4RAYS by SOLAR

Solar 4RAYS: Хроники DFIR

Отчет по итогам
10 месяцев 2024 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, потому что злоумышленники смогли обойти использовавшиеся в атакованных организациях автоматизированные средства защиты, либо потому, что в 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 итоге выстроить эффективную защиту ИТ-инфраструктуры от профессиональных киберпреступников.

В основе отчета – данные, собранные в ходе расследований, проведенных за 10 месяцев 2024 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

- Количество инцидентов, расследованных командой Solar 4RAYS за десять месяцев 2024 года, выросло почти на **45%** в сравнении с тем же периодом 2023 года;

- Количество сфер экономики, в которых работают атакованные организации, выросло **с 4 до 16**. В топе: госорганы, промышленность и телеком-операторы.

- Главные цели активных атакующих: шпионаж, уничтожение данных и вымогательство;

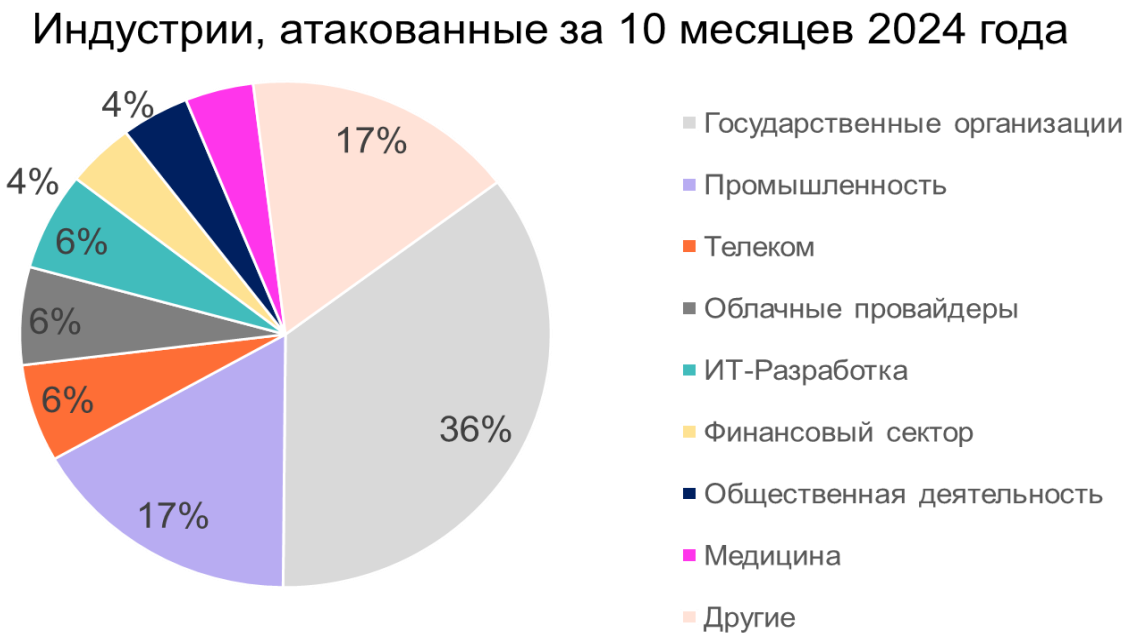
- Около **70%** расследованных инцидентов было связано с деятельностью проукраинских группировок;

- Каждый третий инцидент длился **не более недели**. За год доля таких инцидентов возросла 19%;

- **Уязвимости в веб-приложениях** и **скомпрометированные учетные записи** остаются основными методами первоначального проникновения. Атаки через доверительные отношения сохраняют заметную долю;

Обзор инцидентов: кого атакуют

За 10 месяцев 2024 году эксперты Solar 4RAYS расследовали киберинциденты в организациях из 16 различных отраслей, включая, госсектор, телеком, промышленность, ИТ. В категорию “Другие” попали организации из сферы ритейла, транспорта, логистики, энергетики, общественно-политической деятельности, информационной безопасности и даже религии.



За аналогичный период 2023 года эксперты Solar 4RAYS зафиксировали атаки в 4 индустриях.

