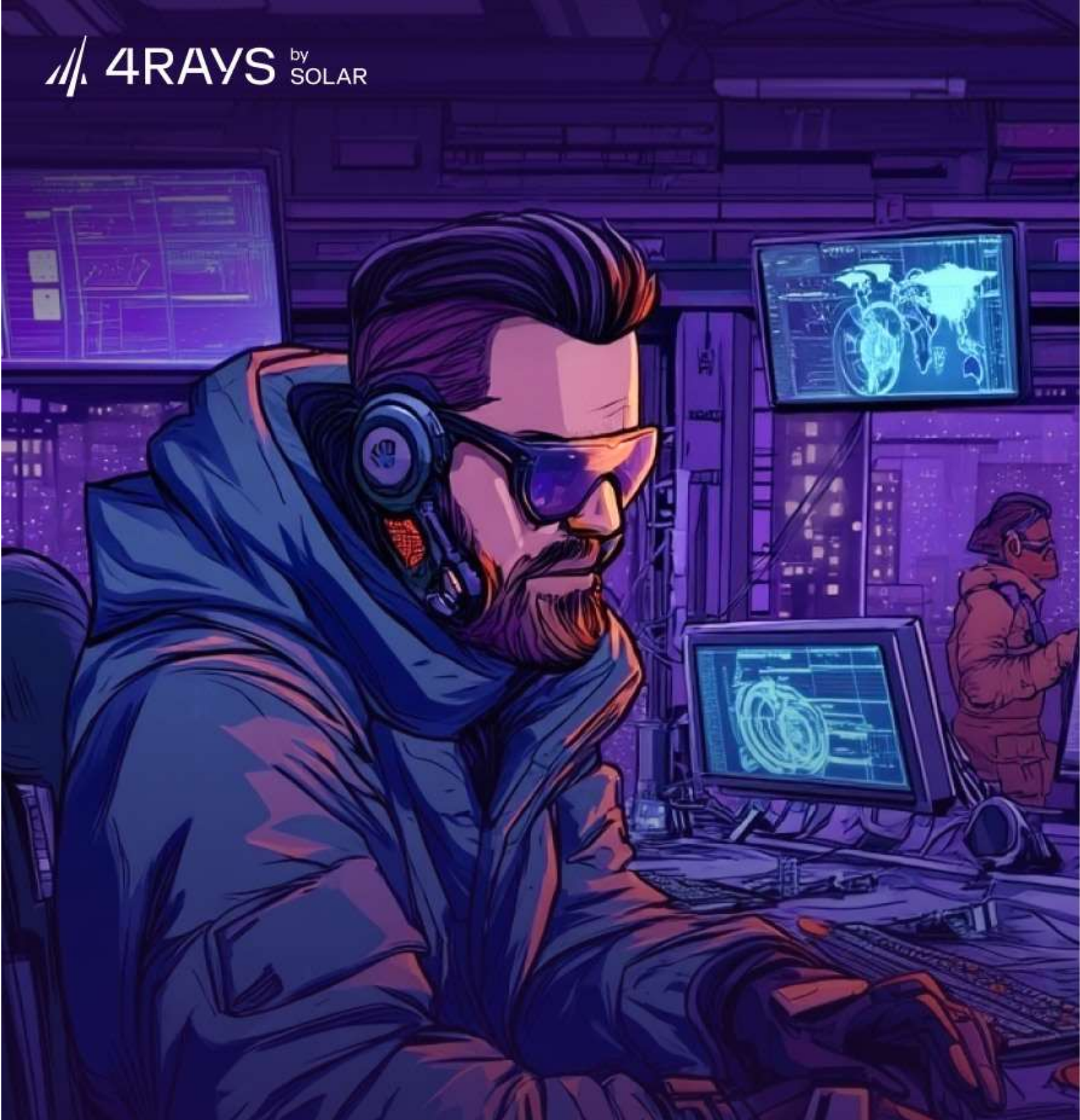
4RAYS by SOLAR



SOLAR 4RAYS: ХРОНИКИ РАССЛЕДОВАНИЙ ИНЦИДЕНТОВ

1-е полугодие 2026 года

Введение

Команда центра исследования киберугроз Solar 4RAYS ГК «Солар» участвует в расследовании десятков ИБ-инцидентов в российских частных и государственных организациях. В абсолютном большинстве случаев речь идет об атаках, осуществленных группами профессиональных взломщиков, преследующих финансовые цели или работающих в интересах иностранных правительств. Как правило, это инциденты, которые произошли по двум причинам: злоумышленники смогли обойти использовавшиеся в атакованных организациях автоматизированные средства защиты или организации просто не имелось соизмеримых угрозе ИБ-инструментов.

