

ИНФОРМАЦИОННАЯ СПРАВКА

от 17 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:2025-06805 CVE-2025-49146</p> <p>Уязвимость драйвера JDBC pgjdbc для подключения Java-программ к базе данных PostgreSQL связана с недостатками процедуры аутентификации. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, реализовать атаку типа «человек посередине».</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>Имеются сведения об использовании драйвера JDBC pgjdbc для подключения Java-программ к базе данных PostgreSQL (Сообщество свободного программного обеспечения) в составе отечественных сертифицированных средств, широко используемых на объектах КИИ.</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> Высокий (8.2)</p> <p>CVSS v3: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N</p> <p><u>Компенсирующие меры:</u></p> <ul style="list-style-type: none">- включение режима проверки сертификата сервера при установлении SSL-соединения;- использование средств межсетевого экранирования для ограничения удалённого доступа к уязвимому программному обеспечению;- использование систем обнаружения и предотвращения вторжений для обнаружения (выявления, регистрации) и реагирования на попытки эксплуатации уязвимости;- использование виртуальных частных сетей для организации удаленного доступа (VPN);- ограничение доступа к платформе из внешних сетей (Интернет). <p><u>Использование рекомендаций:</u> https://github.com/pgjdbc/pgjdbc/commit/9217ed16cb2918ab1b6b9258ae97e6ede244d8a0</p>
<p>BDU:2025-6807 CVE-2025-4922</p> <p>Уязвимость механизма поиска ACL-политик на основе префиксов оркестратора приложений Nomad связана с некорректным присваиванием правил контроля доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, обойти существующие механизмы безопасности путем создания задания со специальным префиксным именем.</p> <p><i>Имеется информация о средствах эксплуатации уязвимости в открытом доступе (https://discuss.hashicorp.com/t/hcsec-2025-12-nomad-vulnerable-to-incorrect-acl-policy-lookup-attached-to-a-job/75396).</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 (8.1)</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">- использование средств межсетевого экранирования для ограничения удалённого доступа к уязвимому программному обеспечению;- сегментирование сети для ограничения доступа к уязвимому программному обеспечению из других подсетей;- ограничить доступ к уязвимому программному

<p><i>Отсутствует информация об использовании уязвимости в реальных атаках.</i></p> <p><i>Имеются сведения об использовании оркестратора приложений Nomad (США) на 2 объектах КИИ.</i></p> <p><i>Экспертная оценка требуемого потенциала нарушителя для эксплуатации уязвимости – базовый повышенный потенциал</i></p>	<p>обеспечению, используя схему доступа по «белым спискам»;</p> <ul style="list-style-type: none"> - использование систем обнаружения и предотвращения вторжений для обнаружения (выявления, регистрации) и реагирования на попытки эксплуатации уязвимостей; - минимизация пользовательских привилегий; - отключение/удаление неиспользуемых учётных записей пользователей. <p><u>Использование рекомендаций:</u> https://discuss.hashicorp.com/t/hcsec-2025-12-nomad-vulnerable-to-incorrect-acl-policy-lookup-attached-to-a-job/75396</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 17 июня 2025 года. Выявлены 1811 атакуемых IP-адресов российских организаций, относящихся к телекоммуникационной сфере.

Также получены сведения о 200 IP-адресах (в том числе 5 российских – Макрорегиональный филиал ОАО «Ростелеком «Южный» в г. Краснодар, ООО «2КОМ» в г. Москва, ООО «СпейсВэб» в г. Санкт-Петербург, АО «ТаймВэб» в г. Санкт-Петербург, ООО «Оптим Коммуникейшнз» в г. Москва), используемых в атаках в качестве прокси-серверов. Наибольшее число прокси-серверов из следующих стран: США (66 IP-адресов), Индонезия (28 IP-адресов), Китай (27 IP-адресов).

2. В дополнение к информационной справке от 13.06.2025 № 841. В информационной справке сообщалось об атаке проукраинской хакерской группировкой Кибер-Партизаны на сайты администраций муниципальных образований Ростовской области.

Информация уточнена.

Опубликован полный список атакованных сайтов государственных учреждений (данные об объектах атаки и результаты анализа полученной информации приведены в таблице).

В ходе анализа информации установлено, следующее:

На момент времени уточнения информации (16.06.2025, 10:52) сайты всех муниципальных образований Южного, Северо-Кавказского и Сибирского федеральных округов недоступны из сети Интернет.

Подтверждение атак проводилось с использованием сервисов «веб-архив».

На момент времени уточнения информации (17.06.2025, 10:15) на сайтах администраций муниципальных образований по-прежнему опубликован баннер хакерской группировки Кибер-Партизаны. Доступ к сайтам был заблокирован 17.06.2025 в 10:22.

С использованием сервиса CMS-Checker определить используемые панели управления контентом и веб-технологии атакованных сайтов не удалось. Вероятно, использовалась специфическая система управления сайтами.

