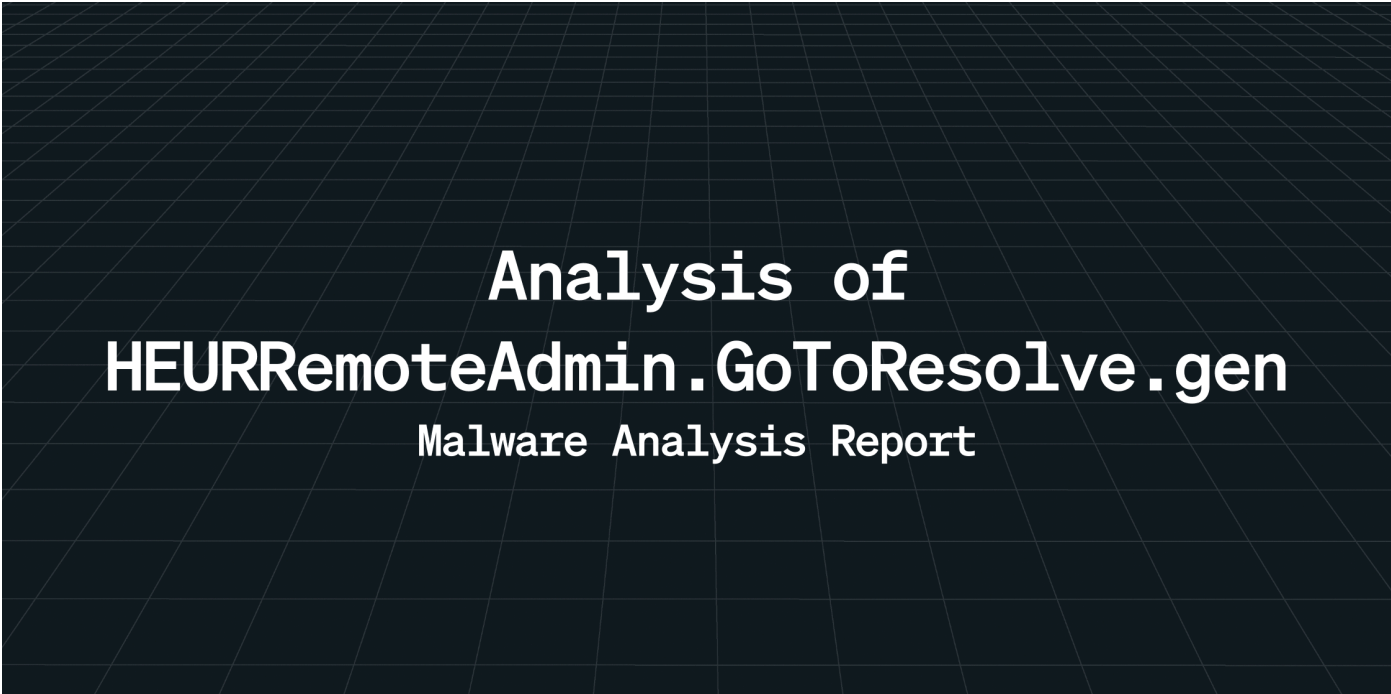


Analysis of HEURRemoteAdmin.GoToResolve.gen

 pointwild.com/threat-intelligence/analysis-of-heurremoteadmin-gotoresolve-gen

Lat61 Threat Intelligence Team

January 21, 2026



Analysis of HEURRemoteAdmin.GoToResolve.gen Malware Analysis Report

Introduction:

This report presents the results of a comprehensive analysis of a Potentially Unwanted Application (PUA) identified during routine security monitoring. PUAs are software programs that, while not overtly malicious in the traditional sense, often exhibit behaviors that undermine system performance, compromise user privacy, or introduce security risks. These applications typically rely on deceptive installation mechanisms, unwanted bundling with legitimate software, or aggressive advertising and tracking techniques.

The purpose of this analysis is to evaluate the sample's functional characteristics, behavioral patterns, and associated risks. The assessment includes static and dynamic analysis, examination of file and registry artifacts, network communication profiling, and a review of persistence mechanisms and privilege requirements.