В ходе расследований эксперты Solar 4RAYS собирают различные данные о характеристиках атак, анализ которых позволяет сформировать представление об актуальных тактиках, техниках и процедурах злоумышленников, оценить уровень ИБ-риска для конкретной организации и в конечном счете выстроить эффективную защиту ИТ-инфраструктуры от профессиональных киберпреступников.

В основе отчета — данные, собранные в ходе расследований, проведенных за первое полугодие 2026 года. Также исследование содержит данные о наиболее атакуемых отраслях, квалификации злоумышленников и их мотивации. Кроме того, в отчете представлен обзор основных кибергруппировок, с деятельностью которых эксперты Solar 4RAYS столкнулись в ходе расследований.

Ключевые тренды

- На организации из отрасли промышленности пришлась большая (31%) часть инцидентов, что на 11 процентных пунктов больше, чем год назад. В фокус интереса атакующих такие предприятия попали в 2025 году впервые за историю наших наблюдений, и в 2026 году тенденция продолжилась.

- Шпионаж остается главной целью атакующих (42%), но также выросла доля инцидентов с неизвестными целями.

- Уязвимости в веб-приложениях — самый частый способ проникновения в организацию (46%). В первом полугодии атакующие концентрировались на популярном российском ПО и ПО на открытом коде.

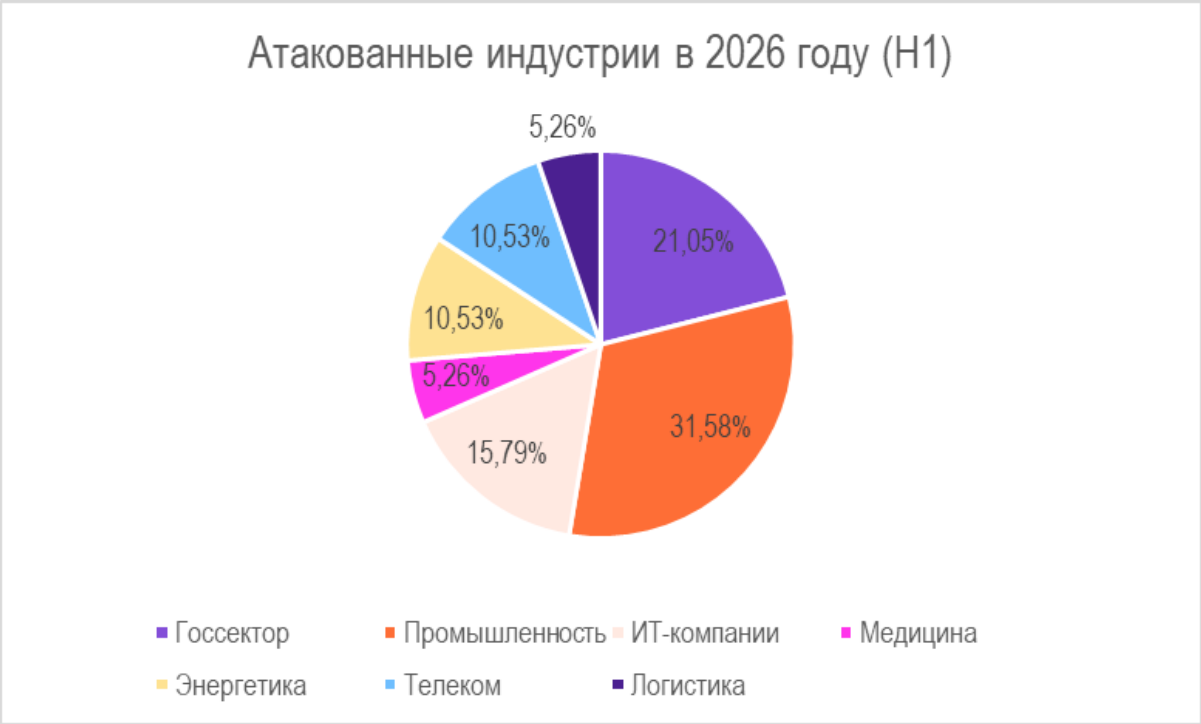
- Среди профессиональных группировок наблюдается аномальное затишье: за первые полгода эксперты Solar 4RAYS зафиксировали активность лишь четырех ранее известных вредоносных кластеров. Годом ранее их было шесть, а по итогам 2025 года — 18.

