

# ИНФОРМАЦИОННАЯ СПРАВКА

от 18 июня 2025 г.

## о результатах мониторинга сведений о критических уязвимостях программного обеспечения государственных информационных систем и объектов критической информационной инфраструктуры, а также связанных с ними компьютерных атаках

### УЯЗВИМОСТИ

Опубликована информация о следующих критических уязвимостях программного обеспечения.

Идентификатор и описание	Возможные меры защиты
<p>BDU:2025-06872 CVE-2025-6087</p> <p>Уязвимость пакета opennextjs сервиса балансировки сетевого трафика для веб-приложений Cloudflare связана с недостаточной проверкой поступающих запросов. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код путём подделки запросов от имени сервера.</p> <p><i>Отсутствует информация о средствах эксплуатации уязвимости в открытом доступе.</i></p> <p><i>Отсутствует информация об использовании уязвимости в реальных атаках.</i></p> <p><i>Сервис балансировки сетевого трафика для веб-приложений Cloudflare (США) широко используется на территории РФ.</i></p> <p><i>Экспертная оценка требуемого потенциала нарушителя для эксплуатации уязвимости – средний потенциал</i></p>	<p>Установка обновлений из доверенных источников. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуется устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.</p> <p><u>Уровень опасности:</u> Критический (9.3)</p> <p>CVSS v3: AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:N</p> <p><u>Компенсирующие меры:</u></p> <ul style="list-style-type: none"><li>- использование межсетевого экрана уровня приложений (WAF) для фильтрации HTTP-трафика;</li><li>- ограничение доступа к уязвимому программному обеспечению, используя схему доступа по «белым спискам»;</li><li>- использование систем обнаружения и предотвращения вторжений для обнаружения (выявления, регистрации) и реагирования на попытки эксплуатации уязвимостей;</li><li>- ограничение доступа к платформе из внешних сетей (Интернет).</li></ul> <p><u>Использование рекомендаций:</u></p> <p>Для opennextjs: <a href="https://www.npmjs.com/package/@opennextjs/cloudflare/v/1.3.0">https://www.npmjs.com/package/@opennextjs/cloudflare/v/1.3.0</a></p> <p>Для Cloudflare: <a href="https://www.npmjs.com/package/create-cloudflare/v/2.49.3">https://www.npmjs.com/package/create-cloudflare/v/2.49.3</a></p>
<p>BDU:2025-06879 CVE-2025-25264</p> <p>Уязвимость программного средства для настройки и параметризации контроллеров WAGO Device Manager связана с ошибками конфигурации политики CORS. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, получить несанкционированный доступ к файловой системе путем отправки специально сформированных запросов.</p> <p><i>Отсутствует информация о средствах эксплуатации уязвимости в открытом доступе.</i></p> <p><i>Отсутствует информация об использовании</i></p>	<p>Установка обновлений из доверенных источников. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуется устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.</p> <p><u>Уровень опасности:</u> Высокий (8.8)</p> <p>CVSS v3: AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N</p> <p><u>Компенсирующие меры:</u></p> <ul style="list-style-type: none"><li>- использование межсетевого экрана уровня приложений (WAF) для фильтрации HTTP-трафика;</li><li>- сегментирование сети для ограничения доступа к уязвимому программному обеспечению из других подсетей;</li><li>- использование систем обнаружения и предотвращения</li></ul>

<p>уязвимости в реальных атаках.</p> <p><i>Имеются сведения об использовании продуктов WAGO (Германия) на 21 объекте КИИ.</i></p> <p><i>Экспертная оценка требуемого потенциала нарушителя для эксплуатации уязвимости – средний потенциал</i></p>	<p>вторжений для обнаружения (выявления, регистрации) и реагирования на попытки эксплуатации уязвимостей;</p> <p>- ограничение доступа к платформе из внешних сетей (Интернет).</p> <p><u>Использование рекомендаций:</u>  <a href="https://certvde.com/en/advisories/VDE-2025-018/">https://certvde.com/en/advisories/VDE-2025-018/</a></p>
--	--

## АТАКИ

1. В результате анализа ВПО получен перечень IP-адресов, используемых проукраинскими группировками в качестве объектов DDoS-атак, а также DNS-, прокси-серверов и серверов управления. Перечень IP-адресов актуален по состоянию на 18 июня 2025 года. Выявлены 2594 атакуемых IP-адресов российских организаций, относящихся к телекоммуникационной сфере.

