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

19.06.2025

Версия 1.0

Этот обзор представляет собой сводку публикаций об APT- и финансовых атаках на промышленные предприятия, информация о которых была раскрыта в первом квартале 2025 года, а также о связанной с ними активности групп, замеченных в атаках на промышленные организации и объекты критической инфраструктуры. 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.

Общие сведения

Хотя результатов исследований атак на промышленные предприятия в первом квартале 2025 года было опубликовано заметно меньше, чем в предыдущий период, среди них немало заслуживающих особого внимания – хотя бы для того, чтобы задаться лишний раз вопросом: «А наша организация от этого защищена надежно?»

Так, например, для организаций в Корее по-прежнему высок риск атак на цепочки поставок, в которых задействованы продукты местной разработки. В этот раз мишенью атаки стал местный разработчик VPN-решения. Пострадала по меньшей мере одна промышленная компания — производитель полупроводниковой продукции.

В двух кампаниях злоумышленники эксплуатировали уязвимости нулевого дня в ходе атак на промышленные организации. Уязвимость в 7-Zip, использовалась в атаках на украинские компании. Вторая история рассказывает об использовании zero-click эксплойта в Microsoft Windows. Она особенно интересна тем, что разработчик отказался устранить уязвимость, несмотря на то, что ее эксплуатация была отмечена в нескольких вредоносных кампаниях, самые ранние из которых отнесены аж к 2017 году.

Техника использования полиглот-файлов, составленных из данных различных форматов таким образом, что их могут интерпретировать различные легитимные приложения, неожиданно стала популярной среди злоумышленников. Исследователи из Proofpoint сообщили об одной такой кампании с использованием полиглот-файлов PDF/HTA и PDF/ZIP, а эксперты «Лаборатории Касперского» — о другой, с применением полиглот-файла PE/ZIP.

Описанные в одной из публикаций изощренные приемы кражи аутентификационных данных для использования на этапах развития атаки

лишний раз демонстрируют, как важно промышленным предприятиям постоянно проверять периметр на предмет признаков возможной компрометации — например, чтобы убедиться, что на страницах входа в систему не внедрено вредоносных имплантов, и контроль над зоной DNS не утерян.

Юго-Восточная Азия и Корейский полуостров

Кампания SalmonSlalom

Исследователи Kaspersky ICS CERT сообщили о кампании SalmonSlalom, нацеленной на организации в Азиатско-Тихоокеанском регионе. Атаки осуществлялись с помощью фишинговых писем, содержащих FatalRAT — многофункциональную троянскую программу, способную записывать нажатия клавиш, манипулировать памятью, просматривать данные браузера, загружать дополнительное ПО (например, AnyDesk и UltraViewer), выполнять операции с файлами, запускать прокси-сервер, сканировать сети и завершать процессы. Кампания была нацелена прежде всего на государственные и промышленные организации, в особенности на предприятия в секторах производства, строительства, информационных технологий, телекоммуникаций, здравоохранения, энергетики, а также логистики и транспорта на Тайване, в Малайзии, Китае, Японии, Таиланде, Южной Корее, Сингапуре, на Филиппинах, во Вьетнаме и Гонконге. Судя по приманкам, используемым в письмах, кампания была ориентирована на китайскоязычных пользователей.

Злоумышленники применили сложную многоступенчатую схему доставки вредоносной нагрузки, чтобы обойти средства обнаружения, в том числе, широко используя легитимные китайские сервисы — сеть доставки контента (CDN) myqcloud и облачный сервис для создания заметок Youdao Cloud Notes. Начальная точка последней зафиксированной цепочки заражения — фишинговое письмо с ZIP-архивом, имеющим имя файла на китайском языке. При открытии архива запускается загрузчик первого этапа, который отправляет запрос к Youdao Cloud Notes для получения конфигуратора FatalRAT и загрузчика DLL второго этапа. Конфигуратор представляет собой DLL-библиотеку, которая загружает содержимое еще одной заметки с note.youdao[.]com, получает конфигурационные данные и открывает файл-приманку. Загрузчик DLL второго этапа отвечает за загрузку основной вредоносной нагрузки FatalRAT с сервера (myqcloud[.]com), указанного в файле конфигурации, и ее установку с одновременным отображением фальшивого сообщения об ошибке запуска приложения.

Важная особенность кампании — применение техники подмены загружаемой DLL (DLL sideloading) в многоэтапном процессе заражения и доставки вредоносного ПО FatalRAT. FatalRAT выполняет 17 проверок, чтобы определить, не запущена ли вредоносная программа на виртуальной машине или в песочнице. При анализе кода вредоносных компонентов исследователи выявили сходство с методами, использовавшимися ранее в кампаниях с применением Gh0st RAT, SimayRAT, Zegost и FatalRAT. У исследователей пока нет общего мнения о том, кто стоит за атаками с использованием FatalRAT.

Атаки с использованием VIP Keylogger

В четвертом квартале 2024 года исследователи HP Wolf Security обнаружили кампанию по распространению вредоносного ПО VIP Keylogger, нацеленную на инжиниринговые компании в Азиатско-Тихоокеанском регионе. Злоумышленники рассылали вредоносные PDF-файлы по электронной почте под видом запросов на коммерческое предложение, адаптируя содержание писем под организации – потенциальные жертвы с учетом продаваемой ими продукции, например, автозапчастей и промышленных компонентов. При открытии PDF-файла пользователь видит размытое изображение документа с двумя сообщениями. Первое - о наличии обновления для программы просмотра PDF. Во втором говорится, что документ сжат, и для загрузки и просмотра его полной версии необходимо кликнуть мышью по изображению. После перехода по ссылке начинается загрузка ZIP-архива. При открытии архива пользователь получает файл с образом диска (IMG). При его запуске Windows монтирует образ диска и отображает его содержимое в новом окне Проводника. Внутри находится всего один файл — исполняемый файл, замаскированный путем изменения иконки под документ PDF. При запуске исполняемого файла начинается финальный этап заражения, в ходе которого устанавливается вредоносная нагрузка — VIP Keylogger, функционально схожий с Snake/404 Keylogger.