- Четверть расследованных инцидентов длилась до недели, а длительность каждой пятой атаки не превышала месяц. Доля «коротких» атак снизилось за счет роста инцидентов длительностью от двух недель до года, при этом доля «длинных» атак более года также снизилась.

Обзор инцидентов

Кого атакуют

За первое полугодие 2026 года эксперты Solar 4RAYS расследовали киберинциденты в организациях из семи различных отраслей, включая госсектор, телеком, промышленность и IT.



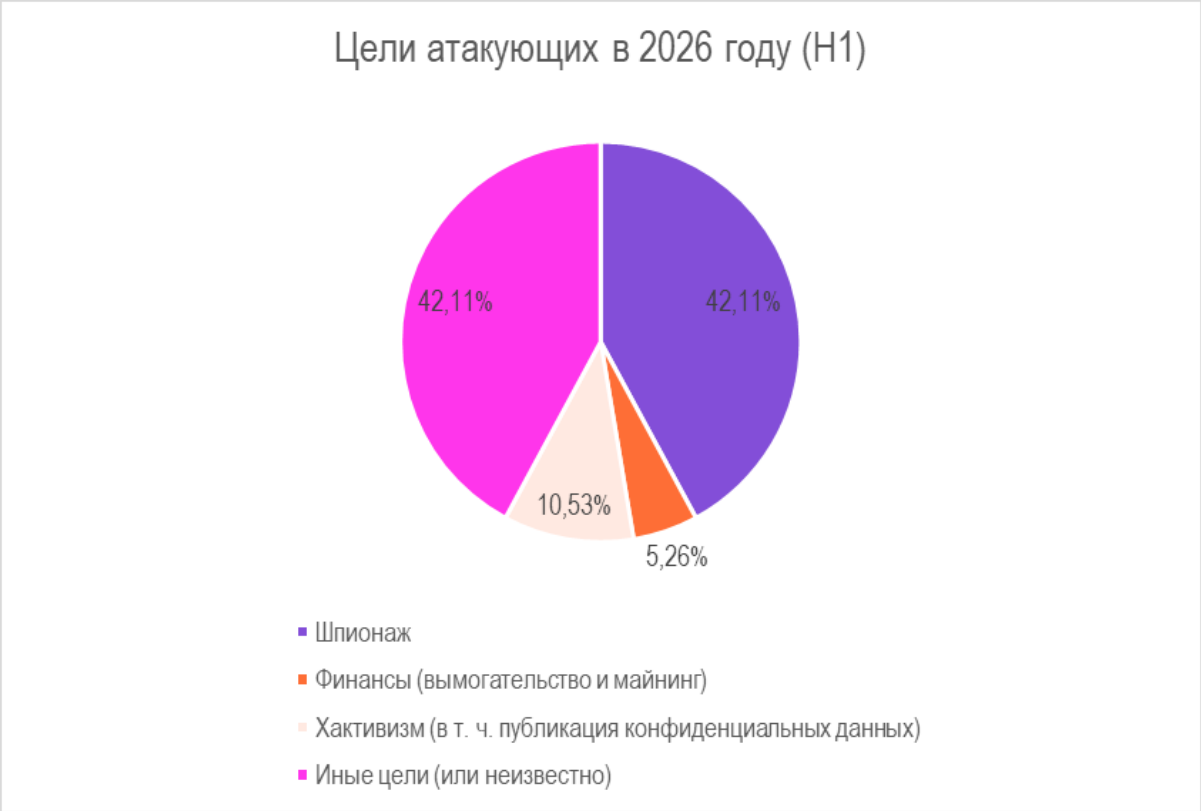
Этот список изменился незначительно в сравнении с аналогичным периодом прошлого года. Наметившийся в 2025 году тренд на рост атак против промышленности продолжает развиваться: доля таких инцидентов за год выросла на 11 процентных пунктов (п. п.), демонстрируя фокус атакующих на производственном секторе. Также выросла доля атак на IT-компании (3,79 п. п.). Доля инцидентов в организациях госсектора сократилась на 14,5 п. п., но все еще значительна: каждый пятый инцидент, который мы расследовали с начала года, происходил в организациях, связанных с государством.

