Kaspersky ICS CERT

kaspersky

APT- и финансовые атаки на промышленные организации во втором квартале 2025 года

04.09.2025

Версия 1.0

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

Прошедший квартал охарактеризовался атаками на промышленные предприятия с применением изощренных тактик и техник. Никого не удивляет, что APT-группы эксплуатируют в атаках уязвимости нулевого дня. Так, Lazarus использовала уязвимость в ПО локального вендора в ходе кампании в Южной Корее, Stealth Falcon – уязвимость в легитимном инструменте Microsoft против крупной оборонной компании в Турции. Sednit рассылала оборонным предприятиям фишинговые письма, эксплуатируя XSS-уязвимость нулевого дня в почтовом сервере MDaemon. Без сомнений, самым сложным и интересным случаем стала атака на российские организации через обновления для защитного решения ViPNet, о которой сообщила «Лаборатория Касперского».

«Продвинутые» злоумышленники не ограничиваются эксплуатацией уязвимостей нулевого дня. Они применяют и другие нетривиальные методы – например, рассылку электронных писем от имени скомпрометированной организации ее контрагентам (BEC-атака). Такую тактику продемонстрировала Cloud Atlas, атакуя российские организации.

Впрочем, чтобы проникнуть в технологическую инфраструктуру жертвы, необязательно прибегать к чему-то сложному (это подтверждает и регулярный статистический отчет нашей команды). Этот факт был проиллюстрирован также проиранской группой, которая, используя скомпрометированные учетные данные для доступа к VPN/SSL-серверам жертв или размещая веб-шеллы на общедоступных серверах, смогла закрепиться в изолированном сегменте сети объекта критической инфраструктуры на Ближнем Востоке, содержащей OT-системы.

О необходимости постоянного соблюдения основных мер кибербезопасности на промышленных предприятиях напомнили в этом квартале еще несколько инцидентов.

По меньшей мере 65 правительственных организаций, а также ИТ-, промышленных и логистических компаний стали жертвами атак, в результате которых на страницах веб-аутентификации их корпоративного Microsoft Exchange Server был внедрен вредоносный код. Внезапно, и четырех лет оказывается кому-то недостаточно для устранения критических уязвимостей в серверном ПО, таких как ProxyShell.

Некоторые крупные организации, включая правительственные учреждения, университеты и даже известные международные корпорации, продемонстрировали на своем примере, что пренебрежение основами кибербезопасности, в частности необходимостью присматривать за выводимыми из эксплуатации корпоративными веб-ресурсами, неизбежно приводит к инцидентам.

Многие злоумышленники, в том числе из тех, что атаковали транспортные, коммунальные, энергетические, финансовые и правительственные организации на Ближнем Востоке, да и вообще по миру, посредством фишинговых кампаний ClickFix, напоминают: обучение персонала кибергигиене должно быть заложено в бюджет любой промышленной организации.

Наконец, заметим, что отчет «Лаборатории Касперского» о деятельности «Киберпартизан», которые стали искать новые цели в России, оказался нечаянным предсказанием новых крупных инцидентов.

Атаки, нацеленные на российские организации

Атаки GOFFEE

Исследователи «Лаборатории Касперского» опубликовали статью о группе GOFFEE (она же Paper Werewolf), действующей с начала 2022 года. Злоумышленники, активность которых направлена исключительно против организаций в России, рассылают фишинговые письма с вредоносными вложениями. С мая 2022 года и до лета 2023 года GOFFEE применяла модифицированный зловред Owowa (вредоносный IIS-модуль), предназначенный для кражи учетных данных и удаленного выполнения команд через приложение Outlook Web Access (OWA).

Эксперты «Лаборатории Касперского» обнаружили Owowa в конце 2021 года. С 2020 года вредоносный модуль использовался в ходе атак преимущественно в Азии. Исследователи показали, что он мог быть разработан человеком, говорящим на китайском. Позднее они выяснили, что с мая 2022 года обновленная версия модуля использовалась исключительно

в атаках на объекты в России. Эксперты связали распространение Owowa с цепочкой заражения на основе почтовых рассылок, которая имитировала активность группы Cloud Atlas.

В 2024 году GOFFEE начала внедрять модифицированные версии explorer.exe посредством целевого фишинга. Во второй половине 2024 года группа продолжила таргетированные атаки на организации в России, используя PowerTaskel – непубличный модульный агент для Mythic, а также новый имплант PowerModul. Атакам подверглись медиа- и телекоммуникационные компании, государственные учреждения, организации из строительной и энергетической отраслей.

Атаки Cloud Atlas

Исследователи Positive Technologies сообщили о новых атаках группы Cloud Atlas, нацеленных на российские организации оборонно-промышленного комплекса. Атаки отличались обновленной сетевой инфраструктурой – это было выявлено в ходе расследования инцидента на одном из предприятий в ноябре 2024 года. Связанные с новой инфраструктурой вредоносные файлы, использованные в кибератаках, появились в начале января 2025 года, в то время как серверы, доменные имена, TLS-сертификаты и необходимые DNS-записи были зарегистрированы и появились в сети еще в конце октября – начале ноября 2024 года.

Вредоносные документы Microsoft Office содержали информацию об управляющей инфраструктуре в потоке 1Table – это характерная техника Cloud Atlas. Ранее исследователи сообщили, что открытие этих документов приводит к выполнению вредоносных VB-скриптов, записанных в альтернативные потоки данных, которые взаимодействуют с API Google Sheets для передачи информации о зараженной системе и загрузки бэкдора PowerShower с последующей эксфильтрацией похищенных данных через облачное хранилище. Обнаруженные в ходе новой волны атак вредоносные документы мимикрировали под приглашения на курсы повышения квалификации, документы, связанные с антикоррупционными проверками и мобилизационными мероприятиями, справки о сотрудниках, резюме операторов станков с ЧПУ и прочее. Исходные документы, скорее всего были украдены группой из сетей ранее скомпрометированных предприятий. Исследователи зафиксировали факт использования злоумышленниками тактики BEC (Business Email Compromise). Вредоносные электронные письма отправлялись с систем ранее скомпрометированных российских предприятий оборонной промышленности их контрагентам.

