

Актуальные киберугрозы для промышленных организаций

(итоги 2022 года)



Содержание

Статистика атак на промышленные организации	3
Кто и как атакует промышленность	4
Вредоносное ПО	5
Дарквеб в помощь	7
Группировки, атаковавшие промышленные организации	11
Последствия атак на промышленность	12
Примеры громких атак на промышленные организации в 2022 году	13
Заключение и прогнозы	14

Статистика атак на промышленные организации

Высокая технологичность предприятия и использование различных цифровых сервисов и ПО повышают шансы злоумышленника найти способ проникнуть внутрь и совершить недопустимое для компании событие. На протяжении нескольких лет промышленные организации не выходили из первой пятерки отраслей по количеству киберинцидентов, и 2022 год не стал исключением: почти каждая десятая успешная атака на организации приходилась на промышленные предприятия.

Статистика основана на многочисленных расследованиях и открытых данных как российских, так и зарубежных авторитетных источников.

В своих исследованиях мы используем только данные об успешных кибератаках.

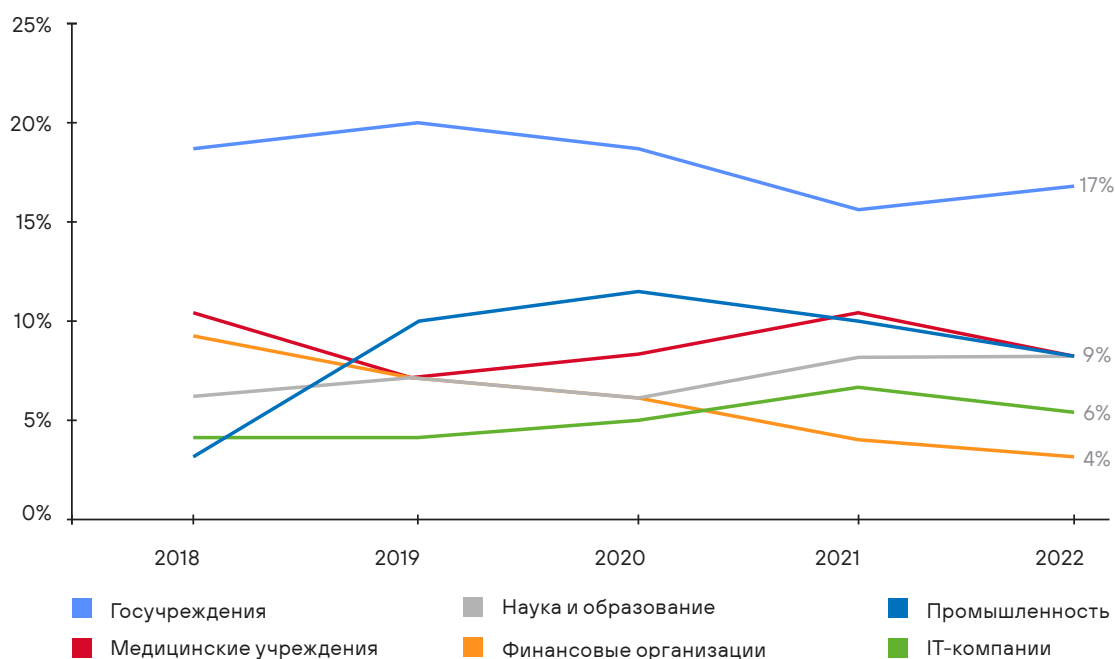


Рисунок 1. Доля атак на промышленные организации (от общего числа атак на организации)

Резкий скачок количества инцидентов в промышленных организациях в 2019 году случился из-за масштабного всплеска активности шифровальщиков. Год 2020-й принес новые вызовы промышленным компаниям: из-за массового перехода сотрудников на удаленную работу традиционно закрытые внутренние системы оказывались доступны извне, если были недостаточно защищены. В 2021–2022 годах стабильно высокий уровень напряженности сохранялся из-за активности шифровальщиков, АРТ-группировок и противостояния в киберпространстве на фоне обострения геополитической обстановки.

