APT- и финансовые атаки на промышленные организации в первом квартале 2024 года

10.06.2024 Version 1.0

Этот документ содержит обзор сообщений об APT- и финансовых атаках на промышленные предприятия, информация о которых была раскрыта в первом квартале 2024 года, а также о связанной с этим активности групп, замеченных в атаках на промышленные организации и объекты критической инфраструктуры. В каждом случае мы постарались кратко изложить основные факты, а также привести полученные исследователями результаты и сделанные выводы, которые, по нашему мнению, могут быть полезны специалистам, занимающимся практическими вопросами кибербезопасности промышленных предприятий.

Как обычно, наиболее частыми способами первоначального проникновения стали социальная инженерия (фишинг) и проблемы безопасности в пограничных системах и доступных из интернета сервисах. Дыры в Ivanti Secure VPN и Microsoft Outlook на момент эксплуатации были уязвимостями нулевого дня — понятно, что для обнаружения атаки на раннем этапе было нужно очень много упорства и везения. Организациям, ставящим перед собой задачу защиты от такого вектора, стоит очень грамотно подойти к построению своей информационной инфраструктуры, разбивая её на домены безопасности таким образом, чтобы компрометация одной системы, пусть и очень важной, не давала злоумышленникам возможности доступа к смежным системам и продвижения таким образом по сети. Это потребует много инвестиций, в том числе в очень квалифицированных специалистов.

Остальные истории являются наглядным доказательством того факта, что, хоть обновление пограничных устройств и доступных из интернета сервисов и обучения сотрудников правилам кибергигиены и не кажется неподъёмной задачей, многие, даже весьма зрелые организации, имея и достаточные бюджеты, и разработанные политики и настроенные процедуры, всё равно, попадаются на крючок.

Одна из историй стоит особняком — в ней описан случай использования сценария adversary-in-the-middle (AitM), чтобы доставлять вредоносный имплант жертвам вместо обновлений легитимного ПО и прятать коммуникации импланта с CnC в атаках на цели из разных стран — Китая, Японии и Великобритании. Самостоятельно защититься от злоумышленников, располагающих такими возможностями, будет очень непросто.

Юго-Восточная Азия и Корея

Атаки на южнокорейских производителей полупроводников

Национальная служба разведки (NIS) Южной Кореи предупреждает, что северокорейские хакеры проводят атаки на южнокорейские компании по производству полупроводников с целью кибершпионажа. Как сообщает NIS, эти атаки участились во второй половине 2023 года и продолжались до недавнего времени.

Для получения первоначального доступа к корпоративным сетям атаковались серверы с доступом в интернет, имеющие известные уязвимости. После проникновения в сеть злоумышленники похищали с серверов конфиденциальные документы и сведения. В случаях, отмеченных NIS, северокорейские злоумышленники прибегли к приему Living-off-the-Land (LOTL), то есть использовали доверенные приложения в преступных целях.

NIS сообщила о двух кибератаках на разные организации, произошедших в декабре 2023 года и феврале 2024 года. В результате взлома серверов управления конфигурацией и политиками безопасности произошла утечка конструкторских чертежей продукции, фотографий производственных объектов и других конфиденциальных данных. Эксперты из NIS считают, что эти кибератаки направлены на сбор ценной технической информации, которая могла бы помочь Северной Корее в разработке собственной программы по производству микросхем и удовлетворении потребностей в военном оборудовании.

NIS уведомила жертву взлома об этих фактах и оказала помощь в реализации соответствующих мер безопасности. Чтобы предотвратить дальнейший ущерб, информация об этих угрозах была передана крупным полупроводниковым компаниям страны для проведения собственных проверок безопасности.

Атаки группы SideWinder

APT-группа, известная как SideWinder, за последние месяцы провела сотни атак на крупные организации в Азии и Африке. Цепочка заражения соответствует процессу, описанному в предыдущих отчетах «Лаборатории Касперского».

