Kaspersky ICS CERT

kaspersky

APT- и финансовые атаки на промышленные организации в первом квартале 2026 года

21.05.2026

Версия 1.0

Данный обзор представляет собой сводку публикаций об APT- и финансовых атаках на промышленные предприятия, информация о которых была раскрыта в первом квартале 2026 года, а также о связанной с ними активности групп, замеченных в атаках на промышленные организации. В каждом случае мы кратко изложили основные факты, а также привели полученные исследователями результаты и выводы, которые могут быть полезны специалистам, занимающимся практическими вопросами кибербезопасности промышленных предприятий.

Выводы по итогам квартала

Анализируя технические публикации команд исследователей кибербезопасности за первый квартал 2026 года, касающиеся атак на промышленные предприятия, можно предположить, что некоторые из тревожных открытий предыдущего квартала – последнего квартала 2025 года – грозят, возможно, новыми тенденциями изменения ландшафта угроз.

Кибератаки на транспортно-логистические предприятия, нацеленные на кражу перевозимых товаров, – одна из таких новых тенденций. Такой киберфизический способ монетизации атак на операторов грузовой перевозки и логистические организации в Америке и Европе выбрала ранее неизвестная армяноязычная группа Diesel Vortex. Вторая тревожная тенденция – использование кибератак для сбора информации с целью подготовки военных ударов и оценки их результативности – похоже, тоже становится частью реальности. Об этом, вероятно, свидетельствует публикация исследователей Check Point Research. Некоторые тенденции изменения ландшафта угроз обусловлены объективными техническими причинами – переоснащением промышленных предприятий и модными технологическими новшествами, сулящими повсеместно прирост эффективности. Так, рост популярности Linux-платформ в промышленности приводит к увеличению разнообразия вредоносного инструментария под эти платформы. В соответствии с текущими направлениями технического прогресса неизбежно растет число фиксируемых случаев использования средств искусственного интеллекта в разработке вредоносного ПО и на других этапах атак, нацеленных на промышленные предприятия.

Почти 16 лет прошло с момента появления первых публикаций об операции «Олимпийские игры» (более известной под названием Stuxnet, данным ей исследователями информационной безопасности), открывшей эру киберфизических атак. Тогда стало понятно, что джинна назад в бутылку

уже не вернуть, и все ждали новых, еще более технически сложных, масштабных и дерзких операций подобного рода. Однако никакого «достойного» с этой точки зрения продолжения не последовало. Публикации о новых атаках были крайне редки, сами вредоносные кампании оказывались раз от разу все более прямолинейными, а используемый в них инструментарий – все менее сложным. Вероятно, количество подобных кампаний ограничивали факторы межгосударственных отношений, а отказ от сложного инструментария был продиктован во многом соображениями рационально-техническими. Жизнь показала, что системы автоматизированного управления промышленности на самом деле гораздо легче доступны для атак, нежели все считали еще 10 лет назад. Сейчас большинство инцидентов, связанных с кибератаками на основные производственные активы, обусловлено весьма тривиальными проблемами информационной безопасности пострадавших организаций – например, такими, что описали специалисты CERT Polska. При этом вместе с ростом внешнеполитической нестабильности растет количество подобного рода инцидентов, расширяется география операций, и на арене появляются новые игроки, иногда ассоциируемые с неожиданными странами.

Атаки, нацеленные на российские организации

Атаки Stan Ghouls

Киберкриминал

Целевой фишинг

RAT

Бэкдор

Вредоносное ПО под Linux

Группа Stan Ghouls (также известная как Bloody Wolf) осуществляет целенаправленные атаки на организации в Российской Федерации, Кыргызстане, Казахстане и Узбекистане как минимум с 2023 года. Ее отличительными особенностями являются тщательно подготовленные атаки, адаптированные под конкретных жертв (преимущественно из производственной, финансовой и ИТ-сфер), специфические вредоносные загрузчики, написанные на Java, а также масштабная инфраструктура с выделенными ресурсами для конкретных кампаний.

Исследователи «Лаборатории Касперского» обнаружили, что Stan Ghouls инициировала новые кампании против организаций в Узбекистане (было выявлено более 50 жертв), затронувшие также предприятия в России, Казахстане, Турции, Сербии и Беларуси (заражения в последних трех странах, скорее всего, случайны). Проанализировав последнюю кампанию группы, исследователи заметили изменения в инфраструктуре злоумышленников, в частности новые домены. Группа рассылала фишинговые письма, содержащие вредоносные вложения в формате PDF.

Ранее Stan Ghouls использовала в качестве вредоносной нагрузки троянец удаленного доступа (RAT) STRRAT (он же Strigoi Master), но в прошлом году сменила тактику и стала использовать легитимное ПО NetSupport. Также исследователи обнаружили признаки того, что группа пополнила свой арсенал ботнетом Mirai, нацеленным на IoT-устройства.

Атаки Head Mare

Киберкриминал

Целевой фишинг

Компрометация легитимных почтовых серверов

Эксплуатация общедоступных приложений

Бэкдор

Подмена легитимных приложений

Исследователи F6 обнаружили новую волну вредоносных рассылок от группы PhantomCore (она же Head Mare) 19 и 21 января. Злоумышленники использовали для отправки писем легитимные адреса электронной почты, что может указывать на их компрометацию. Кампания была нацелена на российские организации из сфер ЖКХ, финансов, электронной коммерции, коммунального хозяйства, потребительских услуг, а также из аэрокосмической, химической, строительной и производственной отраслей. Электронное письмо с темой «ТЗ на согласование» содержало архив под названием «ТЗ на согласование сб 54 от 19.01.26.zip» с DOC- и LNK-файлами. DOC-файл на самом деле являлся RAR-архивом, содержащим одноименный каталог с файлами, относящимися к самому документу. После своего запуска LNK-файл выполнял cmd-команду, инициировавшую загрузку и выполнение PowerShell-скрипта. Этот скрипт в свою очередь загружал и отображал документ-приманку, загружал в память PowerShell-скрипт следующего этапа и обеспечивал закрепление в планировщике задач Windows. Это вредоносное ПО практически идентично ранее известному PhantomCore.PollDL (PhantomRemote).

В конце 2025 года аналитики «Лаборатории Касперского» выявили новую вредоносную активность, нацеленную на российские организации из государственного сектора, а также строительной и производственной отраслей, которую они связали с группой Head Mare. Кампания продолжилась в начале 2026 года. В рамках этой активности группа вновь расширила свой инструментарий, представив новый бэкдор PhantomHeart, который изначально распространялся в виде DLL-библиотеки, а затем был переработан в PowerShell-скрипт. PhantomHeart реализует канал удаленного доступа, сочетающий HTTP-коммуникацию с C2-сервером и возможность развертывания SSH-туннеля по запросу. Закрепление бэкдора обеспечивается запуском через планировщик задач под видом легитимного скрипта обновления, размещенного в директории LiteManager. Кроме того, исследователи обнаружили, что Head Mare переработала ранее известный инструмент PhantomProxyLite и реализовала его в виде PowerShell-скрипта. Цепочка заражения включала эксплуатацию уязвимости BDU:2025-10114 в ПО TrueConf Server. В

некоторых случаях группа по-прежнему использовала фишинговые рассылки.