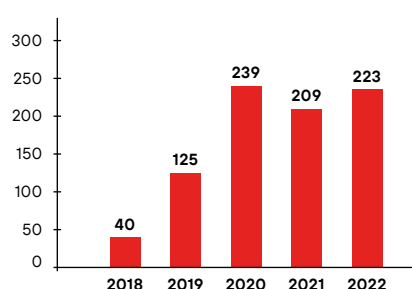


Рисунок 2. Динамика инцидентов (количество по годам)

Всего за 2022 год в промышленных компаниях было зафиксировано 223 инцидента, вызванных атаками злоумышленников, что на 7% больше по сравнению с 2021 годом. Наибольшее количество инцидентов пришлось на II квартал 2022 года — тогда было выявлено 75 успешных атак. Среди атак на организации промышленного сектора 97% являлись целевыми; на атаки АРТ-группировок пришлось 17% от общего количества инцидентов.

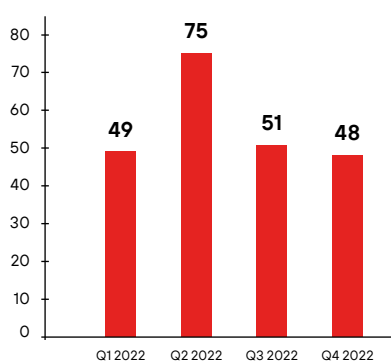


Рисунок 3. Динамика инцидентов (количество по кварталам 2022 года)

Кто и как атакует промышленность

Из успешных атак 87% были направлены на компьютеры, серверы и сетевое оборудование — основные мишени вымогателей. В 44% случаев злоумышленники проводили атаки на персонал промышленных организаций с помощью вредоносных рассылок по электронной почте (94%) и фишинговых сайтов (10%). Направлены на веб-ресурсы (сайты) организаций промышленного сектора были 12% атак.

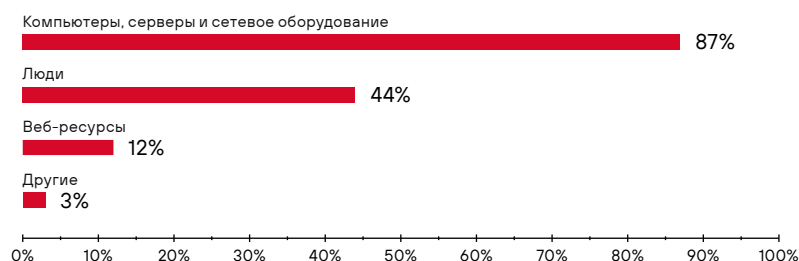


Рисунок 4. Объекты атак на промышленные организации (доля атак)

В большинстве успешных атак (70%) на промышленные организации злоумышленники применяли вредоносное ПО. Почти в половине кибератак (44%) на промышленность были использованы методы социальной инженерии. Доля атак, в которых эксплуатировались уязвимости ПО, составила 43%.

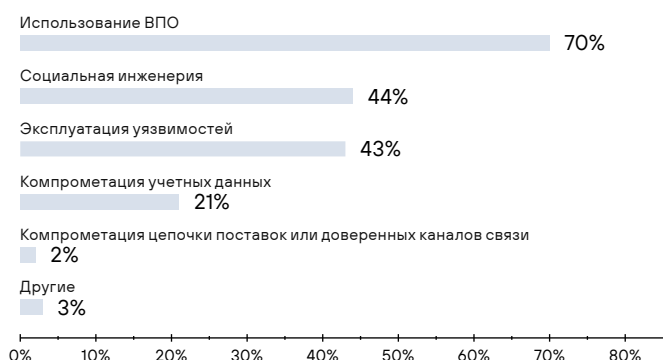


Рисунок 5. Методы атак на промышленные организации (доля атак)

Вредоносное ПО

Наиболее распространенным типом вредоносных программ стали шифровальщики — две трети атак с использованием ВПО были проведены с их помощью. Тремя наиболее популярными типами программ-вымогателей в промышленной отрасли в 2022 году стали LockBit, BlackCat (ALPHV) и Conti. Все три программы-вымогателя имеют реализацию как для Windows, так и для Linux. Каждый штамм представляет серьезную угрозу для предприятий из любой отрасли, не только из промышленной. К ним нельзя относиться легкомысленно, когда речь идет об обеспечении доступности и конфиденциальности данных.