Любопытное изменение первого полугодия: снижение результативности атакующих в нападениях на энергетическую отрасль. В нашем отчете об угрозах на базе сенсоров PDNS за первый квартал 2026 г. мы отмечали большое число индикаторов потенциального заражения вредоносным ПО в предприятиях энергетического сектора, однако в первом полугодии 2026-го нашей команде DFIR не довелось расследовать хотя бы один успешный с точки зрения атакующих инцидент в энергетике. При этом год назад, по итогам первого полугодия 2025 года, таких инцидентов было 12%, а концу года их доля возросла до 17%.

Непросто сделать предположение о причинах такого изменения. Возможно, это следствие общего «затишья», которое мы наблюдаем в сфере сложных кибератак с начала года: кибернападений, которые доходят до стадии, когда необходимо привлекать DFIR-специалистов, стало меньше во всех отраслях. Другой причиной может быть адекватная реакция защитных команд энергетических предприятий на усиление фокуса атакующих, благодаря которой атаки останавливались на ранних этапах.

Цели атакующих

В первом полугодии стало больше инцидентов, по которым к команде DFIR Solar 4RAYS обращались достаточно оперативно, чтобы атаку можно было остановить на раннем этапе. Из-за этого в почти половине случаев, которые мы расследовали, у нас нет достаточно артефактов, чтобы сделать четкий вывод о цели атаки. Атакующие просто не успели совершить действия, которые могли бы сказать об их намерении.



В оставшейся половине случаев мотивация атакующих была прозрачной, и здесь по сравнению с аналогичным периодом 2025 года изменений нет: большая часть атак направлена на шпионаж, а финансы и хактивизм — на втором и третьем местах.

Впрочем, окончательные выводы о целях атакующих делать рано. Ряд инцидентов, случившихся в первом полугодии, все еще расследуются, и общая картина мотивации злоумышленников может стать яснее, когда эти расследования будут завершены.

Способы первоначального проникновения

Наметившийся в прошлом году тренд на рост числа атак через подрядчиков в начале 2026 года оборвался. Пока что мы не столкнулись ни с одним инцидентом, где атакующие проникли бы в целевую инфраструктуру через инфраструктуру одного из своих партнеров.

Превалирующим методом проникновения остаются уязвимости в веб-приложениях, доступных из сети. Их доля возросла с 46% в первом полугодии 2025 года до 58% в первом полугодии 2026-го.

Однако следует отметить, что почти треть инцидентов из первого полугодия все еще находятся в стадии расследования и, как и в случае с предыдущим разделом, «расстановка сил» в рейтинге наиболее распространенных методов проникновения еще может поменяться.

Длительность инцидентов

Метрика «Длительность инцидентов» описывает временной промежуток, в течение которого атакующие оставались в целевой инфраструктуре. По итогам первого полугодия 2026 года самым значительным изменением стало сокращение доли «коротких» инцидентов (до недели) с 32 до 26%, а кроме того, рост доли инцидентов, длящихся около месяца. Атакующим чаще удавалось провести первоначальное закрепление, но в меньшем количестве случаев им удалось сохранить свое присутствие в инфраструктуре на длительное время.

	2025 г. (H1)	**2026 г. (H1)**
До недели	32%	26%
До двух недель	0%	5%
До месяца	16%	21%
До 6 месяцев	16%	16%
До 1 года	12%	16%
До 2 лет	16%	11%
2+ года	7%	5%

4RAYS by SOLAR

ГРУППИРОВКИ И КЛАСТЕРЫ ВРЕДОНОСНОЙ АКТИВНОСТИ

Активность группировок

Если бы была необходимость описать ситуацию в ландшафте группировок, атакующих в первом полугодии одним выражением, то это было бы «аномальное затишье». С начала года и вплоть до июня количество инцидентов оставалось непривычно малым за всю историю наших наблюдений. При этом пассивные инструменты наблюдения (сеть сенсоров PDNS, статистика, аккумулируемая нашим центром противодействия кибератакам Solar JSOC) сигнализировали об активности APT-группировок весь этот период, но лишь единицы из этих примеров выливались в инциденты, требующие участия DFIR-специалистов. В тех инцидентах, что случились, мы совсем перестали видеть следы групп, которые ранее регулярно попадались на наших «радарах». За шесть месяцев мы идентифицировали активность четырех группировок: Fairy Trickster, GOFFEE, NGC5081 и Partisan Zmiy.

