APT- и финансовые атаки на промышленные организации во втором квартале 2024 года

03.10.2024 Version 1.0

Этот документ содержит обзор сообщений об APT- и финансовых атаках на промышленные предприятия, информация о которых была раскрыта во втором 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 кратко изложили основные факты, а также привели полученные исследователями результаты и выводы, которые могут быть полезны специалистам, занимающимся практическими вопросами кибербезопасности промышленных предприятий.

Второй квартал 2024 оказался богат на интересные технические подробности раскрытых атак на промышленные организации. Продвинутые злоумышленники вновь и вновь демонстрируют нешаблонный подход к решению своих задач. Создание фейковых профилей в социальных сетях и бутафорских макетов целых компаний, чтобы втереться в доверие к потенциальной жертве, мы видели и ранее, а вот разработка полноценного ИТ-продукта, например, видеоигры — танкового симулятора с трояном внутри — это уже что-то новое. Поистине, не пожалели сил и средств на подготовку.

Нередко злоумышленникам помогают и разработчики средств защиты. Особенно велики масштабом провалы, когда решение возникает не как естественный ответ вызову безопасности, а по формальному требованию, когда оно продиктовано внешнеполитическими причинами и появляется в силу конъюнктурных обстоятельств, по сложившейся традиции или — как это случилось в Южной Корее — в результате смешения сразу всех перечисленных факторов. Злоумышленники давно начали пользоваться хаосом в требуемых для работы с клиентскими порталами местных банков «приложений для безопасности» от корейских разработчиков. Интересным объектом атаки и способом распространения вредоносного ПО становится WIZVERA VeraPort — приложение-оркестратор для помощи в установке этих самых «приложений для безопасности». И если ранее этот вектор использовался в основном в атаках на банки и их клиентов, то теперь жертвой стали посетители сайта ассоциации, имеющей отношение к строительному сектору.

Читая отчеты команд исследователей, одновременно и любопытно, и тревожно наблюдать, как ландшафт угроз промышленным предприятиям эволюционирует в соответствии с нашими прогнозами. Злодеи меняют цели атак, ломая традиционные представления о своем modus operandi. Финансово мотивированные группы включаются в сферу внешнеполитических противостояний и подключаются к хактивизму, нацеленная на морскую логистику APT атакует не только офисные и портовые системы, но и судна, а АСУТП внезапно становятся входной

точкой в атаках, нацеленных не на производственные активы, а на корпоративные ресурсы и офисные системы, — дотянуться до них из технологической сети через разработанный «домашним» вендором, не сильно озабоченным вопросами безопасности, продукт для АСУ становится проще, чем напрямую из интернета.

Юго-Восточная Азия и Корея

Атаки Andariel

Исследователи AhnLab Security Intelligence Center (ASEC) обнаружили атаки группы Andariel (она же Onyx Sleet), нацеленные на образовательные учреждения, производственные и строительные предприятия в Южной Корее. Злоумышленники использовали те же инструменты, что и в предыдущих атаках, включая кейлоггер, инфостилер, прокси-инструменты и бэкдор Nestdoor. Дополнительно в их арсенале появился новый бэкдор, названый Dora. Dora RAT — относительно простая вредоносная программа, которая поддерживает обратную оболочку и загрузку/выгрузку файлов.

Атаки Kimsuky

В декабре 2023 года компания ESET обнаружила вредоносное ПО Kimsuky на нескольких компьютерах, принадлежащих строительной организации в Южной Корее. Анализ атаки показал, что вредоносное ПО было загружено и запущено сотрудниками на скомпрометированных серверах организации, на которых работало решение WIZVERA VeraPort. По данным ESET, атака продолжалась до января 2024 года. Вредоносное ПО было доступно для загрузки только в определенные временные рамки. За пределами этих временных рамок со скомпрометированных серверов загружались легитимные бинарные файлы. Это было подтверждено в отчете AhnLab, опубликованном в феврале 2024 года. Кроме того, AhnLab подсчитала, что общее количество машин, загрузивших со скомпрометированных серверов вредоносное ПО, составило более 3000.

В середине 2023 года группа Kimsuky использовала вредоносное ПО AlphaSeed, написанное на языке Go, а также вредоносный прокси. В течение оставшейся части 2023 года и начала 2024 года Kimsuky продолжили тенденцию к разработке новых образцов вредоносного ПО на языке Go. В частности, различные вендоры безопасности описали и назвали TrollAgent, Endoor и Nikidoor. Исследователи ESET связывают новое вредоносное ПО с кластером Kimsuky AppleSeed.

