Kaspersky ICS CERT

kaspersky

APT- и финансовые атаки на промышленные организации во втором квартале 2026 года

03.08.2026

Версия 1.0

Данный обзор представляет собой сводку публикаций об APT- и финансовых атаках на промышленные предприятия, информация о которых была раскрыта во втором 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

Второй квартал 2026 года оказался беспрецедентно плотно наполнен публикациями о целевых атаках на АСУ. Упомянутый в нашем обзоре за первый квартал 2026 года джинн киберармагеддона стал делать все более частые вылазки из своей уютной бутылки в разные уголки изменившегося за годы его добровольного заточения мира. При этом на своем пути он все реже и со все меньшим усердием пытается строить замки и все чаще, и все более настойчиво и дерзко, пробует разрушать города.

Самый яркий среди его новых «подвигов» – атака на израильское предприятие пищевой промышленности, значимым результатом которой стала поломка оборудования холодильной установки с выбросом рабочего тела в атмосферу. Безусловно, эта история заслуживает особого внимания – атакующие неожиданно продемонстрировали весьма неплохие знания в области устройства, принципов работы и уязвимостей функциональной безопасности современных промышленных охладительных систем. Следующий по значимости «подвиг» – кампания, нацеленная на ПЛК CompactLogix и Micro850 производства Rockwell Automation, «торчащие» в интернет на объектах критической инфраструктуры США, в результате которой атакующим удалось украсть данные проектов и подменить показатели, передаваемые на HMI и рабочие станции операторов. На третьем месте – масштабная кампания по сканированию и фингерпринтингу доступных из интернета Modbus-устройств с попытками их выборочного DoS, оценка результативности которой осталась за скобками опубликованного исследования.

Несмотря на возрастающую их частоту, многие из современных обнаруженных попыток сделать что-либо нелегитимное с системами промышленной автоматизации кажутся или робкими, или ленивыми, или неуклюжими. Яркий пример тому – вредонос, нацеленный на опреснительные и водоочистные установки в Израиле. То, что в руки исследователей попала настолько сырая и неготовая к «боевой»

эксплуатации версия ВПО говорит, вероятно, о крайней неаккуратности и незрелости его разработчиков.

Огромным контрастом новым стандартам технического и организационного уровня киберфизических атак стал внезапно обнаруженный вредонос fast16, который выглядит как настоящее кибероружие, почти дотягивающее по уровню погружения в предметную область до пресловутого Stuxnet. Нежданная находка оказалась капсулой времени – исследование возвращает нас более чем на 20 лет назад. В 2005 году, когда был создан этот вредонос, траектории полета фантазии атакующих проходили много выше, чем те, что массово расчерчивают цифровое небо сейчас. Целью вредоноса тогда оказались серьезные математические пакеты, использовавшиеся для моделирования сложных физических процессов, таких как процессы детонации. Зловред выбирал вычисления, моделирующие условия запуска неконтролируемой ядерной реакции (читайте атомного взрыва), и вносил тонкие коррективы в расчеты, нарушающие процесс моделирования. По всей видимости, вредонос имел историю практического использования – разработчики явно развивали его, добавляя поддержку других версий целевых программных пакетов моделирования. Интересно: сколькими еще подобными находками нас порадуют киберархеологи? Второй важный вопрос: какое влияние оказали эта и другие, пока никому неизвестные мегаразработки доисторических хакеров на процессы технологического, экономического и политического развития в разных уголках планеты? И третий вопрос, который невозможно выбросить из головы: есть ли еще разработки такого уровня, которые и сейчас незаметно используются, тормозя развитие в направлениях, критически важных для государств и человечества в целом?

Возможно, одним из самых тревожных звонков в наблюдениях за изменениями ландшафта киберфизических угроз прозвучала публикация об использовании ML-агентов и мощных облачных инструментов Claude и GPT-4.1 в атаках на мексиканские государственные организации и промышленные предприятия. В ней описывается пока еще крайне редкий случай применения ИИ на большинстве этапов развития атаки внутри атакованной сети – исследования инфраструктуры, поиска, приоритизации целей и продвижения. В одном из случаев ИИ указал злоумышленникам на интерфейс к OT-части инфраструктуры атакованной организации и предложил способ получения доступа к нему. И хотя эта первая задокументированная попытка ИИ дотянуться до OT и робка, и не увенчалась успехом, мы видим, как ML-средства, включая большие публичные модели, все чаще используются промышленными предприятиями для решения все более разнообразных задач в OT-контуре

и, следовательно, копят в себе все больше знаний о предметной области, которыми обязательно когда-нибудь воспользуются и злоумышленники.

Так что, по все видимости, недалек тот день, когда ML/ИИ-инструменты смогут компенсировать разницу между современными массовыми киберзлодеями и классиками киберфизических атак из недалекого прошлого – и повседневная реальность промышленной кибербезопасности сделает резкий поворот, к которому лучше бы начать готовиться уже позавчера.

Атаки, нацеленные на российские организации

Атаки Geo Likho

APT

Целевой фишинг

Шпионское ПО

Группа Geo Likho (также известная как Batavia) проводит целевые атаки на организации в России и Беларуси как минимум с июля 2024 года. Исследователи «Лаборатории Касперского» изучили недавнюю активность этой группы. Она использовала целевой фишинг в качестве вектора первоначального доступа: когда пользователь переходил по ссылке, которая выглядела как путь к официальному документу, на его компьютер загружался вредоносный VBE-скрипт, запускавший трехступенчатое заражение. Злоумышленники использовали тот же набор инструментов, что и в предыдущих кампаниях, включая VBE-загрузчик, имплант первого этапа атаки на языке Delphi и вредоносный файл второго этапа атаки на C++. Исследователи обнаружили, что атакующие стали создавать отдельное вредоносное ПО под конкретную инфраструктуру жертвы. Были выявлены сходства между кодом VBE-загрузчика из предыдущих и текущих кампаний, кодом функций импланта первого этапа атаки, а также сходства в расшифрованных строках полезных нагрузок. Данные телеметрии «Лаборатории Касперского» позволили идентифицировать примерно 260 жертв в России, около 20 жертв в Беларуси, а также единичные случаи в Германии, Сербии и Гонконге. Жертвы в последних трех странах, скорее всего, случайны. Злоумышленники ориентируются в первую очередь на авиационные и судоходные компании, однако среди мишеней часто встречаются организации из сфер машиностроения, образования, а также госучреждения.

Атаки BO Team

APT

Целевой фишинг

Вредоносное ПО под Linux

Бэкдор

Исследователи «Лаборатории Касперского» продолжают отслеживать атаки группы BO Team на российские организации. В ходе исследования инфраструктуры злоумышленников исследователи выявили несколько примечательных артефактов, а затем обнаружили исходный код в приватном Git-репозитории BO Team. Доступ к кодовой базе позволил провести углубленный анализ основного бэкдора группы под названием ZeronetKit, рассмотреть его архитектуру и ключевые возможности. В недавних атаках активно использовалась новая версия этого бэкдора, предназначенная для работы в операционных системах Linux, что свидетельствует о расширении арсенала злоумышленников и адаптации вредоносного ПО под различные типы целевых систем.

В первом квартале 2026 года BO Team атаковала 20 организаций. Для получения первоначального доступа злоумышленники снова использовали таргетированный фишинг и бэкдор из семейства BrockenDoor. Для закрепления в системе, повторного выполнения полезной нагрузки и запуска образца бэкдора ZeroSSH они использовали задания планировщика Windows. Выявленные исследователями индикаторы указывают на вероятные пересечения с активностью другой проукраинской группы – Head Mare. Изученные кампании BO Team были нацелены на российские организации из нефтегазовой, производственной, телекоммуникационной и других отраслей.

Атаки PhantomCore

Киберкриминал

Целевой фишинг

RAT

Исследователи F6 8 апреля обнаружили таргетированную фишинговую атаку группы PhantomCore (также известной как HeadMare) на российскую промышленную компанию. Фишинговые письма с темой «О рабочем визите делегации КНДР в апреле 2026» рассылались на различные адреса целевой компании. Они содержали файл-приманку в формате PDF и ZIP-архив с вредоносным HTA-файлом со скрытыми атрибутами файла и LNK-файлом, основная цель которого – запуск HTA-файла. HTA-файл содержал в своей разметке тег script, внутри которого располагался VBS-скрипт, выполняемый после запуска файла. В результате исполнения этого сценария на устройство жертвы загружались дополнительные PowerShell-скрипты, которые помещались в ключ реестра для закрепления, а затем запускались. Один из загруженных PowerShell-скриптов представляет собой вредоносное ПО типа RAT, получившее название KermitRAT. В ходе анализа исследователи получили список команд с C2-сервера KermitRAT. В результате выполнения одной из них загружался MeshAgent – агент удаленного мониторинга и управления (RMM) из проекта MeshCentral.

Атаки Eagle Werewolf

APT

Новый актор

Целевой фишинг

Фишинг в Telegram

Бэкдор

RAT

Код, сгенерированный ИИ

В феврале исследователи BI.ZONE выявили три независимо действующих кластера, распространявших вредоносное ПО под видом сервисов для регистрации устройств Starlink и приложений для обучения управлению дронами. Группа Paper Werewolf (она же GOFFEE) развернула EchoGather – RAT на языке C#, закодированный Base64 и зашифрованный алгоритмом XOR, который проверяет запуск в виртуальной среде, а также использует жестко закодированный с помощью SHA-256 ключ для взаимодействия с C2-сервером по HTTPS POST. Группа также собирала учетные данные аккаунтов в Telegram, используя поддельный портал для регистрации устройств спутниковой связи Starlink. Группа Versatile Werewolf (она же HeartlessSoul) выстроила цепочку заражения – от MSI-установщика через написанные с использованием генеративного ИИ PowerShell- и VBS-скрипты до .NET-загрузчика, который устанавливал через легитимный бинарный файл Windows имплант фреймворка постэксплуатации Sliver и создавал для закрепления в системе задачу в планировщике Windows, замаскированную под обновление Microsoft Edge. Исследователи также обнаружили разработанный с помощью ИИ и написанный на JavaScript SoullessRAT, который собирал данные из Outlook и делал скриншоты.

В статье раскрывается информация о третьем акторе, который участвовал в кибершпионской кампании с использованием фейковых сервисов для регистрации устройств Starlink. Эта активность была связана с более ранней атакой, описанной Positive Technologies. После ретроспективного анализа исследователи BI.ZONE решили выделить вредоносную активность в отдельный кластер, который назвали Eagle Werewolf. По их данным, Eagle Werewolf действует как минимум с мая 2023 года и атакует преимущественно государственные организации, промышленные предприятия и физических лиц, связанных с разработкой и производством беспилотников. Для получения первоначального доступа Eagle Werewolf использовала таргетированные фишинговые рассылки. Примечательно, что в феврале группа скомпрометировала один из тематических Telegram-каналов для распространения дроппера на Rust (фреймворк Tauri, AES-256-CBC, деривация ключа с помощью PBKDF2), а также дроппера на Go, который создавал скрытую локальную учетную запись администратора и настраивал SSH-туннелирование. В ходе кампании также устанавливались AquilaRAT (Rust, список адресов C2-серверов, зашифрованный с помощью алгоритма Blowfish, система задач и подзадач на основе JSON, загрузка файлов по частям) и Go2Tunnel для постоянного SSH-туннелирования.