При помощи сервиса <https://web.archive.org/> установлено, что разработчиком сайтов муниципальных образований является компания donspros (<https://donspros.ru/>, ООО «Донспрос», ИНН 6154135778, г. Таганрог).

ООО «Донспрос» осуществляет разработку и поддержку сайтов государственных организаций.

При помощи сервиса <https://web.archive.org/> установлено, что после 21.02.2021 сайт компании donspros недоступен из сети Интернет, а с 30.05.2024 доменное имя сайта компании, предположительно, было выкуплено.

При помощи сервиса <https://2ip.ru/> установлено, что текущие IP-адреса сайта donspros (104.21.61.190, 172.67.213.15) расположены на хостинге Cloudflare, Inc.(США).

При помощи сервиса <https://2ip.ru/> также установлено, что атакованные сайты администраций муниципальных образований расположены на ресурсах хостинг-провайдера timeweb.cloud (<https://timeweb.cloud/>, ООО «ТАЙМВЭБ.КЛАУД», ИНН 7810945525, г. Санкт-Петербург).

Также установлено что некоторые муниципальные образования владеют дублирующими (дополнительными) сайтами, которые функционируют на базе других (альтернативных) хостингов и имеют иное (отличное от атакованного) доменное имя. В ходе анализа информации установлено (16.06.2025, 15:27), что дополнительные сайты муниципальных образований функционировали в штатном режиме, а именно:

- сайт Администрации Казансколопатинского сельского поселения (<https://k-lopatinskoesp.donland.ru/>).

- сайт Администрации Нижнебыковского сельского поселения (<https://nignebykovskoesp.donland.ru/>);

- сайт Администрации Шарнutowского сельского поселения (<https://sharnutovskoe-r08.gosweb.gosuslugi.ru/>);

- сайт Администрации Шумилинского сельского поселения (<https://shymilinskoesp.donland.ru/>);

- сайт Администрации Верхнявского сельского поселения (<https://verhnyakovskoesp.donland.ru/>);

- сайт Администрации Заводского сельского поселения (<https://zavodskoe-r69.gosweb.gosuslugi.ru/>).

Вероятно, атака на сайты муниципальных образований была проведена с использованием учетных данных их разработчика.

Источник информации: https://t.me/cpartisans_by/1658?comment=101853.

Таблица – Результаты проверки атак

№	Наименование муниципального образования	ИНН	Регион	URL-адрес	Подтверждение результатов атаки
1.	Администрация Андреево-Мелентьевского Сельского Поселения	6123013787	Ростовская область	андреево-мелентьево.рф	Подтверждено
2.	Администрация Аршаньзельменского СМО РК	0808900073	Республика Калмыкия	аршаньзельменское-смо.рф	Подтверждено
3.	Администрация Багаевского Сельского Поселения Багаевского района Ростовской области	6103600307	Ростовская область	bagaevskoesp.ru	Не подтверждено ¹
4.	Администрация Барило-Крепинского Сельского Поселения	6130703171	Ростовская область	b-krepinskoesp.ru	Не подтверждено
5.	Администрация Богородицкого Сельского Поселения	6127011082	Ростовская область	bogoroditskaya-adm.ru	Не подтверждено
6.	Администрация Болдыревского Сельского Поселения	6130703157	Ростовская область	boldirevskoesp.ru	Подтверждено
7.	Администрация Большекрепинского Сельского Поселения	6130703140	Ростовская область	bolshekrepskoesp.ru	Подтверждено
8.	Администрация Большенеклиновского Сельского Поселения	6123013949	Ростовская область	большенеклиновское-сп.рф	Подтверждено
9.	Администрация Большинского Сельского Поселения	6133007609	Ростовская область	bolshinskoesp.ru	Подтверждено
10.	Администрация Вареновского Сельского Поселения	6123013882	Ростовская область	varenovskaya-adm.ru	Подтверждено
11.	Администрация Васильево-Ханжоновского Сельского Поселения	6123013794	Ростовская область	v-hangonovskaya-adm.ru	Подтверждено
12.	Администрация Вербовологовского с/п	6108006859	Ростовская область	verbologovsp.ru	Не подтверждено
13.	Администрация Верхнеобливского Сельского Поселения	6134009863	Ростовская область	verhneoblivskoesp.ru	Не подтверждено
14.	Администрация Верхнесвечниковского Сельского	6115902542	Ростовская область	verhnesveshnikov.ru verhnesvechnikovskoe.ru	Не подтверждено

¹ Сайт не функционирует. Подтверждающая информация не обнаружена. Информация уточняется