Согласно отчету исследователей Blackberry, группа Kimsuky атаковала производителя оружия в Западной Европе в ходе сложной кампании кибершпионажа. Злоумышленники использовали бренд General Dynamics в качестве приманки в фишинговом письме, содержащем вредоносный файл JavaScript. Он декодирует файл PDF-приманки и исполняемую библиотеку, которая представляет собой новый инструмент шпионажа, содержащий функции для удаленного выполнения программ атакующими.

Атаки с использованием загрузчика SmallTiger

Центр разведки безопасности AhnLab (ASEC) обнаружил случаи, в которых для атак на южнокорейские предприятия, включая оборонных подрядчиков, производителей автомобильных запчастей и производителей полупроводников, использовался загрузчик SmallTiger. Метод первоначального доступа не был определен, но злоумышленник распространил SmallTiger в системах компаний во время фазы бокового перемещения. Атаки впервые были замечены в ноябре 2023 года. Злоумышленник эксплуатировал программы для обновления программного обеспечения компаний во время фазы распространения по сети жертвы. В конце устанавливался бэкдор DurianBeacon, штамм вредоносного ПО, обнаруженный в прошлых атаках группы Andariel. Тот же злоумышленник возобновил атаки в феврале 2024 года, и конечное распространяемое вредоносное ПО было заменено на SmallTiger. Исследователи полагают, что изучаемые атаки с SmallTiger также связаны с группой Kimsuky. По состоянию на май 2024 года вредоносное ПО все еще использовалось в атаках.

Атаки Moonstone Sleet

Новая группировка, которую исследователи Microsoft назвали Moonstone Sleet (ранее она отслеживалась как Storm-1789), нацелена на отдельных лиц и организации в секторах программного обеспечения, ИТ, образования и оборонной промышленности, используя тактику социальной инженерии. Злоумышленники создали поддельные компании, которые взаимодействовали с потенциальными целями по электронной почте и в социальных сетях, использовали троянизированные версии легитимных инструментов (таких как PuTTY) и вредоносные пакеты npm и даже разработали полнофункциональную игру в танки, которая дополнительно загружает кастомный вредоносный dll-загрузчик, отслеживаемый Microsoft как YouieLoad. Основная цель группы — шпионаж, но она использует и более прямые схемы монетизации. Microsoft заметил, что в апреле 2024 года

Moonstone Sleet загрузила новый вариант кастомного вымогателя, который получил название FakePenny, в компанию, которую она скомпрометировала в феврале. По словам исследователей, Moonstone Sleet изначально пересекалась с Diamond Sleet, но позже перешла на собственную инфраструктуру и атаки, зарекомендовав себя как отдельный субъект угроз.

Атаки с использованием Xctdoor

Центр разведки безопасности AhnLab (ASEC) выявил атаку, нацеленную на южнокорейские компании в оборонной и производственной отраслях с использованием вредоносного ПО Xctdoor. В одном случае злоумышленники проникли в системы, нацелившись на сервер обновлений определенного корейского решения по планированию ресурсов предприятия (ERP). Они внедрили вредоносный код для запуска dll-файла по определенному пути в программу обновления решения ERP неназванного корейского вендора. Этот метод похож на случай, произошедший в 2017 году, когда группа Andariel использовала такой же файл для установки бэкдора HotCroissant. В другом случае был атакован уязвимый веб-сервер с целью распространения вредоносного ПО.

Атаки LilacSquid

Ранее недокументированная кибершпионская группировка, названная Cisco Talos LilacSquid, была связана с целевыми атаками в рамках кампании по краже данных, по крайней мере с 2021 года. Целями являются организации информационных технологий, создающие программное обеспечение для исследовательского и промышленного секторов в США, энергетические компании в Европе и фармацевтический сектор в Азии. Известно, что цепочки атак либо эксплуатируют общеизвестные уязвимости для взлома серверов приложений, доступных из интернета, либо используют скомпрометированные учетные данные RDP для доставки набора инструментов с открытым исходным кодом и кастомного вредоносного ПО. Наиболее отличительной чертой кампании является использование инструмента удаленного управления с открытым исходным кодом под названием MeshAgent, который доставляет кастомизированную версию Quasar RAT под кодовым названием PurpleInk. В случаях заражения с использованием скомпрометированных учетных данных RDP группировка решила либо развернуть MeshAgent, либо использовать загрузчик на основе .NET, получивший название InkLoader, для доставки PurpleInk. Cisco Talos обнаружила в атаках злоумышленников еще один инструмент под названием InkBox для развертывания PurpleInk до переключения на InkLoader.