Атаки FakeTicketer/Операция HollowQuill

Исследователи Seqrite Labs обнаружили кампанию кибершпионажа против российских промышленных предприятий, которая получила название «Операция HollowQuill». Злоумышленники отправляли вредоносный RAR-файл, содержащий .NET-дроппер, который устанавливал написанный на языке Golang загрузчик шеллкода, а также легитимное приложение OneDrive и приманку в виде PDF-файла с конечной вредоносной нагрузкой Cobalt Strike. Приманка имитировала документ под шапкой учреждения Министерства науки и высшего образования России, а именно Балтийского государственного технического университета «ВОЕНМЕХ» имени Д. Ф. Устинова. По всей видимости, это реальное сообщение, адресованное некоторым организациям, в котором, вероятно, обсуждаются исследовательские проекты или проекты взаимодействия с оборонными компаниями. В отчете Seqrite Labs говорится, что целями злоумышленников были высшие учебные заведения, научно-исследовательские учреждения, организации военной и оборонной промышленности, ракетно-космической отрасли и государственные исследовательские организации.

Исследователи F6 обнаружили уникальные артефакты, которые позволяют связать операцию HollowQuill с известной группой FakeTicketer. Активность, описанная в отчете Seqrite Labs, впервые была выявлена исследователями Positive Technologies в конце 2024 года, а дополнительный анализ позволил коллегам из F6 установить пересечения с деятельностью FakeTicketer. По их данным, злоумышленники действуют как минимум с июня 2024 года, их основная мотивация предположительно – шпионаж, а среди целей – промышленные организации, государственные учреждения и спортивные функционеры. Анализ вредоносного ПО и инфраструктуры злоумышленников показал, что у HollowQuill и FakeTicketer есть пересечения по коду дропперов и доменным именам. Оба дроппера – LazyOneLoader (использовался в ходе операции HollowQuill) и Zagrebator.Dropper (использовался в более ранних кампаниях) – написаны на C#, имеют одинаковые имена иконок (faylyk), похожие названия файлов и классов, хранят вредоносную нагрузку и иконку в ресурсах. И в обоих случаях файлы OneDrive*.exe и OneDrive*.lnk используются для сокрытия активности, а код дропперов для создания ярлыков практически идентичен.

Атаки под видом обновления ViPNet

В апреле 2025 года исследователи «Лаборатории Касперского» выявили сложную APT-кампанию неизвестного актора. Злоумышленники заражали компьютеры крупных организаций в России, используя файлы обновлений для программного обеспечения ViPNet. Эти обновления содержали

исполняемый файл загрузчика msinfo32.exe, который считывал зашифрованный файл с полезной нагрузкой. Он обрабатывал содержимое файла и загружал в память бэкдор с универсальным функционалом, – зловред может подключаться к командному серверу по протоколу TCP, позволяя злоумышленнику, помимо прочего, похищать с зараженных компьютеров файлы и запускать дополнительные вредоносные компоненты. 18 апреля разработчик решения ViPNet подтвердил инцидент со сложной целенаправленной атакой на ряд клиентов, выпустил обновления и рекомендации.

Атаки Sapphire Werewolf

Исследователи BI.ZONE сообщили о новой активности группы Sapphire Werewolf, которая использует обновленную версию Amethyst Stealer. Злоумышленники продолжили рассылать вредоносное ПО через фишинговые электронные письма, на этот раз нацеливаясь на топливно-энергетические компании в России. Sapphire Werewolf маскировала вредоносное вложение под служебную записку и отправляла ее жертве от имени отдела кадров. Письмо содержало архив с именем «Служебная записка.rar», внутри которого находился исполняемый файл с таким же названием и иконкой PDF-документа. Этот файл представлял собой .NET-загрузчик, написанный на C# и защищенный .NET Reactor. Он содержал полезную нагрузку в кодировке Base64 – вредоносную программу Amethyst Stealer, тоже защищенную .NET Reactor. Amethyst Stealer может извлекать аутентификационные данные из Telegram, браузеров Chrome, Opera, Yandex, Brave, Orbitum, Atom, Kometa, Edge Chromium, файлов конфигурации FileZilla и SSH, а также конфигурационные файлы с удаленных рабочих столов и VPN-клиентов и различные типы документов (в том числе с внешних носителей).

Атаки Librarian Ghouls

Исследователи «Лаборатории Касперского» сообщили об активностях группы Librarian Ghouls (она же Rare Werewolf и Rezet), специализирующейся на кибершпионских атаках против организаций в России и странах СНГ. В качестве начального вектора заражения злоумышленники использовали целевой фишинг, причем обнаруженные письма содержали вредоносные архивы, защищенные паролем. Внутри находился вредоносный имплант, замаскированный под платежное поручение. Этот образец представляет собой самораспаковывающийся инсталлятор, созданный при помощи утилиты Smart Install Maker для Windows. При запуске он активирует легальные утилиты вроде AnyDesk и Blat, которые в дальнейшем используются для извлечения конфиденциальных данных. Помимо этих

утилит, злоумышленники устанавливали на зараженные компьютеры майнер XMRig.

Исследователи с небольшой долей уверенности предположили, что Librarian Ghouls также использует фишинговые сайты для кражи учетных данных. Найденные страницы выдавали себя за почтовый сервис Mail.Ru. Полученная телеметрия показала, что попытки заражения были зафиксированы в более чем 100 промышленных и научных организациях в России, а также в нескольких организациях в Беларуси и Казахстане.

Атаки Silent Werewolf

Исследователи BI.ZONE обнаружили новые кампании кластера Silent Werewolf, нацеленные на организации в России и Молдове. Атаки прошли в две волны: первая была направлена исключительно против российских организаций в энергетике (атомная промышленность), приборостроении, авиастроении и машиностроении. Злоумышленники использовали фишинговые письма, замаскированные под досудебную претензию и проект строительства жилого помещения, содержавшие ссылку для загрузки ZIP-архива. В нем было два файла: LNK и еще один ZIP-архив с легитимным EXE-файлом, вредоносной библиотекой (C#-загрузчик) и отвлекающим PDF-документом. Загрузчик представлял собой DLL-файл, который запускался с помощью легитимного исполняемого файла H5GDXM70NJ.exe (DeviceMetadataWizard.exe), используя технику подмены загружаемой DLL (DLL sideloading). Он предназначался для скачивания вредоносной нагрузки с сервера злоумышленников, закрепления ее на хосте при запуске системы, а также открытия отвлекающего PDF-документа. На момент проведения исследования вредоносная нагрузка была недоступна, но ретроспективный анализ аналогичных атак Silent Werewolf показал, что скорее всего в качестве такой нагрузки использовалось XDigo.

Вторая волна атак была нацелена в основном на молдавские организации, но с потенциальным распространением на российские. Новая версия загрузчика распространялась под видом графика замены служебных пропусков, рекомендаций по защите информационной инфраструктуры от атак вымогателей. Как и в предыдущей кампании, вредоносная рассылка, предположительно, осуществлялась с использованием фишинговых писем, содержащих ссылку для скачивания архива.

