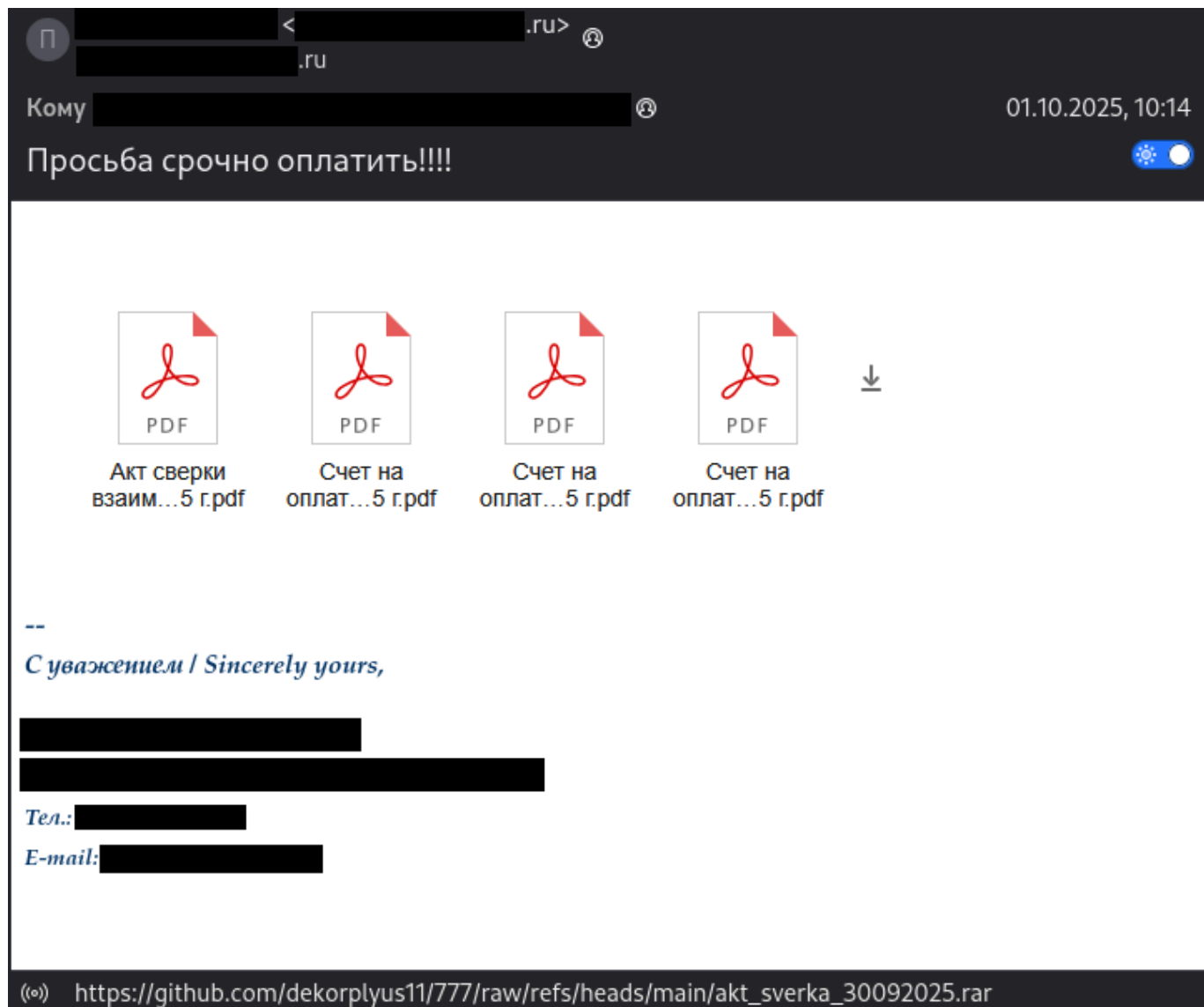


Неугомонный VasyGrek: F6 изучила атаки злоумышленника в августе-ноябре 2025 года

f6.ru/blog/vasygrek-new-attacks-2025

November 25, 2025



В июле 2024 года был опубликован блог об исследовании специалистами Threat Intelligence компании F6 активности [VasyGrek и его сотрудничестве с продавцом ВПО Mr.Burns](#). После публикации F6 VasyGrek прекратил сотрудничество с этим поставщиком вредоносных программ.

Аналитики департамента киберразведки F6 продолжили отслеживать атаки злоумышленника, который не прекращал свою активность и осуществлял новые фишинговые рассылки в адрес российских организаций. Целью киберпреступника был доступ к конфиденциальным данным для их дальнейшего использования. Как правило, VasyGrek применял вредоносное ПО, разработанное пользователем хак-форумов PureCoder. Также специалисты F6 заметили, что в некоторых атаках в дополнение к ВПО от PureCoder шел шифровальщик [Pay2Key](#).

В новом блоге аналитики F6 рассказали об инструментах и атаках VasyGrek в **августе-ноябре 2025** года с техническими деталями и индикаторами компрометации.

VasyGrek и его инвентарь

VasyGrek (Fluffy Wolf) — русскоязычный злоумышленник, атакующий российские компании из различных сфер экономики как минимум с 2016 года. Кибератаки проводились с использованием вредоносного программного обеспечения через рассылки на бухгалтерскую тематику и фишинговые домены, которые, как правило, имитировали сайты финансовых организаций.

В разные периоды VasyGrek использовал вредоносные модификации легитимных программ для удаленного управления RMS и TeamViewer, разработанные злоумышленником Mr.Burns и классифицируемые как семейство BurnsRAT, а также стилеры RedLine и META, троян AveMaria и ВПО разработчика PureCoder (PureCrypter, PureHVNC (PureRAT), PureLogs Stealer).

После публикации в июле 2024 года блога F6 Threat Intelligence с исследованием активности злоумышленника и его сотрудничества с продавцом ВПО Mr.Burns, VasyGrek перестал использовать BurnsRAT, но в целом цепочки заражений из атак злоумышленника с того момента по октябрь 2025 года не претерпевали существенных изменений. Он по-прежнему рассылал фишинговые письма, в которых вредоносный файл доставлялся потенциальной жертве как в виде вложения, так и по ссылкам на репозитории GitHub или на домены, регистрируемые VasyGrek. Вредоносный файл представлял собой архив с исполняемым файлом внутри или сразу исполняемый файл ВПО PureCrypter, которое имеет возможность доставлять на систему жертвы последующие стадии и внедрять полезные нагрузки в нужные процессы. Стадии могли как загружаться с внешних ресурсов, так и храниться локально в зашифрованном виде. VasyGrek отдавал предпочтение инструментам от разработчика PureCoder (PureHVNC, PureLogs Stealer), но иногда к ним в дополнение шла нетипичная полезная нагрузка. Например, в ряде случаев было обнаружено ВПО Pay2Key.

