|  |  |
| --- | --- |
| **Пресс-релиз**19 февраля 2025 года | **Пресс-центр** Елена Шамратова+7 912 612 39 08 elena.shamratova@rt.ru |

**Хакерская киберразведка, уязвимости и вредоносы – как киберпреступники атаковали банки в 2024 году**

Количество кибератак на финансовый сектор за год выросло на треть и достигло 9 тыс. подтвержденных инцидентов. Наибольшую угрозу для отрасли представляют попытки сканирования внутренней сети в целях киберразведки, эксплуатация уязвимостей и заражение вредоносным ПО. К такому выводу пришли эксперты центра противодействия кибератакам [Solar JSOC](https://rt-solar.ru/services/jsoc/) ГК «Солар», проанализировав данные сервиса мониторинга за 2024 год.

С сетевыми атаками было cвязано 27% подтвержденных инцидентов, при том, что год назад их доля составляла 14%. Большинство подобных инцидентов касалось несанкционированного внутреннего сетевого сканирования, то есть изучения злоумышленниками внутренней сети жертвы: веб-приложений, систем и устройств. Факты сетевых атак говорят о том, что хакеры уже преодолели внешний периметр организации и пытаются развить атаку внутри, предварительно проведя киберразведку.

Доля эксплуатации уязвимостей, напротив, сократилась: с 36% до 27%. Уязвимости используются хакерами на всех этапах развития атаки: при попытках взлома, при горизонтальном продвижении по сети и повышении привилегий на хосте, при попытках компрометации систем банка внутри инфраструктуры. И налаженный процесс управления уязвимостями остается основой построения безопасной инфраструктуры.

Заражение вредоносным ПО замыкает топ инцидентов: доля за год выросла с 8% до 14%. Несмотря на то, что финансовый сектор более устойчив к подобным угрозам, чем другие отрасли, вирусы все равно могут нанести серьезный ущерб организациям.

По данным с сети сенсоров и ханипотов центра исследования киберугроз [Solar 4RAYS](https://rt-solar.ru/solar-4rays/blog/4856/), среди всех компаний, у которых есть признаки заражения ВПО, банки занимают всего 4%. Наибольшую угрозу для отрасли представляют инструменты удаленного доступа – Remote Administration Tools (RAT). На них приходится 37% всех заражений. В зависимости от функциональности такие вредоносы позволяют хакерам дистанционно управлять атакованной системой (менять и выгружать данные, делать скриншоты, менять настройки оборудования и т.п.).

Еще 19% инцидентов связано с атакой вирусов-стиллеров. Это ВПО, которое в автоматизированном режиме собирает информацию с зараженной инфраструктуры. А 15 % - с активностью APT-группировок. Как правило, это факты обращения к серверам управления (С2) из зараженной инфраструктуры. Как видно, наибольшую угрозу для отрасли представляют вирусы и вредоносы, которые нацелены на получение доступа к системам, содержащим конфиденциальную информацию, и ее хищение.

«В финсекторе уровень защиты от базовых угроз выше, чем в других отраслях. Поэтому инциденты с применением ВПО здесь находятся на 3 месте, в то время как в остальных отраслях это топ-1 среди угроз. Однако банки интересны злоумышленникам с высокой квалификацией, которые реализуют сложные целевые атаки. Рост внутренних сканирований как раз говорит о том, что хакеры тщательно готовятся к таким киберударам, стараются изучить инфраструктуру жертвы, чтобы спланировать свои дальнейшие шаги. Именно поэтому вовремя выявленная сетевая атака поможет не допустить фатальных последствий для компании, – отметил **директор центра противодействия кибератак Solar JSOC Владимир Дрюков.** – А полноценный мониторинг инфраструктуры с использованием специальных сенсоров (NTA, EDR и проч.), регулярное обучение сотрудников киберграмотности, выстроенный процесс патч-менеджмента в совокупности помогут снизить киберриски для отрасли».

Существенно снизить риски сетевых атак позволяет правильно организованная сегментация сети за счет настройки политик безопасности, а также правил доступа к внешним ресурсам и использованию приложений. Организовать комплексную защиту корпоративных сетей и хранящихся в них данных от сетевых угроз помогают решения для сетевой безопасности, в частности NGFW (Next Generation Firewall) и SWG (Secure Web Gateway). Так, [Solar NGFW](https://rt-solar.ru/products/solar_ngfw/) обеспечивает многоуровневую защиту на сетевом периметре и между внутренними сегментами сети организации, а [Solar webProxy](https://rt-solar.ru/products/solar_webproxy/) ограничивает доступ пользователя к недоверенным ресурсам и имеет на борту интегрированный антивирус для защиты от ВПО. В свою очередь решения по управлению доступом позволяют снизить риск того, что хакеры смогут воспользоваться скомпрометированными учетными данными сотрудников и подрядчиков, имеющих доступ к IT-инфраструктуре компании.

**О компании**

[Группа компаний «Солар»](https://rt-solar.ru/) — архитектор комплексной кибербезопасности. Ключевые направления деятельности — аутсорсинг ИБ, разработка собственных продуктов, интеграция комплексных решений, обучение ИБ-специалистов, аналитика и исследование киберинцидентов.

С 2015 года предоставляет ИБ-решения организациям от малого бизнеса до крупнейших предприятий ключевых отраслей. Под защитой «Солара» — более 1000 крупнейших компаний России. Компания работает в направлениях безопасной разработки программного обеспечения, управления доступом, защиты корпоративных данных, детектирования хакерских атак и угроз, что позволяет закрывать максимум потребностей заказчиков.

Группа компаний предлагает сервисы первого и крупнейшего в России коммерческого SOC — Solar JSOC, экосистему управляемых сервисов ИБ — Solar MSS. По данным независимых аналитиков, «Солар» входит в топ-5 европейских и топ-15 мировых сервис-провайдеров по объему бизнеса.

Работа Центра исследования киберугроз Solar 4RAYS нацелена на изучение тактик киберпреступников. Полученные аналитические данные обогащают разработки Центра технологий кибербезопасности.

Линейка собственных продуктов включает DLP-решение Solar Dozor, шлюз веб-безопасности Solar webProxy, межсетевой экран нового поколения Solar NGFW, IdM-систему Solar inRights, PAM-систему Solar SafeInspect, анализатор кода Solar appScreener и другие. Также ГК «Солар» развивает платформу для практической отработки навыков защиты от киберугроз «Солар Кибермир».

Группа компаний «Солар» инвестирует в развитие отрасли кибербезопасности и помогает решать проблему кадрового дефицита. Для поддержки молодых технологичных проектов и насыщения рынка технологиями созданы венчурный фонд Solar Ventures и программа CyberStage. Совместно с Минцифры России в рамках национального проекта «Цифровая экономика Российской Федерации» реализует всероссийскую программу кибергигиены, направленную на повышение цифровой грамотности населения.

Под защитой «Солара» находятся крупнейшие государственные информационные системы, а также экономические и общественно-политические события в России, в том числе международного уровня.

Штат компании — более 2 000 специалистов. Подразделения «Солара» расположены в Москве, Санкт-Петербурге, Нижнем Новгороде, Самаре, Ростове-на-Дону, Томске, Хабаровске и Ижевске. Технологии компании и наличие распределенных по всей стране центров компетенций позволяют ей работать в режиме 24/7.