Большинство атак начинается с отправки фишингового письма с документом Microsoft Word или с ZIP-архивом, содержащим LNK-файл. Вложенный файл запускает цепочку событий, которые приводят к выполнению ряда промежуточных модулей на языках JavaScript и .NET. Окончательную компрометацию системы производит написанный на .NET вредоносный имплант, который выполняется только в памяти и загружается с помощью самописных упакованных загрузчиков.

В ходе расследования специалисты «Лаборатории Касперского» обнаружили довольно большую инфраструктуру, состоящую из множества различных VPS-серверов и десятков поддоменов. Предполагается, что многие поддомены создавались под конкретных жертв. Схема их именования указывает на то, что злоумышленники пытались маскировать вредоносный трафик под легитимный трафик сайтов, связанных с государственными организациями или логистическими компаниями.

В прошлом активность группы SideWinder была нацелена на правительственные и военные организации в Южной Азии, но в данном случае было замечено расширение круга ее целей. Группа также скомпрометировала системы жертв в Юго-Восточной Азии и Африке. Кроме того, данные телеметрии «Лаборатории Касперского» показали, что компрометации подверглись различные дипломатические организации в Европе, Азии и Африке. Расширение круга целей также затронуло новые отрасли: были обнаружены новые жертвы злоумышленников в сфере логистики, в частности в сфере морских грузоперевозок.

Активность китайскоязычных групп

Атаки группы Blackwood

Специалисты ESET обнаружили продвинутый имплант под названием NSPX30, используемый новой APT-группой, которая, по мнению специалистов, связана с Китаем. Группа, получившая название Blackwood, использует прием adversary-in-the-middle для перехвата запросов на обновление от легитимного ПО и доставки вместо пакетов обновлений вредоносного импланта NSPX30 а также для перехвата трафика импланта чтобы скрыть CnC и снизить вероятность обнаружения.

Для коммуникации с CnC имплант генерировал HTTP- и UDP-запросы на адреса, принадлежащие Baidu, которые перехватывались сетевым имплантом, расположенным, по всей видимости, где-то в телеком-инфраструктуре и перенаправлялись им на сервер злоумышленников.

NSPX30 — это многоступенчатый имплант из нескольких компонентов, таких как дроппер, установщик, загрузчики, оркестратор и бэкдор. Два последних компонента имеют собственные наборы плагинов. Имплант предназначался для перехвата пакетов, что позволило операторам NSPX30 скрыть свою инфраструктуру. Код NSPX30 перекликается с более ранним бэкдором под названием Project Wood — самый старый из найденных образцов был скомпилирован в 2005 году.

Группа проводила кибершпионские операции против частных лиц и компаний из Китая, Японии и Великобритании. Среди ее жертв, в частности, крупная производственная и торговая компания в Китае, а также представительство японской инженерно-производственной корпорации в Китае.

Исследователи полагают, что перехват трафика осуществлялся скорее где-то ближе к жертвам, чем к инфраструктуре Baidu, и вряд ли на стороне китайского оператора — Baidu имеет георасределённую инфраструктуру, доступную через anycast, часть которой расположена за пределами КНР.

Эксплуатация уязвимости в Ivanti Connect Secure VPN

Исследователи Volexity обнаружили целевые атаки, использующие две уязвимости нулевого дня (CVE-2024-21887 и CVE-2024-46805) в VPN-устройствах Ivanti Connect Secure (ICS). Сочетание этих уязвимостей позволяет злоумышленникам удаленно выполнять код без аутентификации.

Изначально эти уязвимости эксплуатировались группой, известной под названием UTA0178 и предположительно работающей из Китая. Однако впоследствии атаки на основе тех же уязвимостей проводили и другие группы.

Специалисты Volexity обнаружили более 1700 таких компрометаций. По их данным, жертвы кибератак распределены по всему миру и представляют собой различные по масштабам и сферам деятельности организации: международные государственные и военные структуры, национальные телекоммуникационные компании, подрядчиков в оборонной промышленности, а также предприятия в аэрокосмической промышленности, авиации, машиностроении и других отраслях.

Компания Ivanti предоставила рекомендации по устранению этих двух уязвимостей и готовит исправление для них.

Атаки группы VOLTZITE

Согласно отчету компании Dragos, APT-группа VOLTZITE проводит операции по разведке и сбору данных в отношении нескольких американских электроэнергетических компаний с начала 2023 года.