В ноябре было замечено изменение цепочек заражения злоумышленника: в качестве вложений писем вместо архивов с исполняемыми файлами внутри стали использоваться архивы с файлами BAT и VBS. В цепочке с файлом VBS конечной полезной нагрузкой было ВПО PureHVNC, но для его доставки вместо привычного PureCrypter использовался другой загрузчик. Подробный разбор новой цепочки будет рассмотрен в статье в соответствующем разделе.

Ниже представлена краткая справка по инструментарию, используемому в атаках VasyGrek в августе-ноябре 2025 года.

PureCrypter, PureHVNC и PureLogs Stealer – инструменты, разработанные и продаваемые пользователем хак-форумов с псевдонимом PureCoder.

PureCrypter – ВПО, продаваемое с марта 2021 года, которое было классифицировано как Downloader. В его функциональные возможности входит загрузка/извлечение следующих стадий, а также запуск определенных стадий в контексте собственного процесса.

ВПО **PureHVNC** начало продаваться на хак-форумах с декабря 2021 года. PureHVNC позволяет собирать телеметрию, сохраненные данные приложений ПК, отправлять их на подконтрольный злоумышленнику сервер, закрепляться в системе, загружать/исполнять в памяти сторонние модули.

PureLogs – вредоносное программное обеспечение класса stealer, разработанное на .NET. Начало продаж – июнь 2022 года. Функционал ВПО позволяет осуществлять хищение данных браузера, криптокошельков и различных приложений, установленных в системе, таких как FTP-клиенты, почтовые клиенты и VPN.

Pay2Key – вымогательский сервис, активизировавшийся с начала 2025 года на теневых форумах, распространяемый как RaaS (Ransomware as a Service) и построенный на базе известного шифровальщика Mimic. Более подробная информация о данном сервисе доступна в [блоге](#) F6.

Атаки в августе-ноябре 2025 года

Приведем детали и индикаторы компрометации из атак VasyGrek за август-ноябрь 2025 года.

За рассматриваемый период VasyGrek атаковал российские компании из следующих сфер деятельности: промышленность, строительство, энергетика, сельское хозяйство, безопасность, торговля, финансы, информационные технологии, медиа, развлечения.

В качестве отправителей писем фигурировали электронные адреса с доменами верхнего уровня .ru, .su, что было сделано злоумышленником с целью имитации активности от имени существующих российских организаций.

На скриншотах ниже представлены примеры разных писем злоумышленника: со ссылкой на вредоносный файл, хранящийся на GitHub, со ссылкой на вредоносный файл, хранящийся на домене VasyGrek, а также с вредоносным вложением. В случаях писем со ссылками переход по ним осуществляется при клике на изображения с иконками файлов.