Атаки SideWinder

В 2024 году исследователи «Лаборатории Касперского» опубликовали статью о группе SideWinder. В ней описан новейший инструментарий группы, а также ранее неизвестный модульный инструмент шпионажа под названием StealerBot. После публикации исследователи зафиксировали бурную активность актора по обновлению арсенала и созданию масштабной инфраструктуры управления скомпрометированными системами. Целевые отрасли остались прежними. При этом отмечено резкое увеличение числа

атак на морскую инфраструктуру и логистические компании. В первой половине 2024 года наблюдалось большое количество атак на указанные отрасли, особенно в Джибути. Позднее злоумышленники расширили географию атак, охватив морскую инфраструктуру от Юго-Восточной Азии до Средиземного моря. Также продолжились атаки на государственные, военные и дипломатические организации. Кроме того, были зафиксированы атаки, указывающие на особый интерес к атомным электростанциям и ядерной энергетике с использованием документов, видимо, предназначенных для сотрудников, работающих в данной отрасли.

Атаки Squid Werewolf/APT37

Исследователи BI.ZONE выявили фишинговую кампанию, организованную группой Squid Werewolf (также известной как APT37, Ricochet Chollima, ScarCruft или Reaper Group). Атака начиналась с фишингового письма на русском языке, замаскированного под предложение о работе от имени HR-специалиста компании «Объединенный промышленный комплекс».
Во вложении находился защищенный паролем ZIP-архив. Он содержал LNK-файл, который при открытии запускал команду на выполнение исполняемого файла (EXE). Далее происходил запуск DLL-библиотеки — обфусцированного загрузчика, написанного на языке C#. Загрузчик отключал автозапуск из папки автозапуска путем изменения параметров ключа реестра, а затем загружал, расшифровывал и запускал вредоносную нагрузку в памяти. На момент исследования вредоносная нагрузка была недоступна. Обнаруженная BI.ZONE Threat Intelligence атака похожа на атаку, описанную экспертами Securonix, которые связывают ее с группой APT37. Ранее злоумышленники применяли похожую библиотеку на C#, но вредоносная нагрузка расшифровывалась с использованием алгоритма сдвига (шифр Цезаря) и представляла собой обфусцированный код на JavaScript. Эта вредоносная нагрузка была еще одним загрузчиком, который отправлял на сервер имя компьютера жертвы и загружал код следующего этапа — написанный на PowerShell троян VeilShell.

Активность китайскоязычных групп

Атаки PlushDaemon

Исследователи ESET сообщили об активности китайскоговорящей APT-группы PlushDaemon, действующей как минимум с 2019 года. Группа причастна к атаке на цепочку поставок, нацеленной на южнокорейского провайдера VPN-сервиса IPany. Программное обеспечение с внедренным в

него троянской функциональностью было обнаружено на официальном сайте провайдера. При этом не применялась селективная доставка — любой запрос на загрузку приводил к получению зараженного инсталлятора. Так, по данным телеметрии ESET, зараженный инсталлятор пытались запустить пользователи из сетей южнокорейского производителя полупроводниковой продукции и неназванной компании – разработчика программного обеспечения. Первые известные жертвы были зафиксированы в Японии и Китае, соответственно, в ноябре и декабре 2023 года.

Основным инструментом группы PlushDaemon является многофункциональный бэкдор SlowStepper, содержащий 30 модулей, написанных на C++, Python и Go. Разработка SlowStepper началась в январе 2019 года, а последняя на момент анализа версия была собрана в июне 2024 года. Инструменты SlowStepper в числе прочих возможностей по сбору данных позволяют записывать аудио и видео с целью шпионажа. Они хранятся в удаленном репозитории исходного кода на китайской платформе GitCode. Также разработчики реализовали в SlowStepper собственную командную оболочку, интегрированную в протокол связи. Кроме того, исследователи ESET зафиксировали случаи проникновения группы с использованием уязвимостей в легитимных веб-серверах.

Атаки J-magic

Исследователи Black Lotus Labs (Lumen Technologies) сообщили о вредоносной кампании, нацеленной на маршрутизаторы и VPN-шлюзы Juniper. В ходе кампании применялось вредоносное ПО под названием J-magic, специально разработанное для операционной системы Junos OS. Название связано с тем, что бэкдор осуществляет постоянный мониторинг TCP-трафика в ожидании «волшебного» пакета, после чего запускает обратную оболочку. J-magic — это модифицированная версия общедоступного бэкдора cd00r – экспериментального прототипа, скрытно осуществляющего пассивный мониторинг сетевого трафика до момента обнаружения «волшебного» пакета и после этого открывающего канал связи со злоумышленником. Вредоносное ПО создает eBPF-фильтр на указанном интерфейсе и порте, информация о которых передается в аргументах командной строки при запуске.

Атаки J-magic были нацелены на организации в следующих отраслях: полупроводниковой, энергетической, промышленного производства, тяжелого машиностроения, строительства, биоинженерии и информационных технологий. По данным Black Lotus Labs, кампания была активна с середины 2023 года по середину 2024 года и отличалась низким уровнем обнаружения и ориентированностью на долговременный доступ.