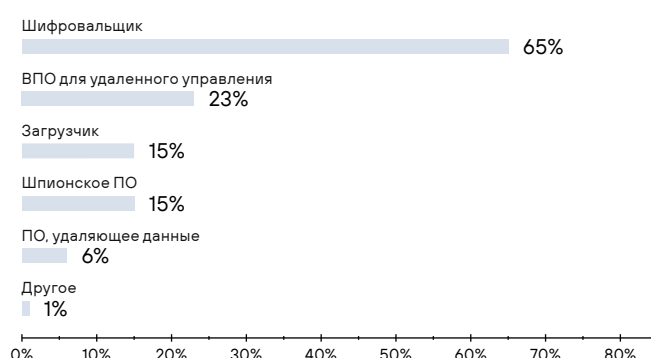


Рисунок 6. ВПО, используемое в атаках на промышленные организации (доля атак с использованием ВПО)

Трендом 2022 года в атаках на промышленный сектор оказалось применение злоумышленниками вайперов — ПО, удаляющего данные. Такое ПО может приводить к нарушениям технологических процессов и выходу оборудования из строя. Вайперы Meteor и CaddyWiper были популярны в первом квартале 2022 года и активно используются до сих пор. Они могут причинить серьезный вред организациям, удаляя или искажая важные данные, нарушая работу сетей, блокируя доступ к системам или приложениям.

ВПО для удаленного управления было использовано в 23% случаев. Здесь можно выделить распространенные трояны удаленного доступа (RAT) PlugX, Remcos и TRISIS, которые применялись для несанкционированного доступа к корпоративной инфраструктуре. Эти трояны могут использоваться для различных операций в системе: например, кражи конфиденциальных данных, нарушения основной деятельности или установки дополнительных вредоносных программ.

В 15% атак применялись программы для шпионажа. Самым популярным оказался вирус-шпион Agent Tesla, который может использоваться для кражи конфиденциальной информации. Он способен собирать и отправлять на командный сервер такие данные, как нажатия клавиш, снимки экрана и сетевой трафик. Чтобы предотвратить распространение шпионского ПО, организациям важно иметь современную систему антивирусной защиты и регулярно сканировать свои сети на наличие потенциальных угроз. Кроме того, сотрудники должны быть обучены тому, как распознавать подозрительные электронные письма или веб-сайты, которые могут содержать вредоносные ссылки.

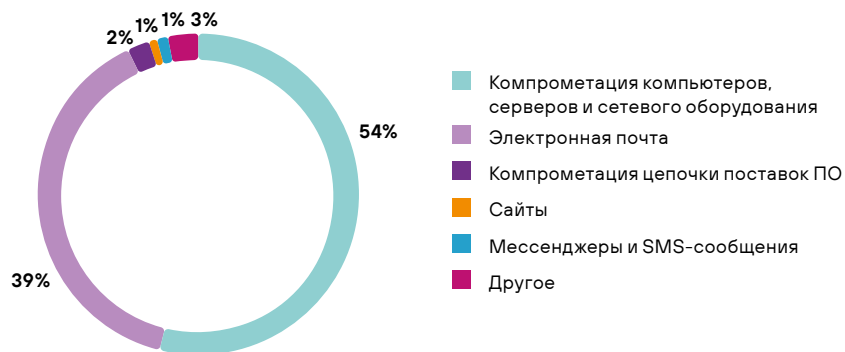


Рисунок 7. Способы распространения вредоносного ПО в атаках на промышленные организации

Наиболее популярным каналом социальной инженерии в промышленном секторе стала электронная почта. С ее помощью злоумышленники доставляют вредоносное ПО, маскируя его под различные документы, и рассылают письма с вредоносными ссылками, при переходе по которым загружается ВПО или открываются фишинговые сайты.