Исследователи «Лаборатории Касперского» обнаружили еще одну масштабную фишинговую кампанию группы Head Mare, на этот раз с новой версией бэкдора PhantomCore (PhantomDL). Активность затронула несколько сотен пользователей из российских организаций, в том числе организаций из государственного сектора и логистической, финансовой и промышленной отраслей. Получателям приходили письма якобы от научно-исследовательской организации с предложением заключить контракт. Во вложениях были зашифрованные архивы, содержавшие несколько LNK-файлов, которые автоматически запускали процесс загрузки и установки бэкдора. При запуске любого из этих файлов выполнялась команда для загрузки промежуточного PowerShell-скрипта, размещенного на сервере злоумышленников. Этот скрипт скачивал с удаленного сервера новый вариант PhantomCore, написанный на C++, загружал и открывал документ-приманку, обеспечивал закрепление в системе и автозапуск. Для закрепления использовалась техника подмены PSFactoryBuffer COM. Основная задача новой версии PhantomCore – предоставление злоумышленникам удаленной командной строки в зараженной системе. После запуска этот бэкдор отправлял на C2-сервер два POST-запроса, содержащие данные в формате JSON. В ответ злоумышленники передавали последовательность команд для бэкдора, включая команду для загрузки и распаковки архива. Внутри архива находился модуль для запуска ssh.exe, написанный на Golang. Закрепление модуля в системе обеспечивалось с помощью задачи планировщика.

В марте исследователи «Лаборатории Касперского» сообщили о новой кампании Head Mare, нацеленной на образовательные и научные учреждения, а также организации энергетического сектора в России. Эта вредоносная активность была обнаружена в феврале, но велась как минимум с декабря 2025 года. Жертвы получали ссылку – приглашение на видеоконференцию, после перехода по которой предлагалось установить сервис для подключения к видеозвонку. В процессе установки происходило заражение системы – на устройство устанавливался ранее неизвестный бэкдор, получивший название PhantomPxPigeon. На момент публикации отчета исследователи наблюдали новую волну подобной активности – они обнаружили несколько скомпрометированных серверов TrueConf у различных организаций из транспортной отрасли, а также у научных и образовательных учреждений. Дистрибутивы клиентского приложения TrueConf, скачанного с этих серверов, были подменены на вредоносные. Вектор атаки, который привел к подмене клиентского приложения, неизвестен, но предполагается, что злоумышленники

использовали уже известную уязвимость BDU:2025-10116, которая была выявлена исследователями и исправлена вендором в августе 2025 года. Вредоносные дистрибутивы, обнаруженные исследователями «Лаборатории Касперского», не имеют действительной цифровой подписи.

Атаки Vortex Werewolf

Новый актор

APT

Целевой фишинг

Фишинг в Telegram

Фишинговые сайты

Инфраструктура облачных сервисов

Сеть Tor

В декабре 2025 года и январе 2026 года исследователи BI.ZONE обнаружили вредоносную активность нового кластера Vortex Werewolf (также известного как SkyCloak), нацеленную на российские организации из государственного сектора и оборонно-промышленного комплекса. Исследователи Cyble и Seqrite сообщили, что ранее Vortex Werewolf также атаковал белорусские правительственные и оборонные структуры. Результаты исследования сетевой инфраструктуры показали, этот кластер действует как минимум с декабря 2024 года. Злоумышленники используют Cloudflare в своей сетевой инфраструктуре. Исследователям не удалось определить способ получения первоначального доступа, но они предположили, что злоумышленники распространяли вредоносное ПО как посредством фишинговых рассылок, так и через Telegram. Жертвам отправляли замаскированную под адрес в Telegram ссылку для загрузки документа – архива, содержащего вредоносный LNK-файл, и дополнительного архива с набором файлов, включая PowerShell-скрипт. Фишинговая страница имитировала процесс загрузки файла, а на самом деле инициировала процедуру восстановления доступа к аккаунту Telegram. Пользователю предлагалось подтвердить код страны и ввести номер телефона, после чего в Telegram приходил код подтверждения. Если для аккаунта была включена двухфакторная аутентификация, жертву также просили ввести облачный пароль. В результате Vortex Werewolf получал доступ к активной сессии пользователя в Telegram. В некоторых случаях, чтобы их действия выглядели еще более правдоподобно, злоумышленники размещали на фишинговой странице документ-приманку с размытым текстом.

Vortex Werewolf использует сервис GitHub Pages для размещения статических ресурсов на JavaScript и CSS, при этом для каждого фишингового домена создается отдельный репозиторий с этими ресурсами. После успешной проверки введенного кода и пароля (если включена двухфакторная аутентификация) генерируется ссылка, при переходе по которой запускается скачивание с Dropbox ZIP-архива с LNK-файлом внутри. После успешной компрометации в системе устанавливаются Tor и OpenSSH, которые для связи с управляющей инфраструктурой используют мосты obfs4, а не общедоступные узлы сети

Tor. Удаленный доступ также настраивается через сеть Tor по протоколам RDP, SMB, SFTP и SSH. Вредоносная программа сохраняется в планировщике задач Windows через создание заданий.

Исследователи BI.ZONE отмечают, что Vortex Werewolf напоминает Core Werewolf (она же Awaken Likho). У кластеров схожие цели и регионы атак, оба используют SSH для получения удаленного доступа к скомпрометированным системам и поддельные документы военной тематики. Впрочем, имеющиеся данные не позволили исследователям отнести Vortex Werewolf к Core Werewolf, поэтому эта активность была рассмотрена как отдельный кластер.

Атаки Toy Ghouls

Киберкриминал

Шифровальщики

Вредоносное ПО под Linux

Эксплуатация общедоступных приложений

Доверенные отношения

Toy Ghouls (она же Bearlyfy и laboo.boo) – финансово мотивированная группа, действующая как минимум с января 2025 года. Она нацелена исключительно на российские организации и использует программы-вымогатели из семейств LockBit и RedAlert для систем Windows, а также Babuk для Linux и ESXi. Основные отрасли, на которые нацелены злоумышленники: производство, строительство, автомобилестроение и телекоммуникации. Некоторые пересечения с инфраструктурой и инструментарием указывают на возможную связь Toy Ghouls с группой Head Mare. Исследователи «Лаборатории Касперского» проанализировали техники и процедуры злоумышленников, использующих унифицированную цепочку атак. Чаще всего для получения первоначального доступа злоумышленники использовали похищенные сертификаты сторонних подрядчиков для аутентификации в VPN. После установления VPN-соединения они подключались ко внутренним системам и перемещались в среде жертвы по RDP.

Группа Toy Ghouls часто эксплуатирует уязвимые серверы 1С, загружая на них 1C-Shell через отдельные EPF-файлы. Для разведки внутренней сети она использует сканеры сети SoftPerfect и fscan, которые способны искать и использовать уязвимости. Toy Ghouls использует запланированные задачи для выполнения различных действий на скомпрометированных хостах, PowerShell – для выполнения вредоносных скриптов, командную оболочку Windows – для выполнения команд в этой ОС, а также Bash – для выполнения команд в системах *nix.

Исследователи F6 тоже отслеживали последнюю активность группы Bearlyfy (она же Toy Ghouls), которая с момента своего появления провела более 70 атак на российские компании. Изначально она использовала LockBit 3 Black для шифрования данных в системах Windows и собственную

модифицированную версию программы-вымогателя Babuk для шифрования в системах Linux. С мая 2025 года в нескольких атаках злоумышленники использовали слегка модифицированную версию программы-вымогателя PolyVice известной группы (RaaS) Vice Society. По данным F6, в марте 2026 года Bearlyfy стала использовать собственную программу-вымогатель под Windows – GenieLocker. Криптосхема и подходы вредоносного ПО явно заимствованы у программ-вымогателей семейств Venus/Trinity. Исследователи считают, что авторы зловреда явно старались продемонстрировать свои познания в криптографии и методах антианализа, пытаясь превзойти LockBit 3. Кроме того, исследователи отметили взаимодействие Bearlyfy с другими, более опытными проукраинскими группами, такими как Head Mare, несмотря на то что группа демонстрирует индивидуальный почерк с самого начала своей деятельности. Возможно, появление в арсенале Bearlyfy собственных программ-вымогателей вызвано желанием выделиться на фоне других злоумышленников.