№	Наименование муниципального образования	ИНН	Регион	URL-адрес	Подтверждение результатов атаки
	Поселения				
15.	Администрация Верхняковского Сельского Поселения	6105006811	Ростовская область	verhnyakovskoesp.ru	Не подтверждено
16.	Администрация Веселовского Сельского Поселения	6108006866	Ростовская область	veselovskaya-adm.ru	Не подтверждено
17.	Администрация Вознесенского Сельского Поселения	6121009560	Ростовская область	voznemenskaya-adm.ru	Подтверждено
18.	Администрация Вольно-Донского Сельского Поселения	6121009552	Ростовская область	volno-donskoesp.ru	Не подтверждено
19.	Администрация Горненского городского Поселения	6148555911	Ростовская область	gornenskoe-gp.ru	Не подтверждено
20.	Администрация Грузиновского Сельского Поселения	6121009591	Ростовская область	gruzinovskoesp.ru	Не подтверждено
21.	Администрация Гусевского Сельского Поселения	6114008974	Ростовская область	gusevskaya-adm.ru	Не подтверждено
22.	Администрация Дегтевского Сельского Поселения	6149010639	Ростовская область	degtevskoesp.ru	Подтверждено
23.	Администрация Дячкинского Сельского Поселения	6133007704	Ростовская область	dyachkinskoesp.ru	Не подтверждено
24.	Администрация Ефремово-Степановского Сельского Поселения	6133007581	Ростовская область	e-stepanovskoesp.ru	Не подтверждено
25.	Администрация Заводского Сельского Поселения	7011005162	Томская область	zavodscoe.ru	Подтверждено
26.	Администрация Зеленовского Сельского Поселения	6133007662	Ростовская область	zelenovskaya-adm.ru	Подтверждено
27.	Администрация Знаменского Сельского Поселения	6121009584	Ростовская область	znamenskaya-adm.ru	Подтверждено
28.	Администрация Индустриального Сельского Поселения	6115902574	Ростовская область	industrialnoesp.ru	Не подтверждено
29.	Администрация Кагальницкого Сельского Поселения	6113016299	Ростовская область	kagalnickoe.ru	Не подтверждено

№	Наименование муниципального образования	ИНН	Регион	URL-адрес	Подтверждение результатов атаки
30.	Администрация Казанского Сельского Поселения	6105006794	Ростовская область	kazanskoe-sp.ru	Не подтверждено
31.	Администрация Казансколопатинского Сельского Поселения	6105006843	Ростовская область	k-lopatinskoesp.ru	Не подтверждено
32.	Администрация Калиновского Сельского Поселения	6101035804	Ростовская область	kalinovskoe.ru	Не подтверждено
33.	Администрация Камышевского Сельского Поселения	6112912750	Ростовская область	kamishevskaya.ru	Не подтверждено
34.	Администрация Киевского Сельского Поселения	6115902510	Ростовская область	kievskaya-adm.ru	Не подтверждено
35.	Администрация Кировского СМО РК	808900066	Республика Калмыкия	kirovsp.ru	Не подтверждено
36.	Администрация Коробкинского СМО РК	0808900080	Республика Калмыкия	korobkinskoesp.ru	Не подтверждено
37.	Администрация Костино-Быстрианского Сельского Поселения	6121009538	Ростовская область	k-bystrsp.ru	Не подтверждено
38.	Администрация Красновского Сельского Поселения	6133007687	Ростовская область	krasnovskoe-sp.ru	Не подтверждено
39.	Администрация Краснооктябрьского Сельского Поселения	6106902948	Ростовская область	kr-octaybrskoesp.ru	Не подтверждено
40.	Администрация Краснополянского Сельского Поселения	6127011156	Ростовская область	krasnopolyanskaya-adm.ru	Не подтверждено
41.	Администрация Кринично-Лугского Сельского Поселения	6117010844	Ростовская область	krinichno-lugskoesp.ru	Не подтверждено
42.	Администрация Куйбышевского СП	6117010837	Ростовская область	kuyb-sp.ru	Не подтверждено
43.	Администрация Лакедемоновского Сельского Поселения	6123013843	Ростовская область	lakedemonovskaya-adm.ru	Не подтверждено
44.	Администрация Малокаменского Сельского Поселения	6114008942	Ростовская область	malokamenskaya-adm.ru	Не подтверждено
45.	Администрация Мещеряковского Сельского Поселения	6105006850	Ростовская область	meherakovskoesp.ru	Не подтверждено

№	Наименование муниципального образования	ИНН	Регион	URL-адрес	Подтверждение результатов атаки
46.	Администрация Мирненского Сельского Поселения	6108006827	Ростовская область	mirnenskoesp.ru	Не подтверждено
47.	Администрация Нижнебыковского Сельского Поселения	6105006829	Ростовская область	nignebykovskoesp.ru	Подтверждено
48.	Администрация Николаевского Сельского Поселения	6123013924	Ростовская область	nikolaevskoesp.ru	Подтверждено
49.	Администрация Новобессергеновского Сельского Поселения	6123013917	Ростовская область	novobessergenovskoesp.ru	Подтверждено
50.	Администрация Новокривошеинского Сельского Поселения	7009003376	Томская область	novokriv.ru	Подтверждено
51.	Администрация Обильненского Сельского Поселения	6101035868	Ростовская область	obilnenskaya-adm.ru	Подтверждено
52.	Администрация Обильненского СМО РК	808900059	Республика Калмыкия	obilnenskoe-smo.ru	Не подтверждено
53.	Администрация Парамоновского Сельского Поселения	6121009619	Ростовская область	paramonovskoe-sp.ru	Не подтверждено
54.	Администрация Первомайского Сельского Поселения	6115902486	Ростовская область	pervomaiskaya-adm.ru	Не подтверждено
55.	Администрация Пешковского Сельского Поселения	6101035882	Ростовская область	peshkovskoesp.ru	Не подтверждено
56.	Администрация Позднеевского Сельского Поселения	6106902923	Ростовская область	pozdnееvskoe-sp.ru	Не подтверждено
57.	Администрация Покровского Сельского Поселения	6123013868	Ростовская область	pokrovskaya-adm.ru	Не подтверждено
58.	Администрация Поливянского Сельского Поселения	6127011170	Ростовская область	polivyanskoaya-adm.ru	Не подтверждено
59.	Администрация Поляковского Сельского Поселения	6123013956	Ростовская область	polyakovskoe.ru	Не подтверждено
60.	Администрация Правобережного Сельского Поселения	2004000189	Чеченская Республика	pravoberegnenskoe-sp.ru	Не подтверждено

