

Рагнарёк: F6 исследовала атаки группировки вымогателей VantaCore — F6

Published: 2026-08-28 · Archived: 2026-09-23 02:01:01 UTC

Специалисты Лаборатории цифровой криминалистики и исследования вредоносного кода компании F6 сообщают о новой угрозе российскому бизнесу. В августе 2026 года специалистами Лаборатории выявлена активность новой группировки, назвавшей себя **VantaCore**.

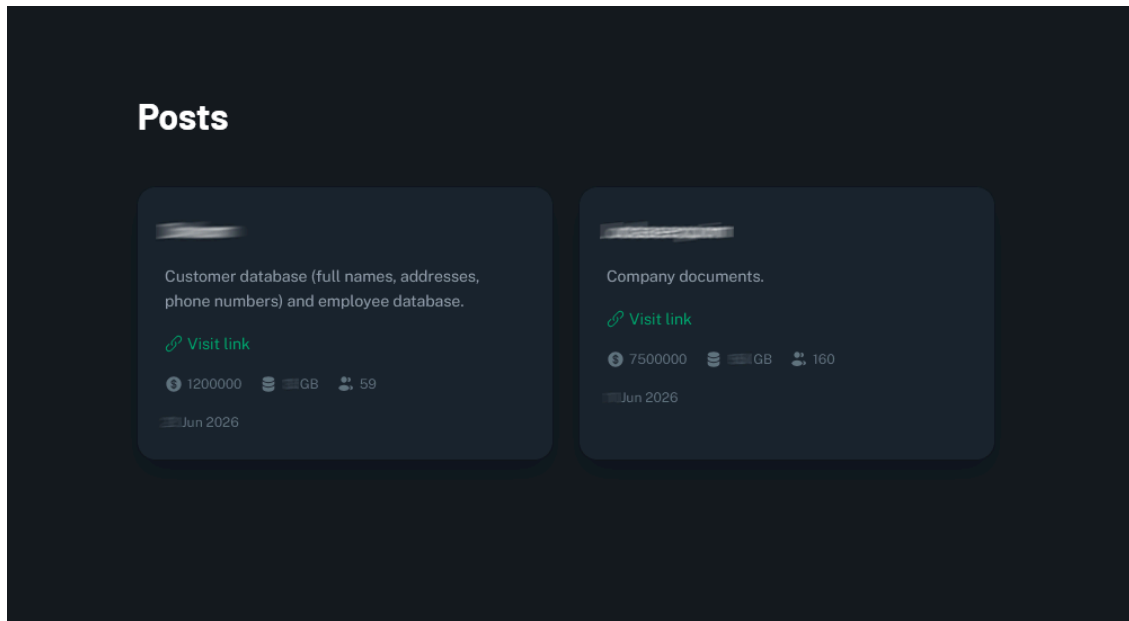
Уточнённое количество известных жертв этой группировки — не менее семи. Атакующие имеют явно нескромные аппетиты: суммы запрашиваемых выкупов составляют миллионы долларов. Вот только вопрос: новая ли эта группа или старая, но в новом облики. По мнению специалистов Лаборатории, есть все основания считать, что новая группировка — ребрендинг ранее известной проукраинской группы — **Thor**.



Специалисты компании F6 не раз заявляли о консолидации и перегруппировке проукраинских группировок в 2025-2026 годах. Сейчас также наметилась тенденция отказа проукраинских кибербанд от популярного тандема шифровальщиков **LockBit 3 Black** и **Babuk** и перехода на программы-вымогатели собственной разработки. В марте 2026 года мы уже [сообщали](#) о перевооружении группировки **Bearlyfy** на собственные шифровальщики **GenieLocker**. В августе же выявлены атаки группировки **VantaCore** с использованием программы-вымогателя собственной разработки VantaCore. Причин отказа от LockBit 3 Black и Babuk несколько. По всей видимости, это и ненавистные участникам группировок русские корни шифровальщиков LockBit 3 Black и Babuk. Перепалки противоборствующих сторон по этому поводу ранее уже вспыхивали в 2023 году на андеграундных площадках. Другая объективная причина — выявленные со временем недостатки в указанных шифровальщиках. Тем не менее, за основу авторы новых шифровальщиков берут все те же LockBit 3 Black и Babuk.