This introduction establishes the context for the technical details that follow and frames the sample's potential impact on system integrity, user experience, and overall security posture.

Preliminary Information About Sample:

MD5: 6717e7dc73fb1d4febb1da10bbcb41c5

SHA-1: 5fb6ae10d167ada29f50b3693af18a961b961057

SHA-256: 2d482953418daf3dd3e16bcdcd2adc4bab16a6b9b3cb190b2840d8d4ffe359b2

Imphash: f8e4a22bcb1b836585534b93f63c1414

Compiler: Microsoft Visual C++

Internal Name: GoToResolveUnattendedUpdater.exe

Static Analysis:

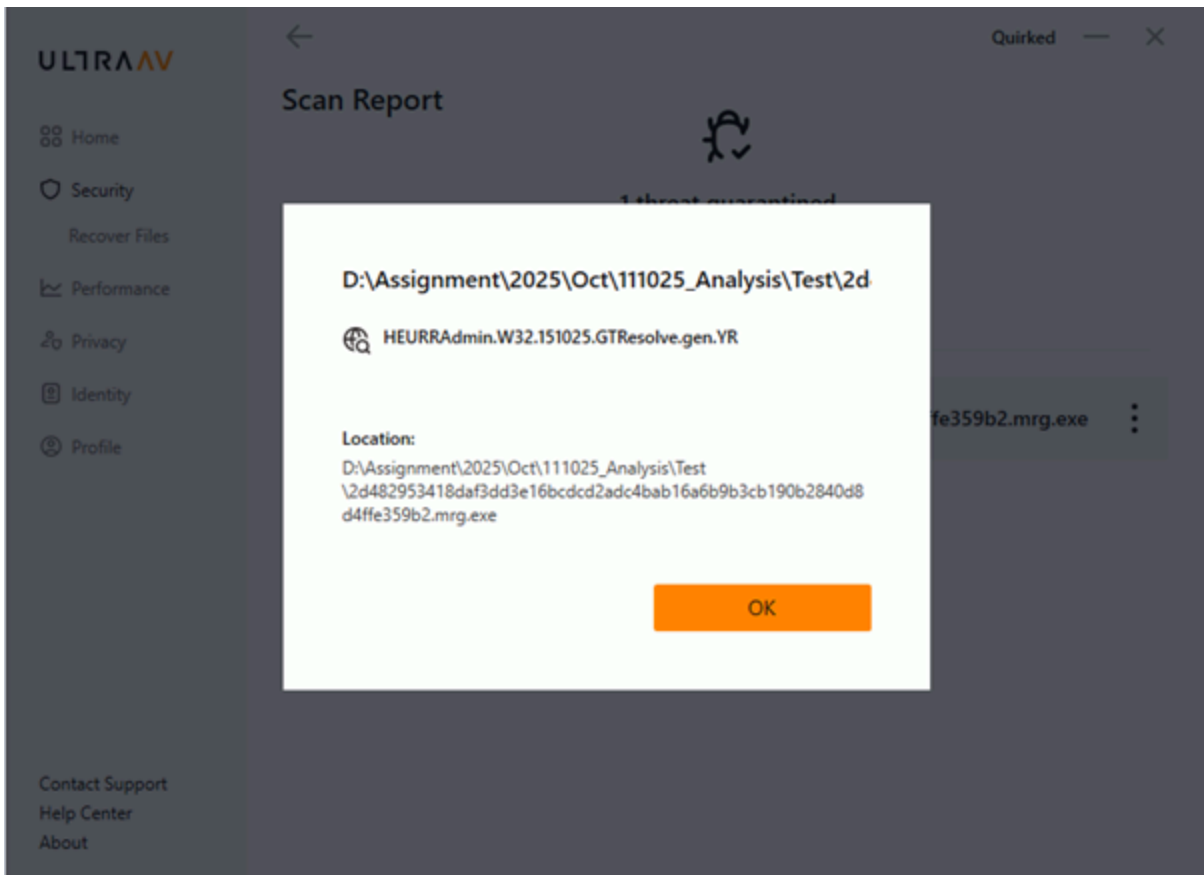


Figure 1: Information about Sample using ExeInfo tool

Digital Signature:

The sample is digitally signed as shown in the following image

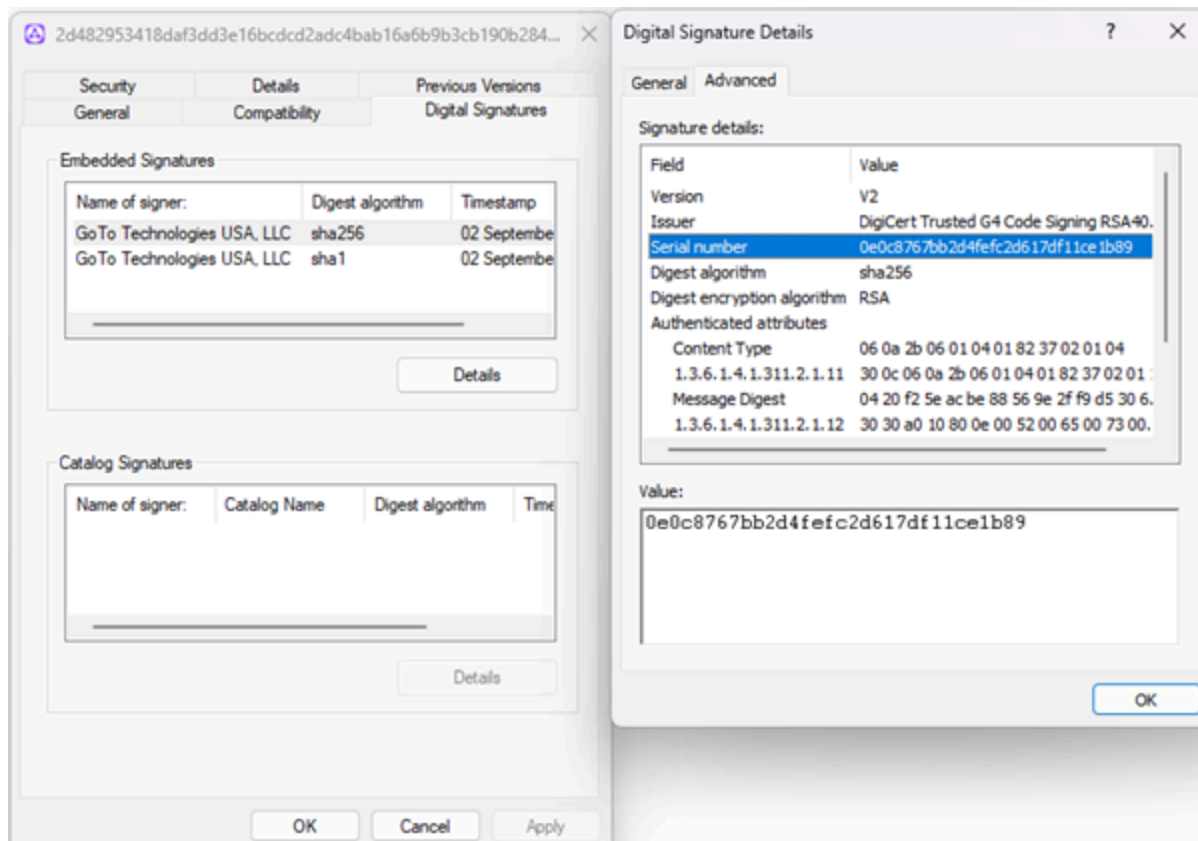


Figure 2: Digital Signature

Company Name: GoTo Technologies USA, LLC

Serial Number: 0e0c8767bb2d4fetc2d617df11ce1b89

Dynamic Analysis:

The sample installs a Potentially Unwanted Application (PUA) and starts threads in the background.

