APT- и финансовые атаки на промышленные организации в четвертом квартале 2025 года

06.03.2026

Версия 1.0

Данный обзор представляет собой сводку публикаций об APT- и финансовых атаках на промышленные предприятия, информация о которых была раскрыта в четвертом квартале 2025 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

В последнем квартале 2025 года исследователи информационной безопасности опубликовали множество интересных историй об атаках на промышленные организации.

Большинство из них подчеркивают актуальность избитых, казалось бы, уже давно проблем. Несвоевременная установка обновлений безопасности, в том числе, на системах, доступных из интернета, небезопасное предоставление удаленного доступа ко внутренним системам, сложность контроля безопасности доверенных партнеров и поставщиков, невозможность гарантировать 100%-ю защиту для традиционных операционных систем с их «родовыми» проблемами информационной безопасности (DLL hijacking, BYOVD и проч.), неготовность персонала противостоять элементарным методам социальной инженерии.

Но среди этих проблем есть и такие, которые хочется упомянуть отдельно. Так, в ряде случаев злоумышленникам удалось не только целенаправленно добраться до OT-систем, но и использовать их для управления технологической установкой или объектом.

Канадский центр кибербезопасности (CCCS) в выпущенном совместно с Королевской канадской конной полицией (RCMP) бюллетене описывает три атаки, в ходе которых хактивистам удалось изменить давление в муниципальном водопроводе, вызвать ложноположительные срабатывания аварийной сигнализации в нефтегазовой компании, поигравшись с системой контроля уровня топлива, и, манипулируя системами управления силосом для сушки зерна, задать некорректные параметры температуры и влажности – ситуация крайне опасная (грозящая не только порчей зерна, но и развитием в нем токсичных грибков), не будь вмешательство вовремя замечено.

Согласно другому бюллетеню, совместно выпущенному Агентством по кибербезопасности и защите инфраструктуры США (CISA) и Федеральным

бюро расследований, хактивистам во многих случаях удавалось через доступный из интернета VNC получить доступ к системам удаленных объектов предприятий американской критической инфраструктуры, относящихся к водоснабжению и канализации, продовольственному и сельскохозяйственному секторам, а также к энергетике. Чаще всего результатом атак становилась временная потеря удаленного управления объектом.

Две истории описывают действия китайско-язычных хакеров, успешно подменявших обновления программных продуктов некоторых китайских же разработчиков, уязвимых к простым методам реализации атак типа «Человек посередине». Атакующие компрометировали пограничные сетевые устройства, устанавливая имплант, перенаправляющий все DNS-запросы на свои серверы. Однако, как минимум в одном случае, они продемонстрировали и способность перехвата и подмены трафика где-то на уровне корневых интернет-маршрутизаторов. От такого вектора атаки защититься своими силами большинству промышленных организаций будет очень сложно.

Интересная тактика замечена в арсенале группировки вымогателей Qilin. Они атаковали Windows-системы, используя вредоносное ПО под Linux, каким-то образом предварительно включив на них Windows Subsystem for Linux (WSL). По всей видимости, это позволяло снизить вероятность обнаружения и блокировки защитными средствами.

Курьезный вредонос был обнаружен командой Socket Threat Research. Sharp7Extend – это вредоносное расширение для библиотеки Sharp7, C#-реализации устаревшей версии протокола коммуникации с ПЛК Siemens S7. Вредоносный код в каждом пятом случае попытки обращения к ПЛК завершает родительский процесс. Вероятно, этот код работает как фильтр, нацеленный на самых безответственных разработчиков, не слышавших о необходимости тестирования функциональности приложения в процессе разработки и перед релизом. Пользователей приложения разработчиков, прошедших этот тест на безответственность, ожидает сюрприз. После 30–90 минут работы приложения вредоносный код начинает выдавать код ошибки на четырех из пяти попыток записи в ПЛК, что, вероятно, по задумке автора вредоноса, должно приводить к сбоям в логике работы приложения. Возникает ощущение, что цель создания вредоноса – повысить культуру работы мелких разработчиков систем промышленной автоматизации.

Пожалуй, наиболее неожиданными и необычными стали публикации следующих исследований.

Все мы понимаем, что данные, добытые в результате кибершпионажа, могут быть использованы в экономических, политических и геополитических противостояниях и как источник военно-разведывательной информации, в том числе в горячей фазе военных конфликтов. В этом квартале в публичном инфополе появилась информация о вероятных следах именно таких применений кибератак.

Исследователи Amazon Threat Intelligence описали сценарии использования кибератаки для поиска и выбора целей в военных конфликтах. В одном случае были атакованы системы геопозиционирования и видеонаблюдения на судне, по которому спустя месяцы был нанесен ракетный удар. Другой описывает компрометацию уличных камер видеонаблюдения в кварталах Иерусалима, подвергшихся через несколько дней ракетным атакам.

Текущие темпы цифровизации сделали судовые системы доступными для атак не только спецслужб, но и рядовых киберзлоумышленников. Исследователи Cydome сообщили об обнаружении нового варианта бот-сети Mirai, названного Broadside. Для распространения ботнет использует эксплойт к уязвимости CVE-2024-3721, в DVR-устройствах (цифровые видеорегистраторы) TBK Vision, часто используемых на судах, создавая угрозу заражения многих из них и недвусмысленно намекая владельцам и операторам флотов, равно как и судостроителям и поставщикам компонентов судовых систем, об острой необходимости уже всерьез озаботиться вопросами кибербезопасности.

Мы неоднократно говорили и писали о возможности различных киберфизических сценариев атак на объекты транспорта и логистики. В этом квартале исследователи Proofpoint описали схему многочисленных кибератак на транспортно-логистические предприятия, конечной целью которых был перехват заказов на перевозку интересных злоумышленникам грузов. Конечный этап – физическая кража грузов, – по мнению исследователей, проводился, вероятно, во взаимодействии с обыкновенными (не кибер-) преступниками. Мы же думаем, что в реализации таких преступных схем выходить за рамки киберпространства больше нет никакой необходимости – последние звенья доставки украденного груза могут также быть хакнуты или использованы втемную, а развитие экосистемы онлайн-продаж и маркетплейсов позволяет полностью автоматизировать доставку украденного товара до произвольных конечных покупателей.

Исследователи Anthropic рассказали о новом уровне использования ML-систем, который они обнаружили в арсенале китайско-язычной группировки GTG-1002. Атакующие использовали Claude Code и ИИ-

агентов на всех этапах развития атаки – от поиска жертв и уязвимостей для первоначального проникновения в их инфраструктуру до исследования инфраструктуры жертвы, продвижения по ней и извлечения данных, автоматизировав таким образом до 80–90% всей работы и оставив людям только контроль качества и небольшую корректировку действий ИИ-агентов по ходу атаки. Исследование, возможно, публично свидетельствует о старте новой гонки – ИИ-кибервооружений.

Активность русскоязычных групп

Атаки Sandworm

APT

Вайпер

Коллаборация групп злоумышленников

Эксплуатация сетевых устройств и общедоступных приложений

Перехват трафика

В отчете об APT-активности исследователи ESET описали атаки группы Sandworm (она же APT44, Seashell Blizzard, BlackEnergy, PHANTOM и Blue Echidna), зафиксированные с апреля по сентябрь 2025 года. Согласно данным исследователей, Sandworm продолжает деструктивные кампании на Украине, внедряя различные вредоносные программы для удаления данных и используя при этом преимущественно групповые политики Active Directory. Так, в апреле злоумышленники запустили два вайпера – ZEROLOT и Sting – в ходе атаки на украинский университет. Примечательно, что Sting был выполнен через задачу планировщика Windows с именем DavaniGulyashaSdeshka. В июне и сентябре Sandworm внедрила несколько вариантов вредоносного ПО для уничтожения данных в украинские организации из правительственного и энергетического секторов, логистической отрасли и зернового комплекса. В отчете говорится, что с 2022 года атакам с использованием вайперов подверглись все четыре сектора, однако зерновой комплекс – в меньшей степени. Изучая активность в течение этого периода, исследователи зафиксировали, что группа UAC-0099 осуществляла первичный доступ к системам жертв, а затем передавала его Sandworm для дальнейших действий. Недавнюю деятельность UAC-0099 подробно описали CERT-UA и Fortinet. Несмотря на то, что в конце 2024 года появились сообщения, свидетельствующие о переориентации русскоязычных групп на шпионскую деятельность, исследователи ESET отмечают, что с начала 2025 года Sandworm продолжает регулярно атаковать украинские организации.