В совокупности на них пришлось 32% всех расследованных инцидентов, а остальные 68% пока что остаются неатрибутированными. Год назад ситуация была похожей.

Однако, как видно на графике, разновидность и география атакующих была заметно разнообразнее. В прошлом году мы отмечали «затишье», наступившее после довольно бурного по количеству инцидентов и активных группировок 2024 года. Вторая половина 2025 года показала значительное увеличение числа активных вредоносных кластеров, всего по итогам года их было около двух десятков. Результаты первого полугодия 2026 года заставляют сделать предположение об установившейся «цикличности» деятельности группировок, в рамках которой первое полугодие — время «тишины», в ходе которого атакующие действуют максимально скрытно или не действуют вовсе, а второе — период видимой активности, когда шаги группировок в атакованных инфраструктурах становятся более решительными и видимыми для ИБ-команд. Действительно ли это так, станет ясно ближе к концу года.

Еще одним характерным признаком первого полугодия стало отсутствие инцидентов, связанных с деятельностью группировок азиатского происхождения. В первом полугодии 2025 года мы расследовали несколько атак Erudite Mogwai, но за первые месяцы 2026-го следов этой группы, как и ее собратьев по региону, мы не наблюдали. В июле ситуация изменилась, и стало ясно, что восточноазиатские группировки продолжают деятельность в российских инфраструктурах, но подробнее об этом мы расскажем в отдельных будущих публикациях.

Наконец, главной неожиданностью полугодия для нас стало возвращение группировки NGC5081. О ее атаках на телеком-компании с помощью сложного бэкдора IDFKA мы рассказывали осенью прошлого года, и в течение нескольких месяцев после этого мы не видели никаких признаков деятельности этого кластера, пока в июне мы не поучаствовали в расследовании инцидента, в котором обнаружили новую версию бэкдора. Чуть более подробно об этом и других группах — в следующем разделе.

Характеристики активных группировок

Partisan Zmiy (Киберпартизаны*)

** Объединение «Киберпартизаны BY» признано экстремистской организацией, его деятельность запрещена на территории РФ.*

Partisan Zmiy — известная хактивистская группировка, сформированная в 2020 году.

В начале своей деятельности основной целью группировки выступала инфраструктура государственных органов Республики Беларусь, однако с февраля 2022 года география атак сместилась на Российскую Федерацию.

Особое внимание к группировке привлекла летняя кампания 2025 года, когда была зафиксирована масштабная атака на инфраструктуру компании «Аэрофлот».

Несмотря на снижение видимой активности в первом полугодии 2026 года, команда Solar 4RAYS считает, что группировка обновляет свой инструментарий. Об этом свидетельствуют расследования конца 2025 — начала 2026 года, где были выявлены новые семплы уже известных инструментов.

Арсенал группировки не претерпел существенных изменений:

- Vasilek;
- Prianik;
- 3proxy;
- GOST proxy;
- Forklift;
- PartisansDNS;
- DNSCat2.

Цели:

Группировка атакует государственные организации, транспортные и телекоммуникационные компании. Их основная задача — создать общественный резонанс и привлечь внимание к своей активности, а также нанести прямой ущерб жертве.

GOFFEE (Paper Werewolf)

GOFFEE — известная проукраинская хакерская группировка, активно атакующая различные организации на территории Российской Федерации. Основные цели группировки — шпионаж и кража данных.

Одним из инцидентов, случившихся из-за действий группировки, стал взлом организации, длившийся несколько лет, который команда Solar 4RAYS расследовала в течение первого полугодия. Одним из последних подтвержденных следов атаки было использование скомпрометированной учетной записи для удаленного подключения через WinRM.

Группировка имеет обширный арсенал инструментов, который не претерпел существенных изменений с прошлого годового отчета:

- Mythic Agent;
- Cobalt Strike;
- QwakMyAgent;
- DumpIt;
- SspiUacBypass;
- Impacket PsExec;
- Owowa;
- PowerTaskel;
- VisualTaskel.

Цели: организации, обладающие ценной информацией, включая государственные структуры, энергетические компании, транспортные системы и крупные корпорации.

