Kaspersky ICS CERT

kaspersky

APT- и финансовые атаки на промышленные организации в третьем квартале 2025 года

27.11.2025

Версия 1.0

Данный обзор представляет собой сводку публикаций об APT- и финансовых атаках на промышленные предприятия, информация о которых была раскрыта в третьем квартале 2025 года, а также о связанной с ними активности групп, замеченных в атаках на промышленные организации. 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.

Выводы по итогам квартала

Третий квартал 2025 года стал богатым на технические детали атак, в которых пострадали промышленные организации по всему миру. В эту статью мы включили больше историй, чем в сводке за прошлый квартал, и значительно больше, чем вошло в статью за третий квартал 2024 года.

Из отчетов и технических статей различных исследователей об атаках на промышленные организации, опубликованных в этом квартале, можно сделать немало выводов. Одни тривиальны и ожидаемы, так как свидетельствуют о тенденциях в изменении ландшафта угроз промышленным предприятиям, замеченных еще ранее, либо лежат в общем фарватере более масштабных процессов, влияющих на кибербезопасность вообще. Другие могут показаться неожиданными и парадоксальными. Есть среди них и такие, которые подсвечивают проблемы безопасности, к которым, казалось бы, давно стоило бы привыкнуть, но никак не получается – вероятно, не позволяет чувство справедливости.

Искусственный интеллект на службе злоумышленников

Ожидаемо, «искусственный интеллект» – вещь полезная не только для аналитиков, инженеров, трейдеров, журналистов, руководителей предприятий, государственных служащих и простых обывателей, но и для злоумышленников. В этом квартале мы чуть больше узнали о способах его использования в атаках на промышленные предприятия.

- Первый и самый очевидный из них – использование его как чистой абстракции. Злоумышленники давно оседлали волну интереса к новым технологиям своих потенциальных жертв и подсовывают вредоносный код под видом всяческих AI-инструментов. Так, в атаках на ближневосточные организации для доставки бэкдора PipeMagic злоумышленники в ряде случаев использовали загрузчик, который распространялся ими под видом клиента ChatGPT.

- Второй, также очевидный – использовать AI в работе по прямому назначению. Так, операторы вымогательской платформы GLOBAL GROUP собрали на чат-ботах с искусственным интеллектом автоматизированную систему для ведения переговоров о выкупе – чтобы не заморачиваться с обучением сотрудников английскому языку.
- Ну и очевидно, что можно комбинировать различные способы использования AI, как поступили, например, злоумышленники, которых даже прозвали EvilAI, – они и маскировали свое вредоносное ПО под инструменты повышения (за счет AI) производительности, и разрабатывали его частично с использованием LLM – используя ее, чтобы придать вредоносному коду вид легитимного.

Использование родовых и исторических проблем безопасности традиционных операционных и прочих ИТ-систем

Как мы и не только мы неоднократно говорили и писали, экспертам кибербезопасности не добиться окончательной победы в противостоянии со злоумышленниками, пока повсеместно используются ИТ-системы и технологии, разработанные без учета потребностей кибербезопасности, к которым относится, в частности, и большинство ОС общего назначения, включая и самые современные. Родовые проблемы безопасности в них, включая архитектурные, не только увеличивают поверхность атаки, но и способствуют ее развитию, затрудняя автоматическое обнаружение и блокировку вредоносной активности.

DLL hijacking / sideloading

Одна из наиболее часто используемых злоумышленниками архитектурных проблем ОС Windows, которая позволяет разработчикам (включая и саму Microsoft) создавать небезопасные приложения, в контекст которых злоумышленники могут загрузить свой вредоносный код, подменив легитимную динамическую библиотеку своей. Такой подход может значительно затруднить обнаружение и блокировку вредоносной активности. Дело в том, что защитные решения из соображений обеспечения производительности защищаемой системы не могут одинаково глубоко анализировать поведение всех запущенных процессов, и поэтому вынуждены снижать глубину анализа для многих процессов самой операционной системы и доверенных приложений.

- Метод DLL sideloading применялся в атаках на организации телекоммуникационного и производственного секторов в странах Центральной и Южной Азии с использованием вредоноса PlugX и в атаках вымогателя Charon на ближневосточные организации – при развертывании шелл-кода.
- Вредоносные компоненты MiniBike, использованные в атаках на европейские телекоммуникационные, аэрокосмические и оборонные предприятия, компилируются индивидуально под жертву и запускаются посредством DLL sideloading. При этом применяется характерный метод модификации таблиц экспорта оригинальных легитимных DLL для «бесшовной интеграции» вредоносного кода.
- Исследователи также рассказали еще о паре интересных методов DLL hijacking. Первый продемонстрировали упомянутые выше злоумышленники, атакующие организации с помощью PipeMagic: в одном из вариантов его загрузчика динамическая библиотека для исполняемого файла обновления Google Chrome содержала вредоносный код в функции DllMain. Второй продемонстрировала группа Nimbus Manticore в атаках на оборонные, телекоммуникационные и авиационные предприятия Западной Европы с использованием бэкдора MiniJunk. В процессе запуска бэкдора техника DLL sideloading применяется дважды. И первый раз – весьма нестандартным образом – посредством манипуляции параметром DllPath структуры RTL_USER_PROCESS_PARAMETERS, используемой в недокументированном низкоуровневом NT API. Этот параметр определяет путь поиска DLL-библиотеки, если она не найдена в директории приложения. Таким образом вредонос загружается из директории, в которую он был скопирован при разархивировании, в память процесса, относящегося к Windows Defender, запущенного совсем из другой директории.

