Kaspersky ICS CERT

kaspersky

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

25.03.2025

Версия 1.0

Интересные факты 3
Юго-Восточная Азия и Корея 5
Атаки PhantomNet 5
Атаки SideWinder 5
Атаки DONOT/Origami Elephant 6
Атаки P8 7
Активность китайскоязычных групп 7
Атаки Estries/Salt Typhoon 7
Атаки TIDRONE 8
Активность, связанная с Ближним Востоком 9
Предупреждение агентства CISA об активности иранских кибергрупп 9
Бэкдор OrpaCrab/IOCONTROL 9
Активность и цели русскоязычных групп 10
Атаки Crypt Ghouls 10
Атаки Awaken Likho/Core Werewolf 11
Атаки Shadow/Twelve 12
Атаки RomCom 13
Атаки Cloud Atlas 13
Атаки Venture Wolf 14
Атаки Unicorn 14
Атаки Sticky Werewolf/Angry Likho 15
Атаки Andromeda/Gamarue 15
Финансово-мотивированные атаки и прочее 16
Предупреждение агентства CISA о вымогателях BianLian 16
Атаки Interlock 17
Атаки TA866/Asylum Ambuscade 18
Атаки Akira/Howling Scorpius 18
Атаки Water Makara 19
Операция Cobalt Whisper 20
Атаки UAC-0185 20
Атаки SmokeLoader 20
Атаки с использованием стилера Lumma и Amadey Bot 21

Этот документ содержит обзор публикаций об APT- и финансовых атаках на промышленные предприятия, результаты исследования которых были раскрыты в четвертом квартале 2024 года. 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.

Интересные факты

Атаки, о которых стало известно в четвертом квартале 2024 года, иллюстрируют некоторые из многочисленных проблем кибербезопасности промышленных предприятий и технологической инфраструктуры. Перечислим основные моменты, на которые мы хотели бы обратить внимание читателей.

Группа TIDRONE в очередной раз была уличена в распространении вредоносного ПО через программное обеспечение ERP, содержащее бэкдор. Скорее всего, это стало результатом атаки на нишевых корейских разработчиков ERP, предлагающих свои решения ограниченному числу клиентов. Эта кампания свидетельствует о том, что атаки на цепочки поставок являются важнейшим фактором риска для промышленных предприятий, особенно, когда они имеют дело с мелкими поставщиками.

OpraCrab — сложный бэкдор на базе Linux, нацеленный на системы автозаправочных станций, был обнаружен в одной из систем управления топливом, которая ранее, судя по сообщению исследователей, была взломана известной группой хактивистов. Еще один пример того, что в целевых атаках на OT-системы может вообще не использоваться какая-либо специальная OT-функциональность (единственное специфическое, что сделали атакующие в данном случае, — они реализовали взаимодействия с командным сервером через протокол MQTT для сокрытия коммуникаций в обычном для атакованных систем трафике).

Группа RomCom в своих атаках на оборонные, энергетические, правительственные, фармацевтические, страховые и юридические организации европейских стран, Украины и США использовала цепочку из двух уязвимостей нулевого дня (одна в браузере, другая в операционной системе), что привело к удаленному выполнению кода без каких-либо действий пользователя. Этот кейс подчеркивает, насколько важно обучать сотрудников кибергигиене и повышать уровень их киберграмотности.

Многофакторная аутентификация — полезная практика обеспечения безопасности, но использовать ее нужно правильно. В противном случае злоумышленники могут ее обойти, как это продемонстрировала проиранская группа хакеров в ходе кампании, нацеленной на промышленные организации в различных секторах. Поскольку для дальнейшего распространения по сети своих жертв злоумышленники пользовались RDP, этот кейс также служит напоминанием о том, как важен мониторинг и контроль использования инструментов удаленного доступа внутри ИТ- и ОТ-периметров.

Несколько интересных техник продемонстрировала группа Shadow/Twelve (предположительно за этими названиями скрывается одна группа, которая меняет название, переключаясь между финансово мотивированными атаками и хактивизмом). Этот кейс подтверждает, что промышленным предприятиям стоит внимательнее относиться к защите систем на базе Linux и к защите виртуальных сред. Участники группы использовали Telegram, чтобы следить за сотрудниками компаний-жертв и оказывать давление на них для получения выкупа. Это доказывает, что личные мессенджеры не следует воспринимать как нечто не подлежащее мониторингу и контролю со стороны корпоративной службы информационной безопасности.

Группа Akira/Howling Scorpius в своих атаках на организации среднего размера в сфере строительства, транспорта, логистики, государственного управления, телекоммуникаций, технологий и фармацевтики обходила защитные решения с помощью комбинации как давно известных техник, например Bring Your Own Vulnerable Driver, так и нового метода, нацеленного на защищенные EDR-решениями виртуальные инфраструктуры. Это еще один аргумент в пользу того, что промышленным предприятиям необходимо инвестировать ресурсы в сбор и анализ информации об угрозах, чтобы заблаговременно разрабатывать адекватные меры безопасности.

В ходе кампании промышленного шпионажа с использованием зараженных USB-накопителей, направленной против производственных и логистических предприятий Азиатско-Тихоокеанского региона, Turla (по версии компаний Mandiant и Cybereason), или Tomiris (по версии «Лаборатории Касперского»), использовала довольно редкую тактику первоначального профилирования жертв. Для этого они захватили командный сервер неактивного ботнета, ликвидированного несколько лет назад в ходе операции международных правоохранительных органов. Хорошее напоминание сотрудникам ИБ-отделов промышленных предприятий, что попытка заражения распространенным вредоносным ПО может быть лишь первым этапом APT-атаки, разворачивающейся внутри сети организации.