Использование MeshAgent примечательно, поскольку ранее его видели в арсенале Andariel — ответвления Lazarus. Другое совпадение с Andariel/Lazarus обнаружено в использовании инструментов туннелирования для поддержания вторичного доступа — так, LilacSquid развертывает Secure Socket Funneling для создания канала связи со своей инфраструктурой.

Атаки Transparent Tribe

Согласно исследователям BlackBerry, группировка Transparent Tribe (также известная как APT36, ProjectM, Mythic Leopard, Earth Karkaddan) несет ответственность за атаки с использованием кроссплатформенного вредоносного ПО, написанного на Python, Golang и Rust, совершенные с конца 2023 года по апрель 2024 года, нацеленные на индийское правительство, оборонный и аэрокосмический секторы. Примечательной особенностью фишинговой кампании группировки является использование популярных онлайн-сервисов, включая Discord, Google Drive, Slack и Telegram, для доставки вредоносных полезных нагрузок в виде вредоносных ISO, ZIP-архивов или ссылок. Исследователи также обнаружили используемый группировкой новый скомпилированный на Golang шпионский инструмент «все в одном», который может находить и извлекать файлы с популярными расширениями файлов, делать снимки экрана, загружать и скачивать файлы и выполнять команды. Исследователи также наблюдали распространение скрипта-загрузчика на Python, скомпилированного в двоичные ELF-файлы.

Активность китайскоязычных групп

Атаки APT31

После публикации в марте обвинительного заключения Министерства юстиции США в отношении семи хакеров, связанных с APT31 (также известной как BRONZE VINEWOOD, Judgment Panda и Zirconium) исследователи проанализировали его. Они считают, что заключение не противоречит ранее существовавшим представлениям исследователей о профессиональной деятельности APT31 и предположениям относительно сотрудничества между государственными и частными китайскими организациями в кибероперациях. APT31 нацелилась на известные организации в западном мире. Список включает правительственные, оборонные и промышленные организации, такие как американская

сталелитейная компания и различные компании в аэрокосмическом секторе. Заключение дает представление об интересах группы, начиная от внешней разведки и заканчивая кражей коммерческих секретов и финансовых данных. Более того, исследователи полагают, что тот факт, что записи данных о звонках «миллионов американцев» были получены злоумышленниками, предполагает взлом по крайней мере одного американского поставщика телекоммуникационных услуг.

Атаки Mustang Panda

В первом квартале 2024 года исследователи ESET выявили наличие загрузчиков Korplug китайскоязычной APT-группы Mustang Panda (также известной как Stately Taurus, Bronze President, Earth Preta, HoneyMyte, Camaro Dragon, RedDelta) в компьютерных системах, принадлежащих компаниям по грузоперевозкам в Норвегии, Греции и Нидерландах, включая те, что, по-видимому, находились на борту самих грузовых судов.
Те же самые экземпляры вредоносного ПО использовались в предыдущих кампаниях Mustang Panda, что в целом не характерно для APT. В некоторых случаях первоначальный дроппер, по-видимому, был запущен с USB-накопителя. Некоторые из образцов, развернутых в компаниях по грузоперевозкам, имеют недействительные подписи Authenticode и, вероятно, использовали подмену порядка поиска DLL-файлов для старой версии Nero WaveEditor. Одна недействительная цифровая подпись была скопирована из двоичного файла, легитимно подписанного неким Клаасом Некеманом (Klaas Nekeman). В другом образце использовалась подпись, скопированная из двоичного файла, легитимно подписанного AVG Technologies USA — фирмой, специализирующейся на компьютерной безопасности.

Атаки RedJuliett

Исследователи Insikt Group выявили кибершпионскую деятельность группы RedJuliett с ноября 2023 года по апрель 2024 года, нацеленную на правительственные, академические, технологические (в особенности на производителей электроники) организации и дипломатические ведомства на Тайване. Группа также нацелилась на организации в Гонконге, Малайзии, Лаосе, Южной Корее, США, Джибути, Кении и Руанде. Для первоначального доступа RedJuliett использовала уязвимости в брандмауэрах, VPN и балансировщиках нагрузки. Группа также использовала SQL-инъекции и уязвимости обхода каталогов. Она также поднимала клиент-серверный или сервер-серверный (мост) VPN-тоннель на SoftEther VPN в сетях жертв.