Атаки Librarian Ghouls

APT

Целевой фишинг

RAT

Исследователи «Лаборатории Касперского» сообщили, что в ноябре 2025 года они зафиксировали новую вредоносную активность Librarian Likho (Librarian Ghouls). Волна атак была нацелена на широкий круг российских организаций из различных отраслей, включая государственный сектор, строительство и производство. Атаки начались с фишинга – злоумышленники отправили более тысячи писем с вредоносными вложениями, которые практически не отличались по функциональности и контексту, что указывает на автоматизацию атаки. Вложение представляло собой вредоносный исполняемый файл, замаскированный под предложение о сотрудничестве или заполненный бланк договора. Это был инсталлятор, созданный в программе Smart Install Maker. После запуска он извлекал два CAB-архива, содержащих файл-приманку в формате DOC, TXT-файл со списком C2-серверов, исполняемый файл и скрипты. Затем вредоносное вложение запускало CMD-файл из архива, который анализировал адреса C2-серверов из текстового файла. В ходе работы скрипт создавал виртуальное окружение и переменные для конкретных адресов, с которых скачивались полезные нагрузки. Он также загружал с C2-сервера два RAR-архива и кастомную версию WinRAR, после чего с помощью архиватора распаковывал скачанные файлы, используя вшитый пароль. RAR-архивы содержали исполняемый файл инструмента удаленного доступа AnyDesk, утилиту для отключения Windows Defender, утилиту для эксфильтрации данных через SMTP, утилиту для сокрытия окон запущенных процессов, утилиту для восстановления паролей с почтовых

клиентов, скрипт для эксфильтрации паролей и обхода средств защиты информации. Основная цель этого скрипта – предоставить оператору данные для подключения и подготовить узел для дальнейшей постэксплуатации. Именно этот скрипт запускался вредоносным вложением.

Атаки PseudoSticky

Новый актор

APT

Целевой фишинг

RAT

Код, сгенерированный ИИ

В ноябре 2025 года исследователи F6 обнаружили вредоносную кампанию, в ходе которой новая группа злоумышленников использовала PureCrypter и DarkTrack RAT. Один из вредоносных компонентов – hta-файл, инициирующий загрузку DarkTrack RAT, – вероятно, был создан с использованием LLM. В пользу этого предположения говорит простота кода, его форматирование, и хорошее документирование при отсутствии грамматических ошибок. Исследование этой активности выявило связь атакующих с группой Sticky Werewolf – это касается как тактик, техник и процедур (TTP) и инструментария, так и прямых упоминаний самими злоумышленниками – строка «StickyWerewolf» использовалась в качестве пароля к одному из их архивов, поэтому новая группа получила название PseudoSticky. При более тщательном анализе стали заметны различия в инфраструктуре, реализации вредоносного ПО и отдельных элементах тактики, исходя из чего исследователи предположили, что в данном случае имеет место не прямая связь, а подражание. С декабря 2025 года PseudoSticky атакует организации из самых разных отраслей – от ретейлеров и девелоперов до научно-исследовательских организаций и приборостроительных предприятий.

PseudoSticky использует фишинговые рассылки с вредоносными архивами во вложениях. Основные типы приманок – это файлы, названия которых связаны с военной промышленностью (от авиационных ракет до беспилотных летательных аппаратов), а также файлы, замаскированные под лицензии для ПО и прочую документацию. Финальной полезной нагрузкой были вредоносные программы DarkTrack RAT и Remcos RAT. В одной цепочке заражения использовался кастомный загрузчик. Он скачивал с ресурса Bitbucket список адресов C2-серверов, а запросы к этим адресам приводили к загрузке другой полезной нагрузки, которую исследователям не удалось получить. Однако на веб-странице вредоносного ПО в публичной онлайн-песочнице они заметили комментарий пользователя песочницы, в котором утверждается, что загружаемой полезной нагрузкой была программа Remcos RAT и она принадлежит группе StickyWerewolf. Позже исследователи обнаружили

конфигурационный файл этого образца в другой публичной онлайн-песочнице.

Киберггруппы, атакующие Россию

Киберкриминал

APT

Целевой фишинг

RAT

Эксплуатация общедоступных приложений

DLL sideloading

Вредоносное ПО под Linux

Исследователи Positive Technologies опубликовали анализ активности киберггрупп, нацеленных на российские организации, за четвертый квартал 2025 года, с описанием их TTP и принципа выбора жертв. Исследователи разделили группы на две категории: специализирующиеся на кибершпионаже и финансово мотивированные. Эти группы атакуют, в частности, аэрокосмические, логистические, производственные и энергетические предприятия.

Среди кибершпионских групп – ExCobalt (также известная как Shedding Zmiy, Red Likho, Cobalt Werewolf), которая компрометирует подрядчиков и получает доступ через опубликованные RDP-сервисы, а также использует бэкдор Cobint для удаленного управления и постэксплуатации. Для шифрования инфраструктуры группа использует Babuk для узлов Linux и гипервизоров VMware ESXi, а также LockBit для узлов Windows. ExCobalt компрометирует учетную запись в Telegram, похищая каталог tdata на устройстве жертвы. Один из способов закрепления в атакованной инфраструктуре, прежде незамеченный в арсенале ExCobalt, – размещение шеллов в виде отдельных EPF-файлов, реализующих механизм внешних обработок в программных продуктах 1С. ExCobalt использует руткит уровня ядра PUMAKIT в системах на Linux для обеспечения долговременной устойчивости и скрытности.

Еще одна кибершпионская группа – QuietCrabs (также известная как Subtle Werewolf, UTA0178, UNC5221, Red Dev 61) – использовала уязвимости (CVE-2025-4427, CVE-2025-4428, CVE-2025-53770), вредоносное ПО KrustyLoader и кроссплатформенный имплант Sliver. В отчете также описаны активности таких групп, как APT31 (Zirconium, Fair Werewolf, Violet Typhoon, Bronze Vinewood, Judgment Panda, Sheathminer), Rare Werewolf (она же Librarian Ghouls, Librarian Likho, Rezet) и PseudoGamaredon (она же Awaken Likho, Core Werewolf, GamaCopy), которые в качестве первоначального вектора атаки используют фишинговые рассылки.

В числе финансово мотивированных групп – Werewolves (она же Lone Wolf, Moonshine Trickster), NetMedved (она же Clubfoot Wolf), Silver Fox (она же Void Arachne), Hive0117 (она же Watch Wolf, Ratopak Spider, UAC-0008), все они используют фишинговые письма с вредоносными архивами. Werewolves в качестве финальной полезной нагрузки использует Cobalt Strike Beacon, NetMedved – NetSupport Manager (NetSupportRAT), Silver Fox

– ValleyRAT, а Hive0117 – PowerShell-кейлоггер и вредоносный JavaScript-скрипт.

Активность русскоязычных групп

Атаки на энергосистему Польши

APT

Вайпер

Эксплуатация сети и устройств АСУ

Целевые атаки на АСУ

Министр энергетики Польши на пресс-конференции 13 января заявил, что в конце 2025 года были предприняты попытки кибератаки на энергетический сектор страны. Согласно сообщению на сайте правительства Польши от 15 января, были целенаправленно атакованы теплоэлектростанции, а также система управления энергией из возобновляемых источников, таких как ветряные турбины и фотоэлектрические станции. Каких-либо негативных последствий – дестабилизации национальной энергетической системы или повсеместного отключения электроэнергии – не было.

Исследователи ESET 23 января опубликовали сообщение с описанием подробностей атаки на энергосистему Польши. Они упомянули использовавшийся вайпер под названием DynoWiper и со средней степенью уверенности связали атаку с APT-группой Sandworm. К такому выводу они пришли, обнаружив сходства с атаками группы, в которых тоже использовались вайперы. 30 января исследователи опубликовали дополнительные технические подробности инцидента, затронувшего организацию в энергетическом секторе Польши. Согласно сообщению, обнаруженные образцы DynoWiper ориентированы исключительно на ИТ-среду, они не имеют функционала, ориентированного на промышленные компоненты сети.