Атаки Cloud Atlas

APT

Целевой фишинг

Компрометация легитимных почтовых сервисов

Компрометация сайтов

Брокеры доступа

Коллаборация групп злоумышленнико

Шпионское ПО

Возможная конвергенция APT и киберкриминала

В конце 2025 года исследователи Positive Technologies обнаружили кампанию группы Cloud Atlas, нацеленную на российские организации из промышленной отрасли и ВПК. Для первоначального проникновения использовалась целевая фишинговая рассылка от имени реального контрагента через скомпрометированный почтовый ящик. В качестве загрузчика использовался DOC-файл-приманка. При открытии он инициировал запрос к удаленному RTF-шаблону, ссылка на который была встроена во внутренний поток 1Table. Последующая доставка промежуточных компонентов и полезной нагрузки осуществлялась через WebDAV-ресурсы, опубликованные на скомпрометированных легитимных сайтах. Конечной полезной нагрузкой стала вредоносная программа DeerStealer, доставленная загрузчиком HijackLoader. Анализ исходного кода страниц на скомпрометированных доменах выявил HTML- и JavaScript-инъекции с функциями перенаправления, отслеживания и загрузки внешнего контента. Характер и логика инъекций не соответствовали типичным тактикам, техникам и процедурам Cloud Atlas. Анализ обнаруженной JavaScript-инъекции показал, что ее структура и логика работы характерны для группы Mustard Tempest (также известной как TA569, DEV-0206, Gold Prelude). Это брокер начального доступа, его основным инструментом является JavaScript-загрузчик SocGholish (FakeUpdates), который внедряется в скомпрометированные сайты и имитирует обновление браузера или программного обеспечения. В то время, когда Mustard Tempest внедряла вредоносное ПО через схему FakeUpdates, с тех же доменов по отдельным URL-адресам распространялось вредоносное ПО Cloud Atlas. Это наблюдение контрастирует с описанными ранее методами и тактиками группы Cloud Atlas. В предыдущих кампаниях она, как правило, использовала фишинговые документы, удаленные шаблоны и полезную нагрузку, размещенные на контролируемых ею серверах, а не на скомпрометированных легитимных сайтах, уже используемых другими злоумышленниками. Таким образом, считают исследователи Positive Technologies, можно рассматривать как минимум две гипотезы. Первая заключается в том, что Cloud Atlas частично скорректировала свои TTP, самостоятельно скомпрометировала легитимные веб-ресурсы и использовала их для доставки вредоносного ПО. Вторая гипотеза указывает на то, что Cloud Atlas изменила свои TTP, но не взламывала веб-ресурсы самостоятельно, а приобрела доступ у Mustard Tempest. Это значительно усложняет анализ: становится труднее разграничивать роли отдельных участников атаки и точно определять группы.

Атаки Unicorn

Киберкриминал

Целевой фишинг

Шпионское ПО

Исследователи F6 30 марта обнаружили новую атаку группы Unicorn, которая с сентября 2024 года атакует российские компании. У злоумышленников узнаваемый почерк: таргетированные фишинговые рассылки, долго используемый C2-сервер и минимальные изменения вредоносного ПО. Главной мишенью новой кампании была авиастроительная промышленность. Письмо содержало ZIP-архив с HTA-файлом внутри. При запуске этот файл извлекал восемь идентичных скриптов в две разные директории.

Исследователи выявили несколько изменений по сравнению с предыдущей активностью. Одно из них – переход с VBS-скриптов на JavaScript-скрипты. Для закрепления JS-скрипты добавлялись в автозагрузку через реестр (RunOnce) и планировщик задач. Возможности JS-скриптов аналогичны тем, что прежде были реализованы в VBS-скриптах Unicorn: сбор файлов с определенными расширениями из директорий пользователя, сбор данных из браузеров и Telegram, а также файлов со съемных дисков, взаимодействие с C2-сервером для получения команд и отправка собранных файлов. Еще одно изменение коснулось HTA-файла – в нем больше нет финального POST-запроса (в предыдущих атаках POST-запрос отправлялся в Discord).

Атаки CapFix

Киберкриминал

Целевой фишинг

Компрометация сайтов

Бэкдор

DLL sideloading

Сертификаты разработчика

Исследователи Positive Technologies раскрыли атаки группы CapFix против российских организаций в промышленной и авиационной отраслях. Ранее группа использовала в атаках технику ClickFix, а также фишинговые файлы на темы криптовалют и бронирования отелей. В конце декабря 2025 года исследователи заметили несколько PDF-документов, содержащих ссылки на скачивание RAR-архива со скомпрометированного легитимного ресурса. Внутри архива находился CHM-скрипт, который загружал со скомпрометированного легитимного домена MSI-файл и открывал подлинный PDF-документ. MSI-файл был подписан компанией QILING Tech и замаскирован под приложение QILING Disk Master. При запуске он создавал папку и загружал в нее несколько DLL-библиотек, а также легитимный исполняемый файл MetadataConvert.exe, уязвимый к технике DLL sideloading. Выполнение этого файла запускало цепочку DLL sideloading, в результате чего загружался CapDoor в качестве полезной нагрузки. Проанализировав множество различных версий бэкдора CapDoor и используемых цепочек его поставки, исследователи установили, что вредоносное ПО активно развивается и регулярно обновляется. В ранних версиях CapDoor распространялся как исполняемый файл, а в

новых атаках – в виде шелл-кода. Прежде для установки CapDoor злоумышленники использовали загрузчик GHOSTPULSE (IDATLOADER или HIJACKLOADER). В более поздних версиях они самостоятельно реализовали сложную цепочку DLL sideloading. Ранние версии CapDoor не позволяли делать скриншоты экрана, эта функциональность появилась в более поздних версиях. Анализируя это вредоносное ПО, исследователи Positive Technologies обнаружили образцы, которые в качестве финальной полезной нагрузки загружали SectopRAT или ArechClient2.

Атаки Fluffy Wolf

Киберкриминал

Целевой фишинг

Ссылки на GitHub

Бэкдор

Шифровальщик

Исследователи BI.ZONE зафиксировали серию атак кластера Fluffy Wolf (также известного как VasyGrek) с марта по май. Злоумышленники рассылали фишинговые письма российским организациям из строительной, машиностроительной и производственной отраслей, а также сфер консалтинга, розничной торговли и электронной коммерции. В письмах они выдавали себя за сотрудников специализированных организаций – предлагали погасить финансовые задолженности и ознакомиться с вложенными документами. Исследовали выявили два типа фишинговых писем. В одном был RAR-архив с вредоносным ПО внутри, а в другом – ссылка на репозиторий GitHub, откуда загружался RAR-архив с вредоносным ПО. Профили злоумышленников на GitHub включали множество репозиториев, содержавших RAR-архивы, исполняемые файлы (с расширениями .scr, .com и .exe), текстовые файлы с полезной нагрузкой (перевернутой и закодированной в Base64), а также обфусцированные Batch- и JS-скрипты. RAR-архивы содержали вредоносные загрузчики и дропперы для доставки на целевую систему стилера PureLogs, трояна удаленного доступа PureRAT и шифровальщика Pay2Key. Злоумышленники использовали множество различных загрузчиков и дропперов, в частности дроппер PureCrypter, загрузчик на Rust, использующий шелл-код Donut, загрузчик на Batch, загрузчик на JavaScript и ранее не описанный сторонний загрузчик PowerLoader, который повышал эффективность проникновения и обхода защитных решений. Как и инструменты PureCoder (PureCrypter, PureLogs, PureRAT), PowerLoader распространяется на теневых маркетплейсах по модели «вредоносное ПО как услуга» (Malware-as-a-Service, MaaS). Кроме того, исследователи обнаружили плагин для PureRAT под названием PluginRemoteDesktop, позволяющий удаленно управлять рабочим столом на скомпрометированной системе. Ранее он не упоминался в атаках на российские компании.

Атаки на российские энергетические компании

Неизвестный актор

Целевой фишинг

RAT

Стилер

Исследователи «Лаборатории Касперского» раскрыли активность ранее неизвестной группы, которая действует с 2024 года и атакует российские университеты, финансовые компании, дипломатические службы и энергетические предприятия. В сентябре 2025 года на GitHub вышел фреймворк для тестирования на проникновение Ravage, а уже в январе 2026 года злоумышленники начали его использовать. Исследователи «Лаборатории Касперского» обнаружили пользователей этого фреймворка среди атакующих, которые поначалу не привлекали к себе особого внимания. Группа, в арсенале которой был замечен Ravage, действовала с большими перерывами – могла «молчать» 3–4 месяца, а затем провести 10 атак за месяц. В 2026 году атаки начинались с рассылки фишингового письма с ZIP-архивом, содержащим XLL-файл, замаскированный под легитимную надстройку для Microsoft Excel. Двойной клик по этому файлу запускал приложение Excel, которое загружало в свой процесс исполняемую DLL-библиотеку, что приводило к выполнению вредоносного кода. Тип файла Microsoft Excel XLL Add-In в сочетании со знакомым логотипом Excel создавал впечатление легитимного документа. В данном случае XLL-файл был собран с помощью открытого фреймворка Excel-DNA и содержал написанный на C# модуль, который скачивал с вшитых в него URL-адресов и запускал два исполняемых файла. Адреса вели на взломанный сайт, куда предварительно были загружены вредоносные файлы. По первому адресу скачивался обычный биндер (программа для сборки файлов различных типов в один) для упаковки известных бэкдоров и стилеров. Он представлял собой самораспаковывающийся CAB-архив, внутри которого находились разделенные на несколько файлов интерпретатор AutoIt и скрипт для него, а также пакетный файл. Скрипт AutoIt содержал вредоносную нагрузку в виде зашифрованного исполняемого файла: он расшифровывал файл, запускал процесс RegAsm.exe и внедрял в этот процесс вредоносную нагрузку – бэкдор PureRAT. По второму адресу скачивалась утилита BatToExe. При выполнении она создавала один пакетный файл и один PowerShell-файл, запускала пакетный файл, а он в свою очередь – PowerShell-скрипт, который загружал фреймворк Ravage. Исследователи также выяснили, что в атаках 2024 года группа использовала инструмент Cobalt Strike и стилер RedLine.