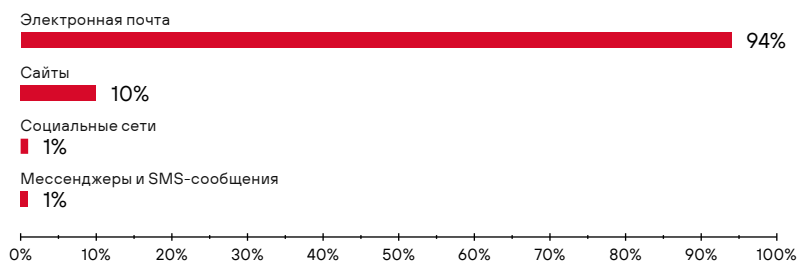


Рисунок 8. Каналы социальной инженерии, используемые злоумышленниками в атаках на промышленность

Дарквеб в помощь

Количество доступов к инфраструктуре промышленных организаций, продаваемых в дарквебе, в 2022 году выросло на 40% по сравнению с 2021 годом.

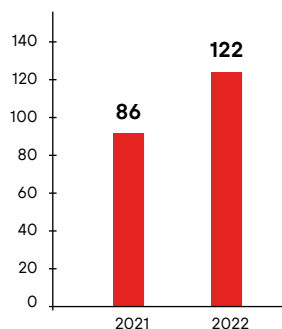


Рисунок 9. Количество продаваемых доступов к промышленным компаниям по годам

В 2022 году доступы составляли 75% от всех объявлений, относящихся к промышленности. Такой перевес объясняется желанием легкого заработка и популярностью этого направления у новичков, которые, получив первоначальный доступ, продают его более квалифицированным злоумышленникам для дальнейшего развития атаки.

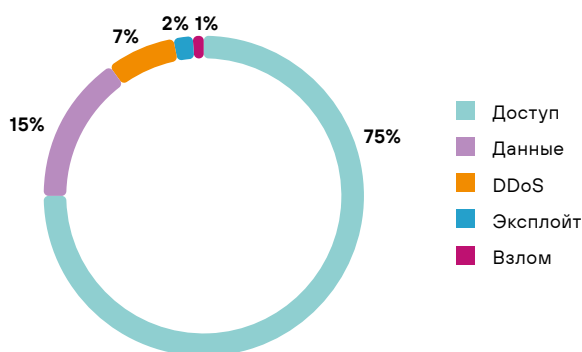


Рисунок 10. Темы объявлений на форумах в дарквебе, касающихся промышленных компаний

На теневых форумах встречаются объявления о продаже большого количества доступов к компаниям по различным ценам: они содержат сведения о доходе организации, количестве устройств в сети и уровне привилегий полученного доступа.

Продажа доступов VPN-RDP
25.11.2022

25.11.2022

Тип доступов: VPN-RDP (Forti)
Все доступы валид.
Всегда готов к гаранту!
Что бы узнать больше о доступе пиши в ПМ

Пользователь
Регистрация: 30.10.2022
Сообщения: 6
Реакции: 1

France/<5 kk\$/Machinery industry/User - 100\$ host 74 / av Windows Defender
Poland/<5 kk\$/Furniture production/User - 100\$ host 41 / av -
Canada/<5 kk\$/Custom steel fabrication/User - 100\$ 50\$ host 13 / av DefCon
Chile/22 kk\$/Manufacturing/Local Admin - 350\$ host 22 / av Eset
Canada/5-10 kk\$/Fabric-textile factory/Local Admin - 120\$ host 56 / av Eset
Italy/6 kk\$/Manufacturing/Domain Admin - 180\$ host 36 / av Malwarebytes
Australia/5 kk\$/Manufacturing/User - 100\$ host 22 / av Webroot
France/<5 kk\$/Non-profit organization/Local Admin - 100\$ host 68 / av Trend Micro
France/7 kk\$/Federal Association/User - 150\$ host 49 / av WithSecure Elements Agent
USA/<5 kk\$/Business consulting firm/Domain Admin - 200\$ host 18 / av SentinelOne
USA/<5 kk\$/Commercial & Residential Construction/Domain Admin - 150\$ host 3 / av -