Атаки PhantomCore

Исследователи F6 сообщили о новых атаках группы PhantomCore (она же Head Mare), которые были проведены в мае 2025 года, а также о ранее

неизвестной активности, датируемой 2022 годом. Инструментарий и цели атак со временем менялись: сначала это были хищение, повреждение и уничтожение данных, к 2024 году акцент сместился на шифрование инфраструктуры жертв и получение финансовой выгоды.

При изучении инфраструктуры PhantomCore исследователи обнаружили пересечения в регистрационных данных доменов, что позволило идентифицировать дополнительные домены и связанные с ними образцы, относящиеся к 2022 году. По данным F6, тогда PhantomCore распространила дроппер VALIDATOR.msi с вредоносной программой StatRAT и исполняемым файлом-приманкой, имитирующим легитимное ПО Валидатор 1.0, которое проверяет сеть на соответствие определенному федеральному закону. Помимо обработки различных команд от командного сервера, вредоносная программа StatRAT имеет модуль стилера и функции повреждения и уничтожения файлов в зараженной системе.

В 2025 году PhantomCore продолжила развивать свои инструменты и переписывать их на различные языки программирования. Так, 5 мая исследователи F6 обнаружили и заблокировали вредоносные рассылки, приписываемые PhantomCore. Среди получателей были промышленные организации, энергетические и коммунальные компании. К электронным письмам был прикреплен исполняемый файл в виде архива с именем «Документы_на_рассмотрение.zip». Внутри находился использовавшийся в качестве приманки PDF-файл «Сопроводительное_письмо.pdf», по содержанию это был договор двух коммерческих компаний на поставку материалов и оборудования. Вредоносный исполняемый файл представлял собой обновленную версию бэкдора PhantomeCore.GreqBackdoor v.2, написанную на языке Golang без обфускации.

Атаки Fairy Wolf

Исследователи BI.ZONE обнаружили кампанию группы Fairy Wolf (она же Unicorn) с новым вектором распространения – через Telegram. Злоумышленники не представлялись генеральным директором или бухгалтером, как это бывало раньше, а прямо предлагали сотрудникам организаций финансовое вознаграждение за инсайдерскую деятельность и передачу им конфиденциальной информации. Они высылали документ с подробными инструкциями «Условия работы.rar», в котором содержался HTML-файл приложения «Документ.hta», представляющий собой дроппер стилера Unicorn. Этот стилер собирает файлы с различными расширениями размером до 100 МБ, а также извлекает содержимое папки %APPDATA%\Telegram Desktop\tdata и учетные данные из браузеров. По данным BI.ZONE, в мае Fairy Wolf провела более 10 атак с распространением

стилера Unicorn на российские энергетические компании, а также организации тяжелой промышленности и военно-промышленного комплекса. Злоумышленники маскировали также вредоносное ПО под резюме специалистов, акты, контракты, трудовые договора и прочее.

Атаки Vengeful Wolf/room155

Исследователи F6 сообщили о деятельности группы room155 (она же DarkGaboon или Vengeful Wolf), о которой исследователи Positive Technologies впервые написали в январе 2025 года. Злоумышленники осуществляли атаки на российские компании и отправляли фишинговые письма с прикрепленным вредоносным архивом. В известных инцидентах по почте распространялись Revenge RAT или XWorm. В ходе исследования F6 были выявлены образцы других вредоносных программ из арсенала злоумышленников: Stealerium, DarkTrack, DCRat, AveMaria RAT, VenomRAT. Образцы различных семейств вредоносных программ были обнаружены на одних и тех же устройствах, а также использовали те же домены, что и командный сервер.

Злоумышленники подписывали вредоносное ПО поддельными сертификатами X.509 и использовали омоглифы в именах исполняемых файлов, темах писем и названиях вложений. Недавно они начали применять для исполняемых файлов двойные расширения (.pdf.scr, .pdf.exe, .xsl.scr, .xlsx.scr), продолжая подменять иконки (на Microsoft Office и PDF). В недавней кампании злоумышленники поочередно использовали протекторы Themida и .NET Reactor, а также обфусцированный .NET-дроппер, извлекающий из себя четыре сохраненных упакованных ресурса, каждый из которых соответствует отдельной вредоносной нагрузке. На протяжении всей своей активности злоумышленники использовали Dynamic DNS-домены, которые образовали два непересекающихся кластера: первый – в период с декабря 2022 года по середину 2023 года, второй – с середины 2023 года по настоящее время. Анализ вредоносных рассылок room155 позволил исследователям определить основные цели группы. Это финансовые организации (51%), транспортные компании (16%), организации розничной торговли (10%), промышленные и логистические компании (по 7%), строительные и коммунальные организации (3%), медицинские, туристические и ИТ-компании (по 2%). Конечной целью злоумышленников было шифрование системы жертвы с использованием LockBit 3.0 и последующее требование выкупа. У группы нет своего сайта утечек (DLS).

Атаки Werewolves

Исследователи F6 обнаружили новую волну вредоносных рассылок, инициированных группой Werewolves. Сообщения с якобы досудебными претензиями и вредоносными вложениями отправлялись от имени завода спецтехники, базы отдыха и производителя электрооборудования. Werewolves – группа вымогателей, использующая такие инструменты, как AnyDesk, NetScan, CobaltStrike, Meterpreter и LockBit, и традиционную технику двойного вымогательства. Действует с 2023 года.

Весной 2025 года исследователи обнаружили вредоносную рассылку банкам, промышленным предприятиям, организациям розничной торговли и логистическим компаниям. В июне Werewolves сделала еще одну рассылку промышленным, финансовым, энергетическим и ретейл-компаниям. Для распространения вредоносного ПО группа отправляла электронные письма юридического и финансового характера, используя те же инструменты, что и в предыдущих атаках. Так, в темах июньских писем были указаны «Досудебная претензия», «Досудебное», «Уведомление (досудебное)». Вложение содержало архив с файлом LNK с двойным расширением .pdf.lnk и документ Microsoft Office, в котором эксплуатировалась уязвимость CVE-2017-11882. Злоумышленники использовали для отправки электронных писем тот же домен, что и в предыдущих рассылках – kzst45[.]ru, мимикрирующий под сайт российского производителя спецтехники. Правда, в ходе последних атак они уже использовали новый – mysterykamchatka[.]ru, имитирующий легитимный сайт в доменной зоне .com. Кроме того, злоумышленники снова использовали спуфинг: в одном из писем они подменили адрес отправителя, чтобы письмо выглядело от имени главного бухгалтера российского аэропорта. Конечной вредоносной нагрузкой был Cobalt Strike's Beacon.

