We observed a wide variety of Remcos configurations, most of which configured keylogging and screenshot theft capabilities as well as duckdns dynamic DNS updates. The following example is a screenshot of a Remcos configuration:

```
..\%Public%\Libraries\easinvoker.exe
```

As an anti-detection measure, DBatLoader creates a mock trusted directory to disguise the execution of the malware. The malicious installer also creates a system service named `KDECO`. This service loads the malicious `easinvoker.exe` into memory, which in turn executes Remcos through process injection. The `easinvoker.exe` script first loads the `netutils.dll` DLL, which hijacks system calls to DLL hijacking enabling the execution of the malicious `KDECO.bat` script.

This directory ensures this criteria is fulfilled. As an anti-detection measure, DBatLoader creates a mock trusted directory to disguise the execution of the malware. The malicious installer also creates a system service named `KDECO`. This service loads the malicious `easinvoker.exe` into memory, which in turn executes Remcos through process injection. The `easinvoker.exe` script first loads the `netutils.dll` DLL, which hijacks system calls to DLL hijacking enabling the execution of the malicious `KDECO.bat` script.

To protect against this threat, it is recommended to consider configuring Windows UAC to auto-elevated executable, meaning that Windows automatically elevates this process without issuing an UAC prompt if located in a trusted directory. However, this is not always reliable, and it is recommended to stay vigilant against malicious network requests to public Cloud instances. The use of public Cloud infrastructure for hosting malware is an attestation to this tactic. When it comes to the malware delivery look legitimate, making detection harder for defenders. This tactic is popular amongst cyber criminals and espionage threat actors.

### Conclusion

For administrators:

- Stay vigilant against malicious network requests to public Cloud instances.
- The use of public Cloud infrastructure for hosting malware is an attestation to this tactic. When it comes to the malware delivery look legitimate, making detection harder for defenders. This tactic is popular amongst cyber criminals and espionage threat actors.
- Consider configuring Windows UAC to auto-elevated executable, meaning that Windows automatically elevates this process without issuing an UAC prompt if located in a trusted directory. However, this is not always reliable, and it is recommended to stay vigilant against malicious network requests to public Cloud instances. The use of public Cloud infrastructure for hosting malware is an attestation to this tactic.

### Recommendations for Users and Administrators

- **For Users:**
  - Remain attentive against phishing attempts, educate users to avoid opening attachments from unknown senders, and deploy advanced security measures.
  - Be cautious when handling email attachments that may contain malware.
  - Use antivirus software and keep it up to date.

- **For Administrators:**
  - Stay vigilant against malicious network requests to public Cloud instances.
  - Configure Windows UAC to auto-elevated executable, meaning that Windows automatically elevates this process without issuing an UAC prompt if located in a trusted directory. However, this is not always reliable, and it is recommended to stay vigilant against malicious network requests to public Cloud instances. The use of public Cloud infrastructure for hosting malware is an attestation to this tactic.
  - Consider using a malware analysis platform to detect and analyze potential threats.

### DBatLoader and Remcos Phishing Emails

We observed download links to Microsoft OneDrive and Google Drive sites (under the drive.google.com and onedrive.live.com domains) with varying permissions. When a user decompresses the attachment and runs the executable within, DBatLoader downloads and executes an obfuscated second-stage payload, which is typically a RAT. The RAT, in turn, downloads and executes additional malware. The malware delivery look legitimate, making detection harder for defenders. This tactic is popular amongst cyber criminals and espionage threat actors.

### Example Remcos Configuration

```
..\%Public%\Libraries\easinvoker.exe
```

As an anti-detection measure, DBatLoader creates a mock trusted directory to disguise the execution of the malware. The malicious installer also creates a system service named `KDECO`. This service loads the malicious `easinvoker.exe` into memory, which in turn executes Remcos through process injection. The `easinvoker.exe` script first loads the `netutils.dll` DLL, which hijacks system calls to DLL hijacking enabling the execution of the malicious `KDECO.bat` script.