Интересную технику уведомления своих жертв об атаке использовали вымогатели BianLian — они оставляли сообщения, печатая их на принтерах, подключенных к скомпрометированной сети. Сотрудникам служб ИБ на заметку — имеет смысл периодически проверять, что печатают ваши принтеры.

Вслед за LockBit еще один шифровальщик теперь поддерживает FreeBSD. Новый шифровальщик Interlock, имеющий вариант под эту ОС, замечен в атаках на промышленные предприятия в Индии, Италии, Японии, Германии, Перу, Южной Корее, Турции и США — надеяться, что серверы под управлением этой платформы находятся в безопасности из-за отсутствия работающего на ней вредоносного инструментария больше нельзя.

Юго-Восточная Азия и Корея

Атаки PhantomNet

PhantomNet — это RAT, впервые описанный специалистами ESET в конце 2020 года. В 2021 году исследователи «Лаборатории Касперского» опубликовали собственный анализ зловреда PhantomNet, который в то время использовался для атак на правительственный сектор Вьетнама. В отчете «Лаборатории Касперского» были подробно описаны плагины и команды, которые поддерживал зловред. Эксперты снова обнаружили PhantomNet в ходе исследования кибератаки на госучреждения и образовательные организации в Бразилии в апреле 2024 года. Они выявили многочисленные скрипты и команды, которые выполняли атакующие, а также билдер PhantomNet. Злоумышленники изменили механизм закрепления таким образом, что вредоносная нагрузка теперь хранится в зашифрованном виде в реестре Windows и извлекается оттуда с помощью специального загрузчика. Статистика по жертвам также демонстрирует изменения: если раньше случаи заражения PhantomNet регистрировались только в Азии, то теперь активность злоумышленников охватывает множество регионов по всему миру и затрагивает целый спектр отраслей, включая промышленное производство, строительство и сельское хозяйство.

Атаки SideWinder

SideWinder — это APT-группа, которая активна как минимум с 2012 года и нацелена в основном на крупные организации в Южной Азии. В ходе одного из расследований эксперты «Лаборатории Касперского» обнаружили, что злоумышленники из SideWinder использовали ранее неизвестный

инструмент последнего этапа атаки StealerBot. Это продвинутый модульный имплант, специально разработанный для шпионажа. Его основной компонент скрыт несколькими уровнями обфускации и механизмом защиты от анализа. Ни один компонент, в том числе и основной, который используется только для связи с удаленными серверами и загрузки дополнительных модулей, не хранится в файловой системе в открытом виде. Все компоненты находятся внутри зашифрованных файлов и загружаются в память с помощью другого вредоносного ПО, такого как Backdoor Loader Module. Модули выборочно устанавливаются злоумышленником на конкретную систему, исходя из потребностей. Всего было обнаружено восемь модулей, с помощью которых совершались атаки на цели в Бангладеш, Джибути, Иордании, Малайзии, Мьянме, Непале, Пакистане, Саудовской Аравии, Шри-Ланке, Турции, ОАЭ и на Мальдивах. Среди пострадавших организаций — государственные и военные структуры, логистические компании и инфраструктура, университеты и финансовые учреждения, телекоммуникационные и нефтяные компании. Атакам также подверглись дипломатические учреждения в Афганистане, Франции, Китае, Индии, Индонезии и Марокко.

Атаки DONOT/Origami Elephant

Согласно отчету лаборатории Cyble Research and Intelligence Labs, APT-группа DONOT (также известная как APT-C-35, Origami Elephant, Brainworm) атаковала предприятия судостроительной и оборонной промышленности в Пакистане. Группа существует с 2016 года. Ее деятельность с самого начала была нацелена на правительственные учреждения, военные структуры и дипломатические миссии, в основном расположенные в странах Южной Азии. Ранее группа DONOT атаковала организации, эксплуатируя уязвимости и используя фишинговые письма и вредоносные вложения в качестве начального вектора заражения. В новой кампании группа использовала фишинговые письма, содержащие вредоносный файл LNK под видом документа RTF. При открытии файла запускались несколько команд PowerShell, которые загружали DLL и документ-приманку RTF. Документ-приманка отсылал к Karachi Shipyard & Engineering Works — крупному оборонному подрядчику из Пакистана. После запуска вредоносный DLL инициирует процесс извлечения из встроенного файла JSON данных конфигурации, включая адреса серверов, ключи шифрования и другие параметры. Затем вредоносное ПО использует эту информацию для связи с командным сервером и запрашивает дальнейшие инструкции по развитию атаки. Для резервного командного сервера используется случайным образом сгенерированное доменное имя.

Атаки P8

Исследователи «Лаборатории Касперского» идентифицировали новый фреймворк атак, получивший название P8. Атакам подверглись предприятия в сфере финансов и недвижимости Вьетнама во второй половине 2022 года. В 2023 году компания Elastic Security Labs сообщила об атаке APT-группы OceanLotus (она же APT32) с использованием набора инструментов под названием Spectral Viper. Хотя эти кампании идентичны, исследователи «Лаборатории Касперского» не могут однозначно атрибутировать P8 к группе OceanLotus.

Фреймворк P8 содержит загрузчик и нескольких плагинов, которые загружаются с командного сервера в память, не оставляя следов на диске. Исследователи считают, что P8 создан на основе проекта с открытым исходным кодом C2Implant, который модифицировали для шпионажа и оснастили расширенным набором функций и протоколов. Целью, предположительно, была реализация еще одной платформы постэксплуатации, подобной Cobalt Strike. С той или иной степенью уверенности можно предположить, что начальным вектором заражения является целевой фишинг. Для сайдлоадинга маяка P8 атакующие использовали устаревшую утилиту «Лаборатории Касперского». Исследователи также обнаружили, что перемещение по сети осуществлялось путем эксплуатации уязвимостей SMB и драйверов для принтера.

