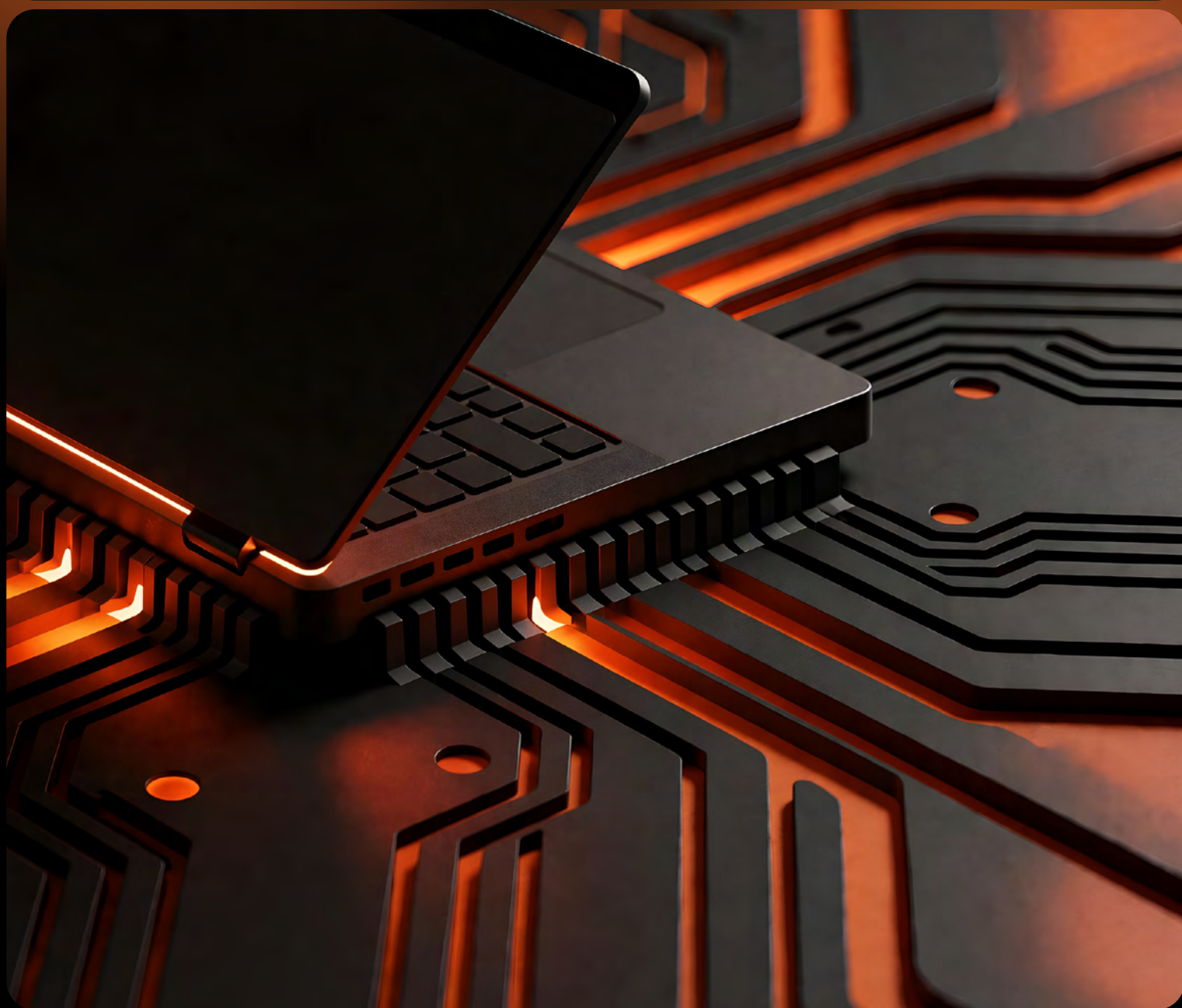
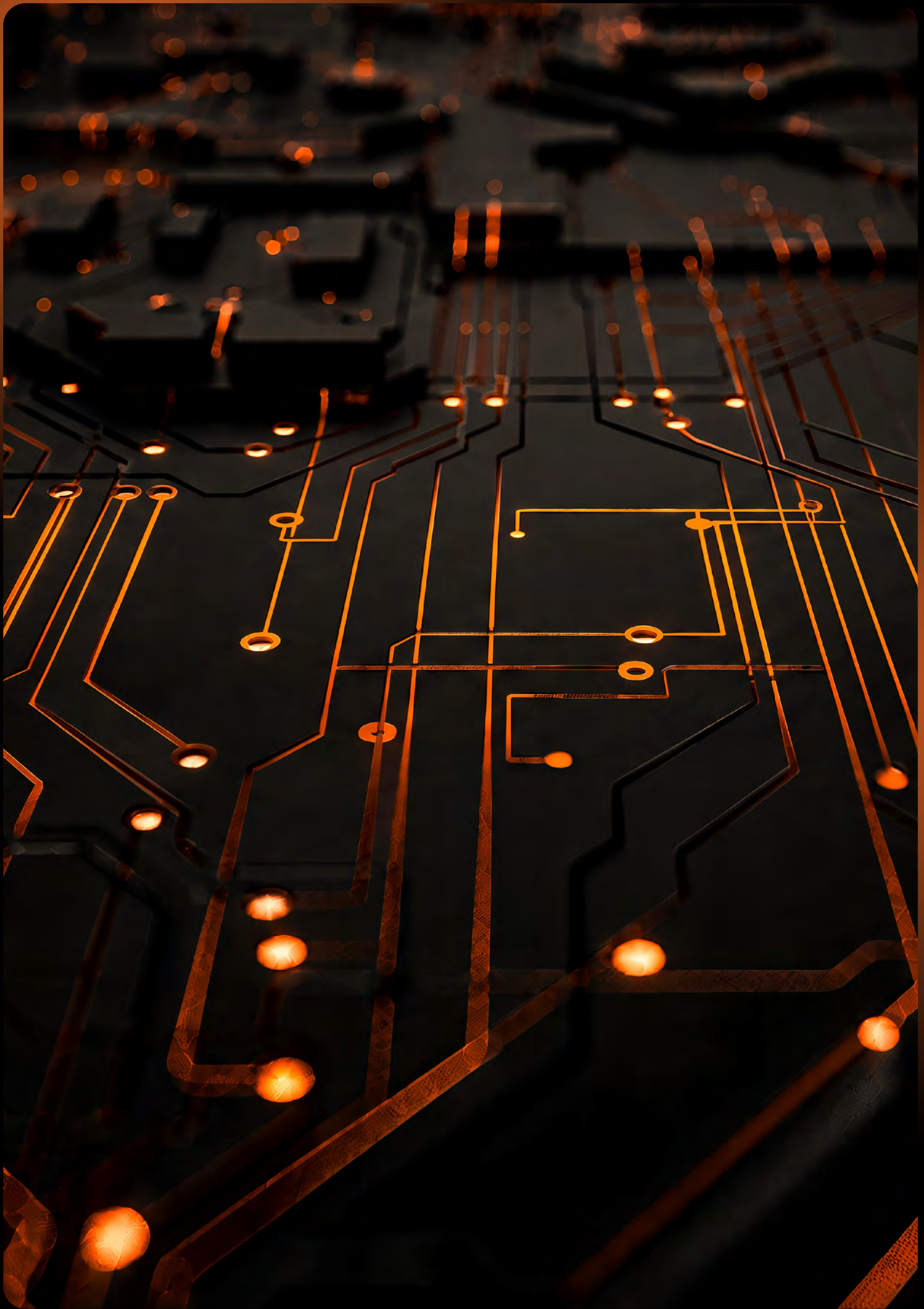


ОТ РЕАГИРОВАНИЯ К ПРЕДОТВРАЩЕНИЮ: ИНЦИДЕНТЫ 2025

ANGARA MTDR | DFIRMA





ГЕОГРАФИЯ ПРЕДОСТАВЛЕНИЯ УСЛУГ ANGARA MTDR

Angara MTDR — это сервисы для управления киберустойчивостью, в которых процесс и его эффективность определяют средства и меры защиты, а не наоборот.

Десятилетний опыт оказания услуг Центром мониторинга и реагирования на компьютерные инциденты (Angara SOC), проверенные годами подходы к проектированию, внедрению и развитию комплексных корпоративных систем защиты, а также собственные запатентованные методы прогнозирования угроз позволили нам создать сервисы, постоянно адаптируемые в зависимости от изменения ландшафта угроз и масштабируемые вместе с потребностями организации заказчика.

Angara MTDR предоставляет комплекс услуг для защиты организаций от актуальных угроз на всех этапах атак (от первичной разведки и подготовки атаки до нанесения ущерба) внутри периметра и за его пределами, в т.ч. расследование, устранение последствий и восстановление ИТ-инфраструктуры, если инцидент уже произошел. В портфель Angara MTDR вошли знакомые вам услуги Angara SOC и новые сервисы.



Международные проекты, в которых участвовали команды Angara MTDR



Мьянма



Монголия



ЮАР



Бразилия



Сьерра-Леоне



Камбоджа



ОГЛАВЛЕНИЕ



ВВЕДЕНИЕ	05
ДИСКЛЕЙМЕР	06
КЛЮЧЕВЫЕ ВЫВОДЫ	07
ЛАНДШАФТ КИБЕРУГРОЗ	09
Кто атакует	10
Кого атакуют	12
Инструменты атакующих	15
Длительность атак	16
РАЗВЕДКА	19
ПОДГОТОВКА РЕСУРСОВ	25
ПОЛУЧЕНИЕ ПЕРВОНАЧАЛЬНОГО ДОСТУПА	29
ВЫПОЛНЕНИЕ	37
ЗАКРЕПЛЕНИЕ В СИСТЕМЕ	43
ПОВЫШЕНИЕ ПРИВИЛЕГИЙ	51
ОБХОД ЗАЩИТЫ	57
ПОЛУЧЕНИЕ УЧЕТНЫХ ДАННЫХ	63
ИЗУЧЕНИЕ ВНУТРЕННЕЙ ИНФРАСТРУКТУРЫ	69
ПЕРЕМЕЩЕНИЕ ВНУТРИ ПЕРИМЕТРА	73
СБОР ДАННЫХ	79
УДАЛЕННОЕ УПРАВЛЕНИЕ СИСТЕМОЙ	83
ЭКСФИЛЬТРАЦИЯ ДАННЫХ	89
ДЕСТРУКТИВНЫЕ ДЕЙСТВИЯ	93
ИНСТРУМЕНТЫ ПРЕДОТВРАЩЕНИЯ	100

ВВЕДЕНИЕ

Итоги 2025 года подтверждают устойчивую тенденцию: **ландшафт киберугроз в России и странах СНГ продолжает усложняться**. Атаки становятся более целенаправленными, цепочки компрометации — многоступенчатыми, а финансово мотивированные группировки все активнее пересекаются с политически мотивированными акторами, как по инструментарию, так и по выбору жертв. Программы-вымогатели, утечки данных и атаки с целью деструктивного воздействия остаются главными векторами ущерба, при этом малый и средний бизнес стабильно попадает в прицел злоумышленников наравне с крупными организациями.

Отдельного внимания заслуживает использование в атаках искусственного интеллекта. Пока его влияние носит точечный характер: в анализируемых вредоносных образцах мы фиксируем артефакты, свидетельствующие о том, что ИИ применялся на этапе написания или отладки кода. Используются характерные комментарии, стиль именования переменных, типичные структуры, которые выдают участие языковых моделей. В нашей практике еще не встречались кейсы с явным использованием сложных ИИ-инструментов атакующими, однако в мировой повестке уже **зафиксированы случаи создания программ-вымогателей с непосредственным участием генеративных моделей**. Развитие этого направления идет медленно, но вектор очевиден и игнорировать его не стоит.



Повторим тезис, который остается актуальным из года в год: ни один набор защитных решений не дает стопроцентной гарантии. Любой инструмент безопасности требует грамотной настройки под конкретную среду и постоянного внимания в процессе эксплуатации, иначе он превращается в дорогостоящую декорацию.

Текущий ландшафт угроз дает однозначное понимание: попытки взлома не зависят от отрасли, масштаба организации или ее публичного финансового профиля. Вопрос не в том, станете ли вы целью, а в том, как быстро атака будет обнаружена и насколько эффективно на нее отреагируют.



ДИСКЛЕЙМЕР

Представленная в этом исследовании статистика основана на результатах нашей практической работы: мониторинге, расследовании инцидентов и реагировании на угрозы в организациях различных отраслей.

Наша выборка охватывает десятки успешно расследованных кейсов, каждый из которых принес уникальный контекст, будь то финансовый сектор, промышленность, ретейл или отдельные государственные структуры.



Мы понимаем, что любая выборка коммерческой компании имеет свои границы и достаточно субъективна. Несмотря на то что накопленные данные демонстрируют устойчивую корреляцию с публично доступными отраслевыми исследованиями и глобальной статистикой угроз, явное сравнение 2024 и 2025 годов для нас стало вызовом.

В 2024 году объем нашей выборки оказался примерно вдвое ниже, а сама структура кейсов заметно изменилась. Если ранее в практике была выше доля относительно типовых и быстро классифицируемых инцидентов, включая массовые атаки с использованием шифровальщиков, то позднее **выборка стала более разнородной и включала больше комплексных случаев,** требующих более глубокого исследования и нестандартных мер реагирования.

Вместе с тем такая динамика отражает как эволюцию самого ландшафта угроз, так и развитие нашей команды, накопление экспертизы и готовность работать со все более сложными и нетиповыми сценариями.



КЛЮЧЕВЫЕ ВЫВОДЫ

Атрибуция инцидентов усложняется



Граница между киберпреступностью и целевыми атаками размывается — то, что выглядит как оппортунистическая активность, во время расследования нередко оказывается частью зрелой кампании, не говоря уже о потенциальных взаимосвязях отдельных группировок.

Доверяй, но проверяй



Атаки через подрядчиков не теряют актуальности. Доверенные отношения, в частности, с ИТ-компаниями, по-прежнему остаются привлекательным вектором как точка входа в инфраструктуру конечной цели. Доверенный подрядчик с широкими правами доступа остается одним из наиболее ценных активов для злоумышленника.



ИИ входит в инструментарий атакующих



В 2025 году мы фиксировали не только использование сгенерированных сценариев или скриптов для автоматизации рутины, но и случаи использования С2-агентов, написанных или адаптированных с помощью ИИ (так называемый вайб-коддинг). Порог входа для создания кастомного инструментария снижается, что усложняет сигнатурное обнаружение и ускоряет появление новых вредоносных инструментов.

Первичный доступ: скорость решает все



Основываясь на нашей статистике, эксплуатация публично доступных сервисов и использование скомпрометированных учетных данных остаются самыми популярными векторами входа. И если вопрос патч-менеджмента поднимается давно, то и мониторинг утечек перестает быть разовой процедурой: вопрос в том, кто быстрее обнаружит утекшие учетные данные, атакующий или защитник.

Атакующие активнее осваивают техники красных команд



Методы, еще недавно встречавшиеся преимущественно в пентестах и редтим-учениях, в ходе которых намеренно используются максимально скрытные техники, переходят в арсенал реальных злоумышленников. Яркий пример 2025 года — кейсы с эксплуатацией Active Directory Certificate Services (AD CS).

Зрелость и осознанность заказчиков растет



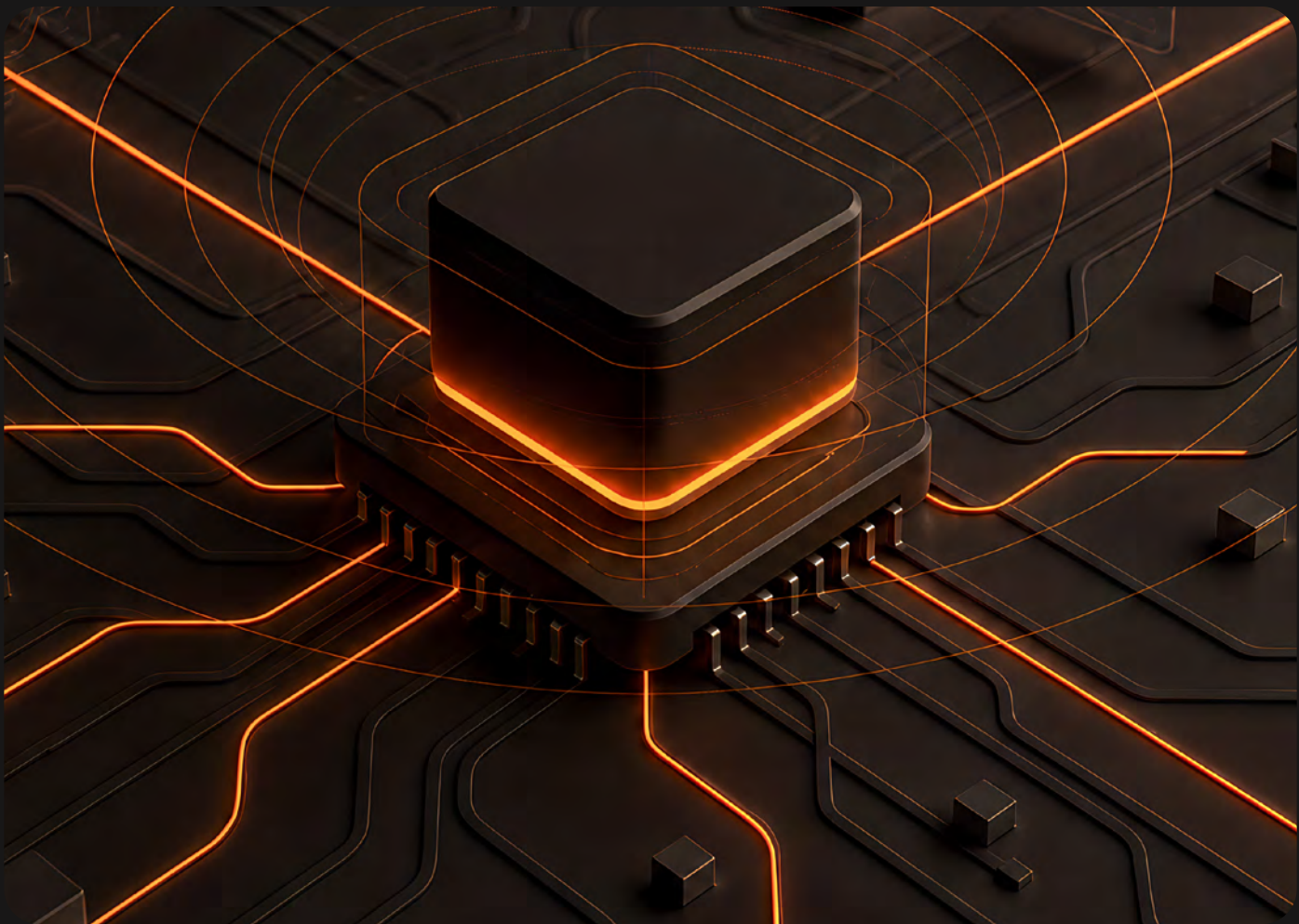
С каждым годом все больше организаций быстрее реагирует на инциденты и подозрительную активность, охотнее взаимодействуют с командами реагирования и осознаннее инвестируют в защиту. Вместе с тем, потенциал для роста остается значительным, особенно в части проактивного обнаружения угроз и готовности к восстановлению.

17 ДНЕЙ

медианный показатель обнаружения злоумышленников

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

наиболее атакуемая отрасль



ЛАНДШАФТ КИБЕРУГРОЗ



КТО АТАКУЕТ

По результатам анализа инцидентов, расследуемых командой реагирования MTDR, в ландшафте киберугроз 2025 года финансово мотивированные атаки остаются доминирующим драйвером на рынке киберпреступности. Быстрый результат, вымогательство, продажа доступов к инфраструктурам компаний, масштабируемость и многопоточность атак, относительно высокий уровень навыков — вокруг этих составляющих строится основная монетизация большинства инцидентов.

Существенная доля инцидентов также пришлась на целевые кампании и активности, которые можно отнести к **APT-группировкам**. Это говорит о наличии атакующих, заинтересованных не только в немедленной выгоде, но и в длительном скрытном присутствии. Так, группировка **Space Pirates** в начале года предприняла попытку вернуться в инфраструктуру одной из государственных организаций, в которой мы расследовали инцидент. Для читателей это сигнал: одних сигнатурных блокировок недостаточно — важно продолжать развивать качество выявления нелегитимной активности, внедряя поведенческий анализ и практики проактивного поиска угроз (threat hunting).

Если в целом описывать угрозы через «группы» и кластеры активности, главный вывод 2025 года — ландшафт достаточно фрагментирован, а атрибуция заметно усложняется.

В течение года мы наблюдали одновременно:

- Появление новых кластеров

В том числе тех, кто, судя по артефактам, мог действовать раньше, но стал различим только после накопления данных. По этой причине в категорию «Другое» были отнесены те инциденты, где нам не удалось точно определить мотивацию атакующих: например, оппортунистическая активность, атаки без ясной дальнейшей монетизации или неоднозначные инциденты.

- «Исчезновение» с радаров части ранее фиксируемых кластеров

Часто это следствие смены инструментов, инфраструктуры и тактик либо ухода в более точечные операции.

- Объединение ранее отдельно отслеживаемых активностей

Новые доказательства (пересечения в инструментах, инфраструктуре, стилях разработки, операционных паттернах) позволяют уверенно говорить об одном операторе или тесно связанном контуре.



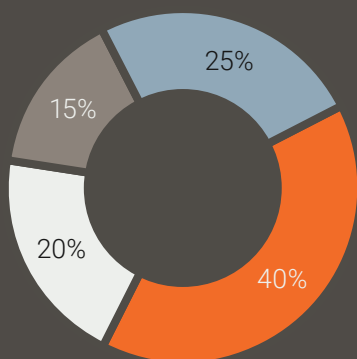


Диаграмма 1.
Мотивация атакующих

- Шпионаж
- Финансовая выгода
- Хактивизм
- Другое

По мере появления дополнительных данных мы также сталкивались с пересмотром классификации некоторых злоумышленников. То, что на ранних этапах выглядит как «обычная киберпреступность», в процессе расследования может приобрести признаки зрелых целевых кампаний: более высокий уровень сокрытия, длительное сохранение доступа, последовательная работа с доменной инфраструктурой и/или собственные инструменты.

Чаще всего во время расследований атак, нацеленных на российские организации, мы встречали группировки **Bearlyfy** и **Thor**. Злоумышленники действуют как минимум с января 2025 года и преследуют финансовые цели (занимаются вымогательством). При этом они не разрабатывают собственные инструменты, а полагаются преимущественно на общедоступные утилиты и слитый код. В качестве финальной полезной нагрузки группа использует программы вымогатели семейства LockBit (в случае Bearlyfy набор дополнен RedAlert для систем Windows, а также Babuk для ESXi). Стоит отметить, что, несмотря на использование «простых» и «известных» инструментов (российские исследователи пишут про LockBit и Babuk уже третий год), их атаки носят достаточно сокрушительный характер.

Хактивизм трансформируется из относительно простых, демонстративных атак в нечто большее. Раньше в категорию хактивистов чаще попадали группировки, ориентированные на публичный

эффект и «шум» (дефейсы, DDoS-атаки, утечки данных). Теперь же значительная часть подобных атак связана с нанесением максимального ущерба российским организациям. **4BID** и **BO Team** — примеры групп, в атаках которых мы видели колоссальный ущерб для организаций.

Да, хактивизм — это все еще про шум, но теперь он не всегда исключает риск реального продолжительного простоя. Фишинговые рассылки как от них, так и от других группировок — **Librarian Likho** (также отслеживаемые как **Rare Werewolf**), **DarkGaboorn** (room155) и **RedCurl**, но уже с иными мотивами — регулярно встречаются нам в телеметрии клиентов наших центров мониторинга.

Для защитников это означает новые вызовы. Требуется более высокая готовность к различным сценариям: от быстрого сдерживания и восстановления систем — до наличия необходимых навыков и средств защиты для обнаружения широкого спектра угроз.



Сайт Angara Security.

Публикация: «Специалисты Angara MTDR зафиксировали активизацию деятельности группировки Rare Werewolf»

Ключевые группировки исследований 2025 года



Silent Crow*



BO Team



4BID



Morlock



Phantom-Core



Space Pirates



ExCobalt



RedCurl



Bearlyfy/
laboo.boo



Warlock Group



THOR

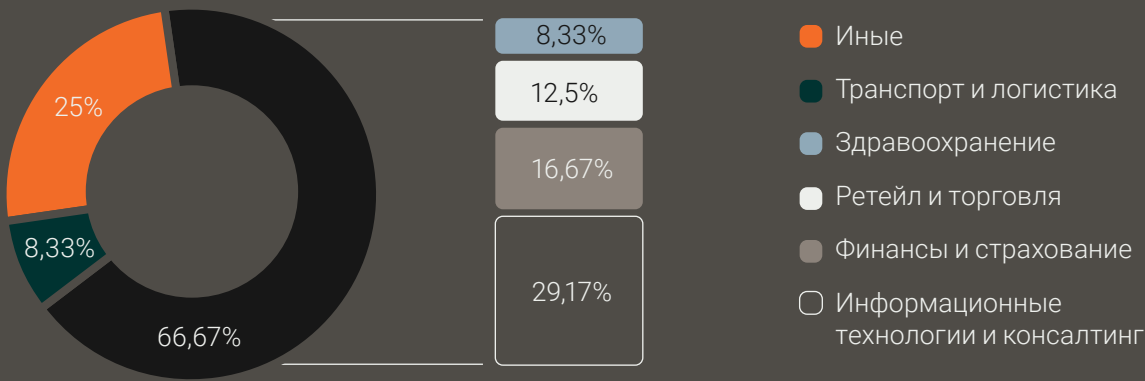


Kinsing

* – признана экстремистской организацией, её деятельность запрещена на территории РФ.

КОГО АТАКУЮТ

Диаграмма 2. Профиль инцидентов по сегментам экономики



По итогам анализа атак за первое полугодие прошлого года, мы уже могли выделить отрасль **информационных технологий** как наиболее атакуемую отрасль. К концу 2025 года такая тенденция сохранилась.

Получая доступ к таким организациям, злоумышленники фактически приобретают потенциальный доступ к десяткам других будущих целей.

Отсюда и рост тренда на получение первоначального доступа с использованием учетных записей других организаций. Для экспертов по кибербезопасности это означает, что защита подрядчиков не менее важна, чем защита собственного периметра.

Для **финансовых** и **страховых организаций** высока ценность данных и понятна монетизация. Для атакующих эта отрасль, где удачно сочетаются вымогательство, кража данных и давление на жертву через репутационные риски.

Существенная доля инцидентов также пришлась на **ритейл, здравоохранение** и **транспортно-логический сектор**, где критичными остаются доступность сервисов, устойчивость операционных процессов и скорость восстановления после инцидента.

Из графика хорошо видно: **четверть** всех инцидентов была отнесена к категории «Иные», что говорит о широкой распространенности атак по всему спектру деятельности организаций, а не только по типовой индустрии.



Мы привлекались в качестве экспертов по реагированию на инциденты и принимали участие в их расследовании — атаки затрагивают широкий перечень отраслей, включая **промышленность, образование, строительную сферу, науку и иные направления**.

Доминирование атак в отдельных отраслях не должно восприниматься остальными как исключение. У российских компаний нет особого отраслевого «иммунитета». Защищаться необходимо всем, и наши данные это подтверждают.

Отметим, что зачастую все исследовательские отчеты формируют статистику на основе ограниченного набора данных: собственные инциденты, обращения клиентов, а также события, попавшие в зону видимости компаний. Это не всегда позволяет в полной мере судить о реальном распределении атакуемых отраслей и доле каждой из них в общей структуре киберинцидентов. Тем не менее полученные нами результаты в целом коррелируют с данными, публикуемыми другими исследовательскими организациями в их годовых отчетах, что косвенно подтверждает корректность сделанных нами выводов и наблюдаемых тенденций.

Таблица 1. Перечень инструментов, выявленных по итогам расследований 2025 года

Закрепление в системе

facefish
NSSM
PUMAKIT

Повышение привилегий

DeadPotato
EfsPotato
JCTokenUtil

Обход защиты

mig-logcleaner
Antivirus Terminator
hackshell.sh
zapper

Получение учетных данных

mimikatz
handlekatz
procdump
secretsdump
Skeleton Key
SSH-IT
BetterSafetyKatz
SharpKatz
Owowa
AccountRestore

Оранжевым цветом — инструменты, которые впервые зафиксированы в 2025 году в атаках

Изучение внутренней инфраструктуры

fscan
netscan
ADRecon
BloodHound advanced
ip scanner advanced
port scanner
NBTscan
SharpHound Everything
masscan
winpcap
SharpHostInfo
SharpUserIP
OXIDScan
adexplorer
nmap

Перемещение внутри периметра

Impacket
Evil-WinRM
psexec
paexec
Netexec
PuTTY
SharpNamedPipePTH

Сбор данных

Adminer
Различные скрипты по сбору конфиденциальных данных

Управление удаленной системой

gsocket
AnyDesk
chisel

Управление удаленной системой

ngrok
Metasploit Framework
rsocx
Stowaway
MetaRAT
Cloudflared
revsocks
localtonet
CobInt
Tactical RMM
devtunnel
MeshAgent
Cobalt Strike
SocksOverRDP
Suo5
Radmin
vnt
Ak47C2
Rtlshare
DeedRAT
Velociraptor
SNAPPYBEE

Экспфильтрация данных

ffsend
Rclone
MinIO Client

Деструктивные действия

LockBit 3.0
Babuk
Warlock
X2anylock
XMRig Miner
kinsing
CrySIS/Dharma

ИНСТРУМЕНТЫ АТАКУЮЩИХ

В 2025 году набор инструментов атакующих по-прежнему выглядит как смесь редких собственных разработок с большим количеством публично доступных инструментов, которые широко распространены и давно присутствуют в арсенале злоумышленников.

Это касается как специализированных утилит для разведки и перемещения внутри инфраструктуры, так и средств удаленного доступа, туннелирования и постэксплуатации. Порой группировки прибегали к использованию легитимных системных утилит и встроенных механизмов Windows, что затрудняло обнаружение злоумышленника антивирусными программами и другими средствами защиты. При этом разнообразие инструментов можно было увидеть на этапах изучения внутренней инфраструктуры и удаленного управления системой.

Во многом это связано с привычками атакующих и необходимостью гибкого подхода: в случае разведки – для сбора информации о домене, сети и доступных сервисах, а для C2 – для организации скрытного и постоянного канала управления с системой жертвы.

В других тактиках набор применяемых средств был заметно меньше, поскольку сами техники не требовали широкого инструментария. Например, далее читатели смогут убедиться, что большая часть действий на этапе повышения привилегий была связана с существующими аккаунтами. А на этапе сбора конфиденциальных данных достаточно было использовать встроенные средства архивации и штатные утилиты.



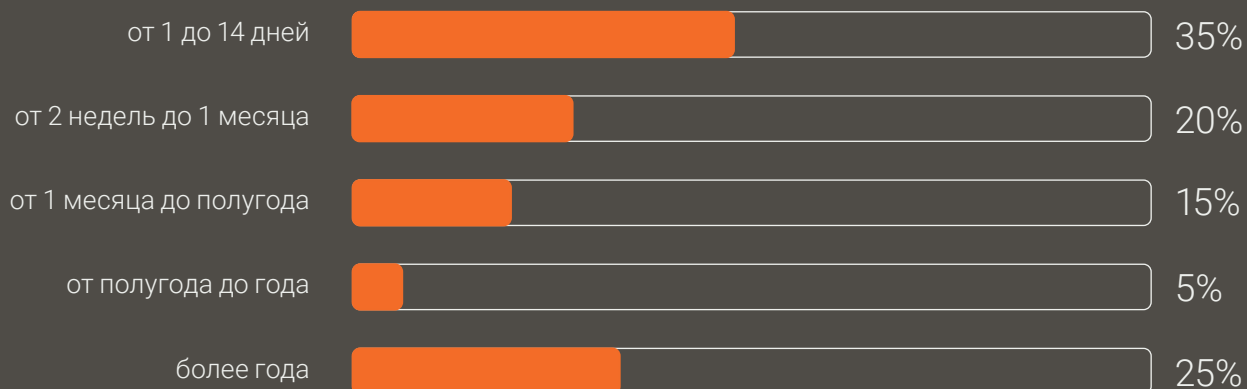
В результате инструментарий атакующих остается стабильным: хорошо зарекомендовавшие средства используются из года в год, поскольку они по-прежнему эффективно решают свои задачи. С одной стороны, это характеризует злоумышленников, которые выбирают инструмент исходя из функционала, а не критериев новизны. С другой стороны это говорит о характере жертв, которые до сих пор испытывают трудности в противодействии современному инструментарию.

В Таблице 1 мы продемонстрировали обнаруженные нами инструменты в расследованных инцидентах 2025 года, а также отметили те инструменты, которые встретились в 2025 году впервые.



ДЛИТЕЛЬНОСТЬ АТАК

Диаграмма 3. Распределение инцидентов по времени их обнаружения



На первый взгляд, данные по продолжительности инцидентов в 2025 году демонстрируют некоторую неоднородность. С одной стороны, в **большей части инцидентов** атакующих обнаруживали за срок **менее одного месяца**. С другой стороны, мы сталкивались с инцидентами, в которых группировки могли существовать в инфраструктурах компании длительный период. Доля таких атак составила **45%**.

Безусловно, существует некоторая погрешность в инцидентах из раздела «Более года», где ряд расследований выявил низкокачественные атаки, за которыми стояли различные ботнет-сети, распространяющие майнеры на уязвимых серверах. В мире сложных угроз появление таких инцидентов объясняется банальным попустительством: некоторые компании до сих пор не готовы вести полномасштабную борьбу с киберпреступностью из-за сложностей в организации комплексных мер по безопасности.

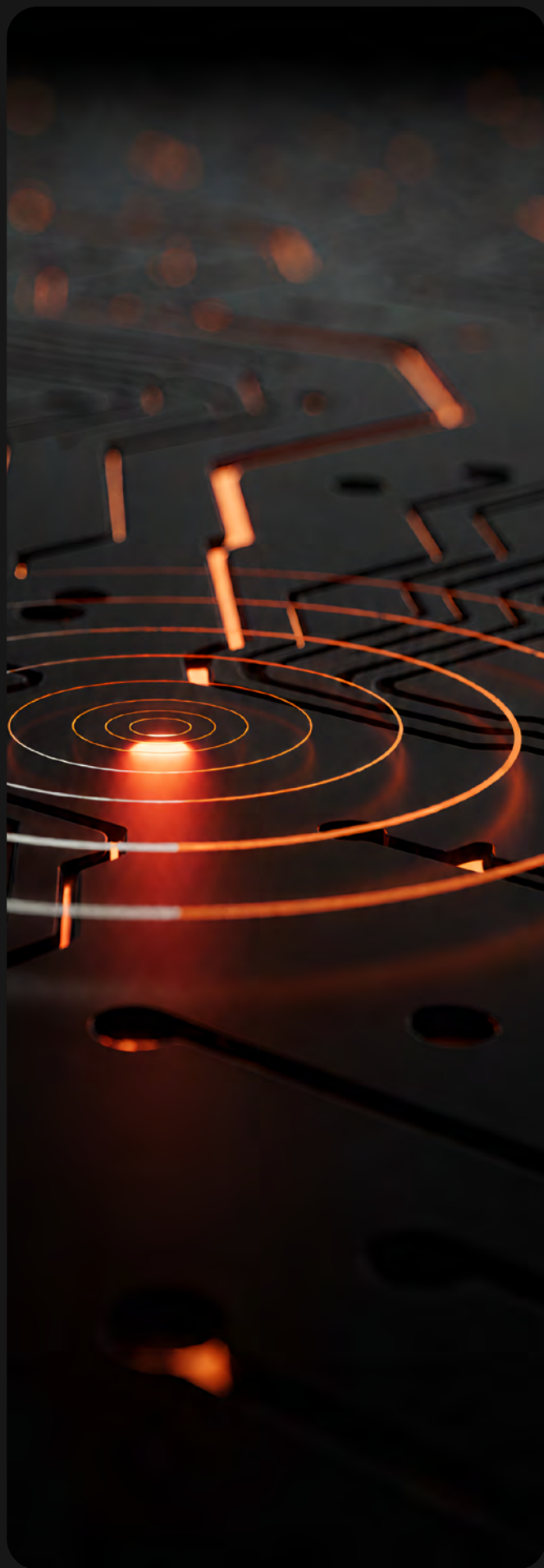


Но при этом все еще остаются компании, в которых атакующие планомерно двигаются по инфраструктуре, создают новые точки закрепления и сокращают возможности организаций оперативно полностью избавиться от злоумышленников в сети. Специализирующиеся на шпионаже группировки стремятся покрыть всю инфраструктуру компании своей тенью и буквально поглотить информационные составляющие, слиться с легитимным трафиком. Их задача — медленно похищать конфиденциальную информацию, чтобы впоследствии использовать ее в своих целях.

Опасность АРТ-группировок заключается в их чрезвычайной скрытности, сложности обнаружения и технических возможностях, борьба с которыми по силу только высококлассным специалистам.

В 2025 год медианный показатель обнаружения злоумышленников составил **17 дней**. Это еще раз показывает быстроту развития современных атак от стадии первоначального доступа и до стадии реализации конечной цели. Если инцидент не локализован защитниками в первые недели, риск перехода атаки в критическую фазу, где она получит свою монетизацию, существенно возрастает.

В атаках с использованием программ-вымогателей со стороны финансово мотивированных группировок медианный показатель обнаружения составляет всего **7 дней**. Зачастую компании обнаруживали сам факт атаки уже на ее конечной стадии. Очевидно, что использующие вымогателей злоумышленники демонстрируют лучшую подготовку в сравнении с хактивистами за счет большего опыта и наличия инцидентов.



Поэтому и противодействие таким атакам должно осуществляться с большей самоотдачей и вовлеченностью специалистов на этапах предотвращения угроз, мониторинга и реагирования.

Возвращаясь к тезису неоднородности, стоит отметить, что она фактически отсутствует при описании длительности атак. Структура распределения атак по времени указывает лишь на различие в мотивации и модели поведения злоумышленников.