Исходя из данных телеметрии, исследователи считают, что примерно половина зараженных устройств использовалась в качестве VPN-шлюзов. Отмечается техническое сходство J-magic с вредоносным ПО SeaSpy, также основанным на бэкдоре cd00r. Однако ряд различий затрудняет установление четкой связи между кампаниями. В целом, исследователи не уверены в связи J-magic и SeaSpy. Вредоносное ПО SeaSpy в 2022–2023 годах применялось для атак на шлюзы Barracuda Email Security Gateway с использованием уязвимости нулевого дня CVE-2023-2868.

Атаки Shadowpad

Исследователи Trend Micro обнаружили, что Shadowpad — семейство вредоносного ПО, связанное с несколькими китайскоязычными группами, — используется для распространения ранее неизвестного семейства программ-вымогателей. Злоумышленники распространяют вредоносное ПО, эксплуатируя слабые пароли и обходя механизмы многофакторной аутентификации. По данным исследователей, от этой активности пострадала как минимум 21 компания из девяти отраслей в 15 странах Европы, Ближнего Востока, Азии и Южной Америки. Чаще всего злоумышленники атаковали компании из производственного сектора, но были затронуты транспорт, издательства, энергетика, фармацевтика, банки, горнодобывающая промышленность, образование и индустрия развлечений. В атаке для запуска вредоносной нагрузки применялась техника подмены загружаемой DLL (DLL side-loading). В двух случаях Shadowpad запускал утилиту CQHashDumpv2.exe, входящую в набор инструментов для тестирования на проникновение CQTools, позволяющую выгружать хэши из системы и менять пароли пользователей. Среди других инструментов постэксплуатации — Impacket и неназванный инструмент (предположительно NTDSUtil), использованный для получения дампа базы данных Active Directory. Исследователи не нашли достаточных доказательств связи этой активности с известными кампаниями или группами. Однако были обнаружены два индикатора, указывающие с низкой степенью уверенности на возможную связь с группой Teleboyi.

Атаки Winnti

Центр реагирования на инциденты LAC сообщил о новой кампании группы Winnti, получившей название RevivalStone. В марте 2024 года были атакованы японские организации из производственного, сырьевого и энергетического секторов с применением вредоносного ПО Winnti с расширенными возможностями и усовершенствованными методами ухода от обнаружения. В ходе первоначального проникновения злоумышленники

использовали уязвимость типа SQL-инъекция в ERP-системе, работающей на веб-сервере компании-жертвы, чтобы установить веб-шелл. С помощью веб-шелла злоумышленники проводили разведку и собирали учетные данные для развития атаки в сети компании-жертвы, а также устанавливали на сервере вредоносное ПО Winnti, чтобы обеспечить себе плацдарм для проведения последующих атак. Для защиты вредоносной нагрузки и каналов связи вредоносное ПО Winnti использует алгоритмы шифрования AES и ChaCha20. Ключи расшифровки формируются на основе уникальных идентификаторов, таких как IP- и MAC-адреса, что затрудняет анализ. Также вредоносная программа устанавливает руткит режима ядра, чтобы скрыть свою активность. Для обхода систем обнаружения и реагирования на конечных точках (EDR) применяется обфускация кода и техника подмены DLL (DLL hijacking).

Атаки Lotus Blossom

Исследователи Cisco Talos сообщили о новых кампаниях китайскоязычной APT-группы Lotus Blossom (известной также как Spring Dragon, Billbug и Thrip), нацеленных на государственные учреждения, организации в производственном и телекоммуникационном секторах и СМИ на Филиппинах, во Вьетнаме, в Гонконге и на Тайване. Атаки проводились с использованием обновленных версий бэкдора Sagerunex. Группа Lotus Blossom известна с 2009 года, а бэкдор Sagerunex применяется как минимум с 2016 года. Предполагается, что он является обновленной версией известного ранее вредоносного ПО Billbug (Evora).

Вектор первоначального проникновения, использованный в последней серии атак, не установлен. Особенностью наблюдаемой активности является применение двух новых вариантов вредоносного ПО, использующих такие облачные сервисы как Dropbox, Twitter и Zimbra в качестве командных серверов. Варианты, использующие Dropbox и Twitter/X, применялись в 2018–2022 годах, а версия, использующая Zimbra, известна с 2019 года. Последняя не только собирает информацию о жертве и отправляет ее на почтовый ящик в Zimbra, но и позволяет злоумышленнику отправлять на зараженную машину команды и управлять ей через содержимое почтового ящика. Если в ящике содержится сообщение с корректными командами, вредоносная программа загружает его и извлекает из него команды. В противном случае сообщение удаляется, и программа ожидает нового письма. Результаты выполнения команд упаковываются в архив RAR, а он прикрепляется к черновику письма, который помещается в корзину почтового ящика. Каждая из версий Sagerunex использует механизмы закрепления в системе, основанные на различных проверках, включая

задержки выполнения и системные проверки. Также в ходе атак применяются дополнительные инструменты: утилита для кражи учетных данных из браузера Chrome, прокси-утилита Venom с открытым исходным кодом, программа для настройки привилегий, кастомное ПО для сжатия и шифрования собранных данных и модифицированный инструмент для ретрансляции соединений mtrain V1.01. Известно также, что злоумышленники запускали такие команды как net, tasklist, ipconfig и netstat для проведения разведки окружения на целевых системах, а также проверяли доступность интернета. Если доступ в интернет был ограничен, применялся один из двух подходов: использовались настройки прокси-жертвы для установки соединения или с помощью утилиты Venom устанавливалось соединение изолированных машин с системами, имеющими выход в интернет.