CERT Polska 30 января опубликовал отчет об инцидентах в энергетическом секторе, произошедших 29 декабря 2025 года. Согласно документу, атаки затронули по меньшей мере 30 ветряных и солнечных электростанций, частную компанию в производственном секторе и теплоэлектростанцию, обеспечивающую теплом почти полмиллиона жителей. В отчете описаны векторы атак и первоначальный доступ, которые использовали злоумышленники, а также приведен список индикаторов компрометации (IoC).

На каждом затронутом объекте присутствовало устройство FortiGate, служившее одновременно VPN-концентратором и файрволом. Везде VPN-интерфейс был подключен к интернету и позволял авторизацию без многофакторной аутентификации. Было установлено, что некоторые из этих устройств в прошлом имели уязвимости, в том числе уязвимости,

позволяющие удаленно выполнять код. В случае с производственной организацией атакующие, получив доступ к устройству, внесли изменения, которые позволяли сохранять доступ даже при смене паролей.

На момент атаки злоумышленники обладали правами администратора на устройстве. Эти привилегии, вероятно, использовались для получения логина и пароля к VPN-аккаунту с доступом ко всем подсетям. Злоумышленники использовали учетные данные, полученные из локальной среды, пытаясь получить доступ к облачным сервисам. После выявления учетных данных, для которых существовали соответствующие учетные записи в Microsoft 365, злоумышленники похитили определенные данные из платформ Exchange, Teams и SharePoint. Особенно их интересовали файлы и сообщения электронной почты, связанные с модернизацией OT-сети, SCADA-системами и техническими работами, проводимыми в организациях. Злоумышленники попытались повысить привилегии, эксплуатируя неправильно настроенные права доступа.

В атаках злоумышленники использовали вредоносные программы DynoWiper и LazyWiper. DinoWiper использовалась в инциденте с объектами возобновляемой энергетики и была запущена на устройстве человеко-машинного интерфейса. В инциденте с теплоэлектростанцией (там тоже использовался DynoWiper) и с производственной организацией (использовался LazyWiper) вредоносное ПО распространялось в домене Active Directory через PowerShell-скрипт, выполненный на контроллере домена.

В отчете CERT Polska упоминаются три вендора АСУ, продукты которых подверглись атаке: Hitachi Energy, Moxa и Mikronika. Что касается Hitachi, то были затронуты удаленные терминальные блоки RTU560, доступ к которым злоумышленники получили, используя учетные данные по умолчанию. Доступ позволил им загрузить вредоносную прошивку. Исследователи обнаружили, что функция безопасности, предотвращающая загрузку вредоносных обновлений прошивки, не была активирована. Впрочем, в обратном случае результат был бы тот же самый, поскольку устройства были подвержены известной уязвимости (CVE-2024-2617), допускающей установку неподписанного обновления. По данным CERT Polska, злоумышленники также атаковали устройства релейной защиты Hitachi Relion. Доступ к ним оказался возможен, потому что не были изменены дефолтные FTP-аккаунт и учетные данные. Кроме того, злоумышленники атаковали RTU и устройства человеко-машинного интерфейса производства Mikronika. Доступ к ним тоже был защищен логином и паролем по умолчанию. Также были атакованы серверы последовательных интерфейсов Moxa NPort. На них был активирован веб-интерфейс, и они

тоже были настроены с использованием стандартных учетных данных для входа. Анализ инфраструктуры злоумышленников показал, что она совпадает с инфраструктурой кластера, широко известного под такими именами как Static Tundra (описана Cisco Talos), Berserk Bear (CrowdStrike), Ghost Blizzard (Microsoft) и Dragonfly (Symantec).

Атаки APT28

APT

Целевой фишинг

Бэкдор

Инфраструктура облачных сервисов

Компрометация легитимных почтовых сервисов

DLL sideloading

Уязвимость нулевого дня

Вайпер

В начале февраля CERT-UA и Zscaler сообщили об атаках группы UAC-0001 (она же APT28, Fancy Bear), эксплуатирующей уязвимость CVE-2026-21509, на украинские правительственные организации и словацкие и румынские госучреждения. Уязвимость позволяет неавторизованному локальному злоумышленнику обойти защитные механизмы в Microsoft Office (Object Linking and Embedding), когда потенциальная жертва открывает вредоносный файл, из-за использования ненадежных данных при принятии решения по безопасности. Злоумышленники использовали метод социальной инженерии, создавая приманки не только на английском, но и на украинском, словацком и румынском языках. На стороне сервера они использовали техники обхода детектирования, отправляя вредоносную DLL только в том случае, если запросы поступали из целевого региона и содержали корректный User-Agent. Исследователи Zscaler обнаружили два варианта дроппера, запускавшего установку MiniDoor (программа для кражи электронной почты на основе макросов Outlook) и PixyNetLoader, который внедрял имплант Covenant Grunt.

В отчете от 4 февраля исследователи Trellix отметили более широкую активность APT28, также нацеленную на морские, транспортные и дипломатические организации в Польше, Словении, Турции, Греции и ОАЭ. Они считают, что атаки были частью целенаправленной 72-часовой фишинговой кампании, в ходе которой было отправлено по меньшей мере 29 различных электронных писем в девяти странах Восточной Европы. Атакующие использовали недавно обнаруженную уязвимость CVE-2026-21509 в течение 24 часов после выпуска вендором 26 января экстренного бюллетеня безопасности с описанием проблемы. Фишинговые сообщения были отправлены со скомпрометированных электронных адресов, принадлежащих правительствам нескольких стран, включая Румынию, Боливию и Украину. Злоумышленники использовали приманки на геополитическую тему вроде предупреждения о международной контрабанде оружия, приглашений на программы военной подготовки, дипломатических приглашений НАТО и Евросоюза, а также сводки о метеорологических чрезвычайных ситуациях. Вложенные файлы были очень похожи на настоящие правительственные документы – возможно,

они были подготовлены на основе украденных материалов. Открытие этих файлов запускало ряд программ, в частности MiniDoor и PixyNetLoader, которые устанавливали на зараженные системы бэкдор Covenant. В ходе кампании также широко использовались легитимные облачные сервисы для сокрытия вредоносной активности. По данным исследователей, APT28 использовала в качестве C2-канала облачную платформу хранения данных Filen.io, маскируя вредоносное ПО под обычный интернет-трафик.

Исследователи Trend Micro выявили кампанию APT-группы Pawn Storm (она же APT28, Fancy Bear, UAC-0001 и Forest Blizzard), которая использовала вредоносный набор PRISMEX в атаках на цепочку поставок украинского оборонного комплекса и его союзников из НАТО. Кампания началась, по крайней мере, в сентябре 2025 года, а в январе 2026-го заметно обострилась: группа стала эксплуатировать две уязвимости Microsoft – CVE-2026-21509 и CVE-2026-21513. Вторая касается сбоя механизма защиты в фреймворке MSHTML и использовалась как уязвимость нулевого дня как минимум за 11 дней до выхода патча Microsoft. Подготовка инфраструктуры для эксплуатации CVE-2026-21509 началась за две недели до публичного раскрытия – то есть злоумышленники были осведомлены о ней заранее. PRISMEX содержит четыре компонента: PrismexSheet – дроппер Excel с поддержкой макросов, способный с помощью стеганографии скрывать полезную нагрузку внутри самого файла, PrismexDrop – встроенный дроппер, обеспечивающий закрепление посредством техники COM hijacking, PrismexLoader – прокси-DLL, восстанавливающая полезные нагрузки из стеганографических PNG-изображений с помощью уникального алгоритма Bit Plane Round Robin, и PrismexStager – имплант Covenant Grunt, эксплуатирующий облачное хранилище Filen.io для зашифрованной коммуникации с C2-сервером. Постэксплуатация включала как сбор данных, так и запуск вайпера для удаления файлов в каталоге профиля пользователя, что свидетельствует как о шпионском, так и о диверсионном характере активности. Кампанию публично подтвердили CERT-UA, Zscaler ThreatLabz, Synaptic Systems и Akamai.