Как видно, за год значительно сократилась доля атак на государственные организации и выросла доля атак на промышленность. К тому же в 2024 году помимо организаций, которые традиционно являются основными целями злоумышленников (госсектор, промышленность, финансы и ИТ), мы наблюдали атаки на сферы в, к которым ранее киберпреступники не проявляли особого интереса. Например, религиозные учреждения и предприятия, занятые в сельскохозяйственной промышленности.

Не станем утверждать, что большее разнообразие атакованных индустрий означает какой-либо серьезный сдвиг в поведении и мотивах атакующих. Скорее становится очевидным, что абсолютно любая организация может стать целью злоумышленников. Наша статистика говорит, что сегодня они нападают буквально на все, до чего могут “дотянуться”.

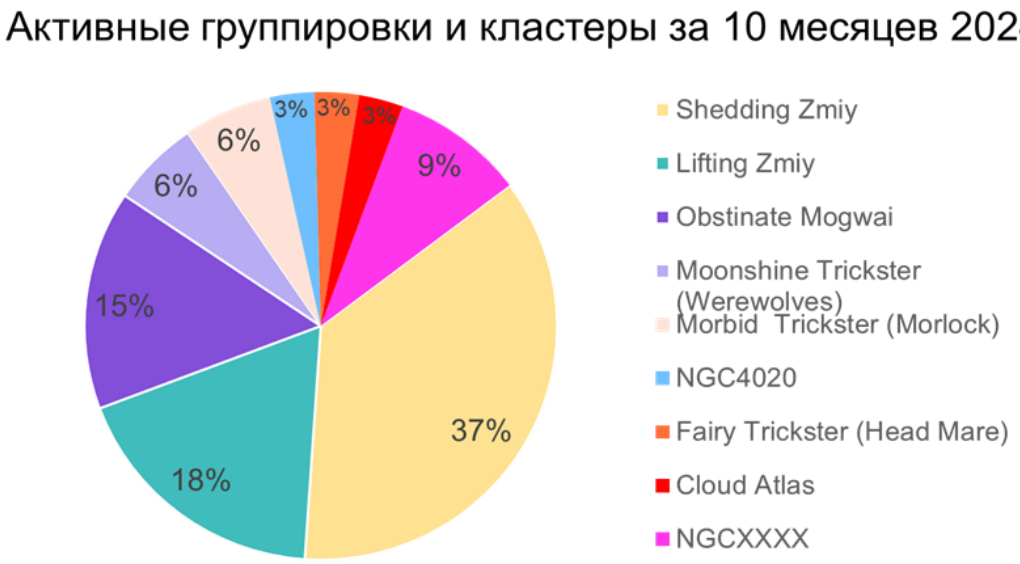
Обзор инцидентов: кто атакует и как атакует

Шпионаж остается главной целью атакующих: 54% расследованных с начала 2024 года инцидентов имели именно такую цель. На втором месте — кибератаки с целью финансовой выгоды (включая, вымогательство и майнинг криптовалют). Уничтожение данных - на третьем месте, но доля таких атак сократилась по сравнению с 2023 годом.

В 2023 году значительную долю заняли атаки с целью хулиганства и хактивизма, а в 2024 доля таких атак резко сократилась. Однако подавляющим большинством атак в этой категории в 2023 году было хулигнаство (то есть несложные и относительно безопасные атаки от любителей). В 2024 году в этой категории почти не осталось хулиганов, и почти все успешные атаки такого вида были политически мотивированы, осуществлялись подготовленными злоумышленниками и имели серьезные последствия (часто публикация конфиденциальных данных в открытом доступе).