Атаки Earth Alux

Исследователи Trend Micro обнаружили ранее неизвестную китайскоязычную группировку Earth Alux, нацеленную на государственные учреждения и организации в ИТ-, технологическом, логистическом, производственном, телекоммуникационном секторах, а также розничной торговле в странах Азиатско-Тихоокеанского региона и Латинской Америки. Впервые активность группы была зафиксирована в Азии во втором квартале 2023 года, а в Латинской Америке — в середине 2024 года. Основными целями стали организации из Таиланда, Филиппин, Малайзии, Тайваня и Бразилии. Цепочки заражения начинались с эксплуатации уязвимых сервисов, доступных через интернет. Через эти сервисы внедрялся веб-шелл Godzilla, с помощью которого разворачивались дополнительные вредоносные компоненты, включая бэкдоры VARGEIT и COBEACON (вариант Cobalt Strike Beacon).

VARGEIT загружает инструменты непосредственно со своего командного сервера (C2) во вновь созданный процесс Microsoft Paint (mspaint.exe) для проведения разведки, сбора и вывода данных. Earth Alux также использует VARGEIT как основной способ управления дополнительными инструментами для различных целей, включая развитие атаки. Кроме того, VARGEIT может применяться как бэкдор первого, второго и последующих этапов атаки, а COBEACON — только как бэкдор первого этапа. COBEACON загружается в виде зашифрованной вредоносной нагрузки, извлекаемой из DLL MASQLOADER, которая устанавливается методом подмены загружаемой DLL (DLL sideloading), либо как shell-код через утилиту командной строки RSBINJECT, написанную на Rust. При запуске VARGEIT устанавливаются дополнительные инструменты, включая компонент загрузчика RAILLOAD, который запускается через DLL sideloading и используется для запуска

зашифрованной вредоносной нагрузки из другой папки. Второй компонент — RAILSETTER — изменяет метки времени, связанные с артефактами RAILLOAD на зараженном хосте, и создает задачу запуска RAILLOAD в планировщике задач. Уникальная особенность VARGEIT — поддержка 10 различных каналов связи с командным сервером по HTTP, TCP, UDP, ICMP, DNS и через Microsoft Outlook. В последнем случае используется Graph API для обмена командами в заранее определенном формате через папку черновиков почтового ящика, управляемого злоумышленниками.

Группа Earth Alux выполняет различные проверки с помощью RAILLOAD и RAILSETTER, в том числе попытки обнаружения и поиска новых хостов для DLL-сайдлоадинга. Также группа использует утилиту ZeroEye — инструмент с открытым исходным кодом, сканирующий таблицы импорта EXE-файлов на наличие DLL, которые можно применять для сайдлоадинга. Кроме того, в арсенале группы есть VirTest — еще один широко используемый в китайскоязычном сообществе инструмент для проведения проверок.

Активность русскоязычных групп и атаки, нацеленные на российские организации

Атаки Sticky Werewolf

В январе исследователи компании F6 опубликовали статью об активности группы Sticky Werewolf, атаковавшей российские научно-производственные предприятия. Злоумышленники рассылали вредоносные письма с инструкциями по размещению заказов предприятий оборонной промышленности в исправительных учреждениях с привлечением заключенных. Письма содержали два вложения: документ-приманку в виде сопроводительного письма от имени Минпромторга и запароленный вредоносный RAR-архив (Форма заполнения.rar). В архиве находились документ Список рассылки.docx и вредоносный исполняемый файл Форма заполнения.pdf.exe, который после запуска в конечном итоге устанавливал троянскую программу удаленного доступа Ozone RAT. В ходе дальнейшего исследования было обнаружено аналогичное фишинговое письмо от 23 декабря 2024 года, содержащее два поддельных документа. Целью атаки также стало научно-производственное предприятие, однако архив с полезной нагрузкой в том письме отсутствовал.

В марте исследователи компании F6 сообщили о новых атаках, на этот раз на производителя нефтегазового оборудования. В обнаруженной рассылке содержался запароленный архив формата 7z. Группа Sticky Werewolf

использовала поддельный документ от Минпромторга. В результате применения классической для группы цепочки атаки, включающей дроппер NSIS, BAT-файл и скрипт AutoIt, создавался процесс RegAsm.exe, в который внедрялся троянец удаленного доступа QuasarRAT. Один из доменов инфраструктуры командных серверов (crostech[.]ru) используется группой с октября 2024 года. Второй домен (thelightpower[.]info) был зарегистрирован в декабре, а первые известные атаки с его применением произошли в марте текущего года.

Атаки Rezet/Rare Wolf

Исследователи компании F6 сообщили об атаках кибершпионской группы Rezet (она же Rare Wolf), действующей с октября 2018 года и причастной более чем к 500 атакам на промышленные предприятия России, Беларуси и Украины. В январе 2025 года были зафиксированы вредоносные рассылки якобы от имени компании, специализирующейся на сопровождении контрактов с предприятиями – исполнителями гособоронзаказа. Письма выглядели как приглашения на семинары по стандартизации оборонной продукции и были адресованы руководителям и специалистам. Мишенями атаки стали предприятия химической, пищевой и фармацевтической промышленности России. Первая рассылка содержала вредоносный файл в запароленном RAR-архиве, включающем файл-приманку в формате PDF и вредоносную нагрузку. При запуске для отвлечения внимания открывался документ-приманка, а в фоне происходило заражение системы. Во второй и третьей рассылках, отправленных несколько дней спустя, содержался архив с двумя вредоносными файлами — PDF-документом и вредоносной нагрузкой. Открытие любого из файлов приводило к заражению системы. Исследователи не уточнили, какая именно нагрузка была применена.