Атаки HeartlessSoul

APT

Целевой фишинг

Вредоносная реклама

RAT

Распространение вредоносного ПО на легитимных платформах

Поддельный установщик

Исследователи «Лаборатории Касперского» сообщили об активности кибершпионской группы HeartlessSoul (также известной как Versatile Werewolf), которая атаковала государственные учреждения и коммерческие организации в сфере промышленности и авиационных систем, а также отдельных пользователей. Основным вектором заражения были фишинговые письма, содержавшие архивы с LNK-, XLL- или MSI-файлами. Некоторые из обнаруженных LNK-файлов эксплуатировали уязвимость ZDI-CAN-25373. Кроме того, злоумышленники запускали вредоносные рекламные кампании, используя поддельные сайты, якобы предлагающие программное обеспечение для авиационных систем, откуда жертвы скачивали зараженные установщики. Группа также распространяла вредоносный установщик через легитимную платформу SourceForge. Он был замаскирован под GearUP – сервис по улучшению соединения в онлайн-играх. Начальное заражение происходило после выполнения PowerShell-команд или скриптов для скачивания с C2-серверов JavaScript-загрузчика. Он, в свою очередь, загружал и выполнял в памяти основной JS-RAT и его модули, среди которых были инструменты для сбора и эксфильтрации данных, кейлоггеры, а также средства захвата экрана и обхода UAC. Конечной целью, по-видимому, был сбор геоинформационных данных и информации со скомпрометированных систем. Исследователи также выявили пересечения в инфраструктуре злоумышленников с APT-группой GOFFEE.

Атаки Paper Werewolf

APT

Целевой фишинг

RAT

Стилер

Поддельный установщик

В марте-апреле 2026 года исследователи BI.ZONE раскрыли кампанию группы Paper Werewolf (также известной как GOFFEE) против российских промышленных, финансовых и транспортных организаций. В этой кампании группа использовала расширенный набор инструментов на основе фишинговых PDF-документов, установщиков Inno Setup, загрузчиков, дропперов, стилеров и имплантов собственной разработки. В одной из цепочек атаки использовался отвлекающий PDF-документ со ссылкой на ZIP-архив с поддельным установщиком плагина Adobe Acrobat внутри. Этот установщик открывал документ-приманку в формате PDF и одновременно запускал RAT EchoGather, что позволяло атакующим собирать системную информацию о скомпрометированном устройстве, взаимодействовать с C2-сервером, отправлять файлы и выполнять команды. Исследователи также выявили PaperGrabber – неописанный ранее стилер на VB.NET, предназначенный для сбора файлов с локальных, сетевых и съемных дисков, кражи данных сессий Telegram и сохранения

учетных данных браузеров. В дополнительных цепочках атаки для выполнения шелл-кода или загрузки .NET-сборок в память использовались загрузчики на JavaScript, C++, Python и MSBuild. В одной из цепочек доставлялся кастомный имплант Mythic, который перед регистрацией на C2-сервере выполнял защищенный обмен ключами на основе RSA, а затем передавал сведения о системе.

Скоординированные кибератаки проукраинских групп

Хактивизм

Киберкриминал

Коллаборация групп злоумышленников

Эксплуатация общедоступных приложений

Бэкдор

Шифровальщик

В процессе изучения деятельности проукраинской хактивистской группы 4BID исследователи «Лаборатории Касперского» выявили серию кампаний, за которой могут стоять несколько связанных друг с другом групп. Исследование показало, что мишени этих атак не ограничиваются российскими и белорусскими организациями, а включают еще и компании в Казахстане, ОАЭ, Сирии и Египте из государственной, медицинской и авиационной отраслей. Такое поведение коррелирует с заявлением одного из участников группы 4BID о том, что «атаковать Россию больше финансово невыгодно».

Анализ атакованных инфраструктур показал, что в большинстве случаев злоумышленники получали первоначальный доступ в результате эксплуатации уязвимости Exchange, а именно – ProxyShell. После они использовали ASPX-веб-шелл с модульной архитектурой, обеспечивающий удаленное управление, передачу файлов и сбор системных данных. В инфраструктуре организации, послужившей отправной точкой для исследования, были выявлены многочисленные индикаторы активности различных проукраинских групп. Исследователи «Лаборатории Касперского» обнаружили несколько образцов BlackReaperRAT, который они приписали группе 4BID, скрипты для загрузки инструментов удаленного мониторинга и управления Panorama9, AnyDesk и Dev Tunnels, шифровальщик ClearWater и несколько образцов Warp RAT, которые они связывают с группой GOFFEE. Кроме того, в рамках описанных кампаний были замечены утилиты Advanced IP Scanner, Nezha Monitoring, Tactical RMM, Sliver, Havoc, Apollo Mythic, Adaptix, бэкдор BlackSalt и EDR-киллеры. Исследователи также сообщили, что в конце января группа 4BID провела серию атак на российские организации, используя обновленную версию программы-вымогателя Blackout Locker, которая распространяется с помощью дроппера, написанного на Rust.

Операция Silent Rotor

Неизвестный актор

Целевой фишинг

Исследователи Seqrite Labs описали «Операцию Silent Rotor» – таргетированную фишинговую кампанию против организаций и специалистов из сферы беспилотной авиации в ЕАЭС. Злоумышленники приурочили операцию к XIII Евразийскому международному форуму «Беспилотная авиация – 2026» в Москве. Они использовали приманки на соответствующую тему, в том числе фейковые подтверждения заказов и технические документы, для доставки вредоносного ZIP-архива. Он содержал 64-битный исполняемый файл на Rust, имитировавший легитимный документ Центра аэронавигационной информации, а также файлы-приманки в форматах PDF, DOCX и XLSX. После запуска вредоносное ПО проводило разведку, собирая такие данные, как имя хоста, серийный номер тома, параметры сетевого адаптера и переменные среды, а затем шифровало их с помощью кастомного XOR-алгоритма и отправляло на C2-сервер через HTTPS. После загрузчик первого этапа атаки скачивал зашифрованную полезную нагрузку второго этапа, расшифровывал ее с помощью AES-256 и выполнял в памяти, предоставляя атакующим дополнительные возможности. Исследователи Seqrite Labs отметили, что кампания была нацелена на специалистов и организации из авиационной отрасли из России, Таджикистана, Центральной Азии, Ближнего Востока и Европы. При этом они не смогли связать эту операцию с какой-либо конкретной группой.

Кибергруппы, атакующие Россию

Киберкриминал

APT

Инфраструктура облачных сервисов

Целевой фишинг

Бэкдор

LOTL

COM Hijacking

Код, сгенерированный ИИ

Компрометация сайтов

Исследователи Positive Technologies опубликовали анализ активности кибергрупп, нацеленных на российские организации, за I квартал 2026 года, с обновленным описанием их TTP, инструментов и принципа выбора жертв. Исследователи разделили группы на две категории: специализирующиеся на кибершпионаже и финансово мотивированные. Эти группы атаковали логистические, промышленные, авиационные, аэрокосмические, оборонные, фармацевтические, сельскохозяйственные, строительные, химические, энергетические, коммунальные предприятия.

В отчете подробно описана деятельность таких кибершпионских групп, как Rare Werewolf (она же Librarian Ghouls, Librarian Likho, Rezet), PhaseShifters (Angry Likho, Sticky Werewolf), PhantomCore (Head Mare), GOFFEE (Paper Werewolf), IAmTheKing (King Werewolf), Tolik (Fairy Werewolf), BO Team (Lifting Zmiy). В категории финансово мотивированных групп описаны Hive0117 (Watch Wolf, Ratopak Spider, UAC-0008) и Fluffy Wolf (VasyGrek). Цепочки атак всех групп начинались с фишинговых писем, содержавших в качестве полезных нагрузок документы Microsoft Word с макросами,

запароленные архивы с LNK-ярлыками, NSIS-инсталляторы с двойным расширением .pdf.exe, HTA-файлы, RTF-документы с эксплуатацией OLE-объектов, XLL-файлы Excel, SFX-архивы и BAT-файлы. Наиболее распространенным инструментом закрепления был планировщик задач Windows, он использовался почти всеми группами. Все группы осуществляли запуск полезной нагрузки через доверенные системные бинарные файлы.

Rare Werewolf переключилась с использования утилиты Blat для эксфильтрации данных по SMTP на использование комментариев на странице GitHub Gist. PhaseShifters хранила URL полезной нагрузки в репозитории Bitbucket, обновляя ссылки через коммиты. Fluffy Wolf размещала архив с дроппером и промежуточные .txt-файлы с закодированной Base64 полезной нагрузкой в репозитории GitHub, а также использовала Firebase Storage для хранения изображения со стеганографической полезной нагрузкой в Base64. PhantomCore размещала стейджеры на скомпрометированных легитимных сайтах. GOFFEE использовала в атаках на российские оборонные предприятия модули с характерными для LLM-генерации признаками.

Атаки Clubfoot Wolf

Киберкриминал

Целевой фишинг

RAT

Инфраструктура облачных сервисов

Исследователи BI.ZONE сообщили об атаках группы Clubfoot Wolf (также известной как NetMedved). Они обнаружили, что в мае и июне группа вела масштабную кампанию против российских промышленных, сельскохозяйственных, логистических, медицинских, научных и ИТ-организаций, а также компаний из сфер розничной торговли и электронной коммерции. Главными мишенями были российские компании, занимающиеся оптовой торговлей химической продукцией, однако злоумышленники также атаковали несколько организаций в Беларуси. Группа Clubfoot Wolf рассылала фишинговые письма, доставляя на целевые системы легитимное программное обеспечение для удаленного администрирования NetSupport Manager. В письмах злоумышленники представлялись сотрудниками компании, заинтересованной в покупке продукции у целевой организации. В ранее зафиксированных кампаниях Clubfoot Wolf тоже действовала под видом российских организаций, распространяя ZIP-архивы с поддельными документами. В описанной кампании письма содержали архив с несколькими файлами-приманками в разных форматах (PDF, JPG, PNG, DOC и DOCX) и вредоносный LNK-файл. Для рассылки использовался сервис «Яндекс.Почта». При запуске вредоносного LNK-файла в интерпретаторе PowerShell выполнялась закодированная в Base64 команда, что позволяло атакующим выполнить

следующий этап непосредственно в памяти процесса PowerShell. Финальный PowerShell-скрипт загружал ZIP-архив, внутри которого, помимо файла программы NetSupport Manager, находился набор файлов, заполненных автоматически сгенерированным бессмысленным текстом. Эти файлы, вероятно, были добавлены, чтобы изменить хеш-сумму архива и придать ему вид легитимного программного дистрибутива. PowerShell-скрипт декодировал и расшифровывал PowerShell-код, отвечавший за закрепление NetSupport Manager в реестре операционной системы.

