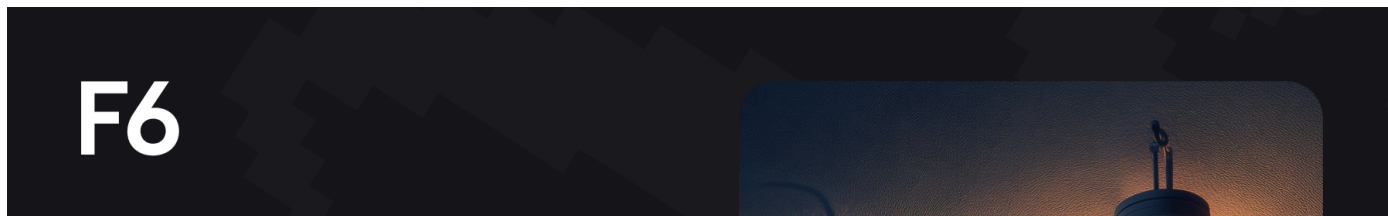


Восточный почерк: исследуем кибератаку азиатской группировки на российскую компанию

f6.ru/blog/eastern-trail

April 9, 2026



Первоначальный доступ, полученный через скомпрометированную инфраструктуру подрядных организаций, нередко становится отправной точкой для дальнейшего развития атаки киберпреступников. В таких случаях злоумышленники используют уже существующие доверенные отношения внутри инфраструктуры (T1199: Trusted Relationship). Опираясь на легитимный доступ, они последовательно исследуют доступные устройства и сетевое окружение, создают механизмы закрепления, а затем распространяют активность на смежные системы, оставаясь в рамках привычной для администратора активности.

В этом блоге мы представили результаты исследования атаки на одну из российских производственных компаний, которую аналитики [Центра кибербезопасности F6](#) обнаружили и локализовали в конце февраля 2026 года в рамках предоставления сервиса [SOC MDR](#). В качестве вектора первоначального доступа злоумышленники использовали сервисную учетную запись подрядной организации, применяемую для доступа во внутреннюю сеть организации через Check Point VPN. Анализ TTPs позволил установить, что злоумышленники использовали бэкдор ShadowPad, активно применяемый китайскими APT-группами.

На фоне участвовавших атак группировок из Азии на российские компании исследуемый инцидент – показательный пример того, как злоумышленники применяют продвинутое оборудование в сочетании с собственными инструментами для обхода современных средств защиты.

Центр кибербезопасности F6 — центр круглосуточного мониторинга и реагирования на инциденты информационной безопасности компании F6. Используя современные технологии для защиты от сложных угроз, аналитики ЦК оперативно обнаруживают и нейтрализуют угрозы на начальных стадиях их развития, тем самым минимизируют последствия инцидентов и обеспечивают надежную защиту инфраструктуры компаний.

SOC MDR — сервис, который объединяет мониторинг, расследование и устранение угроз. Команда MDR не просто обнаруживает атаку, но и самостоятельно принимает меры: изолирует зараженные узлы, блокирует вредоносную активность, восстанавливает системы. Клиент получает уведомление уже о закрытом инциденте с готовым отчетом.

F6 MXDR (ManagedExtendedDetectionandResponse)— система проактивного поиска и защиты от сложных и неизвестных киберугроз. Позволяет своевременно обнаруживать и блокировать подозрительную активность на конечных устройствах ИТ-инфраструктуры, предотвращая дальнейшее развитие атаки. Также позволяет проводить проактивный поиск угроз на основании собираемой телеметрии.

Описание атаки

Для первоначального доступа злоумышленники использовали скомпрометированную сервисную учетную запись, после чего приступили к изучению данных устройств и сетевого окружения с помощью стандартных утилит операционной системы. Для исполнения вредоносного ПО злоумышленники использовали созданные службы в операционной системе Windows. Точками закрепления стали запланированные задачи, созданные службы и автозапуск ВПО через ключ реестра RUN. Для горизонтального перемещения злоумышленники удаленно создавали сервисы на смежных устройствах с помощью стандартной утилиты операционной системы **sc.exe**.