Атаки BO Team

Исследователи «Лаборатории Касперского» проанализировали деятельность проукраинской хактивистской группы BO Team (она же Black Owl, Lifting Zmiy и Hoody Hyena), которая нацелена на российские компании. Группа в основном стремится нанести ущерб инфраструктуре жертвы, но иногда промышляет и вымогательством. BO Team впервые заявила о себе в начале 2024 года в Telegram-канале, где обозначила свою позицию в контексте российско-украинского конфликта. Злоумышленники используют фишинговые письма с вредоносными вложениями, которые запускают цепочку заражения с полезной нагрузкой в виде бэкдоров DarkGate, BrockenDoor и Remcos.

BO Team выдает себя за реальную компанию, специализирующуюся на автоматизации технологических процессов, и потому зачастую не вызывает недоверия при взаимодействии с потенциальными жертвами из государственного, технологического и энергетического секторов. Для маскировки отправителя злоумышленники использовали поддельные домены, имитирующие домены легитимных компаний. После получения первоначального доступа к целевым системам они применяли технологию Living off the Land с PowerShell и WMI. Для обеспечения постоянного доступа к скомпрометированной инфраструктуре атакующие использовали различные техники закрепления, в том числе создание задач в планировщике Windows, а для повышения привилегий – ранее скомпрометированные учетные записи, принадлежащие штатным сотрудникам организации. В некоторых случаях использовались легитимные средства удаленного доступа (RDP, SSH, VPN). После компрометации целевых систем BO Team методично уничтожала резервные копии файлов и виртуальную инфраструктуру компании, а также удаляла данные с хостов с помощью утилиты SDelete. Иногда злоумышленники использовали еще и шифровальщик Babuk для Windows, после чего требовали выкуп.

Активность русскоязычных групп

Атаки Void Blizzard

Исследователи Центра анализа угроз Microsoft выявили глобальную активность с использованием облачных сервисов, ассоциированную ими с группой Void Blizzard (она же LAUNDRY BEAR). Кибершпионские операции группы направлены на конкретные организации в различных секторах – это государственные учреждения, предприятия оборонно-промышленного комплекса, транспортные компании, средства массовой информации, неправительственные и медицинские организации главным образом в Европе и Северной Америке.

Обычно использовались учетные данные, полученные, скорее всего, из логов коммерческих инфостилеров. Однако, недавно аналитики Microsoft обнаружили, что с апреля Void Blizzard стала применять более прямолинейную тактику первоначального проникновения – кражу паролей через рассылку фишинговых писем, обманом заставляющих пользователей раскрыть свои учетные данные. В некоторых случаях компрометаций исследователи обнаружили, что атакующие получили доступ к чатам и сообщениям в Microsoft Teams через веб-приложение сервиса.

Атаки с применением PathWiper

Исследователи Cisco Talos обнаружили ранее неизвестный вайпер, получивший название PathWiper. Это вредоносная программа применялась в атаке на украинский объект критической инфраструктуры и уничтожила все данные на целевых системах жертвы. В атаке было задействовано легитимное решение для управления узлами сети. Вероятно, консоль управления решением использовалась для централизованного распространения PathWiper. Более того, тот факт, что на протяжении всей атаки имена файлов и команды, которые вводились на консоли, выглядели похожими на легитимные, указывает на то, что атакующие заранее изучили решение, возможно, в среде жертвы.

По своим разрушительным свойствам PathWiper чем-то схож с HermeticWiper, который использовался против украинских целей. В некоторых публикациях применение HermeticWiper, также известного как FoxBlade, со средней и высокой (публикация 1, публикация 2) долей уверенности приписывают группе Sandworm. Но в отличие от HermeticWiper, который просто сканирует и стирает данные на всех дисках, PathWiper действует более избирательно – перед тем как уничтожить данные, он идентифицирует и проверяет диски.

Атаки Sandworm

В октябре 2024 года исследователи ESET зафиксировали активность группы Sandworm в нескольких энергетических компаниях Украины. По крайней мере в одном случае, атакующие применили на ранних стадиях взлома программу для удаленного мониторинга и управления Atera Agent. За последние шесть месяцев Sandworm стала активнее использовать в своих операциях вредоносные программы для уничтожения данных. Так, в декабре 2024 года, а также в феврале и марте 2025 года группа внедрила в различные украинские организации новый вайпер ZEROLOT. Для его распространения на компьютерах жертв атакующие использовали групповые политики Active Directory. После запуска ZEROLOT удаляет все файлы в подкаталоге C:\Users\ и корневом каталоге на всех дисках, кроме диска C:, файлы с расширениями .dll, .exe и .sys пропускает. Для перезаписи данных файлов программа использует fsutil.exe, после чего удаляет файлы. Вдобавок ZEROLOT стирает физическую разметку дисков посредством DeviceIoControl Windows API.

Атаки Sednit

Согласно отчету ESET, группа Sednit (она же APT28, Fancy Bear и Sofacy), связанная с операцией RoundPress, расширила поле своей деятельности за счет использования в дополнение к Roundcube других почтовых сервисов: Horde, MDaemon и Zimbra. Атакующие рассылали фишинговые письма с XSS-эксплойтами, нацеленные, как правило, на уже устраненные вендором уязвимости. Эксплойты приводили к выполнению вредоносного JavaScript-кода внутри веб-страницы почтового клиента, открытой в браузере. Исследователи выявили несколько вредоносных JavaScript-нагрузок: SpyPress.HORDE, SpyPress.MDAEMON, SpyPress.ROUNDCUBE и SpyPress.ZIMBRA. Большинство из них собирают письма и контактную информацию из почты жертвы, когда вредоносное письмо получено или просмотрено в уязвимом почтовом клиенте. Затем украденные данные передаются на командный сервер.

Исследователи ESET зафиксировали несколько кампаний Sednit против оборонных предприятий в Болгарии и на Украине. Так, в ноябре 2024 года они обнаружили адресованное болгарской организации фишинговое письмо с темой «Путин се стреми Тръмп да приеме руските условия вдвустранните отношения» (Путин пытается добиться от Трампа согласия на российские условия в двусторонних отношениях), отправленное со взломанной почты. В сообщении были выдержки (на болгарском языке) и ссылки на статьи в официальной болгарской газете News.bg. 1 ноября 2024 года исследователи ESET выявили фишинговые письма, нацеленные на украинские компании, эксплуатирующие XSS-уязвимость нулевого дня в почтовом сервере MDaemon, а конкретно при отображении недоверенного HTML-кода в письмах. Исследователи проинформировали вендора об уязвимости 1 ноября 2024 года, и 14 ноября он выпустил исправленную версию ПО. ESET присвоила уязвимости номер CVE-2024-11182.