Также получены сведения о 398 IP-адресах (в том числе 10 российских - ИП Шаймарданов Константин Рамилевич в г. Линево (Новосибирская область), ООО «Облачные технологии» в г. Москва, ООО «Матрикснет» в г. Омск, ЗАО «МСТН» в г. Москва, ООО «Дата-центр ИМАКЛИК» в г. Москва, ИП Галямин Денис Дмитриевич в г. Санкт-Петербург, ООО «СвязьРесурс-Регион» в г. Краснодар), используемых в атаках в качестве прокси-серверов. Наибольшее число прокси-серверов из следующих стран: США (101 IP-адрес), Китай (62 IP-адреса), Индонезия (52 IP-адреса), Бразилия (14 IP-адресов).

2. Сообщается об атаке на информационные системы оператора спутниковой связи «Морсвязьспутник» (<https://www.marsat.ru/>, ФГУП «Морсвязьспутник», ИНН 7707074779, г. Москва).

*ФГУП «Морсвязьспутник» – национальный оператор системы подвижной спутниковой связи «Инмарсат» на территории Российской Федерации. Предприятие является подведомственной организацией Федерального агентства морского и речного транспорта (Росморречфлот).*

Ответственность за атаку взяла на себя проукраинская хакерская группировка CyberSec's.

**В качестве доказательств** нарушители опубликовали снимки экрана, демонстрирующие недоступность сайта из сети Интернет.

***Информация подтверждена.***

*На момент времени проверки информации (18.06.2025, 9:32) сайт оператора спутниковой связи «Морсвязьспутник» недоступен из сети Интернет.*

*Официальные комментарии представителей компании не обнаружены.*

Источник информации: <https://t.me/badbclubua/330>.

3. Сообщается о возобновлении DDoS-атаки на информационные системы облачного-провайдера RUSONYX (<https://www.rusonyx.ru/>, ООО «Астра Облако», ИНН 7707301630, г. Москва).

Отмечается, что в результате атаки фиксируется невозможность получения доступа к личному кабинету пользователя на сайте компании «Группа Астра» (<https://astra.ru/>, ООО «Русбитех-Астра», ИНН 7726388700, г. Москва).

*В официальном Telegram-канале компании «Группа Астра» ([https://t.me/astralinux\\_chat](https://t.me/astralinux_chat)) сообщается о том, что фиксируемые сбои связаны с DDoS-атакой на инфраструктуру провайдера данных.*

*Установлено, что с 2024 года 80 % активов RUSONYX принадлежат ГК*

«Астра».

**Информация подтверждена** при помощи сервиса <https://downdetector.su/>.

На момент времени проверки информации (18.06.2025, 9:40) сайт облачного-провайдера RUSONYX функционировал в штатном режиме.

В официальной группе Вконтакте облачного-провайдера RUSONYX (<https://vk.com/rusonyx>) опубликовано официальное заявление представителей компании: «...Почти победили самую массированную DDoS-атаку за всю историю Rusonyx. Она длится более суток и является продолжением другой атаки, которая накануне, 12 июня, накрыла крупные сервисы Рунета по всей стране...».

Ни одна из отслеживаемых хакерских группировок не взяла на себя ответственность за атаку на информационные системы облачного-провайдера ООО «Астра Облако».

Объекты ООО «Астра Облако» фиксируются в качестве целей DDoS-атак проукраинской хакерской группировки IT ARMY ofUkraine.

Последняя массированная DDoS-атака на информационные системы ООО «Астра Облако», фиксировалась 16.06.2025 (информационная справка от 16.06.2025 № 844).

Источники информации:

<https://t.me/antiddositarmyua/1112>;

[https://t.me/astralinux\\_chat/710562/1151726](https://t.me/astralinux_chat/710562/1151726).

4. Сообщается о DDoS-атаке на информационные системы интернет-провайдера «Атлас Телеком» (<http://internet.su/>, ООО «Атлас Телеком», ИНН 6829063892, г. Москва).

**Информация подтверждена.**

На момент времени проверки информации (18.06.2025, 11:32) сайт интернет-провайдера «Атлас Телеком» недоступен из сети Интернет.