«Лаборатория Касперского» опубликовала дополнительный отчет с подробным описанием 12 плагинов для перемещения по сети, эксфильтрации данных, кражи учетных данных, создания скриншотов, загрузки и управления файлами. Новые атаки показали, что тактики, техники и процедуры злоумышленников изменились, но главной мишенью по-прежнему остались финансовые учреждения Вьетнама. Среди пострадавших оказалось также одно производственное предприятие. Начальный вектор заражения по-прежнему остается неизвестным, и прямой связи с OceanLotus установлено не было.

Активность китайскоязычных групп

Атаки Estries/Salt Typhoon

В ходе расследования атак на телекоммуникационные компании Юго-Восточной Азии специалисты Trend Micro обнаружили новый бэкдор, получивший название GHOSTSPIDER. Исследователи связывают эти атаки с

китайскоязычной группой Earth Estries (она же Salt Typhoon, FamousSparrow, GhostEmperor и UNC2286). Для организации сложных многоступенчатых атак группа, помимо GHOSTSPIDER, использует набор собственных и общедоступных инструментов: SNAPPYBEE (он же Deed RAT), SparrowDoor, CrowDoor и MASOL RAT для Linux, руткит DEMODEX, NeoReGeorg, frpc и Cobalt Strike. По данным компании Trend Micro, группа Salt Typhoon осуществляла атаки на телекоммуникационные, технологические, консалтинговые и транспортные компании, правительственные учреждения и предприятия химической промышленности Афганистана, Бразилии, Эсватини, Индии, Индонезии, Малайзии, Пакистана, Филиппин, Южной Африки, Тайваня, Таиланда, США и Вьетнама. Особое внимание в отчете уделяется двум кампаниям: Alpha (атаки на государственные структуры и предприятия химической промышленности Тайваня с использованием DEMODEX и SNAPPYBEE) и Beta (продолжительная кампания кибершпионажа в сетях телекоммуникационных и правительственных организаций Юго-Восточной Азии с использованием GHOSTSPIDER и DEMODEX). Первичное проникновение происходило с использованием уязвимостей публичных сервисов: CVE-2023-46805, CVE-2024-21887 (сервис Ivanti Connect VPN), CVE-2023-48788 (FortiClient EMS), CVE-2022-3236 (файрвол Sophos), CVE-2021-26855, CVE-2021-26857-6858 и CVE-2021-27065 (ProxyLogon). Для сбора разведданных и перемещения по сети Salt Typhoon использует LOLbin-подход (Living-off-the-Land Binaries).

Атаки TIDRONE

Китайскоязычная группа TIDRONE была впервые идентифицирована исследователями из Trend Micro, а в сентябре 2024 года описана экспертами компании Acronis. В блоге компании были описаны атаки TIDRONE на производителей дронов и оборонные предприятия Тайваня. Исследователи центра ASEC обнаружили, что принадлежащее группе вредоносное ПО CLINTEND было использовано в ходе атаки на корейские компании в первой половине 2024 года. Эксперты Trend Micro предположили, что в описанных ими случаях группа распространяла вредоносное ПО через содержащее бэкдор программное обеспечение ERP, что, скорее всего, явилось результатом атаки на цепочку поставок. В случаях, описанных ASEC, вредоносное ПО также распространялось через содержащее троянца программное обеспечение ERP, которое эксплуатировалось с июля 2024 года. Но на этот раз ПО было произведено мелкими корейскими компаниями, даже не имеющими официальных веб-сайтов. В отчетах Trend Micro и Acronis было отмечено, что для сайдлоадинга вредоносного ПО использовался легитимный файл

winword.exe. Исследователи ASEC обнаружили, что для этой цели также использовались легитимные файлы VsGraphicsDesktopEngine.exe и rc.exe.

Активность, связанная с Ближним Востоком

Предупреждение агентства CISA об активности иранских кибергрупп

Федеральное бюро расследований США, Агентство по кибербезопасности и защите инфраструктуры (CISA), Агентство национальной безопасности США, Центр безопасности коммуникаций Канады, Федеральная полиция Австралии и Австралийский центр кибербезопасности при Австралийском управлении связи опубликовали совместный бюллетень по кибербезопасности, касающийся деятельности проиранских кибергрупп. Эти группы с октября 2023 года активно атакуют предприятия критической инфраструктуры в таких отраслях, как медицина и здравоохранение, государственное управление, информационные технологии, машиностроение и энергетика. Злоумышленники получают несанкционированный доступ к сетям с помощью брутфорс-атак, таких как password spraying, и бомбардировки запросами (push bombing и MFA fatigue) пользователей систем с многофакторной аутентификацией (МФА). Установив доступ, злоумышленники быстро регистрируют в системе МФА свои устройства, отключают легитимных пользователей и устанавливают контроль над взломанными учетными записями. В одном из описанных случаев злоумышленники через функцию самостоятельного сброса пароля (SSPR) в доступном из интернета интерфейсе Active Directory Federation Service (ADFS) сбросили старые пароли, а затем зарегистрировали новые устройства через решения для единого входа Okta для тех учетных записей, которые владельцы не успели защитить. Оказавшись внутри сети, злоумышленники развивают атаку, перемещаясь по инфраструктуре по RDP. В бюллетене уточняется, что для проникновения злоумышленники использовали системы Citrix, а затем с помощью Microsoft Word открывали PowerShell для запуска mstsc.exe с целью дальнейшего продвижения по RDP. В некоторых случаях они выполняли перебор Kerberos Service Principal Name (SPN) нескольких сервисных учетных записей, чтобы получить тикеты Kerberos, расширяя доступ к системам жертвы.