Кроме того, атакующие исследовали инфраструктуру жертвы и попытались атаковать ее сервисы с помощью сканеров безопасности веб-приложений Acunetix. После первичного проникновения злоумышленники использовали веб-оболочки с открытым исходным кодом и эксплуатировали уязвимость повышения привилегий в операционной системе Linux. Активность RedJuliett пересекается с активностью Flax Typhoon и Ethereal Panda.

Атаки UNC3886

В последние годы группа, отслеживаемая Mandiant как UNC3886, использовала общедоступные руткиты с открытым исходным кодом под названиями Reptile и Medusa, чтобы скрытно присутствовать в виртуальной инфраструктуре VMware ESXi. Злоумышленники также использовали кастомное вредоносное ПО, такое как Mopsled и Riflespine. В качестве C2 были выбраны GitHub и Google Drive. Злоумышленники атаковали организации в правительственном, телекоммуникационном, технологическом, аэрокосмическом, оборонном и коммунальном секторах в Северной Америке, Юго-Восточной Азии и Океании, а также Европе, Африке и других странах Азии. Группа эксплуатировала уязвимости в FortiOS (CVE-2022-41328) и VMware (CVE-2022-22948, CVE-2023-20867), включая уязвимость нулевого дня в VMware vCenter (CVE-2023-34048).

Активность, связанная с Ближним Востоком

Атаки POLONIUM

Исследователи ESET заметили, что в ноябре 2023 года, группа POLONIUM, чьи действия, по мнению исследователей, коррелируют с интересами «Хезболлы», использовала Python-бэкдор MegaPy в атаках на четыре израильских организации в сфере технологий и социальных услуг.
Для размещения CnC и хранилища украденных данных были выбраны MEGA и Nextcloud. Интересно, что для эксфильтрации данных использовался протокол WebDAV. Затем, в январе 2024 года, группа POLONIUM развернула обновленную версию Python-бэкдора для атак на строительные, производственные и медицинские компании в Израиле.
В ней использовались зашифрованые полезные нагрузки, содержащие настраиваемый для каждой жертвы контент, вероятно, чтобы усложнить обнаружение атаки и отслеживание вредоносного инструментария исследователями. Во время этой кампании POLONIUM сменили хостинг CnC на Supabase и Backendless. В одном случае хостинг первоначальной полезной нагрузки был выполнен на домене, использующем типосквоттинг: yutube.com[.]de.

Атаки MuddyWater

С конца октября 2023 года исследователи наблюдали значительное увеличение использования APT-группой MuddyWater (она же Mango Sandstorm, Boggy Serpens) установочных пакетов для легитимных инструментов RMM (удаленный мониторинг и управление) Atera Agent и Tactical RMM. Для этого злоумышленникам потребовались скомпрометированные учетные записи электронной почты корпоративных и частных пользователей. Для размещения этих установщиков RMM были выбраны бесплатные платформы хостинга файлов (так же, как в прошлом, с другими RMM). Жертвы загружали эти файлы, обращаясь по ссылкам в фишинговых письмах. Кроме того, исследователи наблюдали загрузки вредоносной DLL с использованием ключа реестра AutodialDLL. В этой схеме выполняемый через запланированное задание PowerShell-скрипт злоумышленников прописывал вредоносную библиотеку в ключ реестра, запускал Internet Explorer (в контексте которого загружалась библиотека и выполнялся ее код), после чего менял значение реестра на предыдущее, чтобы избежать множественных вызовов импланта (библиотека, прописанная в AutodialDLL грузится в контекст каждого процесса, использующего WinSock2, при попытке его подключения к интернету).

Группа MuddyWater нацелилась на различные организации в Израиле, Индии, Алжире, Турции, Италии и Египте. На основании учетных записей, использованных для регистрации Atera Agents, и проанализированных электронных писем исследователи полагают, что в период с октября 2023 года по апрель 2024 года MuddyWater были нацелены на следующие секторы: авиакомпании, ИТ-компании, телекоммуникации, фармацевтика, автомобилестроение, логистика, путешествия и туризм, агентства по трудоустройству/иммиграции, а также малый бизнес.