Официальные комментарии представителей компании не обнаружены.

Ни одна из отслеживаемых хакерских группировок не взяла на себя ответственность за атаку на информационные системы интернет-провайдера ООО «Атлас Телеком».

Объекты ООО «Атлас Телеком» фиксируются в качестве целей DDoS-атак проукраинской хакерской группировки IT ARMY ofUkraine.

Источник информации: <https://t.me/antiddositarmyua/1113>.

## УТЕЧКИ ДАННЫХ

Информация об обнаруженных утечках данных не относится к области ответственности ФСТЭК России.

## Дополнительная информация

### Сведения о хакерских группировках и ВПО.

В Telegram-канале (<https://t.me/cyberguerre>) опубликовано подробное исследование деятельности хакерской группировки XDSpy (альтернативное название Silent Werewolf, ранее упоминалась в информационных справках).

Установлено, что кампания, начавшаяся в марте 2025 года, связана с эксплуатацией уязвимости нулевого дня **BDU:2025-02936** (ZDI-CAN-25373 – идентификатор международной базы уязвимостей «нулевого дня») в механизме

обработки .LNK-файлов пользовательского интерфейса операционных систем Windows.

Цепочка заражения начинается с того, что пользователь распаковывает ZIP-архив и открывает встроенный файл LNK, который запускает легитимный исполняемый файл. Этот исполняемый файл, в свою очередь, загружает вредоносную библиотеку DLL. Данная библиотека является ВПО типа «загрузчик» на основе C# .NET, получившее название **ETDownloader** (ранее не упоминалось в информационных справках), которое обеспечивает постоянное присутствие нарушителей на хосте. Далее ETDownloader доставляет в компрометируемую систему ВПО типа «стилер» XDigo (ранее упоминалось в информационных справках). Стилер XDigo собирает информацию о взломанном хосте, а также о файлах путем формирования расписаний для выполнения вредоносных функций. Результаты работы стилера отправляются на C2-сервер нарушителей. К вредоносным функциям относятся:

- сканирование домашнего каталога текущего пользователя на наличие файлов с одним из жестко заданных расширений: .doc, .docx, .pdf, .xls, .xlsx, .ppt, .pptx, .zip, .rar, .7z, .odt, .ods, .rtf.

- сканирование домашнего каталога текущего пользователя Desktop на наличие файлов с расширением .txt;

- извлечение содержимого буфера обмена;

- создание снимка экрана;

- сканирование томов, отличных от C: для поиска файлов с одним из вышеупомянутых жестко заданных расширений;

- получение текущего имени пользователя и списка каталогов, расположенных в C:\Program Files\*\\*.

*Индикаторы компрометации:*

*Файловые индикаторы:*

4f1d5081adf8ceed3c3daaaa3804e5a4ac2e964ec90590e716bc8b34953083e8  
59b907430dde62fc7a0d1c33c38081b7dcf43777815d1abcf07e0c77f76f5894  
ccf56b6b727da47c89f7a1a47cc04ab3a41d225c1298a74f16c939a5622b03f2  
b03d9dd170cd82890ee1a5503529b81ce8064893e31a88b87081a8c72610d810  
e14fdb6c0b5b64e1ca318b7ad3ac9a4fd6dec60ef03089b87199306eba6e0cab  
678f79e78847a1274238740bb8cada62f9c41cab96df8537d87d38850502d0a2  
81bb1cf3a805c1375bb3251eea9f1ad132ab1266295a75cda9ffe9278588ac7f  
d5c0fd26ba1504bde3222202f7a257efa9cd6c6949718495a7c33cd6510fce2a  
52a98f2b2de46bc0835a11d2ba22b874a09788596507c13ac22b9b8877a8f3c6  
bc0b9075e3b8504c4e0c7097c6be8aa05f96032053ec43e502d297136aaf375e  
38489af1360af2cb7ba70f61e4c562fa63ce58e59576ba452db560f75ed1680a  
dd279ea6c2a660ff7e70788af4a6c98524836c1b63beed756a77942c83de06fa  
40bc204062a1f936c246fbffbed1a6bb41107ad9e5ad25df8970e4090258e145  
564b2184a7f53d5f1680673ced354f5e956d897b7e1ea7d3f992cc38be6a9b20  
7d6eb47ff307bebf87022575edd19181ad34ee5a5db1f408a25d16cd27d8aa2f  
40e3fcfcc09fd84b2745b75e0e5e7beae866f4300ec8f36e2e9ab3197f198dcd  
0b705938e0063e73e03645e0c7a00f7c8d8533f1912eab5bf9ad7bc44d2cf9c3  
9c1acde0627da8b518b0522d6fed15cecf35b20ed8920628e9f580cfc3f450ed  
5be9aba659baa089bcd253905deaf3f084f2b8f03701e90f2a46b36781165925  
536cd589cd685806b4348b9efa06843a90decae9f4135d1b11d8e74c7911f37d  
cfd0d56ca3d6c9ca232252570522c4b904be2807c461276979b1f8c551ccd4aa  
904db68a915b4bbd0b4b2d665bb1e2c51fa1b71b9c44ce45ccd4b4664f2bfd8e

