JET SECURITY TEAM

ИТОГИ ГОДА

2023

Оглавление

2023 год: краткие итоги

- Ландшафт угроз и общее количество атак в 2023 году от 2022-го отличаются незначительно: центр мониторинга и реагирования на инциденты Jet CSIRT **в 2023 году зафиксировал рост общего числа атак на 11%** по сравнению с предыдущим годом.

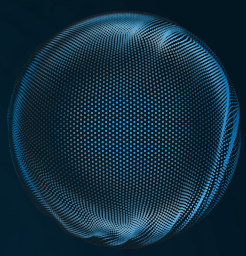
- **Наибольшее число наблюдаемых инцидентов связано с заражением вредоносным ПО:** как через посещение сайтов с вредоносным контентом, так и через фишинговые атаки.

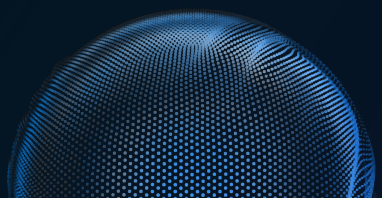
- Проблема проникновения злоумышленников через подрядные организации становится особенно острой в 2023 году. **По данным экспертов, причиной каждого пятого значимого инцидента, по которому проводилось расследование, стал взлом ИТ-подрядчика.**

- **Более 90% анализируемых компаний сталкивались с утечками** корпоративных учетных записей. В **48%** случаев учетная запись упоминается в связке с паролем и в **44%** — в связке с хэшем, что может помочь атакующим скомпрометировать учетную запись.

- **93% компаний**, которым «Инфосистемы Джет» оказывала услугу мониторинга внешних угроз, были предметом обсуждения **на darknet-форумах и в telegram-каналах хакерской тематики.**

- На проектах по мониторингу внешних цифровых рисков **у 72% компаний были найдены критические уязвимости на периметре**, для которых существуют публичные эксплойты. Подобные уязвимости могут послужить точкой входа злоумышленника в инфраструктуру компании.





Аннотация

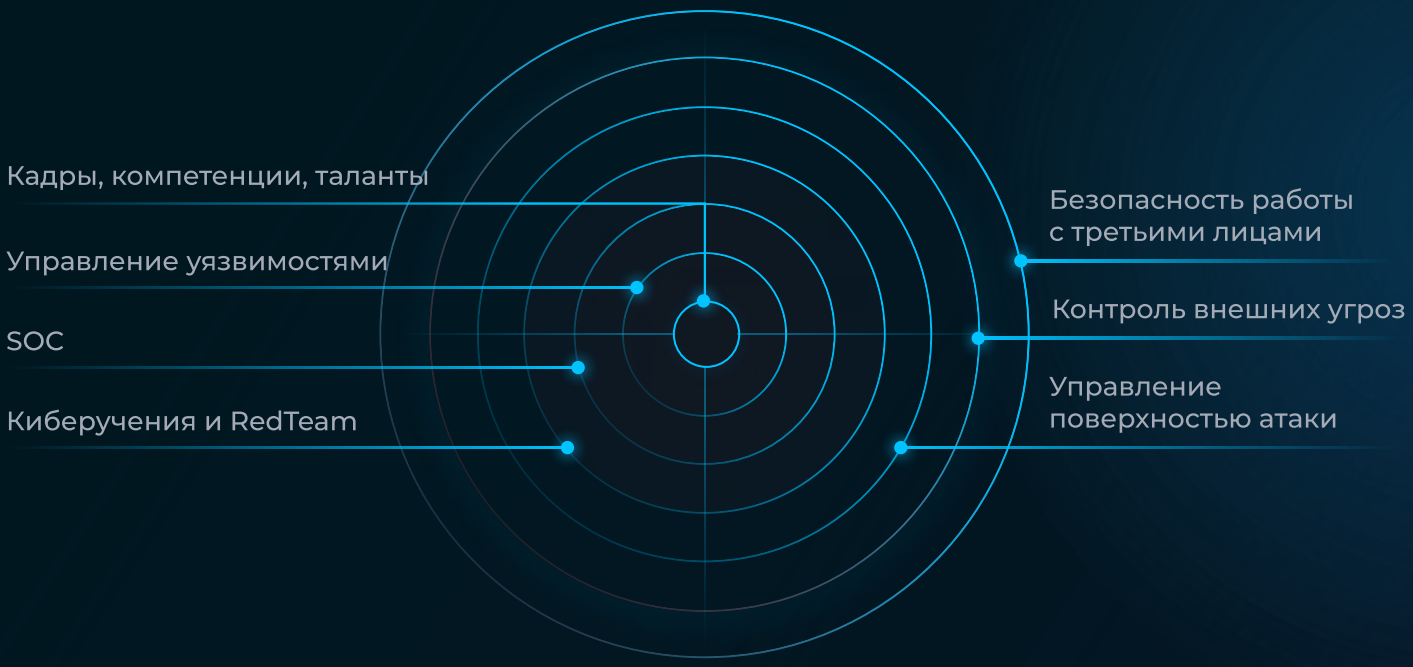
В 2022 году индустрия кибербезопасности столкнулась с необходимостью переосмысления своих стратегий и приоритетов. На волне обострения геополитической ситуации, массовых и зачастую простых атак, имеющих политическую мотивацию, компании во многом выстраивали свою защищенность по принципу «закрыть все границы». Оказавшись не готовыми к новым вызовам, компании ожидаемо ограничивали область контроля периметром своей инфраструктуры. Прошедший 2023 год подсветил растущую необходимость для компаний активно анализировать и контролировать информацию за пределами внутренних сетей, обеспечивать системный контроль защищенности постоянно модернизируемой ИТ-инфраструктуры. Утечки данных и информационные угрозы могут исходить из самых разных источников, включая доверенных партнеров, поэтому критически важно иметь возможность быстро закрывать уязвимости, обнаруживать и реагировать на события, компрометирующие компанию.