Восточная Азия

Операция SyncHole

Исследователи «Лаборатории Касперского» с ноября 2024 года отслеживают кампанию группы Lazarus. В ходе атак, направленных против организаций в Южной Корее, используется сложная комбинация стратегии Watering hole и эксплуатации уязвимостей в южнокорейском ПО Cross Ex и Innorix Agent. Кампания, получившая название «Операция SyncHole», затронула минимум шесть организаций, занимающихся разработкой

программного обеспечения, информационными технологиями, финансами, телекоммуникациями и производством полупроводников.

В самой ранней атаке злоумышленники использовали разновидности утилит ThreatNeedle, загрузчика Agamemnon и wAgent. Цепочки выполнения в последующих случаях были полностью обновлены – тогда использовались вредоносные программы SIGNBT и COPPERHEDGE. SIGNBT имела обновленную версию 1.2, ориентированную на загрузку дополнительного вредоносного ПО. У COPPERHEDGE – вредоносной программы, названной так CISA в 2020 году и исторически связанной с кластером DeathNote, обнаружились расширенные возможности в части команд.

В ходе исследования было установлено, что атакующие выполняли некоторые команды через бэкдор COPPERHEDGE для сбора информации о системах организации-жертвы. В основном они вводили команды в интерпретаторе cmd.exe ОС Windows, причем иногда команды были некорректные. Это свидетельствует о том, что злоумышленники все еще вручную проводят разведку для выявления целей. Проанализировав действия злоумышленников в ходе этой кампании, исследователи «Лаборатории Касперского» определили их рабочие часы и сделали вывод, что они, возможно, работают в часовом поясе GMT+9.

Атаки Swan Vector

Исследователи Seqrite Labs обнаружили кампанию, нацеленную на образовательные учреждения и предприятия машиностроительной отрасли на Тайване и в Японии. Кампания проводится с декабря 2024 года и получила название Swan Vector. Она началась с рассылки целевых фишинговых писем с поддельными резюме кандидатов в качестве приманки. Письма содержали вредоносный ZIP-файл с LNK-файлом внутри – он в свою очередь загружал исполняемый файл, инициирующий установку DLL-импланта Pterois. После применения динамического разрешения API и скрытой загрузки соответствующих библиотечных функций Pterois использовал Google Drive в качестве командного сервера и проходил аутентификацию с использованием легитимных учетных данных OAuth для последующего извлечения вредоносной нагрузки, а затем самоуничтожался. Дальше происходила подмена загружаемой DLL (DLL sideloading) и запускался имплант Isurus, который выполнял динамическое разрешение API и запускал зашифрованный шеллкод Cobalt Strike, после чего запускался Cobalt Strike Beacon. По мнению исследователей, с точки зрения тактики Swan Vector схожа с операциями групп APT10, Lazarus и Winnti.

Активность китайскоязычных групп

Атаки Billbug/Lotus Panda

Исследователи Symantec сообщили о новой кампании китайскоязычной группы Billbug (она же Lotus Blossom, Lotus Panda, Bronze Elgin). Кампания длилась с августа 2024 года по февраль 2025 года и была нацелена на несколько организаций в неназванной стране Юго-Восточной Азии. Целями стали министерство, организация по управлению воздушным движением, оператор связи и строительная компания. Также пострадали информационное агентство и компания, занимающая грузовыми авиаперевозками, из двух других стран региона. Эта серия атак является продолжением крупномасштабной операции в Юго-Восточной Азии, начатой еще в октябре 2023 года и впервые публично упомянутой исследователями Symantec в декабре 2024 года.

Группа Billbug активна с 2009 года, но впервые привлекла к себе внимание в июне 2015 года. Тогда исследователи Palo Alto Unit 42 установили ее причастность к целевой фишинговой кампании, в ходе которой эксплуатировалась уязвимость Microsoft Office (CVE-2012-0158) для распространения бэкдора Elise (Trensil), предназначенного для выполнения команд и манипулирования файлами.

В феврале нынешнего года исследователи Cisco Talos установили связь Lotus Panda с атаками на государственные учреждения, производственные, телекоммуникационные и медиакомпании на Филиппинах, Тайване, в Гонконге и во Вьетнаме, с использованием бэкдора Sagerunex. В ходе последней волны атак, о которой сообщили исследователи Symantec, злоумышленники использовали легитимные исполняемые файлы Trend Micro (tmdbglog.exe) и Bitdefender (bds.exe) для подмены вредоносных библиотек DLL (DLL sideloading). Они в свою очередь служили в качестве загрузчиков для расшифровки и запуска вредоносного ПО следующего этапа, внедренного в локально сохраненный файл. Бинарный файл Bitdefender использовался для подмены еще одной библиотеки DLL, которую исследователям не удалось получить. Злоумышленники применяли обновленную версию Sagerunex – программы из арсенала Lotus Panda. Она умеет собирать информацию о целевом хосте, шифровать ее и передавать на внешний сервер. Атаки также сопровождались применением обратного SSH и двух стилеров – ChromeKatz и CredentialKatz, способных извлекать хранящиеся в браузере Google Chrome пароли и куки. Атакующие задействовали общедоступный инструмент Zrok, использовав его для удаленного доступа к внутренним сервисам. Кроме того, они использовали

легитимный инструмент datechanger.exe, способный изменять временные метки файлов.

Атаки Earth Lamia

Исследователи Trend Micro описали активности группы Earth Lamia, которая атакует различные промышленные отрасли в Бразилии, Индии и Юго-Восточной Азии по крайней мере с 2023 года. Изначально группа была сосредоточена на финансовом секторе, потом переключилась на логистические компании и онлайн-ретейлеров, а в последнее время ее жертвами стали ИТ-компании, университеты и правительственные организации. Операции Earth Lamia упоминаются в некоторых исследовательских отчетах: REF0657, STAC6451 и CL-STA-0048.

Злоумышленники как правило используют известные уязвимости SQL-инъекций в веб-приложениях, таких как Apache Struts2, GitLab, WordPress File Upload, JetBrains TeamCity, CyberPanel, SAP NetWeaver Visual Composer и Craft CMS, и применяют sqlmap для получения доступа к серверам целевых организаций. Чтобы избежать обнаружения, Earth Lamia разработала и настроила специальный инструментарий, в том числе ранее недокументированный модульный .NET-бэкдор PULSEPACK и программу для повышения привилегий BypassBoss. Фаза горизонтального перемещения осуществлялась путем загрузки дополнительных инструментов с помощью certutil.exe или powershell.exe. Программы GodPotato и JuicyPotato использовались для повышения привилегий, Fscan и Kscan – для сканирования сети, rakshasa и Stowaway – для создания прокси-туннелей, а schtasks.exe – для закрепления. Earth Lamia внедряла веб-шеллы в веб-приложения, собирала информацию о контроллере домена и учетные данные с помощью nltest.exe и net.exe, создавала учетную запись «Служба поддержки» в группе администраторов и запускала бэкдоры, созданные с помощью фреймворков для пентестов вроде Vshell, Cobalt Strike и Brute Ratel.