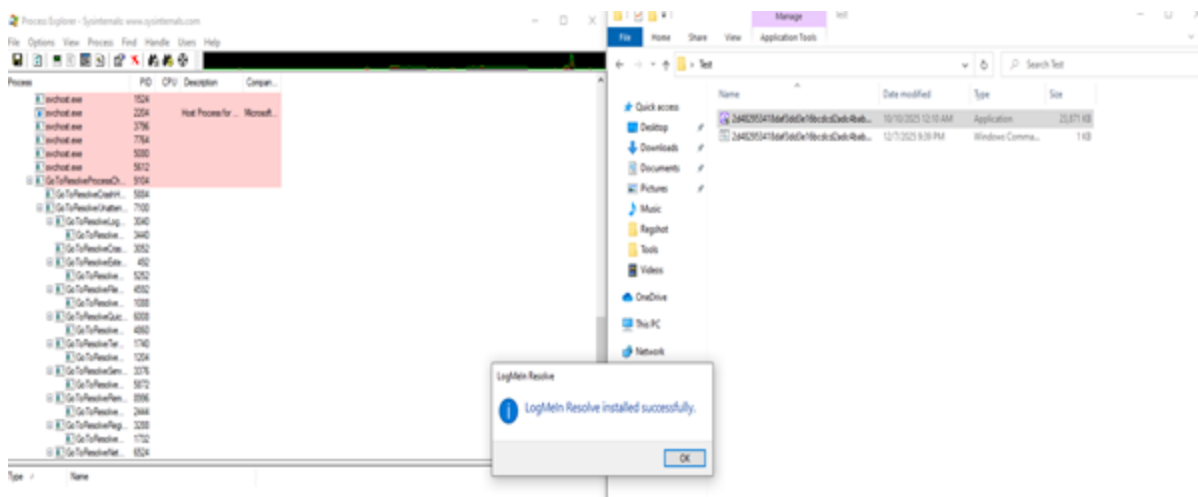


Figure 3: Dialog box When sample is run

GoToResolveUnattended.exe is an executable file for the GoTo Resolve Unattended Access application, which allows IT professionals to remotely access and support computers that are not being actively used by an end-user. This is a component of GoTo's remote support and management software, used for tasks like forced installations and updates.

But malware actors can use such applications to infect and insert their own malicious software like Trojans, Backdoors etc. to carry out malicious attacks or show excessive advertisements.

When the sample is run, it installs an application "GoToResolve".

This PC > Local Disk (C:) > Program Files (x86) > GoTo Resolve Unattended > 6293827109194426909 >

Name	Date modified	Type	Size
.sentry-native	12/10/2025 8:50 PM	File folder	
appdata	12/10/2025 8:50 PM	File folder	
Logs	12/10/2025 8:50 PM	File folder	
remoteprint	12/7/2025 9:39 PM	File folder	
x64	12/7/2025 9:39 PM	File folder	
x86	12/7/2025 9:39 PM	File folder	
FileManager.dll	12/7/2025 9:39 PM	Application exten...	16,622 KB
GoToResolveCrashHandler	12/7/2025 9:39 PM	Application	653 KB
GoToResolveExternalModuleHandler	12/7/2025 9:39 PM	Application	410 KB
GoToResolveFileManager	12/7/2025 9:39 PM	Application	410 KB
GoToResolveLoggerProcess	12/7/2025 9:39 PM	Application	410 KB
GoToResolveNetworkChecker	12/7/2025 9:39 PM	Application	410 KB
GoToResolveProcessChecker	12/7/2025 9:39 PM	Application	410 KB
GoToResolveQuickView	12/7/2025 9:39 PM	Application	410 KB
GoToResolveRegistryEditor	12/7/2025 9:39 PM	Application	410 KB
GoToResolveRemoteControl	12/7/2025 9:39 PM	Application	410 KB
GoToResolveServiceManager	12/7/2025 9:39 PM	Application	410 KB
GoToResolveTerminal	12/7/2025 9:39 PM	Application	410 KB
GoToResolveTools32	12/7/2025 9:39 PM	Application	1,094 KB
GoToResolveTools64	12/7/2025 9:39 PM	Application	1,330 KB
GoToResolveUi	12/7/2025 9:39 PM	Application	410 KB
GoToResolveUnattended	12/7/2025 9:39 PM	Application	410 KB
GoToResolveUnattendedRemover	12/7/2025 9:39 PM	Application	410 KB
GoToResolveUnattendedUi	12/7/2025 9:39 PM	Application	410 KB
GoToResolveUnlock32.dll	12/7/2025 9:39 PM	Application exten...	533 KB
GoToResolveUnlock64.dll	12/7/2025 9:39 PM	Application exten...	699 KB
legacy.dll	12/7/2025 9:39 PM	Application exten...	591 KB
libcrypto-3.dll	12/7/2025 9:39 PM	Application exten...	4,318 KB
libcrypto-3-x64.dll	12/7/2025 9:39 PM	Application exten...	5,899 KB
LibGoToResolve.dll	12/7/2025 9:39 PM	Application exten...	19,930 KB
libssl-3.dll	12/7/2025 9:39 PM	Application exten...	1,130 KB
libssl-3-x64.dll	12/7/2025 9:39 PM	Application exten...	1,440 KB
LMIFilterHook32.dll	12/7/2025 9:39 PM	Application exten...	131 KB
LMIFilterHook64.dll	12/7/2025 9:39 PM	Application exten...	146 KB
LMInputHook32.dll	12/7/2025 9:39 PM	Application exten...	129 KB
LMInputHook64.dll	12/7/2025 9:39 PM	Application exten...	142 KB
Imiscrhook32.dll	12/7/2025 9:39 PM	Application exten...	159 KB
Imiscrhook64.dll	12/7/2025 9:39 PM	Application exten...	202 KB
LMISupport7x32.dll	12/7/2025 9:39 PM	Application exten...	395 KB
LMISupport7x64.dll	12/7/2025 9:39 PM	Application exten...	442 KB
LMISupportM32	12/7/2025 9:39 PM	Application	300 KB
LMISupportM64	12/7/2025 9:39 PM	Application	345 KB