Начиная с первого квартала 2023 года мы наблюдали системное усложнение характера и методов проведения кибератак: применение сложнодетектируемых вредоносов, использование инструментов автоматизации и подготовку атак на базе искусственного интеллекта, многосоставные цепочки взлома через доверенных партнеров. Доля задействованных в прошлогодних атаках низкоквалифицированных хакеров, хактивистов и script kiddie значительно сократилась, вместе с этим заставляя индустрию системно повышать зрелость своих процессов и наращивать компетенции специалистов.

В аналитическом отчете мы рассматриваем ключевые тренды кибербезопасности 2023 года, подчеркивая значимый сдвиг фокуса в сторону раннего обнаружения и ответа на угрозы.

Концепция отчета

Основой для отчета послужила концепция 7 Security Rings, обеспечивающая поддержание киберустойчивости компании. Модель предлагает многоуровневый подход к контролю защищенности организации, начиная с внутреннего мониторинга и заканчивая внешними угрозами и глобальным киберпространством.



Мы рассмотрели глобальные тренды прошедшего года в контексте данной модели, опираясь на результаты работы экспертных команд Jet Security Team за 2023 год, в частности:

- данные и кейсы, полученные в ходе реализации проектов по аудиту информационной безопасности, тестированию на проникновение;
- результаты мониторинга и реагирования на инциденты в рамках оказания сервисов SOC со стороны команды мониторинга и реагирования на инциденты Jet CSIRT;
- информацию по результатам расследования компьютерных инцидентов со стороны экспертов по форензике Jet CSIRT;
- аналитику, полученную по результатам работы группы мониторинга внешних цифровых рисков;
- исследования техник, тактик и процедур (TTPs) киберпреступных группировок за 2023 год;
- а также результаты опросов ключевых заказчиков АО «Инфосистемы Джет» и внешних опросов профильной аудитории (в опросах приняли участие более 100 организаций: представители крупного бизнеса, малые и средние предприятия и организации государственного сектора).

1. Ключевые проблемы глазами индустрии

Мы попросили наших ключевых заказчиков, а также участников Jet CyberCamp 2023 поделиться проблемами, с которыми они сталкивались в 2023 году чаще всего. В опросе приняли участие более 1000 специалистов ИБ из разных отраслей.

По результатам опроса ТОП-5 проблемами стали:

1. Кадровый голод и управление талантами (нехватка кадров, сложность найма и удержания специалистов, отсутствие релевантного опыта).
2. Сложность модернизации ИБ-архитектуры с учетом перехода ИТ на оборудование и ПО от российских производителей (нет необходимых альтернатив).
3. Проблемы с выделением бюджета и защитой инициатив.
4. Проблема поддержания работоспособности текущих зарубежных решений (сложность обновления и поддержки зарубежных СЗИ).
5. Сложности в выстраивании и управлении процессами ИБ.