Активность китайско-говорящих групп

Атаки Silver Fox

APT

Целевой фишинг

RAT

Бэкдор

В декабре 2025 года исследователи «Лаборатории Касперского» обнаружили волну вредоносной рассылки, имитировавшей сообщения от налоговой службы Индии. Спустя несколько недель, в январе 2026 года, началась схожая кампания, нацеленная на российские организации. Исследователи связали эту активность с группой Silver Fox (также известной как Monarch, SwimSnake, UTG-Q-1000 и Void Arachne). Обе волны имели практически идентичную структуру: фишинговые письма оформлялись как официальные уведомления о налоговых проверках или предлагали скачать архив с «перечнем налоговых нарушений». В архиве был модифицированный загрузчик на Rust под названием RustSL, исходный код которого находится в открытом репозитории на GitHub. Этот модифицированный загрузчик зашифровывал вредоносную нагрузку, и использовал все доступные методы обнаружения виртуальных машин и песочниц. Он также проверял, находится ли устройство в заданной стране. В более поздних версиях осталась только геолокационная проверка, однако список стран, в которых разрешалась работа, сильно увеличился. В GitHub-версии загрузчика был только Китай, тогда как список кастомной версии Silver Fox включал Индию, Индонезию, Южную Африку, Россию, Камбоджу, в январе в него добавили Японию. RustSL скачивал и выполнял известный бэкдор ValleyRAT. В ходе исследования также было обнаружено, что злоумышленники доставляли на устройства жертв новый плагин для ValleyRAT, который загружал и запускал ранее недокументированный бэкдор на Python, получивший название ABCDoor. Ретроспективное исследование показало, что он находился в арсенале Silver Fox как минимум с конца 2024 года и использовался в реальных атаках с первого квартала 2025 года по настоящее время.

Кампания затронула производственные, консалтинговые, торговые и транспортные организации. Всего с начала января по начало февраля было зафиксировано более 1600 вредоносных писем. Наибольшее количество атак пришлось на Индию, Россию и Индонезию, чуть меньше – на ЮАР и Японию.

Атаки с использованием ShadowPad

APT

DLL sideloading

LOTL

Атака на цепочку поставок/ доверенных партнеров

Бэкдор

Исследователи F6 раскрыли атаку на российское производственное предприятие в конце февраля 2026 года. В качестве вектора первоначального доступа злоумышленники использовали сервисную учетную запись подрядчика, которая применялась для доступа во внутреннюю сеть организации через Check Point VPN. Анализ тактик, техник и процедур показал, что атакующие использовали бэкдор ShadowPad, активно использующийся китайскими APT-группами. Для выполнения вредоносного ПО они использовали службы в операционной системе Windows. Точками закрепления стали запланированные задачи, созданные службы и автозапуск вредоносного ПО через ключ реестра RUN. Для горизонтального перемещения злоумышленники удаленно создавали службы на смежных устройствах с помощью стандартной утилиты операционной системы sc.exe. На основе имеющихся данных исследователи не смогли установить конкретную APT-группу, стоявшую за атакой.

Атаки Shadow-Earth-053

APT

DLL sideloading

Эксплуатация общедоступных приложений

Бэкдор

Исследователи Trend Micro опубликовали отчет об активности недавно выявленной китайско-говорящей группы, которую они отслеживают под временным названием SHADOW-EARTH-053. Эта группа атаковала преимущественно государственные структуры в Южной, Восточной и Юго-Восточной Азии, в частности в Пакистане, Таиланде, Малайзии, Индии, Мьянме, Шри-Ланке и на Тайване. Кроме того, ее мишенями были компании из технологического сектора, а также несколько транспортных предприятий в Юго-Восточной Азии.

SHADOW-EARTH-053 эксплуатировала известные уязвимости в подключенных к интернету серверах Microsoft Exchange и Internet Information Services (например, цепочку уязвимостей ProxyLogon). Злоумышленники закреплялись в системе через веб-шеллы GODZILLA, а затем разворачивали импланты ShadowPad путем подмены DLL-библиотеки у легитимных подписанных файлов. В одном случае образцы ShadowPad были доставлены через AnyDesk – легитимный инструмент удаленного администрирования, поэтому можно предположить, что

злоумышленники использовали ранее скомпрометированную систему или получили учетные данные иными способами.

После проникновения атакующие устанавливали легитимную утилиту Windows csvde.exe для экспортирования объектов Active Directory в формат CSV. Они использовали командлет Get-DomainUser из PowerView для перебора пользовательских учетных записей и связанных с ними адресов электронной почты с контроллера домена. Также исследователи обнаружили кастомную программу DomainMachines.exe, которая перебирала устройства в домене через LDAP, а после подключалась к портам (SMB, веб-сервер, прокси, RDP, WinRM, MySQL, MS SQL и Kerberos), однако извлечь ее для проведения глубокого анализа им не удалось. Для загрузки вредоносной DLL-библиотеки злоумышленники использовали легитимный исполняемый файл Toshiba Bluetooth Stack. DLL-библиотека извлекала полезную нагрузку из реестра Windows, а не встраивала ее в бинарный файл. Также в арсенале группы были замечены прокси-утилита IOX и туннельные инструменты GO Simple Tunnel и Wstunnel.

Для горизонтального перемещения SHADOW-EARTH-053 использовала WMIC, устанавливала предположительно кастомный RDP-загрузчик и реализацию SMBExec на C#, известную как Sharp-SMBExec. В одном из случаев атакующие распространяли веб-шеллы на дополнительные внутренние серверы Exchange, скопировав их через административные ресурсы. Для сбора учетных данных они использовали инструмент Evil-CreateDump, который, судя по всему, представляет собой модифицированную версию утилиты Microsoft create-dump.exe, нацеленную на память процесса LSASS. Для извлечения учетных данных и дампа локальной базы данных SAM выполнялся Mimikatz напрямую через rundll32.exe с аргументами командной строки. Кроме того, атакующие устанавливали и запускали бинарный файл newdcsync, который, судя по командной строке и названию, скорее всего, использовался для проведения DCSync-атак.

Атаки FamousSparrow

APT

DLL sideloading

Бэкдор

Эксплуатация общедоступных приложений

Исследователи Bitdefender сообщили о многоволновой атаке на азербайджанскую нефтегазовую компанию в период с конца декабря 2025 года по конец февраля 2026 года. С высокой долей уверенности они предположили, что за атакой стояла китайско-говорящая группа FamousSparrow (она же UAT-9244), имеющая тактические сходства с Earth Estries. Для получения первоначального доступа злоумышленники неоднократно эксплуатировали уязвимый сервер Microsoft Exchange (предположительно они использовали уязвимость ProxyNotShell – CVE-

2022-41040, CVE-2022-41082), несмотря на многочисленные попытки остановить атаку. В ходе первой волны они пытались развернуть веб-шеллы для закрепления и в дальнейшем установить бэкдор Deed RAT, который через легитимный бинарный файл LogMeIn Hamachi загружает и запускает вредоносную DLL-библиотеку, отвечающую за выполнение основной полезной нагрузки. Примечательно, что злоумышленники усложнили привычную технику DLL sideloading, основанную только на подмене файлов: они применили двухэтапный механизм, который запускает Deed RAT при естественном выполнении потока управления легитимного приложения LogMeIn Hamachi после вызова двух определенных экспортируемых функций из DLL.

Во второй волне, примерно через месяц, злоумышленники безуспешно попытались применить технику DLL sideloading с легитимным исполняемым файлом Яндекс Браузера deskband_injector64.exe для развертывания через загрузчик шелл-кода Mofu другого бэкдора – TernDoor.

Третья волна атаки на азербайджанскую компанию пришлась на конец февраля. Злоумышленники попробовали использовать цепочку заражения, описанную на ранних этапах атаки, но только с измененной версией бэкдора Deed RAT. Очевидно, что после неудачной второй волны они доработали свой арсенал. В ходе операции атакующие осуществляли горизонтальное перемещение через RDP и SMB, использовали скомпрометированные учетные данные доменного администратора, мощный набор инструментов с открытым исходным кодом и избыточные механизмы закрепления. Такой подход, по мнению исследователей, свидетельствует о долгосрочных планах шпионской миссии в отношении конкретной энергетической компании.

Атаки с использованием DAEMON Tools

APT

Сертификаты разработчика

Атака на цепочку поставок

Троянизированное ПО

Бэкдор

RAT

Исследователи «Лаборатория Касперского» обнаружили продолжающуюся атаку на цепочку поставок с использованием легитимного программного обеспечения DAEMON Tools. Троянизированные версии этого ПО, имеющие цифровую подпись разработчика, распространялись с 8 апреля. Зараженные версии с 12.5.0.2421 по 12.5.0.2434 активировали внутри подписанных бинарных файлов DAEMON Tools бэкдор, связывались с C2-сервером, адрес которого env-check.daemontools[.]cc был создан при помощи тайпсквоттинга, и могли получать shell-команды для загрузки и запуска полезной нагрузки.

С 8 апреля, когда была развернута первая троянизированная версия DAEMON Tools, исследователи «Лаборатории Касперского» наблюдали тысячи попыток установки полезной нагрузки через скомпрометированные бинарные файлы. Заражения наблюдались на устройствах, принадлежащих как частным лицам, так и организациям в более чем 100 странах и территориях, причем большинство жертв находилось в России, Бразилии, Турции, Испании, Германии, Франции, Италии и Китае. Анализ показал, что 10% затронутых систем принадлежат бизнесу и организациям. На большинство устройств доставлялась только полезная нагрузка, предназначенная для сбора информации. Другой, минималистичный бэкдор был обнаружен лишь на десятке компьютеров государственных, научных, производственных и торговых организаций в России, Беларуси и Таиланде. Еще один, более сложный имплант использовался только против одной организации – учебного заведения в России. Он получил название QUIC RAT, поддерживает множество протоколов коммуникации с C2-сервером и способен внедрять полезную нагрузку в процессы. Во вредоносных имплантах исследователи обнаружили артефакты, указывающие на то, что злоумышленник, стоящий за этой атакой, говорит по-китайски.

Разработчик DAEMON Tools, компания AVB Disc Soft, 6 мая подтвердила, что программное обеспечение было заражено в ходе атаки на цепочку поставок, и выпустила обновленную версию, в которой была исключена вредоносная функциональность. Обновление было реализовано менее чем за 12 часов с момента получения компанией уведомления. Согласно заявлению AVB Disc Soft, проблема затронула лишь бесплатную версию DAEMON Tools Lite и не коснулась других продуктов. Компания выявила несанкционированное вмешательство в свою инфраструктуру, в результате которого некоторые установочные пакеты были затронуты в среде сборки и выпущены зараженными.

Атаки с применением вредоносного ПО TencShell

Неизвестный актор

APT

Бэкдор

В апреле исследователи Cato CTRL заблокировали попытку проникновения в международную производственную компанию, имеющую несколько региональных филиалов, – атакован был объект в Индии. Злоумышленники использовали TencShell – ранее недокументированный имплант на основе открытого C2-фреймворка Rshell, написанный на Go. Первоначальный вектор атаки остался неизвестным, однако активность осуществлялась через учетную запись стороннего пользователя, у которого был доступ к среде заказчика. Цепочка атаки включала дроппер первого этапа, шелл-код Donut, замаскированный под файл веб-шрифта с расширением .woff,

внедрение полезной нагрузки в память и взаимодействие с C2-сервером, похожее на обычный веб-трафик. TencShell, который использовался в качестве финальной полезной нагрузки, с точки зрения функциональности представляет собой зрелый инструмент для постэксплуатации. Обнаруженные модули на Go указывают на широкий набор возможностей, таких как выполнение файлов из памяти, выполнение BOF-модулей, проксирование и туннелирование трафика, соединение с C2-сервером через WebSocket и удаленное управление. Имплант также сочетает функционал удаленной оболочки и ОС, позволяет управлять файлами и процессами, обеспечивать закрепление, обходить защитные решения и UAC, делать скриншоты, красть данные из браузера, запускать polling-задачи, структурировать отчетность C2-сервера и перемещаться по внутренней сети с использованием SOCKS5-прокси. Происхождение TencShell от Rshell, имитация путей, похожих на API китайской компании Tencent, а также особенности инфраструктуры дали исследователям основания предположить, что за атакой стоит китайско-говорящий актор, однако точно связать ее с какой-либо группой они не смогли.

