APT и финансовые атаки на промышленные организации в первом полугодии 2023 года

25.09.2023 Version 1.0

Эта подборка представляет собой обзор отчетов и сообщений об APT и финансовых атаках на промышленные предприятия, информация о которых была раскрыта в первом полугодии 2023 года, и о связанной с этим активности групп, замеченных в атаках на промышленные организации и объекты критической инфраструктуры. В каждом случае мы старались представить наиболее важные факты, результаты и выводы исследователей, которые, по нашему мнению, могут быть полезны экспертам, решающим практические вопросы обеспечения кибербезопасности промышленных предприятий.

Активность корейскоязычных групп

Атаки Lazarus

Эксперты из «Лаборатории Касперского» исследовали кампанию группы Lazarus, активную до января 2023 года. В ходе кампании атакующие использовали зараженный клиент UltraVNC для доставки обновленной нагрузки BLINDINCAN. Эта нагрузка имеет новые возможности, включая расширение на основе плагинов. Заражение известных программ с открытым исходным кодом является одним из способов, которыми группа Lazarus пользуется для доставки своего вредоносного программного обеспечения. При выполнении зараженное приложение функционирует нормально, но скрыто собирает информацию о жертве и передает ее на командные серверы.

Телеметрия показала наличие загружаемой в память полезной нагрузки, получаемой зараженным клиентом. Поставляемая нагрузка была идентифицирована как BLINDINCAN, которая ранее также использовалась как вредоносная нагрузка второго этапа. Эта обновленная версия BLINDINCAN имеет схожие характеристики с предыдущими версиями, такие как коммуникация с командным сервером, методы шифрования и процедура инфицирования.

Тем не менее, добавлены новые возможности, включая возможность расширения с использованием плагинов. После анализа и декодирования коммуникации протрояненного приложения, исследователи из «Лаборатории Касперского» обнаружили информацию о нацеленности атаки на компании в отраслях производство и недвижимость в Индии. Анализ командных серверов, скомпрометированных с начала 2020 года, обнаружил также направление атак на телекоммуникационные компании в Пакистане и Болгарии. Исследователи «Лаборатории Касперского» полагают, что данная кампания не ограничивается этими странами и отраслями.

WithSecure опубликовали результаты исследования новой кибершпионской кампании под названием No Pineapple!, за которой, по мнению исследователей, стоит группа Lazarus. Согласно результатам исследования, атакующие смогли незаметно украсть 100 ГБ данных у жертвы, не нанеся ущерба. Кампания проходила с августа по ноябрь 2022 года и была нацелена на организации, занимающиеся научными исследованиями, работающие в сфере здравоохранения, химической инженерии, энергетики, обороны и на ведущий исследовательский университет.

Хакеры Lazarus скомпрометировали сеть жертвы 22 августа 2022 года. Они использовали уязвимости RCE CVE-2022-27925 и CVE-2022-37042, чтобы обойти аутентификацию Zimbra, разместив веб-шелл на почтовом сервере. После успешного взлома сети были развернуты инструменты туннелирования Plink и 3Proxy, позволяющие атакующим обойти брандмауэр. Менее чем через неделю атакующие использовали модифицированные скрипты для извлечения с почтового сервера 5 ГБ информации, сохранив данные в файле CSV, который позже был выгружен на сервер атакующих.

В течение следующих двух месяцев Lazarus развернули свой инструмент Dtrack и новую версию GREASE (известно, что это ПО связанно с Kimsuky) для обнаружения учетных записей администраторов Windows, перемещения по сети и кражи данных с устройств. В ходе исследования WithSecure были выявлены несколько изменений в активности Lazarus, включая: новую инфраструктуру, использующую IP-адреса без доменных имен, обновленное вредоносное ПО Dtrack и GREASE (используется для создания учетной записи администратора и обхода защиты).

Новый вариант Dtrack больше не использует собственный командный сервер для кражи данных, полагаясь на отдельный бэкдор для передачи локально собранных данных в защищенном паролем архиве. Новый вариант GREASE запускается с привилегиями SYSTEM на хосте как DLL с помощью эксплойта Windows Print Spooler RCE/LPE к уязвимости PrintNightmare. Теперь он использует RDPWrap для установки службы RDP на хосте и создания привилегированых учётных записей.