№	Наименование муниципального образования	ИНН	Регион	URL-адрес	Подтверждение результатов атаки
61.	Администрация Рыбасовского Сельского Поселения	6153023694	Ростовская область	ribasovskaya-adm.ru	Не подтверждено
62.	Администрация Салынтугтунского СМО РК	0808900098	Республика Калмыкия	saluntugtunskoe-sp.ru	Не подтверждено
63.	Администрация Самарского Сельского Поселения	6101035917	Ростовская область	samarskoe-adm.ru	Не подтверждено
64.	Администрация Самбекского Сельского Поселения	6123013875	Ростовская область	sambekskoesp.ru	Не подтверждено
65.	Администрация Синявского Сельского Поселения	6123013829	Ростовская область	sinyavskaya-adm.ru	Не подтверждено
66.	Администрация Советинского Сельского Поселения	6123013931	Ростовская область	sovetinskoe-sp.ru	Не подтверждено
67.	Администрация Солонцовского Сельского Поселения	6105006882	Ростовская область	solontsovskoesp.ru	Не подтверждено
68.	Администрация Старицинского Сельского Поселения	7011005130	Томская область	staricinskoe-sp.ru	Не подтверждено
69.	Администрация Тарасовского Сельского Поселения	6133007694	Ростовская область	tarasovskaya-adm.ru	Не подтверждено
70.	Администрация Тацинского Сельского Поселения	6134009983	Ростовская область	tacinskoesp.ru	Не подтверждено
71.	Администрация Терского Сельского Поселения	2004000171	Чеченская Республика	terskoe-sp.ru	Не подтверждено
72.	Администрация Титовского Сельского Поселения	6149010607	Ростовская область	titovskoe-sp.ru	Не подтверждено
73.	Администрация Толстой-Юртовского Сельского Поселения	2004000615	Чеченская Республика	tolstoy-urtsp.ru	Подтверждено
74.	Администрация Троицкого Сельского Поселения	6123013804	Ростовская область	troitskaya-adm.ru	Подтверждено
75.	Администрация Уманцевского СМО РК	0808900115	Республика Калмыкия	umantsevskoe.ru	Подтверждено
76.	Администрация Усть-Донецкого городского Поселения	6135006985	Ростовская область	ustdoneckaya-adm.ru	Подтверждено

№	Наименование муниципального образования	ИНН	Регион	URL-адрес	Подтверждение результатов атаки
77.	Администрация Федоровского Сельского Поселения	6123013900	Ростовская область	fedorovskaya-adm.ru	Не подтверждено
78.	Администрация Федосеевского Сельского Поселения	6110010274	Ростовская область	fedoseevskoesp.ru	Не подтверждено
79.	Администрация Фомино-Свечниковского Сельского Поселения	6115902528	Ростовская область	f-svechnikovsp.ru	Не подтверждено
80.	Администрация Хомутовского Сельского Поселения	6113016316	Ростовская область	homutovskaya-adm.ru	Не подтверждено
81.	Администрация Шарнутовского СМО РК	0808900108	Республика Калмыкия	sharnyt.ru	Не подтверждено
82.	Администрация Широко-Атамановского Сельского Поселения	6121009577	Ростовская область	s-atamansp.ru	Не подтверждено
83.	Администрация Шумилинского Сельского Поселения	6105006836	Ростовская область	shymilinskoesp.ru	Не подтверждено
84.	МБОУ Ленинская СОШ (не является ОГВ)	6106004503	Ростовская область	leninscaya-school.ru	Не подтверждено
85.	МБУК «В-Ханжоновский ДК» (не является ОГВ)	6123014205	Ростовская область	dk-v-hanjonovka.ru	Подтверждено
86.	МУК «Гусевский ЦПСДК» (не является ОГВ)	6114010236	Ростовская область	gusevskoe-sdk.ru	Не подтверждено
87.	МУП БТИ (не является ОГВ)	6123008890	Ростовская область	neklinovka-bti.ru	Не подтверждено
88.	ООО «УК «Единство» (не является ОГВ)	6135008510	Ростовская область	edinstvo-uk.ru	Не подтверждено

УТЕЧКИ ДАННЫХ

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

Дополнительная информация

Сведения о хакерских группировках и ВПО.