Бэкдор OrpaCrab/IOCONTROL

Исследователи компании QiAnXin XLab опубликовали результаты анализа OrpaCrab — Linux-бэкдора, нацеленного на системы производства

компанией ORPAK, которая специализируется на решениях для АЗС и транспортировки нефтепродуктов. Вредоносная программа была загружена на портал VirusTotal в январе 2024 года из США. Характерная черта OrpaCrab — использование протокола MQTT (Message Queuing Telemetry Transport) для связи с командным сервером. После установки OrpaCrab закрепляется с помощью скрипта, который должен запускаться автоматически из каталога /etc/rc3.d/. OrpaCrab использует режим шифрования AES-256-CBC для обфускации своей конфигурационной информации и протокол DNS по HTTPS (DoH) для разрешения доменного имени C2, что позволяет эффективно обходить в некоторых случаях мониторинг DNS. Бэкдор взаимодействует с командным сервером при помощи трех главных топиков MQTT для загрузки первичной информации об устройстве, получения инструкций и возвращения результатов исполнения команд. Зловред поддерживает возможность удаленного выполнения на системе произвольных команд, самоудаление и изменение конфигурации MQTT-брокера.

Компания Claroty присвоила вредоносу имя IOCONTROL. По словам исследователей, он был обнаружен на заправочной станции Gasboy, которая до этого была взломана хакерской группой CyberAv3ngers. Эту группу ранее связывали с кибератаками на системы водоснабжения, в которых эксплуатировались уязвимости в программируемых логических контроллерах Unitronics. По данным Claroty, вредоносное ПО внедрили в платежный терминал Gasboy OrPT. По оценке специалистов, злоумышленники, имея возможность контролировать платежный терминал, могли нарушать работу топливной компании и, потенциально, похищать данные банковских карт ее клиентов.

Активность и цели русскоязычных групп

Атаки Crypt Ghouls

В декабре 2023 года была обнаружена новая вредоносная активность, связанная с атаками шифровальщиков на российские компании и государственные структуры. Дальнейшее исследование привело экспертов «Лаборатории Касперского» к группе, получившей название Crypt Ghouls, и позволило выявить ее связь с другими группами. Crypt Ghouls использовали шифровальщики LockBit 3.0 и Babuk. Новая вредоносная активность группы пересекается с деятельностью MorLock, BlackJack, Twelve/ExCobalt и Shedding Zmiy. В арсенале Crypt Ghouls имеются такие распространенные инструменты, как Mimikatz, XenAllPasswordPro, PingCastle, Localtonet,

Resocks, AnyDesk, PsExec. Большинство русскоговорящих групп, нацеленных на российский бизнес и государственные структуры, использует общий инструментарий и схожие тактики, техники и процедуры. Жертвами атак становятся исключительно российские компании: горнодобывающие, энергетические, финансовые и торговые.

Атаки Awaken Likho/Core Werewolf

Исследователи «Лаборатории Касперского» обнаружили новую кампанию APT-группы Awaken Likho (так же известной как Core Werewolf), направленную на российские государственные учреждения, их подрядчиков и ряд промышленных предприятий. Кампания началась в июне 2024 года и продолжалась как минимум до августа. Злоумышленники существенно модифицировали инструментарий. Теперь они предпочитают использовать агент для легитимной платформы MeshCentral вместо модуля UltraVNC, при помощи которого они получали удаленный доступ к системам ранее. Судя по данным телеметрии, имплант загружался с вредоносного URL-адреса на устройства жертв предположительно через фишинговые письма. Сами письма отследить не удалось, однако в предыдущих кампаниях во вложениях содержались самораспаковывающиеся архивы (SFX) и ссылки на вредоносные модули. Как и в прошлых кампаниях, имплант распространялся в самораспаковывающемся архиве, созданном при помощи 7-Zip. Архив содержит пять файлов, четыре из которых замаскированы под легитимные системные службы и командные файлы. Пятый — агент MeshAgent. Злоумышленники создают задачу планировщика, запускающую командный файл, который, в свою очередь, запускает MeshAgent для установки соединения с сервером MeshCentral. Исследователи «Лаборатории Касперского» уверены, что новая версия этого вредоносного ПО все еще находится в стадии разработки.

По данным исследователей F6, Core Werewolf в начала использовать цепочку VBS-скриптов для UltraVNC. Группа также добавила в свой арсенал новый SSH-бэкдор. Злоумышленники продолжают атаковать российские промышленные предприятия. В октябре Core Werewolf маскировала свои документы-приманки под официальное письмо от заместителя министра обороны РФ и сообщение от Федеральной службы по техническому и экспортному контролю РФ (ФСТЭК). Последняя приманка, судя по контексту, предназначалась для предприятий электроэнергетики, оборонной промышленности и ракетно-космического комплекса.

Атаки Shadow/Twelve

Эксперты компании F6 опубликовали подробное исследование группы Shadow/Twelve, которая атакует крупный и средний российский бизнес, промышленные предприятия и правительственные организации. Исследователи пришли к выводу, что две группы, которые ранее считались независимыми друг от друга, на самом деле являются проектами единого хакерского синдиката. Целью Shadow является вымогательство, в то время как Twelve фокусируется на хактивизме, стремится нанести ущерб ИТ-инфраструктуре своих жертв. К июлю 2024 года злоумышленники атаковали как минимум 50 целей на российской территории. По данным исследователей, в процессе группа меняла свои названия на Comet и DARKSTAR. В качестве начальных векторов атаки она использует купленные на закрытых маркетплейсах учетные данные, сервисы удаленного доступа, такие как RDP и VPN, а также фишинг. В некоторых случаях злоумышленники покупали доступ к корпоративным почтовым ящикам и рассылали персонализированные фишинговые сообщения контактам из взломанных аккаунтов. Известны случаи, когда группа атаковала разработчиков программного обеспечения и системных интеграторов, чтобы через них получить доступ к системам их клиентов. Кроме того, атакующие использовали RCE-уязвимость в Atlassian Confluence (CVE-2023-22515, CVE-2023-22518), цепочку уязвимостей в Zimbra (CVE-2019-9670, CVE-2019-9621), цепочку уязвимостей в MS Exchange (CVE-2021-34473, CVE-2021-34523, CVE-2021-31207) и RCE-уязвимость в JetBrains TeamCity (CVE-2024-27198). В качестве первой точки компрометации для дальнейшего развития атаки злоумышленники обычно выбирают виртуальные системы, к которым редко подключаются сотрудники компаний. На финальном этапе атаки файлы виртуальной системы шифруются на скомпрометированном гипервизоре. В качестве резервного канала доступа (через SSH) группа часто использует взломанные системы на базе Linux. Интересно, что в процессе сбора конфиденциальных данных злоумышленники в том числе восстанавливали их с жестких дисков с помощью инструментов восстановления данных.