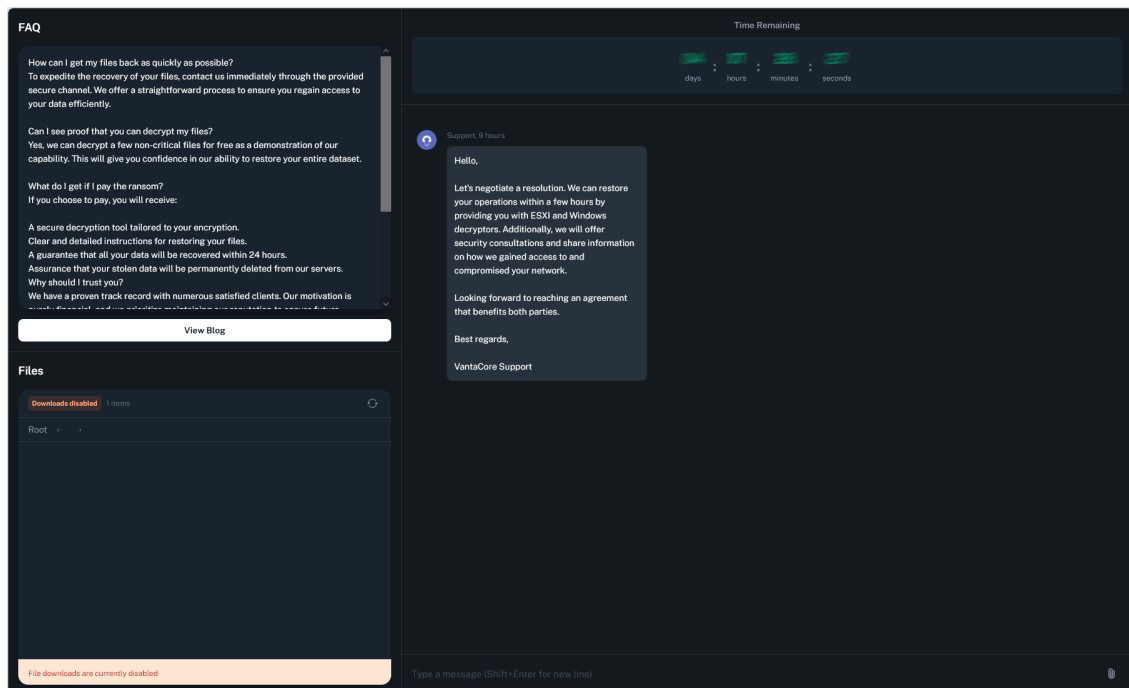
Вероятно, что участники VantaCore, как и пропавшие с «радаров» их коллеги из **Shadow**, решили создать имидж солидной партнерской программы вымогателей и создали сайт утечек (DLS) с информацией об атаках на различные компании в июне этого года. Группировка VantaCore использует схему двойного и

тройного вымогательства для дополнительного давления на жертву. Как свойственно проукраинским группам, похищенные данные спустя некоторое время продаются или просто распространяются на их ресурсах, а затем используются для организации новых атак и других деструктивных действий в отношении российских юридических и физических лиц.



