

FQDN

lastdance[.]mysynology[.]net

masterpanel[.]webredirect[.]org

patolino[.]theworkpc[.]com

secondfloor[.]dynuddns[.]com

Gain access to related IOCs and detailed analysis by subscribing to **AhnLab TIP**. For subscription details, click the banner below.

The banner features a dark blue background with a glowing globe. Overlaid on the globe is a complex network of white lines and nodes, resembling a global communication or threat network. Two curved, glowing lines, one blue and one green, arc across the right side of the globe.

AhnLab TIP

Stay Ahead of Rapidly Evolving Threats Make the Best-Informed Decisions

Get Started with AhnLab's State-of-the-Art Threat Intelligence

atip.ahnlab.com