Figure 4: Installed Application Folder

Installed Path Folder:

C:\Program Files (x86)\GoTo Resolve Unattended\6293827109194426909\

Accessing Restart Manager

The Rstrtmgr DLL (Restart Manager) is being loaded by an uncommon process. This library has been used during ransomware campaigns to kill processes that would prevent file encryption by locking them (e.g. Conti ransomware, Cactus ransomware). It has also recently been seen used by the BiBi wiper for Windows. It could also be used for anti-analysis purposes by shutting down specific processes.

```
.....F.....
.....<...~...p...\...H.....t
...s...9...o.....
...l.....StgOpenStorage..ole32
.dll...RmRegisterResources...RmGetL
ist...RmStartSession....RmEndSessio
n...Rstrtmgr.DLL...VerSetConditionM
ask...NtQuerySystemInformation....R
tlNtStatusToDosError.ntdll.dll.^Pa
thIsDirectoryEmptyW._.PathIsDirecto
ryW..SHLWAPI.dll...CreateDirectoryW
....SizeofResource....GetCommandLin
eW...GetModuleFileNameW....FormatMe
ssageW..w.GetLastError..U.lstrcatW.
...LockResource....CloseHandle...Lo
adResource....FindResourceW.+SetCu
```

Figure 5: RestartManager DLL as seen in the sample

Bundled File:

When the sample is unzipped, we get a bundled file with the sample.