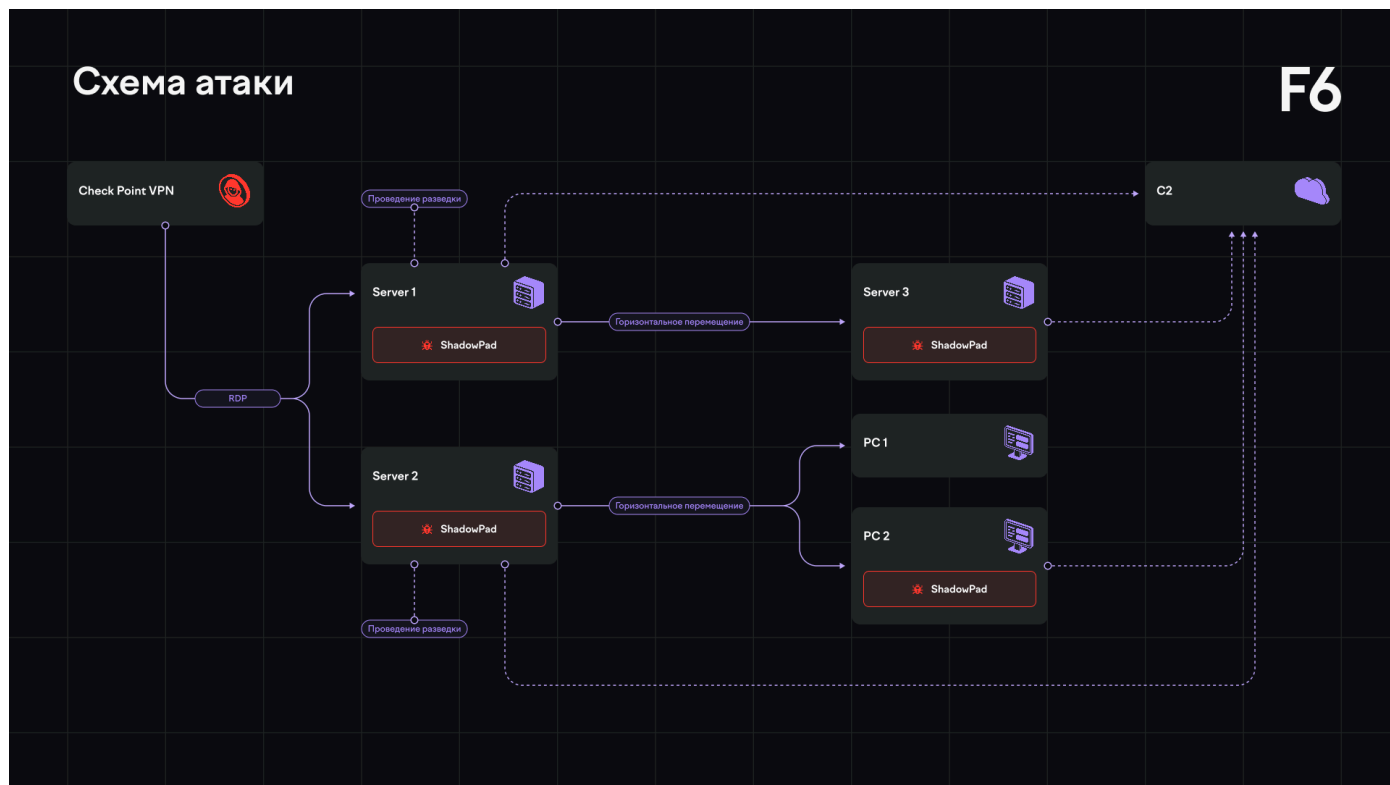


Рисунок 1 – Схема атаки

Первичное проникновение

В качестве вектора первоначального доступа злоумышленники использовали сервисную учетную запись подрядной организации, применяемую для доступа во внутреннюю сеть организации через Check Point VPN. Получив сетевой доступ, атакующие осуществили подключение по RDP-протоколу к внутренним системам.

Разведка

После получения первоначального доступа злоумышленники приступили к разведке скомпрометированных узлов и доменной среды, используя штатные утилиты операционной системы Windows. EDR (Endpoint Detection and Response), модуль F6 MXDR, зафиксировал команды, направленные на перечисление привилегированных групп и учетных записей, получение сведений о доверительных отношениях домена, просмотр активных пользовательских сессий, а также проверку сетевой связности и локального сетевого окружения.

```
net group "domain admins" /domain n!test /domain_trusts netstat -ano quser net user user_name /active:yes /domain net user user_name /domain net group "domain computers" /domain ping -n 1 google.com ping -n 1 local_host arp -a
```

Рисунок 2 – Действия, выполненные злоумышленниками на скомпрометированном устройстве и зафиксированные комплексом F6 MXDR

Доставка и исполнение

Проанализировав телеметрию от агентов EDR, аналитики ЦК F6 установили, что вредоносное ПО было загружено на устройства в рамках активной RDP-сессии.