NGC5081

NGC5081 — относительно молодая, но демонстрирующая высокий уровень зрелости в области кибератак группировка, впервые обнаруженная нами в 2025 году.

В отличие от множества других злоумышленников, NGC5081 демонстрирует комплексный подход к атакам на инфраструктуру потенциальной жертвы. Сложные бэкдоры, подход к мимикрии и скрытию своей активности делают из данной группировки серьезную угрозу.

В первом полугодии Solar 4RAYS стали свидетелями развития инструментария данной группировки. В будущем мы обязательно поделимся с вами новыми интересными кейсами, связанными с NGC5081 и их бэкдором IDFKA, так что следите за нашим блогом.

Инструменты:

- IDFKA;
- IDFKA Dropper;
- TinyShell.

Цели: Телекоммуникационные компании на территории Российской Федерации.

Fairy Trickster (Rainbow Hyena, Head Mare)

Fairy Trickster — хакерская группировка, чья активность впервые была зафиксирована в 2023 году. Со следами их атак в России мы столкнулись в середине 2024 года.

Fairy Trickster преследует различные цели: от обычного хактивизма до целенаправленных атак с целью шифрования данных и последующего вымогательства.

В конце 2025 года и в первые месяцы 2026-го данная группировка провела масштабную атаку на серверы, использующие программное обеспечение для видеоконференцсвязи TrueConf Server.

Инструменты:

- MeshAgent;
- LockBit 3.0;
- PhantomProxyLite;
- Rust SOCKS5 Proxy;
- T1ck3tDump;
- PhantomTaskShell.

Цели: группировка атакует организации любого сектора — от государственных структур до частных компаний. Основная направленность атак — монетизация атаки различными способами, будь то шифрование жертв с целью вымогательства или продажа конфиденциальных данных.

Интересные тактики и техники

Расследования в первом полугодии не отличились наличием сложных или ранее не используемых тактик и техник атакующих. Однако мы решили выделить те, что, на наш взгляд, являются интересными или представляют актуальность в рамках текущего полугодия.

Уязвимости повсюду…

В расследованных нами инцидентах лидирующим способом первичного доступа остаются уязвимости веб-приложений. Привлекательность данной техники для злоумышленников обусловлена потенциалом, который уязвимость предоставляет на начальном этапе атаки: от получения привилегированного доступа до выполнения произвольных команд на сервере.

Основными целями в первом полугодии стали отечественные веб-приложения, open-source-решения, а также самостоятельные проекты.

Например, в конце 2025 — начале 2026 года ряд компаний столкнулся с волной атак через уязвимости **BDU:2025-10114** и **BDU:2025-10116** программы TrueConf Server. Эти уязвимости, объединенные в единую цепочку, позволяли злоумышленникам выполнить произвольные команды от имени процесса tc_webmgr.exe, ответственного за управление панелью, гостевую страницу, личный кабинет, планировщик задач и настройку HTTPS-связи.

Также в первом полугодии мы встречали уязвимости, связанные с эксплуатацией неправильно сконфигурированных или недостаточно защищенных веб-файлов самописных веб-приложений. Так, в одном из инцидентов была обнаружена точка входа — PHP файл, который, по замыслу разработчиков, позволял выполнять SQL-запросы. Однако доступ к этому файлу ограничен не был, чем и воспользовались атакующие. В ряде других случаев мы видели атаки через уязвимости дополнительных программ и сервисов, использовавшихся поверх основных веб-приложений.

Значимым событием текущего периода стала волна атак, направленных на уязвимость программы ViPNet. Техника, примененная атакующими, основана на методе DLL Hijacking. Атакующие отправляли конверт через служебный протокол

MFTP с вредоносным файлом wtsapi32.dll, который сохранялся в файловой системе с использованием уязвимости Path Traversal. После чего процесс ltcsrvup64.exe (служба обновлений ViPNet) загружала его.

В ближайшем будущем мы опубликуем подробное описание данных инцидентов. Следите за нашим блогом!

(Без)опасные службы

Использование служб операционной системы Windows в целях выполнения вредоносного кода стало устоявшейся практикой любых атакующих. Чаще всего злоумышленники создают новую вредоносную службу либо изменяют уже существующую, например подменяя легитимный исполняемый файл. Другим способом использования служб стало комбинирование двух техник, а именно применение сервиса для выполнения и DLL sideloading.