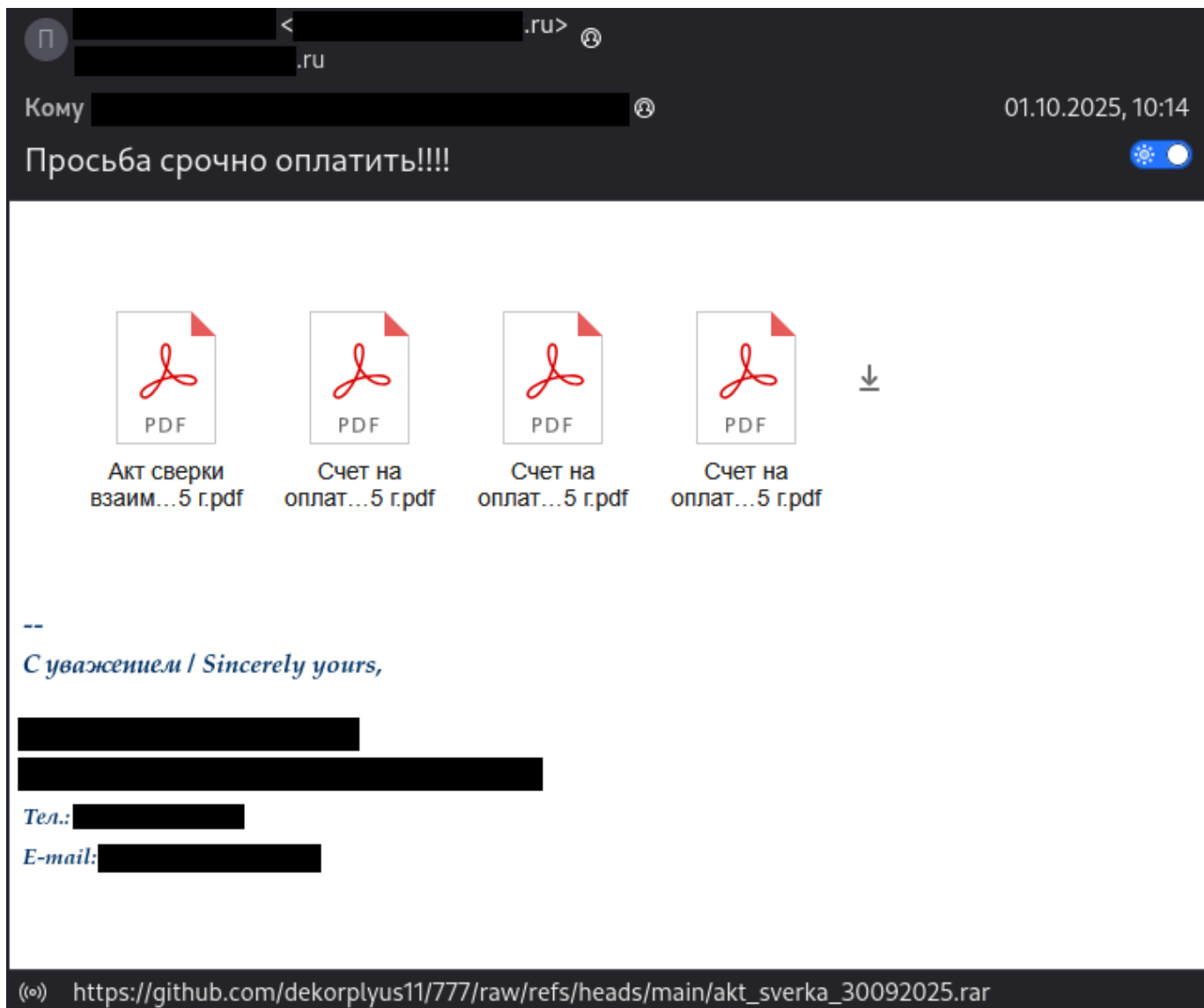


Рис. 1 – Фишинговое письмо со ссылкой на вредоносный архив, хранящийся на GitHub

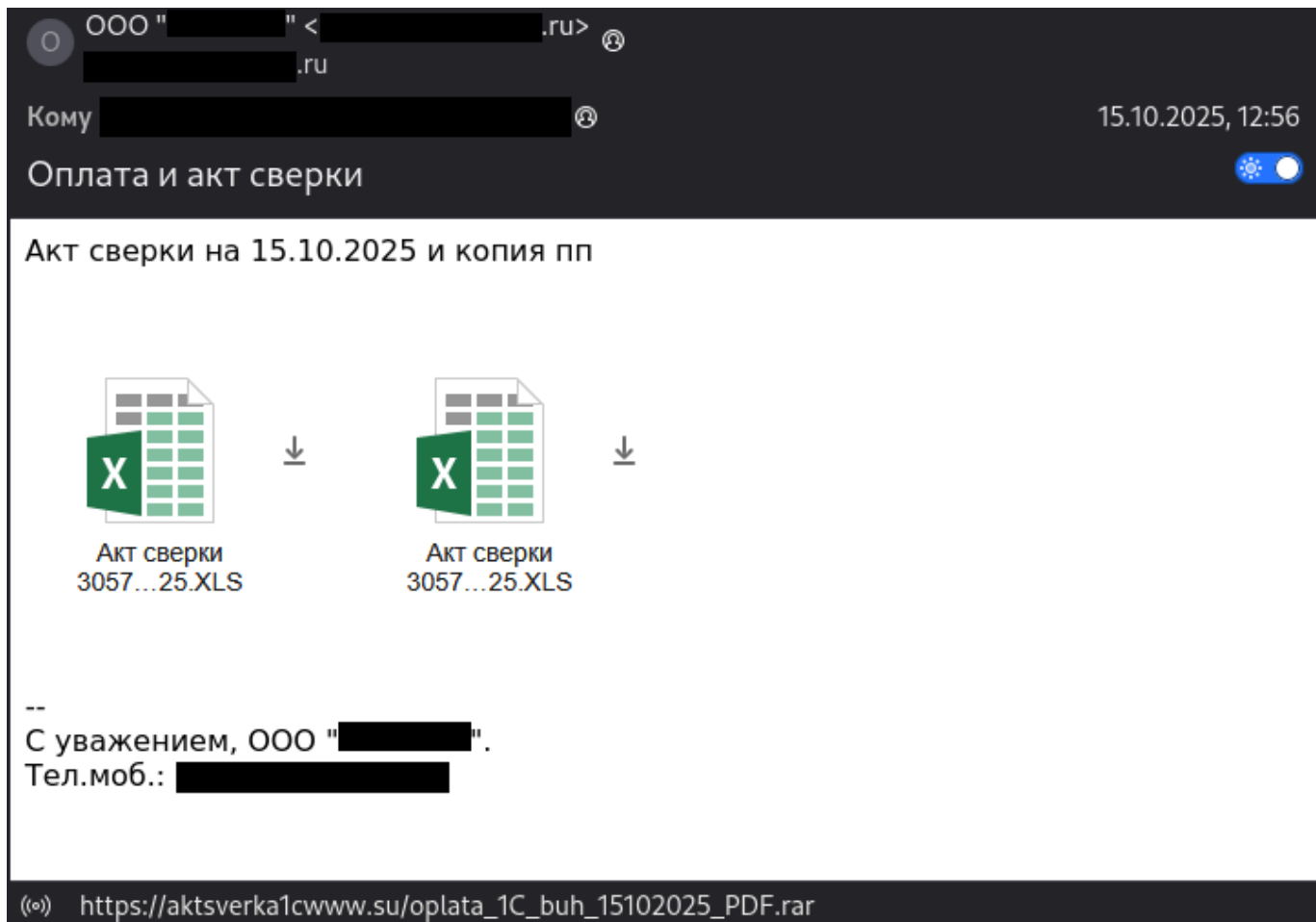


Рис. 2 – Фишинговое письмо со ссылкой на вредоносный архив, хранящийся на домене VasyGrek

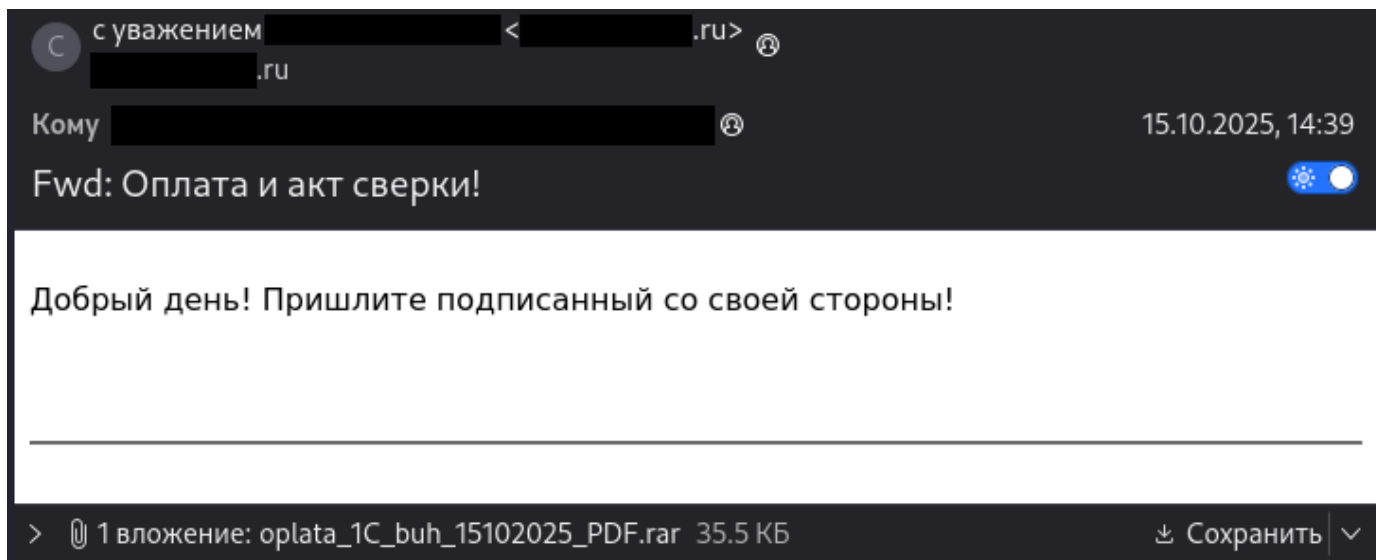


Рис. 3 – Фишинговое письмо с вредоносным архивом во вложении

С августа по ноябрь 2025 года злоумышленник продолжал использовать ранее зарегистрированные и регистрировал новые домены, с которых в ходе атак загружалось ВПО. Для VasyGrek характерны определенные паттерны поведения при регистрации новых доменов. Это позволило аналитикам Threat Intelligence F6 создать правила на сетевую инфраструктуру

злоумышленника и выявить регистрируемые домены еще до начала их использования в атаках. На скриншоте ниже представлен граф связей доменов VasyGrek с уникальными регистрационными данными.