Атаки Earth Ammit

Trend Micro проанализировала две волны кампаний, проведенных группой Earth Ammit в период с 2023 года по 2024 год. Первая волна, VENOM, была нацелена преимущественно на поставщиков программного обеспечения, а вторая, TIDRONE, – на военную и спутниковую отрасли.

Trend Micro впервые сообщила о TIDRONE в сентябре 2024 года, подробно описав атаки на производителей дронов на Тайване. В ходе этой кампании злоумышленники использовали ERP-систему и удаленный доступ к

рабочему столу для внедрения бэкдоров CXCLNT и CLNTEND. Далее злоумышленники повышали привилегии, обеспечивали себе постоянное присутствие, отключали антивирусное ПО и занимались кражей информации.

Во время кампании VENOM злоумышленники проникли в верхнее звено цепочки поставок дронов, задействовав главным образом инструментарий с отрытым исходным кодом. Отличительной особенностью кампании являлись эксплуатация уязвимостей веб-серверов для внедрения веб-шеллов, получения доступа для установки RAT и постоянного доступа к скомпрометированным хостам, а также применение инструментов с открытым исходным кодом – REVSOCK и Sliver. Затем злоумышленники использовали украденные учетные данные жертв для проведения атак на звенья нижнего уровня. В этой кампании они также применяли специальные инструменты SCREENCAP (программа для захвата экрана) и VENFRPC (быстрый обратный прокси-сервер), переделанные из утилит, доступных на GitHub.

Жертвы кампаний VENOM и TIDRONE преимущественно находились на Тайване и в Южной Корее и представляли различные отрасли: военную, спутниковую, тяжелую промышленность, технологическую, медиа, здравоохранение. Связь между этими кампаниями обусловлена выбором жертв и инфраструктурой управления. Исследователи Trend Micro отметили, что TTP Earth Ammit схожи с теми же, что используются другой китайскоязычной APT-группой – Dalbit (m00nlight): обе используют одинаковый набор инструментов.

Атаки UNC5221

Исследователи EclecticIQ обнаружили активную эксплуатацию уязвимостей в программе для управления мобильными устройствами Ivanti (CVE-2025-44277 и CVE-2025-44288), позволяющих выполнять удаленный код без аутентификации на доступных из интернета системах. Примечательно, что первые случаи использования этих уязвимостей были зафиксированы в тот же день, когда вендор опубликовал их описание (15 мая 2025 года). С высокой долей уверенности можно говорить о том, что эта кампания была проведена китайскоговорящей шпионской группой UNC5221. Ее деятельность нацелена на организации из ключевых отраслей, включая здравоохранение, телекоммуникации, авиацию, муниципальное управление, финансы и оборонную промышленность, в Европе, Северной Америке и Азиатско-Тихоокеанском регионе. Среди пострадавших организаций оказались немецкий производитель роторной техники, японский производитель автозапчастей, американские производители медицинского

оборудования и огнестрельного оружия. Злоумышленники применили рефлективную загрузку вредоносного ПО на Java для выполнения команд, внедряли KrustyLoader для загрузки зашифрованных имплантов Sliver, а также использовали жестко закодированные учетные данные от MySQL для извлечения конфиденциальной информации, такой как данные из LDAP и токены Office 365. Дополнительно злоумышленники применяли инструменты вроде FRP (быстрый обратный прокси-сервер) и бэкдора Auto-Color для Linux для разведки и обеспечения постоянного доступа к скомпрометированным системам.

Атаки PurpleHaze/ShadowPad

Исследователи SentinelLabs в апреле раскрыли подробности подготовки атаки на саму SentinelOne, обнаруженной в октябре 2024 года. Исследованный кластер получил название PurpleHaze и был отнесен к активностям групп APT15 и UNC5174. В июне исследователи сообщили об атаке на своего поставщика IT-оборудования в рамках масштабной кампании с использованием модульной вредоносной платформы ShadowPad. SentinelLabs заявляет о пересечениях целей этих атак с атаками PurpleHaze. В период с июня 2024 года по март 2025 года более 70 организаций по всему миру были скомпрометированы образцами ShadowPad, обфусцированными с помощью ScatterBrain. Пострадавшие организации относятся к государственной, производственной, финансовой, телекоммуникационной и исследовательской сферам.

Исследователи SentinelLabs подозревают, что наиболее распространенным первоначальным вектором атаки в ходе глобальной операции ShadowPad было использование шлюзов безопасности Check Point, что согласуется с предыдущими исследованиями на эту тему. Кроме того, была обнаружена коммуникация с командными серверами ShadowPad на базе серверов Fortinet Fortigate, Microsoft IIS, SonicWall и CrushFTP, что тоже указывает на возможную эксплуатацию этих систем.

При анализе атаки ShadowPad на государственное учреждение в Южной Азии в июне 2024 года выяснилось, что вредоносное ПО было доставлено жертве посредством PowerShell. Кроме того, злоумышленники внедрили программу для удаленного доступа с открытым исходным кодом Nimbo-C2 и PowerShell-скрипт, который выполняет рекурсивный поиск конфиденциальных пользовательских документов, архивирует их в защищенный паролем 7-Zip и извлекает их. Google Threat Intelligence связала активность ShadowPad, обфусцированного с помощью ScatterBrain, с китайскоязычной группой APT41.

Активность, связанная с Ближним Востоком

Атаки Lemon Sandstorm

Исследователи FortiGuard Incident Response сообщили о продолжительной кампании группы, финансируемой иранским правительством, против объектов критической инфраструктуры на Ближнем Востоке. Кампания продолжалась как минимум с мая 2023 года по февраль 2025 года, хотя следы компрометации отсылают к маю 2021 года. Исследователи связали эту активность с группой Lemon Sandstorm (ранее Rubidium), которая также отслеживалась под названиями Parisite, Pioneer Kitten и UNC757. Атака проводилась в четыре этапа, причем по ходу того как жертвы реализовали контрмеры, инструментарий злоумышленников менялся.