Директор по информационной безопасности Amazon сообщил о кластере, активность которого была направлена против западных энергетических компаний и который, по его словам, скорее всего связан с группой Sandworm. Он отметил, что до 2024 года в ходе многолетней кампании в качестве вектора для получения первоначального доступа использовались

многочисленные уязвимости в WatchGuard (CVE-2022-26318), Confluence (CVE-2021-26084, CVE-2023-22518) и Veeam (CVE-2023-27532). В 2025 году злоумышленники стали меньше полагаться на уязвимости и больше – на неправильно настроенные периферийные устройства на стороне клиента, такие как корпоративные маршрутизаторы, VPN-шлюзы, устройства сетевого управления, платформы для совместной работы, а также облачные решения для управления проектами. Исследователи Amazon не зафиксировали непосредственно извлечение учетных данных атакованных организаций, однако наличие задержек между компрометацией устройства и использованием учетных данных организации указывают на захват трафика с последующим его анализом для кражи учетных данных. Часть скомпрометированных устройств была размещена на экземплярах AWS EC2 и управлялась пользователями сервиса, исходя из чего исследователи сделали вывод, что злоумышленники скорее всего эксплуатировали не недостатки сервиса AWS, а неправильно настроенные устройства клиентов. Кроме того, они считают, что после компрометации развивать атаку могла группа Curly COMRades (о которой писали Bitdefender) в рамках обширной кампании с участием нескольких специализированных подкластеров, о чем свидетельствует совпадение инфраструктур двух групп.

Атаки RomCom

Коллаборация групп злоумышленников

Компрометация веб-сайтов

Поддельные обновления

Бэкдор

В сентябре 2025 года лаборатория Arctic Wolf обнаружила, что американская инжиниринговая компания была атакована с загрузчиком Mythic Agent, используемым в операциях RomCom (она же Void Rabisu, Storm-0978, Tropical Scorpius и UNC2596). Примечательно, что полезная нагрузка RomCom доставлялась при помощи SocGholish, который связывают с деятельностью TA569. SocGholish – это фреймворк для доставки вредоносных программ на целевые компьютеры, впервые обнаруженный в 2017 году. Он представляет собой загрузчик, распространяемый через вредоносный JavaScript, внедренный на скомпрометированные веб-сайты для обеспечения доставки вредоносных нагрузок, которые в совокупности известны как FAKEUPDATE. Как только пользователь нажимает «Обновить», на его устройство загружается вредоносная программа. После запуска SocGholish, используя POST-запросы, отправляет данные из зараженных систем на командный сервер, позволяя в дальнейшем выполнять множество вредоносных действий. В случае, описанном исследователями Arctic Wolf, жертва непреднамеренно запустила описанную цепочку атаки, выполнив вредоносную нагрузку FAKEUPDATE, что позволило операторам SocGholish запустить реверс-шелл на целевой системе, провести разведку и закрепиться в системе –

преимущественно с использованием команд PowerShell. Через три минуты после проверки доступности командного сервера Mythic на систему был установлен загрузчик шелл-кода RomCom – профиль dynamichttp Mythic Agent. Перед расшифровкой и установкой шелл-кода загрузчик проверял, что домен системы совпадает с жестко закодированным целевым значением. По мнению исследователей, это первый зафиксированный случай, когда вредоносная нагрузка RomCom распространялась через SocGholish. Также на систему была загружена и запланирована к запуску дополнительная вредоносная нагрузка, включающая VIPERTUNNEL – модифицированный бэкдор на Python.

Атаки SHADOW-VOID-042

APT

Киберкриминал

Целевой фишинг

Эксплуатация браузера

Исследователи Trend Micro опубликовали отчет, в котором подробно описали активную, целенаправленную шпионскую кампанию, отслеживаемую под именем SHADOW-VOID-042. В октябре и ноябре 2025 года атаки SHADOW-VOID-042 были нацелены на энергетическую и фармацевтическую отрасли, оборонно-промышленный комплекс, химическую и продовольственную промышленности, финансовый и производственный сектора, логистику и ретейл, сектор информационно-коммуникационных технологий, интернет-провайдеров и кибербезопасность. Атаки начинались с рассылки персонализированных фишинговых сообщений, которые содержали весьма правдоподобно выглядевшие приманки. Одни приманки имитировали обновления легитимного ПО (например, было фейковое обновление Trend Micro) или конфиденциальные внутренние документы вроде жалоб в отдел кадров на неподобающее поведение. Другие приманки, также основанные на социальной инженерии, имитировали просьбу присоединиться к научному исследованию или заполнить анкету на тему, связанную с работой. После перехода по ссылке жертва многократно перенаправлялась и в итоге попадала на HTML-страницу, имитировавшую Cloudflare, где загружались три различных JavaScript-файла. Один из них содержал код, эксплуатировавший уязвимость в Chrome CVE-2018-6065, два других файла исследователям получить не удалось. В случае, если эксплуатация уязвимости не удавалась, жертва перенаправлялась на сайт-приманку, визуально копировавший корпоративный стиль Trend Micro. JavaScript-файл содержал жестко закодированный 64-разрядный шелл-код, который отправлял запрос на C2-сервер и извлекал зашифрованный бинарный файл, который расшифровывался и записывался в жестко закодированный путь к файлу. Конечную вредоносную нагрузку в рамках этих компаний получить не удалось.

Исследователи с низкой степенью уверенности утверждают, что эта операция, в виду пересечений по используемым тактикам, может быть связана с деятельностью группы Void Rabisu (также известной как RomCom, Tropical Scorpius, Storm-0978), которая занимается как финансовыми киберпреступлениями, так и кибершпионажем.

Предупреждение CISA об атаках хактивистов на критически важные организации

Хактивизм

Эксплуатация сетевых устройств и общедоступных приложений

DoS

Атаки на АСУ

Агентство по кибербезопасности и защите инфраструктуры США, Федеральное бюро расследований, Агентство национальной безопасности и ряд других иностранных ведомств и организаций опубликовали предупреждение, в котором освещаются известные тактики, техники и процедуры (TTP) русскоязычных групп хактивистов – Cyber Army of Russia Reborn, Z-Pentest, NoName057(16), Sector16 и еще нескольких, связанных с ними, нацеленных на критически важные организации. В документе речь идет о менее сложных атаках по сравнению с операциями APT. В атаках используются слабо защищенные VNC, доступные из интернета, для получения доступа к OT-устройствам объектов критически важной инфраструктуры, что приводит к последствиям различной степени тяжести. Если опираться на сообщения пострадавших организаций, наиболее частым операционным последствием, вызванным этими атаками, была временная потеря видимости, что вызывало потребность ручного вмешательства для управления оборудованием. Среди целей атак – коммунальное (системы водоснабжения и канализации) и сельское хозяйства, продовольственный и энергетический сектора. Хактивисты успешно атаковали сети SCADA, используя базовые методы, и в некоторых случаях одновременно с этим проводили DDoS-атаки. В атаках использовались популярные инструменты для сканирования сети, такие как Nmap или OpenVAS, для поиска VNC-серверов, доступных через порт по умолчанию 5900 или близлежащие порты (5901-5910), а также инструменты подбора паролей для доступа к устройствам. Цель атаки – получить удаленный доступ к HMI-устройствам.

Атаки, нацеленные на российские организации

Атаки с использованием бэкдора GoRed

Хактивизм

Атака на цепочку поставок

Бэкдор

Эксплуатация общедоступных приложений

Троянизированное ПО

Коллаборация групп злоумышленников

Бэкдор GoRed (он же Bulldog) – сложное вредоносное ПО для кибершпионажа, нацеленное на российские организации и связанное, согласно публичным отчетам, с ExCobalt и Shedding Zmiy (исследователи «Лаборатории Касперского» отслеживают эту активность как Red Likho). Впервые обнаруженный в 2023 году, GoRed был подробно описан в недавнем исследовании «Лаборатории Касперского», где были обнаружены новый вектор заражения, сложная схема доставки этого вредоносного ПО и другие TTP его операторов. Бэкдор GoRed нацелен на организации из разных отраслей, включая ИТ, производство, автомобилестроение, энергетику и разработку программного обеспечения. Недавние кампании показали, что злоумышленники сконцентрировались на отрасли разработки ПО, что указывает на стратегическое стремление атаковать цепочки поставок.

В ходе одного инцидента атакующие скомпрометировали публичный веб-портал и, используя ошибки конфигурации в PostgreSQL, смогли удаленно выполнить команды для загрузки бэкдора GoRed. Такой вектор заражения ранее не встречался в атаках с использованием GoRed. Помимо компрометации веб-портала жертвы, злоумышленники получали первоначальный доступ, используя цепочку уязвимостей ProxyShell, затрагивающую Microsoft Exchange (CVE-2021-34473, CVE-2021-34523 и CVE-2021-31207). Получив повышенные права, злоумышленники загружали вредоносный веб-шелл (.aspx) в корневой каталог сервера Exchange. Используя этот веб-шелл, они проводили первоначальную разведку, а затем через него же загружали бэкдор GoRed, выполняя обфусцированную команду.