2. Что мы наблюдали в 2023 году

2.1 Увеличение числа атак через подрядчиков

Активно развивая взаимоотношения с поставщиками, привлекая внешнюю экспертизу и используя сервисы, бизнес в большинстве случаев оставлял без внимания риски таких взаимодействий, что привело к многочисленным случаям взломов через подрядчиков. По данным команды форензики Jet CSIRT, причиной каждого пятого инцидента стал взлом ИТ-подрядчика.

Несмотря на изменение парадигмы построения архитектуры безопасности в сторону моделей нулевого доверия («никогда не доверяй, всегда проверяй»), в отношении поставщиков доминировала модель «один раз проверяй — всегда доверяй».

С инцидентами эксплуатации доверия в 2023 году столкнулись многие крупные компании, доля таких атак в общем числе киберинцидентов выросла более чем на **20%**:

- **80%** компаний используют защитные меры в отношении подрядчиков/поставщиков услуг, аналогичные удаленным работникам;
- **лишь 20%** определяют набор мер, исходя из специфики взаимодействия и профиля риска поставщика.

Александр Морковчин
Руководитель отдела развития консалтинга ИБ, «Инфосистемы Джет»

Понимая необходимость проверки и контроля уровня ИБ ключевых поставщиков, крупный бизнес начал формировать спрос на проверку их безопасности с использованием сервисов мониторинга внешних цифровых угроз (киберразведка). Также, по нашим данным, в 3,2 раза за последние годы вырос спрос на решения для управления привилегированным доступом (PIM/PAM).

Кейс

Успешный взлом финансовых организаций через ненадежного подрядчика

Микрофинансовая компания пользовалась услугами подрядчика для разработки собственного ПО. Подрядчику была выдана учетная запись с правами администратора на хосте, на котором устанавливается ПО.

Критичная уязвимость на периметре компании-подрядчика позволила злоумышленникам получить доступ во внутреннюю базу знаний, где хранились логины и пароли для доступов в инфраструктуру заказчиков. Так злоумышленники попали в инфраструктуру целевой компании, повысили привилегии, скомпрометировали домен и запустили шифровальщика с последующим требованием выкупа. Как выяснилось позднее, компрометация этого подрядчика была стартовой точкой для развития целого ряда атак на другие предприятия.

Действительно, мало кто застрахован от взлома поставщика услуг, однако регулярный мониторинг безопасности ключевых подрядчиков, а также оценка их благонадежности способны значительно сократить риск подобных инцидентов. А внедрение двухфакторной аутентификации для третьих лиц, имеющих доступ в инфраструктуру, позволит значительно повысить уровень защиты от хакеров, которые действуют из-под учетки контрагента.

2.2 Развитие сервисов мониторинга внешних цифровых угроз для контроля за чувствительными данными

Массовые утечки почти 300 млн пользовательских данных в 2022 году, затронувшие крупнейших игроков на рынке (Яндекс.Еда, СДЭК, Гемотест и пр.), активно использовались злоумышленниками в 2023 году для проведения атак. Мы системно находим «слитые» учетные записи, относящиеся к инфраструктуре, которые активно используются атакующими.

Чувствительные данные обнаруживаются в **98,5%** случаев поиска по целевой компании, где:

- **48%** учетных записей содержат связку логин-пароль;
- **44%** учетных записей упоминаются в связке с хэшем пароля.

Сотрудники чаще всего оставляют корпоративные почтовые адреса в сервисах медицинских клиник, а также в интернет-магазинах.

По данным сервиса защиты от внешних цифровых угроз Jet Nautilus, **9 из 10** анализируемых компаний уже упоминаются на darknet-форумах и в telegram-каналах хакерской или мошеннической тематики. Это могут быть сообщения о поиске инсайдера, продажа уже имеющихся доступов в инфраструктуру или обсуждение организации с точки зрения механизмов ее защиты и их обхода.

Александр Ненахов
Руководитель группы мониторинга внешних цифровых рисков, «Инфосистемы Джет»

Использование слитых учетных данных — дело времени, поэтому сервисы мониторинга внешних цифровых угроз как способ защиты от целевых атак становятся всё более востребованным направлением деятельности в сфере ИБ: рынок платформ и сервисов увеличился в два раза за последние два года и продолжает расти.