Атаки на украинские организации с использованием уязвимости CVE-2025-0411

Согласно отчету Trend Micro, в ходе кампании кибершпионажа против украинских организаций была использована уязвимость нулевого дня в 7-Zip (CVE-2025-0411), с помощью которой злоумышленники устанавливали вредоносное ПО SmokeLoader на компьютерах жертв. Эксплуатация уязвимости была обнаружена в сентябре 2024 года, а патч вышел 30 ноября того же года. Уязвимость позволяет обойти защиту Windows Mark-of-the-Web с помощью двойного архивирования файлов, таким образом избегая основных проверок безопасности и выполняя вредоносный код. Русскоязычные киберпреступные группы активно эксплуатировали уязвимость в ходе целенаправленных фишинговых кампаний с

использованием взломанных почтовых аккаунтов и поддельных расширений файлов документов, чтобы обманным путем заставить пользователей и операционную систему Windows выполнять вредоносные файлы. Согласно опубликованным исследователями данным, жертвами или целями атак могли стать государственные учреждения Украины и другие организации, включая министерство, производителя автомобилей, автобусов и грузовиков, предприятие общественного транспорта, производителя бытовой и электронной техники, администрацию региона, страховую компанию, региональную аптечную сеть, предприятие водоснабжения и городской совет.

Атаки Mythic Likho

Исследователи «Лаборатории Касперского» сообщили об атаках группы Mythic Likho на российские компании. Исследование началось в январе с анализа письма, отправленного в отдел кадров машиностроительного завода. Автор письма, якобы представляющий отдел кадров другой компании, просил предоставить характеристику на бывшего сотрудника. Mythic Likho — это либо новая группа, либо известная группа, значительно усовершенствовавшая свои тактики, техники и процедуры.

Вложение фишингового письма представляло собой архив с несколькими файлами, включая безопасный документ-приманку и LNK-файл, ведущий к заражению. В результате заражения на систему устанавливался агент Merlin — инструмент постэксплуатации с открытым исходным кодом, совместимый с фреймворком Mythic и написанный на языке Go. Merlin поддерживает взаимодействие с сервером по протоколам HTTP/1.1, HTTP/2 и HTTP/3 (комбинации HTTP/2 с протоколом QUIC). Помимо совместимости с фреймворком Mythic исследователи выявили связь между Merlin и атаками с использованием бэкдора Loki. Например, один из экземпляров Merlin с командным сервером mail.gkrzn[.]ru загружал на систему жертвы новую версию Loki 2.0 с командным сервером pop3.gkrzn[.]ru. Как и первая версия бэкдора, Loki 2.0 отправляет на сервер данные о системе и сборке, но набор данных несколько расширен. Кроме того, вероятно чтобы затруднить определение семейства вредоносного ПО, разработчики изменили способ отправки данных с POST на GET. Как и в случае с Loki, атаки с использованием бэкдора Merlin затронули более десятка российских компаний из разных отраслей, включая поставщиков телекоммуникационного оборудования и промышленные предприятия.

Атаки ReaverBits

Исследователи компании F6 опубликовали статью о новой активности группы ReaverBits, действующей с конца 2023 года и специализирующейся на атаках на российские компании в секторах биотехнологий, розничной торговли, агропромышленного комплекса, телекоммуникаций и финансов. С сентября 2024 по январь 2025 года были выявлены три различных цепочки заражения с использованием обновленных инструментов — общедоступного Meduza Stealer и нового вредоносного ПО ReaverDoor. В сентябре 2024 года были обнаружены фишинговые рассылки якобы от Следственного комитета Российской Федерации. В письмах содержалось вредоносное PDF-вложение. При открытии жертве показывалось уведомление о необходимости обновления пакета шрифтов Adobe с ссылкой на загрузку. По ссылке загружался исполняемый файл с именем, имитирующим имя легитимного установщика Adobe Font Package. Исполняемый файл представлял собой загрузчик, написанный с использованием кода из проекта adbGUI, который скачивал и запускал вредоносное ПО следующего этапа — Meduza Stealer.

В январе была обнаружена рассылка еще и от имени МВД России. Письмо содержало ссылку якобы на скачивание документа. При обращении по ссылке сервер проверял языковые настройки браузера жертвы. Загруженный исполняемый файл был основан на .NET и представлял собой загрузчик, аналогичный использованным в предыдущих рассылках. Файл основан на легитимной утилите NBTExplorer с открытым исходным кодом, но в него добавлен вредоносный код. Вредоносной нагрузкой последнего этапа также был Meduza Stealer.

Кроме того, исследователям удалось обнаружить на VirusTotal ранее неизвестный бэкдор ReaverDoor, связанный с IP-адресом, принадлежащим ReaverBits. ReaverDoor основан на легитимном проекте с открытым исходным кодом Optimizer и содержит вредоносный код, загружающий .NET-библиотеку. Для скрытного выполнения вредоносного кода используются различные техники, включая Process Hollowing и сложные схемы шифрования, такие как сочетание алгоритмов AES-256, PBKDF2, XOR и Base64.

Группа Telemancon

Исследователи компании F6 обнаружили ранее неизвестную прогосударственную группу, получившую название Telemancon. По результатам анализа инфраструктуры группы установлено, что ее активность началась в феврале 2023 года. Судя по содержанию фишинговых

документов, мишенями атак были российские производственные предприятия, в частности, из машиностроительной отрасли. Группа использует собственный дроппер, получивший название TMCDropper, и PowerShell-бэкдор TMCShell. Для группы характерны нетривиальные методы сокрытия адресов ее командных серверов (C2) с помощью легитимного сервиса telegra.ph. При изучении одного из образцов TMCShell исследователи определили, что он выполняет на машине жертвы команды, полученные с командного сервера: net.exe user; net.exe user {username}; whoami.exe; whoami.exe /groups /fo csv; ipconfig.exe /all; ARP.EXE -a.