Archive.exe / gswin64c.exe	Легитимное приложение <i>Ghostscript</i> , подписанное действительной цифровой подписью и уязвимое к технике <i>DLL Sideload</i> (<i>T1574.001</i>)
cb.exe / OneSetting.exe	Легитимное приложение <i>ASUS U3Boost U3BoostSvr.exe</i> , подписанное действительной цифровой подписью и уязвимое к технике <i>DLL Sideload</i> (<i>T1574.001</i>)
gsdll64.dll и cbLOC.dll / OneSettingLOC.dll	Обфусцированные загрузчики, реализующие технику <i>DLL Sideload</i> (<i>T1574.001</i>)

Для запуска вредоносного кода злоумышленники создали временную службу, указав в *binPath* легитимный ранее загруженный исполняемый файл, уязвимый к технике *DLL Sideload*. После запуска службы легитимный процесс загружал вредоносную библиотеку, что приводило к выполнению вредоносного кода в контексте доверенного процесса. После успешного запуска временная служба удалялась.

```
sc create aaa binpath= c:\programdata\gswin64c.exe sc start aaa sc delete aaa
```

Рисунок 3 – Процессы создания и запуска служб для исполнения вредоносного ПО

Рисунок 4 – Процесс внедрения вредоносного кода в легитимный процесс

Первый загрузчик **gsdll64.dll** *PE header timestamp: 2024-05-05 12:23:12 (UTC)* загружает зашифрованную полезную нагрузку в виде шелл-кода из раздела реестра *HKLM\SOFTWARE\EpyHenwh* или из файла **C:\ProgramData\63445685**. При этом ключ реестра с зашифрованными данными не является статическим, а генерируется алгоритмом, в который на вход подается дата компиляции *TimeDateStamp* из PE-заголовка загрузчика. В случае загрузчика **gsdll64.dll** это соответствовало значениям **63445685** и *Software\EpyHenwh*. Схожий механизм генерации путей и ключей реестра на основе параметров PE-заголовка ранее уже описывался для *ShadowPad*. Зашифрованные данные хранятся в реестре в виде фрагментов размером примерно по 4 КБ.

Далее шелл-код полезной нагрузки внедряет вредоносный код в специально запущенные процессы с нестандартными параметрами.

```
C:\Program Files\Windows Mail\WinMail.exe -k LocalSystemNetworkRestricted
```

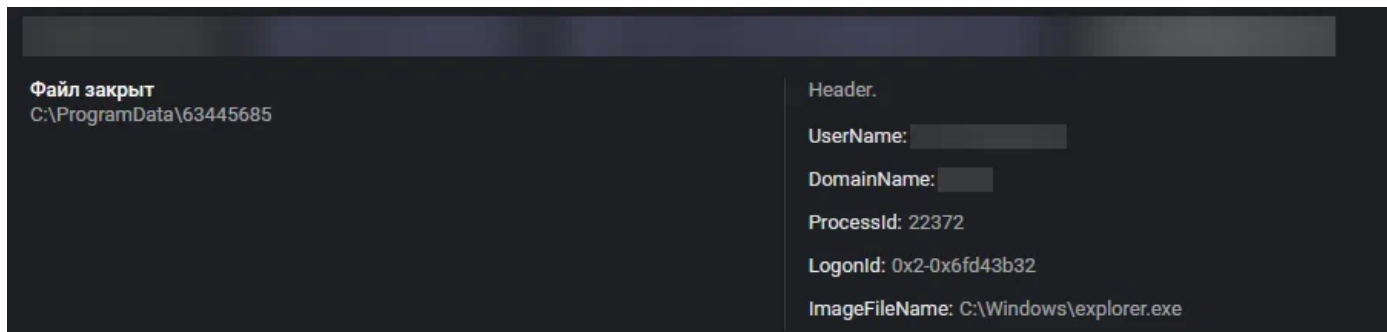


Рисунок 5 – Процесс создания файла для загрузки полезной нагрузки

Рисунок 6 – Событие изменения ключа реестра вредоносным ПО

Рисунок 7 – Внедрение полезной нагрузки в легитимный процесс WinMail.exe

После загрузки в процесс вредоносное ПО предпринимает меры по сокрытию своей активности, удаляя следы выполнения путем создания файлов нулевого размера.