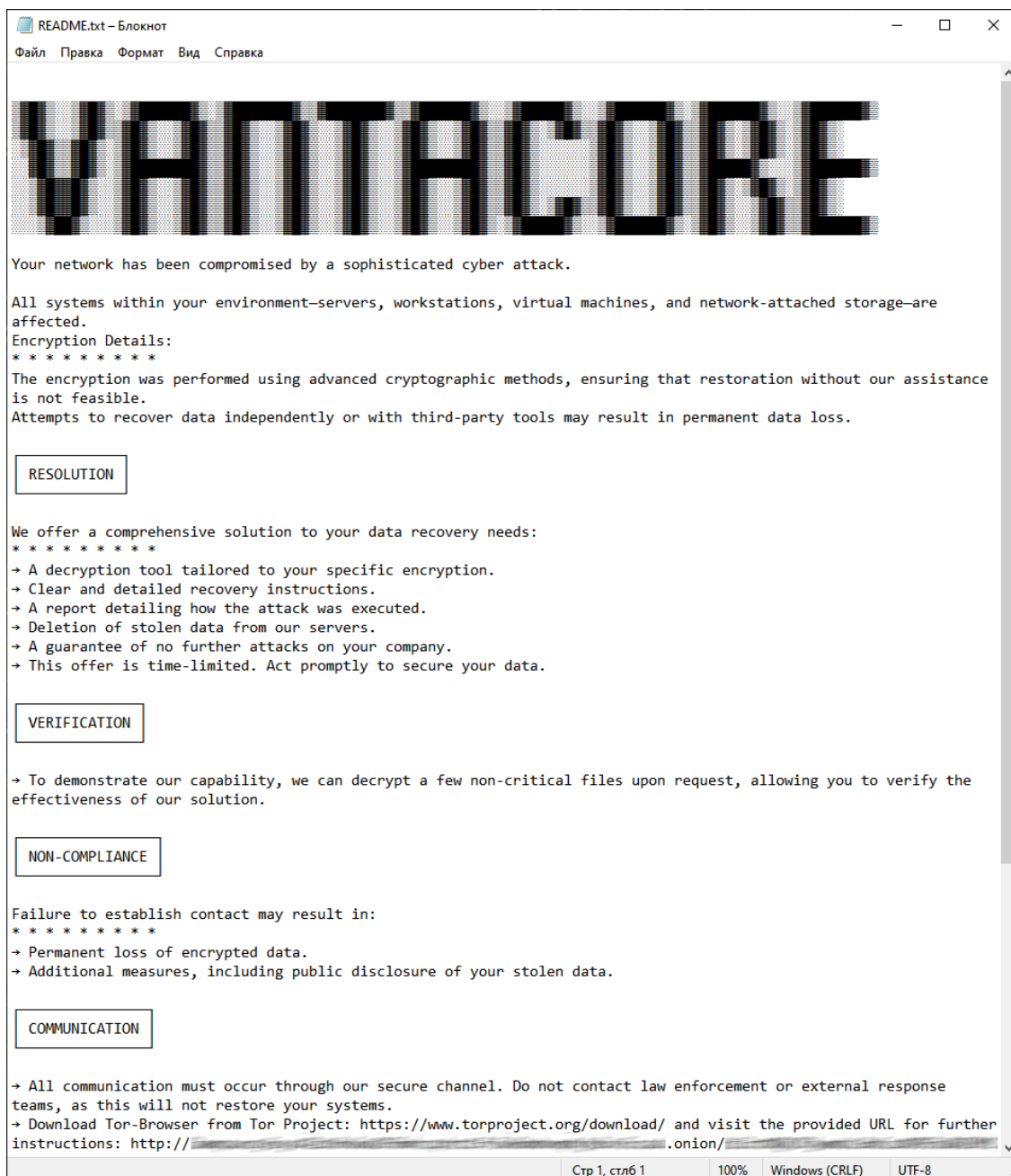
Сайт утечек (DLS) VantaCore

Как и полагается «солидной» международной партнерской программе (RaaS, Ransomware-as-a-Service), общение вымогателей с жертвой происходит в чате в сети Tor.