По данным компании Securonix, такой способ хранения адресов командных серверов ранее использовался группой Shuckworm (также известной как Gamaredon), но в более простой форме, без генерации URL-пути и проверки подписи. В целом, специалисты F6 допускают, что за активностью Telemancon может стоять группа Core Werewolf. Однако доказательств, позволяющих утверждать это, на данный момент недостаточно. Группа Core Werewolf также известна как PseudoGamaredon, потому что она часто копирует тактики, техники и процедуры группы Gamaredon.

Атаки Head Mare

В сентябре 2024 года исследователи «Лаборатории Касперского» расследовали несколько инцидентов, в которых были обнаружены индикаторы компрометации и тактики, техники и процедуры, связанные с хактивистской группой Head Mare. В новых атаках злоумышленники использовали хорошо известные инструменты, ранее отмеченные в других инцидентах, связанных с Head Mare, такие как mimikatz, ngrok, LockBit 3.0, Babuk и т. д., а также новые утилиты на PowerShell. В ходе исследования было обнаружено, что группа использует такие инструменты как бэкдор CobInt, ранее применявшийся другой хактивистской группой — Twelve (известной также как Shadows, Comet и Darkstar). Кроме того, были обнаружены командные серверы (C2), которые до расследования данных инцидентов связывались только с группой Twelve. Это может указывать на связь между группами Head Mare и Twelve. Ранее обе группы атаковали российские государственные учреждения и организации в секторах производства и энергетики.

Исследователи «Лаборатории Касперского» обнаружили новую волну целевых атак Head Mare на российские промышленные предприятия с использованием нового бэкдора PhantomPyramid, написанного на Python. По данным телеметрии «Лаборатории Касперского», в марте 2025 года более 800 сотрудников из почти ста организаций получили рассылку с ранее неизвестным вредоносным ПО. В цепочке заражения использовались

фишинговые письма от имени одного из министерств с вложением в формате .ZIP. От получателя требовалось подтвердить получение информации и ознакомиться с документом, содержащимся в архиве. При открытии архива отображался документ-приманка с запросом на ремонт оборудования. Злоумышленники использовали запароленный .ZIP -архив, который с помощью техники polyglot был присоединен к вредоносному исполняемому файлу. Исполняемая часть polyglot-файла содержала ранее неизвестный бэкдор PhantomPyramid. Один из загружаемых компонентов — программа удаленного управления устройствами MeshAgent с открытым исходным кодом (из состава решения MeshCentral). Архивная часть содержала замаскированный (с помощью Проводника Windows) под PDF-документ LNK-файл с PowerShell-скриптом, открывающим документ-приманку (он извлекал, сохранял на диск и открывал приманку) и запускающим в фоне исполняемый файл бэкдора.

Атаки Seashell Blizzard/Sandworm

Компания Microsoft опубликовала исследование кампании BadPilot — многолетней глобальной кибершпионской операции, проводимой подгруппой группы Seashell Blizzard (также известной как APT44, BlackEnergy, PHANTOM, UAC-0133, Blue Echidna и Sandworm). Мишенями атаки стали государственные учреждения, организации в энергетической, нефтегазовой, судоходной и телекоммуникационной отраслях, а также в производственном секторе. Цель — получить несанкционированный доступ к конфиденциальным системам и данным. Кампания строится на активности 2021–2023 годов, которая была нацелена преимущественно на Украину, Европу и отдельные сектора в Центральной и Южной Азии и на Ближнем Востоке. С начала 2024 года география атак расширилась и включила атаки с использованием уязвимостей на цели в США и Великобритании. Для первоначального доступа эксплуатировались не менее восьми уязвимостей: в ConnectWise ScreenConnect (CVE-2024-1709), защитном решении Fortinet FortiClient EMS (CVE-2023-48788), Microsoft Exchange (CVE-2021-34473), Zimbra Collaboration (CVE-2022-41352), Openfire (CVE-2023-32315), JetBrains TeamCity (CVE-2023-42793), Microsoft Outlook (CVE-2023-23397), JBOSS (неизвестный CVE).

С конца 2021 года Seashell Blizzard использует для закрепления в скомпрометированных системах в основном веб-оболочки. С начала 2024 года для закрепления в системе и в качестве командной инфраструктуры (C2) применяется ПО удаленного управления (RMM), такое как Atera Agent и Splashtop Remote Services. В ряде случаев Seashell Blizzard разворачивала OpenSSH с уникальным публичным ключом, обеспечивая доступ к

скомпрометированным системам через учетные данные злоумышленников. В качестве C2 применялся также метод ShadowLink, позволяющий упростить постоянный удаленный доступ к скомпрометированной системе, сконфигурировав ее как скрытую службу Tor. При выявлении целей, потенциально имеющих стратегическую ценность, Seashell Blizzard зачастую проникала глубже в сеть жертвы с помощью средств туннелирования, таких как Chisel, Plink и Rsockstun, обеспечивая себя выделенными каналами доступа в соответствующие сегменты сети. Исследователи Microsoft также выявили вредоносные вставки на JavaScript на страницах входа организаций-жертв, включая Outlook Web Access (OWA), для кражи учетных данных. Они полагают с некоторой уверенностью, что злоумышленникам удавалось изменять настройки записей DNS типа A части жертв, вероятно, также для кражи учетных данных. По мнению исследователей, эти методы позволили злоумышленникам получить учетные данные для развития атаки внутри сетей нескольких организаций.