Активность, связанная с Азией

Атаки TGR-STA-1030

Новый актор

APT

Целевой фишинг

Бэкдор

Руткит

Вредоносное ПО под Linux

Эксплуатация сетевых устройств и общедоступных приложений

Согласно отчету подразделения Unit 42 компании Palo Alto Networks, новая кибершпионская группа TGR-STA-1030 (она же UNC6619), связанная с государством и действующая из Азии, взломала системы по меньшей мере 70 правительственных организаций и объектов критической инфраструктуры в 37 странах за последний год. Помимо этого, в ноябре и декабре 2025 года она провела активную разведку правительственной инфраструктуры в 155 странах. Группа действует как минимум с января 2024 года. Исследователи Unit 42 считают, что она скомпрометировала Министерство горнодобывающей промышленности и энергетики Бразилии, горнодобывающую компанию в Боливии, организацию Venezolana de Industria Tecnologica в Венесуэле, авиакомпанию в Индонезии, крупного поставщика энергетического оборудования на Тайване, а также объекты критической инфраструктуры в Демократической Республике Конго, Джибути, Эфиопии, Намибии, Нигере, Нигерии и Замбии. Отслеживая время проведения операций группы, исследователи выявили связь некоторых кампаний с реальными событиями. В своих первых кампаниях злоумышленники использовали тщательно составленные фишинговые письма, которые отправляли чиновникам из правительственных учреждений. В письмах находились ссылки на вредоносные архивы с локализованными названиями, размещенные в облачном хранилище Mega[.]nz. Сжатые файлы содержали вредоносный загрузчик Diaoyu и пустой PNG-файл. При выполнении определенных условий загрузчик размещал полезную нагрузку Cobalt Strike и написанный на Go фреймворк C2 VShell.

Инструментарий TGR-STA-1030 также включал веб-шеллы Behinder, Godzilla и Neo-reGeorg и инструменты для туннелирования GO Simple Tunnel (GOST), Fast Reverse Proxy Server (FRPS) и IOX. Кроме того, исследователи Unit 42 обнаружили кастомный руткит уровня ядра Linux eBPF под названием ShadowGuard, который, по их мнению, отличает арсенал именной этой группы. Помимо фишинга, TGR-STA-1030 для получения первоначального доступа эксплуатировала не менее 15 известных уязвимостей, включая уязвимости в SAP Solution Manager, Microsoft Exchange Server, D-Link, Ruijieyi Networks, Eyou Email System и Microsoft Windows. Исследователи обратили внимание на использование C2-доменов, которые могли показаться жертвам знакомыми: например, при атаках на франкоговорящие страны злоумышленники использовали

домен gouvn[.]me, а при атаках на европейские страны – домен dog3rj[.]tech.

Атаки SloppyLemming

APT

Целевой фишинг

Бэкдор

Инфраструктура облачных сервисов

DLL sideloading

С января 2025 года по январь 2026 года исследователи Arctic Wolf отслеживали масштабную кибершпионскую кампанию, которая, по их мнению, осуществлялась группой SloppyLemming (также известной как Outrider Tiger и Fishing Elephant) и была нацелена на госучреждения и объекты критической инфраструктуры в Пакистане и Бангладеш. За это время группа перешла от использования готовых инструментов для пентестов, таких как Cobalt Strike и Havoc C2, к разработке собственных инструментов на Rust, вместе с тем расширив C2-инфраструктуру, развернутую на платформе Cloudflare Workers, как минимум до 112 доменов (год назад было 13).

В ходе кампании злоумышленники использовали две различные цепочки атак. Основной вектор заключался в распространении правдоподобно выглядевших PDF-документов. Эти документы перенаправляли жертв на манифесты приложений ClickOnce, которые развертывали пакет для подмены DLL-библиотеки (DLL sideloading), состоящий из легитимного исполняемого файла Microsoft .NET (NGenTask.exe) и вредоносного загрузчика (mscorsvc.dll). Этот загрузчик расшифровывал и выполнял кастомный 64-разрядный шелл-код-имплант, который исследователи назвали BurrowShell. Во второй цепочке атаки злоумышленники использовали вредоносную Excel-таблицу, при открытии которой запускался VBA-макрос. Он скачивал два файла – легитимный бинарный файл Microsoft (phoneactivate.exe), предназначенный для подмены DLL-библиотеки, и вредоносный загрузчик (sppc.dll) – написанный на Rust кейлоггер с расширенными возможностями для разведки, в том числе функционалом сетевого сканирования. Проанализировав нескольких документов-приманок, соглашений об именовании C2-доменов, метаданных отправки в VirusTotal и инфраструктуру злоумышленников, исследователи пришли к выводу, что они нацелены на организации из ядерной энергетики, оборонно-промышленного комплекса, телекоммуникационной отрасли и правительственного сектора в Пакистане, из сфер энергетики, финансов и медиа в Бангладеш, а также из оборонно-промышленного комплекса в Шри-Ланке.

Активность китайско-говорящих групп

Атаки UAT-8837

APT

Эксплуатация общедоступных приложений

Уязвимость нулевого дня

Бэкдор

Исследователи Cisco Talos отследили группу UAT-8837. Совпадения ее тактик, техник и процедур с методами известных китайско-говорящих групп позволили исследователям сделать вывод, что это китайско-говорящая APT-группа. Она минимум с 2025 года атакует объекты критической инфраструктуры в Северной Америке, а TTP и действия злоумышленников после компрометации указывают на то, что их главная задача – получение первоначального доступа к значимым организациям. UAT-8837 получает первоначальный доступ в результате эксплуатации уязвимых серверов, в том числе с использованием уязвимости нулевого дня «Десериализация ViewState» (CVE-2025-53690) в продуктах SiteCore, или используя скомпрометированные учетные данные. Получив доступ, злоумышленники как правило развертывают программы с открытым исходным кодом для сбора конфиденциальной информации – учетных данных, конфигураций безопасности и сведений об Active Directory, чтобы создать несколько каналов доступа. Инструментарий включает следующее ПО: Earthworm – для туннелирования, SharpHound – для сбора данных из Active Directory, DWAgent – для удаленного администрирования, Certipy – для обнаружения и эксплуатации Active Directory, GoExec – для удаленного выполнения команд, Rubeus – для эксплуатации Kerberos, а также бинарные файлы на основе Impacket. Злоумышленники перебирают различные варианты инструментов, чтобы избежать обнаружения, создают учетные записи для устойчивого доступа к скомпрометированной среде, а в одном случае они украли DLL-библиотеки, используемые в продуктах жертвы – возможно, с целью дальнейшей компрометации цепочки поставок или для поиска эксплуатируемых уязвимостей в этих продуктах.