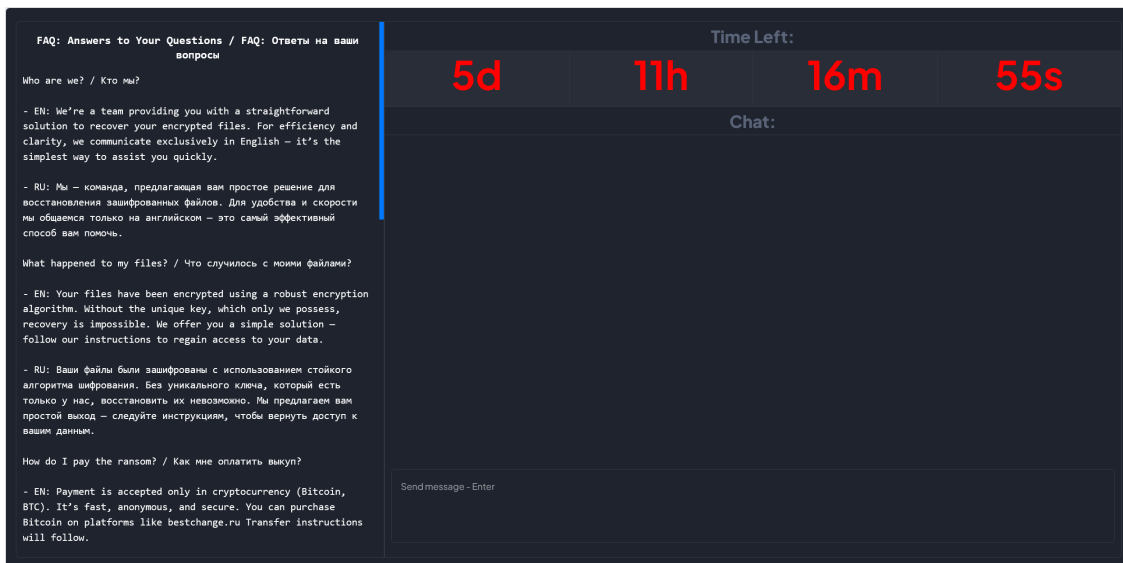
Пример чата с жертвой VantaCore

Ссылка на данный чат содержится в записке с требованием выкупа за расшифровку.



Пример содержимого текстового файла с требованием выкупа за расшифровку данных VantaCore

Даже если не вдаваться глубоко в детали, уже визуально по дизайну чатов прослеживается взаимосвязь с группировкой **Thor**.



Пример чата с жертвой Thor

Сайт утечек (DLS) VantaCore был развёрнут не позднее 7 июня 2026 года, на что указывают цифровые следы, оставленные при его создании. Кроме того, при анализе ресурса по пути /favicon.ico была обнаружена иконка с надписью «THOR», выполненной руническим письмом, что может дополнительно указывать на связь VantaCore с кибергруппировкой Thor.



Выявленная иконка favicon.ico VantaCore

Как и другие проукраинские группы, **VantaCore** в качестве начального вектора атаки используют все возможные варианты, которые могут привести к получению злоумышленниками доступа к ИТ-инфраструктуре жертвы: слабозащищенные публично доступные средства удаленного доступа (RDP, VPN), уязвимости в публичных приложениях, скомпрометированные учетные данные партнеров жертвы и т.п.

Поведение участников VantaCore в скомпрометированной инфраструктуре не сильно отличается от многих группировок вымогателей, их тактики, техники и процедуры во многом эффективны, хотя и не являются изощренными и инновационными. Их цель прежде всего — нажиться на жертве. Одна из особенностей,

отличающая VantaCore от многих других группировок — использование постэксплуатационных инструментов собственной разработки.

Для перемещений по атакуемой инфраструктуре атакующие используют добытые в ходе развития атаки легитимные учетные записи и преимущественно протоколы SMB и RDP. А для сетевой разведки используются как загружаемые сетевые сканеры, так и легитимные утилиты, имеющиеся в любой инфраструктуре, например ping, netsh, quser, qwinsta, net user и др., что во многом позволяет им долгое время оставаться незамеченными.