В атаках Shadow, Twelve, Comet, DARKSTAR использовались одни и те же инструменты, такие как Cobint и gpo.ps1, одинаковые строки в задачах Windows для запуска вредоносного ПО, а также ngrok в качестве одного из резервных каналов для доступа и выполнения других вредоносных действий. Для создания шифровальщиков злоумышленники применяют утекшие в публичный доступ билдеры и исходные коды LockBit 3.0 (Black) и Babuk для ESXi. Одним из фирменных приемов группы стал доступ к сессиям Telegram сотрудников компаний, что позволяло шпионить за ними и оказывать на них дополнительное давление.

Атаки RomCom

Исследователи компании ESET выяснили, что известная своими кибершпионскими операциями связанная с Россией группа RomCom (она же Storm-0978, Tropical Scorpius, UNC2596) причастна к кибератакам с использованием двух уязвимостей нулевого дня — в браузере Mozilla Firefox (CVE-2024-9680) и в Microsoft Windows (CVE-2024-49039). Если жертва, используя уязвимый браузер, попадает на контролируемый злоумышленниками фейковый веб-сайт, ее перенаправляют на сервер, содержащий zero click-эксплойт (не требующий действий пользователя), позволяющий злоумышленникам запустить произвольный код. Шелл-код загружает встроенную библиотеку, которая реализует «побег из песочницы», используя уязвимость в Windows Task Scheduler для получения повышенных привилегий. Библиотека использует недокументированную конечную точку RPC, доступ к которой должен был быть ограничен списком доверенных процессов, для запуска скрытого процесса PowerShell. Этот процесс загружает и исполняет троянца удаленного доступа RomCom RAT на взломанной системе. Собранные ESET данные телеметрии показывают, что большинство жертв, которые посещали зараженный сайт, находились в Европе и Северной Америке. В том же исследовании сообщается, что в 2024 году группа RomCom шпионила за предприятиями государственного, оборонного и энергетического секторов Украины и европейскими государственными структурами, а также атаковала фармацевтические и страховые компании США и юридические компании Германии.

Атаки Cloud Atlas

Эксперт «Лаборатории Касперского» опубликовал отчет о ранее неописанном наборе инструментов, которые Cloud Atlas активно использовали в 2024 году. Для первичного проникновения злоумышленники продолжают использовать фишинговые письма с вредоносными вложениями, нацеленными на уязвимость CVE-2018-0802. При открытии вложения загружается вредоносный шаблон RTF. Он содержит эксплойт для редактора формул, который скачивает и выполняет файл HTA. Скачивание шаблонов RTF и файлов HTA ограничено как по времени, так и по IP-адресам жертв: разрешаются запросы только из заданных регионов. Вредоносный файл HTA извлекает из себя и записывает на диск несколько файлов, являющихся частями бэкдора VBShower. В новой кампании VBShower скачивает и устанавливает другой бэкдор, PowerShower, который группа начала использовать в 2019 году для кражи учетных данных браузера, а также новый имплант VBCloud, похожий на PowerShower. Кроме того, было

замечено использование PowerShell Inveigh — утилиты для Machine-in-the-Middle-атак с подменой данных, а также для сбора хэшей и учетных данных.

Что касается статистики по жертвам, то данные телеметрии «Лаборатории Касперского» указывают на повышенное внимание к региону СНГ — активность злоумышленников была зафиксирована в России, Беларуси, Казахстане, Кыргызстане, Молдове, а также в Словакии и Турции. Список секторов, интересующих злоумышленников, существенно не изменился. Их главными мишенями остаются правительственные и военные структуры, промышленные предприятия, телеком и энергетика, а также некоммерческие организации.

Атаки Venture Wolf

Исследователи BI.ZONE обнаружили ранее неизвестный кластер, который они назвали Venture Wolf, активный как минимум с ноября 2023 года и нацеленный на промышленность, строительство, ИТ, телеком и другие сектора российской экономики. Злоумышленники используют различные загрузчики, чтобы доставлять в целевые системы вредоносное ПО MetaStealer. Venture Wolf распространяет архивы, содержащие загрузчик с расширением .com (реже .exe), а также один или несколько фишинговых документов, которые представляют собой изображения (JPG или PNG) или файлы PDF, DOC/DOCX и ODT. После запуска загрузчик либо создает файл-пустышку .NET, в который внедряется вредоносная нагрузка MetaStealer, либо внедряет ее в процесс RegAsm.exe. Загрузчики являются исполняемыми файлами формата PE. Их код обфусцирован. MetaStealer реализован на C# и является форком другого стилера — RedLine. Важное отличие MetaStealer от RedLine заключается в том, что MetaStealer можно применять в России и странах СНГ. В процессе выполнения MetaStealer собирает информацию о системе, получает данные из браузеров, криптокошельков, клиентов электронной почты и различных приложений, таких как Steam и FileZilla. Для обфускации кода MetaStealer используется протектор .NET Reactor.