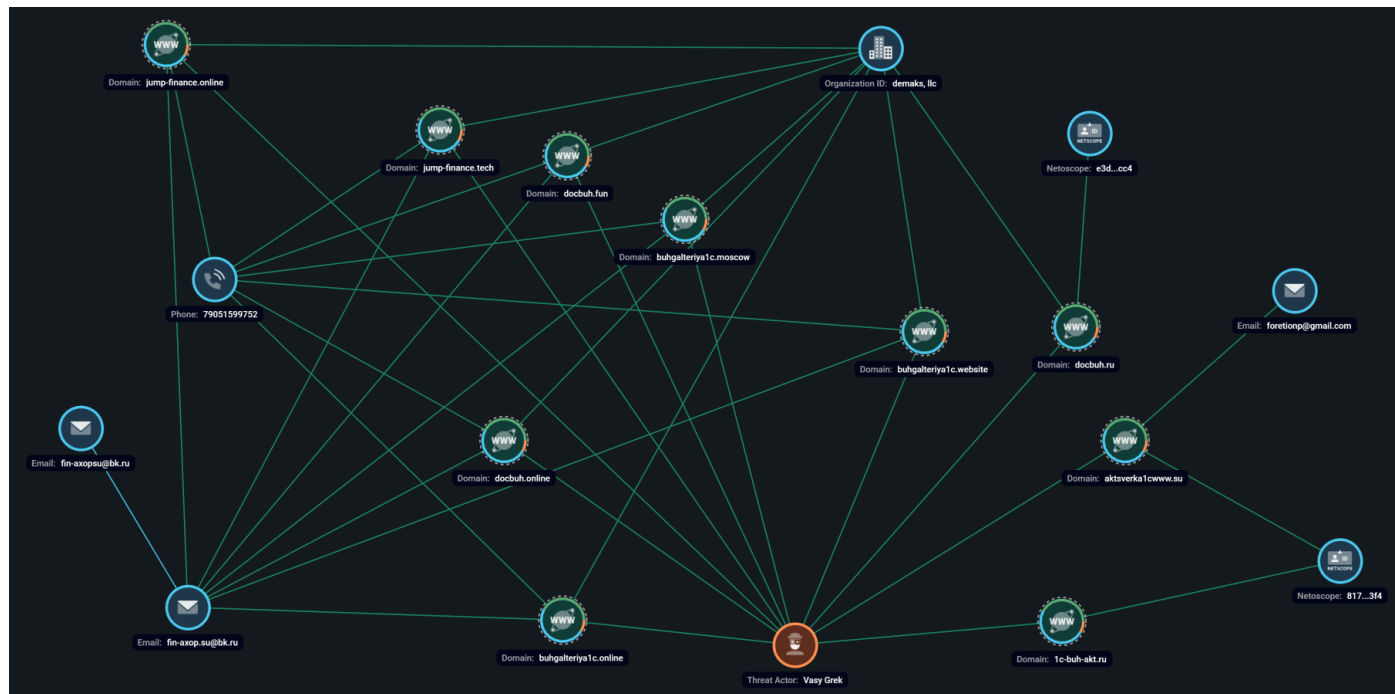


Рис. 4 – Графовый анализ инфраструктуры VasyGrek

Также аналитики F6 заметили, что на доменах злоумышленника размещались страницы, замаскированные под ресурсы с бухгалтерскими услугами. Ниже представлен скриншот страниц, которые были обнаружены в сентябре 2025 года на доменах buhgalteriya1c[.]moscow, buhgalteriya1c[.]website, buhgalteriya1c[.]online.

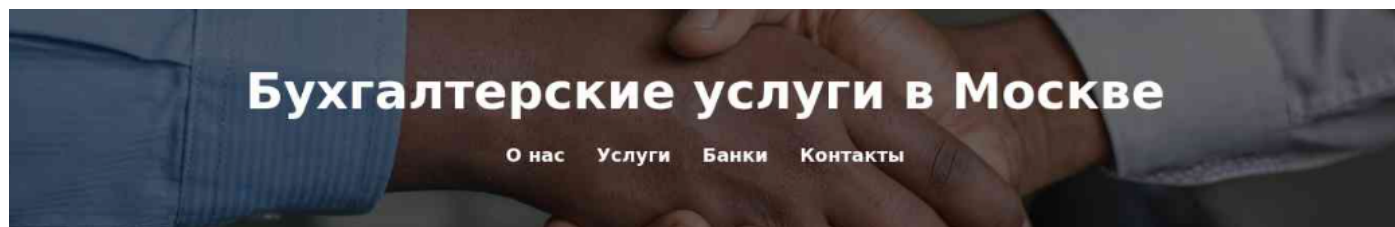


Рис. 5 – Скриншот страницы с мимикрией под бухгалтерские услуги на доменах VasyGrek

Кроме того, за рассматриваемый период на доменах злоумышленника были замечены страницы, имитирующие известные компании из финансовой сферы (платежи, бухгалтерские услуги), ранее также встречались банки.

В качестве C2 VasyGrek почти год использовал IP-адрес 195[.]26[.]227[.]209 (с декабря 2024), но в конце октября 2025 года сменил его на 195[.]26[.]225[.]113.

Анализ одного из вредоносных семплов VasyGrek на Malware Detonation Platform от компании F6 доступен по ссылке: <https://detonation.f6.security/NWe64exGNhxC8PZyVRn7xiFug/>

В данном анализе загрузчик PureCrypter помимо привычной для VasyGrek полезной нагрузки PureHVNC и PureLogs Stealer доставляет на устройство жертвы шифровальщик Pay2Key (enc-build.exe).