Кейс

Как слитые корпоративные адреса позволили хакерам заработать миллионы

Злоумышленники создали фишинговую страницу, имитирующую корпоративный портал логистической компании. Хакеры собрали в интернете слитые почтовые адреса сотрудников и направили им рассылку с просьбой изменить пароль от учетной записи. Многие сотрудники переходили на фишинговую страницу и вводили свои логины и пароли. Хакеры, используя эти данные, попали во внутреннюю почту, изучили переписку и нашли бухгалтера, который готовит платежные поручения. В определенный день платежные документы были подделаны и деньги были перечислены на счет атакующих. **Ущерб оценивается в сотни миллионов рублей.**

2.3 Управление поверхностью атак

Массовый дефейс и атаки на публичные веб-ресурсы в начале 2023 года подчеркнули важность комплексного анализа и управления потенциальными точками входа (периметр сети, открытые репозитории кода, внешние сервисы), которые могут быть использованы злоумышленниками для взлома или компрометации.

По данным сервиса защиты от внешних цифровых угроз Jet Nautilus, при оценке потенциальных векторов атак посредством сканирования обнаруживается, что:

- у **99%** компаний есть публично доступные административные панели авторизации;
- у **41%** компаний код в публичных репозиториях содержит учетные записи в открытом виде;
- **96%** компаний используют на внешнем периметре версии ПО, имеющие уязвимости уровня «Critical» и «High», для которых существуют публично доступные эксплойты.

Руслан Амиров
Руководитель экспертных сервисов мониторинга и реагирования Jet CSIRT, «Инфосистемы Джет»

Все эти факторы значительно упрощают проведение атак злоумышленниками, сокращая время от разведки до проникновения в инфраструктуру жертвы с последующей кражей и шифрованием корпоративных данных.

Так, в рамках проведения работ по тестированию на проникновение за 2023 год в **20%** проектах были выявлены уязвимости веб-приложений, которые позволяют выполнить произвольные команды операционной системы и предоставляют возможность развития атаки вглубь корпоративной сети.

В 2023 году на **30%** чаще к нам стали обращаться с запросом на проведение внешнего тестирования на проникновение.

Кейс

Криптоферма на базе торговой компании

В компании сферы розничной торговли ИТ-служба заметила нетипичную нагрузку: потребление ресурсов стало расти при прежнем объеме рабочих процессов, что стало причиной отказа работы некоторых бизнес-систем. В ходе расследования был выявлен майнер, который тщательно маскировался под различное легитимное ПО (adobeupdate, yandexupdate, officeupdate и др.) и даже изменял свои временные метки, тем самым «представляясь старичком» на зараженной системе. При тщательном анализе ВПО выяснилось, что заражена почти вся ИТ-инфраструктура (несколько тысяч узлов), а точкой входа являлся уязвимый почтовый сервер на периметре. По предварительным оценкам, доход такой фермы мог достигать 1000 $ в день. Регулярный мониторинг поверхности атаки позволил бы выявить уязвимый хост на периметре до того, как его заметили и использовали злоумышленники.

Промышленная компания подверглась серьезной атаке по нелепой ошибке

Злоумышленники обнаружили рабочую станцию, принадлежащую промышленной компании, которая была по ошибке опубликована в интернет по протоколу RDP. Им удалось подобрать пароль администратора хоста методом грубой силы (брутфорс), а затем на том же хосте был скомпрометирован и администратор домена с использованием техники — Dump LSASS (Local Security Authority Subsystem Service). Повысив привилегии до уровня домен-админа, хакеры зашифровали всю инфраструктуру и потребовали внушительный выкуп.

2.4 Киберучения

Неквалифицированные команды работают неэффективно, и значительный рост кибератак в 2022 году подсветил отсутствие опыта противодействия сложным многоступенчатым атакам. Фокус на практическом аспекте обучения стал ключевой стратегией укрепления кибербезопасности многих компаний в 2023 году.

Тренироваться отражать кибератаки без риска ущерба для инфраструктуры позволяют киберполигоны и сервисы киберучений — мы отмечаем **двукратный рост запросов** на такие экспертные сервисы, при этом не только для технических специалистов, но и для топ-менеджмента.

Наибольший спрос на сервисы киберучений в 2023 году мы наблюдали в следующих отраслях:

- промышленность
- финансовая сфера
- телеком

Дмитрий Казмирчук
Руководитель группы сервиса киберучений, «Инфосистемы Джет»

Помимо традиционных сценариев обучения, в 2023 году сформировалась стабильная потребность в оценке отдельных навыков работников. Особенный интерес мы фиксируем в следующих группах навыков: форензика, проактивный поиск угроз и безопасная разработка. В качестве механизма оценки могут использоваться как классические практические задания, так и корпоративные CTF-турниры.