Злоумышленники ошибочно выставили северокорейский IP-адрес в ходе своей деятельности. Кроме того, исследователи из WithSecure обнаружили много совпадений в тактиках, техниках и процедурах (TTPs), инфраструктуре и мишенях с данными, представленными в отчетах Symantec и Cisco Talos (отчеты описывают активность корейскоязычных групп). Кроме того, исследователи заметили, как атакующие вводили различные команды вручную на скомпрометированных сетевых устройствах, используя модуль Impacket atexec.

Атака на цепочку поставок 3CX

29 марта компания CrowdStrike опубликовала предупреждение об атаке на цепочку поставок через программу 3CXDesktopApp, популярное программное обеспечение для VoIP. В своем отчете они предварительно атрибутировали эту атаку корейскоязычной группе APT, известной как LABYRINTH CHOLLIMA (исследователи из «Лаборатории Касперского» идентифицируют ее как Lazarus). 3CX, по оценкам, имеет 600 000 компаний-клиентов по всему миру, включая Toyota, McDonald's, Pepsi, Chevron и компании из отрасли производство.

Исследователи считают, что кампания продолжается уже некоторое время. Репозиторий на GitHub, связанный с кампанией, был создан в декабре 2022 года, другая инфраструктура — в феврале 2022 года. Первые признаки указывают на то, что атакующие попытались скомпрометировать более 1000 целей, заразив установочные пакеты как для Windows, так и для macOS.

Согласно Sentinelone, первая попытка заражения была зарегистрирована их телеметрией в марте. «Лаборатория Касперского» с марта 2023 года отслеживает связанную кампанию. Тогда исследователи заметили всплеск активности, связанной с бэкдором под названием Gopuram. Gopuram известен с 2020 года, и он был замечен вместе с бэкдором AppleJeus на зараженных машинах.

Атаки APT43

Исследователи из компании Mandiant выявили ранее неизвестного актора APT, получившего имя APT43, который, как они считают, действует в интересах правительства Северной Кореи. Группа нацелена на определенные регионы: Южную Корею, США, Японию и Европу. Атакующих особенно интересуют государственные организации, организации, которые работают в сфере образования/исследований, аналитические центры, занимающиеся геополитикой и ядерной политикой, а также компании, оказывающие бизнес-услуги и занимающиеся производством.

Исследователи считают, что активность APT43, продолжающаяся уже более пяти лет, иногда приписывалась другим акторам — конкретно Kimsuky или Thallium. Для сбора информации группа чаще всего использует целевой фишинг и фальшивые веб-сайты. Из инструментов атакующие предпочитают LATEOP — бэкдор, основанный на скриптах Visual Basic. Они применяют и другие эксклюзивные вредоносные инструменты, а также множество общедоступных вредоносных программ, таких как gh0st RAT, QUASARRAT, AMADE и многих других семейств. Группа также использует инфраструктуру и инструменты совместно с другими APT, связанными с Северной Кореей.

Атаки Andariel

Исследователи из «Лаборатории Касперского» пересмотрели кампанию Andariel (подразделение Lazarus) 2022 года, расширив информацию о командах, которые атакующие использовали для развертывания инструмента DTrack, сопутствующих инструментах и вредоносном программном обеспечении для постэксплуатации. Исследователи полагают, что атакующие использовали Log4j для начальной компрометации.

Исследование инфраструктуры атакующих помогло связать случаи заражения Yamabot с этим инцидентом. Было выявлено несколько профилей целей для соответствующих развертываний Yamabot. Атакующих, в частности, интересовали биомедицинские исследования и производство, исследования в области почвоведения, а также энергетический сектор. Также было выявлено новое семейство вредоносного программного обеспечения EarlyRat, которое распространялось через фишинговые документы.

Атаки MATA

В начале сентября 2022 года исследователи из «Лаборатории Касперского» обнаружили использование вредоносных программ из кластера MATA, ранее атрибутируемого группе Lazarus, нацеленных на оборонных подрядчиков в Восточной Европе. Эта кампания оставалась активной до марта 2023 года. Эксперты обнаружили новые активные кампании атакующих с полными цепочками заражения, включая имплант, предназначенный для работы в изолированных (air-gapped) сетях через USB-накопители, а также бэкдор MATA для Linux.

Вредоносное ПО распространялось посредством целевого фишинга в несколько этапов с использованием валидаторов. В процессе атаки было скомпрометировано несколько решений по безопасности от различных вендоров, используемых жертвами. Новая версия MATA Orchestrator получила изменения в шифровании, конфигурации и протоколах связи и, по всей видимости, была переписана с нуля.