В ходе атак GoRed исследователи обнаружили троянизированные образцы, схожие с теми, которые использует группа BO Team. Одна из жертв Red Likho упоминалась среди жертв BO Team в их Telegram-канале. Опираясь на эти факты, исследователи предположили, что две группы проводили совместные операции. Учитывая, что BO Team известна сотрудничеством с другими атакующими российские организации хактивистами, такими как Ukrainian Cyber Alliance, вполне вероятно, что группа обменивается знаниями и инструментами с Red Likho, или это могла быть совместная скоординированная операция.

Скоординированные операции проукраинских групп

Киберкриминал

Хактивизм

Бэкдор

Шифровальщик

Троянизированное ПО

Коллаборация групп злоумышленников

Исследователи «Лаборатории Касперского» сообщили о серии скоординированных кибератак, проведенных несколькими проукраинскими хактивистскими группами. Кампании были нацелены на российские организации из различных отраслей, включая производство, здравоохранение и государственный сектор. Особенность этих инцидентов заключается в том, что одну и ту же жертву одновременно атаковали две или три группы. Этот сценарий значительно усложняет идентификацию злоумышленников, поскольку становится трудно однозначно определить TTP каждой отдельной группы.

Исследователи проанализировали серию кампаний, которые публично приписывались проукраинской группе 4BID. Эта группа появилась в начале 2025 года, свою медиаактивность она ведет преимущественно в Telegram-канале. Изначально 4BID фокусировалась на небольших региональных предприятиях, но впоследствии ее целями стали крупные и значимые компании. В организациях, затронутых этими кампаниями 4BID, исследователи также обнаружили свидетельства активности, связанной с двумя другими известными хактивистскими группами: BO Team и Red Likho. В частности, атакованная 4BID инфраструктура также была заражена бэкдорами GoRed, связанным с Red Likho, и ZeronetKit, связанным с BO Team.

Анализ выявил использование разнообразного инструментария, в том числе собственной программы-вымогателя 4BID, получившей название Blackout Locker. Среди любопытных артефактов – кастомные скрипты для проверки компьютеров в сети на наличие AnyDesk или защитных решений Kaspersky, а также для установки AnyDesk, и пропатченный образец Process Explorer, который загружал Tuoni или Cobalt Strike. Сочетание этих инструментов предполагает совместные или параллельные действия нескольких групп для достижения общих целей, таких как дестабилизация, кража данных и постоянный доступ к критически важным системам.

Атаки Cloud Atlas

APT

Целевой фишинг

DLL sideloading

Бэкдор

Исследователи F6 сообщили об атаках группы Cloud Atlas на российские компании агропромышленного и оборонно-промышленного комплексов. В середине октября 2025 года F6 зафиксировала атаку Cloud Atlas, целью которой была российская компания агропромышленного комплекса. Документ-приманка загружал посредством шаблона RTF-файл, который содержал эксплойт к уязвимости CVE-2017-11882, в результате чего происходила загрузка дроппера VBShower. В ходе аналогичной атаки на

предприятия агропромышленного комплекса в сентябре в качестве вредоносной нагрузки также был бэкдор VBShower.

При исследовании октябрьской атаки F6 обнаружила два дополнительных файла, связанных с используемым злоумышленниками доменом в зоне .live и загруженных на платформу VirusTotal. Названия и содержание этих файлов касаются проведения закупок и сбора данных сотрудников предприятий и указывают на то, что среди потенциальных целей были российские компании оборонно-промышленного комплекса. В процессе анализа был обнаружен еще один домен – в зоне .fr. На момент анализа вредоносная нагрузка была недоступна. Исследователи отметили, что группа Cloud Atlas редко использует домены вне зон .com, .net, .org и .info. Такое поведение было замечено ранее разве что в ноябре 2023 года и в октябре 2024 года, когда группа использовала домены в зонах .online и .cfd в атаках на Россию и Беларусь.

В июле 2025 года на VirusTotal были загружены два похожих LNK-файла, совпадающие с LNK-файлами, которые были загружены в конце 2024 года и содержали PDF-файл в качестве приманки и PowerShell-команды для отправки запроса на сервер и обработки полученного ответа. В обоих случаях вредоносная нагрузка была недоступна, однако анализ инфраструктуры позволил исследователям с высокой степенью уверенности предположить, что за атакой с использованием этих LNK-файлов стояла APT-группа Cloud Atlas.

Исследователи «Лаборатории Касперского» описали цепочку заражения и инструменты, которые Cloud Atlas использовала в 2025 году, включая ранее недокументированные импланты. Среди них – скрипты PowerShower, VBS-файлы VBShower и VBCloud, а также бэкдор CloudAtlas. Бэкдор CloudAtlas устанавливается с помощью VBShower из загруженного архива в ходе атаки DLL hijacking – вредоносная библиотека, загружаемая легитимным VLC-приложением, считывает зашифрованную полезную нагрузку, расшифровывает ее и выполняет. Бэкдор CloudAtlas получает с C2-сервера различную вредоносную нагрузку, включая FileGrabber, PasswordStealer и InfoCollector. Группа Cloud Atlas использует кастомный Python-скрипт для извлечения сохраненных учетных данных из браузеров на зараженных системах. Выявленные цели описанных вредоносных действий находятся в России и Беларуси, причем активность наблюдается с начала 2025 года. Атаки затронули различные отрасли, включая телекоммуникации, строительство, государственные учреждения и заводы.

Кибергруппы, атакующие Россию

Киберкриминал

APT

Хактивизм

Фишинговые веб-сайты

ClickFix

Целевой фишинг

Бэкдор

Исследователи Positive Technologies опубликовали анализ активности кибергрупп, нацеленных на российские организации, за III квартал 2025 года с обновленным описанием их TTP, инструментов и принципа выбора жертв. Исследователи разделили группы на три категории: «Кибершпионы», «Финансово мотивированные злоумышленники» и «Хактивисты». Многие группы атакуют, в частности, логистические, производственные и энергетические компании.

В числе кибершпионских групп – Telemancon, нацеленная на российские промышленные организации. Группа использует кастомный TMCDropper, но если раньше в нем применялась схема с отдельными зашифрованными сегментами кода, то в текущей версии – обфускация на основе виртуальной машины с многослойными уровнями шифрования, что значительно усложняет анализ вредоносного ПО. Другой инструмент группы – бэкдор TMCShell – теперь препятствует своему исполнению в песочнице. В отчете также подробно описывается деятельность таких кибершпионских групп, как PseudoGamaredon, TA Tolik, XDSpy, Rare Werewolf, Goffee и IAmTheKing. Цепочки атак этих групп начинались с фишинговых писем. Группа PhantomCore использовала фишинговые страницы с фейковой CAPTCHA, побуждающей к выполнению PowerShell-скрипта.

В категорию финансово мотивированных групп входят DarkGaboon, DarkWatchman, Fluffy Wolf, которые используют фишинговые письма с вредоносными архивами. Хактивистская группа Black Owl продолжает атаковать компании из транспортно-логистической отрасли, используя целевые рассылки с бизнес-повесткой. Чтобы повысить шансы на успешный запуск вредоносного ПО, злоумышленники стали чаще вкладывать в один архив сразу несколько идентичных образцов, отличающихся только документами-приманками. Используя легитимные инструменты отслеживания прочтения электронной почты, злоумышленники оценивали вовлеченность получателей и приоритизировали дальнейшие действия в отношении тех контактов, которые с наибольшей вероятностью откроют вложение.

Атаки на аэрокосмическую отрасль России

Хактивизм

Целевой фишинг

Фишинговые веб-сайты

Компрометация легитимных почтовых серверов

Бэкдор

Исследователи Intrinsec проанализировали многочисленные кампании, нацеленные на российские аэрокосмические организации, а также организации, связанные с производством средств радиоэлектронной борьбы, военными поставками и энергетикой. Исследователи предполагают, что за этими атаками стоят несколько действующих в интересах украинских властей хактивистских групп, которые используют как фишинговые страницы, так и вредоносное ПО. Злоумышленники рассылали целевые фишинговые письма якобы от имени российских правительственных учреждений со ссылками на фейковые страницы входа, размещенные на таких сервисах, как IPFS, Vercel, Contabo S3 и Cloudflare R2. Более квалифицированные группы вроде Head Mare и Hive0117 использовали вредоносные письма и кастомные вредоносные программы, доставляемые со скомпрометированных российских почтовых серверов.

Атаки Arcane Werewolf

APT

Целевой фишинг

C2, мимикрирующий под сайт промышленной компании

Бэкдор

Исследователи Bi.ZONE сообщили о вредоносной активности кластера Arcane Werewolf (Mythic Likho), нацеленной на российские промышленные компании, зафиксированной в октябре и ноябре 2025 года. Злоумышленники, скорее всего, использовали в качестве вектора первоначального доступа фишинговые письма, как это бывало раньше, однако в этот раз фишинговые письма получить не удалось. Они, предположительно, содержали ссылку на загрузку вредоносного архива с подконтрольного злоумышленникам ресурса, который был замаскирован под сайт российской промышленной компании. Загруженный архив содержал вредоносный LNK-файл, а также каталог «Фото» с набором изображений в формате JPG. После запуска LNK-файла и выполнения команды через PowerShell загружался исполняемый файл, который затем запускался через conhost.exe. Загруженный icon2.png являлся исполняемым файлом формата PE32+ и представлял собой вредоносный дроппер, реализованный на Go. Он содержал вредоносную нагрузку в виде двух файлов в кодировке Base64: исполняемый файл формата PE32+, выполняющий роль вредоносного загрузчика, и отвлекающий PDF-документ с информацией о бракованных партиях электронных товаров. Дроппер декодировал вредоносную нагрузку и сохранял ее в каталоге %TEMP%, после чего выполнял команды, доставляя Loki 2.0.