2.5 Мониторинг и расследование инцидентов ИБ

В 2023 году центр мониторинга и реагирования на инциденты Jet CSIRT, как и годом ранее, зафиксировал более 10 тысяч инцидентов ИБ (именно подтвержденная нелегитимная активность, за исключением ложноположительных срабатываний). Рост общего числа инцидентов незначительный — **11%**, тогда как в 2022 году фиксировалось трехкратное увеличение числа инцидентов.

Ниже представлен список из ТОП-10 наиболее распространенных техник и тактик согласно матрице MITRE ATT&CK, которые чаще всего обрабатывал Jet CSIRT в 2023 году.

Mitre_ID	Mitre_Name	Топ-10 техник 2023 (%)
T1204	User Execution	34,63%
T1562.001	Impair Defenses, Disable or Modify Tools	27,60%
T1190	Exploit Public-Facing Application	17,33%
T1110.001	Brute Force, Password Guessing	8,21%
T1133	External Remote Services	4,82%
T1110.003	Password Spraying	1,37%
T1071.004	Application Layer Protocol, DNS	1,14%
T1090.003	Proxy: Multi-hop Proxy	0,91%
T1021	Remote Services	0,76%
T1219	Remote Access Software	0,37%

T1204 — User Execution

Инциденты, связанные с заражением узлов вредоносными программами (в том числе массовыми), а также обнаружением индикаторов компрометации в защищаемом периметре. Большинство таких инцидентов связано с посещением пользователями вредоносных сайтов, установкой сомнительных браузерных расширений, переходом по недоверенным ссылкам, а также с проведением фишинговых атак, в том числе Spear Phishing[1]. В частности, именно в результате одного из кейсов целенаправленного фишинга нашими аналитиками был обнаружен вредонос DarkGate, подробный разбор которого был опубликован на Хабре.

T1562.001 — Impair Defenses, Disable or Modify Tools

Второй по распространенности тип инцидентов связан с модификацией и отключением средств защиты (чаще всего — средств АВЗ). Сюда относятся случаи отключения антивирусных агентов, агентов EDR, DLP и прочих СЗИ. Основная масса инцидентов связана с переходом антивирусных агентов в «критический» статус, который в основном связан с устареванием антивирусных баз или невозможностью агента соединиться с сервером управления. Однако встречались случаи преднамеренного отключения как устанавливаемых средств защиты, так и встроенных. Например, в рамках расследования шифровальщика LockBit 3.0 мы обнаружили, что он полностью отключает Windows Defender и меняет правила встроенного межсетевого экрана на Windows-узлах.

T1190 — Exploit Public-Facing Application

Инциденты связаны с эксплуатацией публично доступных веб-приложений. В статистику попали как успешные попытки атак, так и неуспешные/заблокированные или же несработавшие попытки использования эксплойтов. Если говорить про успешные случаи эксплуатации уязвимостей, то в 2023 году «фаворитами» в качестве целей злоумышленников являлись приложения на базе продуктов 1С-Битрикс. В частности, наиболее распространенной уязвимостью для атак на 1С-Битрикс является уязвимость в модулях vote/uf.php и html_editor_action.php, которые позволяют загрузить на уязвимый сервер произвольный код и которые стали причиной массового дефейса сайтов в прошлом году.

[1] Spear Phishing (целевой фишинг) — подготовленная атака, направленная на то, чтобы обмануть конкретного человека или сотрудников конкретной компании.

T1110.001 — Brute Force, Password Guessing

Инциденты, связанные с методами брутфорса и угадывания паролей. Сюда входят нетипичные аутентификации, внутренние и внешние попытки подбора паролей, нетипичные действия с учетными данными и нетипичный удаленный доступ.

В основном данный тип инцидентов связан с попытками внешнего брутфорса. Любая внешняя форма аутентификации, которая будет «смотреть» в интернет, будет подвержена данной атаке. В прошлом году брутфорс не раз являлся первичным вектором (Initial Access) проникновения в инфраструктуру.

T1133 — External Remote Services

К данному типу относятся инциденты, связанные с атаками на внешние сервисы, такие как VPN, VNC и другие. Зачастую после таких атак злоумышленники также могли получить доступ к внутренней инфраструктуре.