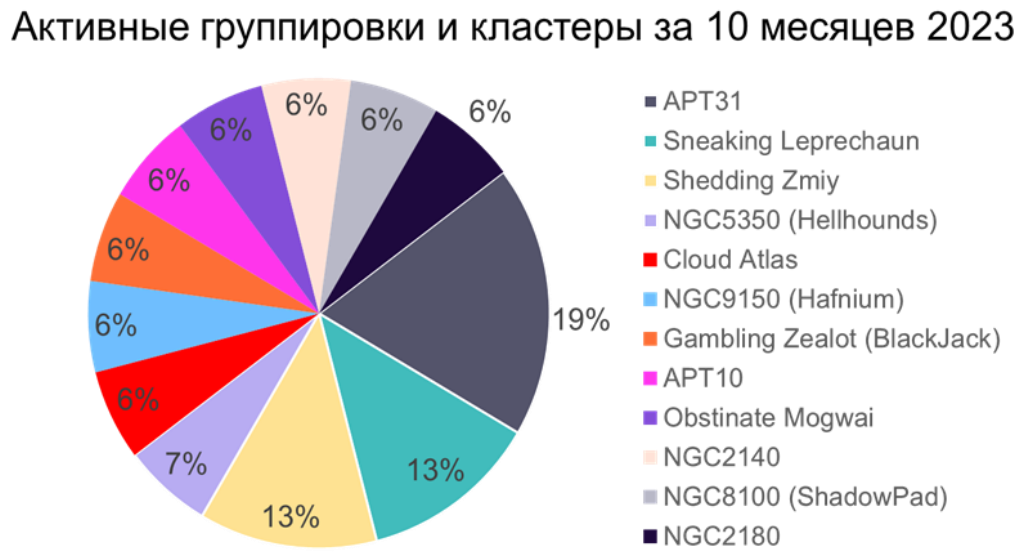
Активные группировки и кластеры

На статистику целей атакующих в отчетном периоде значительно повлияла активность проукраинских группировок, с которыми эксперты Solar 4RAYS имели дело чаще всего.



На группировки Shedding Zmiy и Lifting Zmiy, известные своей проукраинской направленностью, а также Fairy Trickster (Head Mare), Morbid Trickster (Morlock) и Moonshine Trickster (Werewolves) совместно пришлось около **70%** инцидентов.

В 2023 году ситуация была иной: перечень группировок имел более высокую степень диверсификации.



При этом нередко мы наблюдали не столько сами атаки, сколько артефакты, указывающие на то, что исследуемая инфраструктура была скомпрометирована в прошлом. Например, в случае с группировками азиатского происхождения: APT31, APT10 и NGC8100 (использовала ВПО ShadowPad).

Фокус на проукраинских группировках в 2024 году произошел еще и потому, что в отличие от других операторов сложных кибератак, проукраинские злоумышленники часто стремятся нанести максимальный ущерб атакованной инфраструктуре. Из-за этого факт их атаки вскрывается раньше и чаще, чем, например, действия группировок из Азии, которые заинтересованы в долгом скрытном присутствии и сборе конфиденциальной информации.

Другими словами, представленная выше статистика отнюдь не означает, что российские организации атакуют только перечисленные выше группировками, но мы с уверенностью можем сказать, что именно они в 2024 году представляли наибольшую опасность.

Основные наблюдаемые группировки

За 10 месяцев 2024 года мы столкнулись с деятельностью **9** кибергруппировок и кластеров активности. О некоторых из них мы уже рассказывали в отчете за первое полугодие 2024 года. За время, прошедшее с его публикации, мы наблюдали новые атаки Shedding Zmiy, Lifting Zmiy и Obstinate Mogwai (детальнее расскажем о них в отдельных публикациях в нашем блоге).

Мы также видим ряд атак, расследование которых продолжается (на графике выше это NGCXXXX). Пока мы не можем с точностью отнести их к какой-либо известной группировке или определить в них новый уникальный кластер вредоносной активности.

Из нового: в расследовании атаки на компанию из сферы транспорта мы обнаружили следы, характерные для группировки **Cloud Atlas**. Группировка известна с 2014 года, специализируется на шпионских операциях в организациях разной направленности по всему миру и, предположительно, является “наследницей” операции Red October, раскрытой “Лабораторией Касперского” в 2013 году. Данных, позволяющих надежно определить происхождение операторов Cloud Atlas, нет. В публикации о Red October “Лаборатория Касперского” приводила языковые артефакты, оставленные в коде ВПО разработчиками, указывающие на то, что они могут быть русскоговорящими. В ходе расследования мы тоже столкнулись с похожей уликой: в одном из обнаруженных скриптов английское слово domain было буквально транслитерировано с русского: domen_scan.ps1.

Также, по данным “Лаборатории Касперского”, Cloud Atlas чаще всего атакует цели на территории России. Получается, что русскоязычные атакующие нападают на российские организации с целью шпионажа. Такая совокупность признаков может указывать на то, что атакующие действуют в интересах одной из стран постсоветского пространства (Украины, например, ведь проукраинские группировки в последние годы регулярно атакуют российские инфраструктуры). Однако в атаках, описанных в 2019 году, среди целей обнаружились и украинские государственные организации, правда только на территориях Украины, где в то время происходил военный конфликт.