1. В Telegram-канале (https://t.me/Russian_OSINT) сообщается о том, что специалистам Kaspersky ICS CERT удалось выявить и проанализировать вредоносные программы и утилиты, использованные проукраинской хакерской группировкой Кибер-Партизаны (*ранее упоминалась в информационных справках*) в серии недавних атак на промышленные предприятия и государственные учреждения России и Беларуси.

Установлено, что начальным вектором атак является рассылка фишинговых писем, содержащих инсталлятор, который устанавливает в систему легитимную программу FortiClient VPN, а также скрытно устанавливает ВПО типа «бэкдор» **DNSCat2** (*ранее не упоминалось в информационных справках*). Ключевая особенность данного ВПО заключается в способности обходить меры изоляции сети, такие как правила блокирования трафика, поскольку взаимодействие с командным сервером осуществляется по протоколу DNS.

Отмечается, что хакерская группировка Кибер-Партизаны также использует другое ВПО типа «бэкдор», получившее название **Vasilek** (*ранее не упоминалось в информационных справках*). Особенность этого бэкдора заключается в том, что управление им (получение команд и отправка результатов их выполнения) осуществляется не через классический командный сервер (C&C), а через группу в мессенджере Telegram. ВПО Vasilek используется нарушителями для сбора информации о системе (включая коды нажатых клавиш и скриншоты окон приложений), а также для сбора данных о сетевой инфраструктуре атакуемой организации.

Для уничтожения данных компрометируемой системы Кибер-Партизаны применяют ВПО типа «вайпер» Pryanik (*ранее не упоминалось в информационных справках*), функциональность которого активируется в определенную дату и время. Вайпер использует две версии драйвера защитного решения Zemana Anti-Malware, содержащего уязвимость **BDU:2023-03027** (CVE-2021-31728) (одна для систем с архитектурой x86, другая для x64). Затем вредоносная программа получает список процессов, работающих в системе. Если обнаружен процесс, связанный с защитными решениями, Pryanik отправляет управляющий код уязвимому драйверу, чтобы завершить работу этого процесса.

В ходе анализа инструментов, используемых нарушителями, было обнаружено множество утилит, применяемых для развития атаки (т. е. заражения других компьютеров в сети), из которых практически все являются утилитами с открытым исходным кодом. Эти утилиты можно условно разделить на несколько групп:

- полнофункциональные фреймворки постэксплуатации (Metasploit Framework, SharpSploit, Cobalt Strike и Sliver)
- инструменты для кражи учетных данных (Mimikatz);
- средства удаленного доступа (VNC-сервер, Aspia Remote Desktop, PSExec).

В ходе исследования также установлено несколько техник и соответствующих утилит, используемых нарушителями для туннелирования вредоносного сетевого

трафика и, как следствие, сокрытия своего присутствия в инфраструктуре атакуемой организации, среди которых:

- 3проху – утилита для создания прокси-серверов;
- Gost – утилита для проксирования и туннелирования сетевого трафика.

Помимо утилит, группа активно использовала скомпрометированные системы внутри сети жертвы в качестве прокси-серверов.

Анализ деятельности и применяемых инструментов реализации кибератак проукраинской хакерской группировки Кибер-Партианы также позволил выявить специалистам Kaspersky ICS CERT их связь с другой проукраинской хакерской группировкой – IT ARMY of Ukraine (*ранее упоминалась в информационных справках*).

Индикаторы компрометации:

Файловые индикаторы:

7C730289B150582D65622FEE14DAF1DE
A0D7545DCD71267D2D051A4646F91FEB
B3F91A4BFCD2EEB346E323B5CBEF2833
D9F7489A2CB324DB909CE49548E1DB79
021C89550F2CC0067891693C0B2301E6
13F9BE1C7501154E82626D883219B0F1
A4120003348FEDA59ED2A3B278E149BD
B78859EB6FD560548E1A99356D14FBB5
C19970454202AFF1D5AC289B0C0752DA
CC9E931FC7BFE857284BF2EC661399EE
CE338924524961F9553C49B3C2D6EBDE
749B194B2746479157048E08F36C0B05
D1A8081FF646A83666C7AA69204C17A5
0216931A3ED18710FD0CC247E9B98454
0368CCD16376517659B6BA0A63A33086
043A1AE4CB4FD6B2E46D70091FDFDA80
0AB6D6546094D93817E45390F77B840A
1192D60F12AC800DEB3BB94A326E2EFC
1606FF3CA7201B1EDD99A4885AD74479
18769F7D5AE7182135873EA29B586608
1F024F1BCF190DAB60FAE70F0760F92C
28408044F467FD6033E8E9272CF4AD0C
2BA3CE248489F54233FE66D232B8B399
2FFD44AF4277E78C0DCCF0DEB722FA71
3559069687B0F9982F29DCED5FED40B6
39E2604706EB137FF70619E21511F602
3B627D73EDE057BA29E3707736382FD7
457E261456BA5AC6BE9EF9ED4F46518E
45DA308F63B3675E8D0EB4D440D54319
46D785CD365E0B1514D156AB6EBC8C20
4A5EB4BCD4CA4E024DCB608D5E0C2DDD
5047C19C15DF7A356E76959F7921D09A
513AF4462F64719BD7861A2DAFF8E15D
56090EEEF953847D3E4D59729242EC24
5B88416749CDFE192393144EFAE82492
5CA2662B8DE5CC7D56A8E425EF59FBDD