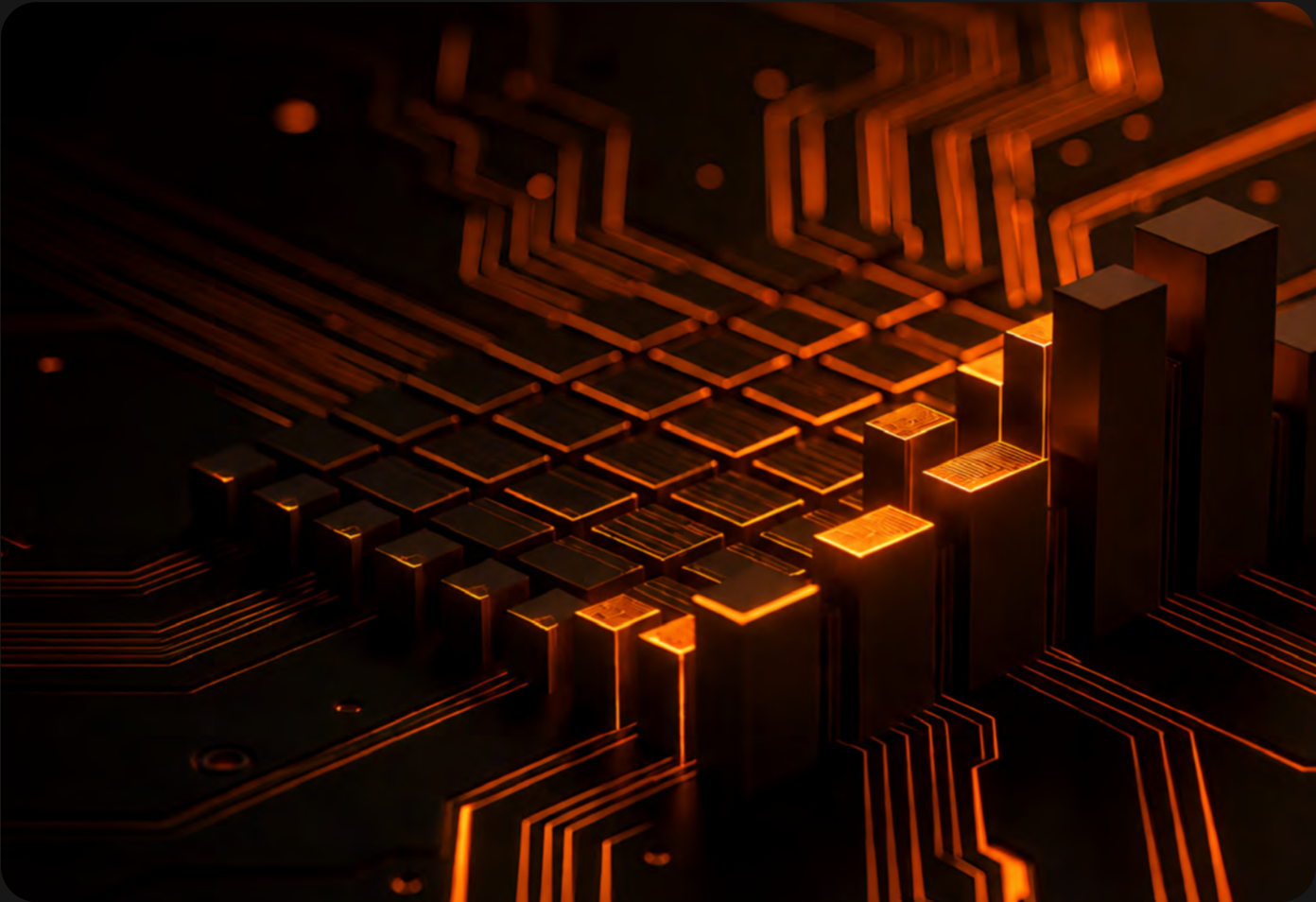
Краткие инциденты чаще будут связаны с кампаниями, в ходе которых требуется получение быстрого результата — кража доступов, шифрование данных и другие примеры оперативной монетизации. Длительные инциденты больше относятся к сценариям, в которых злоумышленникам выгодно оставаться в ИТ-инфраструктурах максимально долго. В результате каждый из столбцов в диаграмме соотносится с конкретным интересом атакующих.

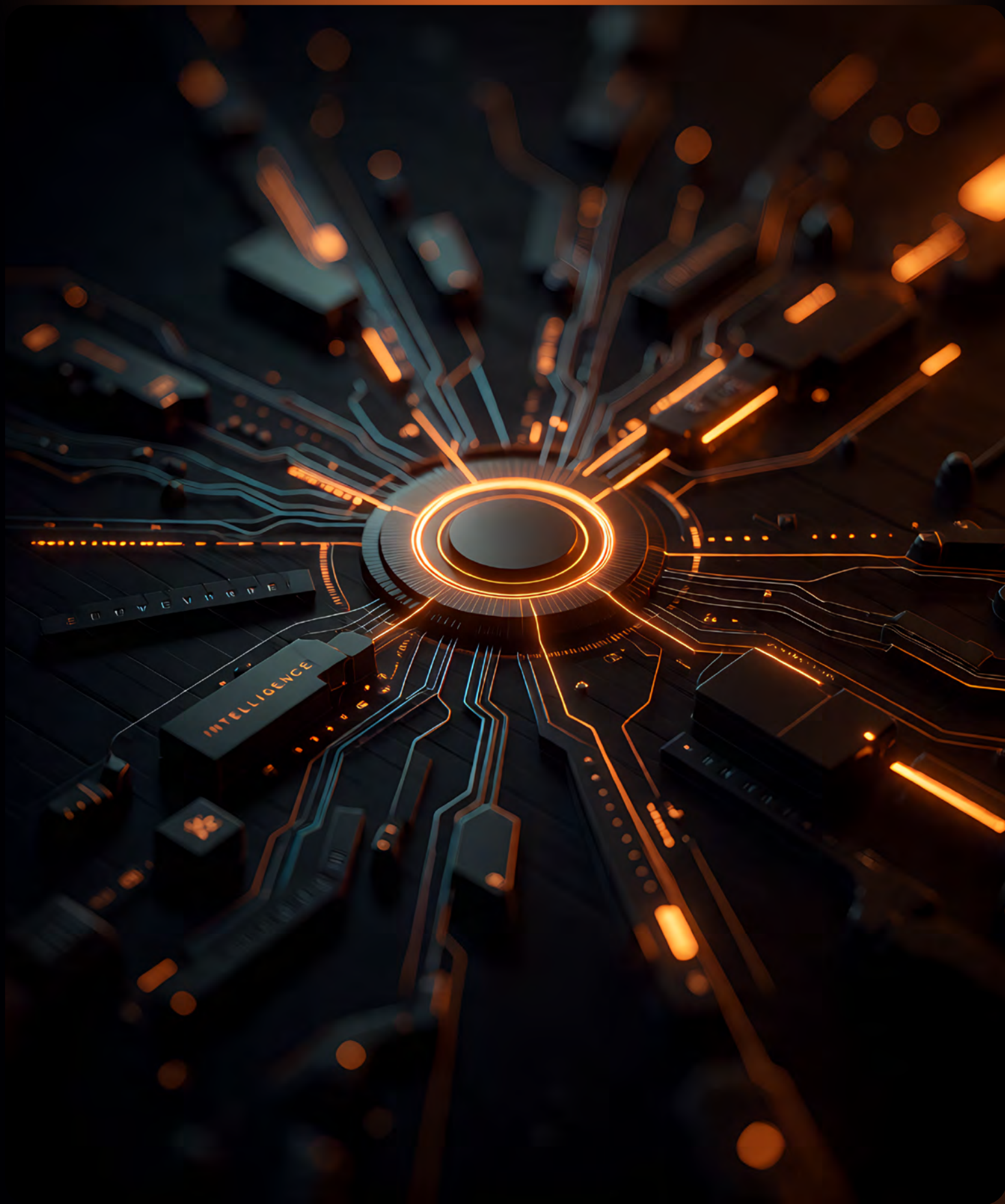
17 ДНЕЙ

медианный показатель
обнаружения злоумышленников
в 2025 году

7 ДНЕЙ

медианный показатель
обнаружения злоумышленников
в атаках с использованием
программ-вымогателей со стороны
финансово мотивированных
группировок





На начальных этапах злоумышленники готовятся к проведению полноценной кибератаки на компанию-жертву. Атакующим требуется собрать все необходимое – импланты, инструменты, инфраструктуру и т.д. – для последующего применения. Первоначально злоумышленникам необходимо получить представление о компании-жертве: инфраструктуре, сотрудниках и другую сопутствующую информацию, способную помочь атакующим для достижения их цели.

Чаще всего злоумышленники анализируют внешний периметр компании с помощью незамысловатых публично доступных инструментов и сервисов, таких как Shodan и Censys. Именно поэтому важно постоянно отслеживать, какие данные о компании присутствуют в открытых источниках, фигурируют в утечках или на теневых ресурсах. Необходимо заблаговременно оценивать, какую ценность эта информация может представлять для потенциального атакующего.

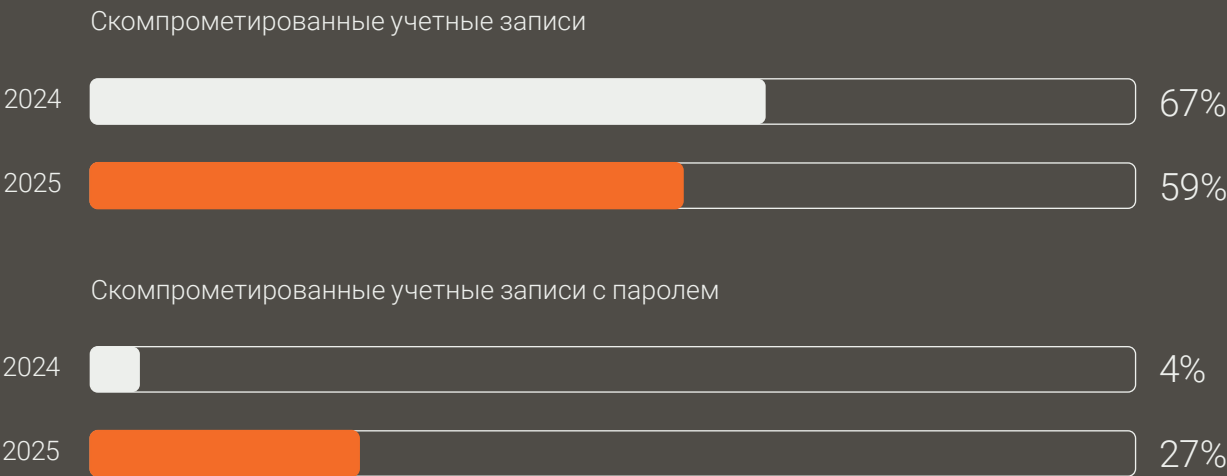
Так, в процессе анализа внешнего периметра заказчиков с целью оценки потенциальных векторов атак было выявлено:

у **54%** компаний найдены сервисы с устаревшими версиями программного обеспечения, содержащими потенциальные уязвимости

в **51%** случаев выявлены корпоративные веб-ресурсы с небезопасным соединением, а также страницы, предназначенные для внутреннего использования

в **51%** случаев обнаружены упоминания компаний в тех или иных мошеннических схемах на форумах в даркнете и в закрытых Telegram-группах

Диаграмма 4. Доля исследуемых компаний со скомпрометированными учетными записями



В 2025 году наблюдается снижение случаев использования корпоративных учетных данных при регистрации на сторонних ресурсах. У 59% компаний были случаи компрометации корпоративных учетных записей, что на 8% меньше, чем в предыдущем году. В 27% случаев вместе с логином был скомпрометирован пароль, что на 23% больше, чем в 2024 году.

Несмотря на снижение случаев использования корпоративных данных на сторонних сервисах, сами инциденты для злоумышленников стали более результативными, поскольку смещен акцент с количества на «качество» атак.

Регистрации сотрудников на сторонних ресурсах с использованием корпоративной почты создают потенциальные точки входа для злоумышленников: такие сайты часто недостаточно защищены, а работники могут использовать корпоративные пароли при регистрации на них.



Таким образом, злоумышленники могут использовать скомпрометированные логины и пароли при авторизации на корпоративных сервисах и легально зайти в инфраструктуру организации.

В 2025 году более половины наших заказчиков упоминались на теневых ресурсах, что на 14% больше, чем годом ранее. Наибольшее число упоминаний (68%) связано с мошенническими схемами. Злоумышленники предлагают услуги «отмыва» и обналичивания денежных средств, а также продают и покупают большие объемы SIM-карт и личных кабинетов банков, зарегистрированных на граждан Российской Федерации и стран СНГ. Доля упоминаний, связанных с поиском инсайдеров, снизилась до 15% против 67% годом ранее. Упоминания, относящиеся к покупке или продаже баз данных компаний, составляют 17% от общего числа упоминаний, что на 16% меньше, чем в 2024 году. Во многом это связано с изменениями в законодательстве, принятыми в ноябре 2024 года и ужесточающими административную и уголовную ответственность за утечки данных.

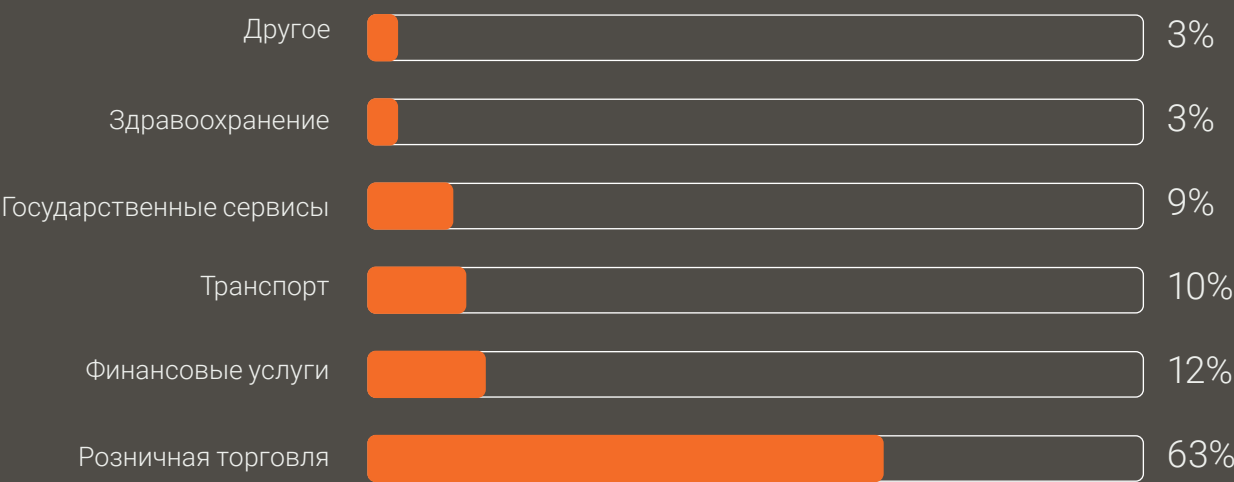
По итогам 2025 года можно отметить снижение доли компаний, имеющих сервисы с потенциальными уязвимостями и корпоративные веб-ресурсы с незащищенными соединениями, предназначенными для внутреннего пользования. По сравнению с 2024 годом их доля снизилась на 11% и 12% соответственно.

Снижение количества потенциально уязвимых ресурсов отражает тренд на глобальное повышение уровня защищенности.



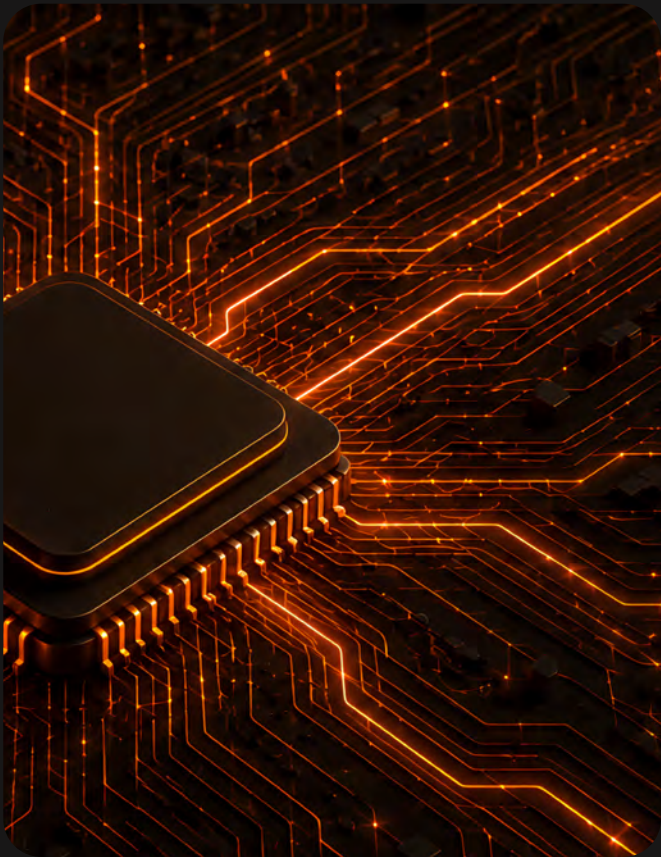
ПРИМЕР ИЗ ПРАКТИКИ

Диаграмма 5. Использование корпоративных данных для регистрации аккаунтов относительно отрасли



Наибольшее количество случаев использования корпоративных данных было зафиксировано при регистрации в сервисах розничной торговли — 63%, что на 18% больше по сравнению с 2024 го-дом. По-прежнему в число основных сфер утечек входят финансовые услуги, их доля снизилась до 12% против 29% годом ранее. На третьем месте — сфера транспортных услуг с долей в 10%. Ранее популярная образовательная сфера вышла из пятерки лидеров.

В рамках анализа сетевой инфраструктуры заказчиков были обнаружены доступные извне страницы авторизации на таких сервисах, как Zabbix, GitLab, Grafana, Kubernetes, а также доступы в административную панель управления маршрутизаторов. Доступность таких ресурсов увеличивает поверхность атаки и риск компрометации инфраструктуры.



КАК ПОСМОТРЕТЬ НА СЕБЯ ГЛАЗАМИ ХАКЕРА И НАЙТИ НЕУЧТЕННЫЕ АКТИВЫ

В идеале для отслеживания активов, в том числе на внешнем периметре, следует использовать выделенную базу данных управления конфигурацией (от англ. Configuration Management Database, CMDB) с выстроенным и регулярно поддерживаемым процессом наполнения. Однако даже при наличии такой системы полезно периодически задавать себе более практичный вопрос: «Что именно видно о нас снаружи прямо сейчас?». И рассматривать его не в теории и не по внутренней документации, а на практике, как это видит реальный интернет-пользователь или... злоумышленник. Такой взгляд извне выявляет забытые поддомены, устаревшие сервисы, открытые порты и другие активы, которые давно выпали из поля зрения, но по-прежнему доступны и потенциально уязвимы.

Для поиска такого рода уязвимостей злоумышленники используют сервисы Shodan, Censys, FOFA, Zoomeye, Securitytrails или Leakix.

Эти системы отличаются синтаксисом, однако позволяют осуществлять поиск по двум основным вариантам: через доступные извне активы либо по конкретным запросам:

01 По доменным зонам и поддоменам организации, по отдельным именам хостов с брендом/сокращением названия компании, а также по обратным записям (PTR), если они «говорящие».

02 По сертификатам TLS или организационному полю в них (если используется), по отпечатку конкретного корпоративного wildcard-сертификата, по Common Name / SAN. Сертификаты часто помогают «сшить» вместе разрозненные IP и домены.

03

По подсетям и ASN (если у вас есть собственные диапазоны / провайдерские блоки).

04

По технологиям, сервисам или службам. Можно делать как прямой поиск по продукту: «Jira» «Microsoft SQL Server» (в том числе их упоминания могут быть в поле title, а также иметь специфичные header или banner), конкретным службам (например, ldap, bitrix, rfc1, itlk) или портам:

- 80/443 (HTTP/HTTPS) 8080
- 22 (SSH), 2222, 22222
- 445
- 3389 (RDP)
- 3306/5432/1433/1521/27017 (БД: MySQL/Postgres/MSSQL/Oracle/MongoDB)
- 6379/11211/9200/5601 (Redis/Memcached/Elasticsearch/Kibana)
- 5900 (VNC)
- 8530, 8531 (WSUS)

Если говорить о конкретных уязвимостях, то в базовом сценарии можно опираться на поиск по известным CVE. Однако для более детального и целенаправленного поиска по конкретным CVE, как правило, потребуется платная подписка.

Аудит важно проводить на регулярной основе, причем с разной периодичностью в зависимости от критичности: ключевые домены и публичные IP-адреса стоит проверять чаще, остальные активы — по заранее установленному расписанию.

Особого внимания при этом заслуживают несколько категорий.

Во-первых, неизвестные активы — те, у которых нет явного владельца, или те, что в принципе не должны быть публично доступны. Во-вторых, административные интерфейсы и панели управления, доступ к которым изначально должен быть ограничен защищенными каналами, а также давно забытые тестовые стенды, оставшиеся открытыми. В-третьих, серверы с уязвимостями высокого и критического уровня, как правило, это уязвимости с оценкой CVSS 8.0 и выше, требующие приоритетной обработки.

Выстроить и автоматизировать этот процесс помогают решения класса EASM (External Attack Surface Management, процесс непрерывного обнаружения, инвентаризации, классификации и мониторинга внешних ИТ-активов организации, которые могут быть потенциально уязвимы для атак) и VOC (Vulnerability Operations Center, Центр управления уязвимостями), которые обеспечивают непрерывный мониторинг внешнего периметра и позволяют оперативно реагировать на появление новых или изменение существующих активов.

Второй способен выполнять следующее:

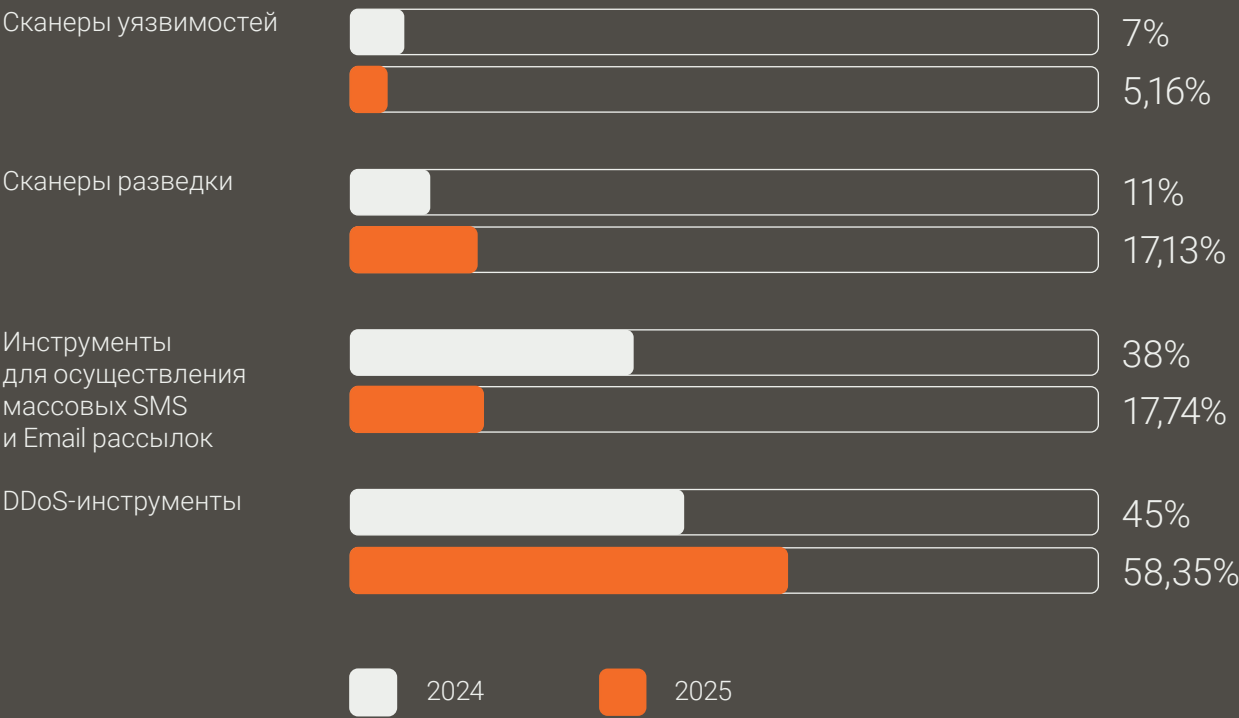
- инвентаризация и выявление неучтенных активов (CMDB), включая поиск теневых активов;
- выявление уязвимостей методами «белого» и «черного ящика»;
- категоризация и приоритизация уязвимостей с учетом мировых трендов о реально эксплуатируемых злоумышленниками дырах в безопасности;
- предоставление кратких, понятных и легко применимых на практике отчетов по сканированию; аналитика и динамика устранения уязвимостей;
- консультации по харденингу операционных систем и контейнеров (Docker) в случае невозможности применения обновлений;
- использование плейбуков для проверки текущего состояния харденинга относительно стандартов CIS Benchmark и приведения его к этим стандартам.



ПОДГОТОВКА РЕСУРСОВ



Диаграмма 6. Типы инструментов, выявленные в открытых источниках



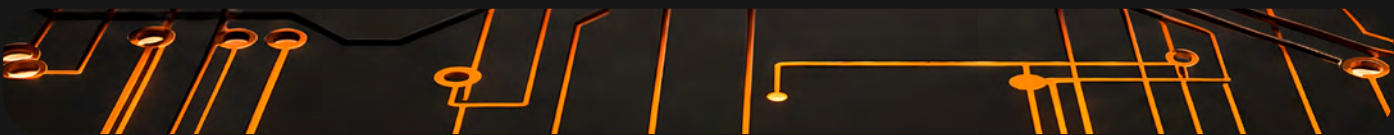
На этапе подготовки к атакам злоумышленники могут использовать репозитории из открытых источников, взяв их за основу для дальнейшей доработки или используя непосредственно в процессе атаки.

Порядка 7% от общего числа репозиториев, проанализированных аналитиками за последний год и включающих упоминания конкретных компаний, содержат инструменты, которые могут использоваться злоумышленниками для разведки и проведения атак. На одну компанию приходится 4 уникальных репозитория с таким функционалом. Самыми распространенными по-прежнему остаются инструменты для проведения DDoS-атак — 56%, что на 11% больше, чем в 2024 году.

Доля инструментов для осуществления массовых СМС-рассылок составила лишь 15%, что на 23% меньше, чем в предыдущем году.

Инструменты для мониторинга и агрегации утечек учетных данных найдены в 7% репозиториев, сканеры для разведки и поиска уязвимостей составили 14% и 3% соответственно.

Больше всего инструментов в репозиториях приходится на компании финансовой (53%) и ИТ (21%) отраслей. 11% инструментов приходится на компании государственного сектора. Еще 11% пришлось на компании промышленной сферы и 5% — на транспортную сферу (Диаграмма 7).



В 2024-2025 годы этап «Подготовки ресурсов» претерпел значительные изменения. В арсенал злоумышленников массово вошли генеративные нейросети (большие языковые модели от англ. Large Language Model, LLM) для создания вредоносного программного обеспечения, фишинговых сообщений и прочих инструментов.

Нейросети уже повседневно применяются для генерации фишинговой нагрузки, подделки голосовых и видео сообщений. Теперь в ходе расследования компьютерных инцидентов мы часто сталкиваемся с [vibeware](#) — ВПО, для создания которого использовались нейросети.

Совершенно органичен следующий шаг злоумышленников. Появилось ВПО, которое генерирует нагрузки при помощи нейросетей ([PromptLock](#), [PromptFlux](#) и [PromptSteal](#)) и само модифицирует свой код в зависимости от выявленных средств защиты ([LAMEHUG](#)).

Большие языковые модели уменьшили разрыв между «скрипт-кидди» и профессиональными разработчиками вредоносного ПО. Доступность инструментов позволяет злоумышленникам автоматизировать создание уникальных образцов ВПО почти в промышленных масштабах. И основная проблема заключается не в «гениальности» кода, написанного при помощи нейросети, а в его большой изменчивости.

Это позволяет существенно экономить время на разработку ВПО, которое не будет выявляться традиционными средствами защиты. Там, где аналитику требуется несколько часов на декомпиляцию и написание сигнатуры, нейросеть за секунды генерирует десятки вариаций с теми же функциональными возможностями, меняя используемый язык программирования, структуру кода, логику работы с API и методы обфускации.

ПРИМЕР ИЗ ПРАКТИКИ

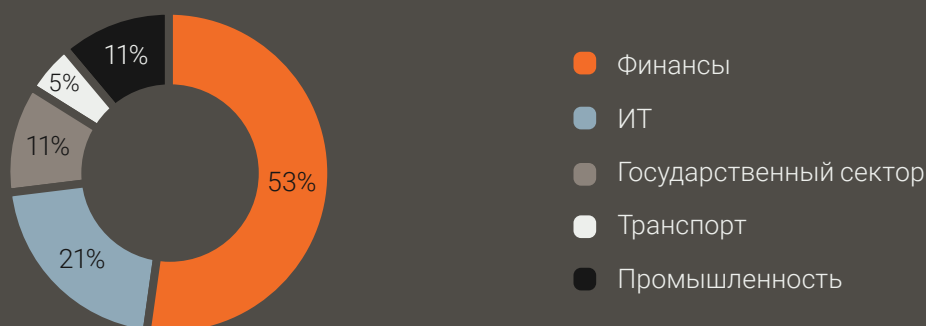
В 2025 году мы столкнулись с деятельностью группировки [4BID](#) (Forbidden Hyena). В ходе исследования инструментов группировки были выявлены странности, которые натолкнули на мысль об использовании нейросетей для генерации кода. Странная логика исполнения, наличие комментариев для очевидных вещей — это признаки, которые выдают факт использования «vibeware». Наши догадки разделили коллеги из [BI.ZONE](#), а потом подтвердили и сами злоумышленники в своем Telegram-канале.

Нового там реально ничего нет (кроме, разве что, самого RATника - и то с натяжкой). Я до сих пор не понял, зачем обфусцировать "рутинные скрипты на PowerShell"? Чтобы красиво выглядело в отчёте? Мы их пишем для скорости и результата, а не для того, чтобы потом в реверсе мучились. AI для генерации boilerplate-кода - это обычная автоматизация рутины.

Рис. 1 Скриншот из Телеграмм-канала злоумышленников



Диаграмма 7. Упоминания компаний в репозиториях, представляющих угрозу



КАК ПОДГОТОВИТЬСЯ К АТАКАМ

В условиях, когда «время жизни» статической сигнатуры существенно сокращается, фокус внимания защиты должен сместиться со статического анализа файлов **на поведенческий анализ (решения класса EDR/XDR)** и отслеживание аномалий в телеметрии: злоумышленникам в любом случае потребуется инфраструктура для рассылки фишинговых писем, размещения своих инструментов и взаимодействия с имплантами.

Стоит отслеживать домены, зарегистрированные недавно или использующие тайпсквоттинг. Через сканеры (Shodan/Censys) можно выявлять IP-адреса, которые имеют известный JARM-отпечаток или другие признаки уже известных угроз. Все выявленные подозрительные ресурсы можно превентивно заблокировать или заранее поставить на мониторинг в SOC. Сбор информации о таких ресурсах можно осуществлять самостоятельно или через TI подписку (от англ. Threat intelligence — сбор, анализ и распространение информации об угрозах безопасности) от MSSP-провайдера. Например, использовать платформу [Angara ECHO](#).

Помимо вышеописанного, есть ряд дополнительных действий, которые помогают заранее усложнить работу злоумышленнику и сократить последствия атаки. Ниже приведен перечень таких мер, на которые стоит обратить внимание.

- Внедрите средства противодействия DDoS-атакам;
- отслеживайте количество попыток входа и ограничивайте их для клиентов и сотрудников;
- внедрите CAPTCHA для обнаружения и противодействия работе ботов;
- внедрите процесс обучения сотрудников по основам информационной безопасности;
- организуйте процесс оповещения сотрудников о последних инцидентах ИБ.



Angara ECHO

Платформа для управления цифровым следом

ПОЛУЧЕНИЕ ПЕРВОНАЧАЛЬНОГО ДОСТУПА

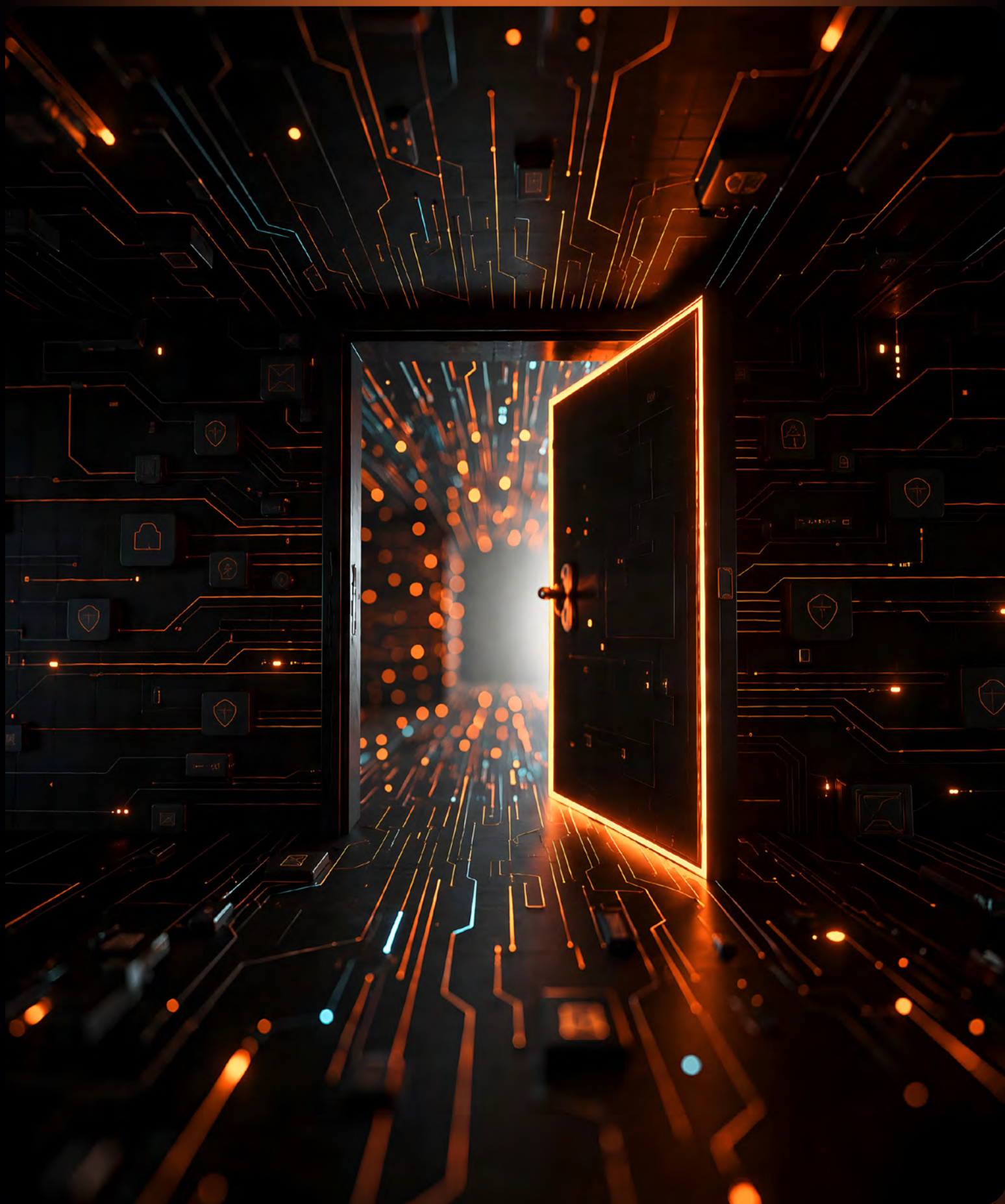
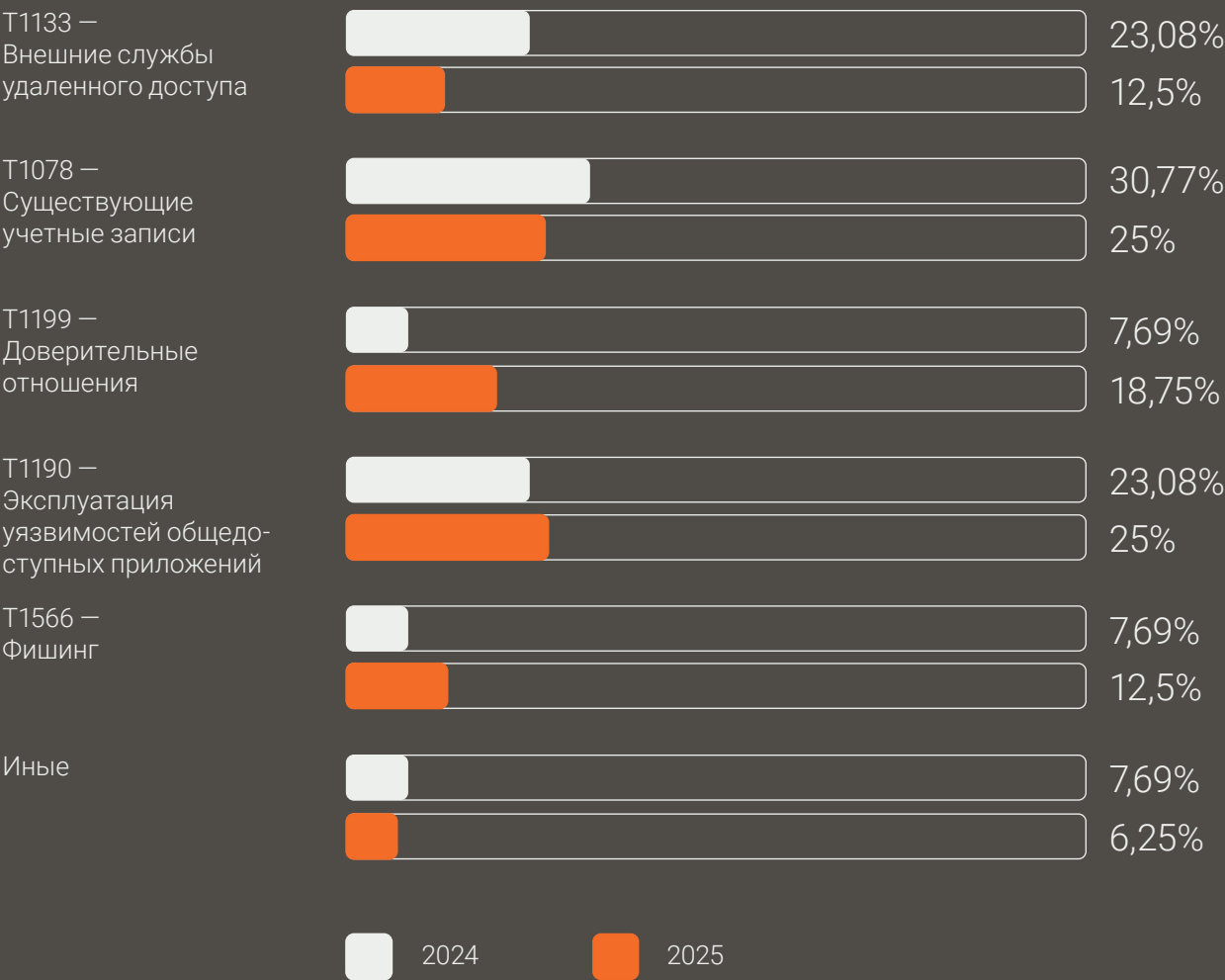


Диаграмма 8. Распределение выявленных техник в рамках тактики первоначального доступа



По итогам 2025 года тройка наиболее распространенных техник получения первичного доступа практически не изменилась по сравнению с прошлым годом: **фишинг, эксплуатация публично доступных приложений и компрометация доверительных отношений**.