Группа использовала украденные учетные данные для доступа к SSL/VPN-серверу жертвы, разместила веб-шеллы на общедоступных серверах, внедрила бэкдоры Havoc, HanifNet и HXLibrary для получения долгосрочного доступа. Далее она внедрила дополнительные веб-шеллы и бэкдор NeoExpressRAT, используя инструменты plink и Ngrok, чтобы глубже проникнуть в сеть, украсть сообщения электронной почты жертвы и осуществить горизонтальное перемещение в пределах виртуальной инфраструктуры. В конце 2024 года группа внедрила новые веб-шеллы и два дополнительных бэкдора, MeshCentral Agent и SystemBC, в ответ на усилия компании-жертвы по локализации инцидента. После этого Lemon Sandstorm предприняла попытку повторного входа в сеть, эксплуатируя уязвимости Biotime (CVE-2023-38950, CVE-2023-38951 и CVE-2023-38952) и проведя фишинговую атаку на 11 конкретных сотрудников, чтобы получить их учетные данные Microsoft 365.

В числе семейств вредоносного ПО и инструментов с открытым исходным кодом, задействованных в атаке: HanifNet, HXLibrary, CredInterceptor, RemoteInjector, RecShell, NeoExpressRAT, DropShell, DarkLoadLibrary. Проанализировав действия злоумышленников, исследователи FortiGuard Incident Response пришли к выводу, что основной целью была OT-сеть жертвы. Они нашли признаки присутствия злоумышленников в изолированном сегменте сети, где были размещены OT-системы. Однако доказательств проникновения нарушителей непосредственно на OT-системы не обнаружили. Большая часть вредоносной активности была связана с ручными операциями, учитывая орфографические ошибки и регулярный график активности. Во время проникновения злоумышленники использовали цепочку прокси-серверов и кастомные импланты для обхода сегментации и перемещения внутри сети. На более поздних этапах

злоумышленники последовательно комбинировали четыре разных прокси-инструмента для получения доступа к внутренним сегментам сети, по всей видимости для увеличения устойчивости к обнаружению и блокированию.

Атаки Stealth Falcon

Исследователи Check Point зафиксировали попытку кибератаки на крупную оборонную компанию в Турции. По их мнению, за этой атакой стоит Stealth Falcon (она же FruityArmor) – APT-группа, действующая по меньшей мере с 2012 года и известная сложными операциями кибершпионажа. Она отличается тем, что приобретает уязвимости нулевого дня и использует специально разработанное вредоносное ПО для атак на объекты по всему Ближнему Востоку. В ходе указанной кампании злоумышленники использовали ранее неизвестную технику запуска файлов, размещенных на подконтрольном им WebDAV-сервере. Это достигалось путем замены рабочего каталога iediagcmd.exe – легитимной утилиты Windows на URL, ведущий на вредоносный WebDAV-сервер, что приводило к загрузке вредоносной программы вместо легитимной route.exe из папки system32. Microsoft присвоила уязвимости номер CVE-2025-33053 и выпустила исправление 10 июня 2025 года. Эксплуатация этой уязвимости позволила злоумышленникам доставить Horus Agent – специальный имплант, построенный на кроссплатформенном C2-фреймворке с открытым исходным кодом Mythic. Он представляет собой усовершенствованную версию ранее использовавшегося группой кастомного импланта Apollo.

Атаки MuddyWater

Исследователи ESET изучили январские и февральские кампании группы MuddyWater. Они примечательны тем, что имели признаки сотрудничества с группой Lyceum (подразделение OilRig), проникновение которой в системы производственной компании в Израиле было зафиксировано сразу после компрометации MuddyWater. MuddyWater получила первичный доступ в результате целевой фишинговой рассылки со ссылкой на установщик программы для удаленного мониторинга и управления Syncro. Позже она установила аналогичную программу PDQ (сегодня именно ее предпочитает использовать MuddyWater). Далее оператор вручную вводил команды Windows Shell, создав при этом много шума с невысокой эффективностью в достижении целей. Наконец, MuddyWater внедрила Mimikatz с помощью кастомного загрузчика и инжектора. В тот же день, вероятно, используя учетные данные, полученные с помощью Mimikatz, Lyceum получила контроль над сетью организации. Ранее исследователи ESET отмечали, что

MuddyWater, возможно, играет роль брокера доступа для других проиранских групп.

В другой кампании MuddyWater использовала инжектор, который загружает бэкдор в память и пытается обойти защитные решения. Кампания длилась два месяца (с сентября по октябрь 2024 года) и была направлена на организации в инженерном и государственном секторах в Израиле.

Киберкриминал и прочее

Атаки с использованием ClickFix

Исследователи Proofpoint раскрыли несколько кампаний, инициированных проправительственными атакующими, в ходе которых впервые был применен метод социальной инженерии ClickFix. При этом пользователю атакованной системы показываются диалоговые окна с инструкциями по копированию, вставке и запуску команд якобы для исправления технической проблемы, но на самом деле вредоносных. С конца 2024 года по начало 2025 года ClickFix использовали группы TA427, TA450, UNK_RemoteRogue и TA422 (она же Sofacy, APT28 и Fancy Bear).

Исследователи Proofpoint зафиксировали, как 13 и 14 ноября 2024 года TA450 целенаправленно отправила фишинговые письма на английском языке по меньшей мере 39 организациям. Сообщение было замаскировано под обновление безопасности от Microsoft с темой: «Требуется срочно обновить систему безопасности – сделайте это немедленно», чтобы убедить пользователей выполнить ряд действий по устранению уязвимости в системе безопасности. Злоумышленникам удалось убедить жертв запустить PowerShell от имени администратора, а затем скопировать и запустить команду, указанную в теле письма. Команда инициировала установку программного обеспечения Level для удаленного управления и мониторинга. TA450 вела свою деятельность на Ближнем Востоке, преимущественно в ОАЭ и Саудовской Аравии, однако объектами становились и цели в других регионах. Среди жертв были транспортные, коммунальные, энергетические компании, но наибольшую популярность у злоумышленников имели финансовые и государственные организации.

Исследователи Proofpoint также изучили целенаправленную кампанию, в ходе которой была задействована скомпрометированная инфраструктура для отправки 10 сообщений сотрудникам двух организаций, связанных с крупным производителем оружия. Это была кампания, предположительно, российской группы UNK_RemoteRogue. Электронные письма содержали

вредоносную ссылку якобы на документ Microsoft Office с названием «RSVP Office – Створюйте, редагуйте документи та діліться ними в Інтернеті» (Ответьте, пожалуйста, на вопросы, которые помогут вам разобраться с ними в интернете). После перехода по ссылке открывалась имитирующая документ Microsoft Word HTML-страница с инструкцией в стиле ClickFix на русском языке по копированию кода из браузера в свой терминал. Веб-страница содержала ссылку на видеоурок на YouTube о том, как запустить PowerShell. Выполнение в терминале команды запускало вредоносный JavaScript, который затем выполнял код PowerShell, ведущий на C2-фреймворк Empire.