This directory ensures this criteria is fulfilled. As an anti-detection measure, DBatLoader creates a mock trusted directory to disguise the execution of the malware. The malicious installer also creates a system service named `KDECO`. This service loads the malicious `easinvoker.exe` into memory, which in turn executes Remcos through process injection. The `easinvoker.exe` script first loads the `netutils.dll` DLL, which hijacks system calls to DLL hijacking enabling the execution of the malicious `KDECO.bat` script.

To protect against this threat, it is recommended to consider configuring Windows UAC to auto-elevated executable, meaning that Windows automatically elevates this process without issuing an UAC prompt if located in a trusted directory. However, this is not always reliable, and it is recommended to stay vigilant against malicious network requests to public Cloud instances. The use of public Cloud infrastructure for hosting malware is an attestation to this tactic. When it comes to the malware delivery look legitimate, making detection harder for defenders. This tactic is popular amongst cyber criminals and espionage threat actors.

### Conclusion

For administrators:

- Stay vigilant against malicious network requests to public Cloud instances.
- The use of public Cloud infrastructure for hosting malware is an attestation to this tactic. When it comes to the malware delivery look legitimate, making detection harder for defenders. This tactic is popular amongst cyber criminals and espionage threat actors.
- Consider configuring Windows UAC to auto-elevated executable, meaning that Windows automatically elevates this process without issuing an UAC prompt if located in a trusted directory. However, this is not always reliable, and it is recommended to stay vigilant against malicious network requests to public Cloud instances. The use of public Cloud infrastructure for hosting malware is an attestation to this tactic.

### Recommendations for Users and Administrators

- **For Users:**
  - Remain attentive against phishing attempts, educate users to avoid opening attachments from unknown senders, and deploy advanced security measures.
  - Be cautious when handling email attachments that may contain malware.
  - Use antivirus software and keep it up to date.

- **For Administrators:**
  - Stay vigilant against malicious network requests to public Cloud instances.
  - Configure Windows UAC to auto-elevated executable, meaning that Windows automatically elevates this process without issuing an UAC prompt if located in a trusted directory. However, this is not always reliable, and it is recommended to stay vigilant against malicious network requests to public Cloud instances. The use of public Cloud infrastructure for hosting malware is an attestation to this tactic.
  - Consider using a malware analysis platform to detect and analyze potential threats.

### DBatLoader and Remcos Phishing Emails

We observed download links to Microsoft OneDrive and Google Drive sites (under the drive.google.com and onedrive.live.com domains) with varying permissions. When a user decompresses the attachment and runs the executable within, DBatLoader downloads and executes an obfuscated second-stage payload, which is typically a RAT. The RAT, in turn, downloads and executes additional malware. The malware delivery look legitimate, making detection harder for defenders. This tactic is popular amongst cyber criminals and espionage threat actors.

### Example Remcos Configuration

```
..\%Public%\Libraries\easinvoker.exe
```

As an anti-detection measure, DBatLoader creates a mock trusted directory to disguise the execution of the malware. The malicious installer also creates a system service named `KDECO`. This service loads the malicious `easinvoker.exe` into memory, which in turn executes Remcos through process injection. The `easinvoker.exe` script first loads the `netutils.dll` DLL, which hijacks system calls to DLL hijacking enabling the execution of the malicious `KDECO.bat` script.

This directory ensures this criteria is fulfilled. As an anti-detection measure, DBatLoader creates a mock trusted directory to disguise the execution of the malware. The malicious installer also creates a system service named `KDECO`. This service loads the malicious `easinvoker.exe` into memory, which in turn executes Remcos through process injection. The `easinvoker.exe` script first loads the `netutils.dll` DLL, which hijacks system calls to DLL hijacking enabling the execution of the malicious `KDECO.bat` script.

To protect against this threat, it is recommended to consider configuring Windows UAC to auto-elevated executable, meaning that Windows automatically elevates this process without issuing an UAC prompt if located in a trusted directory. However, this is not always reliable, and it is recommended to stay vigilant against malicious network requests to public Cloud instances. The use of public Cloud infrastructure for hosting malware is an attestation to this tactic. When it comes to the malware delivery look legitimate, making detection harder for defenders. This tactic is popular amongst cyber criminals and espionage threat actors.