Атаки с использованием GoGo Exfiltration

В конце августа 2024 года неизвестный злоумышленник провел целевую атаку на производственное предприятие в России, которую обнаружили Глобального центра исследований и анализа угроз (GReAT) эксперты «Лаборатории Касперского». Расследование началось с анализа ранее неизвестной DLL-библиотеки, обнаруженной в памяти процесса svchost и имевшей крайне подозрительное имя — exfiltration.dll. В ходе атаки, предположительно, была использована уязвимость первого дня в Microsoft Outlook, а также зарегистрирован домен, имитирующий доменное имя жертвы. В рамках кампании применялся написанный на языке Go постоянно модифицируемый модуль для вывода собранных данных, в честь которого вредоносная программа получила свое название. Некоторые артефакты указывают на возможность наличия других, пока не обнаруженных вредоносных компонентов, таких как троянец удаленного доступа (RAT) или бэкдор.

Атаки NGC4020

Исследователи компании Solar опубликовали отчет о новой APT-атаке под названием NGC4020, которую они выявили в ходе расследования инцидента, затронувшего промышленную организацию. При изучении атакованных систем специалисты установили, что злоумышленники использовали уязвимость (CVE-2019-3980) в DameWare Mini Remote Control для загрузки вредоносного ПО. Эта уязвимость позволяла загружать собственный вредоносный драйвер в пространство ядра от имени учетной записи

LocalSystem, используя также уязвимость CVE-2023-36802. Драйвер предназначен для обхода защитных механизмов и отключения компонентов самозащиты антивирусного программного обеспечения. Помимо этого, были обнаружены написанный на языке Java вредоносный компонент Reverse Shell, утилиты для проведения разведки в системе и троянец удаленного доступа QuasarRAT. Злоумышленники допустили ошибку при создании задачи для закрепления QuasarRAT в системе, что не позволило им развить атаку. Анализ параметров созданной задачи показал, что она должна была запускаться от имени системной учетной записи домена, однако было ошибочно указано условие «Run only when user is logged on» (Выполнять только если пользователь вошел в систему). Для выполнения задач с правами системы требуется иной параметр.

Активность, связанная с Ближним Востоком

Атаки Desert Dexter

Исследователи из компании Positive Technologies сообщили об обнаружении нового актора, получившего имя Desert Dexter, который с сентября 2024 года атакует пользователей на Ближнем Востоке и в Северной Африке с помощью модифицированной версии вредоносного ПО AsyncRAT. Похожая кампания была описана специалистами компании Check Point в 2019 году, однако с тех пор некоторые элементы цепочки атаки эволюционировали. Активность, приписываемая Desert Dexter, впервые была обнаружена в феврале 2025 года. По оценке экспертов Positive Technologies, жертвами кампании стали около 900 пользователей. Большинство пострадавших находились в Ливии, Саудовской Аравии, Египте, Турции, ОАЭ, Катаре и Тунисе. В основном это обычные пользователи, включая сотрудников предприятий в сфере добычи нефти, строительства, информационных технологий и сельского хозяйства.

Злоумышленники создавали поддельные новостные группы в Facebook*, имитируя такие ресурсы, как Libya Press, Sky News, Almasar TV, The Libya Observer, The Times of Israel, для распространения вредоносного ПО и публикации сообщений с рекламой и ссылками, ведущими на файлообменный сервис Files.fm или Telegram-канал. Цепочка атаки начиналась с RAR-архива, содержащего пакетный скрипт или файл JavaScript, запускающие PowerShell-скрипт. Уже на втором этапе атаки этот скрипт обеспечивал закрепление в системе, собирал информацию о ней и передавал ее в Telegram-бот, делал снимок экрана и затем запускал в

* Принадлежит Meta, признанной экстремистской организацией и запрещенной в России.

качестве вредоносной нагрузки AsyncRAT путем внедрения в процесс aspnet_compiler.exe. В сообщениях, отправляемых в Telegram-бот, были обнаружены скриншоты рабочего стола атакующего (название системы — DEXTERMSI), а также ссылка на Telegram-канал под названием Dexterlyly. Подстрока "ly" в названии, по мнению исследователей, может указывать на ливийское происхождение владельца канала. Это подтверждается как геолокацией, содержащейся в отправлявшихся вредоносным ПО данных, так и арабскими комментариями в PowerShell-скрипте.

Атаки UNK_CraftyCamel

Исследователи из компании Proofpoint обнаружили целенаправленную фишинговую кампанию, организованную ранее неизвестной группой злоумышленников, получившей обозначение UNK_CraftyCamel. Кампания нацелена на организации в ОАЭ, прежде всего на предприятия, связанные с авиацией, спутниковой связью и критической транспортной инфраструктурой. В ходе анализа этой активности был обнаружен новый бэкдор на языке Go, получивший название Sosano. Он использует для обфускации вредоносного ПО и вредоносных нагрузок различные методы, включая polyglot-файлы, которые могут интерпретироваться как файлы различных форматов в зависимости от способа их прочтения (в данном случае PDF/HTA и PDF/ZIP). Одной из особенностей цепочки атаки стало использование скомпрометированной учетной записи электронной почты индийской компании INDIC Electronics для рассылки фишинговых сообщений с вложением Sosano. Письма содержали URL-ссылки на домен, маскирующийся под домен индийской компании, на котором размещался ZIP-архив с файлом XLS и двумя PDF-файлами. Файл с расширением .XLS на самом деле представлял собой ярлык Windows (файл LNK) с двойным расширением, имитирующий документ Microsoft Excel. Оба PDF-файла были созданы с помощью техники polyglot: один сочетался с HTA-скриптом, второй — с ZIP-архивом. В зависимости от используемого инструмента (например, файлового менеджера, инструментов командной строки или браузера) оба PDF-файла могли распознаваться как разные допустимые форматы. Цепочка атаки включала запуск LNK-файла, который открывал cmd.exe, а затем mshta.exe для выполнения polyglot-файла PDF/HTA. Этот файл запускал HTA-скрипт, содержащий инструкции по распаковке содержимого ZIP-архива, внедренного во второй PDF-файл. Один из файлов, входящих в состав второго PDF-файла, представлял собой ярлык (.url), указывающий на веб-страницу, по которой загружался исполняемый файл, расшифровывающий и запускающий бэкдор Sosano. Исследователи из Proofpoint отметили, что активность UNK_CraftyCamel не пересекается с

известными группами злоумышленников, но, учитывая выбор целевых отраслей, с высокой долей вероятности связана с Ираном.