Рисунок 11. Объявление о продаже доступов к инфраструктуре промышленных компаний на теневом форуме

Стоимость большинства доступов находится в диапазоне от 500 до 5000 \$. Если цена ниже 500 долларов, речь идет о доступе в небольшую компанию с невысоким уровнем привилегий. Низкая стоимость может также говорить о перепродаже доступа или его продаже сразу нескольким лицам. Количество доступов стоимостью более 5000 \$ невысоко, такая стоимость может быть оправдана большой доходностью и размером компании, а также высоким уровнем привилегий учетной записи. В некоторых случаях продавец может снизить высокую цену, если видит, что она неактуальна.

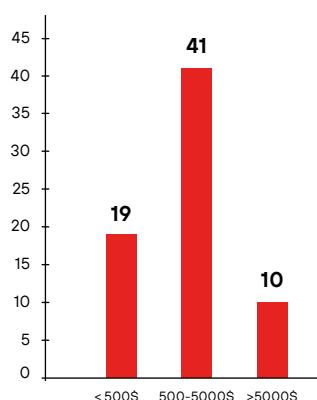


Рисунок 12. Количество доступов в дарквебе по отношению к их цене

 Пользователь Регистрация: 23.06.2022 Сообщения: 25 Реакции: 26	12.07.2022 Производитель упаковки для полупроводников, компонентов медицинского и электронного оборудования. 1500 Сотрудников. Штаб-квартира в Гонконге, производство в Китае, представительства по всему миру. Около 240 устройств в сети. 3 домена, 4 наса, 5 хостов esxi. Доступ к 2 доменам, всем насам и esxi есть. price 7000\$ За подробностями в ГМ. 🗨 Жалоба
 Пользователь Регистрация: 23.06.2022 Сообщения: 25 Реакции: 26	22.07.2022 актуально price 5000\$ 🗨 Жалоба
 Пользователь Регистрация: 23.06.2022 Сообщения: 25 Реакции: 26	27.07.2022 актуально price 2000\$ 🗨 Жалоба
 Пользователь Регистрация: 23.06.2022	13.08.2022 доступ актуален крайнее снижение до 500\$

Рисунок 13. Снижение цены доступа

Если сравнивать количество доступов к компаниям в зависимости от их дохода, то к компаниям с небольшим доходом (до 100 млн \$) доступов на теневом рынке больше на 30%. Это обусловлено низким уровнем защищенности таких организаций, что позволяет злоумышленникам с меньшими усилиями получить первоначальный доступ.