Исследователи из «Лаборатории Касперского» также обнаружили новую, полностью переписанную, версию MATA. MATAv5 предоставляет атакующим богатый набор команд и опций связи. MATAv5 способна функционировать и как служба, и как DLL в различных процессах. Вредоносная программа использует внутренние каналы межпроцессного взаимодействия (IPC) и применяет разнообразные команды, позволяя устанавливать цепочки прокси через различные протоколы — также внутри

среды жертвы. Несмотря на значительную эволюцию MATAv5 (совпадение кода новой версии с кодом предшествующих версий минимально), все же еще осталось некоторое сходство с предыдущими версиями — в протоколах, командах и структуре плагинов. Это указывает на последовательный подход к разработке разных поколений вредоносной программы.

Активность китайскоязычных групп

Атаки Blackfly/APT41

Согласно исследователям из компании Symantec, угроза, известная как Blackfly (а также как APT41, Winnti и Bronze Atlas), нацелена на два дочерних предприятия азиатского конгломерата в секторе материалов и композитов. Атаки, произошедшие в конце прошлого и начале текущего года, больше полагались на инструменты с открытым исходным кодом, чем на специализированные вредоносные программы. Атакующие применяли Backdoor.Winnkit, инструмент для сбора учетных данных, инструмент для создания снимков экрана, инструмент для скрытия процессов, SQL-инструмент, Mimikatz, ForkPlayground и инструменты для настройки прокси. Исследователи считают, что это часть более широкой кампании, нацеленной на различные отрасли в регионе.

Атаки Volt Typhoon/VANGUARD PANDA

Исследователи из компании Microsoft сообщили, что китайскоязычный актор Volt Typhoon смог установить постоянный доступ к критической инфраструктуре в США, включая такие секторы как связь, производство, коммунальные услуги, транспорт, строительство, морская и речная навигации, государственные организации, информационные технологии и образование. Целью атак является шпионаж, но, по мнению Microsoft, существует потенциальная угроза, что, в случае военного конфликта в Южно-Китайском море и более широком регионе Тихого океана, атакующие смогут перейти к более деструктивным действиям.

Атакующие получают первоначальный доступ, компрометируя оборудование Fortinet FortiGuard, доступное из интернета, и используют привилегии этого устройства для извлечения учетных данных из Active Directory и аутентификации на других устройствах в сети. Затем они используют командную строку и легитимное ПО, доступное на скомпрометированных системах, для сбора предварительной информации, продвижения по сети и эксфильтрации данных. Атакующие скрывают свои

следы, перенаправляя сетевой трафик через скомпрометированные SOHO-маршрутизаторы и другие граничные устройства.

В совместном релизе Национальное управление по борьбе с терроризмом в США, а также другие внутренние агентства США и партнеры из Австралии, Великобритании, Новой Зеландии и Канады опубликовали предупреждение, которое ссылается на выводы Microsoft и предостерегает от «недавно обнаруженной активности» из Китая.

Группа Volt Typhoon активна как минимум с середины 2021 года. В последней кампании группа нацеливалась на организации в отраслях связи, производства, коммунальных услуг, транспорта, строительства, морской и речной навигации, правительства, информационных технологий и образования.

Исследователи компании CrowdStrike заметили, что данная группа, которую они назвали VANGUARD PANDA, использует новый подход для получения начального доступа к целевым сетям. CrowdStrike сообщила, что группа использовала эксплойты к Zoho ManageEngine и ADSelfService Plus для получения начального доступа. После этого атакующие применяли кастомные веб-шеллы для достижения постоянного доступа и технику LOTL (living-off-the-land) для перемещения по сети.

Дополнительная обнаруженная вредоносная активность включает в себя получение списка процессов, тестирование сетевого подключения, сбор информации о пользователях и группах, подключение общих ресурсов, перебор доверительных отношений доменов через WMI, а также перебор зон DNS через WMI. VANGUARD PANDA очевидно знакомы с инфраструктурой атакуемой цели. Об этом свидетельствуют как быстрый ввод команд, так и знания специфических внутренних имен хостов и IP-адресов, передаваемых команде ping, подмонтируемые удаленные общие ресурсы и обычные учетные данные для использования WMI.