e62c3135fd708ee420cf767fa1654d8d66ff01f5160ddad633e3cc5eaeaa926  
65209053f042e428b64f79ea8f570528beaa537038aa3aa50a0db6846ba8d2ec  
15277bfc6b784c373d535fbda9396bd16c15d990943423167602fb81b26d0f07  
95060ba948948eea9bfc801731960b97d3efceb300622630afcbccfe12c21ccd  
792c5a2628ec1be86e38b0a73a44c1a9247572453555e7996bb9d0a58e37b62b  
5e34d754b0a938de7e512614f8fc6d7cd6c704f76b05044e07c97bd44bd5d591  
68347b0c6494a56dd0f6492c6c56158b46bcacf44878a8741f6e63ff2946cf30f  
7e04c69685d8612f7fc3512ad9ad1802a28428f75874b8717c0f04e939a3324d  
f3f2c3c5836ce6e3cb92aa6dfc0f133e15a7fd169a3d1049b7d82e49d1577273  
448245612a5388074e32251a0b44769170c586cc4c2ae06cd953c7a461ce34a6  
747dfd7f0ca893034136fd286c737b55edc9276b5794a02c6dd3771da0342729  
5248b0e4af1914762cc1c436a898d12d5f74980b816155f4191dc9692402668f  
7a2af22372a4fd3ba89d36fdee38967cb77f43e14255d0b5ad80da863b146625  
7c0597aa77031a100db0941921b60f08079bec7f710b6e736a15012db6465c39  
031e05d15afabef6010179d2acd09925395167fd442b64b6aa8ffd81bd5e268e  
056cd36bf4bc6efc119a64f2ffedd76f3dcb75daa95c22c59d91664dfcaa6fd5  
fb1df37336d79861b13d5f4ba875393c7e91b12cd73302cb414c1d084104a6a8  
c8899a6e8d3dd11c75217253f8dd78f5029c01e886880cafce0388d5fd6aa54b  
7a2af22372a4fd3ba89d36fdee38967cb77f43e14255d0b5ad80da863b146625  
0d983f5fb403b500ec48f13a951548d5a10572fde207cf3f976b9daefb660f7e  
3aded2a154dcf017ffed634fba593f80df496eb2be4bee0940767c8631be7c1  
49714e2a0eb4d16882654fd60304e6fa8bfc9dbd9cd272df4e003f68c865341  
e32f04362ec4db90e024bfb57adf6e5c02f1061cd17dbf81a5bbc0b588119b25  
ffc538f2c6e91f07be067311ed143d28c5437a8af69974f751c043e2944d60b2  
efd44bc4e0efcab72106ea065c8a89d51d499202732319b21324487e8d00eccf  
2dde92fc0936cb275be79d5864c98772d1270e4a54c01e61ebc4b856b5e048d5  
666f4977abf17db6da2d05b385c5cf53f6500517226a3ac5bd0360eda9193d08  
be6a545180300554eea2ee6ece9f835a12996059d726df810fe13ba0044033cd  
07e2376d2c4318b0f9c472d01342d67e23a2e8edc182533a291336dfeaff4e60  
12fd8d45a181adfd6725ea9806d72ed61b3af1e31d80fa7ddd32e1932a8dfd75  
bcb5df098a79e3bc1d8bcb3b1a354b6643afdb4ca40333e0548e5ed1a9470cac  
f7be89ae645831d519b7c781d69cf8e88e5762b824c9a6753eb16b25c4abef76  
a8d578d4b50ac4029db22b76563e927ab691075aacc87621795b16b388b7d48c  
ef8fdec66751b6a17da45dd4d9c22cef8d3c78604e7a8bc6fc8e2b30342ff408  
9f17ff59172a802bc6ce8490c1ea379a5bf75af839f8b59373fba8c51e878af0  
0993b0bb897402954eb9057bc84ea98e2c12ff1185a87ac3c3a15a241560bb1a  
0a626f1837da9043e65ccf9e23192aef36d58402a1fd56577952c7bb426f2ec5  
e0ffc3442215b888c55d8dfd9d33c5cff315a59089aeb42da4cf6869eed8f5d  
77b2f2ef5bc3b7bb2d1b85491ece85b56da37685652526c6fa6e3562cd12e3b6  
021d13de99e996fbf03e57b78ce67630c19d33242eee8480383d7b065edebb51  
83341b08425a1a247becd79e829064ddb309636d7d62a369338ffd47af6e955  
5409eb70942a6b875d8343437bb04e368f56de1854953fa87890fc8ee8a8bc37  
a9b9022aedd1b9afbd7ab1f11f60f236102e1f70b340658da8cb39c072a9af61  
155b94be1c3dca48314f6f2ee0c89c09553851ecc9ceefc436e16ebb7fca5f1a  
2414dd462e3ca05ecd37aa56dc8841f5ef9588663572e7bc36d07520af7864b1  
bbc5e80d3f068d8eff0cfa745ecba97903a83dfd9fe6f43cf05e803bbe9ce8b9  
e95f2982195399b5f9e453be6db02a346bb516320659a3ade2c385bcb7fc27da  
ef34c433c818774b466ba4e6f677b1c6cf51bb9213a60fd779fd7df39011e97b