Фишинг по-прежнему остается самым «рентабельным» способом входа и используется как для доставки вредоносного кода под видом рабочих документов, так и для перехвата учетных данных через имитацию корпоративных порталов и почты.

Интересно, что мы наблюдаем большой поток фишинговых писем с рассылкой в массовом режиме именно в рамках оперативного мониторинга, и, соответственно, в таких случаях атака не продолжает свое развитие. Тем не менее, злоумышленники до сих пор предпочитают фишинг из-за его стабильной эффективности и низкой стоимости.

Эксплуатация внешних сервисов пребывает в лидерах по той же причине, что и годом ранее: на периметре продолжают жить устаревшие версии ПО, ошибки конфигурации и отложенный патчинг.

Причем атаки все чаще опираются не только на известные критические уязвимости, но и на злоупотребления легитимными функциями приложений и ошибки в бизнес-логике. Критические уязвимости тоже не заставляют себя долго ждать: мы наблюдаем их активную эксплуатацию буквально на следующий день, при этом злоумышленник не затягивает и доходит до стадии воздействия в среднем в течение недели.

В наших расследованиях мы сталкивались с эксплуатацией следующих уязвимостей:

- CVE-2021-34473 (Microsoft Exchange Server),
- CVE-2020-1472 (ZeroLogon) (Windows Netlogon),
- CVE-2025-49704 (Microsoft Office SharePoint),
- CVE-2025-49706 (Microsoft Office SharePoint),
- CVE-2025-53770 (Microsoft Office SharePoint),
- CVE-2025-53771 (Microsoft Office SharePoint),
- CVE-2025-59287 (Windows Server Update Services - WSUS),
- CVE 2021-22204 (ExifTool),
- CVE 2021-22205 (GitLab),
- BDU:2025-10114 (TrueConf Server),
- BDU:2025-10115 (TrueConf Server),
- BDU:2025-10116 (TrueConf Server).

Наиболее примечательное изменение — **рост доли компрометации доверительных отношений**: по нашему опыту, эта техника уже обгоняет знаменитый «RDP наружу» как источник первичного доступа. На этом шаге можно сделать два вывода:

01

Общий сдвиг к более масштабируемым моделям: взлом одной компании-подрядчика способен открыть злоумышленникам дорогу сразу в десятки других организаций, если подрядчик обслуживает инфраструктуры клиентов, имеет административные доступы или эксплуатирует интеграции для поддержки и управления. Малые ИТ-компании нередко пренебрегают базовой гигиеной ИБ — многофакторной аутентификацией, сегментацией, контролем привилегий и мониторингом — и потому становятся удобной точкой входа. Дополнительный фактор риска возникает из-за открытых источников — список клиентов подрядчика

зачастую несложно восстановить по сайту и маркетинговым материалам (кейсы, логотипы, рекомендации), что помогает злоумышленнику заранее выстроить карту целей и приоритизировать атаки.

02

Небольшие компании часто оказываются не готовы к инцидентам организационно: у них нет отлаженных процессов обнаружения и реагирования, заранее определенных ролей и регламентов, понимания, что делать в случае инцидента и кто может помочь. В результате компрометация может оставаться незамеченной дольше, а действия жертвы в первые часы носят хаотичный характер, что повышает ущерб и облегчает злоумышленникам повторный доступ. Именно поэтому мы выделили отдельное решение — базовый мониторинг **Angara ETDR**: он закрывает минимально необходимый уровень видимости и раннего обнаружения для небольших ИТ-команд и дает понятный «первый контур» реакции без внедрения тяжелых процессов.

Отдельно подчеркнем, что техника **использования валидных учетных данных** остается в непосредственной близости к топу. Это логично: такой вход снижает заметность инцидента и позволяет обходиться без шумной эксплуатации уязвимостей, особенно, если скомпрометированная учетная запись уже обладает расширенными правами или доступом к удаленным сервисам и облачным ресурсам. Основных источников таких учетных данных — два. Во-первых, компрометация через инфостилеры: заражаются рабочие и домашние устройства сотрудников, при этом вторую группу контролировать куда сложнее. Во-вторых, банальное хранение секретов в открытом виде — в обычных текстовых файлах, файлах конфигураций, скриптах, документации, общих папках и репозиториях. В этом случае нахождение одного «невинного» артефакта (бэкапа, архива, каталога с логами или настроек) приводит к тому, что злоумышленник получает готовые действующие доступы и использует их как первичный вход без необходимости разворачивать сложную атаку.

ПРИМЕР ИЗ ПРАКТИКИ

В ноябре 2025 года нашей командой проводилось расследование атаки группировки [Warlock Group](#) на компанию в области электроэнергетики и промышленности.

Первоначальное проникновение во внутренний периметр организации стало возможным благодаря оперативной реакции злоумышленников на появление публичной информации об уязвимости. В октябре 2025 года была опубликована информация и PoC-эксплоит для критической уязвимости в службе обновлений Windows Server (WSUS) **CVE-2025-59287**, которая позволяет выполнить удаленный код на сервере. Буквально через несколько часов после публикации началось массовое сканирование интернет-пространства для выявления уязвимых хостов. Группировка **Warlock** использовала этот вектор как основной, отправив на обнаруженный WSUS-сервер жертвы специально сформированный SOAP-запрос. Он содержал вредоносную нагрузку, скомпилированную с использованием известного инструментария (YSoNet), которая при десериализации приводила к выполнению кода на сервере в контексте пула приложений IIS (процесс w3wp.exe).

Перед непосредственным проникновением атакующие проводили разведку: на первом этапе они отправляли тестовую библиотеку, чтобы подтвердить наличие уязвимости. Успешность проверки определялась по появлению специфического HTTP-заголовка **PaloAltoNetwork-AST: vulnerable** в ответе сервера. После злоумышленники доставляли основную нагрузку, завернутую в XML-структуру SOAP-запроса. Наблюдаемая полезная нагрузка использовалась для установки Velociraptor из msi-пакета. Обычно данный инструмент используется командами по реагированию на инциденты для сбора криминалистически значимых данных, но злоумышленники используют его для управления скомпрометированной системой.

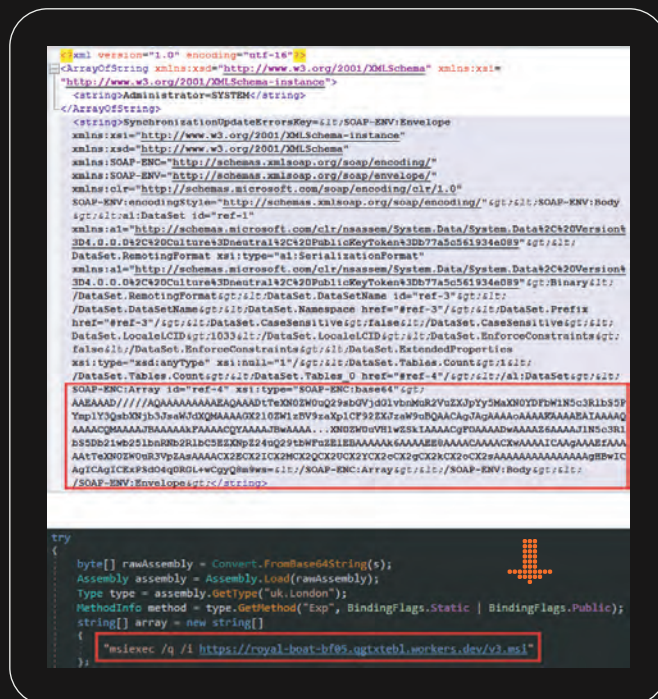


Рис. 2. Полезная нагрузка для установки Velociraptor в качестве инструмента управления скомпрометированной системой

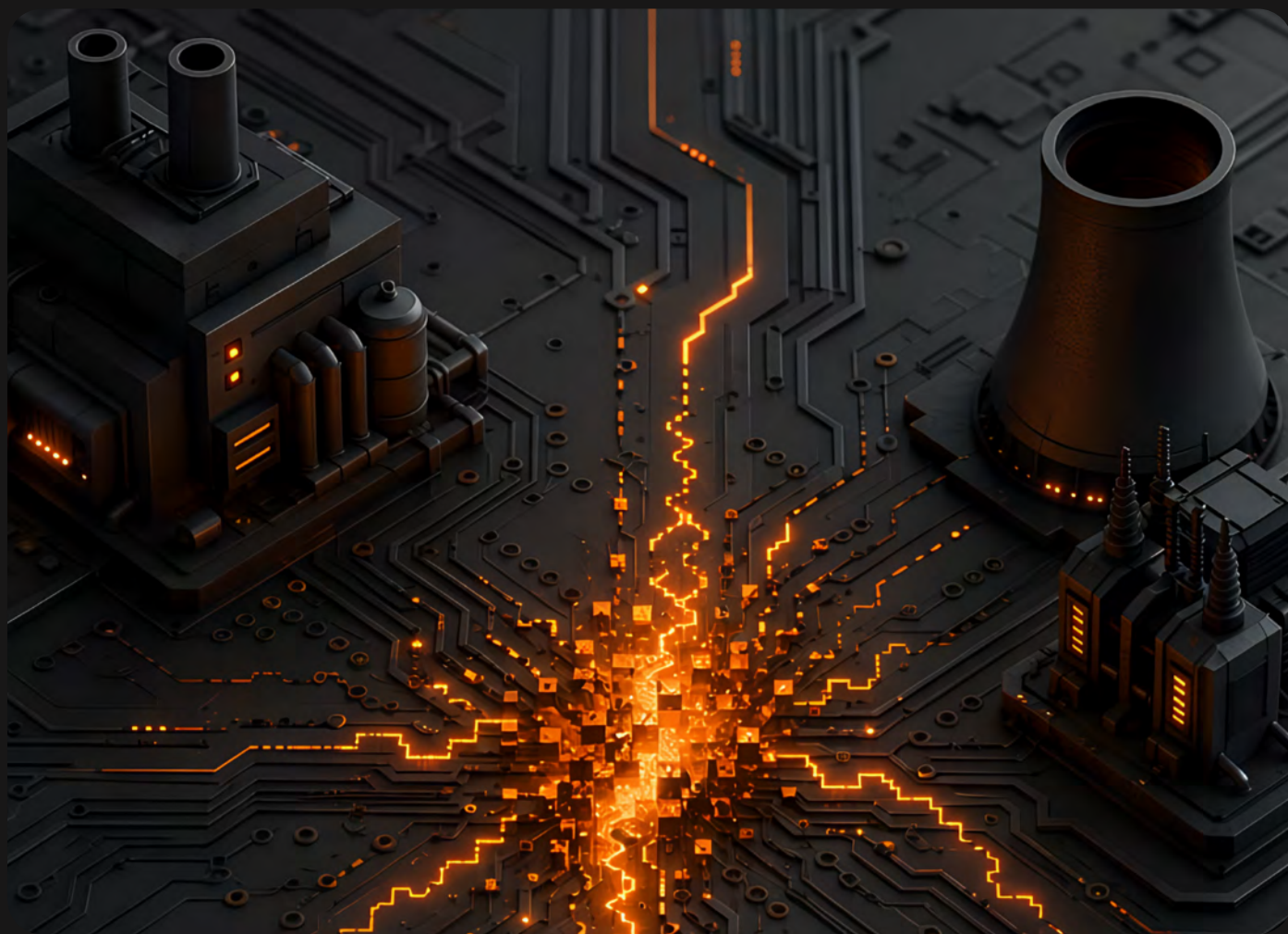


Анализ журналов и базы данных WSUS показал характерные ошибки, связанные с передачей данных для десериализации через класс .NET BinaryFormatter, что является ключевым индикатором попытки эксплуатации данной уязвимости. Критически важным является то, что атака не оставляла значимых следов в стандартных журналах событий Windows.

Сразу после успешной эксплуатации уязвимости и получения доступа к серверу злоумышленники инициировали цепочку действий по закреплению и развитию атаки. Для этого они использовали многоступенчатую обфускацию выполнения команд. В результате выполнения закодированных PowerShell-команд на сервер загружался и запускался агент для фреймворка управления Mythic (агент Apollo), а также троян удаленного доступа (WarlockRAT).

Кульминацией атаки, спустя всего два дня после первоначального проникновения, стал запуск программы-вымогателя Warlock Cryptor. Вымогатель зашифровал критически важные данные на серверах, что привело к остановке основных бизнес-процессов организации и потребовало полного восстановления систем из резервных копий.

Данный инцидент наглядно демонстрирует тренд на сверхскоростную эксплуатацию свежих уязвимостей (временной промежуток между публикацией PoC и началом атаки сократился до нескольких часов). Обнаружение подобных действий крайне затруднено без проактивного сбора и корреляции событий. Для своевременного выявления этого вектора атаки критически важно настроить мониторинг процессов, особенно цепочек запуска от серверных приложений (WSUS, IIS), и внедрить правила корреляции в систему централизованного сбора и анализа логов (SIEM).



АНАЛИЗ ФИШИНГОВЫХ АТАК В РЕТРОСПЕКТИВЕ

Этот чек-лист может использоваться как для перепроверки потенциально скомпрометированного хоста, так и в рамках проактивного поиска угроз (threat hunting).

Так, нам необходимо подтвердить гипотезу, было ли письмо доставлено пользователю, открывалось ли оно и вложения, выполнялись ли переходы по ссылкам. Работать лучше всего по принципу: сначала искать **серверные подтверждения**, затем **хостовые артефакты и сетевые следы**.

01 Зафиксировать индикаторы письма

Перед поиском собрать все известные признаки письма:

- From, Return-Path, Reply-To; тема письма и возможные варианты темы;
- Message-ID, если доступен; имена вложений, размер, хеш-сумма; URL, домены, IP-адреса;
- предполагаемые получатели или рассылочные группы.

Если письмо уже найдено, сохранить его в .eml или .msg вместе с полными заголовками. Это основной источник для дальнейшей корреляции в логах.



Если конкретных параметров письма нет, можно осуществить поиск потенциальных кандидатов через Exchange Management Shell / PowerShell и/или прямым разбором логов на сервере, используя в качестве источника Message Tracking Logs (о нем расскажем ниже). Параметрами для поиска и проверки в таком случае могут выступать:

тема содержит акт|счет|сверка|договор|проверка;
есть вложение ip|rar|7z|doc|docm|xls|xlsx|pdf|one|lnk.

02 Подтвердить факт доставки письма

Основной вопрос: попало ли письмо в почтовый ящик пользователя или было задержано/отклонено на промежуточном узле. Проверить:

- **Exchange Message Tracking Logs** — основной источник для on-prem Exchange: C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\MessageTracking\;
- **почтовый шлюз / антиспам** — факт приема, маршрутизации, карантина, доставки или блокировки; иногда полезно покопаться в заблокированной корреспонденции. Так вы поймете, кто уже сейчас нацелен на вашу инфраструктуру;
- **IIS-логи OWA/ECP** — как дополнительный источник для web-доступа;
- при необходимости — наличие письма в OST/PST, а также в папках: Inbox, Junk Email, Deleted Items, Recoverable Items.

Факт доставки обычно подтверждается сочетанием:

- записи о доставке в транспортных логах;
- наличия письма в ящике, локальном кэше Outlook или в восстановимых элементах.

03 Подтвердить факт открытия или доступа к письму

Прямой признак лучше всего искать на стороне почтовой системы.

Проверить:

- **Exchange Online / Microsoft 365:** событие MailItemsAccessed и другие операции доступа к письму, если аудит и лицензия это позволяют;
- **OWA / webmail:** IIS-логи OWA, прокси/SWG, браузерная история и кэш;
- **Outlook на хосте:** признаки чтения письма в OST/PST, например, изменение статуса Read/Unread.

Косвенные признаки открытия:

- после доставки письма был доступ к веб-интерфейсу почты;
- загружался внешний контент из письма, например, удаленное изображение;
- в прокси, DNS или EDR есть обращения к доменам, встроенным в письмо.

04 Проверить открытие вложений и переходы по ссылкам

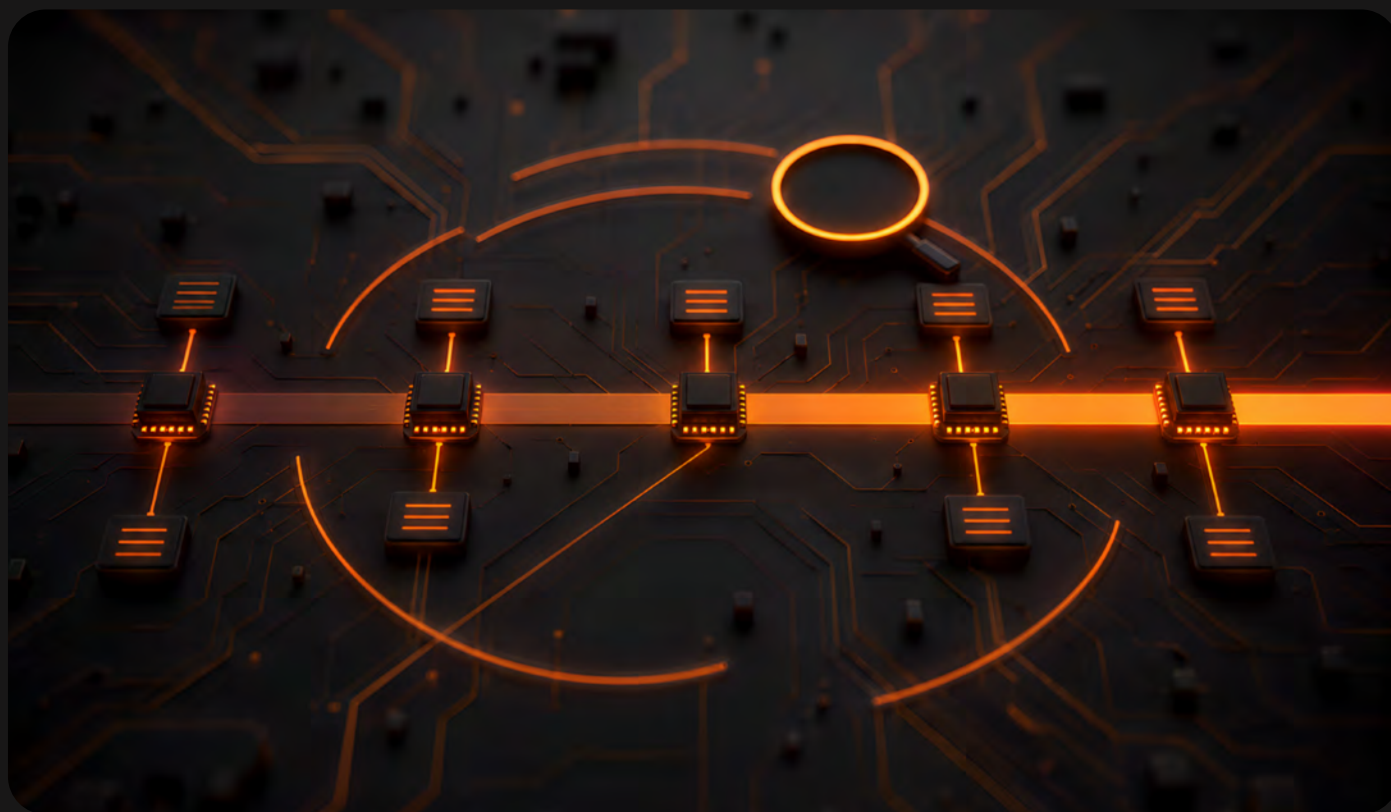
Это самая надежная часть ретроспективного анализа: факт взаимодействия с вложением или URL обычно виден лучше, чем факт чтения письма.

Вложения

Проверить наличие файлов и артефактов открытия в типовых путях:

- %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.Outlook\
(путь из HKCU\Software\Microsoft\Office\<версия>\Outlook\Security\OutlookSecureTempFolder)
- %USERPROFILE%\Downloads
- %USERPROFILE%\Desktop
- %TEMP%
- %LOCALAPPDATA%\Temp
- %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\
- %LOCALAPPDATA%\Microsoft\Office\16.0\OfficeFileCache\

и аналогичные каталоги для используемой версии Office.



Дополнительно проверить:

- Zone.Identifier / Mark-of-the-Web;
- LNK, Jump Lists, RecentDocs, MRU;
- Prefetch для WINWORD.EXE, EXCEL.EXE, AcroRd32.exe, 7zFM.exe, WinRAR.exe и др.;
- временные каталоги архиваторов, если вложение было в формате zip/rar/7z;
- Trusted Documents:
HKCU\Software\Microsoft\Office\<версия>\<Word|Excel|PowerPoint>\Security\Trusted Documents\TrustRecords.

URL и переходы

Проверить все домены и URL из письма в следующих источниках:

- история браузера;
- прокси;
- DNS-логи;
- сетевые события от используемого EDR;
- логфайлы антивирусного ПО / веб-защиты;
- как вторичный источник —
HKCU\Software\Microsoft\Office\16.0\Common\Internet\Server Cache.

Подтверждением перехода считаются:

- HTTP/HTTPS-запросы к URL из письма;
- DNS-запросы к связанным доменам;
- сетевые события EDR в период после доставки письма.

05 Проверить последствия: запуск вредоносной активности

Если вложение было открыто или по ссылке переходили, следует проверить запуск кода и последующую активность:

- дерево процессов и командные строки;
- события PowerShell, cmd, wscript, mshta, rundll32, regsvr32;
- создание новых файлов, задач, служб, записей автозагрузки;
- сетевые соединения с внешними узлами после открытия вложения;
- срабатывания EDR/AV, WER/Crash Reports. Особенно, если возможно использование уязвимости в Office, PDF-reader или архиваторе.



ВЫПОЛНЕНИЕ

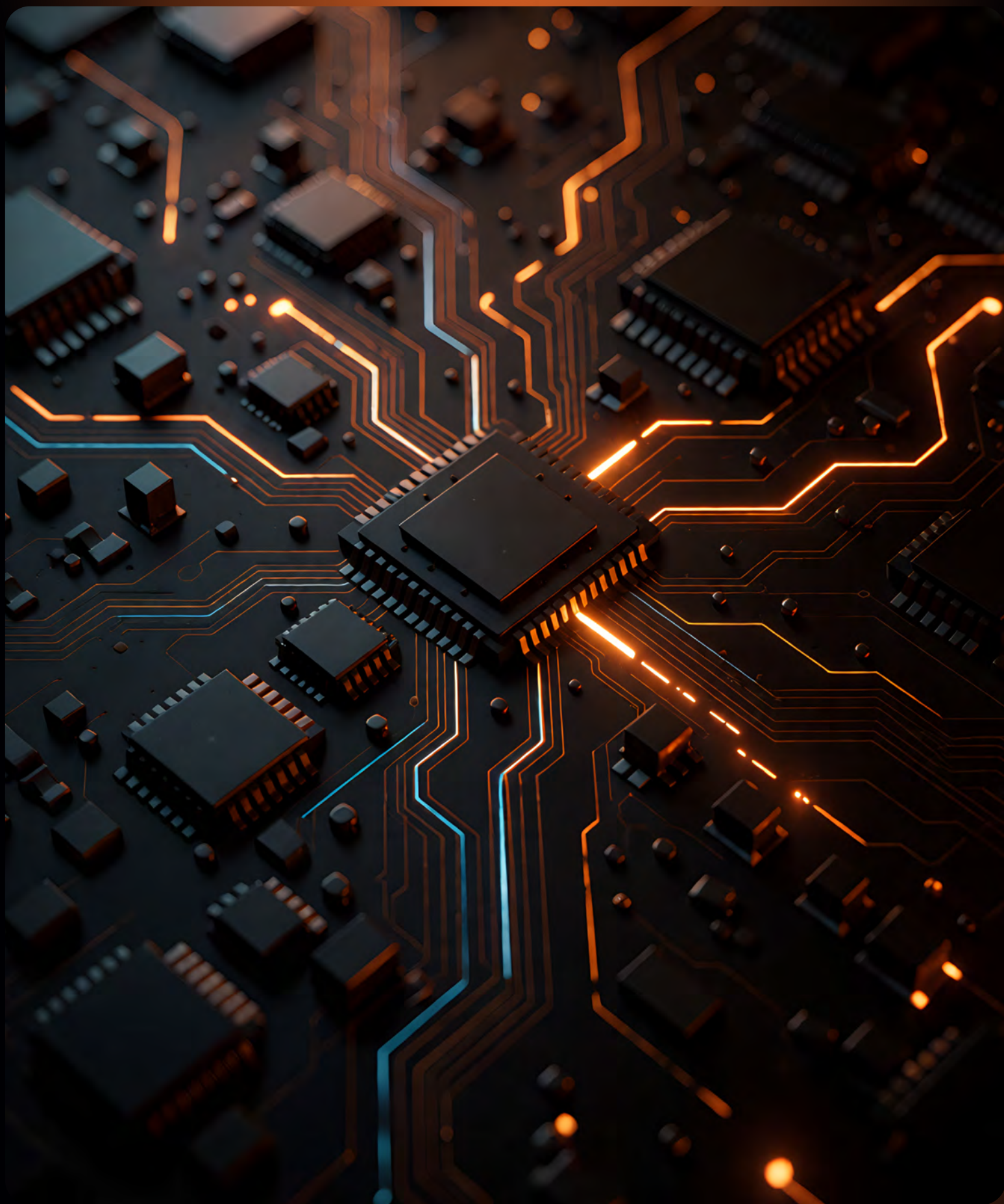
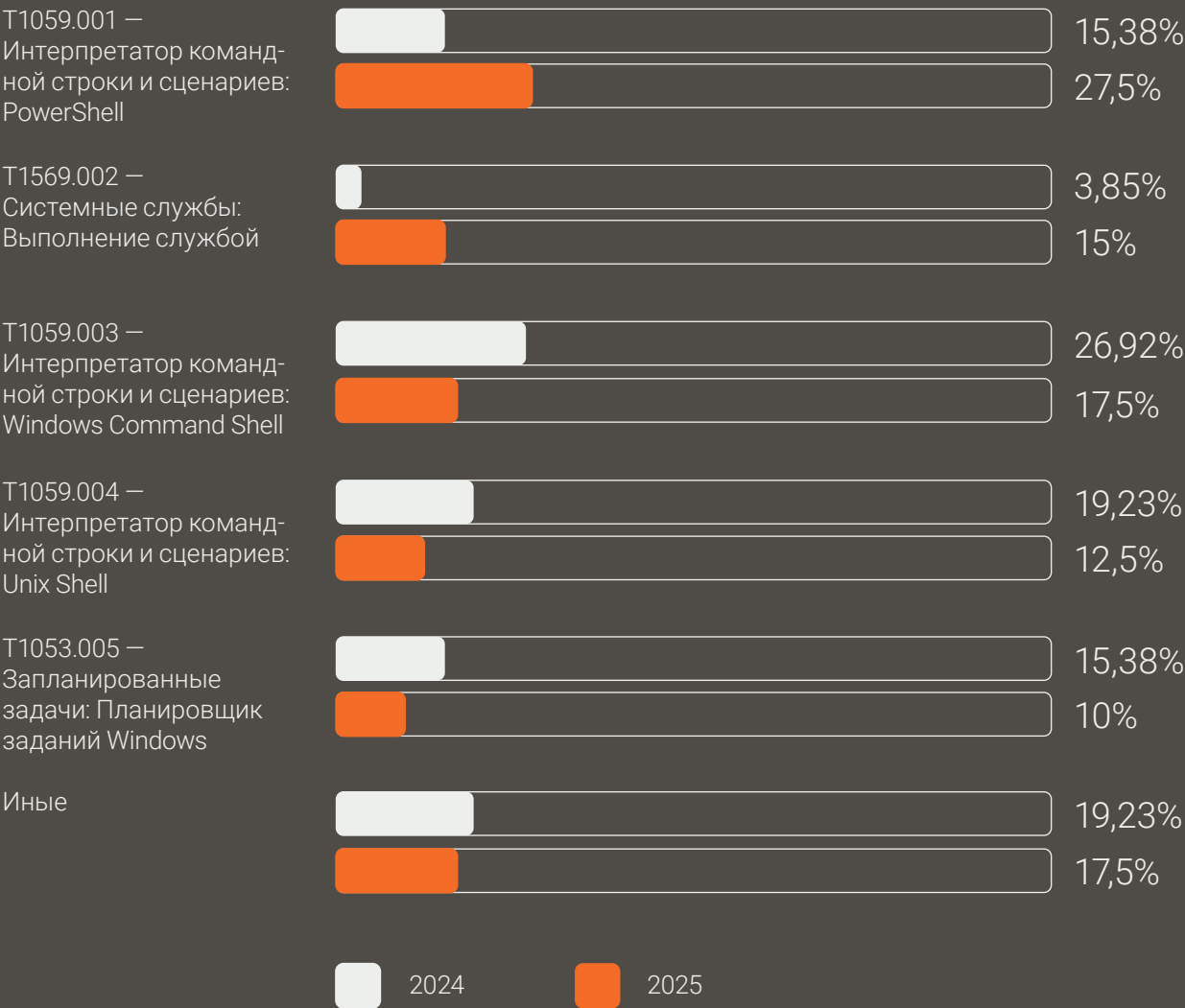


Диаграмма 9. Распределение выявленных техник в рамках тактики выполнения



В тактике выполнения (Execution) первенство вновь удерживают командные интерпретаторы и лидирующая позиция PowerShell здесь закономерна: его повсеместное распространение в корпоративных средах, глубокая интеграция с Windows и широкие административные возможности делают его одновременно незаменимым инструментом для ИТ-команд и удобным оружием для атакующих. Легитимность интерпретатора позволяет вредоносной активности долгое время оставаться в «слепой зоне» стандартных средств обнаружения, смешиваясь с действиями штатных администраторов.

Из наиболее примечательных наблюдений 2025 года — продолжение распространения и выполнения вредоносного кода через панели управления средств защиты, например, антивирусное программное обеспечение. Защитные решения нередко располагают широкими возможностями и привилегированным доступом к инфраструктуре, однако при этом зачастую не выделяются в отдельный сетевой сегмент и не получают дополнительных мер контроля. В результате скомпрометированная консоль управления антивирусом или конечными узлами превращается в плацдарм для распространения вредоносного

кода в масштабах всей организации — именно через те инструменты, которые призваны эту организацию защищать.

Если взглянуть на статистику антивирусных срабатываний в разрезе всех клиентов наших центров мониторинга в рамках тактики выполнения, картина получается весьма показательная, но вывод не так очевиден, как кажется на первый взгляд. Почему? Потому что ТОП-3 сигнатур выглядит вот таким образом:

UDS: DangerousObject.Multi.Generic

HEUR: Trojan.Script.Generic

HEUR: Trojan.Win32.Generic

Чаще всего антивирусные и EDR-решения фиксируют угрозы с, так называемыми, общими детектирующими сигнатурами. За этими названиями стоит важная особенность: речь идет об эвристическом и поведенческом обнаружении, то есть средство защиты зафиксировало подозрительную активность, но не смогло однозначно идентифицировать конкретную вредоносную программу.

Проблема в том, что такие срабатывания нельзя игнорировать, а полноценно понять их не всегда удается. Часть из них может оказаться реальной угрозой: загрузчиком, шифровальщиком или инструментом удаленного доступа на ранней стадии атаки. А часть — легитимным ПО с нестандартным поведением или ложным срабатыванием. Без дополнительного анализа отличить одно от другого невозможно.

Для полноценной оценки таких инцидентов необходимы контекст события (что происходило до и после срабатывания), данные киберразведки (есть ли информация об этом объекте в глобальных базах угроз) и даже вирусный анализ. Именно этот комплекс инструментов и экспертизы предоставляют сервисные решения класса MDR/SOC — там подобные события не просто фиксируются, а своевременно расследуются квалифицированными аналитиками.

ПРИМЕР ИЗ ПРАКТИКИ

Один из трендов в рамках тактики выполнения — использование злоумышленниками инструментов на базе искусственного интеллекта.

Звучит довольно устрашающе, но пока речь идет о вполне прагматичном применении ИИ для автоматизации рутины и быстрой генерации вредоносных скриптов и сценариев. Тем не менее, задачи выполняются вполне серьезные.

Например, в одном из инцидентов с **Bearlyfy** применялись сразу несколько сценариев, один из которых использовался для форматирования несистемных дисков систем резервного копирования VEEAM.

```

# === НАСТРОЙКИ ===
$csvPath = "C:\VEEAM_Disks_Report\...csv"
$logDir = "C:\VEEAM_FullFormat_Logs"
$timestamp = Get-Date -Format "yyyyMMdd_HHmm"

# Создаём папку для логов
if (!Test-Path $logDir) { New-Item -Path $logDir -ItemType Directory -Force }

# === 1. Загрузка отчёта ===
$report = Import-Csv $csvPath

# === 2. Фильтр: диски > 100 ГБ, НЕ C: ===
$targets = $report | Where-Object {
    $_.DriveLetter -and
    $_.DriveLetter -ne "C:" -and
    [double]$_._TotalSizeGB -gt 100
} | Select-Object ComputerName, DriveLetter, Label, TotalSizeGB -Unique

# === 3. Подтверждение ===
Write-Host "`n" + "="*70 -ForegroundColor Red
Write-Host "ЗАПУСК ПОЛНОГО ФОРМАТИРОВАНИЯ НА $($($targets.Count) ДИСКАХ ПАРАЛЛЕЛЬНО" -ForegroundColor Red
Write-Host "ЛОГИ: $logDir" -ForegroundColor Red
Write-Host "="*70 -ForegroundColor Red
$targets | Format-Table ComputerName, DriveLetter, @{n='SizeGB';e={[math]::Round($_.TotalSizeGB,0)}} -AutoSize

$confirm = Read-Host "`nВведи 'START ALL' для запуска (или Ctrl+C для отмены)"
if ($confirm -ne "START ALL") {
    Write-Host "ОТМЕНЕНО." -ForegroundColor Yellow
    exit
}

# === 4. ПАРАЛЛЕЛЬНЫЙ ЗАПУСК ===
$jobs = @()
foreach ($disk in $targets) {
    $computer = $disk.ComputerName
    $diskDrive = $disk.DriveLetter + ":"

```



Рис. 3. Фрагмент кода для форматирования несистемных дисков

Как это можно распознать на практике?

Сгенерированные ИИ-скрипты имеют ряд характерных признаков, в том числе структуру и стиль кода. ИИ-генерируемый код, как правило, избыточно аккуратен: четкие отступы и логичные имена переменных, правильная структура как по учебнику. Это нетипично для скриптов, написанных вручную, которые зачастую намеренно обфусцируют код или пишут его «грязно» и на скорую руку.

Другими схожими признаками могут выступать:

- комментарии в теле вредоносного скрипта или выделение разным цветом выходных данных;
- избыточная обработка ошибок;
- шаблонные техники обхода защит (ведь ИИ воспроизводит популярные техники из публичных источников) или даже явное упоминание факта генерации.



Несмотря на то, что на текущем этапе этот тренд не привносит принципиальных изменений в подходы к защите, его существование говорит о многом — инструменты и техники атакующих будут неизбежно совершенствоваться, и за этим развитием важно следить уже сейчас.



ЖУРНАЛИРОВАНИЕ POWERSHELL: ПОШАГОВАЯ НАСТРОЙКА

Как видно из статистики выше, журналирование командного интерпретатора PowerShell действительно полезно и может быть важным в различных сценариях использования.

Текущая версия 5.1 обладает самым обширным функционалом по аудиту использования PowerShell.



01 Уровень 1. Module logging

Доступен с версии 3.0. Через GPO: **«Computer Configuration» > «Administrative Templates» > «Windows Components» > «Windows PowerShell» > «Turn on Module Logging».**

Event ID 4103
(Microsoft-Windows-PowerShell/Operational).

Записываются сведения о выполнении конвейера PowerShell, фрагменты сценариев, некоторый обфусцированный код и данные, уже отформатированные для вывода. Это позволит зафиксировать некоторые детали, пропущенные другими источниками ведения журнала PowerShell, хотя может ненадежно фиксировать выполняемые команды. В журнал пишется множество данных, тем не менее, эти события позволяют получить ценную информацию, не отраженную в других источниках.

02 Уровень 2. Script block logging

Доступен с версии 3.0. Через GPO: **«Computer Configuration» > «Administrative Templates» > «Windows Components» > «Windows PowerShell» > «Turn on PowerShell Script Block Logging».**

Event ID 4104, (4105, 4106)
(Microsoft-Windows-PowerShell/Operational).

Записываются блоки кода по мере их выполнения ядром PowerShell, тем самым фиксируется все содержимое кода, выполняемого злоумышленником, включая сценарии и команды. Важно отметить, что PowerShell версии 5 автоматически регистрирует блоки кода, если содержимое блока совпадает со списком подозрительных команд или методов написания сценариев, даже если ведение журнала блоков сценариев не включено.

03 Уровень 3. Transcription

Через GPO: «**Computer Configuration**» > «**Administrative Templates**» > «**Windows Components**» > «**Windows PowerShell**» > «**Turn on PowerShell Transcription**», где задается расположение текстового файла.