В ноябре была зафиксирована очередная активность кластера Arcane Werewolf, но, к сожалению, полностью восстановить цепочку атак не удалось. Вредоносный сетевой ресурс имитировал сайт российской промышленной компании. Использовавшийся в качестве приманки PDF-

документ содержал информацию о проведении внутреннего расследования. В ходе этой атаки были обнаружены новый дроппер на C++ и обновленный Loki версии 2.1, совместимый с фреймворками Mythic и Havoc.

Атаки Paper Werewolf

APT

Целевой фишинг

Приманка, сгенерированная ИИ

Бэкдор

Исследователи Intezer установили, что группа Paper Werewolf (она же GOFFEE) запустила новую кампанию против российских военнослужащих и организаций оборонно-промышленного комплекса. В ходе кампании, зафиксированной в октябре, использовался вредоносный XLL-файл, загруженный на платформу VirusTotal сначала из Украины, а затем из России. Файлы с именами «Плановые цели противника.xll» и «Плановые цели противника НЕ ЗАПУСКАТЬ.xll» были созданы так, чтобы автоматически выполнять вредоносный код при открытии Excel. После запуска загружался ранее недокументированный бэкдор, получивший название EchoGather, который позволял злоумышленникам собирать системную информацию, выполнять команды и передавать файлы. Похищенные данные отправлялись на C2-сервер, замаскированный под сайт службы доставки еды.

Кроме того, в качестве фишинговых приманок группа GOFFEE использовала поддельное приглашение на концерт для старшего офицерского состава вооруженных сил. В документе явно прослеживались признаки создания с помощью нейросетей, включая грамматические ошибки и неточное изображение российской символики с двуглавым орлом. Еще одна приманка имитировала письмо заместителя министра промышленности и торговли России с запросом документов, обосновывающих цены государственных оборонных контрактов. Письмо было адресовано крупным оборонным и высокотехнологичным предприятиям, которые, как предполагают исследователи Intezer, и являлись мишенями. Обе приманки также были связаны с бэкдором EchoGather.

Операция FrostBeacon

Киберкриминал

Целевой фишинг

Исследователи Seqrite Labs обнаружили финансово мотивированную киберкампанию, нацеленную на российские B2B-предприятия, в первую очередь из логистической, промышленной и строительной отраслей, а также из сферы технического снабжения. Экосистема злоумышленников включает в себя множество цепочек заражения и приманок, ориентированных на финансовые и юридические отделы российских организаций. Кампания, получившая название «Операция FrostBeacon»,

использует многоуровневую цепочку заражения для доставки маяков Cobalt Strike. Для получения первоначального доступа злоумышленники задействуют два отдельных кластера. Первый кластер использует фишинговые письма с вредоносными архивами, которые содержат загрузчики LNK и HTA. Второй кластер использует устаревшие уязвимости CVE-2017-0199 и CVE-2017-11882 через вредоносные DOCX-файлы. В этом случае фишинговые письма имитируют досудебные претензии о погашении задолженности. Оба кластера в итоге приводят к выполнению обфусцированного PowerShell-загрузчика, который расшифровывает и запускает в памяти шелл-код для развертывания Cobalt Strike. Инфраструктура кампании включает несколько доменов в зоне .ru, сконфигурированных в качестве конечных точек C2 с модифицированным настраиваемым профилем Cobalt Strike, чтобы избежать обнаружения. Исследователи отметили совпадение TTP и целей с Cobalt Group, атаковавшей финансовые учреждения по всему миру, однако каких-либо конкретных семейств вредоносных программ, связанных с этой группой, в ходе операции FrostBeacon не обнаружили.

Атаки VasyGrek

Киберкриминал

Целевой фишинг

Ссылки на GitHub

Бэкдор

Шифровальщик

Исследователи F6 сообщили о новой активности VasyGrek, связанной с фишинговыми рассылками в адрес российских организаций с целью кибершпионажа. VasyGrek (Fluffy Wolf) – русскоязычные злоумышленники, атакующие российские компании из различных отраслей как минимум с 2016 года. В новом отчете F6 подробно описаны инструменты актора и его атаки за период с августа по ноябрь 2025 года. За это время VasyGrek атаковали российские компании из производственной, строительной, энергетической, сельскохозяйственной, торговой и финансовой отраслей, а также из сфер кибербезопасности, ИТ, медиа и развлечений.

После публикации в июле 2024 года исследования об активности VasyGrek и их сотрудничестве с поставщиком вредоносного ПО Mr. Burns злоумышленники перестали использовать BurnsRAT, но в целом цепочки заражения в ходе его атак с того момента до октября 2025 года практически не изменились. Они по-прежнему рассылали фишинговые письма якобы от имени бухгалтерии, в которых вредоносный файл доставлялся потенциальным жертвам как в виде вложения, так и по ссылкам на репозитории GitHub или зарегистрированные им самим домены. Вредоносный файл представлял собой архив с исполняемым файлом внутри или же непосредственно исполняемый файл PureCrypter, который мог доставлять на систему жертвы вредоносное ПО следующего этапа и внедрять вредоносную нагрузку в нужные процессы. ВПО

различных стадий могло как загружаться с внешних ресурсов, так и храниться локально в зашифрованном виде. VasyGrek использовали программные продукты разработчика PureCoder (PureCrypter, PureHVNC/PureRAT, PureLogs Stealer), а также Pay2Key – сервис для вымогателей, распространяемый как RaaS (Ransomware as a Service – шифровальщик как услуга) и построенный на базе популярной программы-вымогателя Mimic.

Некоторые изменения в цепочках заражения были зафиксированы в ноябре: вместо архивов с исполняемыми файлами внутри в фишинговых письмах стали использоваться архивы с BAT- и VBS-файлами. В цепочке, содержащей VBS-файл, конечной вредоносной нагрузкой была вредоносная программа PureHVNC, но для ее доставки вместо привычного загрузчика PureCrypter использовался другой, классифицированный как powershell stego downloader. Этот загрузчик использовался разными злоумышленниками, в частности неоднократно был замечен в арсенале группы Sticky Werewolf.

Корейский полуостров

Атаки Lazarus

APT

RAT

Троянизированное ПО

DLL sideloading

DLL-проксирование

Компрометация веб-сайтов

Целевой фишинг

Бэкдор

Исследователи ESET обнаружили новую волну операции DreamJob, проводимой группой Lazarus и нацеленной на европейские аэрокосмические и оборонные компании, в частности те, что занимаются разработкой технологий для беспилотных летательных аппаратов. Исследователи предположили, что главной целью злоумышленников была кража конфиденциальной информации, в том числе относящейся к технологиям производства. Первоначальный доступ, скорее всего, был получен методом социальной инженерии: потенциальной жертве отправляли приманку в виде документа с описанием вакансии и троянизированное ПО для его открытия. Использовалось ВПО с открытым исходным кодом, такое как модифицированный Notepad++, WinMerge, TightVNC Viewer и проекты MuPDF, для доставки RAT ScoringMathTea. Эта вредоносная программа использовала технику DLL sideloading, рефлективную загрузку кода и шифрование AES/ChaCha20 для сокрытия активности, позволяя осуществлять удаленное управление, манипуляции файлами и кражу данных. Злоумышленники внедряли вредоносные загрузчики в легитимные проекты, и использовали многоступенчатые дропперы и загрузчики, прежде чем развернуть RAT в памяти. Анализ показывает, что Lazarus продолжает развиваться в рамках операции

DreamJob, внедряя новые библиотеки для DLL-проксирования, модульные загрузчики и усовершенствованные методы обфускации, сохраняя при этом последовательную и эффективную стратегию атак на технологический и оборонный секторы.

Исследователи ENKI обнаружили новый вариант программы Comebacker группы Lazarus, распространявшийся через поддельные документы Word, тематически связанные с аэрокосмической и оборонной отраслями, и указывающие на кибершпионский характер операции. Файлы-приманки содержали вредоносные макросы, которые запускали многоэтапный процесс выполнения вредоносного ПО и в итоге загружали бэкдор Comebacker непосредственно в память. Злоумышленники использовали сложную цепочку заражения с модифицированным алгоритмом дешифровки, защищенными ChaCha20-шифрованием загрузчиками и зашифрованными с помощью AES коммуникациями с командным сервером. Все это свидетельствует о явном развитии по сравнению с ранними версиями Comebacker. В ходе исследования инфраструктуры были выявлены дополнительный командный домен и образец Comebacker, датированный мартом 2025 года, что указывает на продолжительность кампании. Приманки были замаскированы под документы таких организаций, как Edge Group, Airbus, а также Индийского технологического института в Канпуре, что свидетельствует о целенаправленности атаки. Целью кампании, судя по всему, является сбор разведданных и обеспечение долгосрочного доступа к организациям из значимых отраслей.