Мы сталкиваемся с Cloud Atlas значительно реже, чем с другими группировками и кластерами. В мае 2023 года мы наблюдали характерную для группировки фишинговую рассылку в адрес российской государственной организации. Тогда инцидент длился не более десяти дней. Расследуя атаку в сентябре этого года (на транспортную компанию), мы обнаружили свидетельства, указывающие, что Cloud Atlas находились в сети атакованной организации более двух лет.

Длительность инцидентов

Под длительностью инцидента мы понимаем отрезок времени между самым ранним обнаруженным артефактом компрометации и временем его обнаружения нашими специалистами.

Длительность	10 месяцев 2023 года	10 месяцев 2024 года
До недели	20%	30%
До двух недель	10%	12%
До месяца	16%	5%
До 6 месяцев	32%	20%
До 1 года	6%	12%
До 2-х лет	6%	12%
2+ года	10%	9%

В 2024 году появилось больше атак, продолжительность которых не превышала недели. Каждый третий исследованный нами инцидент именно такой. Годом ранее большая часть инцидентов длилась от 1 до 6 месяцев. Предполагаем, что изменения преимущественно связаны с тем, что организации стали быстрее реагировать на индикаторы возможной компрометации.

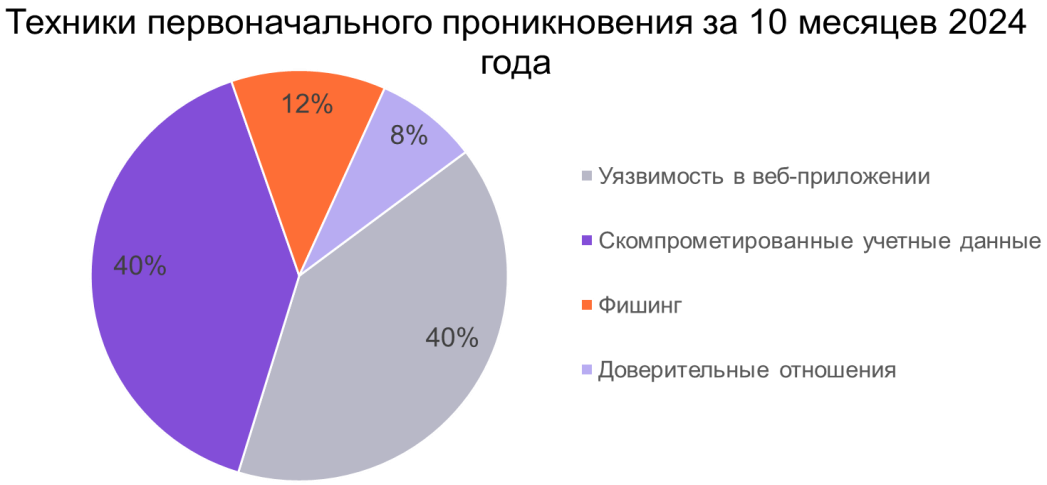
Однако о серьезном сдвиге в сторону ускорения реагирования на атаки пока говорить рано: в 2024 году доля инцидентов, в которых пребывание атакующих в инфраструктуре не превысило один месяц (это сумма результатов категорий “до недели”, “до двух недель” и “до месяца”) составила 46%. Годом ранее таких инцидентов мы зафиксировали немногим меньше – 45%.