Такая «транскрипция» записывает каждый сеанс PowerShell, включая все входные и выходные данные, в том виде, в каком они отображаются в сеансе. Записываются в текстовые файлы с разбивкой по пользователям и сеансам, а также содержат временные метки. Однако транскрипция записывает только то, что отображается в терминале PowerShell, и не включает содержимое выполняемых скриптов.

00 Уровень 0. PSReadline module

Включен по умолчанию, начиная с PowerShell v5 (Windows 10+).

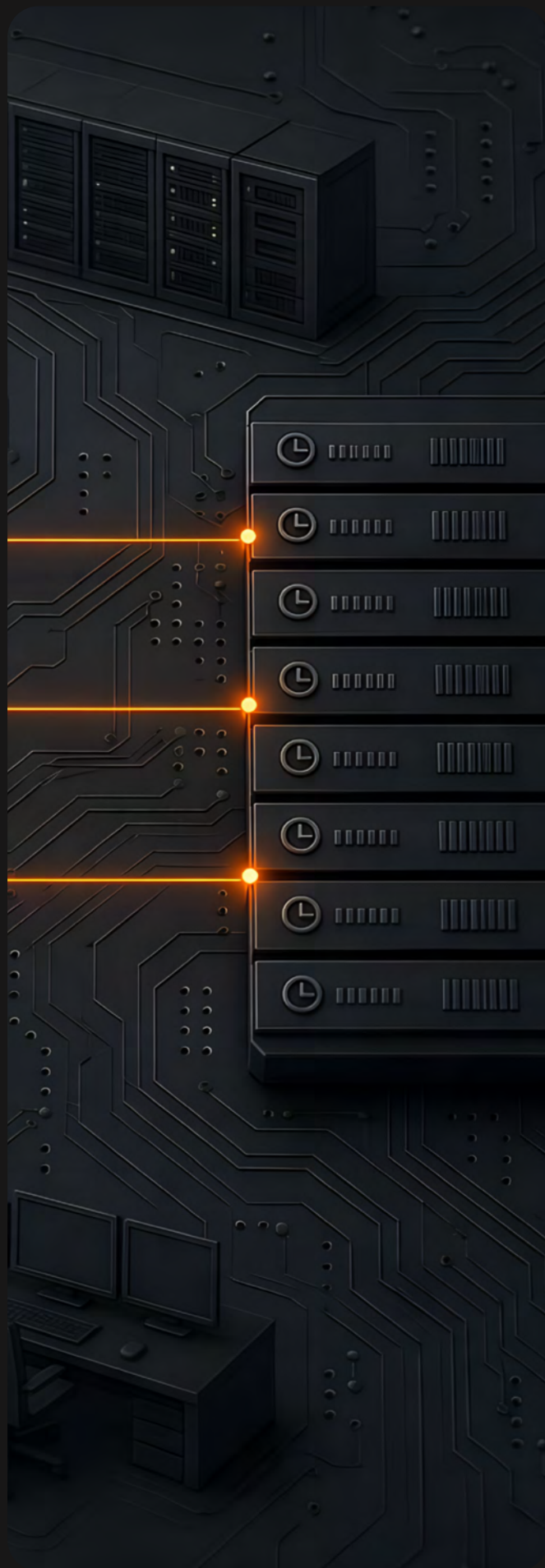
Последний, но в то же время самый интересный источник артефактов. Ведь он сохраняет абсолютно все, что вводилось в окне командной оболочки, даже неуспешно выполненные команды.

Файл по умолчанию:

```
%APPDATA%\Microsoft\Windows\
PowerShell\PSReadLine\
ConsoleHost_history.txt
```

(либо можно узнать расположение через командлет Get-PSReadlineOption)

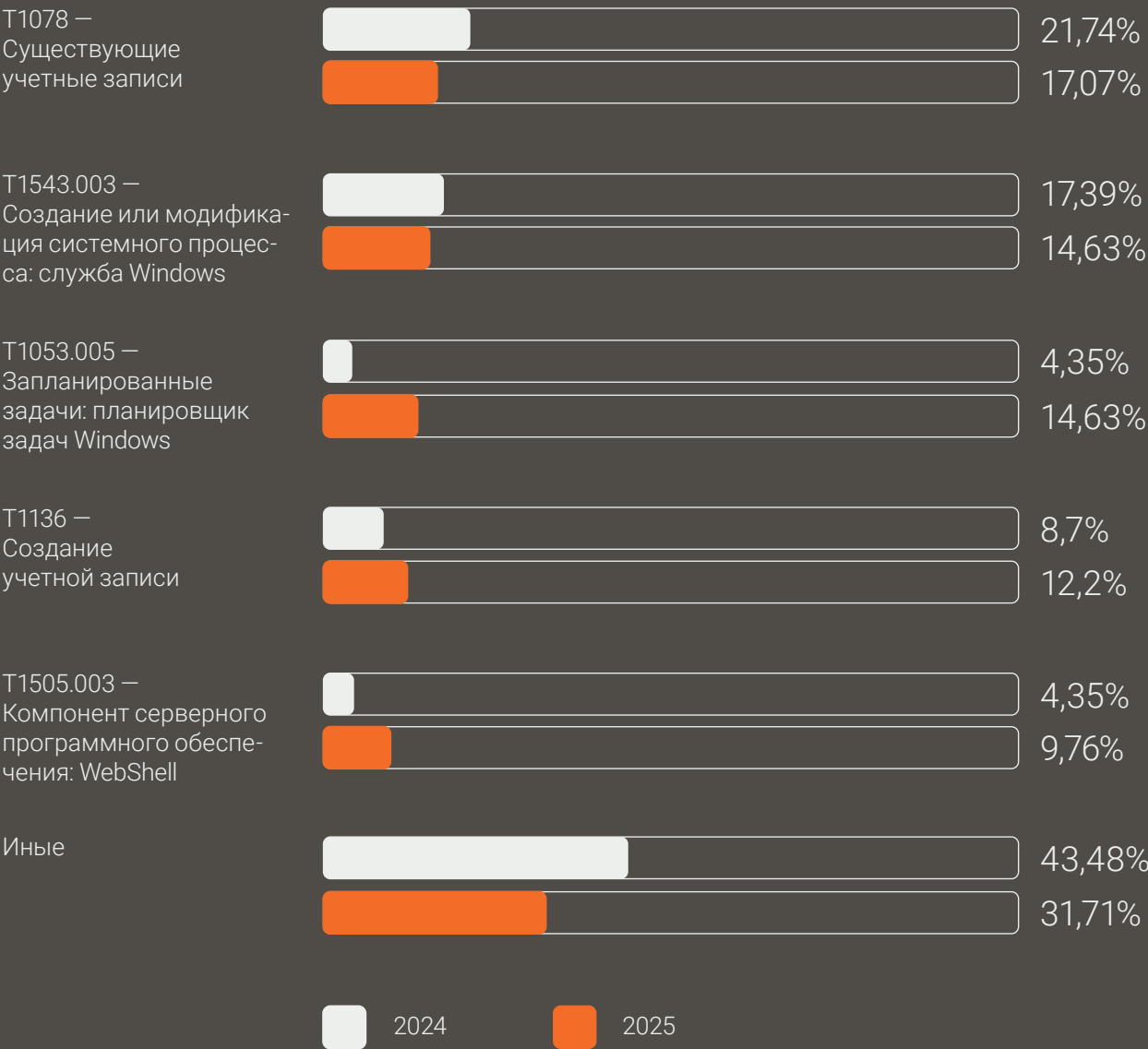
Важно! Terminal-less сессии, то есть удаленные сеансы, полученные, например, через Nishang или Meterpreter, фиксироваться не будут.



ЗАКРЕПЛЕНИЕ В СИСТЕМЕ



Диаграмма 10. Распределение выявленных техник в рамках тактики закрепления в системе



Этап закрепления (Persistence) в скомпрометированной среде характеризуется большим разнообразием применяемых методов и активным использованием как легитимных инструментов, так и специализированного вредоносного ПО. Злоумышленники стремятся обеспечить себе надежный и долговременный доступ к инфраструктуре жертвы, используя для этого широкий спектр техник. Многие из них рассчитаны на обход стандартных средств мониторинга.

В 2025 году мы наблюдали смещение фокуса внимания атакующих в сторону методов, которые сложно обнаружить без глубокого анализа поведения системы.

Если использование легитимных учетных записей еще остается значимым вектором (17,07%), то все большую долю занимают техники, манипулирующие штатными механизмами операционных систем.

Наиболее заметен рост использования планировщика задач — до 14,63% в 2025 году. Атакующие активно создают задачи как в Windows, так и в Unix-подобных системах (T1053.003 Scheduled Task/Job: Cron) для регулярного запуска вредоносного ПО, сбора информации или поддержания обратной связи с командными серверами.

Также значимым методом остается регистрация вредоносных исполняемых файлов в качестве служб Windows. Это позволяет злоумышленникам обеспечить автоматический запуск своего кода с повышенными привилегиями даже после перезагрузки системы.

Помимо наиболее часто встречающихся методов, в 2025 году зафиксировано применение широкого спектра других техник, демонстрирующих высокую техническую оснащенность группировок:

- использование ключей реестра и автозагрузки (T1547.001) остается классическим, но все еще эффективным способом закрепления;
- зафиксированы случаи эксплуатации специальных возможностей Windows (T1546.008), например, замена легитимной системной утилиты специальных возможностей utilman.exe на cmd.exe, что позволяет злоумышленникам после перезагрузки системы открывать командную строку с правами системы непосредственно с экрана входа, нажимая Win+U;
- применялись техники перехвата потока выполнения, включая динамический компоновщик в Linux-системах (T1574.006) и подмену COM-объектов в Windows (T1546.015);
- в атаках на *nix-системы злоумышленники изменяли конфигурационные файлы оболочек (T1546.004) и добавляли авторизованные ключи SSH (T1098.004) для обеспечения постоянного удаленного доступа. Также фиксировалось создание служб systemd (T1543.002);

- выросла и доля использования веб-шеллов (T1505.003), что свидетельствует о сохранении актуальности атак на веб-серверы и стремлении закрепиться на публично доступных узлах;
- злоумышленники продолжают создавать новые локальные и доменные учетные записи (T1136), часто маскируя их под служебные или забытые аккаунты.

Для обеспечения персистентности в скомпрометированных системах злоумышленники в 2025 году применяли широкий спектр инструментов, каждый из которых использовал уникальные механизмы закрепления путем интеграции в штатные компоненты операционных систем.

В Linux-окружениях атакующие активно эксплуатировали как пользовательские, так и системные механизмы автозагрузки. Для утилит с ресурса The Hacker's Choice, таких как **Global Socket** и **SSH-IT**, модифицировались файлы конфигурации оболочек .bashrc и .bash_profile (T1546.004), что обеспечивало запуск вредоносного ПО при каждом входе конкретного пользователя в систему. Параллельно с этим утилита gsocket устанавливалась в качестве systemd-сервиса, гарантируя свою активность при каждой загрузке системы.

Еще более изощренный метод продемонстрировал руткит **Kitsune**, входящий в состав **PUMAKIT**, который перехватывал управление на уровне динамического компоновщика: вредоносная библиотека загружалась раньше пути к ней в файл /etc/ld.so.preload, что позволяло скрывать присутствие вредоносной активности.

Для гарантированного восстановления после перезагрузки ВПО PUMAKIT также модифицировало загрузку в системном файле /etc/init.d/cron.

В среде Windows злоумышленники также демонстрировали разнообразие подходов к закреплению. Легитимный инструмент **Cloudflared** устанавливался как Windows-сервис, обеспечивая постоянное туннелированное соединение с инфраструктурой атакующих. Вредоносное ПО **Rtlshare** использовало более сложную технику перехвата выполнения через подмену COM-объекта `MruPidlList`, прописывая себя в реестре по пути `HKCU\Software\Classes\CLSID\{42aedc87-2188-41fd-b9a3-0c966feabec1}\InprocServer32`, что обеспечивало автоматическую загрузку библиотеки легитимными приложениями. Наряду с этим применялись и классические методы: **Deed RAT** закреплялся через модификацию ключа автозагрузки `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run`, гарантируя свой запуск при каждом входе пользователя в систему.

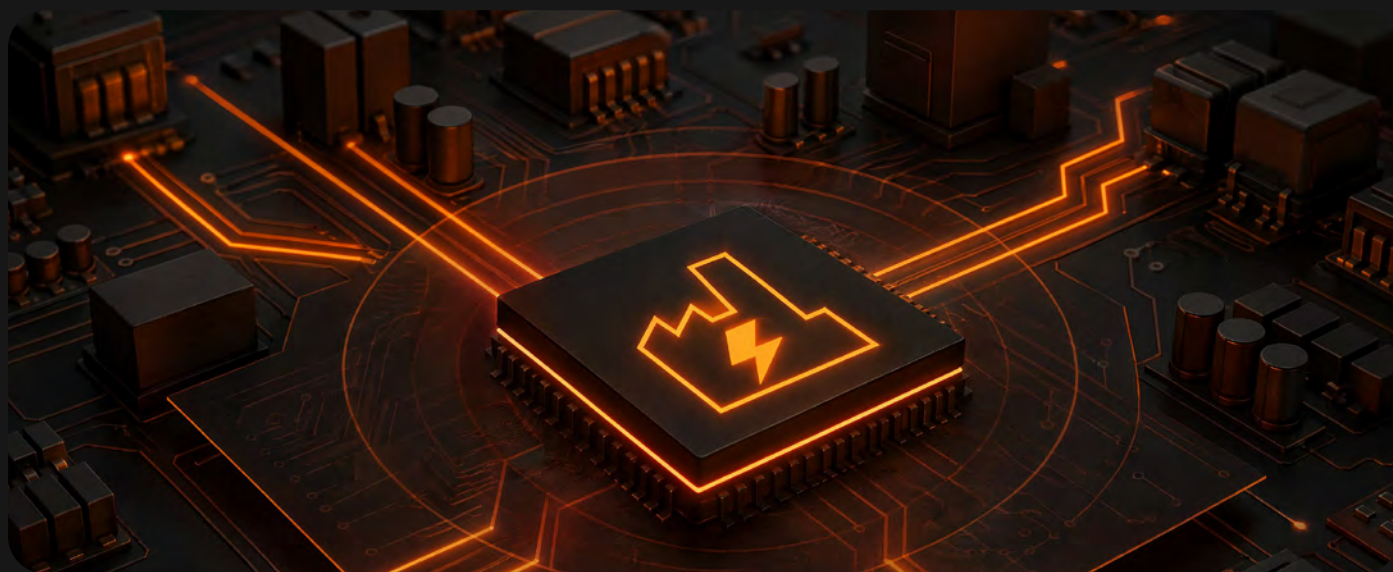
Можно отметить, что в 2025 году средства закрепления в системе характеризовались переходом от простых и легко обнаруживаемых методов к сложным и многоступенчатым.

Злоумышленники активно комбинируют различные техники, используют легитимное ПО для маскировки своей активности и разрабатывают специализированные вредоносные инструменты, нацеленные на долговременное присутствие в инфраструктуре жертвы. Это требует от организаций комплексного подхода к мониторингу, включающего анализ поведения и контроль целостности системных компонентов.

ПРИМЕР ИНЦИДЕНТА

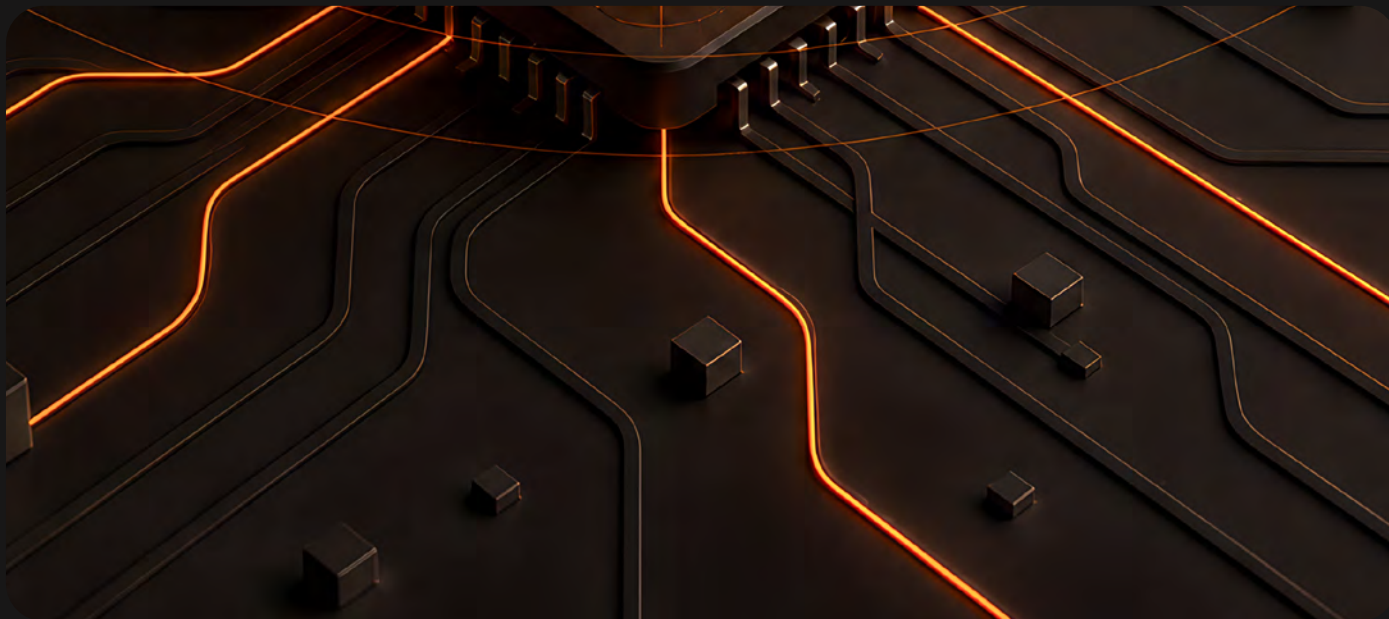
В качестве демонстрации разнообразия применяемых методов закрепления в системе мы выбрали инцидент в организации из сферы электротехнической промышленности. Ее атаковала группировка **PhantomCore (Head Mare)**.

Вектором проникновения злоумышленника в сеть организации послужила эксплуатация уязвимости, позволяющая удаленно выполнять произвольный код в прикладном ПО для видеоконференцсвязи **TrueConf Server** (BDU:2025-10116).



На этапе постэксплуатации атакующие создавали привилегированную учетную запись trueconf2 и в ходе развития атаки перемещались, в том числе, по протоколу RDP с использованием учетных записей локальных администраторов.

Стоит отметить, что наши коллеги из «Лаборатории Касперского» упоминают инструмент adduser.exe, который реализует создание локальной учетной записи, добавление ее в группу локальных администраторов и отключение механизма User Account Control (UAC).



Дополнительным средством закрепления в системе сервера TrueConf после эксплуатации стало использование атакующими устойчивых к обнаружению веб-шеллов, а именно подвергнутых обфускации, включая образец, имитирующий страницу «Ошибки 404».

Основным этапом атаки стало развёртывание в скомпрометированной инфраструктуре PowerShell-реализации ВПО **PhantomProxyLite**, предназначенного для организации обратного SSH-туннеля к инфраструктуре злоумышленников.

В ходе расследования нами были обнаружены скрипты с наименованиями Check-Update.ps1 и SSHService.ps1.

Для закрепления PhantomProxyLite в системе злоумышленники использовали ВПО **PhantomLatch**, представляющее собой PowerShell-скрипт для создания задач в планировщике Windows. В рамках атаки применялись два скрипта с различной периодичностью запуска:

Скрипт Create-Check-Update-Task.ps1 создавал задачу планировщика с именем CheckPowershellUpdate, которая обеспечивала запуск PhantomProxyLite (скрипт Check-Update.ps1) от имени учетной записи SYSTEM с интервалом в **3 минуты**.

Скрипт Create-SSHServiceTask.ps1 создавал задачу с именем SSHService, которая запускала альтернативную версию вредоносного ПО (SSHService.ps1) от имени **SYSTEM**, но с периодичностью **каждые 5 часов**.

В ходе расследования нами был обнаружен новый экземпляр вредоносного ПО этой группы злоумышленников **PhantomCore.PatientShell.SvcExe**, представляющий собой многофункциональный RAT (Remote Access Trojan) с широким спектром возможностей удаленного управления зараженной системой. Реализуемый функционал данного ВПО включает: запуск процессов через cmd.exe, исполнение произвольных команд, поиск файлов на зараженном устройстве, загрузку файлов по URL на атакуемую систему, отправку файлов на удаленный сервер, обновление собственной

конфигурации с хранением параметров в реестре Windows, отправку текущей конфигурации на управляющий сервер.

Данный образец закреплялся в системе путем регистрации Windows-сервиса с именем **WinDef**, что создает ложную принадлежность к компонентам штатного антивирусного решения Windows Defender. Это позволяло ему не только автоматически запускаться при старте системы с высокими привилегиями, но и длительное время оставаться вне подозрений при поверхностном анализе списка запущенных служб.

Несмотря на многообразие средств закрепления, применяемых группировкой в рамках одной атаки, нашей командой были даны рекомендации по полной нейтрализации всех выявленных средств закрепления: удалить вредоносные задачи планировщика, деинсталлировать скомпрометированные сервисы, очистить соответствующие ключи реестра, а также уничтожить тела вредоносных скриптов и исполняемых файлов, включая их копии, замаскированные в директориях легитимного ПО.

СКАНИРОВАНИЕ ИНФРАСТРУКТУРЫ НА ИОС

При реагировании на инциденты или после получения информации об актуальных индикаторах компрометации у заказчиков возникает необходимость проверить инфраструктуру на наличие подобных артефактов. Реализовать это можно разными способами: анализировать сетевую телеметрию, поставив на контроль C2-адреса на межсетевом экране, загрузить их в SIEM-систему, осуществив ретроспективную проверку и проверку в реальном времени, сканировать конечные устройства.

В своей практике мы комбинируем подходы, но считаем последний вариант основным, поскольку он позволяет напрямую

проанализировать главный источник фактического выполнения вредоносной активности.

В качестве инструмента, используемого нами, можем выделить портативную бесплатную версию **THOR Lite** по причине широкого и удобного функционала. Безусловно, есть и аналоги среди ИОС-сканеров — инструментов для обнаружения индикаторов компрометации (Indicators of Compromise, IoC) в виде Fenrir, Loki, YARA-сканера, Redline. Но сегодня мы хотим дать нашим читателям краткую инструкцию, которая поможет компаниям самостоятельно выявить индикаторы компрометации на своих системах именно с помощью THOR Lite.

Разберемся с основными этапами:

01

Скачайте бесплатную версию сканера THOR Lite и лицензии с официального ресурса разработчика под вашу операционную систему.

02

Распакуйте архив и поместите лицензию в корень директории. После развертывания проверьте инструмент на наличие всех необходимых обновлений:

- thor-lite-util.exe update
- thor-lite-util.exe upgrade

Это делается, в том числе, для обновления собственных сигнатур инструмента, которые периодически пополняются и могут использоваться вами для обширного анализа системы.

03

Заполните пользовательский файл списками полученных индикаторов компрометации. Они должны располагаться в директории:

- .\thor10.7lite-win-pack\custom-signatures\iocs

С помощью THOR lite можно проанализировать системы разными типами данных: обнаружить контрольную сумму, определенный IP-адрес или домен, поискать файлы с определенным названием или вовсе использовать YARA-правило со сложными условиями. Принцип составления таких файлов очень похож, но в инструкции приведем наиболее часто используемый случай. В указанной выше директории создаем файл с произвольным названием, но имеющим ключевое слово **hash** и расширение текстового редактора:

- angaraMTDR-**hash.txt**
- my_iocs-**hash.txt**
- TLTR-**hash-iocs.txt**

04

Заполните файл в следующем формате:

Контрольная сумма индикатора (md5, sha1, sha256); скоринговое значение, которое указывало бы на совокупность достоверности индикатора, его надежности и критичности; комментарий, описывающий индикатор.

При желании, последнюю часть можно отбросить и оставить только контрольную сумму и скоринговое значение. Пример заполненного файла:

- 44d88612fea8a8f36de82e1278abb02f; 100; Eicar
- 3395856ce81f2b7382dee72602f798b642f14140; 79
- 275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f; 89; Test

05

После сохранения файла, вам нужно подготовить его для перемещения в среду, которая потенциально может быть скомпрометирована. Для этого вам необходимо зашифровать файлы, связанные с составленными списками индикаторов компрометации. Рассматриваемый нами IoC-сканер имеет встроенную возможность для реализации данной задачи. Выполните команду:

- thor-lite-util.exe encrypt
- .\custom-signatures\iocs\TLTR-hash-iocs.txt

В результате вы получите зашифрованную версию составленных индикаторов. Оригинальный файл необходимо удалить из директории.

06

У вас все готово для запуска инструмента, осталось только выбрать необходимые опции. Из ключевых:

--cpulimit значение ограничивает потребление CPU, что полезно на высоконагруженных системах.

Минимальное значение, при котором инструмент будет работать составляет **15**.

--customonly позволяет сканеру использовать только заготовленные индикаторы компрометации и не использовать свои собственные сигнатуры.

-e директория для создания отчета по результатам анализа инструмента. Для удобства рекомендуем отправлять отчеты в сетевую папку.

Конечная команда будет выглядеть следующим образом:

- `thor64-lite.exe --cpulimit 55 --customonly -e "\\example\NetworkShare"`

Результатом успешного выполнения будут три файла: .csv файл – содержит контрольные суммы, которые сканер выявил в процессе анализа, .txt – журнал запуска THOR lite, .html файл - HTML представление отчета.

Вы можете запустить исполняемый файл как локально на системе, так и распространив его с помощью централизованных решений: групповые политики, ansible-плейбуки и т.д.



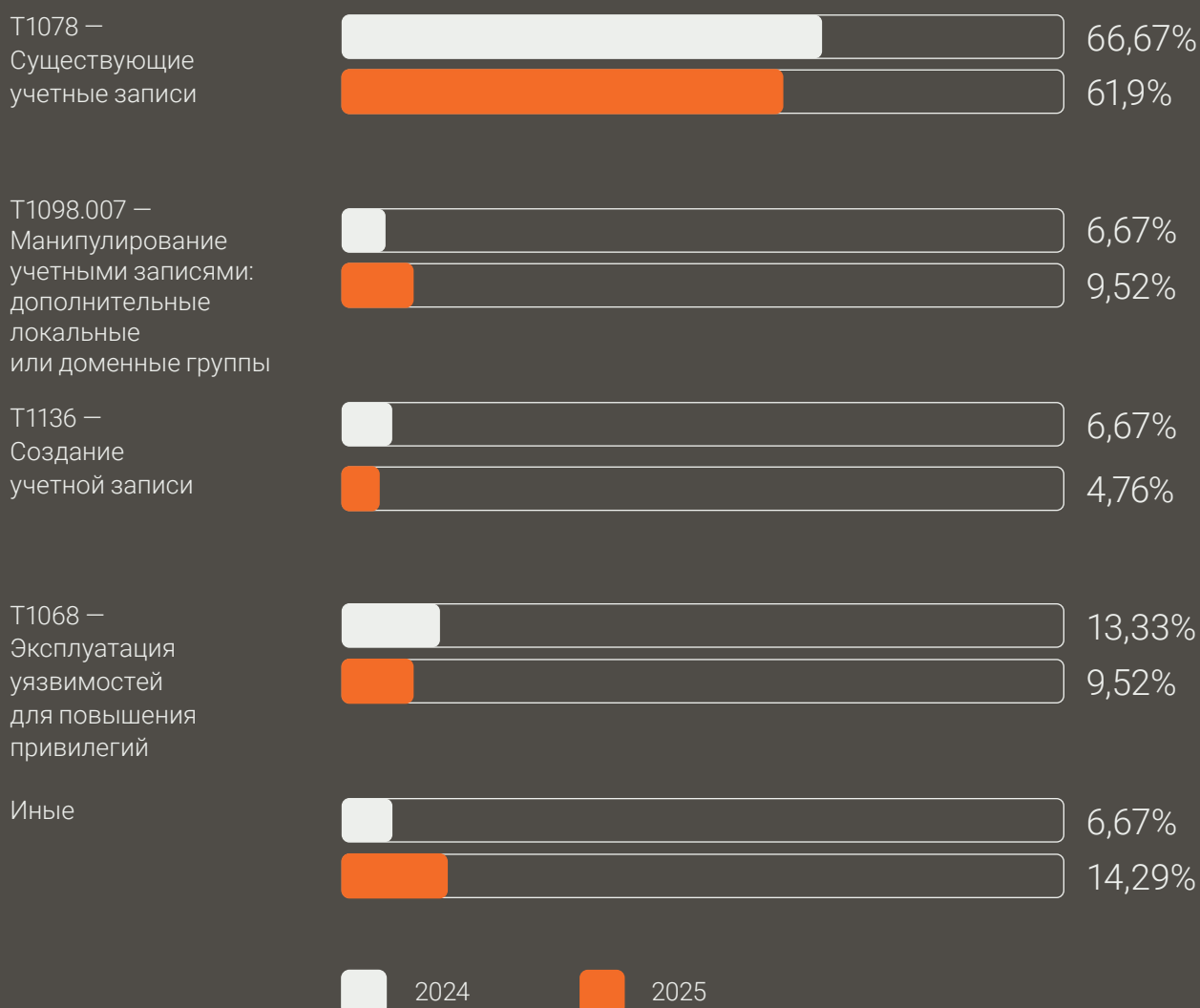
Для получения дополнительной информации по инструменту рекомендуем ознакомиться с [полноценной инструкцией разработчика](#). Наше руководство не является полноценной заменой, но служит введением в инструмент и одним из вариантов решения конкретной проблемы по анализу системы на наличие индикаторов компрометации.



ПОВЫШЕНИЕ ПРИВИЛЕГИЙ



Диаграмма 11. Распределение выявленных техник в рамках тактики повышения привилегий



Анализ результатов инцидентов 2025 года демонстрирует существенную эволюцию тактик злоумышленников на этапе повышения привилегий (Privilege Escalation). По сравнению с предыдущим периодом, ландшафт угроз в этой области стал более фрагментированным и технически сложным.

Доминирующим вектором по-прежнему остается использование легитимных учетных записей (T1078) — 61,9% случаев.

Злоумышленники активно применяют скомпрометированные или слабые учетные данные доменных и локальных пользователей для получения повышенных привилегий. При этом в 2025 году наблюдается качественное усложнение атак: кража учетных данных комбинируется с эксплуатацией уязвимостей и манипуляцией механизмами аутентификации.

Одной из тенденций 2025 года стало активное применение специализированного инструментария. В расследованиях нами неоднократно фиксировалось использование вариаций техники «Potato» (в частности, **EfsPotato** и **DeadPotato**), которые позволяют повысить привилегии, манипулируя механизмами аутентификации. Также отметим применение утилиты **JCTokenUtil**, предназначенной для кражи и манипуляции токенами доступа.

Помимо использования публичных утилит, атакующие активно эксплуатировали свежие уязвимости. Особо отметим случай с применением легитимного инструмента **Velociraptor**, версия 0.73.4 которого содержала критическую уязвимость **CVE-2025-6264**, позволяющую злоумышленникам повысить свои привилегии в скомпрометированной системе. В атаках на виртуальную инфраструктуру зафиксировано использование уязвимости **CVE-2024-37085**, которая давала возможность автоматически добавить скомпрометированную учетную запись в группу администраторов **ESXi**.



Одной из тенденций 2025 года стало активное применение специализированного инструментария.

Значительную долю (9,52%) занимает манипуляция учетными записями и группами (**T1098.007**), что говорит о стремлении атакующих не просто получить права, но и закрепиться в домене, создавая легитимные пути для долговременного доступа.

В 2025 году повышение привилегий превратилось в полноценный, технически насыщенный этап атаки.

Злоумышленники комбинировали легитимные инструменты, эксплойты для свежих уязвимостей (в том числе в самом ПО для атак) и специализированные утилиты, чтобы гарантированно получить максимальный контроль над системой. Это требует не просто мониторинга учетных записей, но и глубокого анализа поведения процессов и своевременного обновления ПО, которое может быть использовано в атаках.

ПРИМЕР ИНЦИДЕНТА

В разделе «**Получение первоначального доступа**» мы уже упоминали одну из атак группировки **Warlock Group** с применением программы-вымогателя **Warlock Cryptor** (**x2anylock**). В данном примере будут рассмотрены действия, которые предпринимали атакующие для шифрования виртуальной инфраструктуры **VMware ESXi** жертвы.

Контролируя учетную запись доменного администратора, полученную на предыдущих этапах, атакующие смогли реализовать один из сценариев эксплуатации уязвимости: они изменили доменную группу с именем «**ESX Admins**» и добавили в нее подконтрольного пользователя.



Это позволило атакующим получить полные права администратора на целевых гипервизорах ESXi, присоединенных к домену, без необходимости дополнительной аутентификации.

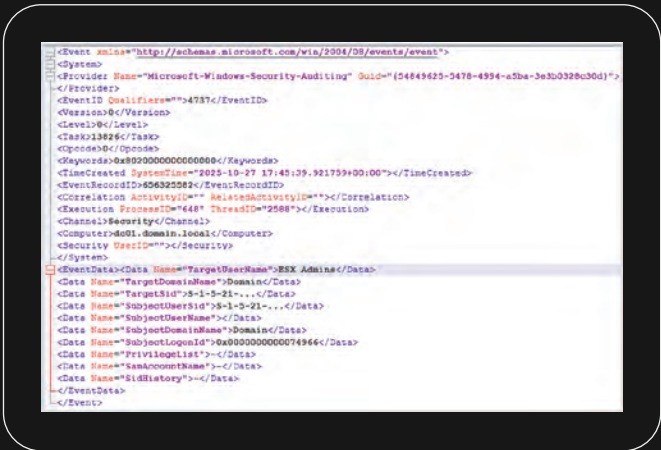


Рис. 4. Событие изменения группы

Суть **уязвимости** заключается в том, что ESXi-серверы, входящие в домен Active Directory, по умолчанию предоставляют полный административный доступ любому члену группы с именем «ESX Admins», независимо от того, существовала ли эта группа в домене изначально. Проверка подлинности группы не выполняется. Злоумышленники, используя права доменного администратора, могут выполнять команды:

- net group "ESX Admins" /domain /add
- net group "ESX Admins" <имя_пользователя> /domain /add

В результате этой манипуляции атакующие смогли получить несанкционированный контроль над гипервизорами, что стало ключевым этапом для развития атаки.

Получив полный административный доступ к ESXi, злоумышленники инициировали процесс массового шифрования данных с использованием программы-вымогателя **Babuk**. Возможность шифровать файловую систему самого гипервизора позволила атакующим одновременно вывести из строя все виртуальные машины, размещенные на зараженных хостах, что привело к критическим простоям в работе сервисов организации.

Этот случай показывает, как уязвимость в инфраструктурном ПО (ESXi) может стать критической точкой отказа, особенно если злоумышленники уже обладают доменными привилегиями. Основной урон был нанесен не только за счет шифрования отдельных рабочих станций, но и за счет компрометации слоя виртуализации.

СНИЖАЕМ ПОВЕРХНОСТИ ЛОКАЛЬНОГО ПОВЫШЕНИЯ ПРИВИЛЕГИЙ

На этапе повышения привилегий злоумышленник, действуя локально, пытается найти в системе слабое место, которое позволит ему повысить

привилегии обычного пользователя. С точки зрения защитника эта стадия особенно неудобна тем, что многие действия атакующего внешне

похожи на обычную системную проверку: он может выводить список служб, анализировать права пользователя, проверять установленные компоненты и искать небезопасные конфигурации. О подобном примере мы расскажем в рамках раздела «[Этап изучения внутренней инфраструктуры](#)». Но именно поэтому наиболее эффективная стратегия здесь заключается не только в детектировании конкретных инструментов, но и в снижении самой возможности локального повышения привилегий.