Активность, связанная с Ближним Востоком

Атаки MuddyWater

APT

Целевой фишинг

Брокеры доступа

Бэкдор

Исследователи ESET раскрыли сложную кибершпионскую кампанию группы MuddyWater, нацеленную на Израиль и Египет, в том числе на правительственные, производственные, транспортные, коммунальные, инженерные и технологические организации. Злоумышленники получали первоначальный доступ, как правило, через целенаправленные фишинговые рассылки, часто содержавшие вложения в формате PDF с ссылкой на установщики ПО для удаленного мониторинга и управления (RMM), размещенные на бесплатных файлообменных платформах вроде OneHub, Egnyte или Mega. Эти ссылки приводили к загрузке таких RMM-инструментов, как Atera, Level, PDQ и SimpleHelp. Среди инструментов, развернутых операторами MuddyWater, также есть бэкдор VAX-One,

название которого составлено из первых букв легального программного обеспечения, под которое он маскируется: Veeam, AnyDesk, Xerox и служба обновления OneDrive. В этой операции также используются ранее недокументированные кастомные инструменты, включая загрузчик в память Fooder и MuddyViper – бэкдор на C/C++, предназначенный для скрытого закрепления в системе, кражи учетных данных и удаленного управления. Fooder использует логику задержки выполнения, как в игре «Змейка», и рефлективную загрузку, чтобы избежать обнаружения, тогда как MuddyViper поддерживает расширенное выполнение команд, извлечение данных и множество механизмов закрепления. В ходе кампании внедряются ВПО для кражи учетных данных и данных браузера (CE-Notes, LP-Notes, Blub), а также обратные туннели go-socks5. ESET отметила снижение «ручной» активности и повышение операционной дисциплины по сравнению с более ранними кампаниями MuddyWater. Примечательно, что в ходе этой активности было зафиксировано операционное пересечение с Lyceum (подгруппа кибершпионской группы OilRig), что может свидетельствовать о сотрудничестве либо о посреднической роли MuddyWater в получении первоначального доступа. В целом, кампания демонстрирует эволюцию MuddyWater – группа расширяет инструментарий, повышает квалификацию, продолжая при этом концентрироваться на кибершпионаже.

Атаки UNC1549

APT

Целевой фишинг

Бэкдор

C2, проксируемый через Azure

DLL sideloading

Сертификаты разработчика

Атака на цепочку поставок/доверенных партнеров

Вредоносное ПО под Linux

Исследователи Mandiant раскрыли подробности продолжительной шпионской операции группы UNC1549 (она же Smoke Sandstorm, TA455, Yellow Liderc, Tortoiseshell, Imperial Kitten), атакующей аэрокосмические, авиационные и оборонные предприятия главным образом на Ближнем Востоке. Злоумышленники используют для получения первоначального доступа две тактики: рассылают специально созданные фишинговые письма и компрометирует доверенных внешних поставщиков, чтобы проникнуть в сети по легитимным подключениям. После проникновения они используют нестандартные методы горизонтального перемещения: прерывают Citrix/VMware-сессии, эксплуатируют внутренние тикет-системы для кражи учетных данных и крадут информацию для создания еще более правдоподобных фишинговых писем. Злоумышленники внедряют несколько модифицированных бэкдоров вроде TWOSTROKE, DEEPROOT, MINIBIKE и GHOSTLINE, часто используя технику DLL hijacking и размещенную на Azure инфраструктуру, что позволяет им оставаться незамеченными. Одна из вредоносных программ в арсенале UNC1549 – DEEPROOT – представляет собой бэкдор для Linux, написанный на Golang. Злоумышленники также в значительной степени полагаются на обратные

SSH-туннели и «спящие» бэкдоры, позволяющие «переждать» попытки обнаружения и вернуться к активности позднее. Кража учетных данных с использованием снимков экрана и поддельных форм входа в систему позволяют повышать привилегии. UNC1549 использует DCSYNCER.SLICK – модифицированную версию инструмента DCSyncer с открытым исходным кодом – для выполнения операций DCSync в Active Directory и извлечения хешей паролей. Замечено, что злоумышленники подписывали бинарные файлы некоторых своих бэкдоров легитимными сертификатами разработчика для создания образцов вредоносного ПО, в частности вариантов GHOSTLINE, POLLBLEND и TWOSTROKE. В сентябре Check Point и Prodaft также сообщили об атаках UNC1549, описав некоторые из перечисленных особенностей.

Исследователи Amazon Threat Intelligence выявили новый тренд, который они назвали киберкинетическим таргетингом – когда информация, полученная в ходе кибератаки, используется для прямой поддержки военных действий. В одном случае группа Imperial Kitten взломала морские системы геопозиционирования и системы видеонаблюдения на судне за несколько месяцев до того, как по нему был нанесен ракетный удар. В другом случае группа MuddyWater получила доступ к камерам видеонаблюдения в Иерусалиме за несколько дней до ракетных ударов Ирана, вероятно, проведя разведку для определения целей. По мнению исследователей, это радикально меняет роль и значение кибероперации – прежде не имевшие непосредственного отношения к военным действиям, теперь они становятся их неотъемлемой частью.

Атаки GalaxyGato

APT

DLL sideloading

Бэкдор

Исследователи ESET сообщили, что действующая в интересах Ирана группа GalaxyGato начала атаковать организации из судоходной отрасли в Греции, аналогично MuddyWater и некоторым группам, связанным с Китаем. С июля 2025 года GalaxyGato использует свой бэкдор C5 (это еще и второе название группы) и постепенно совершенствует его. В ходе кампании против Греции GalaxyGato использовала PowerShell-скрипты для сбора информации о скомпрометированных системах и перечня установленных программ (вероятно, для обхода защитных решений). Использование PowerShell, особенно таким образом, весьма практично, вероятность обнаружения активности аналитиками SOC при этом невысока. По словам исследователей, это был не первый случай обнаружения именно этой версии C5. В июле 2025 года GalaxyGato впервые использовала ее в ходе кампании, нацеленной на одну организацию в Израиле. И снова группа использовала PowerShell-скрипты,

но уже для доставки C5 с командного сервера. При этом бэкдор был обфусцирован с помощью ConfuserEx. Любопытный момент в этой компании – перехват порядка поиска DLL-библиотек, при котором злоумышленники поместили вредоносную DLL в каталог Windows Defender (C:\Program Files\Windows Defender). Windows Defender вызывал библиотеку с тем же именем – Version.dll, однако первой (в силу своего расположения на диске) загружалась вредоносная библиотека. Она вызывала другую вредоносную DLL, расположенную на один каталог ниже (C:\Program Files\Windows Defender\Offline\MMpLics.dll), которую злоумышленники тоже загрузили на систему жертвы. Эта вторая библиотека – MMpLics.dll – вызывается службой LSASS каждый раз, когда пользователь вводит учетные данные; в этот момент MMpLics.dll записывает эти учетные данные в другой файл в каталоге Windows Defender (C:\Program Files\Windows Defender\en-US\MsMpCon.dll.mui). После этого GalaxyGato может извлекать учетные данные для осуществления горизонтального перемещения и повышения привилегий.

Активность китайско-говорящих групп

Атаки PassiveNeuron

APT

Компрометация SQL-сервера

GitHub DDR

C2 на CloudFront

Исследователи «Лаборатории Касперского» обнаружили новую волну заражений Windows Server, связанную с кампанией PassiveNeuron, о которой они рассказывали в 2024 году. Эти случаи заражения были зафиксированы в правительственных, финансовых и промышленных организациях в Азии, Африке и Латинской Америке. Анализ инцидентов позволил получить дополнительные сведения о кампании. В частности, удалось установить, что вектором первоначального заражения была компрометация SQL-сервера, предположительно осуществленная с использованием SQLMap. После компрометации атакующие предприняли попытку развертывания веб-шелла. Кроме того, они использовали Neursite (кастомный модульный бэкдор, написанный на C++), NeuralExecutor (кастомный .NET-имплант, предназначенный для запуска дополнительных .NET-нагрузок) и импланты Cobalt Strike для дальнейшей вредоносной активности на зараженных машинах. Также было отмечено, что имплант NeuralExecutor был обновлен и использовал GitHub как dead drop resolver для получения командного сервера. Исследователи приписали кампанию PassiveNeuron китайско-язычной группе, поскольку строка PDB в одной из проанализированных DLL-библиотек упоминалась в отчете Cisco Talos, где описана активность, предположительно связанная с группой APT41.