BYOVD (Bring Your Own Vulnerable Driver)

Помимо загрузки вредоносного кода из контекста доверенных приложений, что позволяет усложнить его обнаружение и блокировку, злоумышленники могут выполнять вредоносные действия при помощи легитимного кода на уровне ядра ОС – устанавливая в систему или используя уже имеющиеся легитимные драйверы. С их помощью злоумышленники могут иногда полностью отключить или частично ослепить защитное решение (отключив для него, например, возможность перехвата важных системных операций – запуска процессов, открытия файлов и т. д.). Надежная защита ото всех таких сценариев может быть обеспечена только самой ОС. Однако современные

ОС общего назначения (такие как Windows и Linux) такой защиты не предоставляют, и разработчикам защитных решений приходится изобретать всевозможные способы минимизации этого риска.

- В текущем квартале исследователи опубликовали две истории об атаках на промышленные организации, в ходе которых злоумышленники использовали такой подход. Примечательно, что обе рассказывают об операциях вымогателей (Crypto24 и The Gentlemen), а не о действиях APT, что лишний раз свидетельствует о том, что некоторые вымогатели перешли в категорию «продвинутых» во многих смыслах злоумышленников.

Уязвимости нулевого дня

Расширение функциональности ядра ОС установкой дополнительного драйвера – удобное архитектурное решение для третьесторонних разработчиков аппаратных компонентов и периферии или требовательных к производительности приложений, но совершенный кошмар с точки зрения безопасности системы, как мы уже обсудили выше. **К сожалению, уязвимости существуют не только в драйверах от третьесторонних вендоров, но и в драйверах, разрабатываемых и поддерживаемых разработчиками самих ОС общего назначения.** И они тоже используются в атаках, в том числе, и на промышленные организации.

- Об одном таком случае рассказали в этом квартале наши коллеги по «Лаборатории Касперского». Речь идет о CVE-2025-29824 – уязвимости повышения привилегий в драйвере Common Log File System (CLFS), дающей возможность чтения и записи памяти ядра. Удивительно, что это уже 33-я по счету уязвимость, обнаруженная в этом драйвере и четвертая из тех, что эксплуатировались злоумышленниками в атаках. Исследователи предположили, что проблемы безопасности в этом драйвере, по всей видимости, имеют два корня. Первый – в архитектуре системы хранения обрабатываемых им логов, точнее в их формате: они хранят в явном виде структуры данных ядра, включая указатели на память ядра. Вторая – в архитектуре самого драйвера: чтобы защитить ОС от «экранов смерти» при падении драйвера, разработчики обложили его код обработчиками всевозможных исключений, которые маскируют ошибки в коде и затрудняют их обнаружение при помощи фаззинга. Примечательно еще и то, что в этот раз уязвимость нулевого дня была обнаружена в атаках группировки вымогателей, а не APT.

Уязвимости нулевого дня в популярных приложениях, может и не так опасны, как уязвимости в коде, выполняемом в контексте ядра ОС, но они тоже могут давать злоумышленникам существенные преимущества на различных этапах атаки, и в первую очередь на этапах первоначального проникновения и закрепления в системе.

- В этом квартале исследователи рассказали две истории об атаках на промышленные организации с использованием эксплойта к уязвимости нулевого дня CVE-2025-8088 в WinRAR, дававшего злоумышленникам шанс обмануть жертву и обойти защитное решение. Примечательно, что эксплойт этой уязвимости стал применяться в атаках киберкриминальной группировки RomCom раньше, чем в APT-операциях Paper Werewolf/GOFFEE.

Недопатчи и Won't Fix

Еще одной из самых серьезных проблем сложившегося подхода к обеспечению безопасности ИТ- и ОТ-систем, включая их ключевые компоненты, такие как ОС, является относительно невысокий приоритет этой задачи для самих разработчиков, результатом чего мы нередко видим небрежность при разработке и выпуске исправлений безопасности или полное нежелание их выпускать. В этом квартале исследователи безопасности рассказали публично две истории, подтверждающие эту мысль.