Активность, связанная с Ближним Востоком

Атаки MuddyWater

APT

Целевой фишинг

RAT

Бэкдор

Telegram как C2

Код, сгенерированный ИИ

Исследователи CloudSEK выявили фишинговую кампанию, приписываемую APT-группе MuddyWater (также известной как Earth Vetala, MERCURY, Mango Sandstorm, Static Kitten и TA450) и нацеленную на множество отраслей на Ближнем Востоке, в частности на дипломатические, морские, финансовые и телекоммуникационные организации. В ходе этой кампании злоумышленники рассылали фишинговые письма с DOC-файлом, замаскированным под руководство по кибербезопасности. Документ содержал вредоносный VBA-макрос, отвечающий за развертывание написанного на Rust бинарного импланта, который получил название RustyWater. Этот имплант (также отслеживаемый как Archer RAT и RUSTRIC) собирает информацию о компьютере жертвы, обнаруживает установленное защитное ПО и обеспечивает закрепление в системе с помощью ключа реестра Windows, а также устанавливает связь с C2-сервером для выполнения файловых операций и команд. Код макроса, извлеченный из фишингового документа, выдает поразительное сходство атаки с ранее задокументированными кампаниями MuddyWater. Пересечение – в характерном использовании функций WriteHexToFile и love_me_, в частности для встраивания шестнадцатеричной полезной нагрузки в элементы управления UserForm. В ходе анализа исследователи CloudSEK смогли обнаружить множество аналогичных приманок, ориентированных на ОАЭ и Ближний Восток. Эта кампания очень похожа на описанную исследователями Seqrite Labs. В своем отчете в декабре 2025 года они указали на использование RUSTRIC в атаках на ИТ-компании, провайдеров комплексного управления ИТ, кадровые агентства и компании-разработчики ПО в Израиле. Активность была приписана группе UNG0801 и получила название «Операция IconCat».

Команда Group-IB Threat Intelligence сообщила о новой кампании MuddyWater под названием «Операция Olalampo», нацеленной на организации и частных лиц преимущественно из стран Ближнего Востока и Северной Африки. Эта активность была впервые замечена 26 января 2026 года. Она началась с рассылки фишинговых писем с документом Microsoft Office, содержащим вредоносный макрос, и вела к развертыванию нового загрузчика следующего этапа или бэкдора. Были обнаружены загрузчики GhostFetch и HTTP_VIP, бэкдор на Rust под названием CHAR и усовершенствованный имплант GhostBackDoor.

Первая наблюдаемая цепочка начиналась с рассылки вредоносного документа Microsoft Excel якобы от энергетической и морской сервисной компании на Ближнем Востоке. Целью в этом случае, вероятно, были непосредственно эта организация или ее подрядчики. В итоге разворачивался бэкдор CHAR. Вторая цепочка эксплуатировала ту же тематику и была нацелена на те же компании, но выполнение вредоносного документа приводило к развертыванию загрузчика GhostFetch, который загружал GhostBackDoor. В третьем варианте использовался документ Microsoft Word на различные темы, в том числе связанные с авиабилетами и отчетами, его открытие приводило к развертыванию загрузчика HTTP_VIP, который загружал AnyDesk RMM.

GhostFetch – это загрузчик начального этапа, который выполняет первичную разведку системы, проверяет движения мыши и разрешение экрана, сканирует на наличие отладчиков, артефактов виртуальных машин и антивирусного ПО, после чего загружает полезные нагрузки следующего этапа напрямую в память и выполняет их. GhostBackDoor – это бэкдор второго этапа, который устанавливается GhostFetch и поддерживает интерактивную оболочку, чтение/запись файлов и повторный запуск GhostFetch. HTTP_VIP – это загрузчик, который выполняет разведку системы, он связывается с внешним C2-сервером для аутентификации и установки AnyDesk. CHAR – это написанный на Rust бэкдор, который управляется через Telegram-бота (с названием Olalampo и именем пользователя stager_51_bot) и позволяет перемещаться по каталогам и запускать команды cmd.exe или PowerShell. Выполнение PowerShell-команд запускает обратный прокси SOCKS5 или дополнительный бэкдор Kalim, выгрузку данных из браузеров, а также неизвестные исполняемых файлы, которые исследователям получить не удалось. Анализ исходного кода CHAR, в частности наличие эмодзи в отладочных строках, позволил сделать вывод, что ПО было разработано при помощи ИИ-инструментов.

Исследователи Unit 42 из компании Palo Alto Networks представили всесторонний анализ вредоносной активности группы Boggy Serpens (она же MuddyWater) за последний год. Характерная особенность этой группы – использование социальной инженерии и фишинговых рассылок. Boggy Serpens провела целенаправленную кампанию против национальной морской и энергетической организации на Ближнем Востоке. Исследователи выявили четыре волны атак на один объект в период с августа 2025 года по февраль 2026 года, что свидетельствует о настойчивых попытках злоумышленников проникнуть в региональную морскую инфраструктуру. Первая кампания была ориентирована на инженеров, поскольку использовалась отраслевая терминология на тему подводных трубопроводов. Документ-приманка содержал встроенный

макрос. Во второй атаке использовался файл Microsoft Excel, имитировавший внутренние финансовые отчеты организации-жертвы. В таблице были расписаны календарь платежей и денежные потоки. Параллельно злоумышленники атаковали конкретного человека, связанного с организацией. Они подготовили документ Microsoft Word, содержавший персональный авиабилет на рейс Air Arabia. Открытие этого файла приводило к установке бэкдора GhostBackDoor, о котором сообщила Group-IB. В четвертой атаке использовался файл Microsoft Excel, который инициировал установку совершенно нового семейства полезных нагрузок Nuso (исследователи Group-IB назвали его HTTP_VIP).

За год Boggy Serpens регулярно взламывала официальные правительственные и корпоративные аккаунты, чтобы обойти стандартную фильтрацию электронной почты. В недавних кампаниях злоумышленники использовали следующие инструменты для закрепления и обхода защитных решений: бэкдор UDPGangster, бэкдор BlackBeard на Rust, LampoRAT (он же как CHAR, Olalampo), Telegram Bot API, написанный на Rust и используемый в качестве C2-сервера. LampoRAT маскируется под исполняемый файл легитимного защитного ПО «Лаборатории Касперского» (avp.exe) и содержит строку Kaspersky в метаданных файла. Более того, в строках бинарного файла был обнаружен явный стилистический артефакт, однозначно указывающий на то, что для ускорения разработки вредоносного ПО злоумышленники прибегали к помощи ИИ.

Кампания с распылением паролей, нацеленная на облачные среды

APT

Эксплуатация общедоступных приложений

Предположительно киберкинетическая операция

Исследователи Check Point Research сообщили об обнаружении масштабной кампании с распылением паролей от аккаунтов Microsoft 365 государственных и частных организаций, которая началась в начале марта. Злоумышленники нацеливались на израильские организации, однако атака затронула компании в ОАЭ, Саудовской Аравии, Европе, США и Великобритании. Сканирование проводилось с выходных узлов Tor, которые часто менялись для обхода блокировки. При сканировании использовался User-Agent, имитировавший Internet Explorer 10 (IE10): Mozilla/5.0 (совместимый; MSIE 10.0; Windows NT 6.1; Trident/6.0). Когда злоумышленники находили действительные учетные данные, они выполняли полный процесс входа с IP-адресов VPN (диапазон Windscribe 185.191.204.X или диапазон NordVPN 169.150.227.X), геолоцированных в Израиле, чтобы обойти географические ограничения. Хотя подобные кампании распространены, конкретно эта привлекла внимание исследователей, потому что они заметили некоторую корреляцию между

целями кампании и городами, которые подверглись иранским ракетным ударам в марте, что указывает на возможную поддержку кинетических операций и деятельности по оценке ущерба после бомбардировок. Исследователи с некоторой уверенностью предположили, что актор, стоящий за активностью с распылением паролей от аккаунтов Microsoft 365, имеет иранское происхождение. Такой вывод они сделали, полагая, что атаки на израильские органы местного самоуправления и организации из спутниковой, авиационной, энергетической и морской отраслей могут быть выгодны Ирану. Анализ журналов Microsoft 365 выявил пересечения с деятельностью группы Gray Sandstorm – например, использование инструментов для пентеста в проведении атак через выходные узлы Tor. Злоумышленники использовали коммерческие VPN-узлы, размещенные на AS35758 (Rachamim Aviel Twito), что согласуется с недавней активностью, связанной с операциями Ирана на Ближнем Востоке.