Анализ новой цепочки атаки VasyGrek от 13 ноября 2025 года

Рассмотрим измененную цепочку атаки, в которой в качестве вложения письма вместо архива с исполняемым файлом внутри стал использоваться архив с файлом VBS. Цепочка заражения выглядит следующим образом:

1. Запуск файла акт_сверки_PDF.vbs.
2. Загрузка изображения с `hxxps://vvvpmscvtlhcyjbybrwjg[.]supabase[.]co/storage/v1/object/public/sudo/image.jpg?12711343`. Также попытка загрузки такого же изображения с ресурса `hxxps://raw[.]githubusercontent[.]com/ahedsalah88-cyber/file/30ea07d56404ec5d97060cb9719acb756b2ed1f1/pic.jpg?12711343`, однако на момент анализа файл по данной ссылке был недоступен.
3. Из изображения извлекается зашифрованная полезная нагрузка. Ее границы определены заголовками `<<BASE64_START>>` и `<<BASE64_END>>`. После извлечения нагрузки символы `'h@'` заменяются на `'d'` и происходит дешифровка base64. В результате получается .NET-сборка.
4. Внедрение дешифрованной нагрузки в текущий процесс с помощью `System.Reflection.Assembly::Load()`.
5. Вызов из .NET-нагрузки метода `testpowershell.Noaaaaaasdme` с 6 аргументами: `txt.daolpu52021131CV/ur.tka-hub-c1//:s, 2, vbchosting.exe, RegAsm, 0, x86`.
6. NET-нагрузка создает запись в реестре по пути `HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce` для однократного запуска `wscript.exe` с аргументом `C:\ProgramData\vbchosting.exe.vbs` — этого файла еще не существует.
7. NET-нагрузка создает 2 новых процесса `powershell.exe` со следующими аргументами:

принудительное завершение процессов `RegAsm.exe`, `Vbc.exe` и `MsBuild.exe`:

`"Start-Process cmd.exe -ArgumentList '/c taskkill /IM RegAsm.exe /F & taskkill /IM Vbc.exe /F & taskkill /IM MsBuild.exe /F'`

проверка текущей директории: если это не `ProgramData`, то выполняется копирование изначального `акт_сверки_PDF.vbs`, но с новым именем `vbchosting.exe.vbs` в директорию `C:\ProgramData`. Данный файл используется для закрепления в системе (автозагрузка через реестр). Команды отработали и процессы завершились:

```
-WindowStyle Hidden if ((Get-Location).Path -ne 'C:\ProgramData' ) { (Get-ChildItem *.vbs | Sort-Object CreationTime -Descending | Select-Object -First 1) | Copy-Item -Destination 'C:\ProgramData\vbchosting.exe.vbs' -Force }
```

- 8. NET-нагрузка загружает новую полезную нагрузку с `hxxps://1c-buh-akt[.]ru/VC13112025upload.txt`.
- 9. Дешифровка новой нагрузки (`reverse string + base64`). В результате получается новая .NET-сборка: `.exe` и зависимая `.dll`.
- 10. Запуск легитимного исполняемого файла `RegAsm.exe` — включен в состав стандартного .NET-пакета.
- 11. Внедрение новой расшифрованной нагрузки в процесс `RegAsm.exe`.
- 12. Запуск внедренной нагрузки. Запускается `.exe`-нагрузка, которая использует `.dll`-библиотеку. По результатам динамического анализа и анализа полученной конфигурации специалистами Threat Intelligence F6 был сделан вывод, что полезная нагрузка, внедренная в процесс `RegAsm.exe` — это `PureHVNC (PureRAT)`. В конфигурации указаны IP C2, имя мьютекса, номера портов, SSL-сертификат.

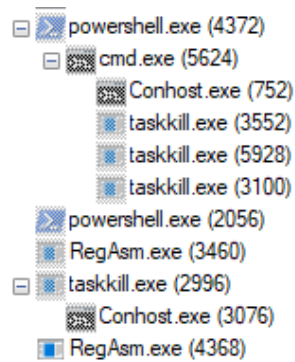


Рис. 6 — Дерево процессов

Name	Value
value	{jAjXX3KxuyAseM5iRCG.h63dhyK0tvhEs78kfo5}
A1VUQ4KvSi	"de88c7d9a8e7"
hlcUnxCU8a	"MIIE5jCCAs6gAwIBAgIQAMM7hmuLoKJGKtiWfJCdTANBgkqhkiG9w0BAQ0FADAUMRIwEAYDVQQDDAIOZndxdWt2eWUwBcNMjQ...
jf6UAvDDpv	true
kVcURvnt1i	true
IsyU4FsR0b	"avtoprint.exe"
oPTUyZyR6J	false
oQrkzBkAaa	Count = 1
[0]	"195.26.225.113"
Raw View	
PFmU9dFVlq	Count = 6
[0]	56001
[1]	56002
[2]	56003
[3]	33523
[4]	2103
[5]	14503
Raw View	
pjPUiKyyCd	"13112025"
xf4UcAhsgQ	"LOCALAPPDATA"

Рис. 7 — Конфигурация PureHVNC

Стоит отметить, что в данной атаке использовался загрузчик, классифицируемый нами как powershell stego downloader. Он использовался разными атакующими, в частности, неоднократно был замечен в арсенале группы Sticky Werewolf. Группа Sticky Werewolf использовала его для доставки полезных нагрузок Ozone RAT и Darktrack и инжектировала их в процесс RegAsm.exe. В данном же случае атрибуция была проведена к VasyGrek на основе формата фишингового письма, связи ВПО с доменом, зарегистрированным VasyGrek, а также по конечной полезной нагрузке — PureHVNC.

Выводы

VasyGrek — пример многолетней угрозы, продолжающий осуществлять кибератаки и взаимодействовать с распространителями различного ВПО. Его действия носят массовый характер и направлены на российские организации из различных сфер. В интересах компаний ознакомиться с деталями этой угрозы и принять меры для защиты от потенциальных атак. Также рекомендуем проводить регулярные обучения сотрудников для повышения уровня их киберграмотности и использовать современные средства для выявления, предотвращения и проактивного поиска киберугроз.

Рекомендуем ознакомиться с решениями от F6: [Business Email Protection](#), [Managed XDR](#) и [Threat Intelligence](#).

Индикаторы компрометации

Темы писем:

Акты! Для бухгалтерии!!!

Акт сверки на 08.08.2025

Fwd: Акт сверки ! Не сходится с вами

Fwd: Акты

Fwd: Акт сверки ! Срочно

Уточнение платежа

Fwd[2]: Копия пп от 22.08.2025

Fwd: Акт сверки

На подпись Акт сверки

Fwd: На подпись Акт сверки

Fwd: Платежное поручение! Пришлите со своей стороны акт сверки

Fwd: Платежка

Документы (акт сверки, договор и кория пп)

Fwd: Документы (акт сверки, договор и кория пп)

Fwd: Акт сверки! Оплатите задолженность!!!!