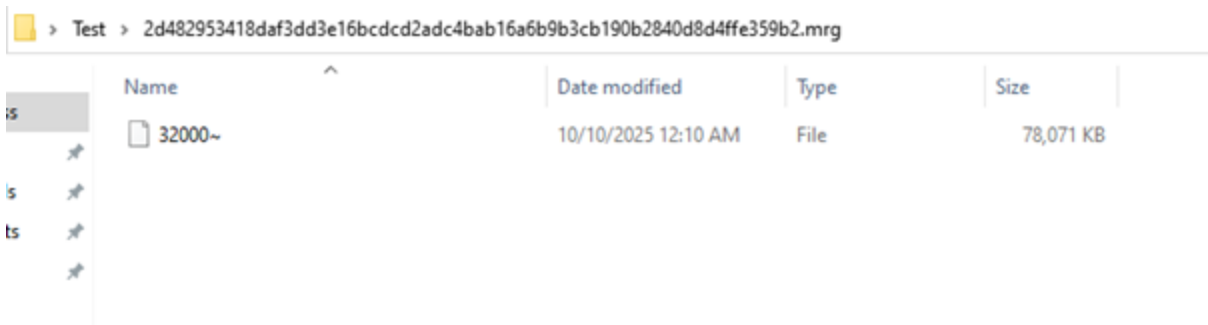


Figure 6: Bundled File

File Info->

Name: 32000~

MD5: d37158f86aa1d35a0ce4a92e2fcb3f74

SHA-1: 170b69d9d1cd1c9daf528fb7a321a21ccad32982

SHA-256: 7da4fff270d5716556c27ccfe231637638e498c004413d362b9d19a76e80716d

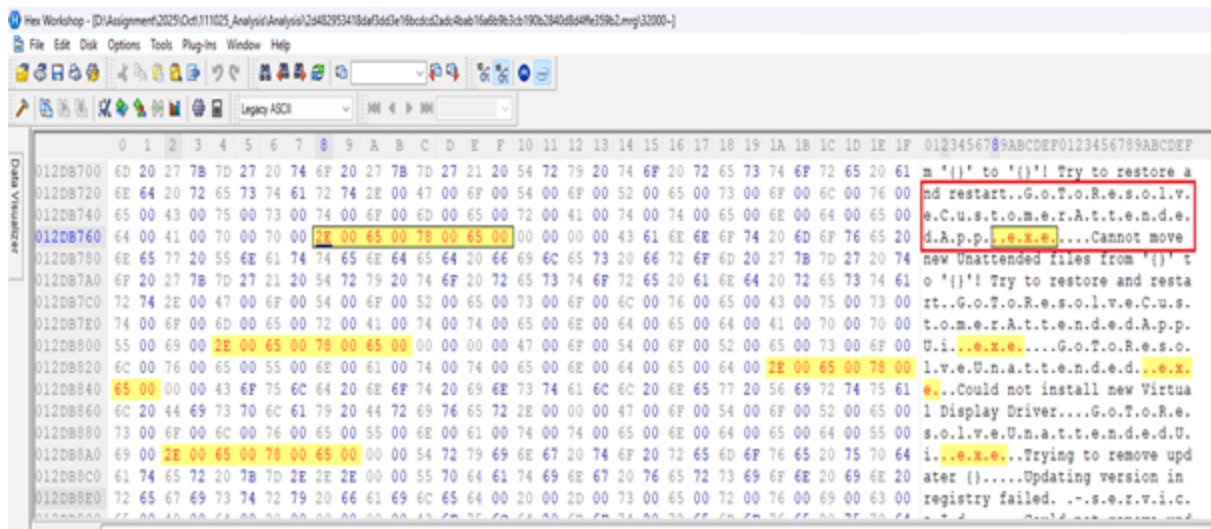


Figure 7: Some EXE names in bundled file

This bundled file contains most of the instructions for installation and management of GoToResolve app.

Detection by UltraAV:

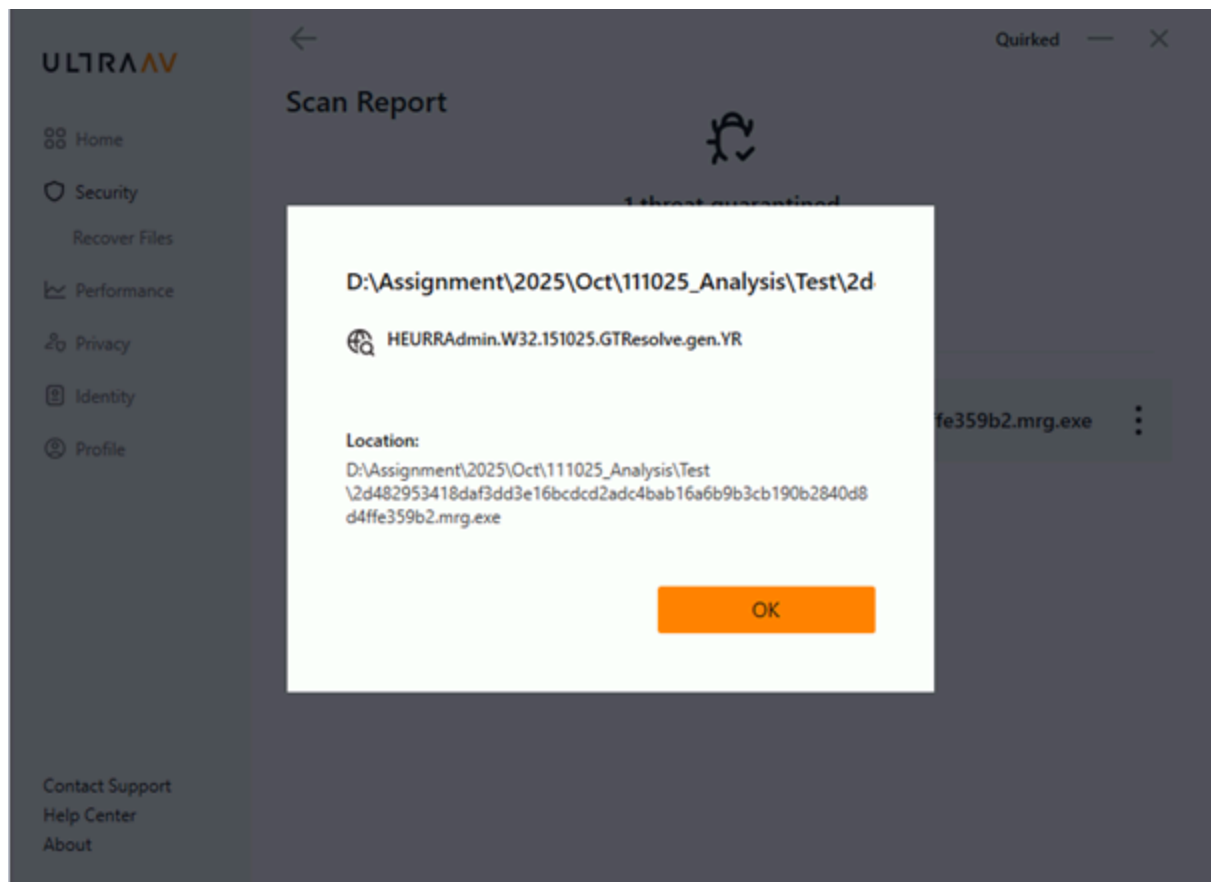


Figure 8: Sample Detected by UltraAV

Conclusion:

- The analysed sample, detected as HEURRemoteAdmin.GoToResolve.gen, is associated with the GoTo Resolve Unattended Access application, a legitimate remote administration tool that can be classified as a Potentially Unwanted Application (PUA) in uncontrolled environments.
- Static analysis confirmed that the executable is digitally signed by GoTo Technologies USA, LLC, indicating a legitimate origin; however, a valid digital signature does not eliminate the risk of misuse.
- Dynamic analysis revealed that the sample installs and executes background threads silently, establishing unattended remote access functionality without clear user interaction or explicit consent.
- The application installs itself persistently under C:\Program Files (x86)\GoTo Resolve Unattended\, indicating long-term presence on the affected system.
- The loading of the Restart Manager (Rstrtmgr.dll) by the sample is notable, as this library has been observed in ransomware and wiper malware to terminate interfering processes, suggesting potential abuse for anti-analysis or operational control.
- While no direct malicious payload was observed during execution, the tool's remote access capabilities present a significant attack surface that can be exploited by threat actors to deploy secondary malware, maintain persistence, or conduct unauthorized system control.
- The detection of the sample by UltraAV further supports its classification as a security risk in enterprise and personal computing environments.
- Based on the observed behaviors and associated risks, the sample should be treated as a PUA with elevated threat potential, warranting removal unless explicitly authorized, monitored, and managed by organizational security policies.
- It is recommended that organizations implement application whitelisting, endpoint monitoring, and user awareness controls to prevent the unauthorized deployment of similar remote administration tools.

Indicators of Compromise (IOC):

MD5: 6717e7dc73fb1d4febb1da10bbcb41c5

SHA-1: 5fb6ae10d167ada29f50b3693af18a961b961057

SHA-256: 2d482953418daf3dd3e16bcdcd2adc4bab16a6b9b3cb190b2840d8d4ffe359b2

Imphash: f8e4a22bcb1b836585534b93f63c1414