Атаки Unicorn

Активность группы Unicorn была впервые зафиксирована исследователями «Лаборатории Касперского» в сентябре. С помощью вредоносных скриптов Trojan-Spy.VBS.Unicorn группа атакует российские энергетические компании, промышленные предприятия, поставщиков и разработчиков электронных компонентов. Позже исследователи F6 выяснили, что злоумышленники распространяли варианты кастомизированного вредоносного ПО под видом коммерческого предложения на покупку со

скидкой оборудования для СВО для его безвозмездной передачи в фонд для нужд военнослужащих. В ходе расследования деятельности группы Unicorn удалось обнаружить дополнительную инфраструктуру и связанные файлы, в том числе новые VBS-скрипты, файл HTA, фишинговые файлы LNK и файлы-приманки PDF. Один из файлов LNK и файл-приманка PDF отсылали к российскому разработчику электронных компонентов.

Атаки Sticky Werewolf/Angry Likho

По данным F6, злоумышленники из Sticky Werewolf продолжили свою кампанию MimiStick с использованием Sliver Implant и Quasar RAT, нацеленную на предприятия российской промышленности. Помимо продолжающейся кампании MimiStick, эксперты выявили вредоносные рассылки в адрес одного из НИИ, а также предприятия-поставщика материалов, оборудования и карьерной техники, где в качестве финальной нагрузки устанавливался троянец Darktrack RAT. Вредоносные письма содержали защищенные паролем RAR-архивы, открытие которых приводило к исполнению установщика NSIS, BAT-файла, загрузчика PowerShell и модуля downloader/injector. В итоге в системе устанавливается Darktrack RAT.

Исследователи «Лаборатории Касперского» опубликовали собственные результаты анализа тактик, техник и процедур группы. В дополнение к инструментарию, описанному F6, они обнаружили использование в цепочке атаки ZIP-архивов, файлов VBS и загрузчика Ande Loader, что в финале также приводило к загрузке Darktrack RAT. По данным «Лаборатории Касперского», группа нацелена на организации не только в России, но и в Беларуси. Злоумышленники используют сторонние сервисы для размещения и загрузки вредоносных файлов. Исследование инфраструктуры злоумышленников показало, что в их арсенале имеется множество других вредоносных инструментов, в том числе стилеры и троянцы удаленного доступа.

Атаки Andromeda/Gamarue

Cybereason обнаружили новый кластер командных серверов, ассоциирующихся с вредоносным ПО Andromeda/Gamarue, с помощью которого осуществляются атаки на производственные и логистические компании в Азиатско-Тихоокеанском регионе, предположительно с целью промышленного шпионажа. На основе доступных данных телеметрии исследователи предположили, что начальный вектор атаки — зараженные USB-накопители. Злоумышленники создавали файлы LNK с типовыми именами, имитирующими популярные имена USB-накопителей и файлов, чтобы обмануть жертву и побудить ее запустить вредонос. В одной из сред

исследователи обнаружили множественные случаи запуска процесса rundll32.exe для загрузки различных файлов DLL с именами в формате ~$W*.USBDrv или ~$W*.FAT32. Вскоре после этого процесс устанавливает соединение с командным сервером. В конечном итоге загружается и внедряется в svchost.exe бэкдор Andromeda/Gamarue. Продолжая исследование данных VirusTotal, специалисты идентифицировали кластер IP-адресов, которые использовались в качестве командных серверов.

Было обнаружено, что на платформе AlienVault Open Threat Exchange (OTX) один из вредоносных доменов Andromeda был ассоциирован с группой Turla (она же UNC4210). Согласно исследованию компании Mandiant, Turla/UNC4210 была замечена в адаптации старого образца бэкдора Andromeda для использования с захваченным группой командным сервером. Этот образец впервые был загружен на VirusTotal в 2013 году. Он распространяется через инфицированные USB-накопители. С учетом всех имеющихся данных Cybereason с некоторой степенью уверенности предполагает, что этот образец связан с кампанией группы Turla. Однако, по мнению исследователей «Лаборатории Касперского», неиспользуемые сервера или домены Andromeda могла на самом деле захватить не Turla, а другая русскоязычная группа — Tomiris. Несмотря на то что эксперты «Лаборатории Касперского» прослеживают связь между Turla и Tomiris, они продолжают считать их двумя разными группами.

Финансово-мотивированные атаки и прочее

Предупреждение агентства CISA о вымогателях BianLian

Федеральное бюро расследований США, Агентство по кибербезопасности и защите инфраструктуры (CISA) и Австралийский центр кибербезопасности при Австралийском управлении связи опубликовали совместный бюллетень по кибербезопасности, касающийся деятельности группы вымогателей BianLian, ее тактик, техник, процедур и индикаторов компрометации, выявленных в ходе расследования. С июня 2022 года от действий группы BianLian пострадали несколько организаций критической инфраструктуры США, включая критически важные предприятия производственного сектора. Кроме того, группа атаковала объекты критической инфраструктуры и предприятия сферы услуг и жилищного строительства в Австралии. Группа получает доступ к системам своих жертв с помощью действительных учетных данных RDP, использует инструменты с открытым исходным кодом и сценарии командной строки для обнаружения и сбора учетных данных. Для эксфильтрации данных

используется FTP, Rclone или Mega. Изначально злоумышленники из BianLian придерживались стратегии двойного вымогательства: сперва извлекали данные, а затем шифровали файлы на системе жертвы. Однако примерно в январе 2024 года они перешли к вымогательству только на основе эксфильтрации и перестали шифровать файлы. Злоумышленники получают первичный доступ путем атаки на инфраструктуру Windows и ESXi, возможно, с помощью цепочки эксплойтов ProxyShell (CVE-2021-34473, CVE-2021-34523, CVE-2021-31207). Они используют Ngrok и модифицированный Rsocks для маскировки направления трафика с помощью туннелей SOCK5, эксплуатируют уязвимость CVE-2022-37969 для повышения привилегий в Windows 10 и 11, а чтобы избежать обнаружения переименовывают бинарные файлы и задания, присваивая им имена легитимных служб и продуктов безопасности Windows. Группа использует PowerShell для сжатия собранных данных перед эксфильтрацией и новый Tox ID для связи со своими жертвами и отправки им записок с требованием выкупа. Примечательно, что записки печатаются на принтерах, подключенных к взломанной сети.