Эта группа имеет общие черты с группой, описанной Агентством по кибербезопасности и защите инфраструктуры США (CISA) в мае 2023 года, и группой Volt Typhoon, описанной Microsoft. Компания Dragos также выявила связи группы VOLTZITE с вредоносным кластером UTA0178, который был обнаружен компанией Volexity. Этот кластер эксплуатирует уязвимости нулевого дня в решениях Ivanti Connection Secure VPN.

Злоумышленники преимущественно пользуются тактикой LOTL, тщательно следят за своей операционной безопасностью и предпочитают инструменты с открытым исходным кодом и веб-шеллы. После кражи учетных данных они занимаются дальнейшим распространением по инфраструктуре.

Группа VOLTZITE нацелена на службы предупреждения и ликвидации последствий чрезвычайных ситуаций, телекоммуникационные компании, операторов спутниковой связи, а также на африканских поставщиков электроэнергии.

Хотя группе VOLTZITE удалось взломать одну из американских электро- и водоснабжающих компаний и похитить данные географических информационных систем, конфигурационные данные систем SCADA и списки важных клиентов компании, они не смогли проникнуть в ее операционную технологическую сеть. По данным отчета Dragos, злоумышленники скомпрометировали такие устройства и программные продукты, как Fortinet FortiGuard, PRTG Network Monitor, ManageEngine ADSelfService Plus, FatePipe WARP, Ivanti Connect Secure VPN и Cisco ASA.

Предупреждение агентства CISA о группе Volt Typhoon

7 февраля Агентство по кибербезопасности и защите инфраструктуры (CISA), Агентство национальной безопасности (АНБ) и Федеральное бюро расследований (ФБР) опубликовали совместные рекомендации и инструкции, касающиеся китайскоязычной группы Volt Typhoon, которая проникла в сеть критической инфраструктуры в США и оставалась там незамеченной как минимум пять лет, пока не была обнаружена.

Volt Typhoon скомпрометировала ИТ-среды множества организаций, в основном из сфер связи, энергетики, транспорта, водоснабжения и водоотведения, в континентальных и неконтинентальных районах США и на федеральных территориях, включая Гуам.

Известно, что хакеры из Volt Typhoon активно используют в своих атаках доверенные приложения (тактика LOTL) и украденные учетные записи. Группа работает весьма скрытно, что позволяет ей избегать обнаружения и надолго закрепляться в скомпрометированных системах. Власти США также опасаются, что Volt Typhoon, пользуясь доступом к критически важным сетям, может добиться разрушительных последствий, особенно в условиях потенциальных военных конфликтов или геополитической напряженности.

К рекомендациям и инструкциям прилагается техническое руководство, содержащее информацию о том, как распознать методы работы Volt Typhoon, а также о мерах по их нейтрализации.

Активность русскоязычных групп

Атаки группы RedCurl

Исследователи из Group-IB сообщили о новых атаках русскоязычной хакерской группы RedCurl, направленных на компании из сфер строительства, логистики, авиаперевозок и горнодобывающей промышленности в Австралии, Сингапуре и Гонконге.

Исследователи смогли заполучить файлы, используемые в обнаруженных кампаниях, в октябре 2023 года. Впервые группа RedCurl был замечена Group-IB в конце 2019 года, однако она активна как минимум с 2018 года. Ранее RedCurl осуществила более 40 атак: половина из них на территории России, остальные — в Великобритании, Германии, Канаде, Норвегии и Украине. В то время Group-IB предполагала, что эти злоумышленники как-то связаны с APT-группой Cloud Atlas, основываясь на профиле жертв и применении инструмента LaZagne и протокола WebDav. Других сходств замечено не было. Для атак всегда использовались оригинальные инструменты собственной разработки.

Злоумышленники занимались исключительно кибершпионажем по заказу. Как правило, группе RedCurl удавалось реализовать свой план в период от двух до шести месяцев с момента заражения до собственно кражи данных. Злоумышленники похищали интересующую их бизнес-информацию: корпоративную переписку, личные дела сотрудников, юридические документы и другую секретную информацию компании-жертвы.