Атаки Mustang Panda

APT

Целевой фишинг

DLL sideloading

Облачные сервисы как C2

Бэкдор

Исследователи Acronis сообщили о двух шпионских кампаниях группы Mustang Panda, нацеленных на гидроэнергетические предприятия и государственные структуры Индии, сотрудничающие с Тайванем. В ходе этих кампаний использовались архивы с приманками на соответствующие темы, скрытые DLL-библиотеки и техника DLL sideloading. При запуске легитимных подписанных файлов на устройство жертвы доставлялся один из нескольких вариантов вредоносной программы SHARDLOADER, которая устанавливала два недавно выявленных импланта – MINIRECON и ZOHOMURK. MINIRECON представляет собой модифицированный вариант бэкдора Toneshell, взаимодействует с C2-сервером через WebSocket-соединение по протоколу HTTPS с возможностью переключения на прокси, обладает функционалом реверс-шелла, передачи файлов, удаленного выполнения команд, а также загрузки и запуска файлов. ZOHOMURK использует Zoho WorkDrive в качестве C2-сервера, для регистрации жертв, получения команд, загрузки результатов и кражи данных, маскируя вредоносный трафик под обращения к легитимному облачному сервису, широко распространенному в индийских госучреждениях. Исследователи Acronis с высокой долей уверенности приписывают эту активность группе Mustang Panda. Они опираются на сходство тактик, пересечения в используемом вредоносном ПО и инфраструктуре, а также на целевую направленность кампаний, которая согласуется со сбором разведывательной информации о

гидроэнергетических проектах Индии и ее связях с Тайванем в сфере обороны.

Атаки CL-STA-1062

APT

Эксплуатация общедоступных приложений

Бэкдор

Исследователи Unit 42 сообщили о кампании CL-STA-1062, нацеленной на госучреждения и объекты критической инфраструктуры преимущественно из энергетической отрасли в Юго-Восточной Азии. По данным исследователей, этот кластер действует как минимум с 2022 года и скорее всего связан с группой UAT-7237. В ходе кампании злоумышленники проникали в системы жертв через уязвимые веб-приложения, после чего запускали ASPX-веб-шеллы, проводили разведку, внедряли инструментарий и похищали информацию из баз данных и исходный код веб-сервера. Они использовали гибридный набор инструментов, сочетавший утилиты с открытым исходным кодом (SoftEther VPN, VNT, Mimikatz, JuicyPotato, RAR), инструменты туннелирования и кастомное вредоносное ПО, включая недавно задокументированный бэкдор TinyRCT на базе .NET. Этот бэкдор умеет проводить первоначальную разведку для идентификации зараженного устройства, регистрировать зараженные системы на C2-сервере, выполнять команды, сканировать и похищать данные, делать скриншоты, загружать полезную нагрузку и удалять следы работы. По мнению исследователей, эта активность представляет собой перманентную региональную угрозу, сфокусированную на стратегических секторах в Юго-Восточной и Восточной Азии.

Активность, связанная с Ближним Востоком

Предупреждение CISA об эксплуатации злоумышленниками ПЛК

APT

Целевые атаки на АСУ

Манипуляция данными

Агентство по кибербезопасности и защите инфраструктуры США, Федеральное бюро расследований, Агентство национальной безопасности и ряд других ведомств опубликовали предупреждение о продолжающихся атаках, нацеленных на программируемые логические контроллеры в объектах критической инфраструктуры США. Атаки сфокусированы на государственных и энергетических организациях, а также муниципальных предприятиях, связанных с водоснабжением и канализацией, и продолжаются как минимум с марта. Предполагается, что за ними стоит связанная с Ираном APT-группа, эксплуатирующая ПЛК Rockwell Automation (линейка Allen-Bradley), а, возможно, и устройства других производителей вроде Siemens S7. Злоумышленники использовали

арендованную инфраструктуру сторонних провайдеров с сервисным ПО, в частности Studio 5000 Logix Designer от Rockwell Automation, для создания подтвержденного подключения к ПЛК жертв. Целевыми устройствами были ПЛК CompactLogix и Micro850. ФБР установило, что в результате этой активности атакующие извлекали проектную документацию и изменяли данные на дисплеях HMI и SCADA.

CISA рекомендует организациям отключить ПЛК от интернета, использовать защищенные шлюзы и межсетевые экраны, проверить журналы в период атаки в соответствии с индикаторами компрометации, например, на наличие подозрительного трафика на портах 44818, 2222, 102, 22 и 502, а также перевести переключатель режима на контроллерах Rockwell Automation в положение Run («Работа»). Кроме того, агентство настоятельно рекомендует ознакомиться со списком мер по смягчению последствий и усилению защиты, индикаторами компрометации и TTP злоумышленников. В предупреждении содержится призыв к производителям предусмотреть изменение настроек по умолчанию, чтобы предотвратить доступ к устройствам из интернета, не брать плату за базовые функции безопасности и обеспечить поддержку многофакторной аутентификации с использованием методов, устойчивых к фишингу.

Атаки с использованием ZionSiphon

APT

Целевые атаки на АСУ

Кибersаботаж

Самораспространяющееся вредоносное ПО

Исследователи Darktrace раскрыли новую вредоносную программу ZionSiphon, разработанную специально для операционных технологий и ориентированную на водоочистные и опреснительные объекты с целью саботажа их работы. Диапазон IP-адресов целей и закодированные политические сообщения позволили исследователям предположить, что ZionSiphon фокусируется на объектах в Израиле. При установке программа проверяла по IP-адресу географию устройства, а также содержит ли оно ПО или файлы, связанные с водоснабжением, чтобы убедиться, что она запущена в целевой системе. При этом исследователи нашли ошибку в логике проверки страны: из-за несоответствия XOR-значений сбивался таргетинг и вместо выполнения полезной нагрузки активировался механизм самоуничтожения. При успешном запуске ZionSiphon ущерб мог бы быть очень серьезным, поскольку эта программа позволяет, например, увеличить уровень хлора в воде, мощность потока или давление до максимума. За это отвечает функция IncreaseChlorineLevel(), которая проверяет жестко закодированный список конфигурационных файлов, связанных с OT-системами и АСУ опреснением, обратным осмосом, хлорированием и водоочисткой. Как только она находит один из таких файлов, добавляет к нему определенный текстовый блок и сразу же

возвращается. ZionSiphon сканировал локальную подсеть в поисках устройств, работающих по протоколам Modbus, DNP3 и S7comm. Исследователи обнаружили лишь частично функциональный код для Modbus и неполную логику для двух других протоколов – это свидетельствует о том, что вредоносная программа находится на стадии разработки. ZionSiphon имеет функционал распространения через USB: программа копирует себя на съемные диски как скрытый процесс svchost.exe и создает вредоносные ярлыки, при клике на которые инициируется запуск.

Атаки Nimbus Manticore

APT

Целевой фишинг

DLL sideloading

Поддельный установщик

Сертификаты разработчика

Код, сгенерированный ИИ

Бэкдор

Отравление SEO

Исследователи Check Point сообщили о новых кампаниях связанной с Ираном группы Nimbus Manticore (также известной как UNC1549) в условиях геополитического конфликта. Они отследили три волны активности – в феврале, марте и апреле.

В февральской кампании злоумышленники использовали фишинговые приманки на тему карьерных возможностей для атаки авиационных предприятий и компаний-разработчиков ПО в Саудовской Аравии и Австралии. В письмах была ссылка на ZIP-архив, размещенный на платформе OnlyOffice. Злоумышленники продемонстрировали измененную цепочку заражения, использовав для выполнения кода технику AppDomain Hijacking вместо DLL sideloading. Такой подход позволил им внедрить вредоносный код в доверенные .NET-приложения и установить новую версию бэкдора MiniJunk.

В марте, в дополнение к фишинговым письмам, обещавшим карьерные перспективы от имени американской авиакомпании, злоумышленники рассылали поддельные приглашения на встречи с троянизированным установщиком Zoom. Вредоносная программа использовала в качестве механизма закрепления системную задачу планировщика, создаваемую инсталлятором Zoom. Таким образом вредоносная активность имитировала обычную легитимную, снижая вероятность обнаружения. Поддельный установщик внедрял ранее неописанный бэкдор MiniFast, который пришел на смену старому семейству вредоносов MiniJunk. Исследователи предположили, что этот бэкдор мог быть разработан при помощи технологий искусственного интеллекта.

В апреле они впервые заметили, как Nimbus Manticore применяет в атаке тактику отравления SEO. Злоумышленники использовали фейковый сайт, похожий на страницу загрузки SQL Developer, – графического инструмента для работы с базами данных. Пользователи, попытавшиеся загрузить ПО с

этого сайта, на самом деле скачивали вредоносный установщик, доставлявший на их устройства бэкдор MiniFast.

Атаки MuddyWater

APT

Эксплуатация общедоступных приложений

Перебор учетных данных

DLL sideloading

Бэкдор

Исследователи Oasis Security проанализировали многоэтапную кампанию группы MuddyWater, нацеленную на авиационные организации, госучреждения, энергетические и инфраструктурные компании в некоторых ближневосточных странах, включая Египет, Израиль и ОАЭ, а также в Португалии и Индии. В ходе операции, которая началась в феврале, злоумышленники провели масштабную автоматизированную разведку, просканировав более 12 000 доступных из интернета систем на наличие пяти недавно раскрытых уязвимостей (CVE-2025-54068, CVE-2025-52691, CVE-2025-68613, CVE-2025-9316, CVE-2025-34291), затрагивающих веб-приложения, почтовые серверы, системы управления и мониторинга ИТ-инфраструктуры, а также инструменты организации и автоматизации рабочих процессов. После сканирования злоумышленники перешли к узконаправленным действиям: с помощью кастомных инструментов и многоцелевых фреймворков, таких как Patator, они перебирали учетные данные Outlook Web Access из организаций в Египте, Израиле и ОАЭ. Для управления скомпрометированными устройствами злоумышленники использовали модульную C2-инфраструктуру, поддерживающую закодированную AES коммуникацию по протоколам TCP, UDP и HTTP. Это поведение соответствует фреймворку ArenaC2, который ранее связывали с MuddyWater.

В ходе операции были украдены конфиденциальные данные из египетской авиационной компании, в том числе копии паспортов и визовые данные, сведения о заработной плате, информация о кредитных картах и внутренние корпоративные документы. Перед выгрузкой злоумышленники разложили по папкам около 200 файлов, что указывает на выборочный сбор данных.