Рисунок 8 – Создание файла нулевого размера от вредоносной библиотеки

Для перемещения на смежные устройства злоумышленники применяли механизм удаленного создания служб с использованием штатной утилиты **sc.exe**, что позволило инициировать запуск полезной нагрузки на удаленных узлах.

```
sc \\Local_IP create aaa binpath= "c:\programdata\gswin64c.exe" sc \\Local_IP start aaa sc \\Local_IP delete aaa
```

Рисунок 9 – Процессы удаленного создания, запуска и удаления служб на смежных устройствах

Второй экземпляр загрузчика **cbLOC.dll/ OneSettingeLOC.dll** *PE header timestamp: 2023-06-07 11:08:14 (UTC)* в свою очередь внедряет полезную нагрузку в следующие процессы.

```
C:\Program Files\Windows Media Player\wmpnetwk.exe -p C:\Windows\system32\spoolsv.exe -p
```

Рисунок 10 – Событие внедрения полезной нагрузки в процесс wmpnetwk.exe

Так как атакующие успели очистить следы на устройстве, на котором отсутствовал EDR-агент в момент перемещения, то при помощи дампа процесса **wmpnetwk.exe** была извлечена полезная информация.

1. Полезная нагрузка – **93FCBFB0.tmp**
2. Загрузчик – **cbLOC.dll /OneSettingeLOC.dll**
3. Легитимное приложение – **cb.exe(U3BoostSvr.exe)**
4. Ключ реестра с зашифрованными данными – **HKLM\SOFTWARE\YpkbsneVqhyt**

5. Адреса командных центров.

Рисунок 11 – Содержимое дампа процесса wmpnetwk.exe

Бэкдор хранит данные в зашифрованном виде в ветке реестра *HKLM\SOFTWARE\YpkbsneVqhyt*.

Рисунок 12 – Зашифрованные данные в ветке реестра HKLM\SOFTWARE\YpkbsneVqhyt

Закрепление

Для закрепления на конечных устройствах злоумышленники использовали запланированные задачи и службы, указывая в качестве запускаемого объекта легитимное ПО с внедренным в память процесса вредоносным кодом. Кроме того, ВПО закрепляется в системе, модифицируя раздел реестра RUN.

Рисунок 13 – Создание службы OneSettings

Рисунок 14 – Содержимое запланированной задачи

Рисунок 15 – Создание точки закрепления в ветке реестра RUN

C2

Коммуникация с командными центрами осуществлялась с применением DNS-туннелирования с использованием публичных DNS – **8.8.8.8**, **8.8.4.4**, **4.4.4.4** и **4.2.2.2**.

Рисунок 16 – Сетевое взаимодействие с применением DNS-туннелирования

Рисунок 17 – Использование DNS-туннелирования

Атрибуция

Анализ TTPs и образцов вредоносного ПО свидетельствует о том, что злоумышленники использовали бэкдор **ShadowPad**, активно применяемый китайскими APT-группами.

В ходе анализа сетевой инфраструктуры атакующих были найдены дополнительные индикаторы: на ip-адресе **192.144.23[.]37** расположены домены **app.axb1[.]com**, **sleive.freecountrys[.]com** и **free.threat7858[.]info**. В свою очередь на домене **free.threat7858[.]info** был ранее замечен SSL-сертификат

C=US, ST=CA, L=Santa Clara, O=Intel Corporation, CN=Intel Corporation - Client Components
GroupSHA-1: 2288836c26829732a1b3c9535c18d8df0c2ba224

также присутствовавший на доменах, замеченных в масштабных атаках китайских АРТ-групп с 2024 по 2025 год, отчеты по которым публиковались зарубежными ИБ компаниями (1, 2, 3), и в которых были найдены множественные пересечения с нынешней атакой. В некоторых отчетах также было упомянуто, что атакующие производили развертывание программ-вымогателей.

Рисунок 18 – Небольшая часть инфраструктуры атакующих

Кроме сетевых индикаторов, в публичные песочницы за период с февраля по март 2026 года были загружены аналогичные образцы загрузчиков из Бразилии, Хорватии и Румынии, что позволяет предположить – похожие атаки были направлены на компании в этих странах. Загрузчик, который использовался в исследуемой атаке – **gsdll64.dll** (*SHA-1: 2b9851ea8fafbc0d66f346cba8965a683522c67b*), был загружен из Хорватии и Греции.

На основании имеющихся данных невозможно однозначно отнести данную кампанию к конкретной АРТ-группе. При этом следует подчеркнуть, что бэкдор **ShadowPad** используется несколькими китайскими АРТ-операторами, что ограничивает круг потенциальных групп. Наблюдаются пересечения с группами **APT41**, **Teleboyi**, **EarthAlux** и **APT15**, однако текущие индикаторы не позволяют точно установить группу атакующих.