T1110.003 — Password Spraying

Инциденты данной категории связаны с использованием метода подбора паролей, когда один пароль тестируется для множества собранных ранее учетных записей. Злоумышленники могут собрать список учетных записей методами OSINT: например, изучить сайт атакуемой организации или найти контакты и конкретных людей, отвечающих за то или иное направление; кроме того, огромное количество контактов содержится в многочисленных утечках учетных записей. Собрав эту информацию, злоумышленники могут не просто перебирать пароли для одной учетной записи, что с высокой долей вероятности будет обнаружено и заблокировано, но тестировать всего один пароль для множества точно существующих записей в организации.

T1071.004 — Application Layer Protocol, DNS

Категория вредоносной сетевой активности, которая включает в себя атаки с применением протоколов прикладного уровня и DNS. DNS — один из наиболее распространенных видов трафика, который генерируется в инфраструктуре, поэтому злоумышленники часто применяют его для коммуникации с командными серверами (C2), а также при туннелировании и маскировании вредоносного трафика.

T1090.003 — Proxy: Multi-hop Proxy

Инциденты, связанные с использованием прокси с множественными прыжками (например, сети Tor и i2p). Часто Tor и другие многоуровневые сети применяются злоумышленниками для сокрытия реального адреса атаки или как средство для обратной коммуникации (backdoor). Дело в том, что в случае использования таких сетей пакеты проходят через множество промежуточных узлов, и на выходе мы будем видеть только адрес так называемой «выходной ноды». Таким образом, злоумышленники могут прятать адреса своей реальной инфраструктуры и избегать их блокировки, т. к. даже если заблокировать адреса одной «выходной ноды», то в следующий раз атаки продолжатся с другой.

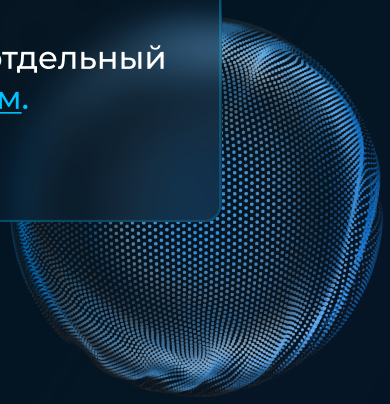
T1021 — Remote Services

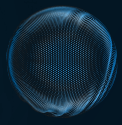
Инциденты, связанные с удаленными службами, когда уже из защищаемого периметра осуществляется нелегитимное обращение к внешним сервисам удаленного администрирования. Зачастую после компрометации какого-либо хоста в инфраструктуре злоумышленник устанавливает соединение с подконтрольной ему инфраструктурой посредством популярных сервисов удаленного администрирования. Это могут быть SSH, RDP, VNC, а иногда и WinRM-сервисы.

T1219 —Remote Access Software

Инциденты, связанные с программным обеспечением удаленного доступа. Зачастую для обеспечения возможности контроля скомпрометированного хоста или же на этапе его заражения (например, в результате фишинговой атаки) злоумышленники разворачивали легитимные программы для удаленного администрирования, такие как AnyDesk, TeamViewer, Ammyy Admin, Radmin, TightVNC и другие. Нередко такие программы использовались инсайдерами, поскольку не требуют специальных настроек, интуитивно понятны в использовании.

В 2023 году мы подготовили отдельный отчет по инсайдерским атакам.





Ринат Сагиров
Руководитель департамента мониторинга и реагирования, «Инфосистемы Джет»

В целом, в прошлом году наблюдался значительный рост обращений от организаций на проведение расследований и оказание экспертных консультаций. Так, количество подобных обращений в 2023 году выросло в 2,5 раза по сравнению с 2022 годом. Один из ярких примеров: в рамках экспертных консультаций мы зафиксировали продажу доступа в целевую инфраструктуру, который затем был продан профессиональной группировке. К счастью, мы успели своевременно предупредить потенциальную жертву, и компания предотвратила атаку на стадии развертывания инструментов на скомпрометированном хосте.

2.6 Управление уязвимостями

2023 год подчеркнул критическую необходимость для организаций реактивно идентифицировать и устранять уязвимости в их ИТ-ландшафте. Временной промежуток между публикацией информации о новой уязвимости и началом ее активной эксплуатации системно сокращается, а окно для реакции и устранения уязвимостей становится всё более узким, требуя от организаций быстрого и эффективного реагирования.