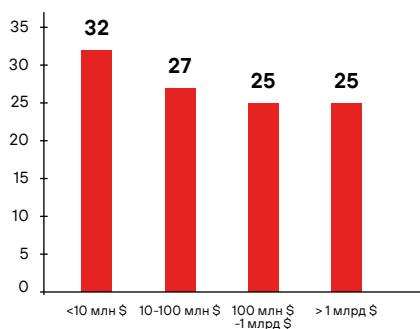


Рисунок 14. Доходность компаний, к которым продавался доступ

Группировки, атаковавшие промышленные организации

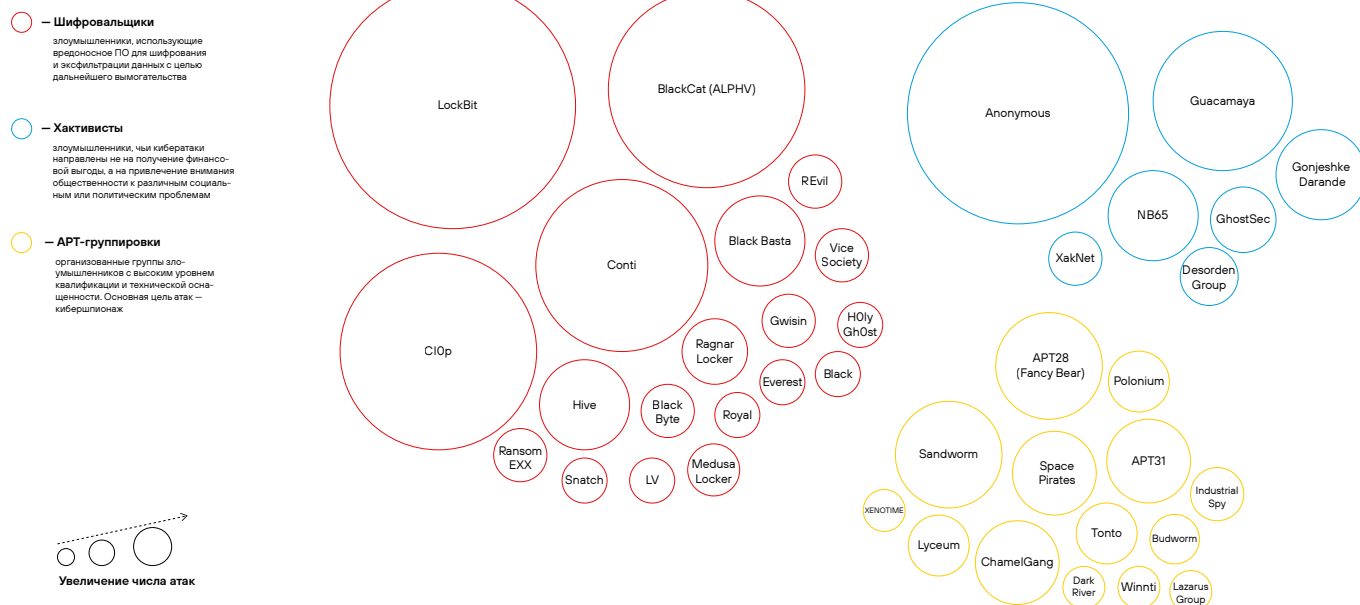


Рисунок 15. Группировки, атаковавшие промышленные организации в 2022 году

Наибольшую активность в отношении промышленного сектора проявляли группировки вымогателей, в частности LockBit, BlackCat, ClOp, Conti. Из успешных атак 70% были проведены с использованием вредоносного программного обеспечения, среди которого явными лидерами оказались программы-шифровальщики.

Атаки хактивистов в основном были направлены на нарушение основной деятельности организаций, создание помех в предоставлении сервисов и похищение конфиденциальной информации. Для достижения своих целей киберактивисты проводили массированные DDoS-атаки, взламывали сайты промышленных компаний, похищали деловую переписку компаний с почтовых серверов.

Среди АРТ-группировок можно выделить Space Pirates, APT31 и ChamelGang. Space Pirates на сегодняшний день наиболее активная из них. С момента публикации нашего [отчета](#) в мае 2022 года эта группа продолжает проводить новые атаки. Среди ее целей государственные учреждения, организации авиационно-космической отрасли, энергетики, ВПК, промышленности. Шпиона за компаниями, эта группировка использует в основном следующие инструменты: Deed RAT, MyKLoadClient, Zupdax, RtlShare. Однако в недавнем исследовании мы обнаружили, что она также использует бэкдор ShadowPad, который применяется и другими злоумышленниками азиатского региона. В своих атаках группа использует фишинг и уязвимости в продуктах компаний на внешнем периметре.

Группа APT31 до 2021 года не атаковала объекты в России. Но недавно специалисты PT Expert Security Center первыми выявили такую активность группировки и подготовили об этом подробный [отчет](#). Группа атакует государственные учреждения, СМИ, ТЭК. Ее целью является шпионаж, у нее тоже есть свой набор инструментов, а в качестве контрольных серверов она использует облачные хранилища для обхода сетевых средств обнаружения. В качестве исходного вектора применяется фишинг.

ChamelGang активизировалась в середине 2021 года. Группа начала свои атаки с эксплуатации уязвимости ProxyShell на серверах Exchange по всему миру. Основная ее цель — шпионаж. Для сокрытия ВПО она использует собственные инструменты и нетривиальные техники.