Атакующие использовали веб-шелл для замены файла tomcat-websocket.jar в библиотеке Apache Tomcat на версию с внедренным бэкдором. Об этой технике закрепления группы VANGUARD PANDA ранее не сообщалось. Этот бэкдор, вероятно, использовался VANGUARD PANDA для обеспечения постоянного доступа к высокоценным целям, которые были выбраны после получения начального доступа с использованием уязвимостей нулевого дня.

Атаки Earth Longzhi

После нескольких месяцев затишья в активности Earth Longzhi (предполагается, что это подгруппа APT41) нацелилась на организации

в сферах здравоохранения, производства, технологий и правительственные организации на Тайване, в Таиланде, на Филиппинах и Фиджи. В ходе кампании злоумышленники компрометируют исполняемый файл Windows Defender для выполнения боковой загрузки библиотек (DLL side-loading), а также эксплуатируют уязвимый драйвер, чтобы отключить установленные на хосты средства безопасности с помощью атаки «BYOVD» (Bring Your Own Vulnerable Driver). Исследователи из компании TrendMicro также обнаружили новый способ отключения средств безопасности — метод, получивший название «stack rumbling», который использует недокументированные значения MinimumStackCommitInBytes в ключе реестра Image File Execution Options (IFEO).

Атаки Lancefly

Исследователи из компании Symantec обнаружили нового актора APT, получившего имя Lancefly, атакующего государственные организации, организации из авиационной отрасли и телеком в Южной и Юго-Восточной Азии с использованием кастомного бэкдора. Бэкдор, используемый группой и названный «Merdoor», разрабатывается с 2018 года. Исходный вектор заражения остается неизвестным, хотя есть свидетельства того, что атакующие используют фишинговые электронные письма, брутфорс SSH-паролей и эксплуатацию уязвимостей серверов с открытым доступом для получения доступа к целевым системам. Группа также использует более новую версию руткита ZXShell, инструмента, который применялся APT17 и APT41. Также было замечено, что группа Lancefly использует функцию «Atexec» из Impacket для немедленного выполнения запланированной задачи на удаленной машине через SMB. Группа Lancefly также применяла RAT PlugX и ShadowPad — инструменты, которые традиционно используют несколько китайскоязычных APT групп.

Кибератаки на Тайвань

Согласно исследователям из Trellix, наблюдается увеличение числа кибератак на Тайвань на фоне роста геополитической напряженности между Тайванем и Китаем. Цель атак — в основном доставка вредоносных программ и кража чувствительной информации.

Отрасли, наиболее подверженные атакам в период, за который ведутся наблюдения исследователей, — это сетевые технологии, производство и логистика. Также отмечается значительное увеличение детектов PlugX — бэкдора для Windows, который многие китайскоязычные акторы используют для управления целевыми компьютерами.

Другие семейства вредоносных программ, нацеленные на Тайвань, включают шпионский инструмент .NET Zmutzy, крадущий информацию инструмент Formbook и неизвестную вредоносную программу под именем Kryptik, идентифицированную только по ее антиотладочным механизмам и реестру обфускации кода.

Активность русскоязычных групп

Атаки YoroTrooper

Исследователи из компании Cisco Talos обнаружили нового актора, которого назвали YoroTrooper. Группа проводит кампании кибершпионажа, нацеленные на правительственные и энергетические организации в странах СНГ с июня 2022 года. Атакующие, стоящие за этими кампаниями, также скомпрометировали учетные записи агентства ЕС, занимающегося здравоохранением, Всемирной организации интеллектуальной собственности (WIPO) и различных посольств СНГ. Исследователи считают, что группа YoroTrooper также могла атаковать другие организации в ЕС и Турции.

Среди используемых инструментов — коммерческое ПО для кражи информации и для получения удаленного доступа (такое как AveMaria/Warzone RAT, LodaRAT), написанные на Python RAT и вредоносное ПО для кражи информации, а также обратные оболочки — на Python и на базе Meterpreter. Инструменты доставляются с помощью фишинговых электронных писем, содержащих вредоносные LNK и приманки в виде PDF-документов. Атакующие регистрировали вредоносные домены, создавали субдомены и использовали домены с именами, похожими на легитимные, но с «опечатками».

Исследователи из «Лаборатории Касперского» заметили пересечение в выборе целей, схожесть образцов вредоносного ПО, сетевых индикаторов компрометации TTP, используемых YoroTrooper и группой Tomiris.