Атаки Interlock

Исследователи компании Fortinet опубликовали отчет, касающийся нового шифровальщика под названием Interlock. Шифровальщик был впервые найден на общедоступном сайте для сканирования файлов в начале октября 2024 года, но, судя по всему, его распространяли и раньше. Interlock доступен в двух версиях: для Windows (Vista, 7, 8, 8.1 и 10) и FreeBSD. Начальный вектор заражения пока неизвестен, но исследователь Сина Хейрха сообщил, что обнаружил на компьютере жертвы ранее неизвестный бэкдор Supper, через который и мог быть развернут шифровальщик. Interlock шифрует файлы на компьютере при помощи алгоритма шифрования AES-CBC. На момент публикации на сайте утечек Interlock значилось шесть пострадавших, пять из которых находятся в США и один в Италии. Для каждой жертвы злоумышленники создают на своем сайте утечек в сети Tor отдельную страницу с описанием организации и списком украденных файлов. Однако данные телеметрии указывают на гораздо большее число жертв. Образцы шифровальщика были замечены в Индии, Италии, Японии, Германии, Перу, Южной Корее, Турции и США. Пострадали организации в сферах образования, финансов, государственного управления, здравоохранения и промышленного производства.

Атаки TA866/Asylum Ambuscade

Исследователи из команды Cisco Talos идентифицировали активность финансово мотивированной группы TA866 (она же Asylum Ambuscade), которая вовлечена во вредоносные и, возможно, кибершпионские кампании как минимум с 2020 года. Для своих атак TA866 использует комбинацию из стандартных и кастомизированных инструментов, часто в сотрудничестве с другими киберпреступными группами. С начала 2023 года злоумышленники изменили способ распространения вредоносного ПО и начали использовать спам-рассылку и вредоносную рекламу для перенаправления жертв в системы распределения трафика (TDS), такие как 404 TDS, с помощью которых происходит доставка вредоносных программ. Было замечено, что группа использует в том числе тактику перехвата электронной переписки (email thread hijacking). Цепочка заражения обычно начинается с вредоносного JavaScript-загрузчика и приводит к развертыванию вредоносного ПО WasabiSeed, которое в свою очередь доставляет дополнительную полезную нагрузку, в том числе ScreenShotter и AHK Bot. Арсенал вредоносных инструментов включает бэкдор Resident, маяки Cobalt Strike, CSharp-Streamer-RAT и Rhadamanthys, которые используются на стадии посткомпрометации. Нередко TA866 устанавливает на взломанные системы инструменты удаленного доступа, такие как AnyDesk и Remote Utilities. Большинство случаев развертывания полезной нагрузки было замечено в США, остальные — на территории Канады, Великобритании, Германии, Италии, Австрии и Нидерландов. Чаще всего жертвами становились предприятия производственного сектора, за ними следуют правительственные и финансовые организации. Недавно исследователи обнаружили связь между деятельностью TA866 и других киберпреступных групп, таких как ShadowSyndicate, а также с кампаниями, организованными вымогателями из ALPHV и IcedID.

Атаки Akira/Howling Scorpius

Команда Unit 42 компании Palo Alto Networks опубликовала статью о группе Howling Scorpius, которая использует шифровальщик Akira для операционных систем Windows и Linux/ESXi. Злоумышленники постоянно обновляют методы атак. По информации исследователей, группа нацелена на малые и средние предприятия в различных секторах экономики на территории Северной Америки, Европы и Австралии, включая: образование, строительство, консалтинг, транспорт и логистику, государственное управление, телекоммуникации, технологический сектор и фармацевтику. Чаще всего целью становятся промышленные производства. Для первичного проникновения Howling Scorpius покупают в даркнете учетные записи VPN-

сервисов, не защищенные многофакторной аутентификацией, атакуют сервисы удаленного доступа, такие как RDP и используют целевой фишинг. Основные инструменты для извлечения учетных данных с целью повышения привилегий, — это Mimikatz и LaZagne. Злоумышленники получают контроль над учетными записями служб и доступ к хранящимся в памяти учетным данным с помощью атаки Kerberoasting. Они копируют куст реестра SYSTEM и файл NTDS.dit с контроллера домена, чтобы получить полный список учетных записей пользователей и соответствующие им хэши паролей. Для закрепления группа создала новые доменные учетные записи. Перемещение внутри взломанных сетей в основном происходит через эксплуатацию уязвимостей сервисов удаленного доступа, таких как RDP и SMB. Злоумышленники, связанные с группой, используют инструменты сканирования сети, такие как NetScan и Advanced IP Scanner, и с помощью команд PowerShell и Windows Net собирают информацию о пользователях и администраторах в Active Directory. Они применяют метод BYOVD (Bring Your Own Vulnerable Driver), используя драйвер антивируса Zemana для отключения защитного ПО. В процессе атаки на виртуальные системы злоумышленники создают собственные новые виртуальные машины, на которых отключают Windows Defender, подключают к ним жесткие диски, останавливают (отключают) работающие с ними виртуальные машины, чтобы высвободить заблокированные файлы, а затем запускают на созданных виртуальных машинах шифровальщик, обходя таким образом инструменты EDR.