Атаки PlushDaemon

APT

AitM

Бэкдор

Атака на цепочку поставок

Эксплуатация общедоступных приложений

Исследователи ESET раскрыли шпионскую операцию китайско-язычной группы PlushDaemon, которая использует сетевой имплант EdgeStepper для перехвата обновлений ПО в атаках типа AitM. Злоумышленники сначала компрометируют маршрутизаторы или другие сетевые устройства, чтобы перенаправить весь DNS-трафик на собственные серверы, заставляя механизмы обновления загружать вредоносные файлы. Исследователи заметили, что PlushDaemon перехватывает обновления редактора ввода иероглифов Sogou Pinyin, аналогичным способом были скомпрометированы обновления и других популярных китайских программ. Загружаемые файлы доставляют LittleDaemon и DaemonicLogistics, которые, в свою очередь, устанавливают бэкдор SlowStepper. Группа также использует эксплойты веб-серверов и атаки на цепочку поставок как дополнительные точки входа. Эта продолжительная кампания нацелена как на частных лиц, так и на организации. PlushDaemon атаковала пользователей и организации в следующих регионах: США, Тайвань, Китай (включая университет и тайваньскую компанию по производству электроники), Гонконг, Новая Зеландия, Камбоджа (включая компанию из автомобильной отрасли и филиал японской производственной компании).

Атаки SinisterEye

APT

AitM

Бэкдор

По данным исследователей ESET, китайско-язычная группа SinisterEye (она же LuoYu и CASCADE PANDA) проводила в Китае кибершпионские операции против местных и иностранных организаций. Имея, по всей видимости, в том числе и доступ к магистральной интернет-инфраструктуре, SinisterEye использовала в качестве основного метода получения первоначального доступа перехват обновлений для доставки своего ключевого бэкдора – WinDealer для Windows или SpyDealer для Android. С мая 2025 года группа постоянно атакует китайские офисы тайваньской компании, работающей в сфере военной авиации. Эта компания также имеет отношение к полупроводниковой промышленности. В августе SinisterEye начала атаковать представителей базирующейся в Китае американской торговой компании и офис греческого правительственного учреждения, тоже в Китае. Исследователи полагают, что в первом случае цель была выбрана в контексте текущего торгового противостояния между США и Китая, поскольку атакованная организация, как сообщается, лоббирует принятие мер, направленных на смягчение определенных американских пошлин в отношении некоторых азиатских стран. В сентябре исследователи обнаружили образцы WinDealer на компьютерах одного из государственных учреждений Эквадора. Хотя

механизм перехвата у SinisterEye, судя по всему, нацелен преимущественно на устаревшие протоколы обновления китайского ПО (например, Sogou Pinyin Method, 360 Total Security, Taobao и You Dao), исследователи зафиксировали случаи, когда исполняемые файлы, вероятно, подменялись при передаче телеком-оператором. Это означает, что возможности SinisterEye по подмене обновлений ПО не ограничиваются жестко заданным набором уязвимых приложений.

Атаки APT24

APT

Целевой фишинг

Компрометация веб-сайтов

DLL sideloading

Атака на цепочку поставок

Бэкдор

Исследователи Google Threat Intelligence Group обнаружили ранее недокументированное вредоносное ПО BadAudio, развернутое китайскоязычной группой APT24 в ходе сложной трехлетней шпионской кампании. ВПО доставлялось жертвам различными способами – посредством фишинга, атак на цепочку поставок и атак типа watering hole. В период с ноября 2022 года по сентябрь 2025 года APT24 скомпрометировали более 20 сайтов различных организаций – региональных промышленных предприятий. В атаке использовался оппортунистический подход к получению первоначального доступа. Легитимные сайты были заражены вредоносным JavaScript. Скрипт собирал отпечатки браузера, соответствовавшие критериям атаки, и отображал жертве имитирующее Chrome всплывающее окно с требованием обновить ПО, побуждая пользователя скачать BadAudio. Начиная с августа 2024 года APT24 перешла к фишинговым атакам, распространяя BadAudio через электронные письма якобы от имени организации по защите животных. В некоторых случаях группа использовала вместо собственных серверов легитимные облачные сервисы Google Drive и OneDrive для доставки вредоносного ПО.

Вредоносное ПО BadAudio сильно обфусцировано. Для загрузки оно использует технику DLL hijacking. BadAudio собирает информацию о системе (имя хоста, имя пользователя, архитектуру), шифрует эти данные с помощью жестко закодированного AES-ключа и отправляет их на жестко закодированный C2-адрес. Затем BadAudio загружает с командного сервера зашифрованную AES вредоносную нагрузку, расшифровывает ее и выполняет в памяти через DLL-загрузчик. В одном из случаев исследователи Google наблюдали развертывание через BadAudio маяка Cobalt Strike, однако не смогли подтвердить наличие маяка в остальных инцидентах.

Атаки Speccom

APT

Целевой фишинг

Бэкдор

По данным исследователей ESET, китайско-язычная группа Speccom в июле 2025 года атаковала энергетический сектор Центральной Азии посредством целевой фишинговой рассылки с вложенным документом, содержавшим вредоносный макрос. Письмо было отправлено, по всей видимости, с адреса скомпрометированной правительственной организации, также находящейся в Центральной Азии. После компрометации разворачивался бэкдор первого этапа, получивший название CalaRat. Он использовался для внедрения варианта бэкдора BLOODALCHEMY, который ранее был публично проанализирован Elastic Security и ITOCHU Cyber & Intelligence и, вероятно, используется китайско-язычными группами. Группа Speccom внедряла еще два бэкдора: один получил название kidsRAT из-за использования DWORD-значения 0x6B696473 (kids в ASCII) в его протоколе связи, а другой, написанный на Rust, – название RustVoralix.

Атаки WARP PANDA

Новый актор

Эксплуатация сетевых устройств и общедоступных приложений

Облачные сервисы как C2

Вредоносное ПО под Linux

Бэкдор

Исследователи CrowdStrike раскрыли инструментарий ранее неизвестной китайско-язычной группы, получившей название WARP PANDA и ответственной за продолжительные атаки на инфраструктуру VMware vCenter и ESXi юридических, технологических и производственных компаний в США. Группа, действующая как минимум с 2022 года, демонстрирует высокий уровень знаний принципов операционной безопасности (OPSEC) и облачных технологий, сосредоточиваясь преимущественно на краже данных. WARP PANDA развернула уникальный стек вредоносных программ, который включает в себя BRICKSTORM – бэкдор на Golang, использующий WebSockets, а также DNS-over-HTTPS (DoH) и облачные сервисы для сокрытия командного сервера. Группа также внедряла два ранее неизвестных импланта, ориентированных на ESXi, – Junction и GuestConduit, которые обеспечивают туннелирование трафика через VSOCK. Первоначальный доступ обычно достигался за счет эксплуатации доступных из интернета периферийных устройств и уязвимостей vCenter, после чего осуществлялось горизонтальное перемещение с использованием SSH и привилегированной учетной записи vpxuser. Злоумышленники поэтапно извлекали данные из снэпшотов виртуальной машины в реальном времени, клонировали виртуальные машины контроллера домена и использовали облачный доступ для сбора данных из Microsoft 365. В целом, эта активность свидетельствует о высокой квалификации шпионской группы в части виртуализации и облачных технологий.

Киберкриминал и прочее

Атаки с использованием загрузчика PhantomVAI

Киберкриминал

Целевой фишинг

RAT

Инфостилер

Стеганография

Исследователи Unit 42 раскрыли глобальные фишинговые кампании, в ходе которых распространялся PhantomVAI – усовершенствованный вредоносный .NET-загрузчик, доставляющий несколько инфостилеров, в частности Katz Stealer, AsyncRAT, XWorm, FormBook и DCRat. Атаки реализуются в несколько этапов – начинаются с рассылки фишинговых писем, содержащих обфусцированные JavaScript- или VBS-файлы, за которыми следуют PowerShell-загрузчики, использующие стеганографию для сокрытия вредоносной DLL-нагрузки в GIF-изображениях. После запуска PhantomVAI распознает виртуальную машину, закрепляется в системе, используя задачи планировщика и ключи реестра Run, а затем применяет технику process hollowing (обычно на MSBuild.exe) для внедрения финальной вредоносной нагрузки. PhantomVAI изначально связан с распространяемым по модели MaaS (Malware-as-a-Service) Katz Stealer, который собирает учетные данные, данные криптокошельков, данные Telegram, а также системную информацию, избегая при этом выполнения в системах из стран СНГ. Злоумышленники используют загрузчик PhantomVAI в атаках по всему миру против организаций из различных отраслей: производство, образование, коммунальные услуги, технологии, здравоохранение, ИТ, правительство.