Исследователи Symantec сообщили о шпионской кампании группы Seedworm (она же MuddyWater, Temp Zagros, Static Kitten), которая затронула как минимум девять организаций в девяти странах. Среди них крупный южнокорейский производитель электроники, государственные учреждения, международный аэропорт, промышленные предприятия, финансовая компания, учебные заведения и поставщики профессиональных услуг. Злоумышленники использовали технику DLL sideloading с легитимными подписанными бинарными файлами Fortemedia и SentinelOne, маскируя вредоносные DLL-библиотеки под обычное ПО. Эти библиотеки содержали ChromElevator – общедоступный инструмент

для постэксплуатации, умеющий красть пароли, файлы cookie и данные платежных карт из браузеров на базе Chromium. Также злоумышленники использовали загрузчик на базе Node.js, управлявший PowerShell-скриптами для разведки, создания скриншотов, кражи учетных данных, извлечения SAM-куста реестра, повышения привилегий и туннелирования через SOCKS5-прокси.

В сети скомпрометированного южнокорейского производителя электроники Seedworm находилась почти неделю, установив вредоносные программы и обеспечив закрепление через Run-ключ. Злоумышленники собирали учетные записи и выкачивали информацию через файлообменный сервис sendit[.]sh. В ходе этой компании Seedworm продемонстрировала высокую операционную дисциплину, рассчитывая на продолжительный сбор разведывательной информации и незаметную кражу данных.

Атаки Cyber Isnaad Front

Хактивизм

Целевые атаки на АСУ

Киберсаботаж

Вайпер

Эксплуатация общедоступных приложений

Манипуляция данными

По данным Profero, группа Cyber Isnaad Front, действующая в интересах правительства Ирана, провела разрушительную кибероперацию против израильской промышленности. Мишенями стали организации из военно-промышленного и топливно-энергетического комплексов, пищевой промышленности, транспортной и логистической отраслей, причем от атак пострадали как ИТ-, так и ОТ-среды. Специалисты Profero установили, что злоумышленники развернули в ИТ-сетях инструментарий удаленного доступа GRAT (Go Remote Access Toolkit), замаскированный под обновления Microsoft, который представляет собой гибрид RAT и вайпера. Одновременно атакующие устроили саботаж в ОТ-среде – перепрограммировали контроллеры промышленной холодильной системы предприятия пищевой промышленности, что привело к физической поломке компрессоров. Для одной из установок они изменили рабочие параметры контроллеров, установив их за пределами нормальных безопасных значений, поменяв при этом и пороговые противоаварийные параметры (protection thresholds), и сигнальные значения (alarm and alert limits), что в совокупности, если б работники организации не заметили изменений, привело бы к порче продукции. В другом случае злоумышленники пошли еще дальше. Они стерли всю конфигурацию контроллеров, перезаписали значения цифровых и аналоговых входных сигналов от датчиков температуры и измерителей давления, сигналы ошибок, цифровые выходные сигналы старта компрессоров и аналоговые сигналы управления вентилями и вентиляторами. Восстановление системы потребовало полной ее конфигурации, заняв несколько дней.

Более того, атакующие перевели клапаны системы охлаждения газа и ресивера в ручной режим, оставив их открытыми, открыв также и клапаны потребителей, что запустило свободную циркуляцию рабочего тела в системе и привело к попаданию жидкой углекислоты в компрессоры и, соответственно, к их разрушению, а также к выбросу углекислого газа из системы в атмосферу. Ремонтникам пришлось заменять вышедшие из строя компрессоры на неаналогичные, значительно переделывать всю установку и накачивать в нее новую порцию рабочего газа, что заняло б*о*льшую часть недели.

Напоследок злоумышленники сменили учетные данные центрального контроллера, лишив операторов доступа к управлению.

Все это свидетельствует о хорошей подготовке атакующих в осуществлении их намерения достичь киберфизического эффекта. В публикации помимо описания киберфизической части атаки приводятся индикаторы компрометации ИТ-части инфраструктуры и рекомендации по защите.

Активность, связанная с Азией

Атаки Andariel

APT

RAT

Шифровальщик

В марте исследователи ESET обнаружили вредоносную программу TigerRAT на компьютере инжиниринговой компании из Южной Кореи. По их данным, за атакой стоит группа Andariel, а пострадавшая компания производит высококачественное промышленное оборудование для некоторых важных отраслей. Последняя атака, описанная исследователями ESET, в ходе которой наблюдались характерные для Andariel тактики, техники и процедуры, была два года назад, и тоже против южнокорейской компании. Таким образом, видимо, можно говорить о возвращении этой группы.

Злоумышленники пытались взломать несколько конечных точек сети компании, использовав несколько версий шифровальщика Rook. Статус атакованной компании, вероятно, свидетельствует о стремлении группы украсть стратегически важные технологии. Исследователи полагают, что шифровальщик мог быть использован как для отвлечения внимания, так и с намерением потребовать выкуп.

Атаки OceanLotus

APT

Атаки на цепочку поставок/ доверенных партнеров

DLL sideloading

Эксплуатация публичных приложений

Бэкдор

Исследователи ESET выявили две кампании OceanLotus с 2024 года по начало 2026 года. В каждой из них группа использовала собственный бэкдор SPECTRALVIPER. В одном случае она взломала вьетнамскую корпорацию, занимающуюся инфраструктурным и транспортным строительством, и присутствовала в сети жертвы с ноября 2024 года по февраль текущего года. Вектор первоначального доступа исследователям определить не удалось, однако, проанализировав публичные сервера жертвы, они предположили, что злоумышленники могли использовать уязвимость удаленного выполнения кода (RCE) в Microsoft SQL Server. В другом случае OceanLotus провела атаку на цепочку поставок с использованием FireAnt MetaKit – программной платформы, которую вьетнамские инвесторы используют для отслеживания финансовых рынков и анализа. Первую вредоносную нагрузку, установленную с легитимного адреса платформы, исследователи обнаружили 2 октября 2025 года. Они обратили внимание, что вредоносное ПО доставлялось не массово, а выборочно – это свидетельствует о фокусе злоумышленников на определенные организации. В обоих случаях полезной нагрузкой был бэкдор SPECTRALVIPER, он доставлялся с использованием техники DLL sideloading с легитимными подписанными файлами Toolbox.exe и dtlupdate.exe. Исследователи пришли к выводу, что обе кампании связаны с усилением антикоррупционных мер во Вьетнаме, однако не смогли точно определить, является ли нацеленность OceanLotus на внутренний рынок ее временной или долгосрочной стратегией.

Активность русскоязычных групп

Атаки Sednit

APT

Целевой фишинг

Бэкдор

Облачные сервисы как C2

Троянизированное ПО

В течение нескольких месяцев исследователи ESET отслеживают активность группы Sednit (также известной как APT28, Fancy Bear, Sofacy), которая использует продвинутый инструментарий для развертывания в Украине имплантов Covenant и BeardShell. Атаки обычно начинались с контакта через десктопные версии мессенджеров Signal и WhatsApp, после чего жертве отправлялся троянизированный документ Word или Excel. Исследователи ESET ранее описали эти импланты и указали на их прямое сходство с имплантами, которые группа использовала в 2010-х годах. Мишенями атакующих в основном являются украинские военнослужащие, а также украинские производители беспилотников и организации, связанные с разработкой БПЛА.

В одной из атак жертве был отправлен троянизированный документ Excel. При открытии с отключенными макросами в документе отображалось только изображение беспилотника, побуждавшее получателя включить макросы. Если это сделать, то отображалась еще и техническая информация о беспилотнике. Вся последовательность действий приводила к установке импланта Covenant через кастомный загрузчик KoalaLoader, который извлекал полезные нагрузки из дополнительных стеганографических PNG-файлов. После из импланта Covenant злоумышленники развертывали BeardShell. Подобная избыточность позволяла операторам быстро восстанавливать доступ, если инфраструктура одного из имплантов оказывалась нарушена. BeardShell больше не взаимодействует с облачным хранилищем IceDrive, а использует облачный сервис для работы с документами Drime. Использование сразу двух имплантов, по всей видимости, обусловлено задачей вести продолжительную слежку за украинскими военными, в то же время этот подход применяется и в более широких кампаниях. Например, в ходе оппортунистической кампании в марте 2025 года BeardShell распространялся через троянизированное украинское приложение для управления беспилотниками, размещавшееся на торрентах. В январе этого года Covenant доставлялся через фишинговые рассылки, эксплуатировавшие уязвимость CVE-2026-21509, в ходе атак на правительственные учреждения на Украине, логистические компании в Турции и транспортные компании в Польше.

Атаки Sandworm

APT

Вайпер

Шифровальщик

Сеть Tor

По данным ESET, с декабря 2025 года по март 2026 года группа Sandworm усилила атаки против украинских организаций, распространяя несколько вариантов вредоносного ПО для уничтожения данных через групповые политики Active Directory. В январе исследователи ESET зафиксировали активность, имитировавшую атаку вымогателей, жертвой которой стала украинская зерновая компания. Злоумышленники использовали RansomTuga – открытое вредоносное ПО, доступное на GitHub, которое можно настроить и как вайпер, и как программу-вымогатель. После этого они потребовали выкуп в криптовалюте – 600 Zcash. Наряду с RansomTuga, атакующие развертывали Tor-службы. Аналогичный подход применялся в ходе кампании BadPilot, описанной Microsoft Threat Intelligence: тогда злоумышленники использовали ShadowLink для изменения конфигурации системы и ее регистрации как Tor-службы через легитимный бинарный файл Tor-службы и конфигурационный файл torrc. Конфигурация в том случае включала переадресацию портов для обычных служб, таких как RDP и SSH. А в случае, о котором пишут исследователи ESET, присутствовала

только переадресация портов по протоколу RDP. Microsoft Threat Intelligence приписала кампанию BadPilot группе Seashell Blizzard (она же Sandworm).

В феврале Sandworm внедрила свою первую вредоносную программу для уничтожения данных, написанную на Rust и получившую название ZeroRays. CERT-UA обозначил ее как ZEROSETH. При запуске без аргументов вредоносное ПО рекурсивно перебирает файлы на всех логических дисках, исключая определенные каталоги и типы файлов, запускает подпроцессы для удаления файлов, обнуляя дескрипторы открытых файлов через FSCTL_SET_ZERO_DATA, и в итоге вызывает немедленную перезагрузку системы. Эта вредоносное ПО использовалось в атаках на региональное госучреждение, теплоэнергетические и страховые компании на Украине. Кроме того, исследователи выявили еще одну программу для уничтожения данных, загруженную на VirusTotal из Украины. Это – незначительно модифицированная версия вайпера NikoWiper, использующего утилиту SDelete. Помимо нее, MSI-файл содержит текстовый файл с ASCII-артом, раскрывающим внутреннее имя вредоносного ПО – Occultus.