Последствия атак на промышленность

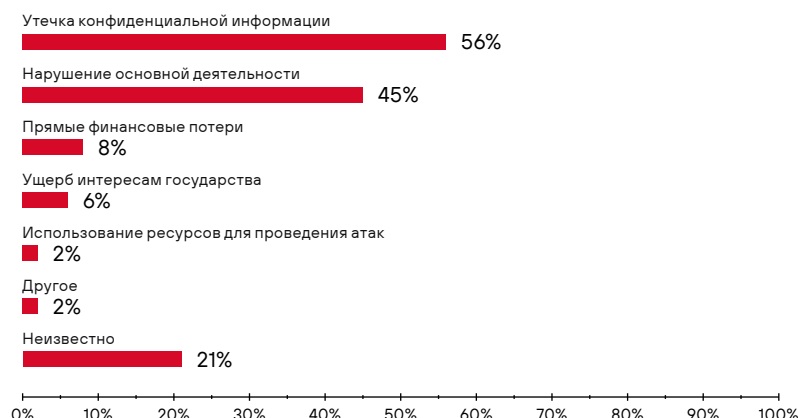


Рисунок 16. Последствия атак на промышленные организации (доля атак)

Общая тенденция переключения злоумышленников на похищение конфиденциальной информации не обошла стороной и промышленный сектор: 56% успешных атак привели к утечкам значимых данных. Наиболее распространенными типами украденных данных стали сведения, содержащие коммерческую тайну, и персональные данные. В 45% случаев атаки привели к нарушению основной деятельности промышленных организаций: из-за атак шифровальщиков становилась недоступной их инфраструктура.

В III квартале особое внимание злоумышленников привлекли организации топливно-энергетического комплекса. Из-за атаки вымогателей BlackCat оказались недоступными клиентские порталы оператора газового трубопровода и электросети Creos Luxembourg. В результате взлома была похищена техническая документация, сведения о контрактах и данные о клиентах оператора. С разницей в несколько дней были совершены атаки на системы итальянского нефтеперерабатывающего гиганта Eni и итальянского энергетического агентства Gestore dei Servizi Energetici. Обе атаки привели к масштабным утечкам конфиденциальной информации, недоступности сервисов и сбоям в обслуживании клиентов.

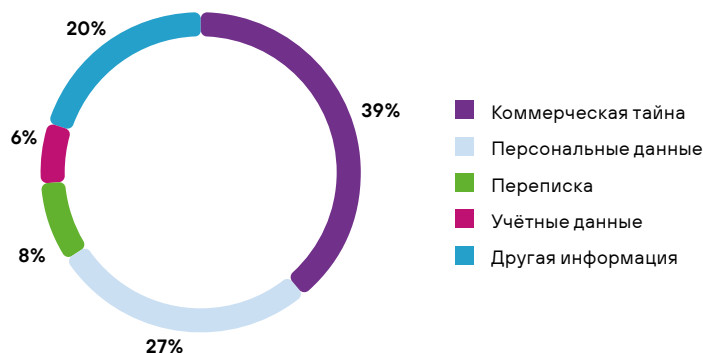


Рисунок 17. Типы украденных данных

Примеры громких атак на промышленные организации в 2022 году

1. Атака на крупнейшего производителя мясной продукции «Тавр». С помощью вредоносного ПО злоумышленникам удалось поразить инфраструктуру компании (серверы, рабочие станции и пр.). Это вызвало нарушение бизнес-процессов организации, что впоследствии вылилось в экономические потери в десятки миллионов рублей.

2. Атака хактивистов на агрохаб «Селятино». Злоумышленникам удалось получить доступ к промышленному контроллеру управления холодильным оборудованием и изменить температуру с -24°C до $+30^{\circ}\text{C}$, что чуть было не привело к порче 400 тыс. тонн замороженной продукции. Сотрудники вовремя заметили атаку и отреагировали на нее.