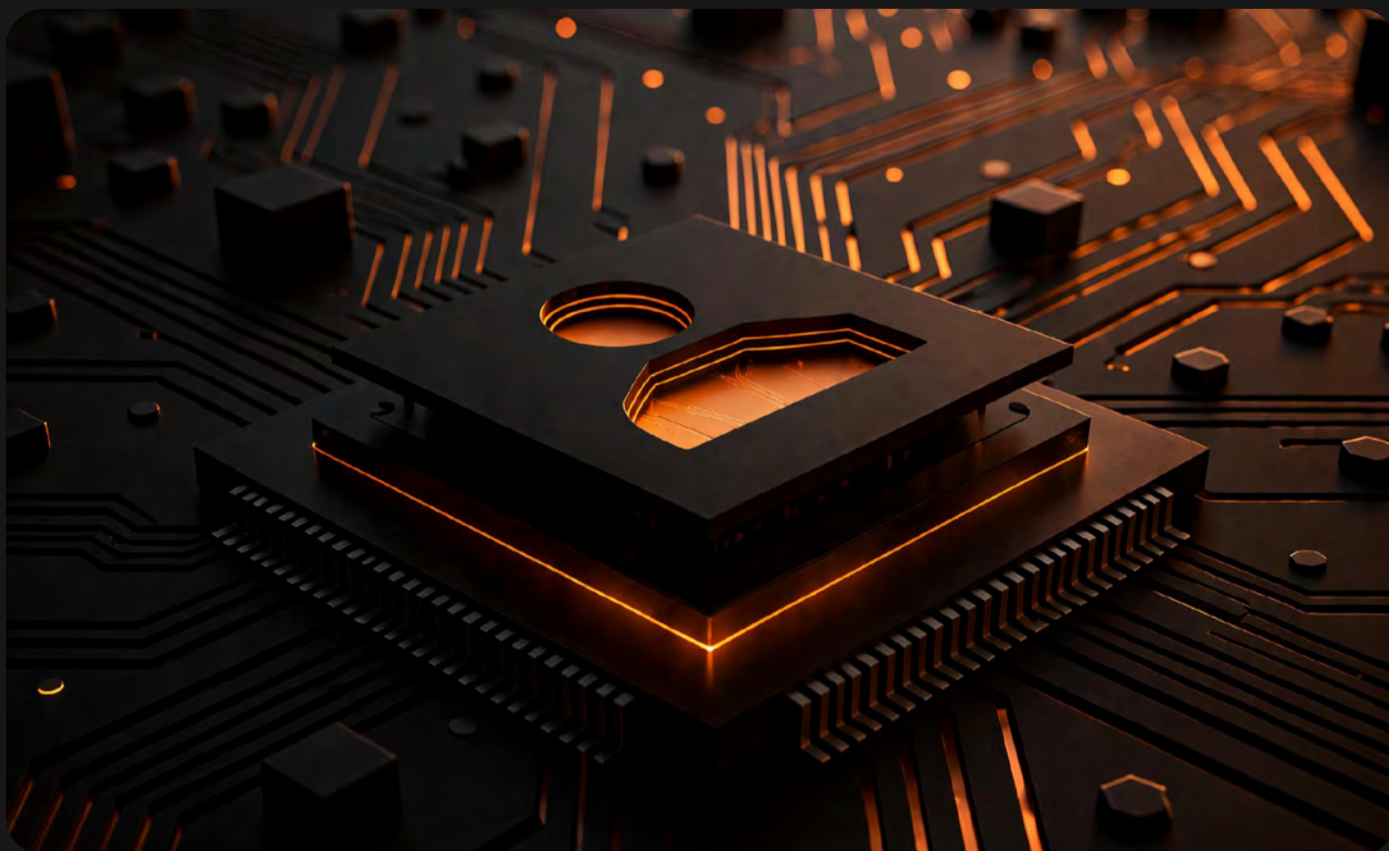
- **Сокращение поверхности для Potato-инструментария**

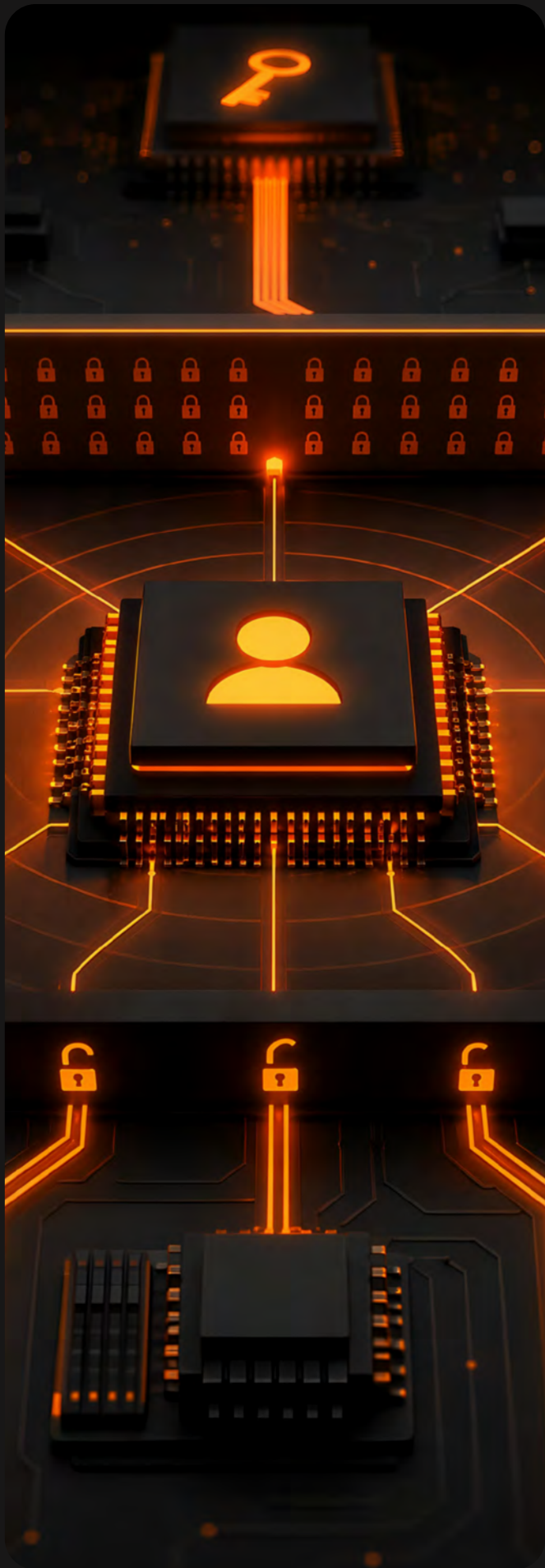
Семейство Potato-эксплойтов опирается на злоупотребление механизмами Windows, связанными с токенами, службами, NTLM, RPC, DCOM и имперсонацией. Поэтому защитникам важно отключать или ограничивать компоненты, которые чаще всего участвуют в подобных сценариях. Это относится к **Print Spooler** на серверах и доменных контроллерах, а также к ненужным службам, работающим с высокой степенью доверия.

Дополнительно полезно ограничивать NTLM там, где это возможно, сокращать круг сервисных учетных записей и проверять, какие привилегии реально выданы службам на конкретных системах. Чем меньше доступных атакующему механизмов имперсонации, тем сложнее реализовать Potato-подобную эскалацию.

- **Контроль типовых локальных мисконфигураций**

При этом стоит признать, что большая часть локального повышения привилегий строится не на сложной эксплуатации, а на ошибках в конфигурации системы. Сюда относятся и запуск вредоносных программ, используя пути к службам и ярлыкам, в которых нет кавычек, и слабые права на каталогах, пароли и секреты в переменных, а также небезопасные настройки вроде `AlwaysInstallElevated`. Отдельно стоит контролировать, какие учетные записи имеют права на изменение сервисов и задач планировщика, поскольку именно через такие объекты часто реализуется эскалация без использования эксплойта в классическом смысле.





- Ограничение привилегий и чувствительных прав

Для локального повышения привилегий критично наличие таких прав, как:

- SeImpersonatePrivilege,
- SeAssignPrimaryTokenPrivilege,
- SeDebugPrivilege,
- SeLoadDriverPrivilege.

Если подобные привилегии выдаются слишком широко, атакующий получает дополнительные варианты для запуска эскалации даже без уязвимости в коде. Поэтому важно минимизировать число локальных администраторов, избегать лишних членств в привилегированных группах и по возможности разделять пользовательские и административные контексты.

В итоге борьба с локальным повышением привилегий сводится к двум вещам: во-первых, нужно уменьшать число доступных атакующему сценариев за счет харденинга инфраструктуры; во-вторых, нужно внимательно отслеживать любые изменения в службах, задачах и привилегированных настройках системы, поскольку именно там чаще всего и проявляется попытка эскалации. Там, где нельзя быстро предотвратить попытку эскалации, можно хотя бы сделать ее заметной, дорогой и нестабильной для атакующего.

ОБХОД ЗАЩИТЫ

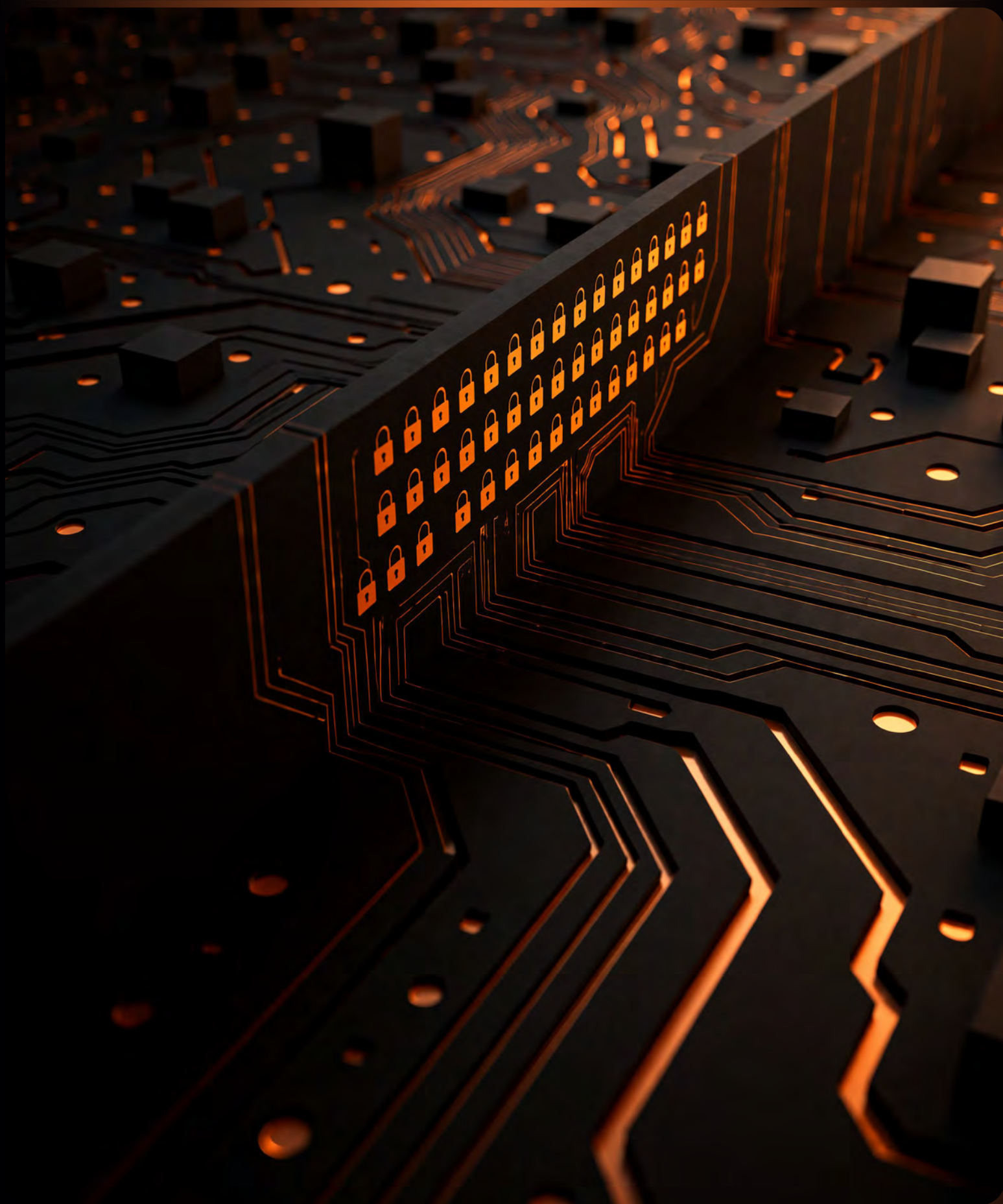
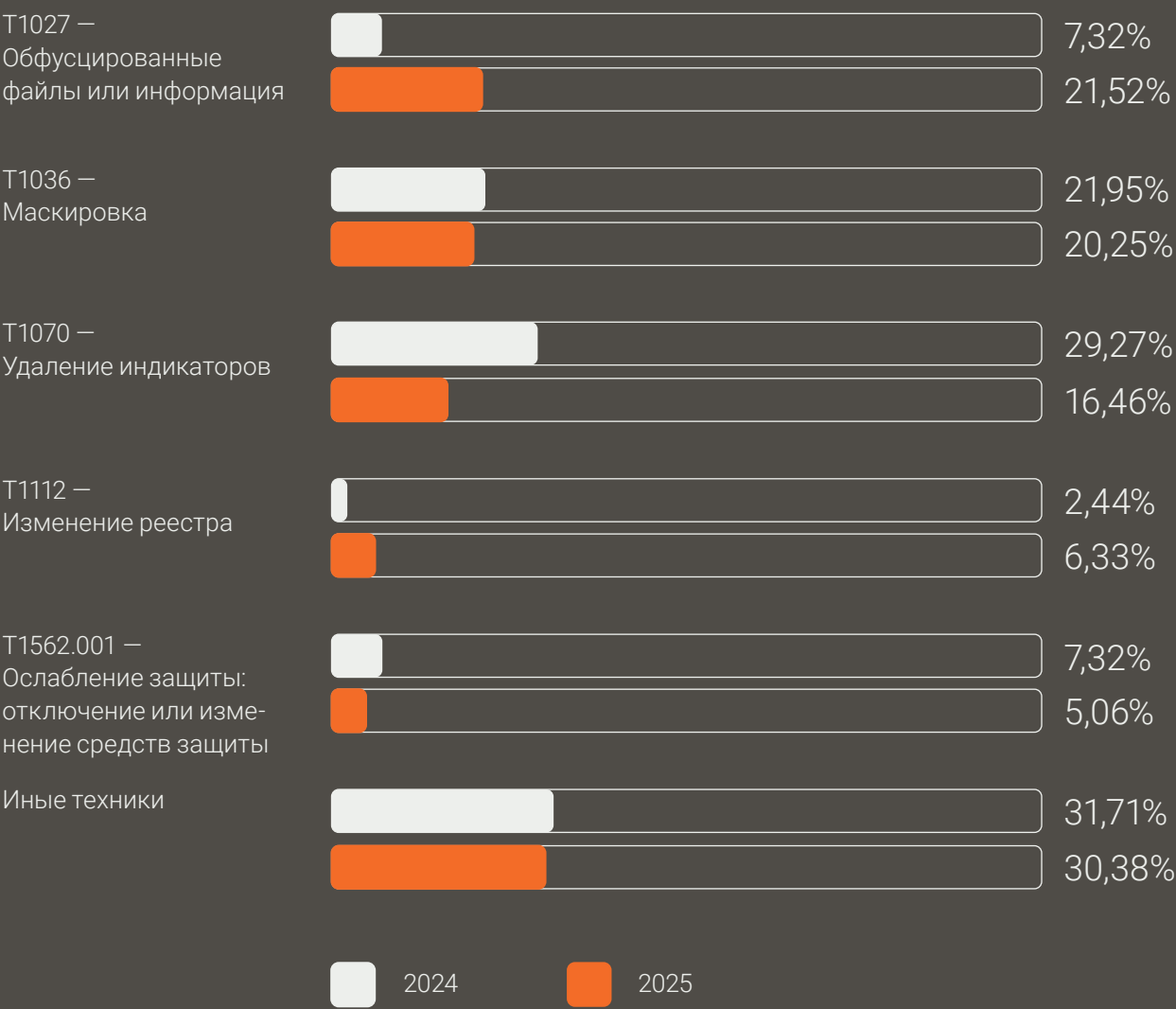


Диаграмма 12. Распределение выявленных техник в рамках тактики обхода защиты



Удаление индикаторов (T1070) и маскировка (T1036) по-прежнему удерживают лидирующие позиции по частоте применения на этапе обхода защитных механизмов (Defense Evasion). Очистка журналов событий, удаление артефактов с диска, переименование вредоносных исполняемых файлов под названия системных процессов (svchost.exe, explorer.exe) или модификация вполне легитимных утилит, например, Process Explorer, с внедрением в них функционала ВПО типа RAT — все это остается повседневной практикой. Относительно простой и достаточно эффективной.

Заметный тренд 2025 года по общей статистике расследованных инцидентов — рост интереса к различным видам обфускации (T1027). Злоумышленники вкладывают больше усилий в то, чтобы вредоносный код в принципе не был распознан средствами защиты. Именно выбранный нами плейбук для этого раздела посвящен данной тематике.

Отдельного внимания заслуживают техники, которые встречаются реже, но представляют особую аналитическую сложность.

Реестр Windows и его модификация остается одним из ключевых векторов закрепления и скрытого управления поведением системы. Полностью мониторить весь реестр — задача нереалистичная, он содержит миллионы ключей. Но это и не нужно. Критически важно держать под контролем как минимум приоритетные ветки, которые традиционно используются для закрепления и обхода защиты. Не обойтись и без своевременного реагирования.

Намеренное сокрытие файлов и директорий, модификация групповых политик, в частности, политик по умолчанию позволяют атакующему закрепиться в инфраструктуре так, что следы его присутствия не бросаются в глаза при стандартном осмотре.



Модификация групповых политик (англ. Group Policy Objects, GPO) особенно опасна в корпоративной среде: однажды измененная политика может тиражировать вредоносные конфигурации или код на сотни машин домена.

Еще более показательны угрозы, существующие и работающие исключительно в оперативной памяти. В процессе работы такие угрозы не оставляют артефактов на диске, а вот обнаружение связанных или вторичных признаков требует дополнительного мониторинга и часто навыков криминалистического анализа, что уже предъявляет высокие требования к квалификации аналитика.

ПРИМЕР ИНЦИДЕНТА

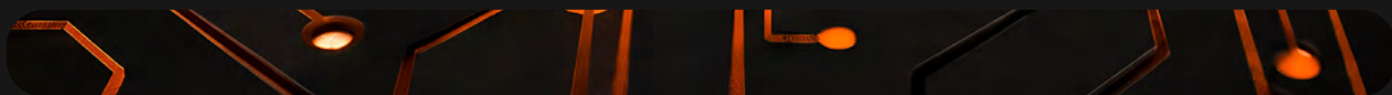
В ходе расследования одного из инцидентов была выявлена картина, которая наглядно демонстрирует, насколько эффективной может быть грамотно выстроенная тактика обхода защиты. Атакующие присутствовали в инфраструктуре организации более трех лет, оставаясь полностью незамеченными. Они неоднократно обновляли инструментарий, однако неизменно придерживались одних и тех же методов маскировки. И, как видно по времени их присутствия в сети жертвы, действительно работающих методов.

Одним из центральных приемов была имитация системной активности на уровне имен и путей.

Задачи планировщика Windows (Task Scheduler) создавались с названиями, характерными для штатных системных процессов, например:

- C:\Windows\System32\Tasks\Microsoft\Windows\StateRepository

Такое размещение и именование визуально неотличимо от легитимных задач Windows при беглом просмотре. Администратор, не проводящий целенаправленного аудита планировщика, без проверки командной строки задачи и исполняемых файлов просто не обратит на это внимания.



Аналогичный подход применялся и к размещению вредоносных файлов. Атакующие использовали директории, имитирующие системные пути:

- C:\Windows\System32\config\systemprofile\AppData\Local\Maintenance

Дополнительно для запуска вредоносного кода использовалась утилита pcalua.exe — легитимный компонент Windows (Program Compatibility Assistant), который позволяет выполнять произвольные команды, фактически перенаправляя запуск через доверенный системный процесс (техника Living off the Land):

- pcalua.exe -a C:\Windows\system32\config\systemprofile\AppData\Local\Maintenance\tty4298cc6c05f50fae.exe

Техника, хотя и является довольно известной, достаточно специфична для определенной группировки в данном исполнении.

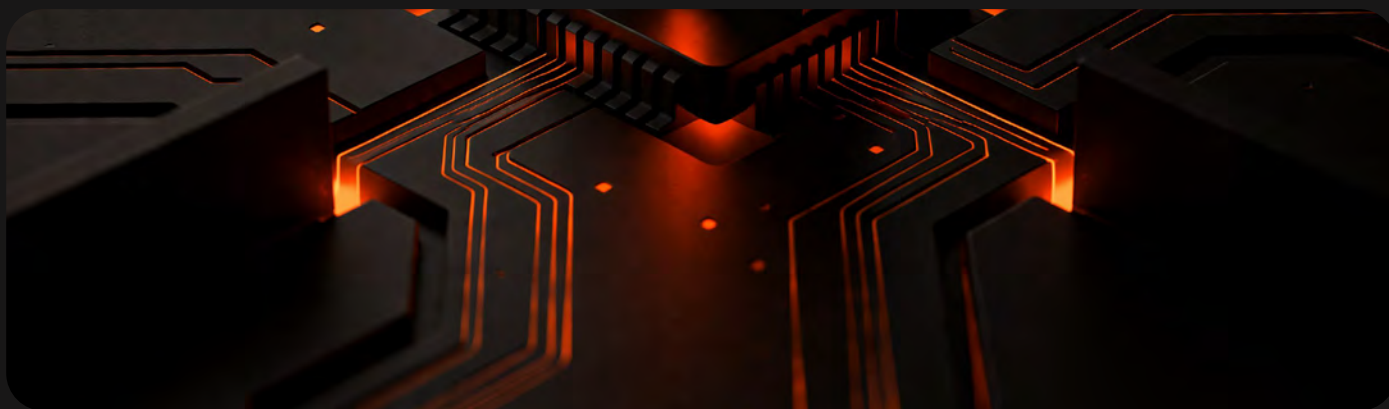
По завершении каждого этапа атакующие аккуратно устраняли артефакты своей активности: удаляли временные файлы, каталоги, в которых агрегировались данные перед выгрузкой, а также отдельные инструменты после их применения. Это существенно затрудняло ретроспективный анализ и восстановление полной хронологии атаки.

Совокупность описанных техник, характерные артефакты и общий профиль активности однозначно указывают на группировку **RedCurl** (также известную как Earth Kapre и Red Wolf), специализирующуюся на корпоративном шпионаже.

Основная цель участников данной группировки — документы, составляющие коммерческую тайну, и персональные данные сотрудников.

Примечательно, что в марте 2024 года была опубликована информация о принципиально новом векторе в деятельности группы: впервые зафиксировано, что RedCurl применила собственный шифровальщик. До этого момента, на протяжении всей известной истории своей активности, группировка преследовала исключительно цели шпионажа — без деструктивных действий. Это означает, что даже «тихие» шпионские кластеры могут эволюционировать в сторону атак с прямым финансовым ущербом для жертвы.

После того как наша команда развернула в инфраструктуре заказчика EDR-решения и провела полную очистку зараженных узлов, доступ злоумышленников к сети был утрачен. В последующий период фиксировались попытки восстановить контроль над инфраструктурой с использованием ранее оставленных механизмов закрепления, однако, благодаря своевременно принятым мерам, вернуть доступ атакующим не удалось.



ПЕРВИЧНЫЙ АНАЛИЗ ОБФУСЦИРОВАННОГО POWERSHELL СКРИПТА

Для выявления обфусцированных скриптов можно анализировать события ScriptBlock PowerShell Windows, мониторинг которых необходимо настроить заранее. Лучше всего настроить централизованный сбор событий, чтобы очисткой журналов злоумышленник не мог скрыть свои следы. Запущенные скрипты PowerShell, в зависимости от размера, будут попадать в одно или несколько событий с EventID 4103 и 4104.

Поскольку в ScriptBlock попадают как вызовы функций в скрипте, так и результаты работы командлета Invoke-Expression (IEX), один сложный скрипт может создавать довольно большое количество событий.

Примечательно, что если для обфускации выбран метод выполнения строк как кода через IEX, то в события попадут деобфусцированные строки PowerShell.

Туда будут попадать и вызовы легитимных скриптов, поэтому стоит обращать внимание на путь исполнения и количество ScriptBlock.

Для восстановления скриптов PowerShell из скриптблоков можно воспользоваться модулем [Revoke-Obfuscation](#). Он умеет анализировать как события из журнала через Get-WinEvent, так и напрямую разбирать evtx-файлы. Единственное ограничение – PowerShell 5.1, в более новых версиях модуль не работает.

```
Get-WinEvent -LogName
Microsoft-Windows-PowerShell/
Operational |

Get-RvoScriptBlock -Verbose

Get-ChildItem .\Demo\demo.evtx |

Get-RvoScriptBlock -Verbose

Get-RvoScriptBlock -Path 'log.evtx'
-Verbose
```

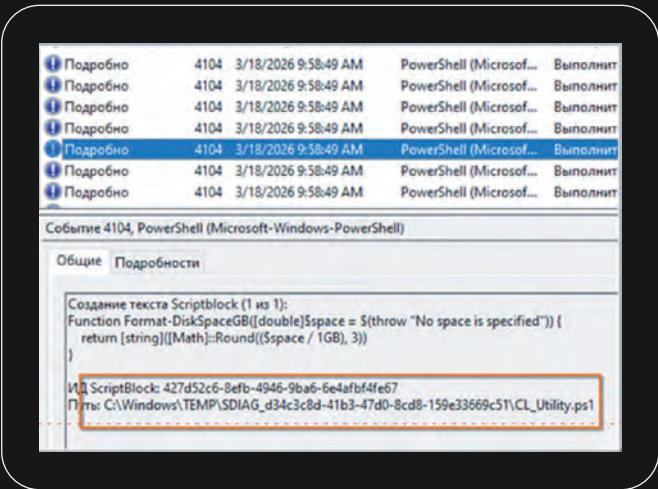
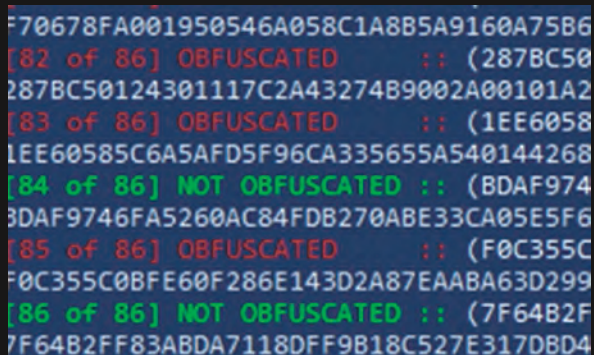


Рис. 5. Пример события PowerShell с запуском скрипта

Собранные PowerShell скрипты можно проверить антивирусом или проанализировать командлетом Measure-RvoObfuscation из модуля Revoke-Obfuscation, чтобы выявить подозрительные. При этом желательно рассматривать только скрипты длиной более 50 символов, так как оценка степени обфускации на меньших объемах работает не всегда адекватно.




```
Get-WinEvent -LogName
Microsoft-Windows-PowerShell/Operational |
Get-RvoScriptBlock -Verbose | ?
ScriptBlockLength -gt 100 |
Measure-RvoObfuscation -Verbose
```



The screenshot shows the output of the 'Measure-RvoObfuscation' command. It lists several script blocks with their IDs and obfuscation status. For example, '[82 of 86] OBFUSCATED :: (2878C50...)' and '[84 of 86] NOT OBFUSCATED :: (BDAF974...)'. The text is color-coded: red for 'OBFUSCATED' and green for 'NOT OBFUSCATED'.

Рис. 6. Пример результата вывода командлета Measure-RvoObfuscation

Код в событиях ScriptBlock все равно будет полностью или частично скрыт в зависимости от используемых методов обфускации и может потребоваться дополнительный анализ, чтобы понять его предназначение и алгоритм работы.

Если анализировать статистику по скриптблокам в журнале событий, то можно выявить аномальные события, которые связаны с активностью злоумышленника. При этом надо обратить внимание на:

- всплески событий от среднего значения дня/часа;
- активность в нерабочее время;
- появление SID пользователей, которых не было ранее;
- большие скриптблоки.

#Пример построения статистики

#с пересборкой блоков -- медленнее

```
Get-WinEvent -LogName
Microsoft-Windows-PowerShell/Operational |
Get-RvoScriptBlock -Verbose | group
-Property { $_.TimeCreated.Date }
```

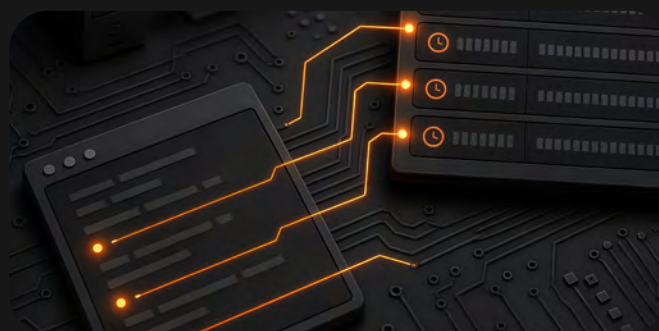
#Просто по количеству событий 4104

```
Get-WinEvent -FilterHashtable
@{LogName='Microsoft-Windows-PowerShell/Operational'; ID=4104} | group {
$_TimeCreated.Date }
```

#По дням недели

```
Get-WinEvent -FilterHashtable
@{LogName='Microsoft-Windows-PowerShell/Operational'; ID=4104} | group {
$_TimeCreated.DateOfWeek }
```

Приведенные примеры выявления вредоносной активности на основе фильтрации и выгрузки PowerShell скриптов представляют базовую концепцию такого подхода. Очевидно, что они не могут заменить полноценную работу аналитика.



ПОЛУЧЕНИЕ УЧЕТНЫХ ДАННЫХ

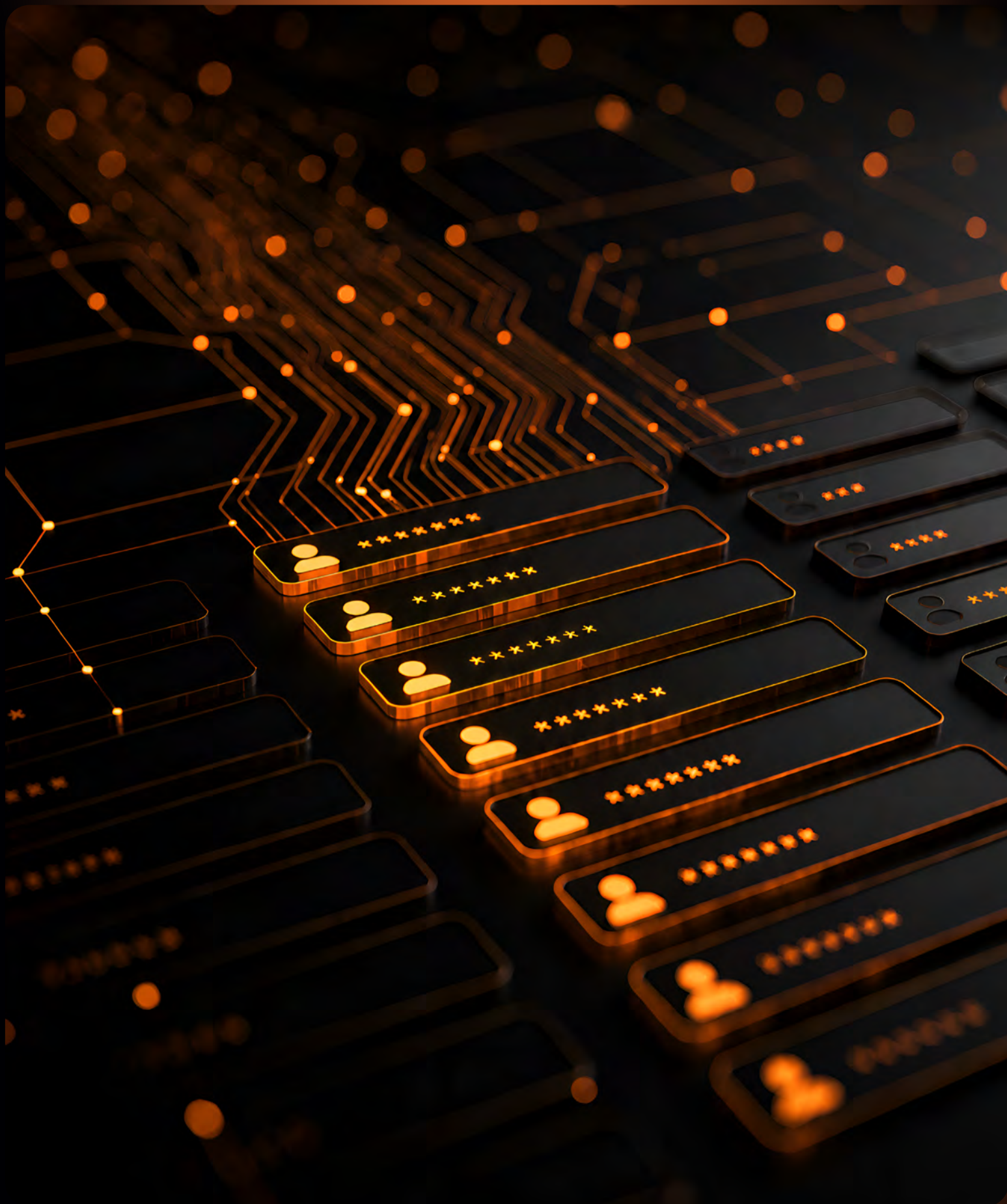
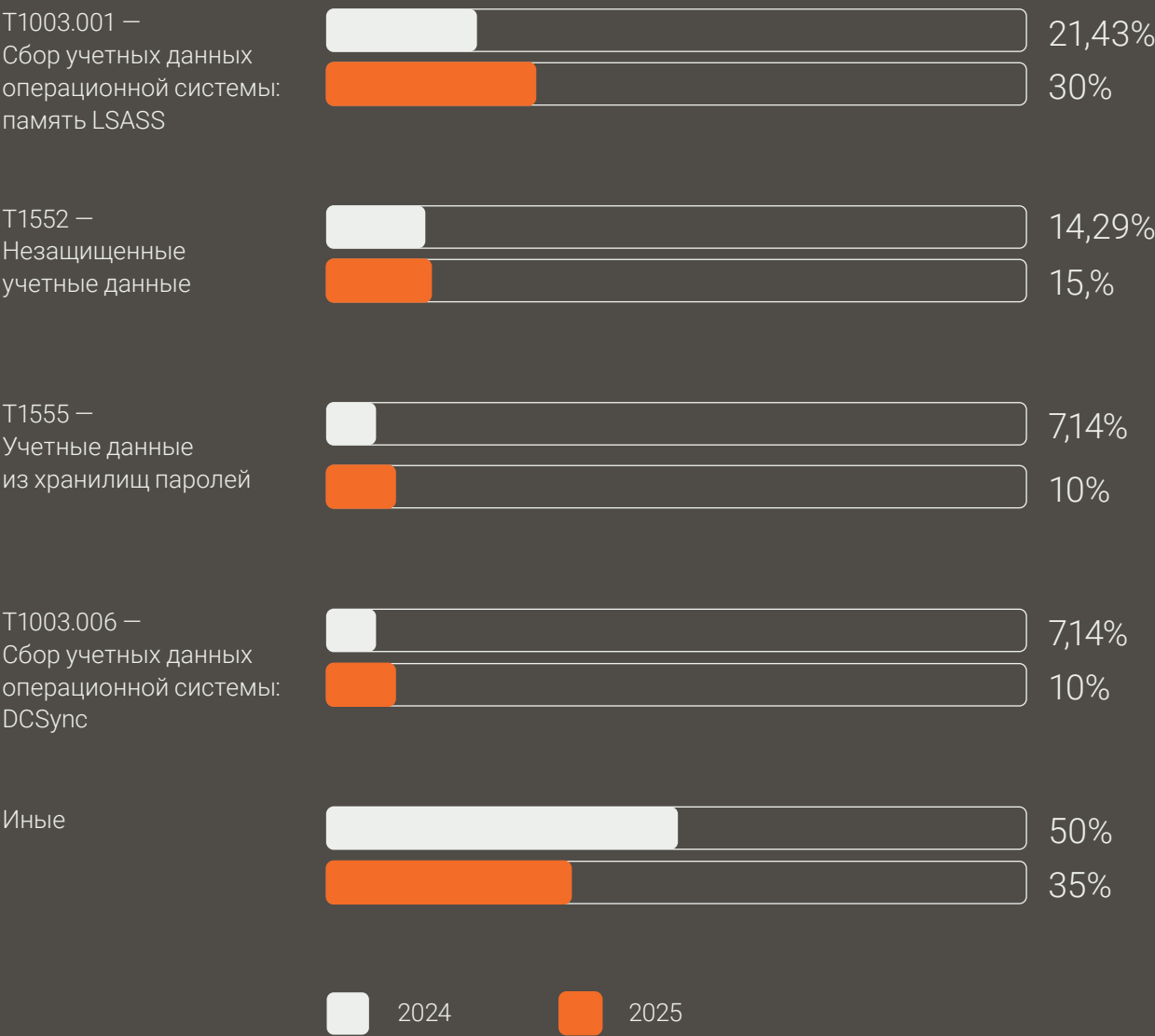


Диаграмма 13. Распределение выявленных техник в рамках тактики получения учетных данных



В 2025 году структура наиболее часто используемых методов кражи учетных данных (Credential Access) сохранила прошлогодние тенденции — ключевыми векторами остались извлечение учетных данных из памяти процесса LSASS, сбор незащищенно хранящихся паролей и токенов в файловых системах и конфигурациях, а также хищение сохраненных учетных данных из браузеров и менеджеров паролей.

Несмотря на развитие средств защиты, основным вектором кражи учетных данных остается прямой дамп **памяти процесса LSASS**. Злоумышленники продолжают активно использовать классические инструменты, такие как Mimikatz, для извлечения паролей и хешей непосредственно из памяти, а также легитимную утилиту ProcDump от Microsoft для создания дамп-файла процесса LSASS с последующим его анализом на стороне атакующих.

Кроме того, в отчетном периоде отмечен рост инцидентов, связанных с кражей учетных данных из виртуальных сред: при компрометации гипервизора злоумышленники создают и забирают целиком файлы оперативной памяти (.vmem) виртуальных машин штатными средствами управления виртуализацией (например, через снапшоты), после чего в офлайн-режиме извлекают из них учетные данные все тем же Mimikatz.

Поиск учетных данных в незащищенных местах остается одним из наиболее простых и стабильно эффективных способов их компрометации. В 2025 году злоумышленники по-прежнему массово находили пароли в открытом виде, сохраненные в самых разных местах: в текстовых файлах на рабочих столах и в документах с названиями вроде «пароль.txt» или «RDP.xlsx», в конфигурационных файлах приложений и сервисов, где учетные данные прописаны в незашифрованном виде, а также в файлах резервных копий и дампах баз данных.

Активно сканировались локальные и сетевые диски на предмет файлов с чувствительной информацией, включая журналы. Особое внимание уделялось анализу истории команд (bash_history, ConsoleHost_history.txt), где пользователи и администраторы нередко оставляли пароли, переданные в качестве аргументов при запуске скриптов или подключении к удаленным ресурсам.

Атаки на менеджеры паролей продемонстрировали незначительный рост. Увеличилось количество инцидентов, связанных с кражей файлов баз данных менеджеров паролей (например, .kdbx) для последующего офлайн-брутфорса. Зафиксированы инциденты, связанные с дампом базы данных Passwork — популярного корпоративного менеджера паролей, включенного в реестр отечественного ПО. Атакующие, получив доступ к серверу Passwork, формировали дамп базы данных с помощью штатного инструмента mongodump.exe



Поиск учетных данных в незащищенных местах остается одним из наиболее простых и стабильно эффективных способов их компрометации.

ПРИМЕР ИНЦИДЕНТА

В одном из инцидентов атакующий получил доступ к целевой инфраструктуре через скомпрометированного подрядчика, оказывающего услуги по финансовому аудиту в целевой организации. После получения доступа атакующие произвели разведку: определили некоторые критически важные системы, выявили назначение используемой учетной записи, ее права в Active Directory.

Выяснилось, что расширенных привилегий у данного аккаунта не было, поэтому атакующий начал искать способы получения доступа к учетной записи с более широкими правами.