Вывод: китайские группировки по-прежнему представляют собой серьезную угрозу для организаций. Применение продвинутых техник в сочетании с инструментами собственной разработки, позволяет обходить даже продвинутые средства защиты и оставаться незамеченными в течение длительного периода.

Авторы выражают благодарность за помощь в исследовании главному специалисту Лаборатории цифровой криминалистики и исследования вредоносного кода F6 Андрею Жданову и руководителю отдела реагирования на киберинциденты ЦК F6 Аветику Надиряну.

Конфигурация ShadowPad

63445685

Процесс: C:\Program Files\Windows Mail\WinMail.exe -k LocalSystemNetworkRestricted C2: HTTPS://177.136.225[.]191:443 SSL://177.136.225[.]191:443
DNS://dns.reasonsbatesystem[.]xyz:53 WSS://app.reasonsbatesystem[.]xyz:443
SSL://app.reasonsbatesystem[.]xyz:443 HTTPS://app.reasonsbatesystem[.]xyz:443 Порты: 32440, 39527, 52353

93FCBFB0.tmp [Анализ ВПО опубликован на MDP F6 \(F6 Malware Detonation Platform\)](#)

Процессы: %ProgramFiles%\Windows Media Player\wmpnetwk.exe -p
C:\Windows\system32\spoolsv.exe -p C2: DNS://dns.axb1[.]com:53
DNS://cdn.freecountrys[.]com:53 Служба: OneSettings (Phone Service) Реестр:
SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Индикаторы компрометации

Файлы

Легитимные файлы, уязвимые к DLL Sideloadng

C:\ProgramData\cb.exe

C:\ProgramData\gswin64c.exe

C:\ProgramData\Microsoft\Windows\OneSetting\OneSetting.exe

C:\Program Files\Microsoft\Windows\ClipSVC\Archive\Archive.exe

ShadowPad Loader

C:\ProgramData\gsdll64.dll

C:\ProgramData\cbLOC.dll

C:\ProgramData\Microsoft\Windows\OneSetting\OneSettingLOC.dll

C:\Program Files\Microsoft\Windows\ClipSVC\Archive\gsdll64.dll

AudioXloc.dll

DRMloc.dll

ShadowPad Backdoor

C:\ProgramData\93FCBFB0.tmp

C:\ProgramData\63445685

SHA-1

2b9851ea8fafbc0d66f346cba8965a683522c67b

f5ea8e39139e8eb12f746f32fe23e682d67ba237

ec76dc98a3673be08d997974def855d5310c38f6

31693c3129c89942f178c9a16f584d881a5ab7c7
681f1d27e391dcb54dfa9805e52a6b6f76d549e3
d54e47741c6858cabd16c0cb7d9919c9d5559f59
ee1c6f778363b0395a08e1d918a96a2123a51110
9e2f1a1b3c5d16d744864f1ad2e8aabf94097b28
a05405e90087aeb57326a4f54bcc455dd0c20e2b

Сетевые

*.reasonsbatesystem[.]xyz

*.axb1[.]com

*.freecountrys[.]com

*.trustaviators[.]top

*.threat7858[.]info

177.136.225[.]191

138.199.21[.]251

192.144.23[.]37

193.56.255[.]178

86.106.85[.]51

SSL-сертификаты

Issuer: C=US, ST=CA, L=Santa Clara, O=Intel Corporation, CN=Intel Corporation - Client Components Group SHA-1: 2288836c26829732a1b3c9535c18d8df0c2ba224 SHA-256: d3b98f011bebe4a99eea0989b2788544adaa8e1f11b37b3d99f2215466ae8558 Issuer: C=US, ST=Washington, L=Redmond, O=Microsoft Corporation, CN=Microsoft Corporation SHA-1: cfd9e58f770ca8c0cdb55893f6ee69cd8e449516 SHA-256: 17ea3b39a5c7a86d136d961adccd5d8768f40418e7e4a72f97da77e835ec1749 Issuer: CN=dl.delivery.mp.microsoft.com SHA-1: 04045b132da52a5266e34226aecf568878c99a5b

Службы

OneSettings

aaa

Запланированные задачи

Microsoft\Windows\Archive\Archive

Реестр

SOFTWARE\Microsoft\Windows\CurrentVersion\Run\OneSettings

Значение: C:\ProgramData\Microsoft\Windows\OneSetting\OneSetting.exe