Наряду с этим с целью обеспечения длительного скрытного присутствия в инфраструктуре, а также для противодействия криминалистическому анализу злоумышленники используют следующие средства:

- применяют обфускацию в бэкдорах и других инструментах
- по завершении удаляют загруженные ими инструменты и файлы с результатами их работы
- повсеместно очищают все доступные журналы событий на Windows устройствах с помощью однострочного скрипта PowerShell и штатной утилиты wevtutil
- при наличии достаточного уровня привилегий отключают антивирусное ПО и другие средства защиты вручную или с помощью программы класса AV/EDR-killer на основе техники BYOVD
- мимикрируют под легитимную активность, маскируя расположение и имена своих инструментов под штатные компоненты Windows

На скомпрометированных Windows-системах злоумышленники закрепляются, создавая системные службы, а в качестве средств удаленного доступа ими используются свободно распространяемая программа удаленного доступа **Tactical RMM** и бэкдор собственной разработки **VantaCoreRAT**.

Изучив скомпрометированную инфраструктуру и получив полный контроль над ней, злоумышленники производят эксфильтрацию данных жертвы, а затем приступают к заключительному этапу атаки.

На этом этапе вымогатели реализуют деструктивные действия в отношении систем резервного копирования и шифруют критически важную информацию, что в результате позволяет им вымогать денежные средства за их расшифровку.

Для уничтожения резервных копий корпоративных данных злоумышленники прибегают к использованию функциональных возможностей свободно распространяемой утилиты bootice. С помощью данной утилиты злоумышленники записывают произвольными данными RAID-массивы хранилищ резервных копий, что блокирует восстановление инфраструктуры из бэкапов.

Для шифрования данных на устройствах серверного и пользовательского сегментов атакующие используют программу-вымогатель **VantaCore**.

Ее доставка и запуск на тех или иных системах осуществляется как вручную, в контексте нелегитимных RDP-сессий, так и с помощью собственного инструмента автоматизации **VantaCoreLoader**, который используется для массовой доставки и запуска программы-вымогателя на все выявленные хосты, используя схожие с PsExec/WinExec механизмы.

Стоит отметить, что во избежание обнаружения и удаления программы-вымогателя антивирусными средствами, прежде чем доставить вымогатель на целевую систему, злоумышленники останавливают процессы антивирусных средств с помощью упомянутой выше программы класса AV/EDR-killer. Для ее автоматизированной массовой доставки и запуска также используется VantaCoreLoader.

Краткое описание некоторых инструментов собственной разработки приведено ниже.

Программа-вымогатель VantaCore

Программа-вымогатель VantaCore разработана на языке программирования C++, часть строк обфусцирована. Программа-вымогатель имеет достаточно простые функциональные возможности: остановка/отключение системных служб и собственно шифрование файлов. Для запуска программы необходимо указать в командной строке пароль, который явно содержится в ее коде. Для шифрования данных используются криптографические алгоритмы ChaCha20 и X25519, в коде программы содержится открытый ключ X25519.

```
VANTACORE windows x64

USAGE
vantacore.exe [options]

OPTIONS
-h      Show this help
-pw     Password (required)
-k      Stop services and terminate processes
-v      Show progress bar
-nmx    Allow multiple instances (no mutex)
-pn     Print note to all printers
-d      Delay before start (seconds)
-p      Encrypt specific path only

EXAMPLES
vantacore.exe -pw [password] -k -pn
vantacore.exe -pw [password] -v [show progress bar]
vantacore.exe -pw [password] -nmx -p [local | \\remote]
```

Справка по использованию программы-вымогателя VantaCore

Невольно напрашиваются аналогии по дизайну с шифровальщиком **GenieLocker** другой группировки **Bearlyfy**.

```

GENIELOCKER v1 ESXI/Linux x64

GLOBAL OPTIONS:
-h                Display help information

PROCESSING OPTIONS:
-p <perc>         Encryption percentage (0-100, default 5, 0: Encrypt only file header)
-j <workers>      Parallel worker threads (0: Auto-detect CPU cores)
-r <dir>          Recursive directory processing (default: /vmfs/volumes)

RUNTIME CONTROL:
-w <sec>          Initial delay before execution
-d               Daemon mode (background process)
-l <logfile>      Log output destination

BUILD CONFIGURATION:
Target extensions: .vmdk, .vmx, .vmem, .vmxf, .vmss, .nvram, .vmsn, .vmsd
Lock extension:   .6d59e7e05ae7aebc
Auto-start delay: 10 seconds
Self-destruct:    no

USAGE:
genie_encrypt [options] <target_path>