Активность русскоязычных групп и цели в России

Атаки Sandworm

Исследователи лаборатории WithSecure наблюдали, что ранее не документированный бэкдор под названием Kapeka использовался в атаках на цели в Центральной и Восточной Европе по крайней мере с середины 2022 года. Kapeka функционирует как универсальный бэкдор, предоставляя инструментарий как для первоначальных фаз атаки, так и для долгосрочного

доступа в инфраструктуру жертвы. Kapeka включает в себя дроппер, который загружает и выполняет компонент бэкдора на целевом компьютере, после чего он удаляется. Исследователи обнаружили совпадения между атаками с использованием Kapeka, программы-вымогателя Prestige и GreyEnergy, что позволяет предположить, что Kapeka является новым дополнением к набору инструментов Sandworm (он же APT44 и Seashell Blizzard). В феврале Microsoft обнаружил бэкдор с похожими на Kapeka характеристиками и назвал его KnuckleTouch. WithSecure подтвердила Recorded Future News, что KnuckleTouch и Kapeka — это один и тот же бэкдор. WithSecure заявила, что обнаружила следы Kapeka в середине 2023 года при анализе атаки на эстонскую логистическую компанию, которая произошла в конце 2022 года.

Согласно отчету, опубликованному 19 апреля группой реагирования на компьютерные чрезвычайные ситуации Украины (CERT-UA), хакеры использовали несколько новых и ранее уже известных вариантов вредоносного ПО для заражения около 20 поставщиков электроэнергии, воды и отопления в 10 регионах страны в марте. Во время последних атак на украинскую критическую инфраструктуру группа использовала бэкдор Kapeka. CERT-UA также выявила новые варианты Kapeka на базе Linux, разработанные Sandworm и названные Biasboat. Инжектор полезной нагрузки для Linux, использующий ptrace API, был назван Loadgrip. Biasboat и Loadgrip были установлены на украинских Linux-устройствах, предназначенных для автоматизации технологических процессов на критически важных объектах. На скомпрометированных Linux АСУТП-компьютерах работало «специальное программное обеспечение» неназванного украинского разработчика, в котором были уязвимости и бэкдоры. Агентство подтвердило, что по крайней мере в трех случаях первоначальная компрометация коррелирует с первой установкой этого программного обеспечения. Это говорит о том, что злоумышленники либо эксплуатировали уязвимости в нем, либо скомпрометировали поставщика и использовали его доступ к целевым системам. Скомпрометированные системы объектов критической инфраструктуры затем использовались для горизонтального перемещения в корпоративные сети предприятий. Злоумышленники также развернули вредоносное ПО Gossipflow — инструмент туннелирования, обеспечивающий функциональность SOCKS5 прокси-сервера, который использует библиотеку мультиплексоров Yamux на компьютерах под управлением ОС Windows. По словам CERT-UA, Sandworm использовал Gossipflow с 2022 года — во время атак на украинские объекты водоснабжения с применением вайпера SDELETE. По мнению исследователей, среди факторов, которые привели к описанным в отчете атакам, было отсутствие изоляции серверов и низкий уровень зрелости безопасности поставщиков «специального программного обеспечения».

Атаки Forest Blizzard/STRONTIUM/Fancy Bear

Исследователи Microsoft Threat Intelligence опубликовали результаты своего исследования вредоносного ПО, разработанного группой Forest Blizzard (также известной как Strontium и Fancy Bear). С июня 2020 года злоумышленник использовал инструмент под названием GooseEgg для эксплуатации уязвимости диспетчера очереди печати Windows (CVE-2022-38028) для повышения привилегий и кражи учетных данных из скомпрометированных систем. Злоумышленник нацелился на организации на Украине, в Западной Европе и Северной Америке, включая неправительственные организации, организации сферы образования и транспорта.