Атаки Void Manticore

Хактивизм

Вайпер

Код, сгенерированный ИИ

Исследователи Check Point Research опубликовали технический профиль группы Void Manticore (также известной как Storm-0842, Red Sandstorm и Banished Kitten), проводящей разрушительные операции со взломом и кражей информации. Группа управляет несколькими онлайн-персонажами, включая Handala Hack, на ней ответственность за многочисленные атаки на организации в Израиле, а в последнее время она распространила свою деятельность на американские предприятия – одной из жертв стал производитель медицинских приборов и оборудования Stryker.

За последние несколько месяцев исследователи Check Point Research зафиксировали сотни попыток входа с подбором паролей в корпоративную VPN-инфраструктуру – в этой брутфорс-атаке использовалась инфраструктура Handala. Эта активность обычно исходила из коммерческих VPN-узлов. В недавней атаке, приписываемой Handala, первоначальный доступ к сети предположительно был установлен за несколько месяцев до разрушающей фазы. Чтобы добраться к хостам, к которым не было прямого доступа из-за пределов сети, злоумышленники вручную установили NetBird. В ходе разрушительной фазы атаки они, по словам исследователей, одновременно применяли четыре различные техники уничтожения данных.

В первом случае через сценарий входа в систему, заданный групповой политикой (Group Policy logon scripts), создавалась запланированная задача, запускавшая batch-файл, который, в свою очередь, запускал Handala Wiper в виде исполняемого файла, который переписывает данные и удаляет MBR.

Во втором случае злоумышленники внедряли дополнительный кастомный PowerShell-вайпер, который также распространялся при помощи logon-скриптов, заданных в групповой политике. Изучив структуру кода и комментарии, исследователи предположили, что этот PowerShell-скрипт был разработан с использованием искусственного интеллекта.

Иногда вместо кастомных вайперов злоумышленники пытались использовать VeraCrypt – популярную легитимную утилиту для шифрования дисков. В этом случае они подключались к скомпрометированному хосту через RDP и использовали дефолтный веб-браузер системы для загрузки программного обеспечения с официального сайта.

Наконец, иногда операторы Handala Hack просто вручную удаляли виртуальные машины с платформы виртуализации или файлы со скомпрометированных компьютеров. Этот процесс подразумевал вход через RDP, выделение всех файлов и их удаление.

RDP-соединения злоумышленников инициализировались с хостов, имеющих дефолтные имена в формате DESKTOP-XXXXXX или WIN-XXXXXX.

Киберкриминал и прочее

Атаки с использованием LockBit 5.0

Киберкриминал

Шифровальщики

Вредоносное ПО под Linux

Двойное вымогательство

В сентябре 2025 года вышла новая версия программы-вымогателя LockBit, совместимая с Windows, Linux и ESXi. Как рекламировали злоумышленники, в этой версии улучшен функционал обхода защиты и быстрого шифрования. Они утверждали, что программа-вымогатель может работать на всех версиях Proxmox – платформы виртуализации с открытым исходным кодом, которая внедряется на предприятиях в качестве альтернативы коммерческим гипервизорам, что делает ее еще одной привлекательной целью атак вымогателей. Подразделение Threat Research Unit (TRU) компании Acronis проанализировало программу-вымогатель LockBit версии 5.0 и информацию о ее жертвах на сайте утечки данных. Там указано, что LockBit позволят атаковать любые организации, включая объекты критической инфраструктуры и медицинские учреждения. Вместе с тем запрещает атаки на страны постсоветского пространства. Анализируя список последних жертв с сайтов утечки данных, исследователи отметили, что чаще всего с использованием LockBit атаковали частные предприятия. Жертвами также стали медицинские и образовательные учреждения, финансовые и производственные компании,

государственные организации. Большинство жертв находятся в США, Италии, Бразилии, Испании, Мексике. LockBit 5.0 использует ту же схему шифрования, что и его предшественник: XChaCha20 – для симметричного и Curve25519 – для асимметричного шифрования. Новая версия предлагает опцию мьютекса для обеспечения работы только одного экземпляра в среде единовременно, функционал вайпера и функцию, позволяющую отложить выполнение перед шифрованием.

Атаки Diesel Vortex

Киберкриминал

Новый актор

Целевой фишинг

Конвергенция кибер- и традиционной преступности

В феврале исследователи Have I Been Squatted – компании-разработчика платформы для защиты брендов от тайпсквоттинга, вместе с сообществом независимых исследователей Ctrl-Alt-Intel обнаружили финансово мотивированную группу Diesel Vortex, которая похитила учетные данные грузовых и логистических операторов в США и Европе в ходе фишинговых атак с использованием 52 доменов. В рамках кампании, которая проводится с сентября 2025 года, группа украла 1649 уникальных учетных данных ключевых платформ и поставщиков услуг из сферы грузоперевозок. Исследователи раскрыли эту кампанию после того, как обнаружили уязвимый GIT-репозиторий с SQL-базой данных фишингового проекта, который Diesel Vortex назвала GlobalProfit и продавала другим злоумышленникам под именем MC Profit Always. Репозиторий содержал файл с логами Telegram-вебхуков, позволивший раскрыть взаимодействие операторов фишингового сервиса. Учитывая язык, на котором велась переписка, исследователи сделали вывод, что Diesel Vortex – армяноязычная группа.

Diesel Vortex разработала специализированную фишинговую инфраструктуру для платформ, которыми ежедневно пользуются фрахтовые брокеры, автотранспортные компании и операторы цепочек поставок. Группа атаковала доски объявлений о загрузке, порталы управления автопарком, системы топливных карт и биржи грузовых перевозок. В ходе атаки она рассылала фишинговые письма с помощью специального пакета, который включал Zoho SMTP и Zeptomail, в поля «Отправитель» и «Тема» вписывала кириллические символы вместо идентично выглядящих латинских, что позволяло обходить фильтры безопасности. Кроме того, она использовала голосовой фишинг и проникновение в Telegram-каналы, популярные среди сотрудников транспортных и логистических компаний. При клике на ссылку жертва попадала на минималистичную HTML-страницу в домене .com с полноэкранным iframe, загружающим фишинговый контент. Далее запускался 9-этапный механизм маскировки, в результате которого

запрашивался «системный» домен (.top/.icu), на котором находилась финальная фишинговая страница. Поддельные страницы представляли собой попиксельные клоны конкретных логистических сервисов и в зависимости от задач захватывали учетные данные, информацию о разрешениях на различные виды деятельности, идентификаторы компаний и транспортных средств, логины для входа в специализированный сервис, коды двухфакторной аутентификации, токены безопасности, суммы платежей, имена получателей и номера чеков. Оператор фишингового сервиса решал, когда перейти к следующему этапу атаки, через Telegram-боты. Он мог дополнительно запросить пароль для входа в Google, Microsoft Office 365 и Yahoo, двухфакторную аутентификацию, перенаправить жертву или оборвать сессию.

Исследователи заявляют, что операция Diesel Vortex, в которой использовались домены панелей управления и фишинговые домены, а также репозитории GitLab, была пресечена совместными усилиями специалистов GitLab, Cloudflare, Google Threat Intelligence, CrowdStrike и Microsoft Threat Intelligence Center. Опираясь на факты, исследователи определили, что группа Diesel Vortex не только похищала учетные данные, но и координировала действия других злоумышленников, которые выдавали себя за перевозчиков, взламывали почтовые ящики, занимались двойным посредничеством или перенаправляли грузы. Двойное посредничество заключается в следующем: злоумышленники, используя украденные данные перевозчика, бронируют грузы, а затем перераспределяют или перенаправляют их в подставные пункты выдачи, чтобы физически похитить товар.