Атаки Water Makara

Стало известно о новой кампании целевого фишинга, направленной на предприятия в странах Латинской Америки, особенно в Бразилии. Злоумышленники доставляют банковское вредоносное ПО под названием Astaroth (также известное как Guildma) с помощью обфусцированного кода JavaScript. Trend Micro отслеживает эту активность как Water Makara. По данным компании, эта активность нацелена в основном на производственные организации, предприятия розничной торговли и государственные учреждения. Строительство, автомобилестроение и сельское хозяйство также занимают верхние строчки в списке атакованных секторов. Mandiant присвоила похожей кампании с доставкой того же самого вредоносного ПО пользователям в Бразилии название PINEAPPLE. Обе эти кампании схожи в том, что начинаются с рассылки фишинговых сообщений от имени государственных структур, например от налоговой службы Бразилии Receita Federal, чтобы обманом вынудить получателей загрузить вложенный ZIP-архив под видом налоговых документов. Вредоносный ZIP-файл содержит ярлык Windows (файл LNK), который

использует процесс mshta.exe и выполняет обфусцированный код JavaScript для установки соединения с командным сервером.

Операция Cobalt Whisper

Исследователи SEQRITE Labs обнаружили кампанию кибершпионажа, получившую название Operation Cobalt Whisper. Она затронула множество секторов экономики в Гонконге и Пакистане, включая оборону, образование, экологическую инженерию, электротехнику, энергетику, кибербезопасность, авиацию и здравоохранение.

SEQRITE идентифицировала более 20 цепочек заражения, в которых использовались RAR- и ZIP-архивы, содержащие документы-приманки в формате PDF и файлы LNK. Процесс заражения состоит из двух этапов: сначала файл LNK выполняет VBSript, чтобы закрепиться и скрыть активность, а затем маяк Cobalt Strike, замаскированный под легитимный исполняемый файл, устанавливает связь с атакующим. SEQRITE относит разные кластеры активности к кампании Operation Cobalt Whisper на основании пути к файлам, ID компьютеров и тому подобных артефактов. Кроме того, в этих кластерах прослеживаются похожие паттерны связи с командными серверами, зарегистрированными в инфраструктуре Tencent.

Атаки UAC-0185

Украинский центр реагирования на компьютерные инциденты CERT-UA опубликовал информацию о вредоносной кампании, направленной на предприятия оборонно-промышленного комплекса Украины. Злоумышленники рассылали поддельное письмо от имени Украинского союза промышленников и предпринимателей, содержащее URL-адрес, по которому загружался файл LNK. В результате его выполнения загружался документ-приманка и выполнялся код JavaScript, который в свою очередь запускал две команды PowerShell. В финале цепочки загружался ZIP-архив и устанавливался MeshAgent RAT. По мнению CERT-UA, за атакой стоит группа UAC-0185 (она же UNC4221), которая активна как минимум с 2022 года. Цели группы — кража учетных данных мессенджеров Signal и Telegram, а также систем военного назначения, таких как DELTA и TENETA.

Атаки SmokeLoader

В сентябре 2024 года исследователи FortiGuard Labs выявили атаку с использованием вредоносной программы SmokeLoader на Тайване. Под удар попали компании из сферы производства, здравоохранения, ИТ и других отраслей. Как выяснили FortiGuard Labs, атака начиналась с

фишингового письма с вложенным файлом Microsoft Excel. Открытие этого файла приводило к эксплуатации старых уязвимостей (включая CVE-2017-0199 и CVE-2017-11882). В результате через VBS устанавливался загрузчик Ande Loader, который в свою очередь использовался для развертывания SmokeLoader на скомпрометированном хосте. SmokeLoader состоит из двух компонентов: стейджер и основной модуль. Задача стейджера — обеспечить закрепление в системе и дешифровать, распаковать и внедрить основной модуль в процесс explorer.exe. Основной модуль отвечает за коммуникацию с командным сервером и загрузку плагинов. Зловред поддерживает несколько плагинов, которые могут похищать учетные данные для входа в систему и FTP, адреса электронной почты, куки-файлы и другую информацию из браузеров, Outlook, Thunderbird, FileZilla и WinSCP.

Атаки с использованием стилера Lumma и Amadey Bot

Cyble Research and Intelligence Labs идентифицировали вредоносную кампанию с использованием файла-приманки LNK, нацеленную на предприятия производственного сектора. Файл маскируется под PDF и размещен на удаленном сервере WebDAV. Ссылка на него, как правило, приходит в фишинговом письме. Вредоносный LNK-файл размещается по URL-адресу, который маскируется под LogicalDOC — облачную систему управления документацией, которой часто пользуются в производственных и инжиниринговых организациях. В ходе кампании используется несколько двоичных файлов Living-off-the-Land Binaries (LOLBin), например ssh.exe, powershell.exe и mshta.exe. В цепочку атаки входит сайдлоадинг DLL при помощи легитимного файла syncagentsrv.exe и загрузчика IDAT Loader, что приводит к развертыванию стилера Lumma и зловреда Amadey Bot. Это дает возможность атакующему установить контроль над компьютером жертвы и похищать конфиденциальную информацию. Неизвестные злоумышленники, стоящие за этой вредоносной кампанией, используют URL-адрес AMP-страницы Google и сокращенный URL-адрес, чтобы избежать обнаружения обычными URL-сканерами. Чтобы обеспечить закрепление в скомпрометированной системе, атакующие используют Task Scheduler.

Kaspersky Industrial Control Systems Cyber Emergency Response Team (Kaspersky ICS CERT) is a global Kaspersky project aimed at coordinating the efforts of automation system vendors, industrial facility owners and operators, and IT security researchers to protect industrial enterprises from cyberattacks. Kaspersky ICS CERT devotes its efforts primarily to identifying potential and existing threats that target industrial automation systems and the industrial internet of things.

Kaspersky ICS CERT ics-cert@kaspersky.com