Прочее

Атаки с использованием вайпера Lotus

APT

Вайпер

Исследователи «Лаборатории Касперского» обнаружили новый вайпер, появление которого они связали с геополитической напряженностью в Карибском регионе в конце 2025 года – начале 2026 года. Вредоносная программа, получившая название Lotus Wiper, была загружена в публичные сервисы для проверки безопасности файлов вместе с другими артефактами. Поначалу исследователи подозревали, что этот вайпер связан с новой атакой с использованием шифровальщика, однако не смогли выявить пересечения ни с одной известной группой вымогателей. Более того, они не нашли никаких требований о выкупе. Анализ метаданных, полученных из сканера вредоносного ПО, показал, что появление этой программы совпало с публичными сообщениями об атаках с использованием вайперов на энергетические и коммунальные компании в Венесуэле. Поэтому исследователи считают, что это – таргетированная и не связанная с вымогателями атака, цель которой – уничтожение всех файлов и данных на устройстве.

Исследователи обнаружили два пакетных файла, которые выполняли определенную последовательность действий и подготавливали среду, а затем запускали Lotus Wiper. Второй пакетный файл выполнял

вредоносный бинарный файл, замаскированный под легитимный файл задачи в HCL Domino (ранее Lotus Domino) на Windows. Он передавал в качестве аргумента другой вредоносный бинарный файл, имя которого отсылает к компонентам HCL Domino, что в итоге приводило к извлечению и выполнению полезной нагрузки Lotus Wiper. Такая техника предполагает наличие у атакующих доступа к системам жертвы, поскольку исполняемые файлы должны быть размещены на них заранее. Lotus Wiper предоставляет все привилегии, указанные в его текущем токене, для доступа к административным функциям (на основе ранее полученных повышенных привилегий), удаляет точки восстановления и стирает данные с каждого физического диска, записывая нули в их сектора. Затем он стирает записи изменений данных в журналах томов и сканирует все тома в поисках файлов для удаления.

Атаки методом Watering hole через CPU-Z и HWMonitor

Неизвестный актор

Компрометация сайтов

Watering hole

Атака на цепочку поставок

DLL sideloading

RAT

Исследователи «Лаборатории Касперского» выявили компрометацию сайта cpuid[.]com, на котором размещались установщики популярного ПО для системного администрирования CPU-Z, HWMonitor (и HWMonitor Pro) и PerfMonitor 2. Они обнаружили, что в период примерно с 15:00 UTC 9 апреля по 10:00 UTC 10 апреля легитимные URL-адреса для загрузки установщиков этих программ были заменены на URL-адреса, ведущие на вредоносные сайты. Эти сайты распространяли вредоносное ПО как в виде ZIP-архивов, так и в виде автономных установщиков. Эти файлы содержат легитимный подписанный исполняемый файл соответствующего продукта и вредоносную DLL, загружаемую с помощью техники DLL sideloading. Эта DLL отвечает за взаимодействие с C2-сервером и дальнейшее выполнение полезной нагрузки. Перед этим она также выполняет несколько проверок на наличие песочницы. Примечательно, что злоумышленники повторно использовали как адрес C2, так и конфигурацию соединения из кампании марта 2026 года, в ходе которой они разместили поддельный сайт FileZilla, распространявший вредоносные файлы. Загрузчик также содержит огромный массив MAC-адресов (представленных в виде строк), которые впоследствии формируют полезную нагрузку следующего этапа путем преобразования шестнадцатеричных символов в MAC-адресах в их байтовые значения. После набора вспомогательных загрузчиков цепочка выполнения приводит к сложному RAT. Злоумышленники решили в качестве финальной нагрузки повторно использовать так называемый STX RAT, о котором сообщали исследователи eSentire, хотя вредоносная программа и детектируется приведенными в статье YARA-правилами.

Злоумышленники пытались скомпрометировать популярный сайт с программным обеспечением, но не сумели избежать обнаружения по известным индикаторам компрометации. На основе телеметрии «Лаборатории Касперского» было выявлено более 150 жертв, большинство из которых – частные лица. Но были затронуты и несколько организаций из различных секторов, включая розничную торговлю, производство, консалтинг, телекоммуникации и сельское хозяйство, причем большинство заражений зафиксировано в Бразилии, России и Китае.

Вредоносное ПО fast16

APT

Кибersаботаж

Самораспространяющееся вредоносное ПО

Нацеленность на моделирующие и инжиниринговые системы

Исследователи SentinelLabs обнаружили ранее неописанный фреймворк для кибersаботажа, который они отслеживали как fast16. Его основные компоненты датируются 2005 годом, то есть он как минимум на пять лет старше Stuxnet, а значит является первой операцией подобного плана. Все началось с того, что исследователи проследили происхождение техники, использовавшейся в сложнейших вредоносных семействах Flame и Project Sauron. В тех операциях использовалась встроенная система скриптов Lua, позволявшая атакующим обновлять поведение вредоносного ПО на месте. В процессе поисков старых коллекций вредоносных программ, использовавших Lua, исследователи обнаружили подозрительный файл 2005 года под названием svcmgmt.exe. Он выглядел, как обычная служба Windows, но на деле содержал зашифрованный код Lua и ссылки на второй компонент – fast16.sys. Название fast16 отсылает к громкому инциденту, когда группа Shadow Brokers взломала Агентство национальной безопасности США и похитила вредоносный инструментарий Territorial Dispute. По мнению исследователей, fast16 был разработан как кибероружие, которое незаметно распространялось по сетям Windows, прежде чем вмешиваться в определенные процессы моделирования. В отличие от Stuxnet, который напрямую атаковал оборудование критической инфраструктуры, fast16 был разработан для вмешательства в исследовательский и проектный процессы. Исследователи заявили, что вредоносное ПО изменяло результаты вычислений высокоточных инженерных программ и программ для моделирования середины нулевых годов (LS-DYNA 970, PKPM, платформа гидродинамического моделирования MOHID), внося неприметные ошибки в код, используемый для структурного анализа, физического моделирования и других сложных задач. Вмешательство в такие расчеты могло привести к некорректным исследованиям, порче систем и дорогостоящим проектным ошибкам, которые потом невозможно исправить.

Исследователи Symantec опубликовали еще более обширный отчет о вредоносном ПО fast16. Они изучили его механизм перехвата и подтвердили, что вредонос ориентировался на программы LS-DYNA и Autodyn. Исследователи подробно описали три уникальных механизма вмешательства в математические расчеты программ для моделирования. Fast16 проникала во внутренние компьютерные сети, распространялась по целевой инфраструктуре и вносила изменения в конкретный физический процесс моделирования. Алгоритм активировался исключительно при моделировании взрыва при сжатии материала до плотности более 30 г/см³, что соответствует плотности урана или оружейного плутония при сжатии перед взрывом. При достижении этих значений вредоносный код занижал значения выходного давления. В результате инженеры получали искаженные данные о поведении урана, а расчеты сверхкритического состояния получались неточными. Один из механизмов изменял результаты вычисления тензора напряжений Коши исключительно при использовании специального уравнения состояния для взрывчатых веществ. Исследование является свидетельством беспрецедентной компетентности создателей fast16 в области ядерной физики, процессов детонации и моделирования ядерных взрывов.

Атаки Dragon Boss Solutions

Киберкриминал

AV-киллер

Сертификаты разработчика

Исследователи Huntress 22 марта обнаружили подозрительную активность – рекламная программа, имеющая цифровую подпись разработчика, доставляла на системы жертв полезную нагрузку, используя повышенные привилегии и отключив антивирусную защиту. Исполняемые файлы были подписаны компанией Dragon Boss Solutions LLC, которая занимается «исследованиями монетизации поиска». За сутки были зафиксированы 23 565 уникальных IP-адресов из 124 стран, пытавшихся подключиться к инфраструктуре оператора, при этом сотни зараженных устройств находились в сетях важных организаций. Это учебные заведения, электроэнергетические предприятия и кооперативы, транспортные сети, подрядчики компаний из критической инфраструктуры, правительственные и медицинские учреждения.

Исследователи обнаружили, что для развертывания полезных нагрузок MSI и PowerShell использовался механизм обновления из платного инструмента Advanced Installer. Анализ конфигурационного файла процесса обновления выявил несколько флагов, которые делали операцию полностью незаметной и не требующей взаимодействия с пользователями. Этот инструмент также устанавливал полезные нагрузки с повышенными привилегиями, не позволял пользователям отключать

автоматические обновления и часто проверял наличие новых обновлений. Исследователи отметили, что при обновлении извлекалась полезная нагрузка MSI, замаскированная под GIF-изображение. Она содержала несколько легитимных DLL, которые Advanced Installer использовал для определенных задач, таких как выполнение PowerShell-скриптов и поиск на устройстве определенного программного обеспечения, а также для других пользовательских действий, указанных в отдельном файле, содержавшем инструкции для установщика. Перед развертыванием основной полезной нагрузки установщик MSI проводил разведку, проверяя статус администратора, обнаруживая виртуальные машины, проверяя подключение к интернету и запрашивая в реестре установленные антивирусные продукты Malwarebytes, Kaspersky, McAfee и ESET. Защитные решения отключались через PowerShell-скрипты. Исследователи предупредили: хотя вредоносный инструмент в настоящее время действует как уничтожитель антивирусов (AV-киллер), он способен внедрять в зараженные системы гораздо более опасные полезные нагрузки и может быть использован в любое время для эскалации атак.

Атаки на транспортные и логистические организации

Киберкриминал

Сертификаты разработчика

Конвергенция кибер- и традиционной преступности

Целевой фишинг

RMM

В ноябре 2025 года исследователи Proofpoint описали, как злоумышленники компрометируют судоходные компании с целью кражи грузов и перехвата платежей. Исследование получило продолжение: в конце февраля 2026 года специалисты Proofpoint запустили в среде-приманке вредоносную программу, которую злоумышленники рассылали по почте в ходе атаки на транспортные компании. Получив доступ, атакующие установили шесть отдельных инструментов удаленного доступа – четыре экземпляра ScreenConnect, Pulseway Remote Monitoring and Management (RMM) и SimpleHelp RMM, страхуясь таким образом на случай, если какой-либо из них заблокируют. Четвертый загруженный экземпляр ScreenConnect использовал PowerShell-скрипт, который разворачивал переподписанные сторонним провайдером электронной подписи установщики и компоненты ScreenConnect с действительным сертификатом.

В процессе «атаки» исследователи насчитали как минимум 13 PowerShell-скриптов – в совокупности они должны были показать злоумышленникам, принадлежит ли скомпрометированное устройство перспективному с точки зрения получения выгоды пользователю. Скрипты перебирали все локальные учетные записи пользователей и профили браузеров, извлекали историю посещений, копировали заблокированные базы данных браузеров, идентифицировали жестко закодированные URL-адреса,

связанные с банковскими, платежными и логистическими сервисами, сервисами управления флотом, а также с платформами для ведения бухгалтерского учета. Они сканировали системы на наличие криптовалютных кошельков и вручную проверяли учетные данные PayPal. PowerShell-скрипт на зараженном устройстве выполнял поиск точек доступа к финансовым организациям, сервисам для денежных переводов и онлайн-платформам для бухгалтерского учета. Исследователи предположили, что злоумышленники намеревались украсть не только деньги, но и груз, ведь помимо всего прочего из интересовали платформы управления грузоперевозками, фрахтовых брокеров и операторов топливных карт.