Сетевые индикаторы:

pdf-базар. <url>

pdfdepozit. <url>

файл-bazar.com

вашазагрузка365.com

melodicprogress. <url>

печальноебудущее.com

quan-miami.com

согревающийнапиток.com

seychaspozze.com

аос-управление.com

bukhgalter-x5group.com

bystryvelosiped.com

список ячеек. <url>

дверстекло. <url>

dwd765m.com

khoroshayamych.com

krasnayastena.com

магнитгрупп. <url>

ru-pochta365.com

ru-система. <url>

темная машина.com

утреннее солнце.com

zelenyysalat.com

zhestovyyliker.com

зимние развлечения.com

laultrachunk.com

promenimath. <url>

сломанный монитор.com

проверенные файлы.com

faylsklad.com

мой-pdf. <url>

nevynosimayapchela.com

pdf-реестр.com

pdf-sklad. <url>

реестр-файлов.com

serayagrust. <url>

protej.org.nniir.com

nniir.ком

файл-magazin. <url>

pdfmagazin. <url>

скачивание-файлов.com

чистыйвоздух.com

svobodnoepredlozheniye.com

ваш-диск. <url>

zagruzkadannykh.com

zetta-страхование.com

khitrayalisitsa.com

*tvoi-fayly.com*  
*клетчатая рубашка.com*  
*загрузка24.com*  
*easy-download24.com*  
*полный загрузчик. <url>*  
*скачивание-файлов24.com*  
*обмен файлами.com*  
*твой-диск. <url>*  
*www.ваши-файлы.com*  
*загрузка файла.com*  
*faylbox365.com*  
*загрузка-pdf.com*  
*мой-файл.com*  
*отправка файлов.com*  
*pdfsklad. <url>*

***Возможными мерами защиты являются:***

- получение файлов только от известных отправителей, проверка их с использованием средств антивирусной защиты;
- использование систем обнаружения вторжений при организации доступа к сети Интернет;
- проверка имени домена отправителя электронного письма в целях идентификации отправителя;
- реализация мер изолированной программной среды;
- минимизация пользовательских привилегий.

**Источники информации:**

<https://t.me/cyberguerre/3227>;

<https://harfanglab.io/insidethelab/sadfuture-xdspey-latest-evolution/>.