Обычно, при проверке настроек безопасности Active Directory методом «серого ящика» (когда у исследователя имеется доменная учетная запись и, как следствие, появляется возможность взаимодействовать с внутренними сервисами, требующими прохождения процедуры аутентификации) также проверяется конфигурация одного из внутренних сервисов — AD CS (Active Directory Certificate Services). Выявление и последующая эксплуатация мисконфигурации в таком сервисе позволяет атакующему получить доступ к другой учетной записи, в том числе привилегированной. Для расследования таких атак хорошо подходят журналы самого сервиса AD CS — события 4886 и 4887 содержат необходимые сведения: когда, кто, для кого и по какому шаблону запросил сертификат.

Однако, на момент расследования этого инцидента система с сервисом AD CS была недоступна, и одной из зацепок стало событие запроса TGT на контроллере домена на имя администратора домена с нестандартным набором флагов «TicketOption: 0x40800010». Такой набор характерен для Rubeus (инструмент для взаимодействия с протоколом Kerberos) или Certipy (инструмент для перечисления шаблонов сертификатов и поиска в них уязвимых параметров). После обнаружения подобного события мы обратили внимание на существующие шаблоны сертификатов и наличие уязвимых конфигураций. Как вариант, можно использовать уже упоминавшийся инструмент Certipy с ключом «vulnerable». Однако в нашем случае это было невозможно, так как на момент инцидента отсутствовала возможность запуска контроллеров домена (которые должен опрашивать Certipy). Поэтому искать уязвимые шаблоны пришлось вручную. Для этого пригодилась обнаруженная база данных AD — ntds.dit, дамп которой сделал атакующий с одной из рабочих станций.

Во время анализа ntds.dit был обнаружен шаблон, имеющий следующие атрибуты.

```
#Разрешает проводить
аутентификацию с помощью
этого сертификата

PKI-Extended-Key-Usage = 1.3.6.1.5.5.7.3.2

#Установленный флаг
ENROLLEE_SUPPLIES_SUBJECT,
который дает возможность
выпускать сертификат на имя
другого пользователя

msPKI-Certificate-Name-Flag =
0x00000001

#Содержит в себе SID-ы
пользователей/групп, которые могут
выпустить сертификат. Опасным
является значение, соответствующее
SID-у широкой группы, например,
«Пользователи домена»

NT-Security-Descriptor = <REDACTED>
```

Такой шаблон уязвим к сценарию атаки «ESC 1».

Получив учетную запись доменного администратора, атакующий развернул программу-вымогатель семейства Lock-Bit.



ПРОТИВОДЕЙСТВИЕ НЕЛЕГИТИМНОМУ ПОЛУЧЕНИЮ УЧЕТНЫХ ДАННЫХ

На просторах Интернета можно найти огромное количество статей по выявлению нелегитимного получения учетных данных. Один из примеров: [детектирование дампа памяти процесса LSASS](#) от наших коллег из мониторинга.

- Отслеживайте открытие или запуск команд поиска файлов с паролями в открытом виде, например:

```
findstr /si pass  
ls -la | grep -ir pass
```

- Отслеживайте доступ к файлам браузерных хранилищ паролей (Login Data, logins.json) из процессов, не являющихся браузером.
- Мониторьте попытки доступа к базам (например, к файлам .kdbx) защищенных хранилищ паролей из необычных расположений.

Кроме этого, мы хотим поделиться чек-листами по возможному противодействию получения учетных данных злоумышленниками.

Повышение защищенности учетных данных:



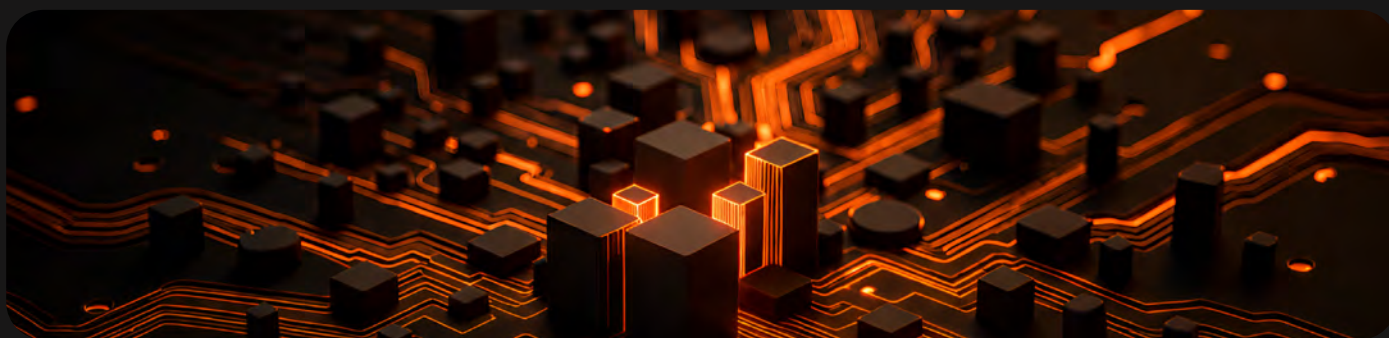
Защита LSASS:

- Включите LSA Protection (RunAsPPL) для предотвращения доступа недоверенных процессов к памяти LSASS.
- Включите Credential Guard, тогда дамп одного только процесса lsass.exe будет малоэффективен для атакующего.
- Ограничьте права отладки процессов (SeDebugPrivilege) тем учетным записям, которым они не нужны.



Предотвращение хранения незащищенных паролей:

- Проводите регулярные аудиты репозитория и общих ресурсов на предмет наличия учетных данных.
- Не передавайте пароли в аргументах командной строки, используйте переменные окружения или интерактивный ввод.
- Запретите хранение паролей в открытом виде — внедрите сканирование сетевых дисков и рабочих станций на наличие файлов с паролями (для этого можно использовать DLP-системы).



03

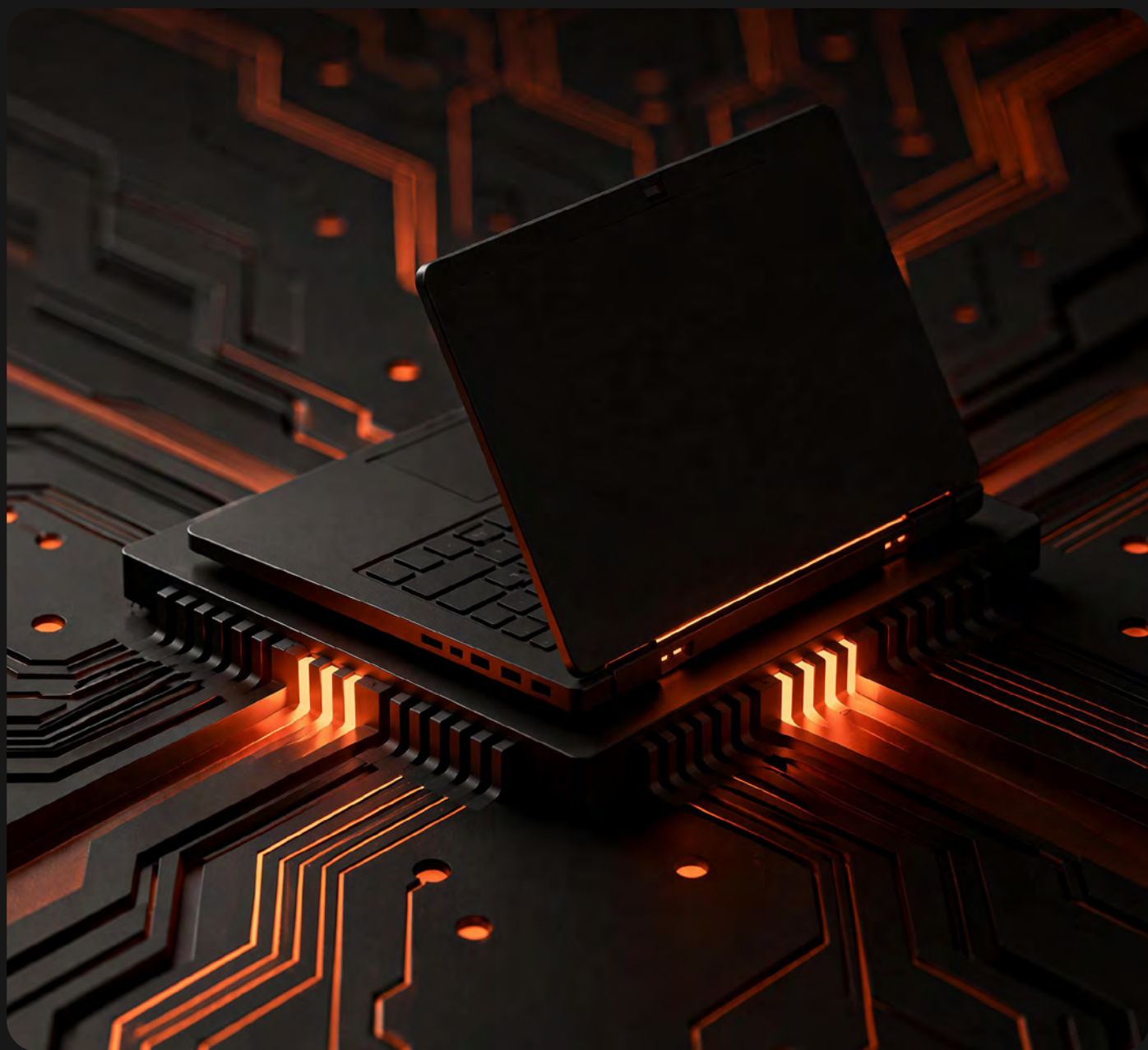
Защита парольных хранилищ:

- Для централизованных менеджеров паролей: размещайте базы данных на изолированных серверах, ограничьте доступ к ним по сети, включите многофакторную аутентификацию для входа в консоль администратора и просмотра хранилищ.
- Для браузерных хранилищ: запретите сохранение паролей в браузерах через групповые политики.

04

Общие меры:

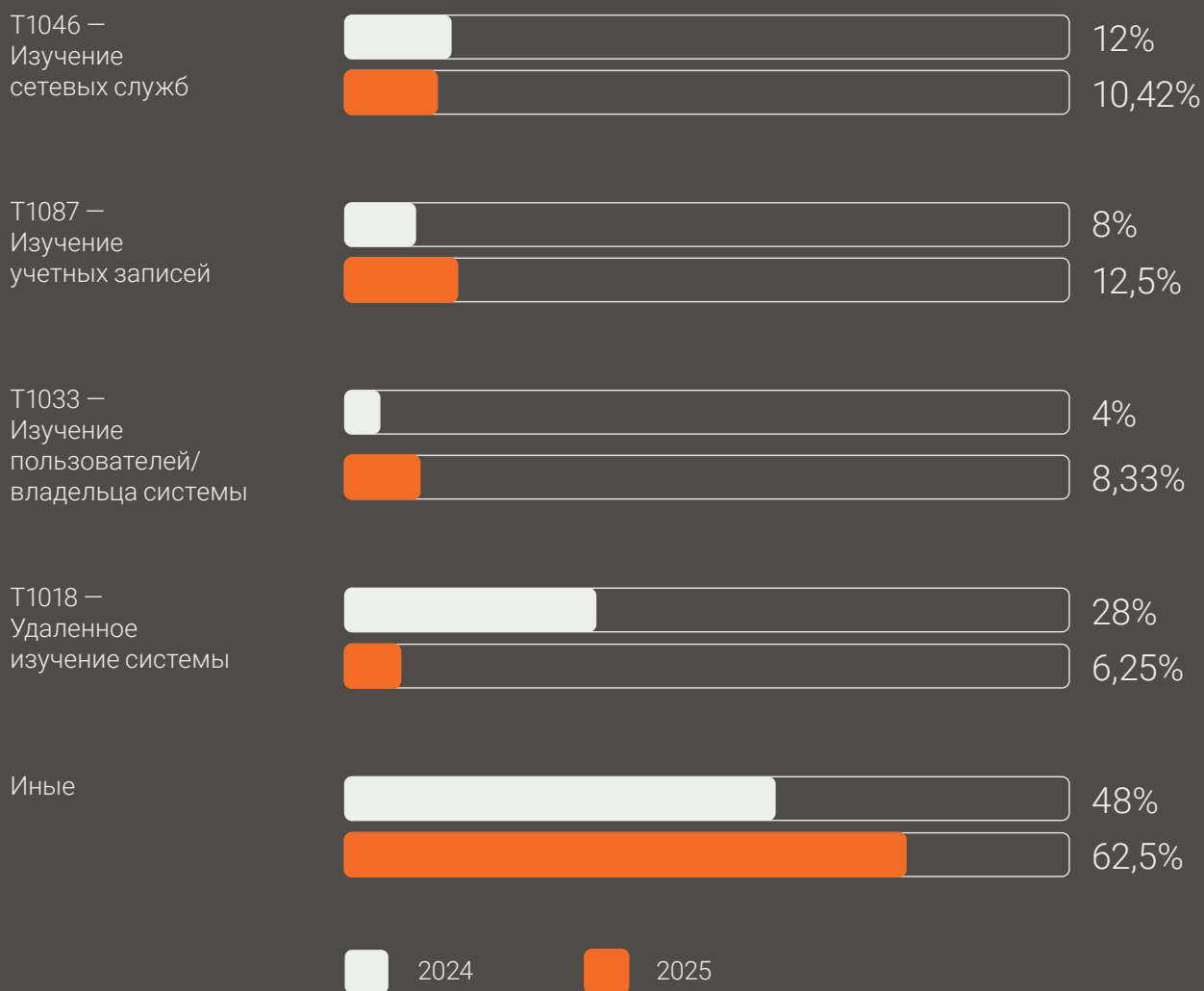
- Внедрите многофакторную аутентификацию для всех критичных систем — даже при краже пароля злоумышленник не сможет его использовать без второго фактора.
- Сегментируйте сеть и применяйте принцип наименьших привилегий: учетная запись пользователя должна иметь доступ только к тому, что ему необходимо для работы.
- Регулярно проводите тренировки для сотрудников по безопасному обращению с паролями.



ИЗУЧЕНИЕ ВНУТРЕННЕЙ ИНФРАСТРУКТУРЫ

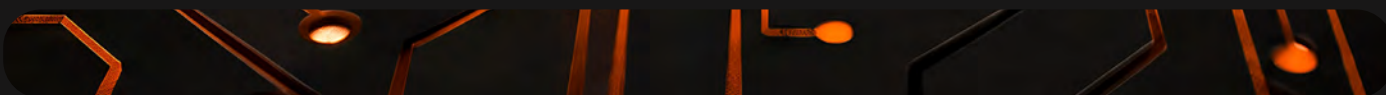


Диаграмма 14. Распределение выявленных техник в рамках тактики изучения внутренней инфраструктуры



Большое количество доступных для использования инструментов и встроенных возможностей операционной системы способствует разнообразию техник в разделе «Изучение внутренней инфраструктуры (Discovery)». Попав в неизвестную инфраструктуру, атакующим нужно получить максимум полезной информации о своей жертве.

Чаще всего злоумышленники использовали процедуры, которые позволяли отдать список служб на удаленных устройствах инфраструктуры, информацию о пользователях и их правах в системе, а также контекст используемой учетной записи. Последнее, с пресловутыми командами вроде `whoami` и `quser`, часто применяется в случаях успешной эксплуатации уязвимой системы, но безусловно не ограничивается этим примером.



Fscan, **netscan** и другие инструменты хороши за счет своей многофункциональности, которая давно не ограничивается только сканированием портов. Полученные результаты позволяют злоумышленникам планировать дальнейшие действия по компрометации новых систем.

При этом в нашей практике нападающие не сильно стремятся к какой-либо скрытности на этапе изучения внутренней инфраструктуры в сравнении с другими этапами жизненного цикла атаки. Можно было бы предположить, что причина кроется в уверенности в беспрепятственности своих действий. И действительно, такие «крупницы» просто тонут в потоке легитимных команд, создавая для защитников дополнительные вызовы.

Также важна уверенность атакующих в своих навыках и скорости. Низкий уровень зрелости процессов информационной безопасности многих жертв не позволяет им эффективно противостоять современным злоумышленникам.

Значительная доля случаев была отнесена нами к категории «Иные». В ней сложно выделить какие-то ключевые техники, помимо уже описанных. В ряде инцидентов поиск информации в системах позволял не только найти учетные данные из текстовых файлов к другим системам, но и конфиденциальные сведения, которые использовались для шантажа жертв. Иногда злоумышленники проявляли изобретательность, стараясь мимикрией запутать расследование.



В целом, высокий процент техник в категории «Иные» только подчеркивает всю вариативность тактики, которая сформировалась путем комбинирования зарекомендованных временем специализированных инструментов вместе с административными средствами.

ПРИМЕР ИНЦИДЕНТА

Часто злоумышленникам не удается сразу получить повышенные привилегии на скомпрометированной системе. В таких случаях некоторые из них прибегают к использованию различных инструментов, например, **winPEAS** и **PowerUp.ps1**, позволяющих в автоматизированном режиме выявить слабые места. С упрощением поиска для атакующих облегчается и работа для защитников: множество написанных сигнатур, большой шум при работе и характерность поведения. Поэтому иногда атакующие идут по другому пути и используют ручной поиск.

В одном из инцидентов мы столкнулись с реализацией техники T1518 «Изучение установленного ПО» (Software Discovery). В ходе компрометации Linux-сервера злоумышленники использовали штатные средства пакетного менеджмента, чтобы определить наличие библиотеки **polkit**, позволяющей непривилегированным процессам выполнять действия с административными правами.

```
dpkg -s policykit-1  
rpm -q polkit
```

Также они анализировали журнал изменений пакета `rolkit` на наличие упоминаний CVE-2021-4034 (**PwnKit**). Все это — не попытка эксплуатации как таковая, а подготовительный этап: прежде чем переходить дальше, злоумышленник убеждается, что цель действительно уязвима.

Это очень хороший пример, показывающий, что даже «простые» команды могут быть частью серьезной цепочки атаки, и требующий от защитников отдельного внимания при мониторинге инфраструктуры на Unix-системах.

ХАНИПОТЫ КАК СПОСОБ ВЫЯВЛЕНИЯ РАЗВЕДКИ

Как уже было сказано в этом разделе, сложность обнаружения атаки на этапе изучения внутренней инфраструктуры заключается в фильтрации событий среди большого объема легитимной активности персонала компании. Даже при наличии развитого мониторинга, аналитики каждый раз будут оказываться в ситуациях, требующих уточнения правомерности действий со стороны пользователей. Один из вариантов решения проблемы этапа «Discovery» заключается в использовании, так называемых, «приманок» и «ловушек», сработки на которых позволят вам сфокусировать внимание при обнаружении нелегитимных действий. Эффективная борьба защитников достигается не за счет обнаружения техник разведки, а за счет обнаружения их на ложных целях.

- **Локальные учетные записи и группы в Active Directory**

В качестве вариантов размещения можно использовать фиктивные учетные записи и группы с повышенными привилегиями. Очевидно, что имена таких аккаунтов должны быть правдоподобными и соответствовать политике именования учетных записей в организации. Учитывая популярность действий злоумышленников, связанных с поиском информации о пользователях системы, такие приманки могут быть наиболее эффективными.

- **Файлы-приманки**

Отслеживание событий с Event ID 4656, 4663 и подобных на дисках файлового сервера будет выдавать колоссальную нагрузку. Альтернативой этому можно предложить точечный аудит файлов, который будет связан с приманками. Пароли.txt, secret.txt и подобные названия находятся злоумышленниками с периодичной успешностью и действительно используются в инцидентах. Почему бы не применять это против злоумышленников?

- **Фальшивые сетевые ресурсы**

Ориентированы на выявление массовых сканирований со стороны злоумышленников. Важно помнить, что доступ к таким ресурсам не должен вызывать ошибок, при этом реальными пользователями такие ресурсы не должны использоваться.

Принцип размещения фальшивых сетевых ресурсов должен соответствовать правдоподобности приманок: отсутствие искусственных мест, создание правдоподобной картины, точечное размещение вместо широковебательного. Также важно помнить, что любая ловушка должна быть безопасной для инфраструктуры, а значит в ней не должны присутствовать реальные секреты, связи с какими-либо критическими системами.

ПЕРЕМЕЩЕНИЕ ВНУТРИ ПЕРИМЕТРА

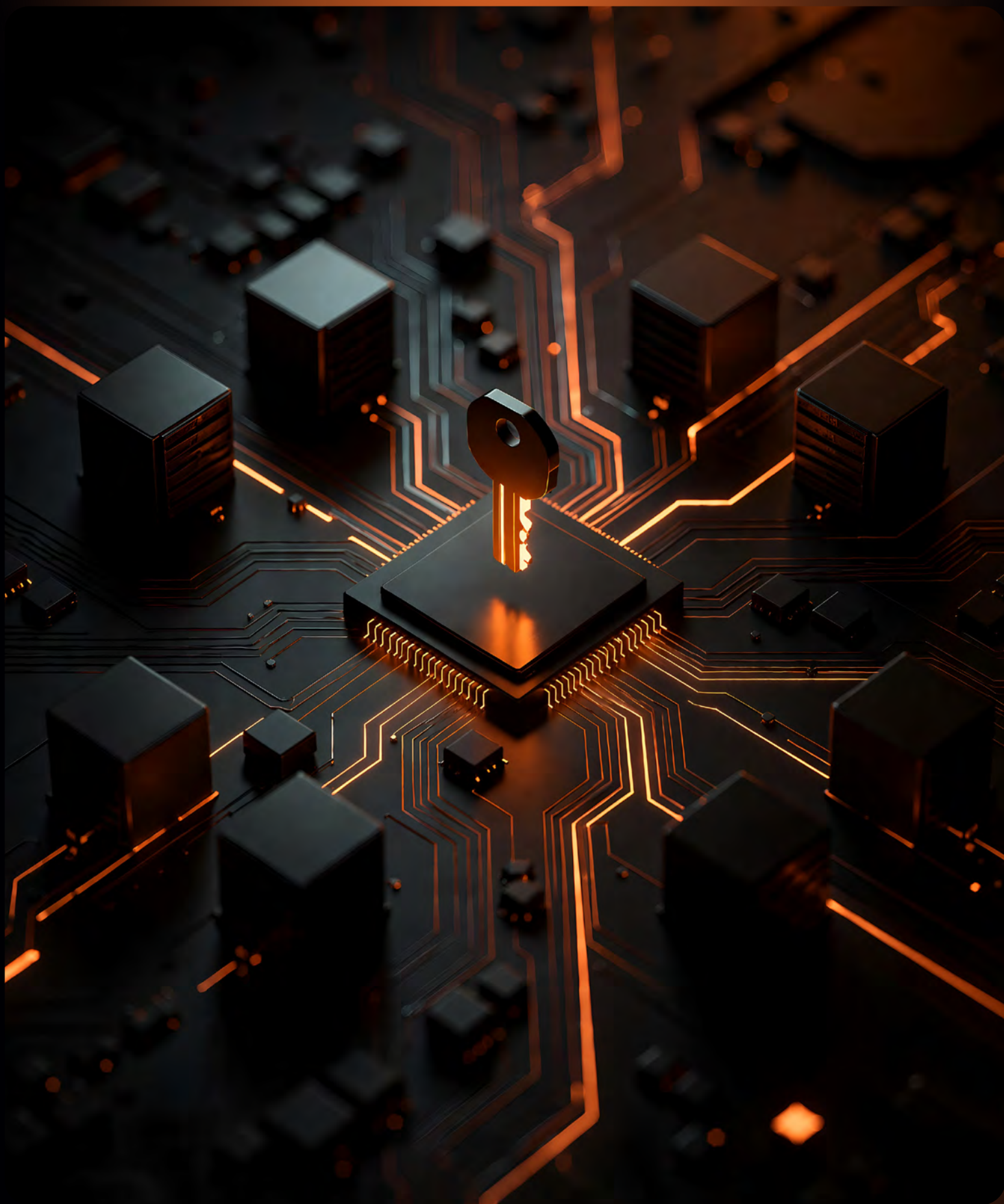
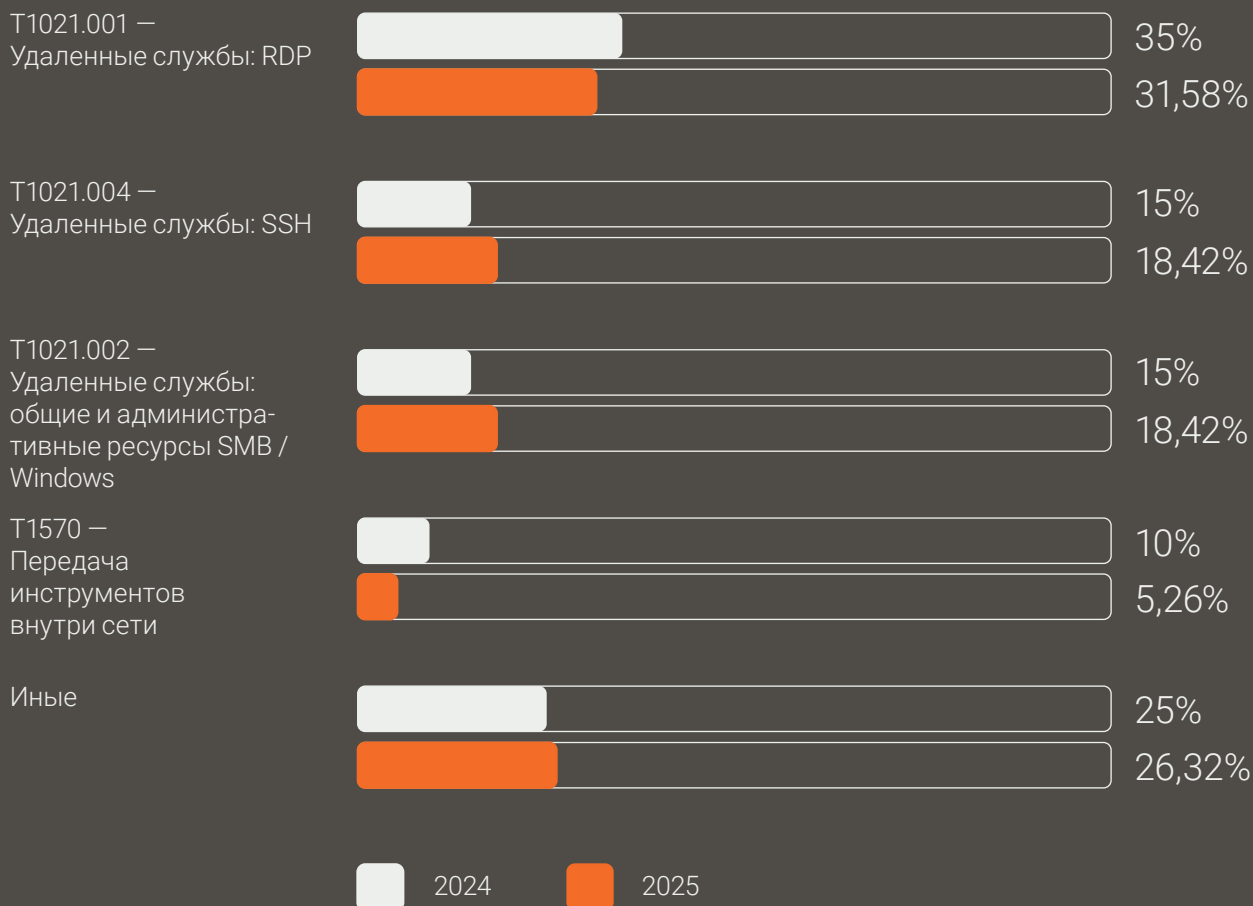


Диаграмма 15. Распределение выявленных техник в рамках тактики перемещения внутри периметра



На этапе перемещения внутри периметра организации (Lateral Movement) злоумышленники стремятся решить ряд задач по эскалации своих привилегий и дальнейшему распространению. Если до этого компрометация одного узла являлась единичным успехом, то начиная с данного этапа злоумышленники проводят полноценную операцию.

Стремление максимально быстро обнаружить и получить доступ к критическим узлам вытекает и из мотивации атакующих. Как следует из ландшафта киберугроз, в большинстве своем злоумышленники стремятся получить выкуп от организаций после атак. Соответственно, атакующим нужно в кратчайшие сроки подвергнуть инфраструктуру компании шифрованию и перейти

к следующей жертве. Кроме того, более долгое присутствие — большой риск обнаружения и противодействия. Поэтому выбор методов и инструментов сводится к использованию стандартных протоколов и хорошо известных утилит, использующихся повсеместно.

Сохраняется консервативное преобладание техник, нацеленных на платформы под управлением операционной системы Windows. Такой трафик выглядит идентично легитимному, а значит создает для защитников вызовы для поиска других поведенческих маркеров. Архитектуры большинства корпоративных сетей строятся вокруг централизованной модели с использованием контроллеров домена на базе Active Directory.

На практике нам не доводилось встречать компании, которые используют только Unix-подобные системы, а значит проблема защиты платформ на базе Microsoft будет еще долго актуальна. При этом важно не столько разнообразие операционных систем, используемых в компаниях, сколько скорость передвижения злоумышленников с ключевых узлов (где будут добываться необходимые привилегии) до централизованной платформы распространения программного обеспечения (групповые политики, SCCM, административные панели антивирусной защиты). Достижение таких объектов позволяет злоумышленникам масштабировать воздействие на максимально возможное количество систем.

На данном этапе превалируют такие инструменты как **Impacket** с его набором Python-скриптов и **NetExec** (улучшенная реализация инструмента CrackMapExec). Это популярные средства, известные благодаря наличию широкого функционала, который позволяет выполнять команды на удаленных

системах с использованием аутентификационных данных, полученных на предыдущих этапах атаки. При взаимодействии с сетевыми ресурсами особо полюбился атакующими и **PAExec** за быстроту и стабильность. По сравнению с утилитой PsExec он использовался заметно чаще.

Как и ранее, мы сталкивались с реализацией техники, связанной с протоколом **WinRM**. Несмотря на то, что она не нашла отражения на графике, в 2025 году злоумышленники использовали данный протокол в 13% инцидентов. В качестве инструмента атакующие чаще прибегали к **Evil-WinRM** с широкими возможностями интерактивной оболочки PowerShell, передачей файлов и другими полезными функциями. Сетевая сегментация, использование принципа минимальных привилегий, ротация и уникальность паролей, отключение функций, не требующих использования в системах, — все это эффективные методы для создания барьеров на пути перемещения злоумышленников.

ПРИМЕР ИНЦИДЕНТА

Нам, как специалистам по реагированию, всегда нужно быть готовым и к редким случаям применения данной тактики для оперативного расследования инцидентов. Однажды мы столкнулись с использованием внутреннего фишинга как способа передвижения внутри сети.

Все начиналось как по методичке. В качестве вектора первоначального проникновения атакующие использовали перебор паролей у учетных записей на почтовом сервере организации, где отсутствовала мультифакторная аутентификация.

Получив доступ к ряду почтовых ящиков пользователей, злоумышленники принялись рассылать фишинговые письма с тщательно продуманной легендой.

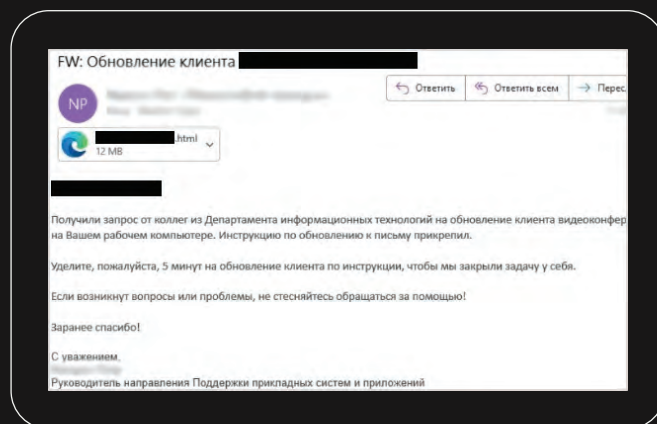


Рис. 7. Пример фишингового письма

Во вложении к письму содержался HTML-документ, в теле которого находился обфусцированный JavaScript-код. При открытии HTML-документа выполнялась загрузка архива, который содержал вредоносный файл типа бэкдор, на системы жертв. Вредоносное программное обеспечение мимикрировало под средство обновления системы видеоконференцсвязи. Кроме полезной нагрузки, ВПО содержало часть, отвечающую за отрисовку графического интерфейса приложения, где, якобы, отображалось обновление приложения и тем самым отвлекало внимание пользователей.

В результате такой активности злоумышленникам удалось оперативно распространить свое присутствие на нескольких системах заказчика.

ВЫЯВЛЯЕМ УСПЕШНЫЕ ПОДКЛЮЧЕНИЯ ПРИ ИСПОЛЬЗОВАНИИ RDS

Возможно, вы пропустили наш [Telegram-пост](#) о событиях при RDP-соединении, которые помогут вам в расследовании RDP-подключений в инцидентах, когда злоумышленники удалили ряд ценных журналов. Предлагаем разобраться с основными событиями в журналах службы удаленного рабочего стола (RDS) при удачном подключении пользователя.



Telegram-канал
Angara Security.
Публикация про RDP

RDS (Remote Desktop Services) — это серверная платформа Windows для централизованного представления удаленных рабочих столов. Как правило включает в себя:

- портал входа (**RD Web Access**) – средство, через которое пользователи проходят аутентификацию для предоставления сеанса удаленного рабочего стола;
- шлюз входа (**RD Gateway**) — предоставление пользователям из общедоступных сетей доступа к рабочим столам, часто располагается с ролью RD Web Access;
- брокер подключений (**RD Connection Broker**) — система, отвечающая за управление входящими подключениями к удаленному рабочему столу. Направляет пользователей на подходящий сервер;
- наконец одна или более систем (**RD Session Host**), которые предоставляют сессию для пользователей. Такие точки очень удобны для злоумышленников как основной плацдарм для дальнейшего перемещения внутри сети.

Исследование начинается с анализа журналов RD Web Access, где фиксируются первые успешные прохождения аутентификации пользователя через веб-ресурс.

На шлюзе можно увидеть выполнение политики авторизации подключения и выдачи доступа к ресурсу. Здесь же можно увидеть IP-адрес злоумышленника, который подключился к инфраструктуре. Из журналов брокера подключений важны события, связанные с обработкой запроса на подключение, где будет отмечен ресурс, к которому пользователь сможет подключиться.

Анализ фактического входа в рабочую сессию на конечном узле (RD Session Host) не сильно отличается

от анализа целевой системы с классическим RDP-доступом. Поэтому читатели могут обратиться к вышеупомянутому посту из Telegram канала.

Дополнительно отметим лишь журнал Microsoft-Windows-User Profile Service/Operational, в котором указываются события загрузки профиля пользователя в Event ID 5. После успешной аутентификации пользователя в системе начинается инициализация профиля и возникает соответствующая сессия.

КЛЮЧЕВЫЕ СОБЫТИЯ ДЛЯ ВЫЯВЛЕНИЯ УСПЕШНЫХ ПОДКЛЮЧЕНИЙ ПРИ ИСПОЛЬЗОВАНИИ RDS

Этап	Журнал	EventID	Ключевые поля	
			Название поля	XML-представление
RD Web Access				
Первичная аутентификация	Security.evtx	4624	Пользователь	Param1
			Тип входа	LogonType
RD Gateway				
Проверка доступа и установление канала	Microsoft-Windows-Terminal Services-Gateway/Operational.evtx	200	IP-адрес источника подключения	IpAddress
			Пользователь	Username
		300	IP-адрес источника подключения	IpAddress
			Пользователь	Username

Этап	Журнал	EventID	Ключевые поля	
			Название поля	XML-представление

RD Gateway

		302	IP-адрес источника подключения	IpAddress
			Пользователь	Username
		303	IP-адрес источника подключения	IpAddress
			Пользователь	Username
			Продолжительность сеанса	SessionDuration

RD Connection Broker

Назначение целевой системы	Microsoft-Windows-Terminal Services-SessionBroker/Operational.evtx	800	Пользователь	Param1
		801	Пользователь	Param1
			IP-адрес RD Session Host	param3
	Microsoft-Windows-Terminal Services-SessionBroker-Client/Operational.evtx	1307	Пользователь	Param2
			IP-адрес RD Session Host	param4

RD Session Host

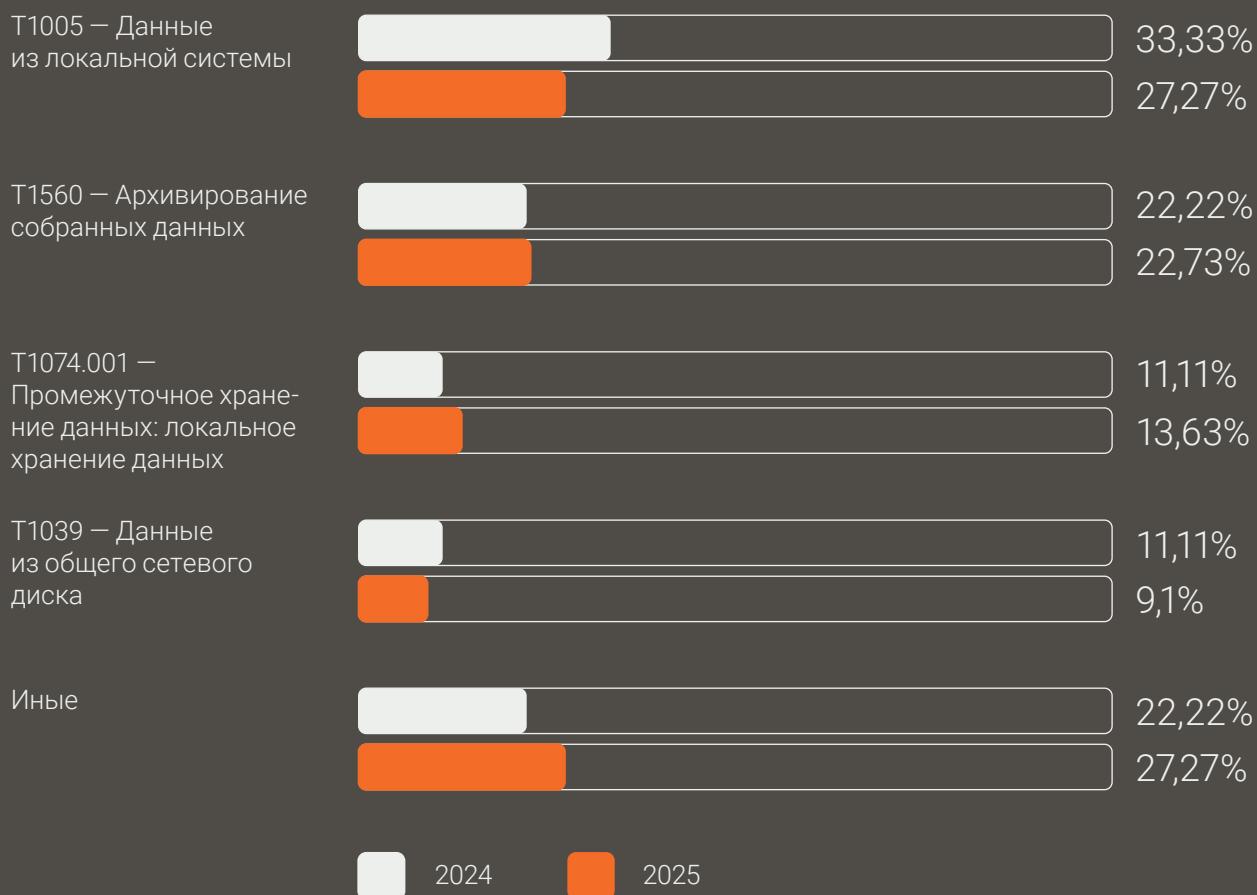
Интерактивный вход и выполнение действий	Microsoft-Windows-User Profile Service/Operational.evtx	5	Имя системы	Computer
			Пользователь	Security UserID
			Описание события	Data Name



СБОР ДАННЫХ



Диаграмма 16. Распределение выявленных техник в рамках тактики сбора данных



Основная активность злоумышленников на этапе сбора данных (Collection) была сосредоточена вокруг двух ключевых векторов: изъятие чувствительной информации с локальных систем и кража данных с сетевых дисков и общих ресурсов. Собранные данные перед эксфильтрацией практически всегда архивируются для удобства выноса и сокрытия структуры украденной информации.