5E29F706DB2FF0BFA9BE481960D52B0C
5F0E6A992521661AA30F627981C89CFD
60290EA2D6149BA5678A8F1FB7ABD1E1
6ADA80A78D15C39B6511D435389A0C32
6CB10D35E6884089CB192E3AB09BF921
718DF1E53B6B208AC46CF135251661DF
74D7FD33236D1024ADAD272C27FA4A04
7524640B6C66411C9F7A4494FA9ACA1C
7EE9A254AC0F571C6889793AF4CFCD3B
89ED6D4EF883A6B6C095CBB2CCFD774E
916B54455CCB7673FB28469B08B3340B
99634F5A23DB7AF8827AFFD095C5E0C0
9A102379C85547C543CA4B4A8FAB99EC
9B5E70FA77FFDC845AC96EAE7F013BB0
9F61EABEE7FEDE49BEEB7DA793FE4025
A268C3D5CAC25D9C03A2960E4EC6F756
A402859D74BCCDEB1E074D1EF837BF70
A5B2129462C6D78521F544A37F8CA21F
A681FE14BC71B14A91000FA8065153BF
A70AF2DB482B8BC2C442B5E55AB6F91B
A7EE2BE8288FCDAE91B5E4022B95AD3A
ADDBB3DEA38C7F114D9B55AC473AF9BD
BAC437D80CD0C65A7937681A9BF5A5E0
BE47583211DF677350E13EF82198D2D5
C060237A1C8D2DCCEFD46F99209312B9
C8C7128B536ACFB2A1531B0CB016F1CE
CE3CB372FC86A1BF8B8965F941903909
E596F7165F9792E9B201E00585ED3694
E5D80BF63B2D4DA0E6B1E91B4DC0E35A
E6F319DA7D9230850974E0B2FA664450
ED03D170568479661BBE47D3B72AABB6
F82207C8CA5C44FF3F3D3341C5B01F4C
FB966F7055BCDF8D21CE32E4DD71317C
FCE38AB03134AD9C4B63845FA456C3E2
FF230F470B3E77CF63CB17BC7A2745BB
6470C04186BD618D612FF765B4234C61
eef8bb0e23f4633ca53d3ac767294b20
a31f4e073c5700f3195b52caaa950971
21a558d7fc3934055302b8a0da78f830
952FC71A3B89BB6E6BB191A66EB4CA12
F72E9453C6B9044FBE5BAC9B5EE4E65F
05c17f58b31dbeb2c15d44d1a460a3e0
0633ed1e19ad9e1c6212c1f326e03d73
8CE8DF9CA659D0678F0236CB13FE8505
BF33354D4D1EDD928617B68365C2DF02
9BBBC01EE96D575DCFC2137FD319A379

Сетевые индикаторы:

3a01.net

0ce.org

gov-by.com

7cp.org

9lj.org

vmware.org.mx

103.219.153.203

p-society.org

Имена служб:

FortiGateUpdate

Ключи реестра:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\FortiGateUpdate

Пути к файлам:

c:\program files\common files\adobe\adobegcclient\agmservice.exe

c:\program files\common files\microsoft shared\update\wsussvc.exe

c:\program files\realtek\audio\hda\rtkaudioservice.exe

c:\program files\teamviewer\version9\tv_w64.exe

c:\teamviewer\version9\tv_w640001.exe

c:\users\user\appdata\roaming\telegram desktop\telegramupdater.exe

c:\users\user\appdata\roaming\telegram desktop\update0002.exe

c:\users\user\appdata\roaming\telegram desktop\updater.exe

c:\windows 2016 update\wsus.exe

c:\windows 2016 update\wsus0001.exe

c:\windows\bddeeeee.sys

c:\windows\bits.exe

c:\windows\def.dll

c:\windows\netsvc.exe

c:\windows\s.exe

c:\windows\spp.exe

c:\windows\ss.exe

c:\windows\system32\graphics2d.dll

c:\windows\system32\gsdll32.dll

c:\windows\system32\lvfs.exe

c:\windows\taskmon.exe

c:\windows\vmtoolsd.exe

c:\windows\vmware.exe

c:\Program Files\forefront tmg client\FwcProxy.exe

C:\Windows\System32\FortiGateUpdate.manifest

C:\Windows\System32\FortiGateUpdate.dll

C:\Windows\Temp\Rar.exe

C:\Program Files (x86)\Google\GoogleUpdater\129.0.6651.0\Crashpad\evx.exe

C:\Program Files (x86)\Google\GoogleUpdater\129.0.6651.0\Crashpad\spp.exe

C:\Program Files (x86)\Google\GoogleUpdater\129.0.6651.0\Crashpad\updater.exe

c:\Users\%UserName%\AppData\Roaming\Brother\pew.exe

c:\Users\%UserName%\AppData\Roaming\Brother\pde.exe

C:\WINDOWS\TEMP\mstfc.exe

C:\windows\system32\iis.exe

c:\windows\system32\winhttp.exe

c:\windows\temp\httpdr.log

Вердикты защитных решений
HEUR:Trojan.Win32.Vasilek.gen
Trojan.Win64.Vasilek.p
HEUR:Trojan.Win64.Vasilek.gen
Trojan.Win64.Agent.qwkbkz
Trojan.Win64.Vasilek.q
not-a-virus:NetTool.Win32.Agent.aelf
Trojan.Win32.Agentb.lnij
HEUR:Trojan.Win32.Agent.gen
Trojan.Win64.Agent.qwkciw
Trojan.Win32.Agent.xbnfrj
Trojan.Win32.Agent.ildg
Trojan.Win32.Vasilek.ak
Trojan.Win64.Agentb.kyfw
Trojan.Win64.Vasilek.r
Trojan.Win32.Vasilek.j
Trojan.Win32.Zapchast.bkvf
Trojan.Win64.Vasilek.s
Trojan.Win64.Agentb.kyfv
not-a-virus:NetTool.Win64.Agent.bw
Trojan.Win64.Agent.qwkswp
Trojan.PowerShell.Agent.aiw
Trojan.Win32.Agent.xbdvtb
not-a-virus:NetTool.Win32.Agent.aele
Trojan.Win32.Agent.ildf
Trojan.Win32.Vasilek.p
Trojan.Win64.Vasilek.o
Trojan.Win64.Kryptik.hx
Trojan.Win32.Vasilek.am
Trojan.Win32.Vasilek.z
Trojan.Win32.Agentb.live
Trojan.Win32.Vasilek.n
Trojan.Win32.Vasilek.an
Trojan.Win32.Vasilek.l
HEUR:HackTool.Win32.Gost.gen
HackTool.Win64.Gost.ac
HackTool.Win64.Gost.ae
HackTool.Win64.Gost.p
HackTool.Win64.Gost.a
HackTool.Win64.Gost.ai
HackTool.Win64.Gost.t
HackTool.Win64.Gost.v
HackTool.Win64.Gost.as
HackTool.Win64.Gost.aq
HackTool.Win64.Gost.au
HackTool.Win64.Gost.bd
Trojan-Dropper.Win32.Vasilek.a
Trojan.Win32.Vasilek.at

Trojan.Win32.Vasilek.au
Trojan.Win32.Agentb.lnii
Trojan.Win32.Vasilek.ao
Trojan.Win32.Agentb.miyo
HackTool.Win64.Agent.ly

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, включая блокирование/ограничение/контроль выполнения Powershell-скриптов, WMI-команд, Windows Shell-команд.
- минимизация пользовательских привилегий.

Источники информации:

https://t.me/Russian_OSINT/5675;

<https://ics-cert.kaspersky.ru/publications/reports/2025/06/05/ttps-of-cyber-partisans-activity-aimed-at-espionage-and-disruption/>.

2. На сайте СМИ (<https://www.rbc.ru/>) сообщается о выявлении нового вредоносного приложения SuperCard, которое используется нарушителями для кражи данных банковских карт.

В мае 2025 года были зафиксированы первые попытки атак на клиентов российских банков с помощью вредоносной версии приложения **SuperCard** (*ранее не упоминалось в информационных справках*). Это модификация легитимного инструмента NFCGate (*ранее упоминался в информационных справках*), предназначенного для работы с бесконтактными платежами. SuperCard позволяет перехватывать NFC-трафик и красть данные банковских карт, что может привести к несанкционированному списанию денежных средств.

В апреле 2025 года специалисты F6 обнаружили несколько Telegram-каналов, через которые распространялась подписка на это приложение. Сразу после запуска приложения пользователю показывается окно, предлагающее произвести сканирование QR-кода, предоставляемого разработчиками. В этот код вшиты username, password и host сервера, с которыми производится аутентификация пользователя на сервере нарушителей. Таким образом нарушители реализовали функционал для предоставления вредоносного ПО по схеме MaaS (Malware-as-a-Service) – покупателю достаточно лишь отсканировать QR-код для организации доступа к функционалу приложения.

Также установлено, что некоторые образцы SuperCard могут получать не только NFC-трафик, но и данные банковской карты, считанные с помощью отправки команд на ее EMV-чип.

Таким образом, нарушители получают:

- номер карты;
- дату окончания срока действия;
- информацию о платежной системе;
- программное обеспечение чипа карты.