Глобальная кампания, нацеленная на ПЛК с поддержкой Modbus

Неизвестный актор

Целевые атаки на АСУ

Эксплуатация общедоступных приложений

DDoS

Исследователи Cato Networks отследили глобальную кампанию, связанную с подозрительной активностью по протоколу Modbus/TCP и нацеленную на подключенные к интернету ПЛК, однако стоящих за ней злоумышленников определить не смогли. С сентября по ноябрь 2025 года было зафиксировано 14 426 целевых IP-адресов из 70 стран, при этом наибольшая доля активности пришлась на США. На протяжении трех месяцев исследователи наблюдали тысячи запросов от самых разных инфраструктур преимущественно с низкой репутаций, хотя встречались и представлявшие интерес инфраструктуры, в частности расположенные в Китае. Исходя из поведения атакующих, они разделили их на пять категорий – от простой разведки до попыток манипуляций с потенциально серьезными последствиями.

Значительная часть активности заключалась в автоматизированных операциях чтения. Атакующие пытались извлечь данные из регистров хранения, чтобы получить информацию о состоянии процесса или конфигурации. За время наблюдения было зарегистрировано более 235 000 таких запросов. Другой паттерн представлял собой так называемый фингерпринтинг: злоумышленники использовали скрипты для целенаправленного запроса метаданных – производителя, названия продукта и версии устройства. Еще один тип запросов касался расширенной идентификации устройства (в сущности это была более тщательная разведка) и оказался редким и кучным: всего 175 запросов с шести IP-адресов. Большинство этих источников находились в Китае и имели высокую репутацию. В некоторых случаях исследователи наблюдали высокочастотные массовые операции чтения, напоминающие DDoS-атаку. Но больше всего их заинтересовали систематические операции записи в доступные регистры хранения. Было идентифицировано

более 3000 запросов на запись, причем все – с одного IP-адреса. Записи выполнялись в соответствии с согласованной структурой, начиная с адреса 0x0BB8 и охватывая от 27 до 122 регистров. Самым пострадавшим сектором стало производство – злоумышленники атаковали подключенные к интернету устройства с поддержкой Modbus. Чуть меньше атак пришлось на медицинскую, строительную, технологическую, транспортную, финансовую и автомобильную отрасли.

Атаки на водоканал в Мексике

APT

Взлом с помощью ИИ

С декабря 2025 года по февраль 2026 года неустановленный актор скомпрометировал и похитил большие объемы данных из девяти мексиканских государственных структур, атаковав их с использованием технологий искусственного интеллекта. По данным Gambit, большую часть технической работы выполняли Claude и GPT-4.1 – они проводили разведку, модифицировали эксплойты, добивались повышения привилегий, картографировали архитектуру баз данных, разрабатывали инфраструктуру для кражи данных, настраивали цепочки туннелей и собирали учетные данные.

Компания Dragos присоединилась к исследованию Gambit, уделив особое внимание инциденту на муниципальном водоканале Servicios de Agua y Drenaje de Monterrey и установив, что компрометация корпоративной ИТ-среды предприятия переросла в попытку проникновения в OT-среду. Злоумышленник использовал Python-скрипт размером 17 000 строк, полностью сгенерированный Claude, который служил основным фреймворком для постэксплуатации. Скрипт, который нейросеть назвала BACKUPOSINT v9.0 APEX PREDATOR, включал в себя 49 модулей, построенных на общедоступных техниках обеспечения безопасности, перебора данных в сети, сбора учетных данных, запросов к Active Directory, получения доступа к базам данных, повышения привилегий, извлечения облачных метаданных и автоматизации горизонтального перемещения. При этом Claude последовательно совершенствовал фреймворк на протяжении всей атаки, добавляя возможности и нивелируя слабые стороны в ответ на оперативную реакцию. Исследователи Dragos предположили, что злоумышленник искал информацию для кражи, пока не заметил, что сеть водоканала содержит OT-интерфейс. Claude идентифицировал промышленный vNode-шлюз предприятия как критически важный и ценный актив. Злоумышленник поручил нейросети провести атаку – та предпочла метод распыления паролей, однако попытка оказалась неудачной, что, вероятно, указывает на использование на предприятии надежных паролей. Исследователи Dragos не обнаружили

свидетельств дальнейшего воздействия на интерфейс vNode или получения злоумышленником доступа в OT-среду предприятия. В своем отчете они указали, что ИИ способен делать OT-системы более видимыми для атакующих, которые уже проникли в ИТ-среду, и отметили, что все более частое использование ИИ в атаках убеждает их в том, что мер безопасности, ориентированных исключительно на предотвращение, теперь становится недостаточно.

Атаки с использованием CRM-системы SmartOffice

Неизвестный актор

APT

Стилер

Уязвимость нулевого дня

Бэкдор

Эксплуатация общедоступных приложений

В марте исследователи ESET заметили, что неизвестные злоумышленники развернули в сети оборонной компании в ОАЭ стилер паролей из браузеров, написанный на .NET. Расследование показало, что активность началась 18 января, когда атакующие скомпрометировали сервер, на котором работала CRM-система SmartOffice компании Zinnia, и загрузили на него веб-шелл. Поскольку в CRM-системе не было найдено известных уязвимостей удаленного выполнения кода, исследователи пришли к выводу, что злоумышленники могли эксплуатировать уязвимость нулевого дня. Атакующие осуществили горизонтальное перемещение внутри скомпрометированной сети и внедрили несколько кастомных реверс-шелл-инструментов, написанных на Rust. Вдобавок они установили OpenSSH-клиент с действительной подписью Microsoft.

Спустя несколько дней, 22 января, злоумышленники загрузили кастомный hands-on-keyboard-инструмент для постэксплуатации с внутренним названием Koshka. Предварительный анализ показал, что он обладает множеством функций, например умеет собирать информацию о скомпрометированной системе (доступные диски, установленные драйверы, текущие процессы, драйверы мини-фильтра, сеансы входа в систему, статус домена, активные TCP- и UDP-соединения, содержимое буфера обмена) и проверять, работает ли она внутри гипервизора. Кроме того, этот инструмент может эксплуатировать уязвимость CVE-2024-26229 для получения повышенных привилегий, создавать новые учетные записи, добавлять пользователей в существующие группы, запускать SOCKS-прокси, удалять NTLM-хеши из базы данных SAM и приостанавливать службу EventLog. Еще он может загружать PE-файлы Windows, но для этого полезная нагрузка должна быть зашифрована с помощью жестко закодированного ключа RC4.

Благодаря телеметрии исследователи обнаружили, что злоумышленники пытались развернуть несколько образцов написанного на Rust кастомного инструмента для реализации обратного прокси, который использует протокол QUIC поверх TLS для создания зашифрованного туннеля. Строка

в отладчике PDB выдает внутреннее название инструмента – revsocks_rust. Помимо него был обнаружен бинарный файл, исходный код которого основан на утилите с открытым исходным кодом portal-tunneler. Прогнав revsocks_rust через VirusTotal, удалось выявить множество вариантов того же вредоносного ПО, которые были загружены в этот онлайн-сервис из Йемена, что указывает на возможный таргетинг в этой стране.

Предупреждение CISA об атаках на системы контроля топливных резервуаров

Целевые атаки на АСУ

Манипуляция данными

Агентство по кибербезопасности и защите инфраструктуры США, Федеральное бюро расследований, Агентство национальной безопасности, Министерство энергетики и другие правительственные ведомства опубликовали совместное предупреждение об атаках на доступные из интернета системы автоматического контроля резервуаров (ATG). Такие комплексы широко используются в энергетической, химической, пищевой, сельскохозяйственной и транспортной отраслях для автоматизированного и дистанционного мониторинга различных параметров резервуаров, например уровня топлива или других жидкостей и их температуры, а также для обнаружения утечек. Ведомства настоятельно рекомендовали пользователям принять защитные меры – отключить системы от интернета и использовать надежные пароли. В ходе недавно зафиксированной, но еще не приписанной конкретной группе вредоносной активности злоумышленники скомпрометировали подключенные к интернету системы автоматического контроля резервуаров, а затем с помощью определенных команд изменили в них некоторые параметры. По данным ведомств, атакующие получили доступ, использовав уязвимости, позволяющие обходить аутентификацию, а также жестко зашитые учетные данные, недостатки в выполнении команд на уровне ОС, SQL-инъекции и ошибки повышения привилегий. В случае успешной компрометации системы злоумышленники могут изменять настройки сети, идентификаторы продуктов, данные об объеме содержимого и параметры управления насосами. Более того, они могут отключить системные оповещения и создать условия, не позволяющие операторам контролировать уровень заполнения резервуаров. Это способно привести к утечкам или сбоям в работе оборудования. В мае CNN сообщил, что за серией атак на такие системы на автозаправках в нескольких штатах стояли иранские хакеры.

Атаки INC

Киберкриминал

Целевой фишинг

Вредоносное ПО под Linux

Эксплуатация сетевых устройств и общедоступных приложений

LOTL

Шифровальщик

Специалисты подразделения по исследованию угроз компании Acronis проанализировали эволюцию INC от относительно нового сервиса типа «Шифровальщик как услуга» до одного из наиболее активных глобальных кластеров вымогателей в 2026 году. С момента появления в 2023 году INC заявил о более чем 800 жертвах и расширил свою активность за счет партнерской модели, использующей тактику двойного вымогательства. По данным отчета, больше всего пострадавших (65%) – в США, преимущественно это организации из производственной, строительной, технологической отраслей, здравоохранения и отрасли права. В своих последних кампаниях INC продолжает атаковать необновленные периферийные устройства и общедоступные приложения, используя для получения первоначального доступа такие уязвимости как CVE-2023-3519 (Citrix NetScaler), CVE-2023-48788 (Fortinet EMS), CVE-2024-57727 (SimpleHelp RMM) и CVE-2025-5777 (CitrixBleed 2), тогда как партнеры INC, помимо эксплуатации перечисленных уязвимостей, прибегают еще и к услугам брокеров начального доступа. После компрометации злоумышленники исследуют сети, сбрасывают учетные данные с серверов резервного копирования Veeam и используют комбинацию легитимных системных средств (Living off the land), таких как RDP и PsExec, а также платные инструменты удаленного мониторинга и управления (RMM) для перемещения по сети жертвы и расширения доступа. Ключевой вехой в эволюции INC стала разработка шифровальщиков для Linux/ESXi и перенос полезных нагрузок как для Windows, так и для Linux на Rust, что повысило мобильность и операционную устойчивость. По мнению исследователей, продажа исходного кода INC в 2024 году способствовала появлению связанных семейств программ-вымогателей со значительным совпадением кода, включая Lynx и Sinobi, что свидетельствует о существенном влиянии кластера на киберкриминальный ландшафт.

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