Прочее

Атаки MintsLoader

Исследователи из компании ESentire опубликовали отчет о текущей вредоносной кампании, впервые обнаруженной в январе 2025 года. В ходе кампании применяется загрузчик MintsLoader, используемый для доставки вторичных вредоносных нагрузок, таких как инфостилер StealC и легитимная платформа распределенных вычислений с открытым исходным кодом Berkeley Open Infrastructure for Network Computing (BOINC). MintsLoader представляет собой вредоносный загрузчик на основе PowerShell, который распространяется через спам-рассылки со ссылками на сайты Kongtuke/ClickFix или с вложениями в виде JScript-файлов. В нем реализован алгоритм генерации доменов (DGA), использующий в качестве входных параметров текущий день месяца и константу, а также применяющий техники избегания запуска на виртуальных машинах для противодействия анализу в песочницах и разбору исследователями вредоносного ПО. Кампания нацелена на предприятия в секторах электроэнергетики, нефти и газа и юридических услуг в США и Европе.

Атаки с использованием уязвимости ZDI-CAN-25373

Исследователи компании Trend Micro опубликовали отчет о том, как прогосударственные и киберпреступные группы используют уязвимость ZDI-CAN-25373 (известную также как ZDI-25-148) в ярлыках Windows (.lnk-файлах), позволяющую скрытно выполнять вредоносные команды на компьютере жертвы с помощью специально сформированных ярлыков. В ходе атак для запуска вредоносных компонентов используются скрытые аргументы командной строки в .lnk-файлах, что затрудняет их обнаружение. Уязвимость была использована APT-группами из разных стран, включая Water Asena (Evil Corp), Earth Kumiho (Kimsuky, APT43), Earth Imp (Konni), Earth Anansi (Bitter) и Earth Manticore (APT37). С 2017 года от атак пострадали государственные учреждения и организации в финансовом, телекоммуникационном, военном и энергетическом секторах в Северной Америке, Европе, Азии, Южной Америке и Австралии. Анализ кампаний, использующих ZDI-CAN-25373, и связанных с ними методов вторжения показал, что почти 70% атак были нацелены прежде всего на кибершпионаж и кражу информации, а более 20% — на получение финансовой выгоды. В

качестве вредоносной нагрузки в таких атаках использовались Lumma Stealer, GuLoader, Remcos и другие распространенные вредоносные программы. По информации исследователей, компания Microsoft отказалась устранять уязвимость, сочтя, что она «не соответствует критериям обслуживания».

Предупреждение CISA о группе Ghost/Cring

Федеральное бюро расследований, Агентство по кибербезопасности и безопасности инфраструктуры США (CISA), а также Австралийский центр кибербезопасности Управления радиоэлектронной борьбы Австралии опубликовали совместный бюллетень по кибербезопасности. Он посвящен вымогательскому ПО Ghost (Cring), а также его индикаторам компрометации и тактикам, техникам и процедурам, выявленным в ходе расследования, проведенного ФБР в январе 2025 года. Среди жертв атак с использованием этой вредоносной программы — объекты критической инфраструктуры, школы и университеты, учреждения здравоохранения, правительственные сети, религиозные организации, технологические и промышленные компании, а также многочисленные малые и средние предприятия более чем в 70 странах мира.

В бюллетене указывается, что группа Ghost впервые заявила о себе в 2021 году. Эта группа, базирующаяся, по мнению исследователей, в Китае, регулярно меняла исполняемые файлы своего вымогательского ПО, изменяла расширения зашифрованных файлов, модифицировала тексты записок с требованием выкупа и использовала многочисленные адреса электронной почты для связи. Это затрудняло идентификацию группы. Со временем она стала известна под разными именами: Ghost, Cring, Crypt3r, Phantom, Strike, Hello, Wickrme, HsHarada и Rapture.

ФБР зафиксировало случаи, когда злоумышленники из группы Ghost получали первоначальный доступ к сетям, используя уязвимости в устройствах Fortinet FortiOS (CVE-2018-13379), серверах с установленным Adobe ColdFusion (CVE-2010-2861 и CVE-2009-3960), Microsoft SharePoint (CVE-2019-0604) и Microsoft Exchange (CVE-2021-34473, CVE-2021-34523 и CVE-2021-31207 — цепочка атаки, известная как ProxyShell). Кроме того, зафиксированы случаи загрузки злоумышленниками из группы Ghost веб-оболочек на скомпрометированные серверы и использования командной строки Windows и/или PowerShell для загрузки и запуска вредоносного ПО Cobalt Strike Beacon, которое затем внедряется в системы жертвы. Злоумышленники иногда создают новые локальные и доменные учетные записи, а также изменяют пароли к существующим аккаунтам. В 2024 году было отмечено, что они размещали веб-оболочки на веб-серверах жертв

для закрепления в системе. Получив повышенные привилегии, участники группировки использовали WMI-интерфейс командной строки (WMIC) для запуска PowerShell-команд на других системах в сети жертвы — зачастую для заражения новых систем вредоносным ПО Cobalt Strike Beacon. Злоумышленники используют такие исполняемые файлы, как Cring.exe, Ghost.exe, ElysiumO.exe и Locker.exe — все они представляют собой программы-вымогатели с аналогичным функционалом.

Kaspersky Industrial Control Systems Cyber Emergency Response Team (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