Специалисты компании F6 также сообщают, что в первом квартале 2025 года ущерб от всех версий NFCGate и SuperCard в России составил 432 млн рублей, а количество заражённых Android-устройств превысило 175 тысяч.

Индикаторы компрометации:

Файловые индикаторы:

MD5: 37ed019e1dcaeab3053de98e1f77f7f6

SHA1:ea2f253c82e27a06e89fb7a4a5ddbb5ed96f9168

SHA256: 318a0bf427b185b9b4c8be53e2f2e2b4521ef725203e340e5c24de9648d5f81d

MD5: d2bbe5e1f10ab721103ace0e5c67486b

SHA-1: 568f96b0f7bdca3c1c66c8cf3c0a77f7e29e45aa

SHA-

256:ffd418d938ea06ae4ba954cccbc311aeacd0d6da823fca4a6d1ed4b89ed1267e11

Возможными мерами защиты являются:

- установка приложений только из достоверных источников;
- использование средств антивирусной защиты;
- ограничение доступа к конфиденциальной информации банковских карт (PIN-или CVV-коды).

Источники информации:

https://www.rbc.ru/life/news/6850fd3f9a794728365642b1?utm_source=yxnews&utm_medium=desktop&utm_referrer=https%3A%2F%2Fdzen.ru%2Fnews%2Fstory%2F5abc68b2-388c-5c3e-bf15-dc56ada42a89;

<https://www.anti-malware.ru/news/2025-06-17-111332/46356>;

<https://www.f6.ru/blog/supercard/>.

3. На сайте (<https://rt-solar.ru/>) опубликована информация о ВПО типа «бэкдор» LuckyStrike Agent (*ранее упоминалось в информационных справках*), применяемом хакерской группировкой Erudite Mogwai (*ранее упоминалась в информационных справках*).

Установлено, что ВПО LuckyStrike Agent состоит из следующих модулей:

- LuckyStrike.dll – загрузчик, является .NET-библиотекой, расшифровывает и запускает основную вредоносную нагрузку;
- log.cached - зашифрованный конфигурактор вредоносной нагрузки;
- netfxsbs9.hkf – зашифрованная вредоносная нагрузка;
- UevAppMonitor.exe – легитимный файл, является частью технологии UE-V;
- UevAppMonitor.exe.config – конфигурактор, используемый для инъекции вредоносной библиотеки.

Данное ВПО использует технику AppDomain Manager Injection (T1574.014). Она позволяет загружать вредоносные .NET-сборки в легитимные .NET-приложения. В качестве такого приложения нарушители используют UevAppMonitor.exe. В качестве C2-сервера используется OneDrive, однако архитектура бэкдора позволяет использовать и другие облачные сервисы.

Установлено, что бэкдор LuckyStrike Agent выполняет следующие функции:

- исполняет консольные команды;
- загружает и исполняет кастомные сборки (Assembly);
- удаляет и загружает файлы;

- собирает информацию о файлах в директориях - имя, размер, путь, base64 от иконки, время последней записи в файл и является ли путь директорией;

- собирает информацию о дисках - имя диска и объем.

Индикаторы компрометации:

Файловые индикаторы:

0a61f81d4c24fdc2f7360c6b19b569055aa1f3adb6fc15d500a81fc9862c7a49
d676a8bbaf95612305efa9500356294ec14d332baa16ed4980e4c47a8d4b831b
6f3b79f32625e568d48bd59887d3bd0b0648256fe24a3677ef6bef154d120118
fd647324461f4114d258102ccafaddf4a50041f7d5425f62009b89395166d588
94a16337fefbed7c77826731bf32f922f4ad8fa3a6ac19febcd4343f5a41a623
0d02ebe3b7c366b8458e5518d7424befb1ecd85117c769b880b59fa979e8408b
26ac58cd3addf226ebcc1173f0b237942176ed7cf311e0ff8bfa6bf5c6ea80e8
89fcea271d9a647aab772bf13407407b4f93ab3926f7feef68e13a1bbbf7fc4d
efa406b93ccb39704c2cbdbe5e49611777b17786834b416d1fb7256d3d914452
89fcea271d9a647aab772bf13407407b4f93ab3926f7feef68e13a1bbbf7fc4d
e4cb17978d132ab8518cfbd6362cbfa7f281cacf1b79eead24286ad7b5b7b94d
c97d88ea4b6592b42bc6b1b9d890c5f7c498b82741a57d4a634bae02b9bc3048

Возможными мерами защиты являются:

- использование средств межсетевого экранирования;

- использование систем обнаружения вторжений при организации доступа к сети

Интернет;

- использование средств антивирусной защиты;

- использование SIEM-систем для отслеживания событий безопасности;

- ограничение доступа к устройству из внешних сетей (Интернет);

- использование надежных паролей;

- реализация мер изолированной программной среды;

- минимизация пользовательских привилегий.

Источники информации:

https://t.me/four_rays/97;

<https://rt-solar.ru/solar-4rays/blog/5603/>.