3. Атака шифровальщика на крупнейший агрохолдинг «Мираторг». Из-за атаки шифровальщика ряд компаний холдинга лишился возможности оформлять в электронном виде производственные и транспортные ветеринарные документы, что осложнило реализацию продукции.

4. Атаки шифровальщиков на операторов ветряных турбин Nordex и Deutsche Windtechnik. Из-за атак компании были вынуждены отключить ИТ-системы и удаленный доступ к управляемым турбинам.

5. Атака шифровальщиков на Junta Administrativa del Servicio Eléctrico de Cartago (JASEC). Масштабная атака Conti вывела из строя государственное агентство, управляющее энергетикой в Картаго (Коста-Рика). Группа вымогателей лишила клиентов возможности оплачивать счета за электричество и интернет.

6. Атака на поставщика электроэнергии ECG в Гане. В результате атаки программы-вымогателя были недоступны сервисы для оплаты и покупки электроэнергии, что вызвало перебои в электроснабжении, а в некоторых областях страны жители несколько дней оставались без электричества.

7. Атака хактивистов на три иранских сталелитейных завода. В результате крупной атаки были нарушены технологические процессы производства, а на одном из заводов злоумышленникам удалось обрушить ковш с жидким чугуном, что вызвало пожар в цехе. По некоторой информации, в атаке использовалось ПО, удаляющее данные.

8. Атаки на нефтяные компании Oiltanking и Mabanaft, нефтяные терминалы в Бельгии и Нидерландах. В результате этих атак многие автоматизированные технологические процессы, связанные с загрузкой и разгрузкой резервуаров, были отключены. Компании временно не могли выполнять договорные обязательства. Также были атакованы крупные нефтяные терминалы SEA-Invest в Бельгии и Evos в Нидерландах — эти события повлияли на работу портов во всей Европе и Африке и привели к задержкам в поставках топлива.

Заключение и прогнозы

В текущих реалиях вопрос обеспечения кибербезопасности промышленных предприятий стоит особенно остро. Количество инцидентов остается по-прежнему высоким, злоумышленники реализуют все больше недопустимых событий, которые влияют не только на отдельные организации, но и на целые отрасли.

В 2023 году целями преступников, стоящих за кибератаками на промышленные предприятия, будет не финансовая выгода или получение крупных сумм выкупа, а перебои в деятельности компаний, остановка их важнейших технологических процессов и аварии. В связи с этим мы прогнозируем появление новых вредоносных программ, ориентированных на промышленные системы, а также более широкое применение вайперов, приводящих к уничтожению данных на устройствах. Также мы ожидаем появления новых кампаний кибершпионажа в отношении промышленных предприятий и ТЭК.

2023 год не станет легким для организаций промышленного сектора: к отрасли приковано значительное внимание не только атакующих, но и регуляторов, которые намерены значительно повысить состояние защищенности отрасли. Это, в свою очередь, потребует активной работы и большого объема ресурсов для обеспечения необходимого уровня безопасности и соответствия новым, повышенным требованиям регуляторов.

Множество новых злоумышленников, появившихся в предыдущем году, обратили свое внимание на промышленный сектор. Текущий год не станет исключением в тенденции появления новых игроков.

Организациям стоит изучить свои информационные активы, определить слабые места и возможные угрозы. В первую очередь необходимо определить возможные события, которые недопустимы для функционирования бизнеса, и регулярно проводить верификацию таких событий на практике с помощью тестирования на проникновение или размещения цифровых двойников на киберполигонах. Такой подход поможет выстроить систему комплексной защиты и мониторинга, которые не позволят злоумышленникам нанести ущерб организации и ее клиентам. Из-за тенденции к нарушению основной деятельности промышленных организаций с помощью различного ВПО (шифровальщики, вайперы) решения резервного копирования позволят быстро восстановиться, если атака все-таки достигла своей цели. Важно помнить о влиянии человеческого фактора на успешность кибератак и проводить мероприятия для повышения бдительности и осведомленности в сфере кибербезопасности, а также обучение по противодействию атакам методами социальной инженерии.

Для заметок