Атаки с использованием C77L

Киберкриминал

Шифровальщики

Эксплуатация общедоступных приложений

Исследователи F6 выявили активность вымогателей, в рамках которой менее чем за год были атакованы более 40 российских и белорусских предприятий. Программа-вымогатель C77L, распространяющаяся по модели RaaS, вышла в марте 2025 года и нацелена на российский и белорусский малый и средний бизнес, в первую очередь из сфер торговли, производства и услуг. Среди жертв оказались и государственные организации. По итогам 2025 года C77L заняла шестое место по количеству атак с использованием программ-вымогателей. Исследователи полагают, что C77L была создана как отдельная партнерская программа участниками Proton. C77L имеет схожие черты с такими семействами, как Proton, Proxima и LokiLocker. Она разработана на C++ и отличается высокой скоростью шифрования данных. Менее чем за год разработчики выпустили пять версий программы-вымогателя. Атаки с использованием

C77L непродолжительные: злоумышленники не стремятся похитить данные жертв, а сосредотачиваются исключительно на шифровании информации в расчете на быструю и стабильную прибыль. По словам исследователей, основной вектор атаки партнеров C77L – это подбор паролей к аккаунтам общедоступных служб удаленного доступа (RDP и VPN). Злоумышленники обычно проникают в инфраструктуру жертв ночью. Их атаки нацелены только на Windows-системы. Партнеры C77L не утруждают себя использованием сложных или инновационных методов. Для таких атак не нужна высокая квалификация – злоумышленники следуют шаблонным инструкциям и используют для автоматизации действий готовые скрипты. Несмотря на это, большинство атак на российские и белорусские предприятия оказалось успешными.

Атаки Warlock

Киберкриминал

Шифровальщики

Эксплуатация общедоступных приложений

BYOVD

DLL sideloading

Исследователи Trend Micro зафиксировали новую тактику вымогателей Warlock. Группа продемонстрировала новые техники закрепления, горизонтального перемещения и обхода защиты. Она стала использовать программу для удаленного управления TightVNC для сохранения контроля, новые инструменты с открытым исходным кодом для связи с C2-сервером, а также технику BYOVD, которая подразумевает эксплуатацию уязвимости в драйвере NSec для завершения процессов безопасности. Метод получения первоначального доступа к сетям жертв у Warlock не изменился и по-прежнему предполагает эксплуатацию необновленных серверов Microsoft SharePoint. Согласно данным телеметрии Trend Micro, рабочий процесс SharePoint (w3wp.exe) запускал агент Cobalt Strike, использующий технику DLL-sideloading с легитимным бинарным файлом MsMpSrv.exe для браузера Microsoft Edge, утилиту EndProcess.exe, которая, вероятно, использовалась для отключения защитных решений или других процессов, и msiexec.exe, которая использовалась для автоматической загрузки и установки легитимного инструмента Velociraptor, скрывавшегося под названием v4.msi и размещенного в облачном хранилище Supabase. Кроме того, было замечено, что процесс w3wp.exe записывал веб-шелл cproxy.aspx на диск, чтобы сохранить присутствие в среде IIS/SharePoint. Злоумышленники также использовали новый и легковесный инструмент туннелирования Yuze с открытым исходным кодом. Этот инструмент, написанный на C, предназначен для проникновения в интранет и поддерживает прямое и обратное туннелирование через прокси-сервер SOCKS5. Злоумышленники использовали групповые политики Active Directory для массового распространения компонентов программ-вымогателей, размещенных в общих папках SYSVOL и NETLOGON. Согласно данным на сайте утечек Warlock за второе полугодие 2025 года,

больше всего пострадали технологическая и производственная отрасли, правительственный сектор и сфера образования, а наиболее часто атакованными странами были США, Великобритания, Германия и Россия.

Операция CamelClone

APT

Целевой фишинг

Облачные сервисы как C2

APT-команда Seqrite Labs выявила кампанию, получившую название «Операция CamelClone», которая была нацелена на несколько стран. Пострадали государственные учреждения, оборонные и военные ведомства, департаменты иностранных дел и международного сотрудничества, политические и дипломатические учреждения, организации из энергетической и других стратегических отраслей в Алжире, Монголии, Кувейте и на Украине. Злоумышленники использовали целевые фишинговые письма с ZIP-вложениями. Внутри одного из архивов были LNK-файл и изображение-приманка с логотипом MonAtom LLC – монгольской госкомпании, занимающейся разведкой и добычей урана, а также развитием атомной энергетики. LNK-файл содержал вредоносную PowerShell-команду, которая скачивала из анонимного облачного хранилища JavaScript-загрузчик, отслеживаемый как HOPPINGANT. Он загружал документ-приманку и еще один архив с исполняемым файлом – легитимной версией программы Rclone v1.70.3, которая собирала и скачивала файлы с системы жертвы. В этой кампании для размещения и доставки вредоносных программ использовались общедоступные сервисы. Например, в качестве удаленной конечной точки для украденных данных злоумышленник использовал общедоступное облачное хранилище MEGA[.]nz. На момент публикации отчета в марте исследователи не связывали эту кампанию с какой-либо известной группой.

Атаки Hydra Saiga

APT

Целевой фишинг

Telegram как C2

Бэкдор

LOTL

Эксплуатация общедоступных приложений

Атаки на АСУ

Согласно анализу, проведенному VMRay, группа Hydra Saiga (также известная как Yorotrooper и Tomiris) скомпрометировала как минимум 34 организации в восьми странах и провела разведку на более чем 200 дополнительных объектах по всему миру, среди которых критически важные водные и энергетические объекты в Центральной Азии. В период с сентября 2024 года по март 2025 года Hydra Saiga осуществила масштабную кампанию, нацеленную на важнейшие объекты водного хозяйства, научно-исследовательские институты и министерства. Атаки были сосредоточены на инфраструктуре, связанной с двумя крупнейшими реками в регионе: Сырдарьей и Амударьей. В результате были скомпрометированы оператор гидроэлектростанций и связанная с водным хозяйством компания в Кыргызстане, региональная администрация,

научно-исследовательский институт и Министерство водного хозяйства в Узбекистане, а также Министерство энергетики и водных ресурсов в Таджикистане.

Кроме того, по данным исследователей, 29 апреля 2024 года операторы Hydra Saiga попытались получить доступ к нескольким уязвимым SCADA-системам и производителям промышленного оборудования в различных странах, включая Аргентину, Бразилию, Индию, Нидерланды и Чехию. Эти попытки, по всей видимости, не увенчались успехом, тем не менее уже на следующий день злоумышленники попытались получить доступ к газораспределительной системе в российском регионе, граничащем с Казахстаном. Исследователи предполагают, что операторы Hydra Saiga проверяли свои возможности и экспериментировали с SCADA-терминалами в рамках подготовки к атаке на российские организации, поскольку цели в этот раз не совпадали с обычными жертвами группы.

Исследователи выявили две целевые фишинговые кампании с использованием защищенных паролем RAR- или ISO-архивов, проведенные группой в декабре 2024 года. Отличительной чертой группы является использование Telegram Bot API для связи с C2-сервером. На этапе постэксплуатации использовались ручной ввод команд с клавиатуры, метод LOTL и новый инструмент для кражи данных браузера, который обходит Chrome App-Bound Encryption – проприетарный механизм Chrome защиты пользовательских данных. Злоумышленники также использовали комбинацию кастомных имплантов, написанных на Rust, Go и Python. Исследователи обнаружили образцы JLORAT – бэкдора на Rust, который «Лаборатория Касперского» впервые описала в апреле 2023 года и связала с группой Tomiris.

Центр реагирования на инциденты информационной безопасности промышленных инфраструктур «Лаборатории Касперского» (Kaspersky ICS CERT) — глобальный проект «Лаборатории Касперского», направленный на координацию усилий производителей систем автоматизации, владельцев и операторов промышленных объектов, а также исследователей ИТ-безопасности для защиты промышленных предприятий от кибератак. Kaspersky ICS CERT направляет свои усилия в первую очередь на выявление потенциальных и существующих угроз, нацеленных на системы промышленной автоматизации и промышленный интернет вещей.

Kaspersky ICS CERT ics-cert@kaspersky.com