Инструмент COSMICENERGY

Исследователи из компании Mandiant выявили ПО под названием «COSMICENERGY», разработанное для симуляции атак на электроэнергетические сети. Они обнаружили это вредоносное ПО после его загрузки на VirusTotal. Исследователи полагают, что COSMICENERGY, возможно, было разработано как инструмент для учений по реагированию на атаки на системы электроэнергетики,

организуемых российской компанией по кибербезопасности Rostelcom-Solar. ПО нацелено на устройства IEC 60870-5-104 (IEC-104), включая удаленные блоки управления (RTU). Оно напоминает Industroyer. Пока исследователи не заметили ни одной активности с нецелевым использованием этого инструмента в дикой природе.

Атаки BlueDelta/Sofacy

Согласно Insikt Group компании Recorded Future и Украинскому центру реагирования на компьютерные чрезвычайные ситуации (CERT-UA), группа BlueDelta (также известна как Sofacy, APT28, Fancy Bear и Sednit) использовала уязвимости в Roundcube Webmail для взлома более чем 40 украинских организаций, включая государственные учреждения и военные организации, занимающиеся инфраструктурой авиационных объектов.

Атакующие использовали новости о русско-украинском конфликте, чтобы спровоцировать жертв открыть вредоносные электронные письма, в результате чего эксплуатировались уязвимости (CVE-2020-35730, CVE-2020-12641 и CVE-2021-44026). С помощью вредоносного скрипта атакующие перенаправляли на контролируемый ими адрес электронной почты входящие письма целей и собирали данные из скомпрометированных учетных записей. Судя по всему, выявленные Insikt Group атаки группа BlueDelta проводит с ноября 2021 года.

Атаки Midnight Blizzard

Эксперты из компании Microsoft выявили всплеск атак группы Midnight Blizzard (также известной как Nobelium, APT29, Cozy Bear, Iron Hemlock и The Dukes), направленных на кражу учетных данных. Группа Midnight Blizzard привлекла всемирное внимание в декабре 2020 года, когда их жертвами стали компания SolarWinds и её многочисленные клиенты.

Атакующие используют разнообразные методы, включая password spraying, брутфорс, кражу токенов и воспроизведение сессий с целью получения несанкционированного доступа к облачным ресурсам. Кроме того, Midnight Blizzard / APT29 использует резидентные прокси-сервисы для маскировки вредоносного трафика и сокрытия соединений, которые они устанавливают с помощью украденных учетных данных. Эти атаки нацелены на правительства, поставщиков IT-услуг, НПО, оборонную промышленность и критическую инфраструктуру в производстве.

Деятельность, связанная с Ближним Востоком

Атаки Mint Sandstorm/Charming Kitten

Группа Mint Sandstorm (также известна как Charming Kitten, а ранее отслеживалась как Phosphorous), связанная по мнению исследователей с иранским правительством, согласно информации компании Microsoft, проводит кибератаки на критическую инфраструктуру США. Атакующих особенно интересуют организации в секторах энергетики и транспорта.

Группа обычно использует PoC эксплойты сразу после того, как они становятся известными общественности — исследователи наблюдали атаку с использованием Proof-of-concept эксплойта к Zoho ManageEngine в тот же день, когда он был опубликован. Атакующие также используют известные уязвимости, такие как Log4Shell, для взлома непропатченных устройств. Получив доступ к целевой сети, атакующие запускают кастомный скрипт PowerShell для сбора информации о зараженной инфраструктуре, чтобы определить, является ли она ценной. После перемещения по сети они развертывают кастомные бэкдоры для закрепления и установки дополнительных нагрузок.

Исследователи Bitdefender выявили жертв Mint Sandstorm в Соединенных Штатах, Европе, Турции и Индии, а также предоставили дополнительные детали по набору инструментов и индикаторам компрометации.

Атаки типа watering hole на веб-сайты отраслей судоходства и логистики

ClearSky Cyber Security обнаружила атаку методом watering hole (атака на водопой) на по крайней мере восемь израильских веб-сайтов, принадлежащих судоходным, логистическим компаниям и компаниям, предоставляющим финансовые услуги, и с низкой степенью уверенности атрибутировала их иранской группе Tortoiseshell (также известной как TA456 или Imperial Kitten).