Атаки CrazyHunter

Исследователи Trend Micro представили анализ атак новой группы вымогателей CrazyHunter, которые нацелены на критически важные сектора на Тайване, включая здравоохранение, образование и промышленность. Вымогатели используют в ходе своей операции инструменты с открытым исходным кодом с GitHub, в том числе ZammoCide для остановки работы AV/EDR, SharpGPOAbuse для повышения привилегий и горизонтального перемещения, а также написанный на языке Go шифровальщик с открытым исходным кодом Prince. Вредоносная программа применяет алгоритмы шифрования ChaCha20 и ECIES для надежного шифрования файлов. Злоумышленники доработали ее, чтобы она добавляла к зашифрованным файлам расширение .Hunter. После она оставляет записку с требованием о выкупе Decryption Instructions.txt", меняет обои рабочего стола на компьютерах жертвы и требует оплаты.

Предупреждение CISA об атаках на нефтегазовый сектор

Агентство по кибербезопасности и защите инфраструктуры США (CISA) выпустило предупреждение об активности злоумышленников, нацеленной на АСУ и SCADA внутри критической инфраструктуры Соединенных Штатов, преимущественно в энергетической отрасли и секторе транспортировки нефтепродуктов и природного газа. Согласно документу, эти атаки часто строятся на простейших техниках проникновения. Однако несоблюдение основных правил кибергигиены и наличие незащищенных активов могут привести к серьезным последствиям вроде порчи данных, изменения конфигурации, нарушения производственных процессов в особо тяжелых случаях. CISA, Федеральное бюро расследований, Агентство по охране окружающей среды и Министерство энергетики опубликовали список первоочередных мер для снижения риска компрометации. Подробное руководство призывает организации принять меры, такие как

ограничение доступа к интернету для устройств, непосредственно задействованных в технологическом процессе, изменение паролей по умолчанию, защита инструментов удаленного администрирования и сегментация технологических сетей от корпоративных ИТ-инфраструктур. Подробностей инцидентов и связанных с ними акторов CISA не предоставила.

Атаки с внедрением NetBird

Компания Trellix сообщила о фишинговой кампании неизвестных атакующих, нацеленной на финансовых директоров и других руководителей банков, энергетических, страховых и инвестиционных компаний в Европе, Африке, Канаде, на Ближнем Востоке и в Южной Азии. Атака начиналась с электронного письма якобы от рекрутера Rothschild & Co, предлагающего «стратегическую возможность» трудоустройства. В письме была ссылка на страницу на Firebase, замаскированную под брошюру, защищенную специальной капчей с математическим примером. После введения ответа жертве предлагалось загрузить ZIP-файл, содержащий скрипт VBS. Запуск скрипта инициировал автоматическую установку двух легитимных MSI-пакетов – NetBird и OpenSSH, а также создание скрытого аккаунта локального администратора и включение RDP, что обеспечивало злоумышленнику зашифрованный канал для удаленного управления системой. NetBird незамедлительно приняла меры – закрыла доступ злоумышленникам к своей платформе, чтобы исключить ее использование в указанной вредоносной кампании.

Атаки Hazy Hawk

Исследователи Infoblox изучили кампании группы Hazy Hawk, которая захватывает забытые корпоративные ресурсы в облачных инфраструктурах, такие как корзины S3 и конечные точки служб для виртуальной сети Azure, зарезервированные за крупными организациями, в том числе правительствами, университетами и корпорациями вроде Honeywell и Unilever. Захват осуществлялся путем эксплуатации устаревших и более некорректных DNS-записей, в частности записей CNAME, указывающих на ресурсы во внешних облачных сервисах, более не зарезервированных за организацией. Атакующие таким образом получали контроль над поддоменами доверенного домена, которые после использовали для распространения мошеннических сообщений, вредоносного контента и push-уведомлений через сложные многоуровневые цепочки переадресаций и распределения трафика. Исследователи Infoblox отметили, что такие сайты используются для реализации различных мошеннических схем, включающих

фиктивную техподдержку, ложные антивирусные предупреждения и продвижение фейковых стримингов и порносайтов.

Атаки через Microsoft Exchange Server

Исследователи Positive Technologies изучили серию атак с внедрением кейлоггера в страницу веб-аутентификации скомпрометированного Microsoft Exchange Server. Подобная атака, с тем же кодом кейлоггера, была зафиксирована в мае 2024 года. Исследователям удалось обнаружить образцы вредоносного кода, которые были разделены на два типа: те, что записывают собранные данные в локальном файле, к которому есть доступ извне, и те, что сразу отправляют собранные данные на внешний сервер. В ходе расследования было выявлено около 65 жертв в 26 странах, причем большинство скомпрометированных серверов были обнаружены в государственных организациях, а также в ИТ-, промышленных и логистических компаниях.

Атаки Anubis

Исследователи Trend Micro сообщили о новой операции группы Anubis, распространяющей вредоносное ПО по принципу «Программа-вымогатель как услуга» (Ransomware-as-a-Service, RaaS). Операция сочетает в себе шифрование и уничтожение файлов.

Anubis завела аккаунт в X (ранее Twitter) в декабре 2024 года, и к началу лета 2025 на ее сайте утечек значилось семь жертв. Деятельность группы нацелена на ряд отраслей, включая здравоохранение, машиностроение и строительство, в Австралии, Канаде, Перу, США и других странах. Среди последних образцов вредоносных программ в арсенале группы был вайпер, который, по мнению исследователей, использовался для усиления давления на жертв, чтобы заставить их быстрее выплачивать выкуп. При запуске вайпер удаляет все содержимое файлов, уменьшая их размер до 0 КБ, но сохраняя имена и структуру каталогов. Жертва по-прежнему видит все эти файлы, но их содержимое безвозвратно уничтожено.

Атаки начинались с рассылки фишинговых писем с вредоносными ссылками или вложениями. Анализ показал, что Anubis поддерживает несколько команд при запуске, включая повышение привилегий, исключение определенных каталогов и указание путей для шифрования. По умолчанию исключаются критические системные и программные каталоги. Программа-вымогатель удаляет теневые копии томов и завершает процессы и службы, которые могут помешать шифрованию. В схеме шифрования используется ECIES (Elliptic Curve Integrated Cryptography – криптография на основе

эллиптических кривых), имеющая некоторое тактическое сходство в имплементации EvilByte и Prince. К имени каждого зашифрованного файла добавляется расширение .anubis, а в соответствующие каталоги помещается HTML-уведомление с требованием выкупа. Кроме того, шифровальщик пытается изменить обои рабочего стола на компьютере жертвы.

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