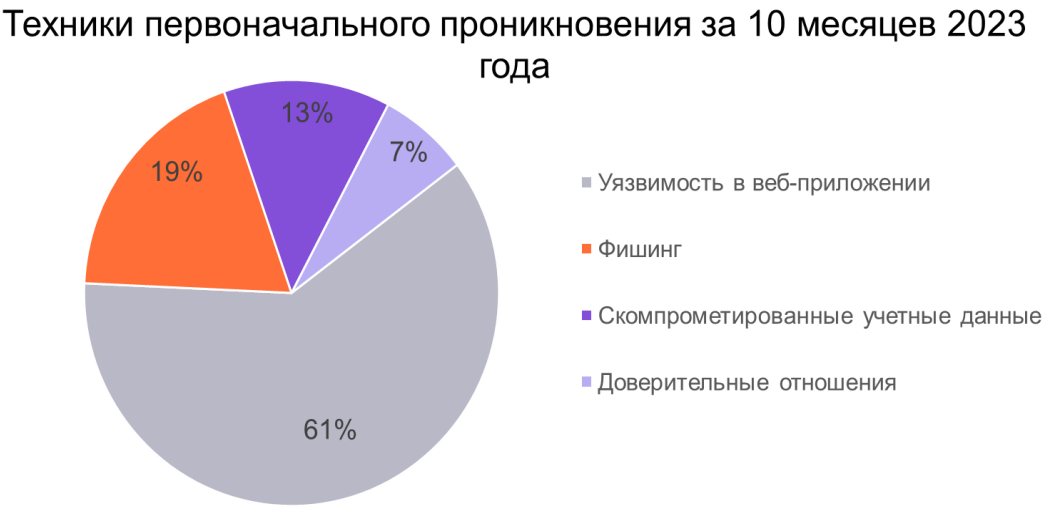
Также мы стали находить больше атак, длительностью до двух лет и более – в 2023 году на их долю пришлось 16%, а в 2024 – уже 21%. В этом году мы обнаружили несколько инцидентов, продолжительность которых составляла около 3,5 лет. Самые старые следы компрометации из обнаруженных нами в 2023 году имеют возраст около 2,5 лет.

Рост числа длительных инцидентов говорит не столько о каком-то особом профессионализме конкретных групп атакующих, сколько о росте компетенций компаний в области реагирования на существующие в открытом доступе индикаторы компрометации – они стали чаще использовать ИБ-продукты на базе киберразведки и, как результат, стали обнаруживать в своих сетях то, чего ранее не могли увидеть из-за недостатка сведений.

Распространенные методы проникновения

Уязвимости в веб-приложениях и скомпрометированные учетные данные – самые частые методы первоначального проникновения в инфраструктуры организаций.





В 2023 году уязвимости в веб-приложениях составляли абсолютное большинство (61%). А на втором месте был фишинг (19%). Сокращение доли веб-уязвимостей может быть связано с тем, что в 2022-2023 годах в сети было опубликовано множество различных баз учетных данных, украденных из российских организаций. Вероятно, что атакующие активно использовали скомпрометированные сведения для получения доступа к инфраструктурам и не испытывали острой нужды в развертывании фишинговых кампаний, направленных на похищение парольных и логинов.

На это косвенно указывает тот факт, что из всех инцидентов в 2024 году, где в качестве метода проникновения применялись скомпрометированные учетные данные,

применение грубой силы (брутфорса) мы нашли только в 20% случаев. То есть в большинстве атак у злоумышленников, скорее всего, уже были данные для входа, и их не нужно было подбирать.

Что же до уязвимостей в веб-приложениях, то излюбленными целями атакующих остаются серверы Exchange, программы для совместной работы, такие как Confluence, Битрикс24, CMS-системы, ПО для управления серверами и ПО для удалённого доступа.

Статистика говорит очевидное: службам безопасности организаций стоит пристально следить за парольной политикой (отслеживать данные об утечках и вовремя менять скомпрометированные данные). Кроме того, необходимо следить за выходом обновлений безопасности для систем, доступных из сети. В одном из инцидентов, которые нам довелось расследовать в мае этого года, для первоначального проникновения атакующие использовали критическую уязвимость в ПО для непрерывной интеграции и развертывания для DevOps. С момента публикации proof-of-concept для этой уязвимости в открытом доступе и до компрометации инфраструктуры атакованной организации прошло всего около четырех часов.

Основные выводы

Опираясь на результаты наших расследований, мы можем выделить следующие тенденции на российском ландшафте сложных киберугроз.

- **Атакуют всех.** Рост числа сфер экономики, на которые обращают внимание киберпреступники, свидетельствует о том, что у группировок (особенно проукраинских) нет фокуса на определённый тип организаций, как это было в прежние годы.

- **Уровень атакующих растет**. В 2024 году стало меньше хактивистских атак и больше атак, целью которых является кража данных (в некоторых случаях с целью последующей перепродажи или передачи иным заинтересованным лицам), а также атак с целью разрушения работоспособности инфраструктуры.