Согласно отчету ClearSky Cyber Security, группа Tortoiseshell активна по меньшей мере с июля 2018 года. На скомпрометированных веб-сайтах атакующие применяли скрипт для сбора начальной информации о пользователях, включая язык операционной системы пользователя, IP-адрес, разрешение экрана, а также URL, с которого был посещен веб-сайт. Атакующие использовали четыре домена и, добавляя «jQuery» в их имена, выдавали их за легитимный фреймворк JavaScript jQuery. Трюк с использованием доменных имен, имитирующих jQuery, был замечен в предыдущей иранской кампании 2017 года.

Другие атаки

Атаки вымогателей Vice Society

Группа Vice Society, также известная как DEV-0832, специализируется на вымогательских атаках и активна по меньшей мере с июня 2021 года. Изначально она была сосредоточена в основном на организациях в отраслях образование и здравоохранение в США. Несмотря на единое название, атакующие используют различные семейства программ-вымогателей (например, BlackCat, QuantumLocker и Zeppelin).

В январе TrendMicro опубликовала блог-пост, поделившись данными своей телеметрии и суммируя выявленные тактики, техники и процедуры (TTPs) группы. Например, группа использует кастомные скрипты PowerShell, а для начального заражения полагается на уязвимые общедоступные веб-сайты и компрометированные учетные данные RDP.

Исследователи заметили, что группа также нацеливается на производственные компании, что свидетельствует о ее способности и стремлении проникать в различные отрасли. Присутствие Vice Society было обнаружено в Бразилии (в первую очередь атакующие нацелились на производственные компании страны), в Аргентине, Швейцарии и Израиле.

Атаки вымогателей Royal

После предупреждения CISA о группе Royal, специализирующейся на атаках с использованием программы-вымогателя, компания Trend Micro опубликовала свой отчет о группе. Отчет содержит новые индикаторы компрометации, цепочку заражений и методы атаки, а также статистику по организациям-мишеням и географии атак.

Согласно данным Trend Micro, с сентября 2022 года по январь 2023 года наибольший интерес среди клиентов Trend Micro для Royal представляли отрасли производство и транспорт, на эти отрасли приходится по 33,7% всех выявленных попыток атак группы.

Несколько атак группы Royal были зафиксированы в 2022 году, в основном на организации в США и Бразилии. Согласно сайту Royal, на котором они публикуют информацию о своих жертвах, в четвертом квартале компании малого бизнеса составили чуть более половины жертв Royal, в то время как на организации среднего размера пришлось около 30% жертв вымогателей. Большие компании составили 14%.

В своих кампаниях группа применяет смесь старых и новых методов. С одной стороны, они используют метод «callback phishing» для привлечения жертв к установке вредоносного ПО для удаленного доступа. С другой стороны, использование прерывистого шифрования и разработка вариантов вымогательского вредоносного ПО для Linux, которое также нацелено на серверы ESXi, показывает, что группа следит за современными тенденциями в сфере вымогательских атак.

APT-атаки с использованием фреймворков CommonMagic и CloudWizard

Исследователи из «Лаборатории Касперского» обнаружили кампанию, активную с третьего квартала 2021 года, нацеленную на правительственные, сельскохозяйственные и транспортные организации в районах конфликта в Восточной Европе. В рамках этой кампании используется ранее неизвестный набор вредоносных программ. Отмечается, что жертвы скачивают архив, содержащий вредоносный файл LNK, который загружает и устанавливает PowerShell-бэкдор с названием «PowerMagic". Затем запускается сложный модульный фреймворк с названием CommonMagic. Плагины CommonMagic способны похищать файлы с USB-устройств, а также создавать снимки экрана и отправлять их атакующему.

Дополнительное расследование привело к обнаружению фреймворка CloudWizard, который используется как минимум с 2017 года. У фреймворка модульная архитектура, и его функции включают создание снимков экрана, запись звука с микрофона, а также кражу файлов и паролей. Собранная с помощью этого фреймворка информация загружается в облачные хранилища. Исследователи видят связи CloudWizard с операциями Groundbait (Prikormka), BugDrop и кампаниями CommonMagic.

Исследователи Malwarebytes также отслеживали эту деятельность и дали угрозе имя RedStinger. Исследователи отслеживают их операции с 2020 года. Примечательно, что в ходе их операций были атакованы как пророссийские, так и проукраинские цели. Обе кампании отличаются своей настойчивостью и агрессивностью.