Начальный этап новых атак RedCurl остался прежним — рассылка сотрудникам электронных писем с вложениями в виде SVG-файлов

или RAR-архивов, содержащих SVG-файлы (раньше в письмах использовались ссылки). SVG-файлы содержат ссылки на файл RedCurl.ISO, который, в свою очередь, содержит LNK-файл и каталог со множеством DLL-файлов.

После активации ярлыка с помощью rundll32.exe выполняется команда, запускающая RedCurl.SimpleDownloader, который загружает компонент следующего этапа и отображает сайт-приманку. Если необходимые проверки пройдены, RedCurl.Downloader собирает информацию о системе и отправляет ее на командный сервер.

После этого активируется компонент следующего этапа — RedCurl.Extractor, который извлекает компонент RedCurl.FSABIN и закрепляет его в системе. RedCurl.FSABIN отправляет запросы на командный сервер, чтобы получить ключ расшифровки и зашифрованный BAT-скрипт, который расшифровывается и запускается на зараженной системе (RedCurl.Commands).

Атаки группы Pawn Storm / Sofacy / APT28

Компания TrendMicro сообщила, что группа Pawn Storm (также известная как APT28, Sofacy, Fancy Bear, Sednit и Forest Blizzard) в период с апреля 2022 года по ноябрь 2023 года проводила relay-атаки с перехватом NTLMv2-хеша для проникновения методом перебора в сети правительственных, оборонных, военных, энергетических и транспортных организаций по всему миру.

В тот период группа эксплуатировала критическую уязвимость нулевого дня с повышением привилегий (CVE-2023-23397), чтобы собирать дайджесты NTLMv2 из целевых учетных записей Outlook посредством relay-атак с перехватом хеша и рассылать вредоносные приглашения в календарь.

Чтобы скрыть следы, группа Pawn Storm использовала широкий спектр инструментов, включая VPN-сервисы, Tor, IP-адреса легитимных дата-центров и скомпрометированные маршрутизаторы на базе EdgeOS. Кроме того, группа Pawn Storm скомпрометировала множество учетных записей электронной почты по всему миру, используя их в качестве стартовой площадки для рассылки фишинговых писем.

Далее в кампании применялись более продвинутые методы, в том числе скрипты на платформе Mockbin и URL-адреса, которые перенаправляли на PHP-скрипты на сайтах с бесплатным хостингом. Pawn Storm также использовала уязвимость CVE-2023-38831 в WinRAR для relay-атак с перехватом хеша. В конце 2023 года была развёрнута фишинговая

кампания против различных организаций в Европе и Северной Америке. В кампании использовались URL-адреса webhook[.]site и IP-адреса VPN.

В феврале Федеральное бюро расследований (ФБР), Агентство национальной безопасности (АНБ), Киберкомандование США и международные партнеры выпустили совместный бюллетень по кибербезопасности (CSA), в котором предупредили, что злоумышленники компрометируют маршрутизаторы Ubiquiti EdgeRouters (EdgeRouters) на базе Linux для проведения вредоносных кибероперaций по всему миру.

Согласно информации из бюллетеня, эти операции направлены на организации различных сфер, включая аэрокосмическую и оборонную промышленности, образование, энергетику, коммунальные услуги, государственные учреждения, гостиничный бизнес, производство, нефтегазовый сектор, розничную торговлю, технологические компании и транспортные предприятия. Операции проводились в Чехии, Италии, Литве, Иордании, Черногории, Польше, Словакии, Турции, Украине, Объединенных Арабских Эмиратах и США.

Расследование ФБР показало, что злоумышленники из группы APT28 получали доступ к маршрутизаторам EdgeRouters, скомпрометированным с помощью ботнета Moobot, который устанавливает троянизированный пакет OpenSSH на скомпрометированное оборудование. Атакующие использовали скомпрометированные маршрутизаторы EdgeRouters для сбора учетных данных, проксирования сетевого трафика, а также размещения поддельных стартовых страниц и самописных инструментов, используемых после компрометации жертвы. Имея root-доступ к скомпрометированным устройствам, злоумышленники получали неограниченные привилегии в операционных системах на базе Linux и устанавливали общедоступные инструменты, такие как Impacket ntlmrelayx.py и Responder, для выполнения relay-атак NTLM и поддельной NTLMv2-аутентификации на хостах при проведении вредоносных кампаний.