Злоумышленники сканируют **локальные диски** в поисках файлов, представляющих ценность: текстовые файлы с паролями, офисные документы, файлы баз данных, переписки из мессенджеров и почтовых клиентов. Особое внимание уделяется папке с файлами сессии мессенджера Telegram.

После получения доступа к учетной записи пользователя, атакующие подключаются к **сетевым дискам и общим папкам** (SMB-шары, NAS-хранилища), чтобы собрать данные, доступные широкому кругу сотрудников. Целью становятся корпоративные документы, отчеты, базы знаний, резервные копии и общие файловые архивы.

Собранные файлы перед отправкой на подконтрольную атакующему систему **упаковываются в архивы**. Это позволяет объединить множество разрозненных файлов в один для удобства эксфильтрации и уменьшить объем передаваемых данных.

ПРИМЕР ИНЦИДЕНТА

В одном из инцидентов мы столкнулись с группировкой, специализирующейся на корпоративном шпионаже. Атакующие получили доступ к целевой инфраструктуре с помощью фишингового письма. Спустя время, когда злоумышленники подняли свой уровень привилегий в домене до уровня легитимных администраторов, они начали собирать почтовую корреспонденцию с интересующих их систем.

Для реализации сбора атакующие создали запланированную задачу с нагрузкой в виде PowerShell-сценария.

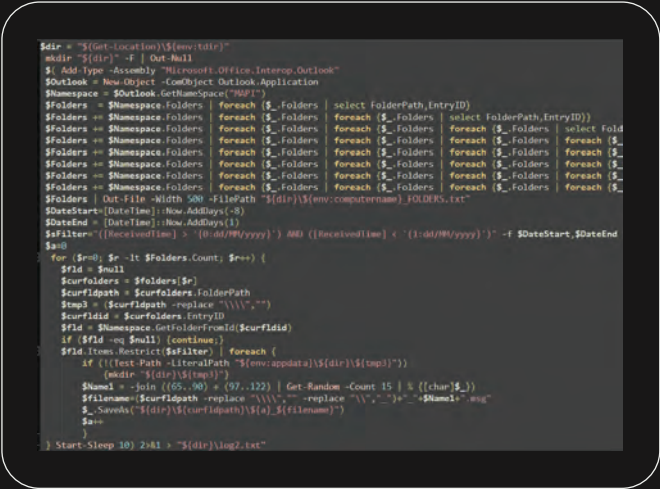


Рис. 8. Фрагмент полезной нагрузки PowerShell скрипта

Данная часть указанного PowerShell-сценария реализует выгрузку всех писем за последние 8 дней из всех папок пользователя, использующего приложение Outlook.

Еще одним источником для сбора информации стали сетевые диски, с них выгружались файлы аналогичным образом с помощью PowerShell-сценария и запланированных задач. Пример:

```
$($d1 =
((Get-Date).AddDays(-8)).ToString("yyyyMMdd"))

robocopy "Z:\<REDACTED>"
"\temp\<REDACTED>" *.* /MAXAGE:$d1
/XO /S /R:0 /W:0 /XF "Thumbs.db" "*~$*"
*.png *.ai *.mxf *.eps *.mov *.mp4
*.zip *.wmv *.jpg *.tif *.csv *.ipynb
*.7z | Out-File -FilePath
\temp\<REDACTED>)
```

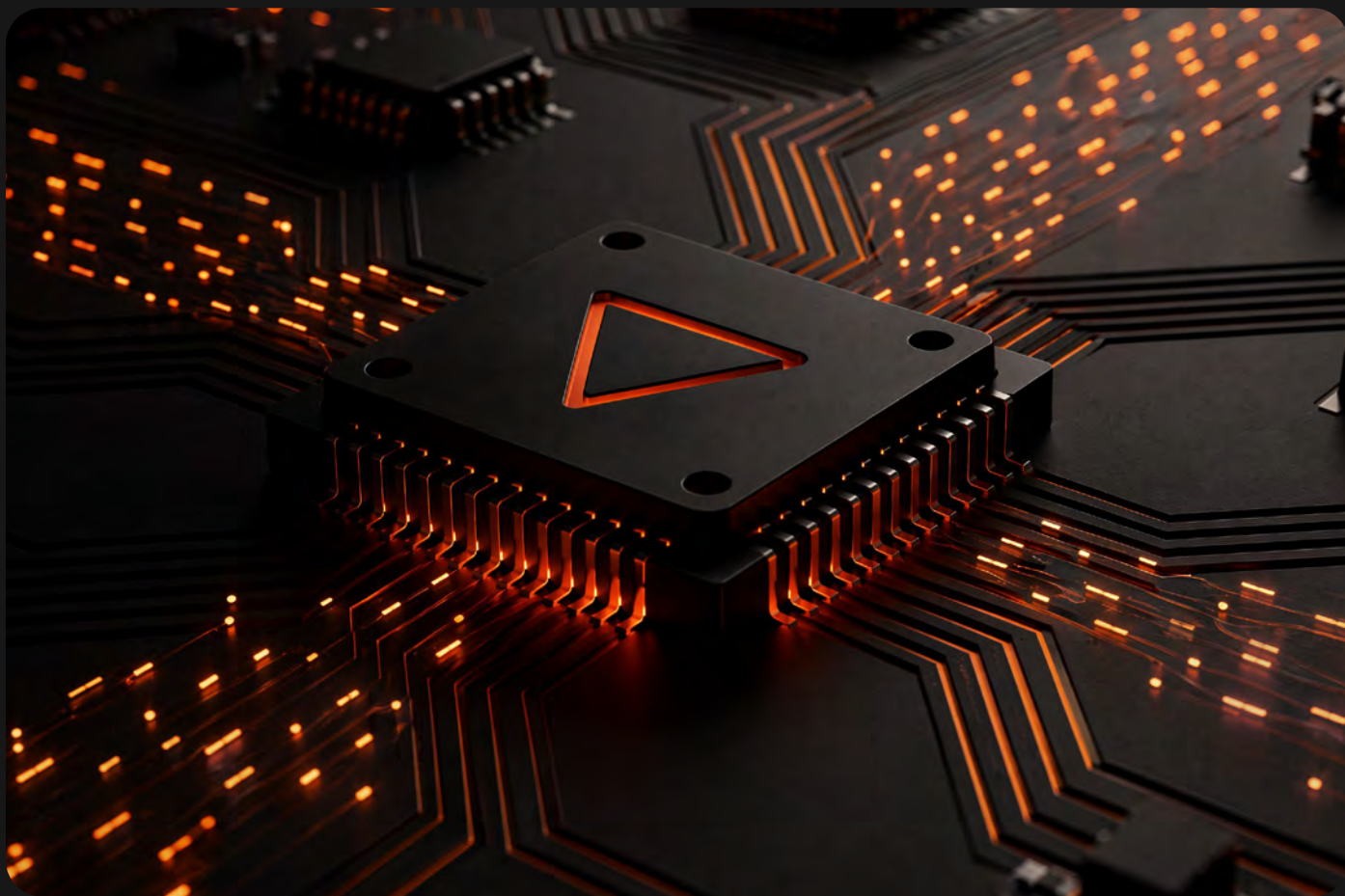
При выполнении вышеуказанный сценарий копирует содержимое каталога с сетевого диска на локальную систему. Перед этим сценарий проверяет, что файл был модифицирован не позднее восьми дней назад и имеет расширение, отличное от .png, .ai, .mxf, .eps, .mov, .mp4, .zip, .wmv, .jpg, .tif, .csv, .ipynb, .7z.

Таким образом, атакующий выгружал данные, пока его активность не была случайно обнаружена ИТ-администратором. Этот инцидент послужил поводом для обращения в Angara MTDR.



КАК БОРОТЬСЯ ПРОТИВ НЕСАНКЦИОНИРОВАННОГО СБОРА ДАННЫХ

- Отслеживайте аномальное количество обращений к файловым ресурсам за короткий промежуток времени.
- Контролируйте доступ к сетевым дискам со стороны необычных процессов.
- Отслеживайте запуск специализированных утилит для копирования данных типа Robocopy, Rsync и т.д.
- Храните особо ценные данные в зашифрованном виде. Даже при успешном копировании атакующий не сможет их прочитать без ключа шифрования.
- Используйте DLP-системы, они хорошо подходят для контроля перемещения чувствительных данных, а также для обнаружения попыток массового копирования или архивации.
- Обращайте внимание на создание архивов больших объемов, а также на архивацию большого количества офисных документов или каталогов с ними на рабочих станциях.



УДАЛЕННОЕ УПРАВЛЕНИЕ СИСТЕМОЙ

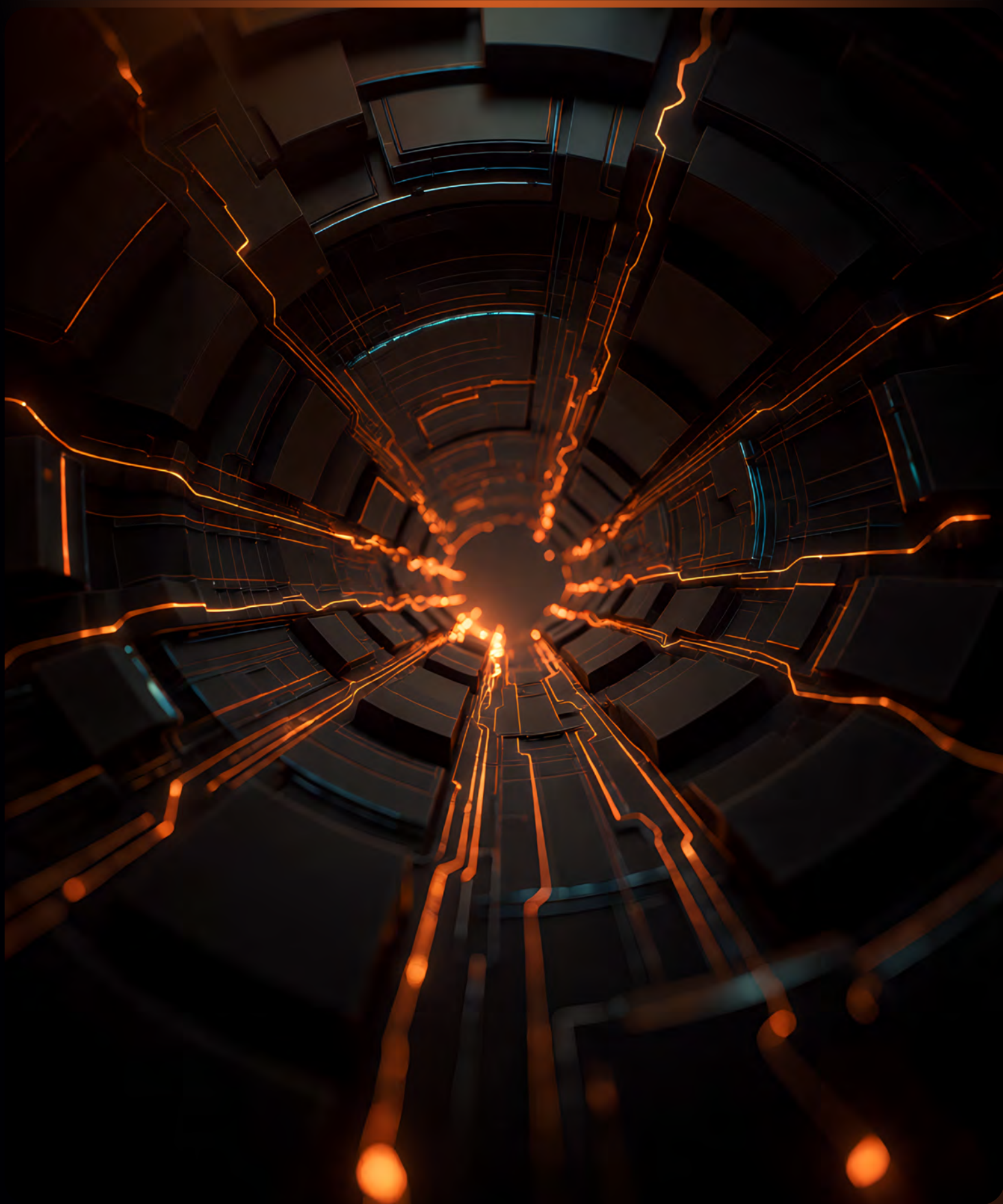
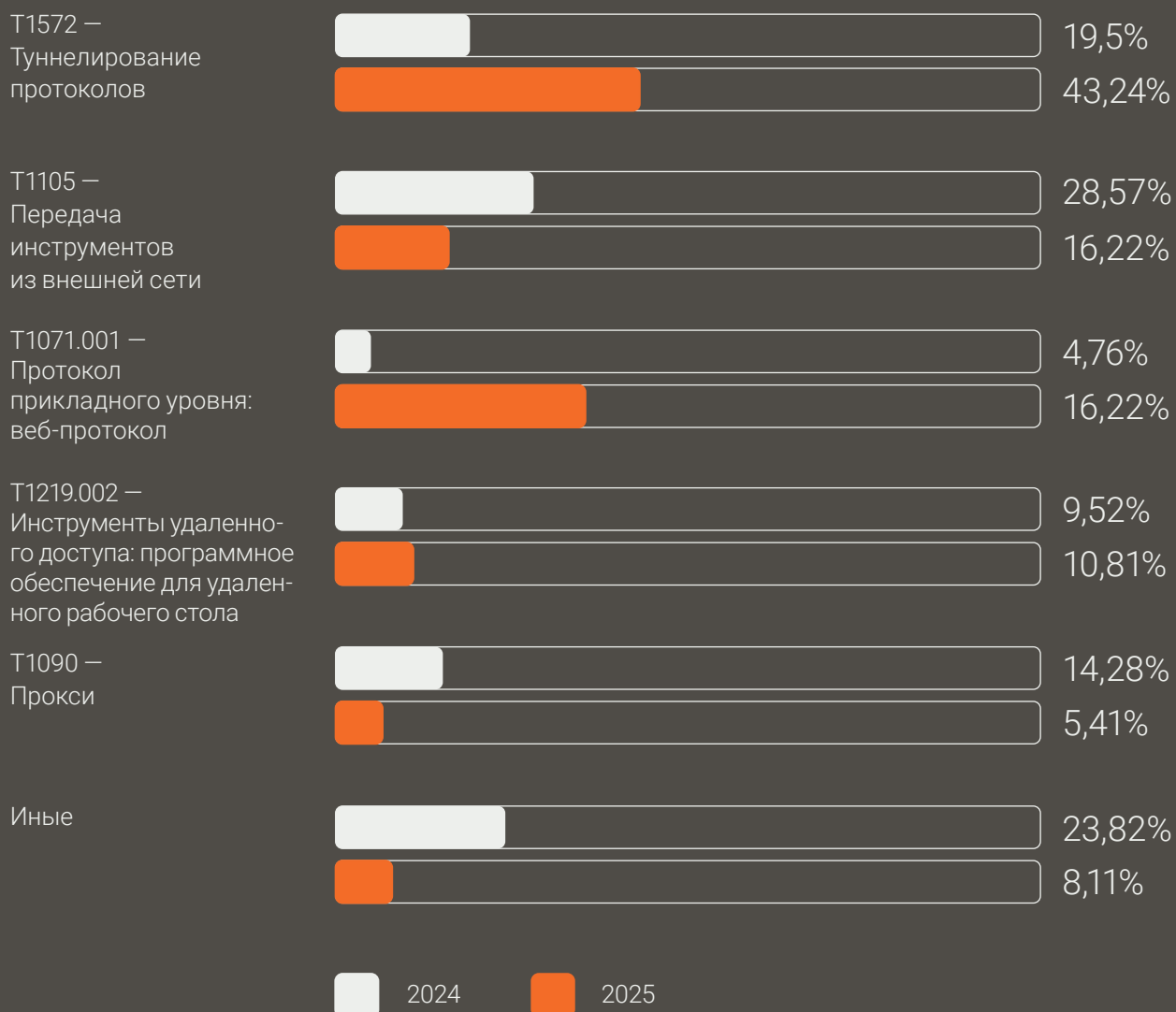


Диаграмма 17. Распределение выявленных техник в рамках тактики удаленного управления системой



Распространенность туннелирующих инструментов в 2025 году существенно возросла по сравнению с предыдущим годом. Такая популярность обусловлена простотой развертывания и использования в скомпрометированных системах, а также эффективностью скрытой работы на уровне сетевой телеметрии за счет использования обычного веб-трафика и легитимных сервисов.

При этом пик активностей таких инструментов как **gsocket** и **ngrok** в наших расследованиях выпал именно на первую половину 2025 года. Заметный спад использования произошел после того, как инфраструктура некоторых сервисов стала недоступна в России из-за введенных санкций, тогда как другие инструменты к этому моменту были хорошо описаны в сообществе, что позволило большому числу лиц превентивно противодействовать злоумышленникам.

Атакующие адаптировались к трудностям. Менее известные ранее утилиты, такие как **localtonet**, **cloudflared**, SOCKS-подобные инструменты типа **SocksOverRDP** и, наконец, **devtunnel**, который до этого практически не появлялся в инцидентах, пришли на смену ранее доминировавшим инструментам.

Мы рекомендуем блокировать инфраструктуры такого рода средств на сетевом периметре, если вы не используете их в рабочих задачах.

Название	Домен
Gsocket	*.gsocket.io *.gs.thc.org
Localtonet	*.localtonet.com *.localto.net
Devtunnel	*.devtunnels.ms

Таблица 2. Домены туннелирующих инструментов, которые потенциально могут использоваться злоумышленниками

Альтернативой туннелирующих утилит для злоумышленников часто служили инструменты удаленного доступа и RMM (Remote Monitoring and Management). **AnyDesk**, **MeshAgent** стоят особняком среди прочих, но нам встречались **Radmin** и **Tactical RMM**. Последний был использован группировкой **THOR** как резервный инструмент постоянного доступа к скомпрометированной инфраструктуре одного из заказчиков. Никуда не пропали и различные фреймворки постэксплуатации вроде **Cobalt Strike**. Они имеют низкий порог вхождения благодаря хорошей описанной документации, стабильны, относительно скрытны и решают большинство задач после первичного проникновения. Но и для них существуют способы обнаружения. Поэтому, кроме хорошо известных инструментов в этой категории, появляются и новинки. Осенью 2025 года в расследованном инциденте мы впервые столкнулись с полезной нагрузкой от **AdaptixC2**, для которой существует гораздо меньше всевозможных сигнатур. Это говорит о поиске со стороны атакующих более эффективных инструментов.



Не Cobalt Strike и не Brute Ratel: почему злоумышленники выбрали AdaptixC2, и как его обнаружить

Однако в целом существенных перемен за прошедший год в техниках этапа «Управление системой» не произошло. Безусловно, некоторые злоумышленники использовали и менее распространенные техники: алгоритмы генерации доменов (DGA), резервные каналы связи. Такие методы требуют от атакующих больших финансовых и временных затрат. Зачем прибегать к ним, если есть доступная инфраструктура туннелирующих утилит, хорошо проверенных временем? Большая часть изменений в статистике, скорее, связана с локальными особенностями инфраструктур организаций и примененным инструментарием на предыдущих этапах атаки, чем с новыми тенденциями у злоумышленников.

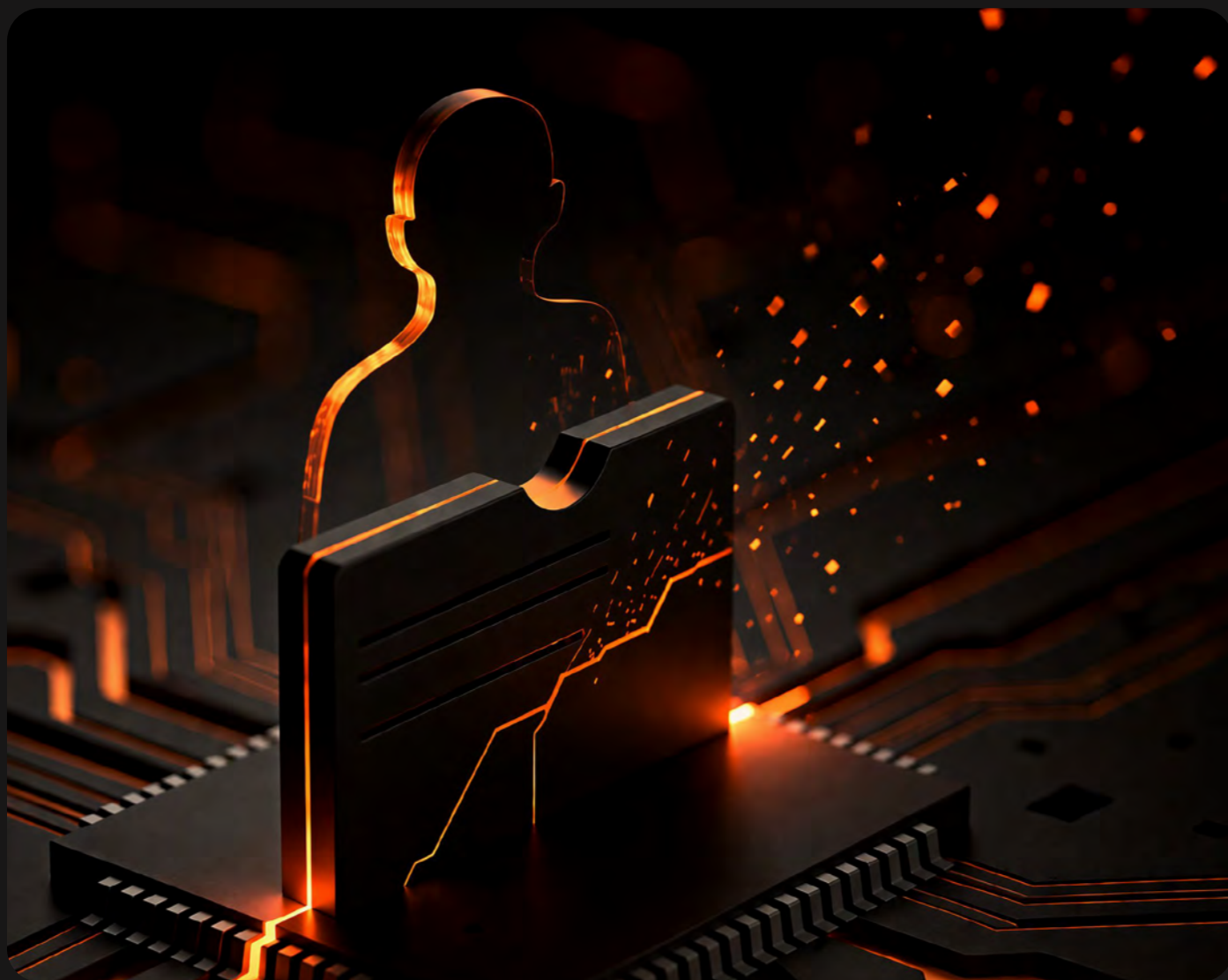
ПРИМЕР ИНЦИДЕНТА

В конце 2025 года мы столкнулись с атакой неизвестного злоумышленника, который подключился к инфраструктуре жертвы из сферы здравоохранения с помощью учетной записи подрядчика. В ходе атаки злоумышленник создал несанкционированную базу в прикладном программном обеспечении «1С:Предприятие» для возможности выполнения кода с повышенными привилегиями. Для закрепления в системе атакующий использовал инструмент удаленного доступа Mesh Agent. Здесь интересен именно конфигурационный файл агента. В нем содержался идентификатор самого подрядчика, через которого было инициировано подключение:

```
MeshName=<REDACTED>
```

В дальнейшем злоумышленник попытался перебрать пароли учетных записей организации.

К счастью, заказчик вовремя заметил нелегитимные действия и пресек дальнейшую эскалацию инцидента.



АЛЬТЕРНАТИВНЫЕ СПОСОБЫ БЛОКИРОВКИ ВРЕДОНОСНОГО C2

Реагируя на инциденты, порой мы сталкиваемся с техническими ограничениями по блокировке найденных вредоносных C2-адресов из-за отсутствия межсетевого экрана в организации заказчика. Блокировка сетевой инфраструктуры атакующих позволяет оперативно ограничить распространение инцидента внутри организации, разорвать соединение текущих сеансов, снизить риск повторной компрометации и обеспечить дополнительное время для анализа затронутых систем.

Нам бы хотелось предложить 4 альтернативных способа эффективного противодействия в таких ситуациях:

- Блокировка на уровне DNS.

Используя управление разрешением доменных имен, мы ограничиваем взаимодействие между инфраструктурой и подконтрольными злоумышленникам доменами. Техническая реализация осуществляется с помощью добавления локальной DNS-записи, указывающей на несуществующий IP-адрес. Например, loopback-адрес 127.0.0.1.

Важно убедиться, что все DNS-запросы к заблокированным доменам будут журналироваться

01

Открыть меню «Start» > «All Programs» > «Administrative Tools» и запустить оснастку DNS.

02

В открывшейся консоли выбрать «DNS server», на котором планируется настроить DNS debug logging, нажать правую клавишу мыши и выбрать «Properties».

03

В открывшемся окне выбрать закладку «Debug Logging».

04

Выбрать «Log packets for debugging», поставив галочку в чек-боксе, затем выбрать необходимые опции для записи событий в журнал аудита (рекомендуется оставить опции, отмеченные по умолчанию):

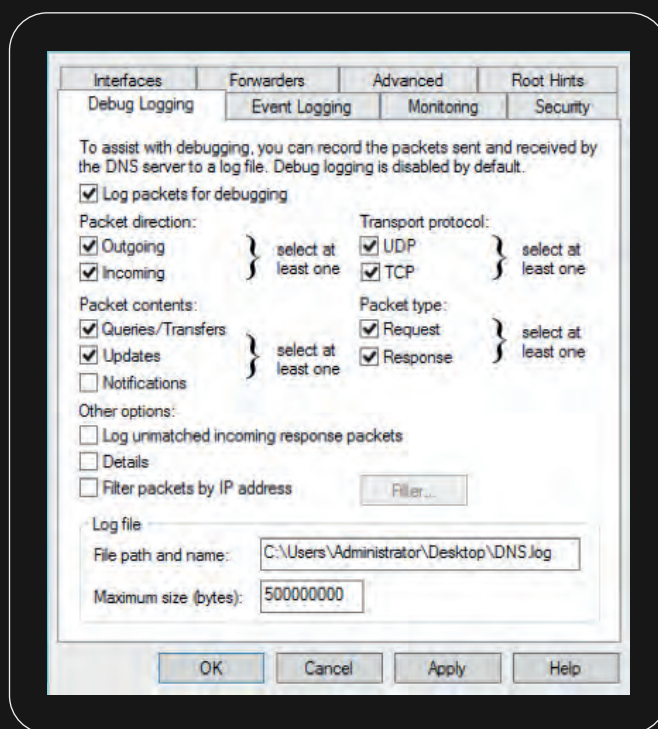


Рис. 9. Окно с настройками DNS debug logging

Важно помнить, что на системах в конфигурации DNS-сервера должен быть указан только тот сервер, который выполняет функцию блокировки домена. Ряд конечных точек может взаимодействовать с вредоносными доменами, используя DNS-кэш. В таких случаях его необходимо предварительно очистить.

При отсутствии доменной инфраструктуры можно воспользоваться системным файлом `hosts`, который отвечает за ручное сопоставление доменного имени с IP-адресом.

Примеры расположения:

```
C:\Windows\system32\drivers\etc  
/etc/hosts
```

- Блокировка на локальном межсетевом экране системы.

Используя локальные межсетевые экраны на конечных устройствах, мы ограничиваем сетевое взаимодействие с вредоносной инфраструктурой на уровне самой системы. Техническая реализация достигается за счет добавления правил на входящие и исходящие соединения в такие решения, как Брандмауэр Windows, `iptables`, `nftables`, `UFW`. Такой подход будет полезен в том числе в случаях, когда С2 используют напрямую IP-адреса, а также как дополнительный уровень защиты поверх реализации DNS-блокировки.

- Блокировка с помощью АВПО.

Антивирусное программное обеспечение (АВПО) — один из самых популярных типов средств защиты, который почти всегда установлен у заказчиков. Добавление правил на такое решение схоже с локальной реализацией, но предоставляет преимущество в виде централизованного распространения.

- ACL на маршрутизаторах.

Если в компании может не быть межсетевого экрана, то сетевое оборудование обязано существовать для корректной маршрутизации внутри организации. Сетевые маршрутизаторы и их списки контроля доступа (ACL) позволяют блокировать соединения уже на уровне сети. Зная ряд вредоносных IP-адресов, можно гибко блокировать С2-инфраструктуру и не давать доступ к целевым сегментам, не полагаясь на разрешение доменных имен.



ЭКСФИЛЬТРАЦИЯ ДАННЫХ

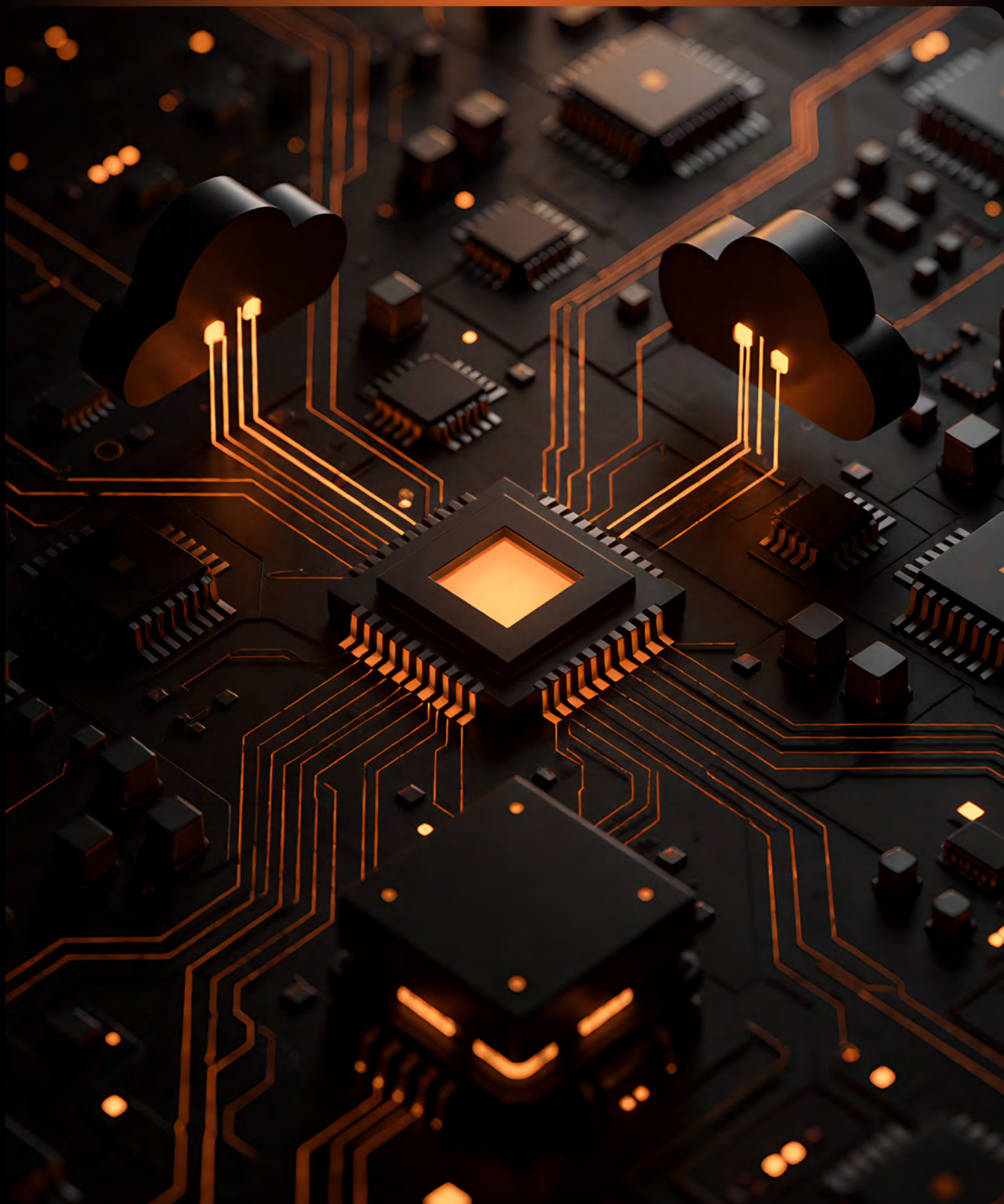
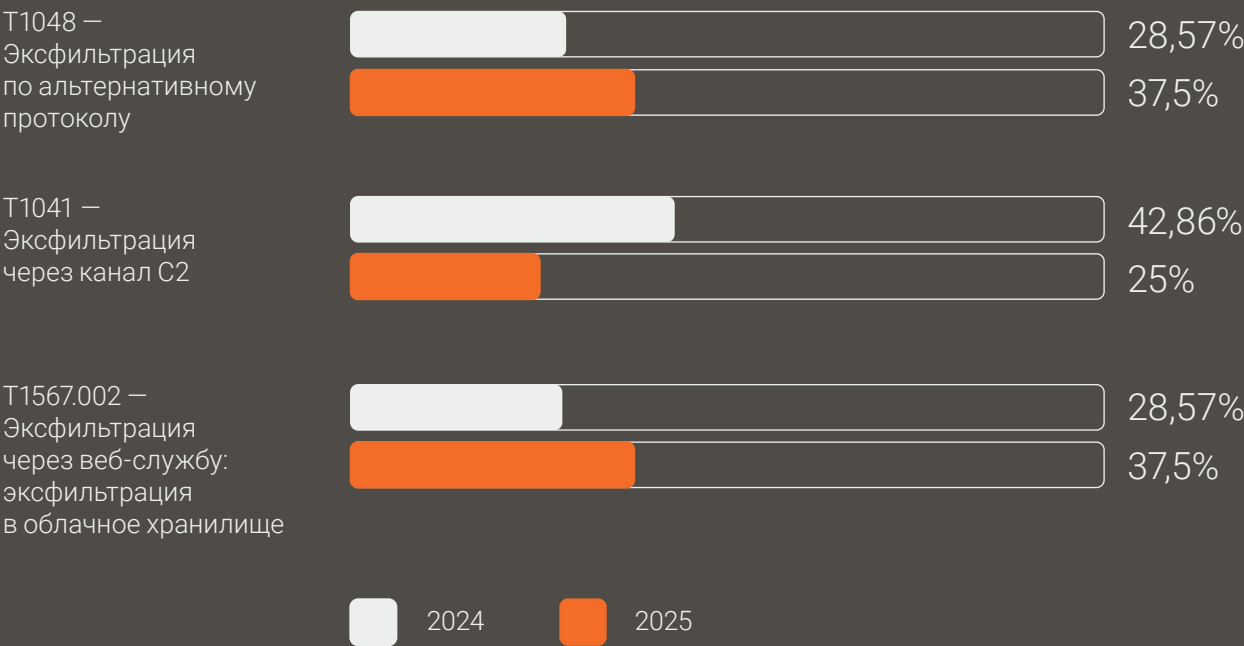


Диаграмма 18. Распределение выявленных техник в рамках тактики эксфильтрации данных



Анализ инцидентов 2025 года показывает изменение предпочтений злоумышленников на этапе эксфильтрации данных (Exfiltration). Наблюдается устойчивый рост доли техник, связанных с использованием легитимных облачных сервисов и альтернативных протоколов, в то время как доля эксфильтрации непосредственно через каналы C2 снижается. Выбор в пользу легитимных облачных сервисов, трафик к которым реже вызывает подозрения у средств защиты, демонстрирует осознанный подход атакующих к этапу эксфильтрации.

В ходе реагирований наша команда фиксировала целенаправленную выгрузку следующих категорий данных:

- Аутентификационный материал:** злоумышленники выгружали ключи реестра SAM, SYSTEM, SECURITY для извлечения хешей локальных учетных записей, а также базу данных ntds.dit для компрометации всех доменных учетных записей. Кроме того, отмечался интерес кластера **Bearlyfy**,

известного как Laboo.bo0, к конфигурационным файлам .rdg (Remote Desktop Connection Manager), содержащим параметры подключений к удаленным рабочим столам, а также кластера BO Team к приватным ключам SSH (id_rsa) для обеспечения бесшовного доступа к *nix-системам.

- Почтовые данные:** в средах Microsoft Exchange фиксировалась выгрузка писем (вместе с вложением) в .msg-файлы, а также целых почтовых ящиков в формате .pst. В том числе использовался командлет New-MailboxExport-Request для экспорта почтовых ящиков в сетевые папки и последующей выгрузки на подконтрольный ресурс. Группировка **RedCurl** применила .bat-скрипты для автоматизированного сбора данных из Microsoft Outlook и выгрузки WebDAV-ресурсов.
- Файлы на сетевых дисках и базы данных:** мы наблюдали использование специализированных скриптов для поиска и выгрузки документов с определенными расширениями из заданных директорий. Отдельно стоит отметить атакованные

группой хактивистов **Silent Crow*** системы управления сайтом «1С-Битрикс». С использованием утилит Adminer и scp злоумышленники «дампчили» базы данных и выгружали их на подконтрольные ресурсы.