В рамках проектов по тестированию на проникновение 2023 года мы выделили следующие основные категории уязвимостей:

- **46% — Небезопасная конфигурация.** К этой категории относятся уязвимости, которые вызваны отсутствием практики безопасной конфигурации инфраструктуры (использование протоколов LLMNR/NBT-NS/mDNS, доступность административных интерфейсов, раскрытие информации о компонентах приложения).

- **23% — Устаревшее ПО.** Сюда относится эксплуатация уязвимостей в старом ПО или устаревших компонентов (Log4j). В том числе в 2023 году всё еще встречается уязвимость MS17-010.

- **23% — Простые или словарные пароли пользователей и сервисных учетных записей.** Для различных внутренних задач разработчики и администраторы часто не заморачиваются с паролями и используют распространенную пару «admin:admin». В части пользователей обычно используемые пароли напрямую зависят от парольной политики. Чем чаще пользователям необходимо менять пароли — тем проще они будут.

Кейс

Зарплаты всей компании по паролю 11111

В рамках проведения работ по тестированию на проникновение веб-приложения системы управления персоналом, доступной из сети интернет, помимо уникального пароля все пользователи имели еще один — технический. Сбор логинов из почтовых адресов и доступных страниц в социальных сетях и пять цифр простого пароля привел к получению доступа к данным по кадровым перемещениям, личным данным и ФОТ всего персонала.

Владимир Ротанов
Руководитель группы практического анализа защищенности, «Инфосистемы Джет»

Несмотря на то, что каждый день появляются новые уязвимости, база для взлома остается прежней: уязвимости 2-3-5-летней давности, слабые конфигурации, а особенно — пароли по умолчанию, которые приводят к успешной компрометации инфраструктуры и данных.

2.7 Кадры, компетенции, таланты

В 2023 году отмечалось стабильно большое число вакансий ИБ-специалистов и рост конкуренции среди работодателей: санкции, переход на отечественное ПО, рост числа атак увеличили нагрузку на уже задействованных работников, что потребовало расширения штата. Нехватку персонала ИБ мы наблюдали у **93%** наших заказчиков, особенно трудности с наймом компании испытывали при поиске специалистов на руководящие позиции и аналитиков SOC.

Уход ключевого работника означает уход экспертизы, поэтому многие HR сфокусировались на стратегии планирования преемственности и удержания талантов.

Текучка, выгорание, дороговизна экспертов во многом стали драйверами привлечения молодых кадров (студентов). Так, **23%** компаний готовы рассматривать студентов-выпускников, которые проходили практику в других компаниях, либо самоучек с хорошими базовыми знаниями.

Многие компании готовы рассматривать ИТ-специалистов без профильного высшего образования в ИБ и наращивать компетенции по мере выполнения рабочих обязанностей (как извне, так и внутренних специалистов).

Елена Агеева
Ведущий консультант по ИБ, куратор направления работы с профильными вузами, «Инфосистемы Джет»

В 2023 году мы наблюдали возрастающий интерес крупных компаний к работе со студентами профильных специальностей: образовательные мероприятия, стажировки, CTF и другие мероприятия проводились силами ИТ/ИБ-компаний. Отрасль стремится подготовить как можно более зрелые кадры уже на этапе получения образования. Привлечение к реальному миру ИБ дает свои плоды: 79% студентов говорят о том, что направление ИБ им интересно и они планируют работать по специальности, а 27% студентов либо уже совмещают учебу и работу по специальности, либо проходили стажировку в области ИБ.

3. Итоги и прогнозы

От масштабных кибератак и усовершенствования методов хакеров до прогрессивных изменений в законодательном регулировании — 2023 год был полон событий, которые определят дальнейшее развитие индустрии. Что будет с киберпространством в 2024 году? Мы публикуем ключевые вызовы кибербезопасности, которые ожидаем в новом году.

Рост числа атак на цепочки поставок

В современном мире кибербезопасность не может быть ограничена только пределами одной организации — она должна распространяться на экосистему партнеров и поставщиков. В 2023 году мы увидели широкий интерес злоумышленников к атакам на взаимосвязанные компании, публичными стали десятки крупных инцидентов. Управление рисками цепочки поставок станет одним из ключевых приоритетов повышения киберустойчивости бизнеса в 2024 году.