Атаки FIN7

В конце 2023 года аналитики BlackBerry обнаружили кампанию целевого фишинга, запущенную группой FIN7 (также известной как Carbon Spider, Elbrus и Sangria Tempest) и нацеленную на американского производителя автомобилей. Кампания была обнаружена на ранней стадии, зараженная система была изолирована до того, как хакеры смогли глубже проникнуть в сеть. BlackBerry с большой уверенностью приписала атаку FIN7 из-за характерных методов обфускации. В кампании использовались электронные письма целевого фишинга, содержащие ссылки на вредоносный URL-адрес «advanced-ip-sccanner.com», имитирующий легитимный веб-сайт сканирования IP-адресов. В конечном итоге веб-сайт перенаправлял жертв на принадлежащий злоумышленнику Dropbox, заставляя неосознанно загружать вредоносный исполняемый файл, который считывает и расшифровывает файл .wav для извлечения закодированной полезной нагрузки. Первоначальная полезная нагрузка инициировала многоступенчатый процесс выполнения для развертывания окончательной полезной нагрузки — бэкдора, известного как Anunak или Carbanak. Анализ сетевой инфраструктуры злоумышленника, проведенный BlackBerry, выявил взаимосвязанную сеть доменов и прокси-серверов, которую FIN7 использовала для облегчения доставки и поддержания доступа к скомпрометированным системам.

Атаки Hellhounds

Исследователи Positive Technologies сообщили о продолжении атак Hellhounds на российские компании, в ходе которых были атакованы по меньшей мере 48 организаций из государственного сектора, ИТ,

космической промышленности, энергетической, транспортной и логистикой отраслей, горнодобывающей промышленности и т. д. В статье раскрываются технические подробности атаки на Windows-инфраструктуру жертвы как развитие успеха атаки на Linux-серверы, описанной исследователями ранее. Hellhounds атакует российские компании по меньшей мере с 2021 года. Предполагается, что злоумышленник компрометирует целевые сети с помощью атак на цепочки поставок. Hellhounds маскирует свои инструменты под процессы легитимных приложений. Хотя практически весь инструментарий Hellhounds основан на проекте Pupy RAT с открытым исходным кодом и почти идентичен ранее изученному Decoy Dog для Linux, злоумышленнику удалось обойти защиту вредоносного ПО и сохранить устойчивость в целевых сетях.

Атаки PhantomCore

Исследователи F.A.C.C.T. обнаружили новый вредоносный загрузчик PhantomDL (PhantomGoDownloader), который, вероятно, имеет отношение к PhantomCore и используется с марта 2024 года. С января 2024 года PhantomCore находит в России цели, предположительно связанные с военно-промышленным комплексом.

В конце марта исследователям удалось найти на платформе VirusTotal защищенный паролем архив RAR, в котором содержались исполняемый файл и документ-обманка в формате PDF, имеющий вид акта приемки-передачи строительной площадки для работ на территории российского предприятия атомной отрасли. Злоумышленники использовали вариацию эксплойта уязвимости CVE-2023-38831 в WinRAR. Исполняемый файл представляет собой загрузчик, написанный на языке Go и предположительно обфусцированный с помощью утилиты Garble. Через месяц после первого обнаружения загрузчика исследователи идентифицировали новый образец, который, в отличие от более раннего, не имел обфускации классов и методов. Это позволило исследователям идентифицировать название проекта (D:\github\phantomDL) и присвоить этому загрузчику имя PhantomDL. Исследователи обнаружили совпадения в загрузчике PhantomDL и PhantomRAT, который, как известно, является основным инструментом APT PhantomCore.

Атаки Werewolves

Исследователи F.A.C.C.T. сообщили о новой волне атак с вредоносными рассылками от группировки вымогателей Werewolves, которая специализируется на вымогательстве с использованием версии программы-вымогателя LockBit3 (Black), собранной с использованием утекшего конструктора. В апреле вымогатели были замечены в проведении массовых рассылок на темы весеннего призыва и досудебных исков. Целью новых атак стали российские промышленные предприятия, телекоммуникационные и ИТ-компании, финансовые и страховые организации. Злоумышленники создали поддельный сайт крупного российского производителя спецтехники, полностью скопировав содержимое оригинального портала с помощью HTTrack Website Copier. Они зарегистрировали то же доменное имя, но в зоне .ru (оригинал был в .com). Письма с темами «Досудебная претензия» и «Рекламация» содержали вредоносные вложения, загружающие Cobalt Strike Beacon. После того, как жертва открывает прикрепленный документ Complaint.doc, загружается RTF-документ, который эксплуатирует уязвимость CVE-2017-11882.
HTA (HTML-приложение) доставляется на устройство жертвы, которое выполняет команду PowerShell. Эта команда распаковывает и запускает шелл-код Cobalt Strike Stager, который загружает Cobalt Strike Beacon с определенным водяным знаком в его конфигурации.