Сессии мессенджера Telegram: злоумышленники использовали специализированные PowerShell-скрипты для поиска и выгрузки папки tdata, содержащей файлы сессий, включая токены аутентификации, которые позволяют получить полный доступ к аккаунту жертвы.

Для выгрузки собранных данных применялся широкий спектр инструментов, от простых скриптов до специализированных утилит:

В 2025 году самой популярной утилитой для эксфильтрации в облачные хранилища стала **Rclone**.

* – признана экстремистской организацией, её деятельность запрещена на территории РФ.

Принцип работы Rclone заключается в синхронизации файлов между локальной системой и более чем 70 поддерживаемыми облачными сервисами. Возможно, выбор в пользу этой утилиты обусловлен высокой скоростью и устойчивостью соединения благодаря поддержке многопоточности и докачки файлов.

В атаках группировки **Warlock** была зафиксирована ранее не наблюдавшаяся нами утилита **MinIO Client (mc)**. Этот клиент позволяет взаимодействовать с многими S3-совместимыми хранилищами.

Выгружаемые данные направлялись на различные внешние ресурсы. Самыми популярными оказались: MEGA, Dropbox, Google Drive, OneDrive, также был замечен анонимный файловый хостинг с поддержкой загрузки через TCP и Curl.

ПРИМЕР ИНЦИДЕНТА

В 2025 году в практике нашей команды реагирования был зафиксирован инцидент, где от рук финансово-мотивированной группы **THOR**, также отслеживаемой как **Asgard Wolf**, пострадала организация из сферы здравоохранения.

Точкой проникновения в сеть послужила учетная запись подрядной организации. На протяжении двух месяцев злоумышленники активно продвигались по сети под видом подрядчиков, изучая доменную среду и собирая необходимые учетные данные путем дампа процесса аутентификации lsass.exe с помощью публично доступного инструмента mimikatz.

Для закрепления на периметре атакующие применяли утилиты для удаленного администрирования.

В результате компрометации инфраструктуры атакующие развернули программу-вымогатель семейства LockBit с целью дальнейшего требования выкупа.

Однако до шифрования систем с файловых серверов целевой инфраструктуры выгружались финансовые документы и иные чувствительные данные. Для этого злоумышленники использовали свободно распространяемую утилиту **Rclone**.

Конфигурационные файлы этого инструмента (обычно C:\Users\<REDACTED>\AppData\Roaming\rclone\rclone.conf), хранят тип удаленного хранилища (например, sftp), а также параметры соединения (в том числе IP-адрес подконтрольного сервера). Запуск Rclone производится командой вида `rclone copy source:sourcepath dest:destpath`

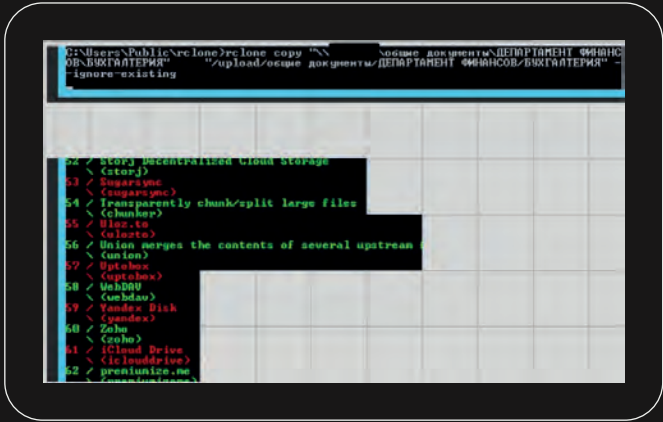


Рис. 10. Частично восстановленный кэш изображения удаленного рабочего стола с выполняемой командой

Примечательно, что кэш изображений удаленного рабочего стола одного из скомпрометированных пользователей содержал выполняемую команду и процесс выгрузки. Кроме того, непосредственно перед шифрованием данных атакующие запускали PowerShell-сценарий для автоматизированного сбора и выгрузки папки tdata, содержащей файлы сессий мессенджера Telegram.



Telegram-канал
Angara Security

Публикация
про группировку
THOR

ЭКСФИЛЬТРАЦИЯ ДАННЫХ – ПРОТИВОДЕЙСТВИЕ

Тенденция к использованию легитимных облачных сервисов для эксфильтрации существенно усложняет обнаружение утечек, поскольку этот трафик сложно отличить от легитимной активности.

Для противодействия этому можно:

01

Внедрить мониторинг запуска специализированных утилит (rclone.exe, mc.exe) и аномального поведения встроенных средств (ssh.exe, powershell.exe с обращениями к MailboxExportRequest).



02

Анализировать сетевой трафик на предмет подключений к известным облачным хранилищам со стороны нехарактерных процессов (например, консольных утилит, а не браузеров).

03

Использовать SIEM-системы для корреляции событий доступа к файлам и последующих сетевых соединений с внешними файловыми хостингами.

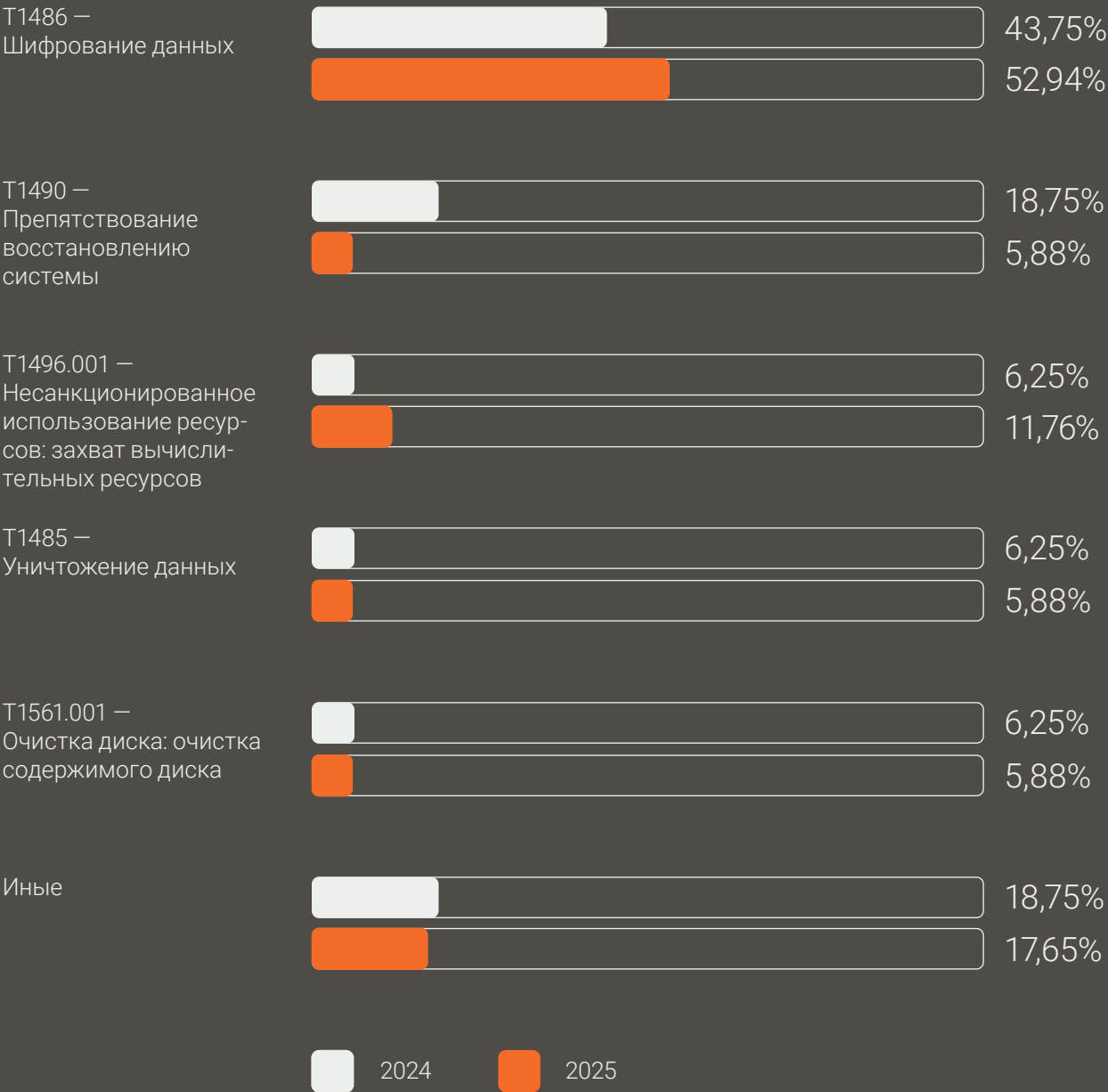
04

Применить проактивные меры защиты: ограничить через веб-прокси доступ к категории «File Sharing» и «Cloud Storage» для узлов, не нуждающихся в этом по бизнес-логике.

ДЕСТРУКТИВНЫЕ ДЕЙСТВИЯ



Диаграмма 19. Распределение выявленных техник в рамках тактики деструктивных действий



Тактика воздействия на инфраструктуру (Impact) традиционно замыкает цепочку атаки. Именно здесь злоумышленники реализуют конечную цель, ради которой проделаны предыдущие этапы.

Программы-вымогатели который год стабильно доминируют в этой тактике. И, судя по всему, ситуация в обозримой перспективе не изменится.

Уже стало традицией, прежде чем запустить шифрование, атакующие пытаются уничтожить или заблокировать возможности восстановления, включая «примитивное» удаление теневых копий через `vssadmin delete shadows /all /quiet` или `wmic shadowcopy delete`, отключение служб резервного копирования, в ряде случаев осуществляется целенаправленная атака

на подключенные сетевые хранилища и системы резервного копирования.

Отдельная картина складывается в сегменте малого и среднего бизнеса (МСБ). Здесь атаки нередко развиваются настолько стремительно — от первоначального доступа до шифрования за считанные часы — что злоумышленники «не успевают» зачистить резервные копии. Впрочем, это редко имеет значение: часто организации МСБ не имеют полноценной системы резервного копирования. Потеря данных в результате атаки оказывается для них катастрофой именно по этой причине.

Не снижается число атак, цель которых — не вымогательство, а вывод инфраструктуры из строя. В отдельных случаях атакующие даже не оставляют записок с требованиями и не сопровождают действия политическими заявлениями. Отсутствие явного «послания» от атакующих существенно усложняет атрибуцию и понимание истинных целей инцидента.

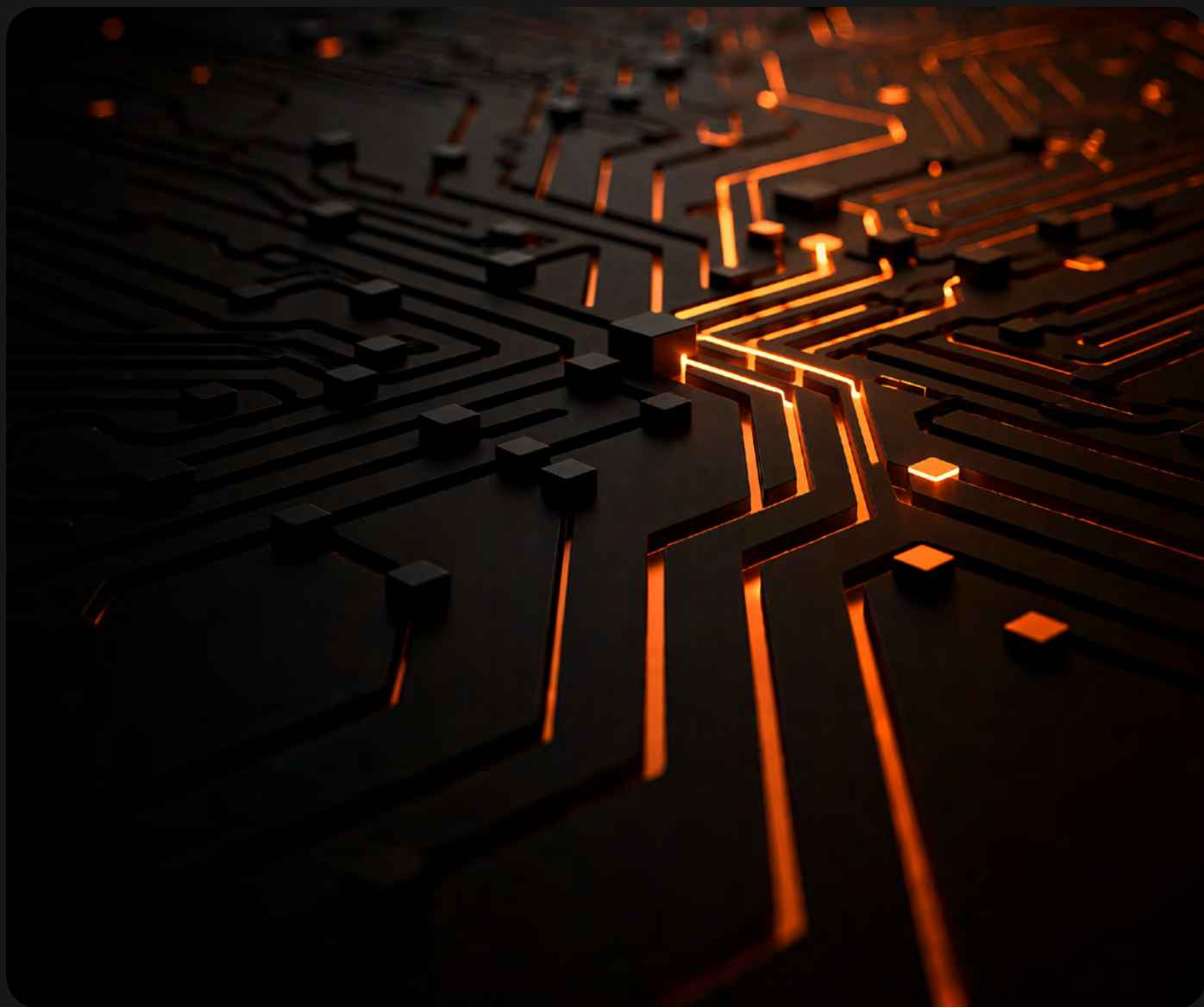
Атаки с несанкционированной установкой майнеров занимают заметное место в нашей статистике. Однако здесь важна оговорка: их число в нашей выборке не вполне репрезентативно. Заказчики редко приходят в отдел криминалистики с конкретной проблемой майнера. Как правило, организации справляются с атакой самостоятельно или силами ИТ-подразделения, не квалифицируя произошедшее как полноценный инцидент. На нашей практике майнер устанавливается на уже скомпрометированную систему попутно с основной атакой либо напрямую через эксплуатацию уязвимости в публично доступном сервисе. Отдельной аналитической ценности этот тип атак в нашем контексте не представляет, но игнорировать его не стоит: майнер на хосте — индикатор того, что периметр был преодолен, а полноценное расследование инцидента необходимо вне зависимости от кажущейся «безобидности» последствий.

ПРИМЕР ИНЦИДЕНТА

Показательная часть обращений 2025 года имела нетипичную отправную точку: организации приходили к нам не после того, как, например, шифровальщик уже отработал, а значительно раньше — получив официальное уведомление от Национального координационного центра по компьютерным инцидентам (НКЦКИ) о возможной компрометации инфраструктуры.

Это принципиально иная ситуация. В классическом сценарии специалисты по реагированию приезжают на инцидент, когда все самое страшное, скорее всего, уже произошло, и восстанавливают хронологию атаки ретроспективно. В описываемом случае атакующие были уже внутри инфраструктуры, но активную фазу еще не начали.





Стоит отметить, что сами организации далеко не всегда понимали, каким образом факт компрометации стал известен регулятору. Тем не менее зрелые команды безопасности относились к такому сигналу как к достоверной информации и не тратили время на сомнения, а немедленно начинали внутреннюю проверку.

При первичном анализе в подобных кейсах, как правило, мы фиксировали следы присутствия атакующих в инфраструктуре, злоумышленники успели закрепиться и проводили разведку: изучали топологию сети, перемещались между сегментами, собирали учетные данные. Индикаторы этой активности присутствовали в журналах событий, однако без целенаправленного поиска терялись в общем потоке.

Именно такой сценарий — когда есть время действовать до деструктивной фазы — наиболее ценен с точки зрения реагирования. Локализация и ограничение доступа атакующих к инфраструктуре до запуска шифровальщика на порядок менее затратны, чем восстановление после него. И то, что организации в подобных ситуациях не игнорировали уведомление и обращались за помощью, говорит о реальном росте культуры реагирования на инциденты.

ПЕРВООЧЕРЕДНЫЕ ДЕЙСТВИЯ ПРИ АТАКЕ ШИФРОВАЛЬЩИКА

01 Изолировать зараженные узлы, но не выключать их

Отключить от проводной и беспроводной сети, но сохранить электропитание. В оперативной памяти работающей системы могут находиться криминалистически значимые артефакты, в редких случаях — даже ключи шифрования.

02 Защитить то, что ещё не тронuto

Физически отключить от сети серверы резервных копий, контроллеры домена, гипервизоры, серверы БД и системы централизованного управления. Если они в виртуальной среде — немедленно создать снапшоты (или поставить их на паузу), так останутся артефакты сетевых взаимодействий. Возможно, злоумышленники еще не успели до них добраться.

03 Проверить и при необходимости отключиться от сети Интернет

Проанализировать исходящий трафик: атакующие в этот момент могут продолжать выгружать данные. При обнаружении подозрительных сессий — зафиксировать скриншотами и логами, после чего изолировать сегменты или всю сеть от сети Интернет. Это достаточно серьезная, но наиболее эффективная мера, если об атаке ничего неизвестно и нельзя однозначно утверждать, что злоумышленник уже не в сети и не имеет механизмов восстановления доступа (управления).

04 Не подключать носители с резервными копиями к скомпрометированным системам

До установления источника угрозы нельзя разворачивать резервные копии в зараженную среду. Если подключение неизбежно, предварительно сделайте побитовую копию носителя на изолированном чистом компьютере и подключайте строго в режиме «только чтение».

То же касается восстановления из резервных копий. Пока мы не знаем дату компрометации, есть риск восстановить уже зараженную копию.

05 Не переустанавливать ОС и не удалять данные

Переустановка системы до сбора криминалистических данных может уничтожить следы первоначальной компрометации. Перед любыми действиями с дисками важно собрать триаж, побитовые образы, файлы виртуальных машин.

06 Сохранять образцы вредоносного программного обеспечения

Все подозрительные файлы и исполняемые объекты необходимо сохранить для анализа командой DFIRMA. Нельзя загружать их на публичные сервисы (VirusTotal и аналоги): злоумышленники нередко встраивают в тело ВПО данные о жертве, и такая загрузка раскроет факт и характер атаки.



Важно! Необходимо зафиксировать состояние до прибытия DFIRMA-команды

Последовательно ответить на следующие вопросы и задокументировать ответы:

- Как и когда был обнаружен инцидент?
Есть ли точные дата и время первых признаков?
- Какие хосты затронуты (серверы / рабочие станции, примерный процент от общего числа)?
Есть ли между ними что-то общее — сегмент сети, прикладное назначение?
- Каков статус резервных копий — доступны, зашифрованы, частично повреждены?
- Если злоумышленники вышли на связь — через какой канал, какие выдвигают требования?

Организационные действия

07 Перевести коммуникации за пределы корпоративной инфраструктуры

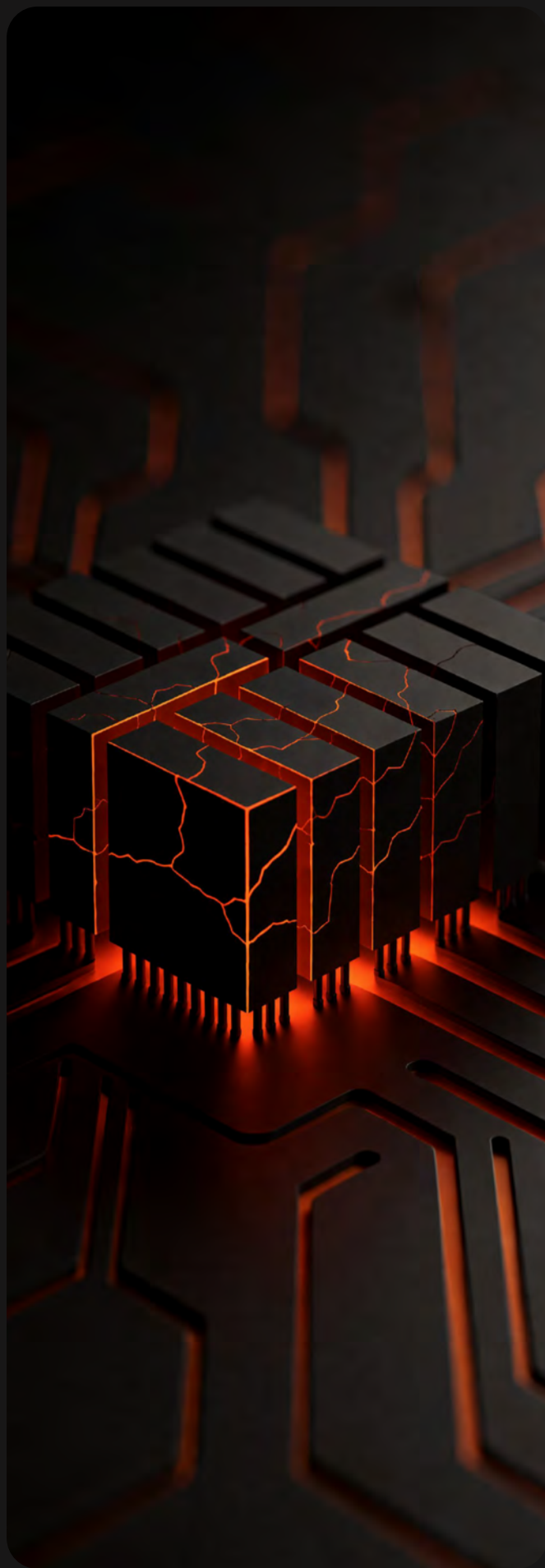
Корпоративная почта, мессенджеры и чаты, авторизованные на скомпрометированных устройствах, могут читаться злоумышленниками в реальном времени. Все рабочие коммуникации стоит вести только через личные устройства. Важно завершить все активные сессии корпоративных мессенджеров (Telegram, MAX, eXpress и др.), включая (!) текущую, и перезайти заново. Убедиться, что в аккаунты не было входа с корпоративных устройств.

08 Назначить координатора и ответственного за расследование и реагирование на инцидент

09 Определить цели реагирования

Уголовное преследование и публичная огласка или минимизация публичного резонанса — это разные стратегии, требующие разных действий и ресурсов. Определиться с приоритетом как можно раньше.

10 Обратиться в правоохранительные органы после предварительного согласования с юридической службой организации



Коммуникации

11 Единая точка внешних коммуникаций

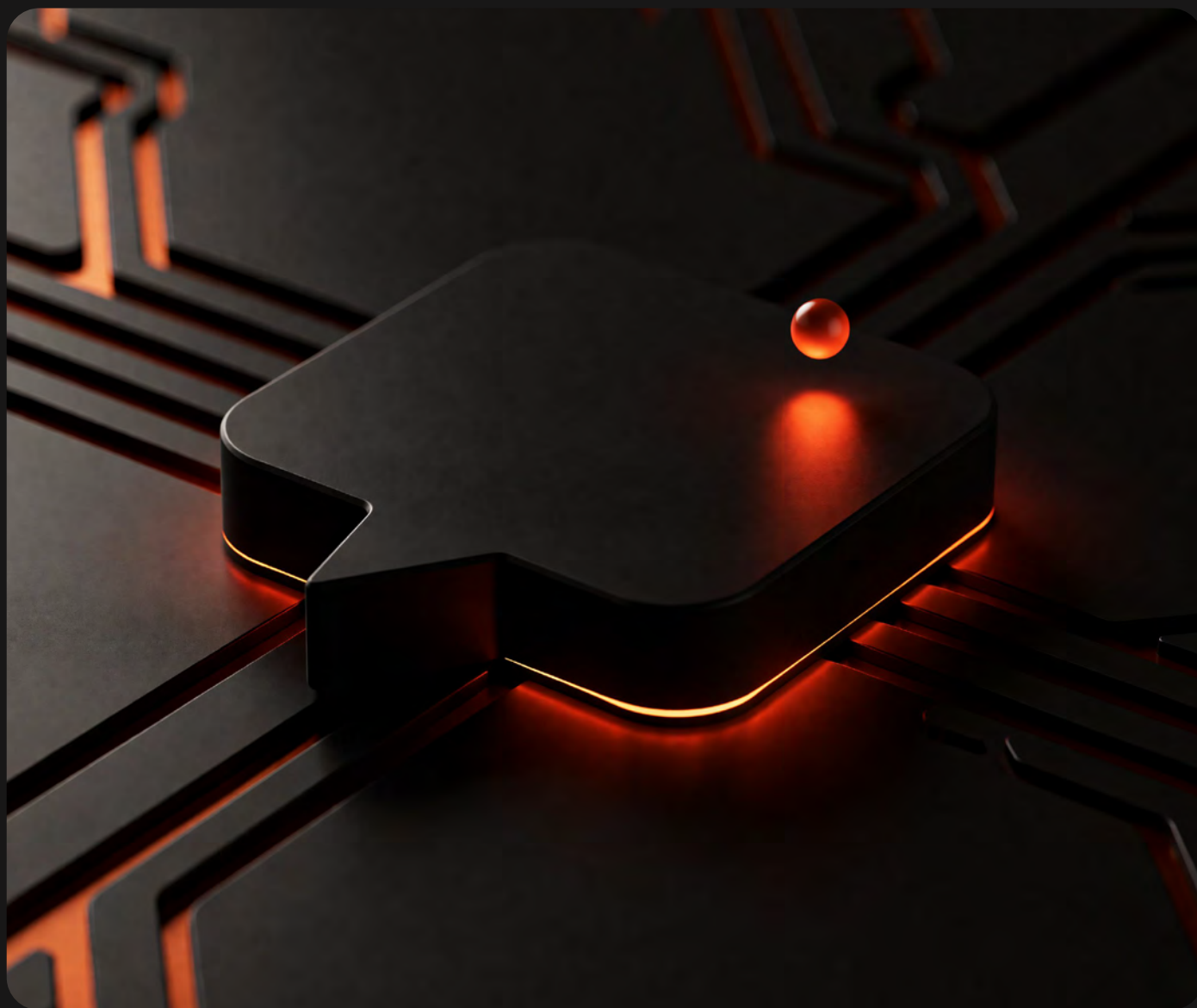
Назначить одного ответственного за все публичные заявления (как правило, представитель PR/маркетинга).

Все тексты согласовывать с юристом и готовить исключительно вне скомпрометированной инфраструктуры, так как злоумышленники могут читать внутреннюю переписку и следить за подготовкой заявлений. Рекомендуется подготовить заранее согласованные шаблоны сообщений компании на случай длительной недоступности сервисов, утечки данных или дефейса сайта.

12 Информировать партнеров и клиентов, при необходимости

Если скомпрометированная инфраструктура связана с партнерами через VPN, общие системы или учетные записи, то они могут быть под угрозой. Уведомление согласовать с юристом. Все тексты направлять только через некорпоративные каналы.

Отдельно и повторно выделим самое главное правило: не торопитесь восстанавливать системы до завершения криминалистического сбора данных. Поспешное восстановление может навсегда уничтожить возможность понять, как произошла атака — а именно это поможет не допустить ее повторения.



ИНСТРУМЕНТЫ ПРЕДОТВРАЩЕНИЯ

Сервисы для управления киберустойчивостью на всех этапах kill chain внутри организации и за ее пределами, построенные на базе Angara SOC

Центр мониторинга и реагирования на инциденты информационной безопасности (Security Operations Center)

Выявление и расследование киберинцидентов, реагирование на них (ручное и автоматизированное, выездное и удаленное, активное и проактивное), а также устранение последствий и восстановление. Сервис позволяет быстрее выявлять инциденты, снижать издержки на устранение проблем и сделать систему более управляемой.

Центр управления активами и уязвимостями (Vulnerability Operations Center, VOC)

Управление уязвимостями и активами, как внутри периметра (AVM), так и за его пределами (ASM). Регулярные сканирования и инвентаризации активов, верификация результатов, предоставление кратких и понятных отчетов. Рекомендации и консультации по харденингу, а также анализ динамики устранения уязвимостей.

Сервис мониторинга и реагирования на конечных устройствах (Endpoints Threat Detection and Response, ETDR)

Мониторинг и реагирование на инциденты ИБ на основе данных, собираемых EDR. Облачное решение с быстрым запуском для предотвращения ущерба.

Сервис защиты веб-приложений от внешних угроз (Web Application Firewall, WAF)

Защита веб-приложений от угроз с использованием облачного WAF. Фильтрация трафика, блокировка нежелательных запросов и рекомендации по повышению безопасности защищаемых ресурсов.

Реагирование на инциденты и цифровая криминалистика (Digital Forensics, Incident Response, Malware Analysis, DFIRMA)

Реагирование на инциденты, цифровая криминалистика и анализ вредоносных инструментов для оперативной локализации и минимизации ущерба. Реконструкция инцидента, рекомендации по повышению безопасности и экспертная поддержка при обращении в государственные органы и органы судебной власти.

Поиск следов компрометации инфраструктуры (Compromise Assessment)

Поиск следов компрометации инфраструктуры для выявления скрытого присутствия злоумышленника или фактов прошедших ранее атак.

Платформа для управления цифровым следом организации (ANGARA ECHO)

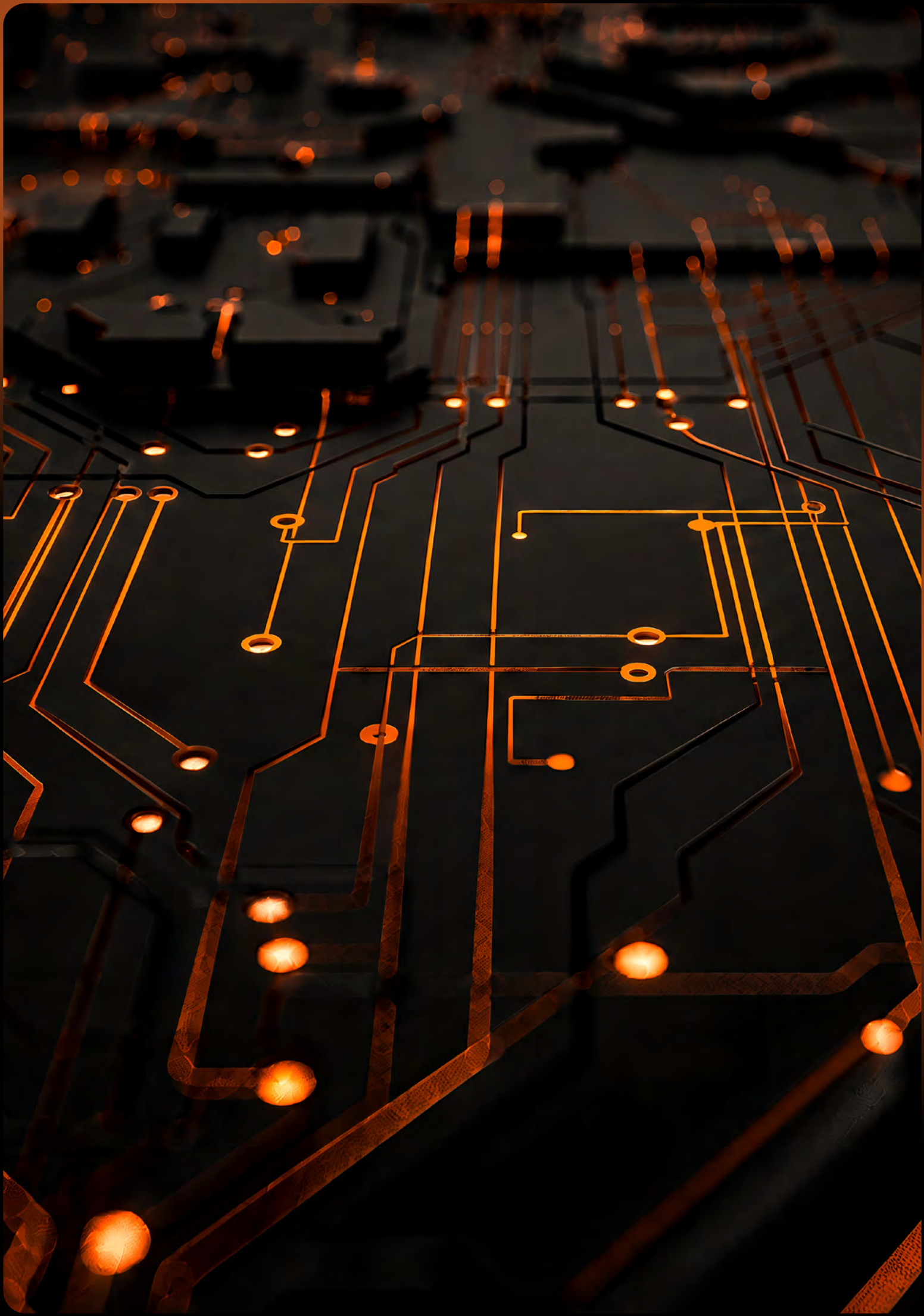
Управление цифровым следом с платформой Angara ECHO для поиска утечек секретов (логины/пароли сотрудников, ключи доступа, токены и т.д.), чувствительных данных организации, сведений о готовящихся атаках и подкупе сотрудников, а также для выявления фишинговых ресурсов и мошеннических схем. Услуга может быть использована для проверки подрядчиков и контрагентов.

Данные о киберугрозах (CyberThreat Intelligence, CTI)

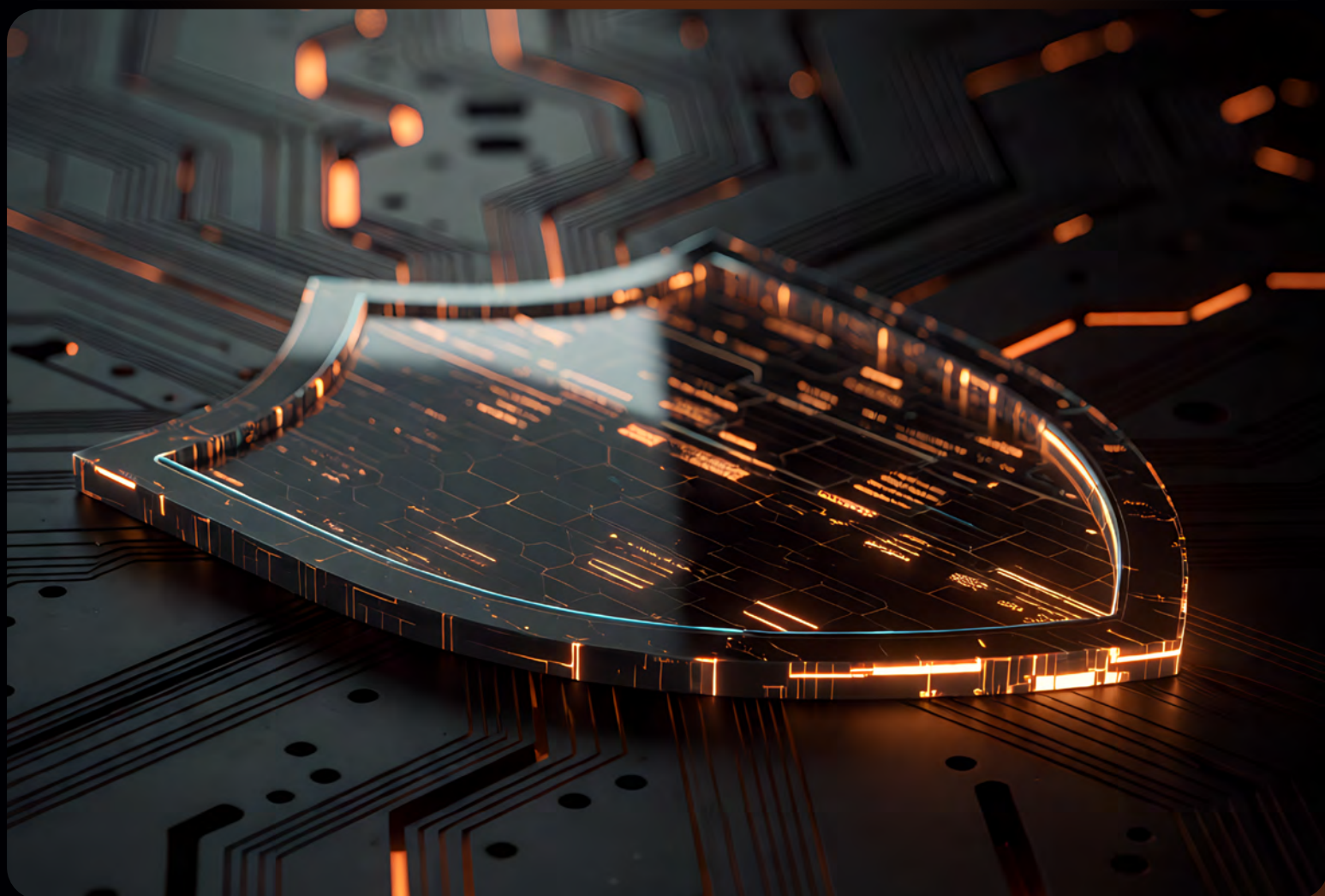
Наборы верифицированных индикаторов для обнаружения вредоносной активности, превентивной блокировки ресурсов и инструментов злоумышленников.

Сервис для выявления и блокировки вредоносной активности на уровне доменных имен (Secure DNS)

Фильтрация DNS-трафика для выявления вредоносной активности и ее блокировки. Запрет доступа к потенциально вредоносным сайтам из корпоративной сети.



ВАША КИБЕРБЕЗОПАСНОСТЬ В ЦИФРОВОМ МИРЕ



СВЯЗАТЬСЯ С НАМИ

+7 (495) 269 26 06

info@angarasecurity.ru

response@angarasecurity.ru

angarasecurity.ru



mtdr.angarasecurity.ru