Развитие рынка киберстрахования

Увеличение количества кибератак и их сложности постепенно приводит к увеличению инвестиций в рынок киберстрахования. Крупные компании начнут серьезнее рассматривать страхование в качестве компонента стратегии управления бизнес-рисками для минимизации финансовых потерь.

Широкое использование искусственного интеллекта (ИИ) для проведения атак

Как и в случае с любой современной технологией, использование ИИ злоумышленниками — вопрос времени. В настоящее время потенциал использования ИИ для проведения кибератак еще недостаточно раскрыт, поэтому в 2024 году мы ожидаем более широкого использования данных технологий для целей мошенничества и продвинутого фишинга как точки входа в инфраструктуру.

Увеличение числа инсайдерских атак

С начала 2023 года мы наблюдали рост инсайдерских атак от рядовых пользователей в 1,5 раза по сравнению с аналогичным периодом 2022 года, а объявления о покупке и продаже инсайдерской информации составляют около трети всех предложений форумов Даркнета. В 2024 году мы прогнозируем, что злоумышленники продолжат активно вербовать инсайдеров изнутри для получения доступа в сеть компании и «слива» критичных данных.

Рост значимости человеческого фактора в безопасности

Мы прогнозируем, что всё больше внимания будет уделяться обучению и повышению компетенций служб реагирования с использованием сервисов киберучений, так как человеческие ошибки и недостаток практических навыков противодействия сложным атакам остаются одной из основных причин успешных кибератак.

Более широкое внедрение инструментов проактивной безопасности

Мониторинг теневых форумов для выявления готовящихся атак, анализ поверхности атаки и других доступных данных о компании позволяет заранее понять, с какими угрозами может столкнуться организация в ближайшее время, и предпринять меры для их предотвращения. Мы прогнозируем широкое распространение данных сервисов и услуг, что сделает эту практику доступной даже для организаций с ограниченными ресурсами.

Увеличение числа масштабных и сложных атак: «играй по-крупному или иди домой» (Go Big or Go Home)

В 2024 году мы ожидаем увеличения числа сложных многоступенчатых кибератак. Во многих крупных организациях, которые представляют интерес для злоумышленников, уже есть SOC (in house или аутсорс), поэтому хакерам необходимо действовать незаметно, тратить много времени на изучение особенностей поведения пользователей, чтобы «смешаться с толпой» для нанесения урона. В прошлом году хакеры активно осуществляли многоэтапные атаки через подрядчиков, и в этом году схемы взломов могут становиться еще более сложными и изощренным.

О нас

Центр информационной безопасности компании **«Инфосистемы Джет»** — это профессиональное сообщество специалистов по ИБ. Мы защищаем коммерческие компании и государственные организации от киберугроз уже более 25 лет. Сегодня наша команда — это более 400 экспертов в области информационной безопасности, которые реализуют порядка 300 комплексных проектов в год для защиты бизнеса от киберугроз в России и СНГ.

Наша главная задача — создание и внедрение систем, обеспечивающих реальную безопасность бизнеса.

«Инфосистемы Джет» — одна из крупнейших ИТ-компаний в России. С 1991 года работает на рынке системной интеграции, реализуя ежегодно более 1000 проектов. Штат — более 2000 сотрудников.

Входит в **ТОП-5** крупнейших российских ИТ-компаний (RAEX 2023г.). Лидер на рынке ИТ-аутсорсинга в России (Tadviser 2022г.), **№1** среди крупнейших поставщиков инфраструктуры дата-центров (Cnews 2022г.), **№2** среди крупнейших поставщиков ИТ-услуг (RAEX 2023г.), **№2** среди крупнейших интеграторов в сфере защиты информации (CNews Analytics, 2022г.), **№2** среди крупнейших поставщиков для промышленности (Tadviser 2022г.), **№2** среди крупнейших поставщиков для российских банков (Tadviser 2022г.).

Ключевые направления деятельности «Инфосистемы Джет»: ИТ-инфраструктура, сети и инженерные системы, ИТ-аутсорсинг, информационная безопасность, машинное обучение, заказная разработка ПО, внедрение и сопровождение бизнес-приложений enterprise-уровня, промышленная безопасность и IoT.

jetcsirt.su

csirt@jet.su

+7 495 411-76-01

127015, г. Москва, ул. Большая Новодмитровская,
д.14, стр. 1, офисный центр «Новодмитровский»

Инфосистемы Джет