Целями «Операции Четыре» стал в том числе украинский военный, работающий в критической инфраструктуре. Атакующие скомпрометировали целевые устройства для сбора снимков экрана и документов, а также записи аудио. «Операция Пять» была нацелена на чиновников, организующих референдумы в Донецке и Мариуполе. Один из них имел отношение к Центральной избирательной комиссии России. Другой занимался транспортной инфраструктурой (возможно, железнодорожной) в регионе.

Атаки вымогателей RA

Исследователи из Cisco Talos обнаружили ранее неизвестную кампанию по распространению вымогательского вредоносного ПО. Группу атакующих, ответственных за эту кампанию, исследователи назвали RA. Группа активна по меньшей мере с 22 апреля 2023 года. Она атакует компании в США и Южной Корее с использованием вредоносного ПО, созданного на основе утекшего исходного кода программы-вымогателя Babuk.

Скомпрометированы организации в разных бизнес-вертикалях, включая производство, управление активами, страхование и фармацевтику. Как и другие группы вымогателей, группа RA использует модель двойного шантажа и ведет сайт, на котором продает украденную информацию. Вымогательское вредоносное ПО шифрует только файлы и папки, которые не входят в жестко закодированный список, что позволяет избежать шифрования файлов, способных нарушить работу зараженной системы.

Атаки группы Void Rabisu

В связи с конфликтом между Россией и Украиной границы между APT-угрозами, хактивистами и киберпреступниками стали размытыми. Один из примеров этого — изменение использования бэкдора RomCom. За этим вредоносным ПО стоит группа Void Rabisu (также известная как Tropical Scorpius), ранее, исходя из связей с программой-вымогателем Cuba, считавшаяся финансово мотивированной.

Однако исследователи из TrendMicro отметили применение RomCom против украинских правительственных и военных целей, а также предприятий водоснабжения, энергетических и финансовых организаций в стране. Злоумышленники использовали целевой фишинг и рекламу Google Ads, перенаправляющую пользователей на сайты-ловушки с RomCom. На этих сайтах предлагаются троянские версии подлинных приложений, таких как AstraChat и Signal, программы для просмотра PDF, менеджеры паролей и приложения для удаленного доступа.

Бюллетени CISA

Программа-вымогатель Royal

Федеральное бюро расследований США (FBI) и Агентство кибербезопасности и инфраструктурной безопасности США (CISA) выпустили совместное предупреждение для распространения известных индикаторов компрометации (IOCs) и тактик, техник и процедур (TTPs) вымогательского вредоносного ПО Royal.

Эти индикаторы компрометации и TTPs были выявлены ФБР в ходе расследования инцидентов, которое проходило вплоть до января 2023 года. В предупреждении отмечается, что группа Royal нацелена на объекты критической инфраструктуры нескольких отраслей, включая производство, связь, образование и здравоохранение. Недавняя активность атакующих, которые используют конкретный вариант вредоносного ПО, отслеживается с сентября 2022 года.

ФБР и CISA считают, что этот вариант ПО, использующий собственную программу для шифрования файлов, развивается из более ранних версий, которые в качестве загрузчика использовали «Zeon». После получения начального доступа к целевым сетям через фишинг, RDP и другие методы, атакующие отключали антивирусное программное обеспечение на компьютерах жертв и выгружали большие объемы данных. Наконец, они развертывали вымогательское вредоносное ПО и шифровали системы. CISA предложило ряд рекомендаций для уменьшения вероятности и смягчения последствий атак вымогательского вредоносного ПО.

Вредоносное ПО Snake

Агентство кибербезопасности и инфраструктурной безопасности США (CISA) опубликовало подробный анализ вредоносного ПО Snake — одного из имплантов, которые приписываются группе Turla.

Это вредоносное ПО предназначено для долговременного сбора информации о высокоприоритетных целях с использованием пиринговой сети скомпрометированных систем по всему миру. Инфраструктура, связанная с данной угрозой, была обнаружена в более чем 50 странах Северной Америки, Южной Америки, Европы, Африки, Азии и Австралии, причем цели включали правительственные сети, исследовательские учреждения и журналистов. Внутри США в числе целей были организации, работающие в сфере образования, малый бизнес, медиа и производственные компании критической инфраструктуры.

Министерство юстиции США выдало ордер, разрешающий ФБР удаленно получить доступ к восьми компьютерам в США, зараженным Snake, и прекратить работу вредоносного ПО на этих компьютерах.

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