Классическим примером совмещения техник стал один из расследованных нами инцидентов. Атакующие в ходе своей активности создали сервис, запускающий программу для резервного копирования данных веб-приложения. Несмотря на то что исполняемый файл службы был легитимным, в его процессе мы зафиксировали подозрительный модуль неизвестного происхождения. Модулем являлось ВПО класса «бэкдор». При запуске сервиса его исполняемый файл загружал вредоносную библиотеку в результате DLL sideloading из того же каталога, в котором сам и был расположен. Библиотека, в свою очередь, загружала вредоносный код бэкдора из зашифрованного файла .dat, который располагался в том же каталоге, что и все файлы сервиса.

Использование сервисов и DLL sideloading является эффективной, но при этом стандартной комбинацией техник атакующих. Нам встречались и более интересные методы взаимодействия с сервисами.

Одним из таких методов стало использование инструментов, позволяющих динамически изменять параметры службы, например NimExec, scshell или StealthyWMIExec. Такие инструменты позволяют атакующим выполнить необходимую команду без подмены исполняемого файла или создания нового сервиса. Более того, параметры после выполнения могут быть изменены на изначальные, что затрудняет обнаружение как на уровне файловой системы, так и в логах событий.

Заключение: обманчивое затишье

Первое полугодие 2026 года нельзя назвать напряженным, по крайней мере с точки зрения числа инцидентов, разнообразия применяемых атакующими техник и иных существенных перемен. Предприятия промышленности — ключевая цель атакующих, а уязвимости в веб-приложениях (особенно отечественных или самописных на базе открытого кода) — главный способ проникновения в инфраструктуры. Эти два вывода указывают на то, что нужно в первую очередь обратить внимание на внешний периметр любой организации, а именно обновить до актуальных версий веб-приложения и настроить мониторинг веб-серверов и т. д. Особенно это важно для компаний промышленного сектора.

В отчете за первое полугодие 2025 года мы уже отмечали, что наблюдаем «затишье» — инцидентов случалось сравнительно мало, ранее активные группировки ушли в тень. Второе полугодие показало, что «затишье» было перед «бурей»: количество инцидентов и активных групп значительно возросло. Отчет за первое полугодие 2026 года мы заканчиваем, находясь уже во втором полугодии, и отсюда видим, что и в этом году «спокойствие» первого полугодия было обманчивым: список расследований, в которых мы участвуем, увеличивается почти каждую неделю.

Чтобы снизить вероятность возникновения киберинцидента с серьезными для атакованной организации последствиями, мы рекомендуем не пренебрегать следующими мерами безопасности:

1. Уделяйте пристальное внимание своевременному обновлению ПО и защите веб-приложений (WAF). Атаки через уязвимости в веб-приложениях остаются самым распространенным способом первоначального проникновения, а WAF поможет заблокировать вредоносный трафик и предотвратить взломы на уровне приложений.
2. Соблюдайте парольные политики, пользуйтесь сервисами мониторинга утечек учетных записей и вовремя их обновляйте. Использование утекших учетных записей для первоначального проникновения — второй по популярности способ первоначального проникновения.
3. Серьезно относитесь к уведомлениям о возможной компрометации от Национального координационного центра по компьютерным инцидентам (НКЦКИ) и частных компаний, обладающих экспертизой в области ИБ.
4. Создавайте бэкапы, следуя принципу «3–2–1», который предполагает наличие не менее трех копий данных, хранение копии как минимум на двух физических носителях разного типа и наличие минимум одной копии за пределами основной инфраструктуры.
5. Используйте продвинутые средства защиты (EDR, SIEM) наряду с классическим защитным ПО, чтобы получать полную картину значимых для безопасности событий в инфраструктуре и вовремя обнаруживать нежелательные.
6. Делайте оценку компрометации регулярно и в случае подозрения на атаку не медлите с привлечением специалистов по реагированию на инциденты.

7. Повышайте киберграмотность сотрудников, ведь успешная атака на основе социальной инженерии возможна даже в самой защищенной инфраструктуре.
8. Следите за тем, чтобы служба ИБ имела постоянный доступ к последним сведениям о ландшафте киберугроз конкретного региона и индикаторам компрометации. Например, подпишитесь на наш телеграм-канал «Четыре луча». В нем мы публикуем информацию о самых свежих опасных уязвимостях, а также новых тактиках и техниках группировок атакующих.