Fwd[2]: Акт сверки на 01.10.2025 За вами задолженность !

Просьба срочно оплатить!!!!

Акт сверки на подпись! СРОЧНО надо подписать!!!

Акт сверки взаимозачетов на 07.10.2025

Fwd: Копия пп и акт сверки

Копия п/п от 14.10.2025

Оплата и акт сверки

Fwd: Платежное поручение и акт сверки!!!!!!!!

Fwd: Оплата и акт сверки!

Сверка! Надо подписать срочно!!!

Счет и доверенность!

Fwd: Счет и УПД

Акт сверки на подпись

Fwd: Акт сверки срочно подписать!!!!!!

Fwd: платежное поручение возврат

Fwd[2]: Копия пп и акт сверки

Акт сверки

Fwd: Счет на оплату!

акт_сверки 13/11/2025

Акт сверки (счет на оплату задолженности)

Счет на оплату задолженности! (Акт сверки)

Fwd: Счет на оплату задолженности (Акт сверки)

FW: Счет на оплату задолженности (Акт сверки)

Домены:

jump-finance[.]tech

jump-finance[.]online

buhgalteriya1c[.]website

buhgalteriya1c[.]moscow

buhgalteriya1c[.]online

docbuh[.]fun

docbuh[.]online

docbuh[.]ru

aktsverka1cwww[.]su

1c-buh-akt[.]ru

URLs:

hxxps://jump-finance[.]tech/buh_1C_Doc_0487563232_www_PDF.rar

hxxps://jump-finance[.]tech/PDF_doc_1C_Buh04866266dwde5f6rfvrregfe5fef.rar

hxxps://jump-finance[.]tech/kopiya_pp_Buh_1C_PDF.rar

hxxps://jump-finance[.]online/akt_sverki_1C_9856665_PDF.rar

hxxps://jump-finance[.]tech/doc_028389932ddfp34r4jkk32e2_www_pdf.rar

hxxps://github[.]com/Mts123stm/22081/raw/refs/heads/main/doc_028389932ddfp34r4jkk32e2_www_pdf.rar

hxxps://github[.]com/zverdanya24/buh/raw/refs/heads/main/1C_akt_Buh_27082025_PDF.rar

hxxps://buhgalteriya1c[.]moscow/akt_BUH_1C_PDF.rar

hxxps://jump-finance[.]tech/doc_1C_akt_085698554_PDF.pif

hxxps://jump-finance[.]tech/panel/uploads/lpgeyghzc.pdf

hxxps://buhgalteriya1c[.]moscow/encryptor.exe

hxxps://buhgalteriya1c[.]moscow/panel/uploads/Afisr.mp3

hxxps://github[.]com/zverdanya24/buh/raw/refs/heads/main/vnc27krip.exe

hxxps://raw[.]githubusercontent[.]com/zverdanya24/buh/refs/heads/main/vnc27krip.exe

hxxps://buhgalteriya1c[.]online/1C_doc_17092025_PDF.pif

hxxps://buhgalteriya1c[.]online/doc_18092025_kopiya_PDF_www.rar

hxxps://buhgalteriya1c[.]website/doc_26092025_1C_655d5fsdfs_PDF.rar

hxxps://github[.]com/dekorplyus11/777/raw/refs/heads/main/akt_sverka_30092025.rar

hxxps://docbuh[.]ru/kopiya_doc_07102025_dfdfsf5rew5rgr5grew_PDF.rar

hxxps://aktsverka1cwww[.]su/oplata_1C_buh_15102025_PDF.rar

hxxps://1c-buh-akt[.]ru/doc_21102025_kopiya_1C_PDF.rar

hxxps://github[.]com/selmatanya/buh2025/raw/refs/heads/main/OOO_1C_kopiya_PP_29_10_2025_PDF.rar

hxxps://aktsverka1cwww[.]su/vc13krips.exe

hxxps://1c-buh-akt[.]ru/panel/uploads/Rqcemqysy.vdf

hxxps://aktsverka1cwww[.]su/vcKrip15.exe

hxxps://1c-buh-akt[.]ru/panel/uploads/Rxqsjpi.mp3

hxxps://1c-buh-akt[.]ru/panel/uploads/Ztdef.mp3

hxxps://aktsverka1cwww[.]su/vcKKKKKKKrip.exe

hxxps://docbuh[.]online/vncserver.exe

hxxps://docbuh[.]online/panel/uploads/Mxbljgkod.vdf

hxxps://docbuh[.]online/panel/uploads/Gndpbnfiwe.vdf

hxxps://docbuh[.]fun/panel/uploads/Wqddwm.mp3

hxxps://docbuh[.]fun/panel/uploads/Ylevwh.wav

hxxps://buhgalteriya1c[.]moscow/panel/uploads/Wcumbhc.wav

hxxps://buhgalteriya1c[.]moscow/panel/uploads/Czgisiy.pdf

hxxps://buhgalteriya1c[.]moscow/panel/uploads/Fyfoxv.vdf

hxxps://buhgalteriya1c[.]online/hostVnc.exe

hxxps://buhgalteriya1c[.]moscow/panel/uploads/Isozfh.wav

hxxps://buhgalteriya1c[.]moscow/panel/uploads/Auvmrm.mp3

hxxps://buhgalteriya1c[.]moscow/panel/uploads/Odfygzi.dat

hxxps://buhgalteriya1c[.]moscow/panel/uploads/Qtyvvt.mp4

hxxps://aktsverka1cwww[.]su/kriptoPRO.exe

hxxps://1c-buh-akt[.]ru/panel/uploads/Jymrjniaz.mp4

hxxps://1c-buh-akt[.]ru/panel/uploads/Ayjjzmx.mp3

hxxps://1c-buh-akt[.]ru/VCKrip.exe

hxxps://1c-buh-akt[.]ru/vckrip.exe

hxxps://1c-buh-akt[.]ru/panel/uploads/Vfkmyhtt.pdf

hxxps://1c-buh-akt[.]ru/panel/uploads/Ubdbvdphmv.mp4

hxxps://1c-buh-akt[.]ru/panel/uploads/Nyltryq.dat

hxxps://vvvpmscvtlhcjbybrwjg[.]supabase[.]co/storage/v1/object/public/sudo/image.jpg?12711343

hxxps://raw[.]githubusercontent[.]com/ahedsalah88-cyber/file/30ea07d56404ec5d97060cb9719acb756b2ed1f1/pic.jpg?12711343

hxxps://1c-buh-akt[.]ru/VC13112025upload.txt

IP-адреса:

195[.]26[.]227[.]209:5403

195[.]26[.]227[.]209:2105

195[.]26[.]227[.]209:1384

195[.]26[.]227[.]209:56001

195[.]26[.]227[.]209:56002

195[.]26[.]227[.]209:56003

195[.]26[.]227[.]209:7203

195[.]26[.]227[.]209:15064

195[.]26[.]227[.]209:22045

195[.]26[.]227[.]209:2803

195[.]26[.]227[.]209:7705

195[.]26[.]227[.]209:5444

195[.]26[.]225[.]113:56001

195[.]26[.]225[.]113:7727

195[.]26[.]225[.]113:55601

195[.]26[.]225[.]113:55602

195[.]26[.]225[.]113:55603

195[.]26[.]225[.]113:33523

195[.]26[.]225[.]113:2103

195[.]26[.]225[.]113:14503

Файловые индикаторы:

Имя файла: doc_028389932ddfp34r4jkk32e2_www_pdf.rar

SHA1: 102c76a8576baf1f93ddeced0065e335d7f0f04f

Имя файла: 1C_akt_Buh_27082025_PDF.rar

SHA1: 2632a376de234c119017e577e8c66172f6f34601

Имя файла: buh_1C_Doc_0487563232_www_PDF.rar

SHA1: e58878f232491553fbcd1809d5a675fc5c455a40

Имя файла: kopiya_pp_Buh_1C_PDF.rar

SHA1: 0e80af7046e8c05f23f3c42e09abc2025d730f8b

Имя файла: PDF_doc_1C_Buh04866266dwde5f6rfvrregfe5fef.rar

SHA1: 8ff581830f0ed9f4690fb083543bc3831ec24e04

Имя файла: kopiyaPP_1C_Buh10092025_PDF.rar

SHA1: 43332536cf84acde72cdaf9fafbadf4422497930

Имя файла: akt_sverki_1C_9856665_PDF.rar

SHA1: b146d7ec50d47d693c7d310450fd39249ee19bc5

Имя файла: akt_BUH_1C_PDF.rar

SHA1: e5c8bfca57de2719dc99a2dead810f9c328ec663

Имя файла: Buh_1C_doc_17092025_PDF.rar

SHA1: 4885ea29cfcedc878169c5ffbbbcd0287cf0f9a7

Имя файла: doc_18092025_kopiya_PDF_www.rar

SHA1: 30fab82c082823c7052c167d46462ffc73e0ea9

Имя файла: doc_26092025_1C_655d5fsdfds_PDF.rar

SHA1: b3da4166134a41a73fa22dbbfd701fc8e9ae03d5

Имя файла: doc_1C_0dfd5fd56fdvf6svcdr_01102025_BUH_PDF.rar

SHA1: e6ae0307c655c1975de037547af1ad8139075287

Имя файла: akt_sverka_1C_PDF.rar

SHA1: 38a9cd803b1de9a378506fe46a30e91804d8f8e1

Имя файла: akt_sverka_30092025.rar

SHA1: 8938abda904c5cee07248b2e764074b0744a5a95

Имя файла: kopiya_doc_07102025_dfdfsfg5rew5rgr5grew_pdf.rar

SHA1: b54bff088b6f456b19be1d7a8e50f5bec825b217

Имя файла: oplata_1C_buh_15102025_PDF.rar

SHA1: 14532f05248f4484abb78fb3b7ece6f59082571d

Имя файла: buh-doc_0595665fdeegrghw6sgagrg6ergesg_PDF.rar

SHA1: ddb02fd8e053c0eca6977225f0684671a42b232a

Имя файла: doc_21102025_kopiya_1C_PDF.rar

SHA1: 23bdd254caf9de4ed036d9271d75eda6f8c3a545

Имя файла: doc_22_10_2025_buhgalteriya_1C_pdf.rar

SHA1: 431b28cdd938495e7d40b6a6a3e736023ce3bf6c

Имя файла: Doc_1C_Buh_0frg5r6gr56eff_PDF.rar

SHA1: 66531fc5ddcf43fc8a145e2b8131cbcacc645ca2

Имя файла: doc_f0ef5re5f6ew56fsfsfs_PDF.rar

SHA1: ba09d21ee55ec671b8132c938c50f2fb997c3966

Имя файла: OOO_1C_kopiya_PP_29_10_2025_PDF.rar

SHA1: 25074b3a30ed36d3d0a4f5ece8191a845e465496

Имя файла: schet_31102025_buh_PDF.rar

SHA1: 21cf3e047b16a2e393f66802623efc158a7e7dd6

Имя файла: doc_1C_buh_31102025_d.rar

SHA1: 2cc660cd3f15fe51cdbda7c41ff5bce7621b7f93

Имя файла: акт_сверки.rar

SHA1: 1139016fca312c0adde1718d745c7e1f9f4198dc

Имя файла: doc_19.11.2025_bank.rar

SHA1: 5c626a094b542517943074401f728c768aeb9d70

Имя файла: vnckriptus.exe

SHA1: 5c6d73fde4a622e5d82dec6530d22f93dabeaafa

Имя файла: doc_1C_akt_085698554_PDF.pif

SHA1: 8979f4be92aa96d9289d0664260852a5ce0fc0d9

Имя файла: vnc27krip.exe

SHA1: 3c8b1525c2b474d4a13a9631d5d1a97b50e269a4

Имя файла: buh_1C_Doc_0487563232_www_PDF.com

SHA1: 02566cbc6c3a29c684f2828df412e403e0ce0ab9

Имя файла: PDF_doc_1C_Buh04866266dwde5f6rfvrregfe5fef.com

SHA1: 2f9847a820632b6077bb477e8afb2623741107ae

Имя файла: VNCKRIPTORS.exe

SHA1: 785d7f52cf47af37d2cb7e9fbde9d746edb96aad

Имя файла: VNcKrip.exe

SHA1: c46ec319fe9e3d3939866c43c28f2be88ec7590c

Имя файла: akt_sverki_1C_9856665_PDF.com

SHA1: 77df4d25256cc68d764f54862b4ac93e5de0e12f

Имя файла: VNCKrip04.exe

SHA1: 7dfc8e50232195d09c8e8cd2656d633fca55e83c

Имя файла: STL1108krip.exe

SHA1: 5a216bef71d8fd3e8244c7b660abc1d63b8ef2b

Имя файла: kopiyaPP_1C_Buh10092025_PDF.com

SHA1: 79735b4e21394aa9aeca90919128de245232daaa

Имя файла: doc_028389932ddfp34r4jkk32e2_www_pdf.com

SHA1: 8c8f60a0e811f63cd2b83e821c6d9376aea40565

Имя файла: vncKrip0408.exe