- **Уровень защищенности организаций пока оставляет желать лучшего.** Не смотря на вал атак на российские организации, начавшийся в 2022 году, далеко не все целевые атаки, которые мы наблюдали, можно назвать сложными. Зачастую не нужно быть профессиональным взломщиком, чтобы проникнуть в инфраструктуру организации. В одном из инцидентов для проникновения в организацию использовались учетные данные, которые были скомпрометированы несколько лет назад. Уровень атакующих растет быстрее, чем уровень защищенности атакуемых организаций. О значительном повышении безопасности инфраструктуры в подавляющем большинстве случаев задумываются только компании, столкнувшиеся с серьезными инцидентами, нанёсшими значительный ущерб или получившими публичную огласку.

- **Многочисленные утечки корпоративных данных создали “плацдарм” для атакующих.** Использование скомпрометированных учетных записей в 2024 году стало одним из самых распространенных методов проникновения в организации. Предположительно, злоумышленники используют утекшие учетные записи, которые не обновили вовремя или о которых до сих пор неизвестно, что они были скомпрометированы.

- **Время между публикацией Proof-of-concept и началом “боевой” эксплуатации уязвимостей сокращается**. Некоторые группировки стараются максимально оперативно эксплуатировать свежие уязвимости. Атакующим нужно всего несколько часов, чтобы взять Proof-of-concept и использовать его в реальных атаках пользуясь, задержкой между выходом патчей и их массовой установкой в инфраструктурах.

- **Linux атакуют всё чаще**. В 2023 году мы обнаружили первую в нашей практике сложную целевую атаку, направленную преимущественно на Linux-инфраструктуры. В нашей таксономии эта операция получила название NGC2140. В ней использовался чрезвычайно скрытный вредонос GoblinRAT, о котором мы рассказываем в отдельном исследовании. В 2024 года мы стали чаще встречать инструменты, направленные на Unix-системы (преимущественно Linux). Их активно применяет, например, группировка Shedding Zmiy. Рост попыток атак на такие системы подтверждает и статистика центра противодействия кибератакам Solar JSOC. Это все противоречит многолетнему убеждению, что на Unix-системах вредоносного ПО нет. Более того, некоторые группировки атакующих специализируются именно на атаках данного семейства операционных систем и сознательно не хотят в своих атаках обширно затрагивать другую инфраструктуру.

- **Прицел на виртуализацию.** Одной из характерных черт при попытках уничтожения инфраструктуры является повреждение или уничтожение серверов виртуализации. Многие важные части инфраструктуры сегодня размещают на виртуальных серверах, и их повреждение обычно приводит к выводу из строя критически важных систем, остановке важных бизнес-процессов. Атаки на такие системы – не новая тактика. Она встречалась и ранее, но в этом году наиболее ярко проявилась в наших расследованиях, в том числе потому, что существует несколько эффективных способов вывести из строя виртуальную инфраструктуру, и любой из них нанесет такой же ущерб, как гораздо более сложная и продолжительная атака на физические серверы. Кроме того, атаки шифровальщиков-вымогателей в этом году тоже нередко направлялись на виртуальную инфраструктуру. Одной из предпосылок этой тенденции может быть публикация исходного кода шифровальщика Babuk для Linux и ESXi, случившаяся в 2023 году. В 2024 году группировки освоили появившийся в свободном доступе вредоносный инструмент.

- **Вымогатели-шифровальщики представляют серьезную угрозу.** За громкими новостями о политически мотивированных атаках шифровальщики будто бы ушли в тень, но в 2024 году мы периодически сталкивались с такими шифровальщиками, как Blackshadow, Enmity, Lockbit.

- **Проукраинские группировки атакующих остаются главной угрозой для российских ИТ-инфраструктур.** Хотя в течение года мы наблюдали атаки группировок, имеющих иное происхождение (например, восточноазиатская группа Obstinate Mogwai), атаки проукраинских групп превалируют и обычно имеют более разрушительный эффект. Характерный modus operandi этих атакующих: получить максимально глубокий доступ к инфраструктуре, собрать все конфиденциальные данные и, когда атакованная инфраструктура перестает представлять ценность или возникает угроза обнаружения, уничтожить ее.