```

Справка по использованию программы-вымогателя GenieLocker

Программа распространения по сети VantaCoreLoader

Для распространения в сети программы-вымогателя и других инструментов, например, **SnowKiller**, группировка использует инструмент собственной разработки **VantaCoreLoader**, который по сути является реализацией метода самораспространения с помощью общих сетевых ресурсов (Admin Shares) в LockBit 3 Black (psexec_netspread). Программа осуществляет поиск компьютеров, используя запросы LDAP. На доступные компьютеры программа копирует свои агенты, для которых удаленно создает системные службы, далее с агентами взаимодействует через именованные каналы IPC, с помощью которых загружает на компьютеры полезную нагрузку и параметры ее запуска.

```

[Logo]
v2.0 - Vantacore

Build: [redacted] (Seed: [redacted])

[-] Payload not found: C:\Users\Public\payload.exe
Usage:
C:\Temp\VantacoreLoader.exe [options]      Deploy payload (uses config.h defaults)
C:\Temp\VantacoreLoader.exe -s [options]   Scan mode (recon only)

Options:
-p <path>      Local path to payload (default: C:\Users\Public\payload.exe)
-d <path>      Target directory on remote hosts (default: C:\ProgramData)
-a <args>      Arguments for payload (default: "")
-t <threads>   Number of threads (default: 50)
-s            Scan only mode
-o csv        Output results to CSV
-v            Verbose/debug mode
-h            Show this help

Examples:
C:\Temp\VantacoreLoader.exe                # Use defaults from config.h
C:\Temp\VantacoreLoader.exe -p C:\beacon.exe -a "-A" # Custom payload with args
C:\Temp\VantacoreLoader.exe -s -t 100        # Scan only with 100 threads

```

Справка по использованию VantaCoreLoader

Бэкдор VantaCoreRAT

Группировка использует бэкдор авторской разработки **VantaCoreRAT**, который разработан на языке программирования Go, часть образцов обфусцирована с использованием Garble. Бэкдор имеет богатые функциональные возможности: может передавать различную информацию о скомпрометированной системе, загружать и передавать файлы, выполнять команды, предоставлять удаленный доступ к командной оболочке (Reverse Shell), работать в режиме прокси SOCKS5, обновлять и деинсталлировать себя. Бэкдор также использует различные методы обхода средств защиты. На компьютеры бэкдор доставляется с помощью небольшой программы-загрузчика, которая загружает в зашифрованном виде бэкдор по содержащейся в коде загрузчика веб-ссылке.

SnowKiller

Злоумышленники в своих атаках используют инструмент для нейтрализации программных средств безопасности (антивирусного ПО и EDR) под наименованием **SnowKiller**. Указанный инструмент использует технику BYOVD (Bring Your Own Vulnerable Driver) для завершения следующих процессов средств безопасности:

MsMpEng.exe, wsccommunicator.exe, wsc-service.exe, avp.exe, ekrn.exe, ksde.exe, efwd.exe, AvastSvc.exe, aswEngSrv.exe, aswToolsSvc.exe, aswidsagent.exe, bdntwrk.exe, bdagent.exe, bduserhost.exe, bdredline.exe, bdservicehost.exe, dwengine.exe, dwantispam.exe, dwwatcher.exe, dwscanner.exe, dwcloudhost.exe, dwarkdaemon.exe, NortonSvc.exe, MBAMService.exe, PtWatchDog.exe, PtSvcHost.exe, PtSessionAgent.exe, TmsaInstance64.exe, afwServ.exe, kavfs.exe, kavfsgr.exe, kavfsw.exe, kavfswp.exe, klnagent.exe, avpsus.exe

Если ваша организация столкнулась с атакой вымогателей, рекомендуем обращаться за профессиональной помощью к экспертам **F6** в рамках сервиса [«Реагирование на инциденты»](#)

Source: <https://www.f6.ru/blog/vantacore/>