Активность, связанная с Ближним Востоком

Атаки группы UNC1549

Компания Mandiant сообщила о продолжающейся кампании кибершпионажа, направленной на предприятия аэрокосмической, авиационной и оборонной промышленности Израиля, Объединенных Арабских Эмиратов, а также, возможно, Турции, Индии и Албании.

Кампания началась еще в июне 2022 года и проводилась группой, которой Mandiant дала название UNC1549. Эту группу исследователи связывают с Ираном, а кампания имеет сходства с другой хакерской кампанией, известной как Tortoiseshell.

Специалисты Mandiant отмечают множество способов маскировки, к которым прибегла группа UNC1549. Особенно выделяется их активное использование облачной инфраструктуры Microsoft Azure, а также применение методов социальной инженерии для распространения двух уникальных бэкдоров: MINIBIKE и MINIBUS.

Зловред MINIBIKE первый раз был замечен в июне 2022 года, а последний раз — в октябре 2023 года. Он осуществляет эксфильтрацию и выгрузку файлов, умеет выполнять команды и использует в своей работе облачную инфраструктуру Azure. MINIBUS — это самописный бэкдор с более гибким интерфейсом для выполнения кода и расширенными возможностями сбора данных. Впервые он был замечен в августе 2023 года, а последний раз — в минувшем январе. Эти две вредоносные программы ведут себя как типичные инструменты кибершпионажа: они собирают учетные данные и выполняют произвольный вредоносный код, подготавливающий почву для дальнейшего шпионажа.

Исследователи также обнаружили авторский инструмент туннелирования, получивший название LIGHTRAIL. Он, вероятно, создан на базе SOCKS4A-прокси с открытым исходным кодом, который перенаправляет данные через облачную инфраструктуру Azure.

Другое

Атаки группы Scaly Wolf

Исследователи из компании BI.ZONE сообщили о новых кампаниях группы Scaly Wolf, нацеленных на логистические и промышленные объекты в России.

Злоумышленники рассылают фишинговые письма от имени российских государственных служб (письма от якобы Роскомнадзора, Следственного комитета, Военной прокуратуры, а также судебные решения и другие нормативные предписания) и побуждают получателей запустить вредоносный файл, после чего внедряют на компьютер жертвы стилер White Snake. Вредоносная программа почти всегда находится в защищенном ZIP-архиве, пароль к которому содержится в имени архивного файла.

White Snake — основной инструмент в арсенале Scaly Wolf. Впервые этот стилер появился в феврале 2023 года в даркнете. White Snake может запускаться кросс-платформенно с помощью загрузчика, написанного на языке Python. В версии стилера для Windows реализован функционал троянца с удаленным доступом, в том числе кейлоггер, также поддерживаются XML-файлы с индивидуальной конфигурацией. Кроме того, стилер использует сервис Serveo.net для SSH-доступа к зараженному компьютеру, что позволяет злоумышленникам выполнять команды на скомпрометированных хостах. Еще одна функция этого стилера — отправка уведомлений о новых зараженных устройствах в телеграм-бот.

Группе Scaly Wolf удалось обойти ограничения разработчиков стилера, которые запретили его использование в России и странах СНГ. Для этого злоумышленники модифицировали ПО и отключили фильтрацию по IP-адресам, определявшую принадлежность жертвы к заблокированному сегменту адресов.

Операция FlightNight

Исследователи из EclecticIQ обнаружили новую кампанию шпионажа, нацеленную на индийские правительственные организации и предприятия энергетической промышленности. Используется модифицированная версия стилера HackBrowserData с открытым исходным кодом, который может собирать учетные данные для входа в браузер, файлы cookie и историю посещений. Исследователи дали этой кампании название FlightNight, однако не связали ее с конкретной группой.