Атаки Sapphire Werewolf

Исследователи BI.ZONE сообщили о деятельности группы Sapphire Werewolf, которая осуществляла атаки с целью кибершпионажа. С марта 2024 года Sapphire Werewolf осуществила более 300 атак на российские организации в сфере образования, промышленности, ИТ, ВПК и аэрокосмической отрасли с помощью стилера Amethyst, который основан на программе с открытым исходным кодом SapphireStealer.
Злоумышленники распространяли вредоносное ПО с помощью фишинговых писем под видом постановления о возбуждении исполнительного производства, листовки ЦИК, а также указа Президента Российской Федерации. Установленный стилер собирает файлы конфигурации мессенджера Telegram, файлы с различными расширениями, в том числе с внешних носителей, данные из браузеров (Chrome, Opera, Yandex, Brave, Edge и т. д.), а также логи использования PowerShell и конфигурации FileZilla и SSH. Собранные данные архивируются и отправляются в CnC, а в последних версиях стилера создается архив, защищенный паролем.
CnC-сервер для отправки архива реализован на базе Telegram-бота, токен бота хранится в стилере.

Атаки Sticky Werewolf

Согласно отчету Morphisec, Sticky Werewolf, считающаяся хактивистской группой, атаковала организации авиационной отрасли в России и Беларуси в ходе новой фишинговой кампании. Ранее злоумышленники атаковали государственные учреждения, а затем расширили круг своих целей, включив в него фармацевтическую компанию и научно-исследовательский институт. Фишинговые письма были отправлены якобы генеральным директором московской компании по производству самолетов и космических аппаратов АО «ОКБ “Кристалл”». В этих письмах использовались защищенные паролем архивы, два файла LNK и поддельный PDF-документ. При нажатии на файл LNK устанавливались распространенные RAT и программы-стилеры (в их числе RAT Rhadamanthys и Ozone), предназначенные для кражи конфиденциальных данных.

Атаки Shedding Zmiy

Исследователи Solar 4RAYS опубликовали отчет, описывающий деятельность хакерской группы Shedding Zmiy, которая с начала 2022 года атаковала десятки российских компаний в сфере энергетики, госсекторе, ИТ и других секторах, с целью кибершпионажа. Злоумышленники не только использовали данные скомпрометированных компаний для последующих атак, но и публиковали их в открытом доступе, в основном в проукраинских Telegram-каналах. Каждый раз хакерам удавалось до неузнаваемости менять свой арсенал, находя новые методы атак: кастомные загрузчики, бэкдоры и веб-шеллы. Исследователи связывают Shedding Zmiy с известной с 2016 года группой Cobalt ((ex)Cobalt), которая атаковала исключительно кредитные и финансовые организации и преследовала только материальную выгоду, согласно публичным отчетам. Всего исследователи заметили следы использования 35 различных инструментов для разведки, повышения привилегий, доставки вредоносного ПО, бокового перемещения и кражи данных. Используются как общедоступные, так и собственные уникальные вредоносные программы. Для проникновения в сеть, повышения привилегий и закрепления злоумышленники использовали до 20 известных уязвимостей в распространенном корпоративном программном обеспечении. Shedding Zmiy также владеет навыками социальной инженерии. Группировка научилась отлично заметать следы: она имеет обширную сеть CnC-серверов в России и за рубежом, арендует ресурсы у хостинг-провайдеров и на облачных платформах, чтобы избегать блокировки по GeoIP. Исследователи объединили в один кластер разрозненные инциденты со схожими признаками использования вредоносного ПО, уязвимостей и инфраструктуры.

Другое

Атаки ChamelGang

Исследователи SentinelLabs и Recorded Future отслеживали два отдельных кластера активности, нацеленных на правительственные организации и секторы критической инфраструктуры по всему миру в период с 2021 по 2023 год. Кибершпионские группировки, в частности APT-группа ChamelGang, использовали программы-вымогатели в качестве заключительного этапа своих операций. ChamelGang атаковала Всеиндийский институт медицинских наук в Индии и аппарат президента Бразилии в 2022 году, используя программу-вымогатель CatB. Также она атаковала правительственную организацию в Восточной Азии и критическую инфраструктуру на Индийском субконтиненте в 2023 году. Еще один кластер атак с использованием инструментов шифрования BestCrypt и BitLocker был нацелен на различные отрасли в Северной Америке, Южной Америке и Европе, преимущественно на производственный сектор США. У атак обнаружены совпадения с прошлыми атаками, связанными, предположительно, с китайско- и корейско-говорящими APT-кластерами.

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