Прогнозы развития ландшафта сложных киберугроз в 2025 году

Инциденты, которые мы наблюдали в течение года, позволяют сделать некоторые предположения о том, каким может быть грядущий год:

- **Количество инцидентов сохранится или вырастет, а разнообразие атакуемых отраслей сохранится.** Количество атак и атакованных организаций в последние годы (особенно после начала СВО) только увеличивалось. Комментируя свои действия в социальных сетях, представители проукраинских группировок нередко указывают на связь кибератак с военными действиями на Украине. Вероятно, рост числа инцидентов продолжатся, пока будут продолжаться военные действия. Также сохранится разнообразие целевых инфраструктур, поскольку атакующие очевидно не выбирают конкретные цели, а вместо этого используют все доступные возможности.

- **В атаках будет применяться больше кастомных вредоносных инструментов.** Все чаще атакующие используют либо полностью кастомные, либо существенно доработанные публично доступные вредоносные инструменты. Мы считаем, что этот тренд сохранится. Злоумышленники активно модернизируют свой арсенал, добавляют новую функциональность в инструменты, уделяя все большее внимание скрытности и техникам обхода защитных решений. Например, после серии публикаций об атаках Shedding Zmiy группировка существенно обновила свой арсенал, отказавшись от применения инструментария, о котором в первой половине года рассказывали и Solar 4RAYS, и коллеги по индустрии.

- **Атакующие сфокусируются на более масштабных целях**. После всплеска массовых хактивистских атак в 2022 году (дефейс сайта, например, или политически мотивированные DDoS-атаки), последний год их число падает. А более изощренных операций стало больше. Уровень злоумышленников, вовлеченных в атаки на российские инфраструктуры, вырос, и в 2025 году мы ожидаем, что станет больше инцидентов, направленных на кражу конфиденциальных корпоративных данных, перехват ключевых сервисов, уничтожение ключевой инфраструктуры, взлом подрядчиков для доступа к целевым сетям и т.д.

- **Linux останется в фокусе атакующих.** В российских организациях растет количество Linux-систем и, соответственно, будет расти количество атак на них. Также связываем этот тренд с традиционно более низким уровнем знаний Linux-систем по сравнению с Windows у многих специалистов, администрирующих такие системы внутри атакуемых организаций. Защитные решения для NIXов также, как правило, уступают по уровню погруженной в них экспертизы своим аналогам для Windows.

Заключение и рекомендации

События, происходящие на российском ландшафте сложных киберугроз в последние годы, можно образно охарактеризовать, как большое и продолжительное тестирование на проникновение всей российской ИТ-инфраструктуры. Пока что, судя по статистике инцидентов, “красная” команда ведет с большим отрывом, но для организаций эта ситуация может стать поводом для кардинальных перемен в подходе к обеспечению информационной безопасности своих инфраструктур.

Из нашего анализа мы делаем вывод, что даже базовые меры безопасности при грамотном подходе, если не исключат вероятность успешной кибератаки полностью, то серьёзно её снизят.

Мы рекомендуем:

- Строго контролировать удаленный доступ в инфраструктуру, особенно для подрядчиков.
- Предельно ответственно относиться к соблюдению парольных политик, пользоваться сервисами мониторинга утечек учетных записей и вовремя их обновлять.
- Серьезно относиться к уведомлениям о возможной компрометации от Национального координационного центра по компьютерным инцидентам (НКЦКИ) и частных компаний, обладающих экспертизой в области ИБ.
- Создавать инфраструктуру бэкапов, 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.
- Использовать продвинутые средства защиты (EDR, SIEM) наряду с классическим защитным ПО, чтобы иметь возможность отслеживать события в инфраструктуре и вовремя обнаруживать нежелательные.
- Оперативно обновлять все используемое в инфраструктуре ПО.
- Заниматься повышением киберграмотности сотрудников – ведь успешная атака на основе социальной инженерии возможна даже в самой защищённой инфраструктуре.
- Следить за тем, чтобы служба ИБ имела постоянный доступ к последним сведениям о ландшафте киберугроз конкретного региона и индикаторам компрометации.
- В случае подозрений на атаку, не медлить с проведением оценки компрометации инфраструктуры. Своевременный Compromise Assessment и реагирование позволят остановить до наступления последствий.

Привлеките команду расследования и реагирования Solar 4RAYS, чтобы проверить гипотезу о присутствии злоумышленника в инфраструктуре.