Стилер доставлялся жертвам посредством фишингового PDF-документа, замаскированного под письмо-приглашение от индийских военно-воздушных сил. Исследователи предполагают, что оригинальный PDF-документ, скорее всего, был похищен во время одного из предыдущих вторжений и повторно использован злоумышленниками. Этот документ содержал LNK-файл, указывающий на вредоносную программу. Эта вредоносная программа после запуска немедленно начинала пересылать документы и данные из кеша браузера с устройства жертвы в каналы корпоративного мессенджера Slack. Похищалась такая информация, как внутренние документы, частные электронные письма и данные из кеша браузеров.

Хотя так и не удалось вычислить хакерскую группировку, стоящую за этой кампанией, сходство в ее вредоносном ПО и методах доставки явно указывает на связь этой кампании с атакой, о которой сообщалось в январе.

В тот раз злоумышленники нацелились на служащих BBC Индии с помощью вредоносной программы GoStealer, которая крадет учетные данные. По мнению EclecticIQ, обе кампании, скорее всего, являются делом рук одной и той же группы.

Атаки с использованием стилера Rhadamanthys

Согласно исследованию Cofense, обновленная версия стилера Rhadamanthys применялась в фишинговых атаках на компании нефтегазового сектора. В кампании используются тщательно подготовленные фишинговые письма и PDF-файл, замаскированный под сообщение от Федерального бюро транспорта.

Операторы фишинговой кампании создавали различные провокационные темы писем, например «Уведомление: участие вашего автомобиля в ДТП» или «Внимание: столкновение с вашим автомобилем». Письмо включает вредоносную ссылку, которая посредством уязвимости открытого перенаправления (Open Redirect) загружает страницу, на которой вместо упомянутого PDF-документа содержится его изображение. Если нажать на него, загрузится ZIP-архив с вредоносной программой-стилером.

Атаки StrelaStealer

Исследователи из Palo Alto Networks выявили волну масштабных кампаний StrelaStealer, затронувшую более ста организаций в ЕС и США из таких сфер, как производство, коммунальные услуги, энергетика, строительство, высокие технологии и др. Кампания, нацеленная на кражу учетных данных из почтовых ящиков, достигла своего пика в период с конца января по начало февраля 2024 года.

Для атак использовались фишинговые письма с вложенными ZIP-архивами, содержащими JScript-файлы. При их активации запускалась DLL-библиотека и доставлялась полезная нагрузка StrelaStealer. Это отличается от предыдущей тактики, когда вредоносная программа запускалась через фишинговые письма с ISO-файлами.

При этом, как отмечают исследователи, используется обновленная версия StrelaStealer. Основная задача этой вредоносной программы остается той же — кража учетных данных электронной почты. Однако злоумышленники обфусцировали поток управления и убрали PDB-строки, чтобы ее было сложнее обнаружить.

Атаки группы Magnet Goblin

Исследователи из Check Point обнаружили новую группу с финансовой мотивацией, получившую название Magnet Goblin. Она проводила атаки на американские медицинские, производственные и энергетические компании, используя уязвимости в продуктах Ivanti.

Предполагается, что злоумышленники скомпрометировали уязвимые серверы Ivanti Connect Secure VPN и использовали их для установки бэкдоров в целевых ИТ-системах. Среди вредоносных программ, применяемых злоумышленниками, — бэкдор для Linux под названием MiniNerbian (новая версия NerbianRAT), JavaScript-стилер под названием WARPWIRE, а также Ligolo — инструмент туннелирования с открытым исходным кодом, написанный на языке Go. Кроме того, используются легитимные инструменты удаленного мониторинга и управления, такие как ScreenConnect и AnyDesk.

Центр реагирования на инциденты информационной безопасности промышленных инфраструктур «Лаборатории Касперского» (Kaspersky ICS CERT) — глобальный проект «Лаборатории Касперского», нацеленный на координацию действий производителей систем автоматизации, владельцев и операторов промышленных объектов, исследователей информационной безопасности при решении задач защиты промышленных предприятий и объектов критически важных инфраструктур.

Kaspersky ICS CERT ics-cert@kaspersky.com