Атаки Qilin

Киберкриминал

Шифровальщик

BYOVD

Вредоносное ПО под Linux

Фишинговые веб-сайты

ClickFix

Исследователи Trend Micro выявили группу вымогателей Agenda (она же Qilin), которая внедряла на Windows-системы разработанный под Linux шифровальщик, пользуясь легитимными средствами удаленного администрирования и передачи файлов. С января 2025 года от деятельности Agenda пострадали более 700 жертв в 62 странах, в первую очередь организации на развитых рынках и из отраслей с высокой добавленной стоимостью. Больше всего жертв было в США, Франции, Канаде и Великобритании, сильнее всего пострадали промышленный, технологический и финансовый сектора, а также здравоохранение.

Исследователи предполагают, что злоумышленники инициировали свою кампанию через сложную схему социальной инженерии с использованием страниц с поддельной CAPTCHA. Анализ встроенного в эти страницы обфусцированного JavaScript позволил выявить многоступенчатую систему доставки вредоносной нагрузки. Судя по всему, эти страницы доставляли на скомпрометированные системы инфостилеры, которые

впоследствии собирали токены аутентификации, куки браузера и сохраненные учетные данные.

Цепочка атаки включала сложные техники, например, Bring Your Own Vulnerable Driver (драйвер eskle.sys, вероятно, относится к игровому пакету), для обхода защитных решений. Для связи с командным сервером была развернута инфраструктура из множества экземпляров SOCKS-прокси-сервера, в качестве которого использовался бэкдор COROXY. Злоумышленники пользовались легитимными инструментами, в частности ScreenConnect и AnyDesk, которые устанавливали через платформу удаленного мониторинга и управления ATERA Networks. Группа Agenda также использовала приложение для удаленного доступа Splashtop Remote (SRManager.exe) для запуска бинарного кода программы-вымогателя под Linux на системах под управлением Windows, что, скорее всего, позволяло снизить вероятность обнаружения. Для запуска этого кода злоумышленникам потребовалось, видимо, включить на атакованных системах Windows Subsystem for Linux (WSL). Группа Agenda целенаправленно атаковала инфраструктуру резервного копирования Veeam, чтобы собирать учетные данные, зная, что такие системы часто хранят учетные данные для доступа к множеству систем на предприятии. На скомпрометированных системах планомерно внедрялись многочисленные SSH-клиенты PuTTY для упрощения горизонтального перемещения.

Предупреждение CCCS, касающееся доступных из интернета промышленных систем

Хактивизм

АСУ, доступные из интернета

Канадский центр кибербезопасности (CCCS) и Королевская канадская конная полиция выпустили предупреждение в связи с сообщениями об инцидентах, затронувших доступные из интернета АСУ. В документе описаны три недавних инцидентах, в ходе которых хактивисты нарушили работу критически важных систем. В первом случае злоумышленники изменили давление воды на городском водоканале, что привело к перебоям в обслуживании населения. Во втором случае воздействовали на датчик системы контроля уровня топлива в резервуаре нефтегазовой компании, вызвав ложное срабатывание сигнализации. В третьем случае злоумышленники сумели задать некорректные параметры температуры и влажности в системе управления силосом для сушки зерна, что могло привести к потенциально опасной ситуации, если бы это вовремя не обнаружили. Канадские власти предполагают, что это не сложные атаки и они не были заранее спланированы, а носили оппортунистический характер, преследуя цель привлечь внимание медиа и нанести репутационный ущерб. В ответ на рост активности хактивистов канадские

власти рекомендуют провести инвентаризацию и оценку всех устройств АСУ, доступных из интернета, отключить доступ к интернету там, где в нем нет необходимости, использовать VPN с двухфакторной аутентификацией, систему предотвращения вторжений и управление уязвимостями, а также провести тестирование на проникновение.

Атаки на транспорт и логистику в Северной Америке

Неизвестный актор

Киберкриминал

Конвергенция кибер- и традиционной преступности

Целевой фишинг

Компрометация легитимных почтовых сервисов

RMM

По данным исследователей Proofpoint, неизвестные злоумышленники компрометируют компании в сфере грузоперевозок и логистики, используя инструменты удаленного мониторинга и управления, чтобы перехватить заказы на доставку груза и физически его похитить. Затем злоумышленники отправляют украденный груз за рубеж или продают его онлайн, предположительно, взаимодействуя с организованными преступными группами. Как минимум с июня 2025 года злоумышленники использовали три тактики для внедрения RMM-инструментов в эти компании. В рамках первой тактики злоумышленники компрометируют учетную запись на бирже грузоперевозок, где транспортные компании бронируют заказы на доставку грузов. Они размещают на бирже поддельный заказ и отправляют откликнувшимся перевозчикам фишинговые ссылки. Как только жертва попадается, злоумышленники устанавливают средства удаленного доступа, после чего от его именит делают ставку на реальный заказ на доставку, используя скомпрометированную учетную запись перевозчика, а затем перехватывают груз. Вторая тактика предполагает интеграцию вредоносного контента и URL-ссылок в уже существующие переписки скомпрометированных ранее почтовых аккаунтов партнеров перевозчика (тактика BEC). В рамках третьей тактики злоумышленники целенаправленно атакуют по электронной почте крупные компании, в том числе перевозчиков с собственным автопарком, фрахтовых брокеров и поставщиков из цепочек поставок.

Злоумышленники используют различные RMM-инструменты, включая ScreenConnect, SimpleHelp, PDQ Connect, Fleetdeck, N-able и LogMeIn Resolve. Описанные в отчете кампании аналогичны активности, которую исследователи Proofpoint задокументировали в сентябре 2024 года. Однако им не удалось точно установить, проводились ли прошлые и текущие кампании одной и той же группой или несколькими группами. Несмотря на то, что кампании, которые Proofpoint рассматривает в своем отчете, касаются кражи грузов в Северной Америке, проблему стоит считать глобальной. По данным Munich RE, сегодня карта «горячих точек» краж грузов охватывает Бразилию, Мексику, Индию, США, Германию, Чили

и Южную Африку, а наиболее популярными товарами у похитителей являются продукты питания и напитки.

Предупреждение CISA о группе вымогателей Akira

Киберкриминал

Эксплуатация общедоступных приложений

Вредоносное ПО под Linux

LOTL

Шифровальщик

Агентство по кибербезопасности и защите инфраструктуры, Федеральное бюро расследований, Министерство здравоохранения и социальных служб США, Центр киберпреступлений Министерства обороны (DC3) и несколько европейских организаций по борьбе с киберпреступностью опубликовали рекомендации по кибербезопасности, в которых приводятся индикаторы компрометации и TTP группы вымогателей Akira, выявленные в результате расследований ФБР и благодаря сообщениям доверенных компаний вплоть до ноября 2025 года. В ходе инцидента в июне 2025 года злоумышленники впервые зашифровали файлы на диске виртуальной машины Nutanix AHV (тем самым более не ограничиваясь VMware ESXi и Hyper-V), использовав уязвимость SonicWall CVE-2024-40766 для получения первоначального доступа. Платформа AHV от Nutanix – это Linux-решение для виртуализации, которое запускает виртуальные машины и управляет ими в инфраструктуре Nutanix. Для проникновения в корпоративные сети аффилированные с Akira группы также часто используют украденные или подобранные путем перебора учетные данные VPN и SSH на незащищенных маршрутизаторах. Далее они эксплуатируют уязвимости CVE-2023-27532 или CVE-2024-40711 на непропатченных серверах резервного копирования и репликации Veeam, чтобы получить доступ к резервным копиям и удалить их.

Внутри сети участники Akira, как было замечено, используют такие утилиты, как nltest, AnyDesk, LogMeIn, скрипт wmiexec.py из набора Impacket, а также VB-скрипты для проведения разведки, горизонтального перемещения на другие системы и закрепления. Злоумышленники также часто удаляют защитные решения конечных узлов и создают новые учетные записи администратора для сохранения доступа. В одном инциденте они выключили виртуальную машину контроллера домена, скопировали ее VMDK-файлы, прикрепили их к новой виртуальной машине, а затем извлекли файл NTDS.dit и куст реестра SYSTEM, чтобы получить учетную запись администратора домена. В конце бюллетеня отмечается, что инструмент Megazord, который ранее связывали с операциями Akira, группа, видимо, перестала использовать еще в 2024 году.

Группа вымогателей Akira ассоциируется с такими группами, как Storm-1567, Howling Scorpius, Punk Spider и Gold Sahara, и может быть связана с ныне несуществующей группой вымогателей Conti. Akira атакует преимущественно малый и средний бизнес, однако среди ее жертв есть и

крупные организации из различных отраслей. Прослеживается фокус злоумышленников на образовательных учреждениях, критически важных производственных организациях, а также организациях из ИТ, здравоохранения, финансовой отрасли, пищевой и сельскохозяйственной промышленности.