SHA1: e162ab0fdeff5f2ddb747f508a041853ccd764cb

Имя файла: akt_BUH_1C_PDF.com

SHA1: d680686b6ddefc2cb9fca9463701249096de48e4

Имя файла: 1C_akt_Buh_27082025_PDF.com

SHA1: 0fe1e803bf39a794453e36dafa2593f0cb617ff8

Имя файла: kopiya_pp_Buh_1C_PDF.com

SHA1: d0200719c989096d76003cb8afd62ae3124cda69

Имя файла: VncKrip1808.exe

SHA1: 3746a50425547ce35e761448747559e232864be4

Имя файла: VNCKriptor.exe

SHA1: 502bdf389fc73d135bf144a77704bdf5260c7708

Имя файла: 1C_doc_17092025_PDF.pif

SHA1: f5e1b3bc4478775000ad2ac4b41bd7fa4fba83c2

Имя файла: Buh_1C_doc_17092025_PDF.com

SHA1: 5c16ab36f9ed396eb92aa4e4a1a4191650a9a392

Имя файла: doc_18092025_kopiya_PDF_www.com

SHA1: 54dd082ebb2f55114c304dfb21fe14df7fcfa5e

Имя файла: VNCKRIPT18.exe

SHA1: 7805379668b738a0e283b4b5ab46dbef9fa3ad8c

Имя файла: vnc26krip.exe

SHA1: 4895c53dac84963e5a28b7898e9bb27902afefce

Имя файла: doc_26092025_1C_655d5fsdfs_PDF.com

SHA1: 749519e3fe8550e0a8540d27008476c4eb68cc6b

Имя файла: Акт_Сверки_1C_бухгалтерия_PDF.com

SHA1: c8c9afb9f9d1a8b3c7908bfd572ff5ec62dff5a4

Имя файла: doc_1C_0dfd5fd56fdvf6svcdr_01102025_BUH_PDF.com

SHA1: c29045805d780cbb9b66ee1d4e3c749b679f1a14

Имя файла: akt_sverka_1C_PDF.com

SHA1: 917793fb759a139f1be189e0018853ec0bb04641

Имя файла: StilKripos.exe

SHA1: b582723b6cec4e446a0bf603ff46c20e98c83879

Имя файла: sti3009.exe

SHA1: 2d666aaed718d54fd4d28da683376fb1e8c862ee

Имя файла: doc_1C_buh_01102025_PDF.com

SHA1: 360b7e9fe48fe6c2dcf803f0f664b7e4168323ab

Имя файла: kopiya_doc_07102025_dfdfsfg5rew5rgr5grew_PDF.com

SHA1: d6aeebe05bed4ccdf55c7e48cb3b91c03bf79d1e

Имя файла: VNCKRIP.exe

SHA1: bc736356358f73d087786655ca7c9f7a239bb15a

Имя файла: stlkrip.exe

SHA1: a3a0823d1ab1f848b75c8a8b9ae547f7fd38dd8d

Имя файла: kopiya_1C_PP_PDf.photo.jpg.pif

SHA1: 4dc6f7787be32f1cd0fe1090c687356cddf4c6df

Имя файла: stlKrip.exe

SHA1: 4b3e1ab88b8ce00c755c01757d74dd5e39d7f045

Имя файла: buh-doc_0595665fdeegrghw6sgagrg6ergesg_PDF.com

SHA1: 44565b62af2994620f15430f00df45815c5fdcc0

Имя файла: stl13krip.exe

SHA1: 4c9c1ee8a1db381d7287257fa8137acf28426b55

Имя файла: oplata_1C_buh_15102025_PDF.com

SHA1: 741db52873b3091a1e1b195bddaea2587ed11e54

Имя файла: doc_21102025_kopiya_1C_PDF.com

SHA1: a07710d7189f615c3f529025a2adf1a5fbf0b63c

Имя файла: vckrip.exe

SHA1: 5e82d4232241f665d4a38dda93e3440ad387189d

Имя файла: doc_22_10_2025_buhgalteriya_1C_pdf.bat

SHA1: e63422b4d7e9120dbac8333aa93a302346278e18

Имя файла: kriptoSTL.exe

SHA1: 7e26fd9a1f41c240df52882092305ae90c135301

Имя файла: Doc_1C_Buh_0frg5r6gr56eff_PDF.com

SHA1: 46b824005e72182eb72c689042301e471310f482

Имя файла: VCKRIP.exe

SHA1: 8588c5204d4556da31f81a9efb851944ba436bb9

Имя файла: STLkripos.exe

SHA1: c512a553d2a041f3e316b907b33732e6322d2688

Имя файла: kripSTL.exe

SHA1: 66a8867670168b1e0f36fe5cb1125f47245614fb

Имя файла: kopiya_1C_PP_28_10_2025_PDF.exe

SHA1: c5eedb7c4929ca1ce319c6aab7f9179852389cba

Имя файла: OOO_1C_kopiya_PP_29_10_2025_PDF.com

SHA1: 2fa6f0ebb0ca0aff3c74d409b5ce4f63a00ddeae

Имя файла: doc_1C_buh_31102025_d_PDF.com

SHA1: 91bb0f2cced2b13440208634574c171357d2fe3d

Имя файла: vncKrip.exe

SHA1: f4a34aee575bd2fd48069806c96b3d407b1b0321

Имя файла: schet_31102025_buh_PDF.exe

SHA1: db546655a1df9c8e043611237081243ee1fb05b3

Имя файла: doc_f0ef5re5f6ew56fsfsfs_PDF.scr

SHA1: 759a565c9cbd0c619b195c083575309ac92007d6

Имя файла: kripVC.exe

SHA1: 0a247db9f32de13545139613a0af42df65e78173

Имя файла: vcKrip.exe

SHA1: e70f22c612fb5402a6c89250ec5234eb43119b07

Имя файла: 15zvejff.5n5.exe

SHA1: c845b19e1b01f2245445f3ae4d9c845693802958

Имя файла: enc-build.exe

SHA1: 9a8d370a3dcab6afc3292633812bbd222a8493ab

Имя файла: акт_сверки_PDF.vbs

SHA1: b966d21cae3d4b4e6b0dfac462abfdc627421433

Имя файла: pic.jpg

SHA1: edbd8f727dcc162fb49dcb6d20695f5830f706b3

Имя файла: VC13112025upload.txt

SHA1: 19a7196ede2a7d8242b1f2d395316200d20e3621

Имя файла: doc_19.11.2025_bank.bat

SHA1: 9e42b9bb5f0284e8419971a4fca0e07d226718c4

© 2003 – 2025 F6 — российский разработчик технологий для борьбы с киберпреступлениями.