Кампания Beamglea

Неизвестный актор

Киберкриминал

Фишинговые веб-сайты

Доверенная инфраструктура

Исследователи Socket Threat Research раскрыли 175 вредоносных npm-пакетов (более 26 000 загрузок), которые служили инфраструктурой для широкомасштабной фишинговой кампании, нацеленной на более чем 135 промышленных, технологических и энергетических компаний по всему миру. Кампания использовала публичный npm-реестр и сеть доставки контента (CDN) unpkg.com для размещения скриптов, перенаправлявших жертв на страницы сбора учетных данных, визуально похожие на бизнес-страницы или страницы входа в системы Microsoft. Злоумышленники автоматизировали свой рабочий процесс с помощью Python-скриптов, которые генерировали случайные имена пакетов, внедряли специфичные для конкретных жертв сведения и публиковали их в npm, при этом unpkg.com автоматически предоставлял каждый пакет как достоверный HTTPS-ресурс. HTML-приманки, замаскированные под заказы на закупку, спецификации проектов и технические документы, загружали эти скрипты непосредственно с unpkg.com, что позволило быстро масштабировать кампанию без затрат на хостинг или управление SSL.

Атаки с использованием пакетов NuGet

Вредоносные пакеты

Атака на цепочку поставок

DoS

Extension method hijacking

Сертификаты разработчика

Исследователи Socket Threat Research обнаружили вредоносные пакеты NuGet, загруженные в 2023 и 2024 годах, предназначенные для выполнения вредоносного кода после наступления определенных дат в 2027 и 2028 годах и способные вызвать DoS-атаку на базы данных и системы промышленной автоматизации Обнаруженный набор включает девять вредоносных пакетов NuGet, автором которых является пользователь по имени shanhai666. Это MyDbRepository, MCDbRepository, Sharp7Extend, SqlDbRepository, SqlRepository, SqlUnicornCoreTest, SqlUnicornCore, SqlUnicorn.Core и SqlLiteRepository. Пакеты были загружены в общей сложности 9488 раз. Всего злоумышленник опубликовал 12 пакетов – остальные три работают как заявлено и не имеют вредоносного функционала. Все они уже удалены из NuGet. Вредоносные пакеты поддерживают RDBMS, которые наиболее часто используются в .NET-приложениях (SQL Server, PostgreSQL, SQLite), Один из них – Sharp7Extend – нацелен на системы промышленной автоматизации.

Sharp7Extend реализует два механизма саботажа: немедленное случайное завершение родительского процесса и имитации псевдослучайного сбоя при операций записи в контроллер, которые начинаются через 30–90 минут после установки. Пакет рассчитан на пользователей легитимной библиотеки Sharp7, которая является .NET-реализацией протокола коммуникации с ПЛК Siemens S7.

Вредоносная программа использует методы расширения в C# (C# extension) для прозрачного внедрения вредоносной логики в операцию с базой данных и ПЛК. Добавление новых методов к существующим типам без изменения их исходного кода – это мощная функция C#, которую злоумышленники используют для перехвата операций.

Вредоносные пакеты добавляют метод расширения Exec() к типам кработы с базами данных и метод .BeginTran() к объектам S7Client. Каждый раз, когда приложение выполняет запрос к базе данных или операцию с ПЛК, эти методы расширения запускаются автоматически, проверяя текущую дату на соответствие установленным датам срабатывания.

В случае Sharp7Extend вредоносная логика активируется сразу после установки и остается активной до 6 июня 2028 года. После наступления этой даты механизм завершения останавливается. Восемь других пакетов, ориентированных на системы баз данных, завершат работу с вероятностью 20% уже после наступления установленной даты. Активация некоторых реализаций SQL Server, PostgreSQL и SQLite в комплекте с другими пакетами запланирована на 8 августа 2027 года и 29 ноября 2028 года. Хотя пока неизвестно, кто стоит за атакой на цепочку поставок NuGet, анализ исходного кода и имя shanhai666 позволили исследователям Socket Threat Research связать ее с китайско-зычным злоумышленником.

Атаки GTG-1002

Атака под управлением ИИ

Исследователи Anthropic подробно описали обнаружение, по их мнению, первого задокументированного случая кибершпионской кампании, практически полностью организованной и осуществленной искусственным интеллектом. Операция приписывается предположительно китайско-язычной группе GTG-1002, целью которой были около 30 крупных организаций, включая технологические корпорации, финансовые учреждения, компании-производители химической продукции и государственные ведомства во многих странах. Специалисты подчеркивают особую роль искусственного интеллекта в новой эре кибервойн, когда автономные ИИ-агенты постепенно становятся оружием в киберпространстве. В отчете утверждается, что злоумышленники

использовали Claude Code и ИИ-агентов на всех этапах атак, от разведки до кражи конфиденциальных данных. По словам исследователей, ИИ-агенты самостоятельно выполняли до 80–90% тактических операций, действуя как единая команда пентестеров с сверхчеловеческой скоростью. Первоначально злоумышленники использовали метод социальной инженерии, убедив модель Claude LLM в том, что она участвует в законном тестировании на проникновение. ИИ продемонстрировал умение самостоятельно обнаруживать уязвимости, создавать полезные нагрузки и успешно развертывать их в реальных операциях, однако одновременно появились и недостатки. Галлюцинации ИИ стали серьезным препятствием для злоумышленников, поскольку модель периодически фальсифицировала данные и преувеличивала результаты. Для расследования атаки исследователи Anthropic активно использовали собственные модели ИИ, подчеркивая двойственную роль искусственного интеллекта в кибербезопасности.

Атаки ботнета Broadside

Эксплуатация сетевых устройств

DDoS

Шпионское ПО

Исследователи Cydome сообщили об обнаружении нового варианта ботнета Mirai под названием Broadside, активно атакующего отрасль морской логистики. Этот ботнет эксплуатирует критическую уязвимость командной инъекции CVE-2024-3721 в DVR-устройствах (цифровые видеорегистраторы) TBK Vision, обычно используемых на судах. Уязвимость затрагивает как видеорегистраторы TBK, так и модели других производителей: CeNova, Night Owl и QSee. Ботнет Broadside использует кастомный протокол C2 на TCP-порту 1026 с резервным каналом связи TCP 6969, пакеты помечаются уникальной 4-байтовой сигнатурой («Магическое число»): 0x36694201. Кроме того, ботнет использует Netlink-сокеты ядра и полиморфизм вредоносной нагрузки, чтобы избежать обнаружения. Ботнет также содержит модуль Judge, Jury and Executioner – механизм самозащиты, который динамически уничтожает конкурирующее вредоносное ПО или нежелательные процессы. Он ведет списки разрешенных и запрещенных процессов в памяти, обеспечивая выполнение только контролируемых им операций. Помимо запуска распределенных атак типа «Отказ в обслуживании» (Distributed Denial of Service, DDoS) на основе UDP, Broadside похищает конфиденциальные файлы учетных данных, такие как /etc/passwd и /etc/shadow, что упрощает повышение привилегий и горизонтальное перемещение внутри скомпрометированной сети. Исследователи Cydome в течение нескольких месяцев наблюдали изменяющуюся инфраструктуру ботнета, что свидетельствует о его постоянных обновлениях. Они также подчеркнули риск для морских судов, поскольку DDoS-атаки могут нарушить работу

судовой сети и спутниковой связи и потенциально повлиять на другие критически важные системы.

Атаки GOLD SALEM

Киберкриминал

Эксплуатация общедоступных приложений

BYOVD

DLL sideloading

Облачные сервисы как C2

Шифровальщик

Исследователи Sophos Counter Threat Unit проанализировали шестимесячную активность, приписываемую киберпреступной группе GOLD SALEM, и с высокой степенью уверенности пришли к выводу, что эти операции были направлены на внедрение программы-вымогателя Warlock. Исследование 11 инцидентов в организациях из сельскохозяйственной, энергетической и автомобильной отраслей, розничной торговли, инженерного и правительственного секторов позволило определить последовательную схему действий, которая включает эксплуатацию локальных уязвимостей SharePoint (в том числе цепочку эксплойтов ToolShell), создание постоянных учетных записей администратора, кражу учетных данных из LSASS с помощью Mimikatz, а также активное использование легитимных инструментов, таких как Velociraptor, VS Code (режим туннелирования) и Cloudflared, для установки связи с командным сервером и горизонтального перемещения. Обход защитных решений основывался на технике BYOVD (Bring Your Own Vulnerable Driver) с использованием драйверов от китайских поставщиков услуг кибербезопасности для отключения AV/EDR-решений, на эпизодической подмене библиотеки DLL (техника DLL sideloading) и поэтапной доставке инструментов через домены Cloudflare Workers. Хотя основной вредоносной нагрузкой был Warlock, в некоторых случаях использовались варианты LockBit и Babuk, что свидетельствует о тактической гибкости злоумышленников, они не зацикливаются на одном семействе программ-вымогателей. Исследователи предположили, что за этой активностью стоят финансово мотивированные злоумышленники, обладающие техническими возможностями выше среднего, исповедующие оппортунистический подход при выборе жертв и постоянно совершенствующие инструментарий, а не кибершпионская группа, действующая в интересах какого-либо государства.

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