- Первая повествует о цепочке уязвимостей ToolShell, которая использовалась в атаках на серверы SharePoint, работающие в сетях организаций во многих странах, в том числе промышленных. Первоначально выпущенные Microsoft исправления (CVE-2025-49704 и CVE-2025-49706) оказались недостаточными. По утверждению исследователей, для их обхода в коде эксплойта достаточно было поменять всего один байт. Разработчику пришлось исправлять уязвимости второй раз выпуском CVE-2025-53770 и CVE-2025-53771.
- Вторая рассказывает об атаках брокеров доступа на ASP.NET-приложения, в том числе и на публично доступных ресурсах промышленных компаний. Злоумышленники похищали «машинные ключи» и внедряли, используя их, вредоносные модули в память IIS (Internet Information Services) – веб-сервера от Microsoft. Эта техника известна с 2014 года как «Десериализация Viewstate» и эксплуатировалась в атаках на различные ASP.NET-сервисы, использующие технологию сериализации, проблему безопасности которой Microsoft пометила как «Won't Fix».

Обход UAC

Еще одна системная проблема безопасности современных ИТ- и ОТ-сред заключается в том, что разработчики их ключевых компонентов, таких как ОС, даже разработав механизм повышения их безопасности, не всегда заботятся о поддержании его эффективности – другие функциональные элементы системы, параллельно разрабатываемые и внедряемые ее разработчиками, часто могут давать злоумышленникам возможность обойти ранее внедренную защитную меру. Так получилось, например, с механизмом UAC (User Account Control), который требует дополнительного подтверждения пользователя системы, когда запущенный от его имени процесс пытается выполнить привилегированное действие. Поскольку среди таких процессов есть и системные, этот механизм имеет множество исключений, дающих злоумышленнику возможность его обойти. На сегодняшний день известно несколько десятков техник обхода UAC, многие из которых мы нередко видим в атаках, в том числе и на промышленные предприятия.

- Один из таких случаев описан в упомянутой выше компании вымогателей Crypto24, в ходе которой злоумышленники обходили UAC одним из наиболее часто используемых методов – эксплуатации COM-интерфейса CMSTPLUA.

Использование доверительных отношений

Всем известно, что, помимо проблем чисто технических, некоторые из которых мы описали выше, злоумышленники повсеместно эксплуатируют организационные недостатки своих вероятных жертв, используют психологические приемы в разработке методов социальной инженерии, действуя в том числе и «на доверии». Однако и доверительные отношения между людьми и организациями, в свою очередь, часто имеют, помимо чисто психологических и коммуникативных, еще и сугубо техническое выражение. Это могут быть дополнительные каналы связи, обходящие периметр безопасности или слабее покрытые защитными мерами, и отсутствие технической возможности одной стороной полностью и досконально проверить состояние информационной безопасности технологических компонентов и различных цифровых артефактов, предоставляемых ей другой.

- Из опубликованных в квартале технических историй к наиболее интересным можно отнести атаку китайскоязычных APT-групп, нацеленных на организации телекоммуникационного, правительственного, транспортного, военного и жилищного секторов

разных стран. Основное внимание злоумышленников сосредоточено на ядрах сети крупных телекоммуникационных провайдеров, а также на пограничных маршрутизаторах провайдеров и клиентских организаций. Скомпрометированные устройства и доверенные отношения используются далее для компрометации сетей все новых жертв.

Легитимные, в том числе украденные сертификаты для цифровой подписи

Самый частый из способов автоматизации отношений доверия в ИТ и ОТ основан на использовании механизмов криптографической подписи. Так, почтовый сервер подписывает отправляемые им сообщения электронной почты ключом DKIM, чтобы сервер-получатель мог удостовериться, что письмо, прошедшее на своем пути, возможно, множество релеев, отправлено именно с заявленного сервера. Отправитель письма подписывает его с использованием механизмов SMIME или PGP, чтобы его читатель мог уверенно идентифицировать отправителя и убедиться заодно, что содержимое письма не поменялось при доставке. ОС проверяет цифровую подпись исполняемого файла перед запуском, чтобы удостовериться, что он был создан легитимным разработчиком и не был изменен после создания. Специализированное защитное решение проверяет ее же, чтобы выбрать уровень глубины анализа поведения приложения (о чем написано выше в главе про DLL hijacking). К сожалению, злоумышленники, завладев приватным ключом подписи, могут им воспользоваться, чтобы обмануть механизмы доверия. И сделать они это могут либо методом кражи (украв ключ у законного владельца), либо методом обмана удостоверяющего центра (например, создав липовую организацию или, в некоторых случаях, временно захватив доменную зону легитимной организации). Два подобных случая попали в опубликованные в этом квартале истории об атаках на промышленные организации.

- Так, Subtle Snail в атаках на европейские телекоммуникационные, аэрокосмические и оборонные предприятия, как минимум с мая 2025 года, использует цифровую подпись для своих вредоносных программ – все вредоносные бинарные файлы, задействованные в атаках группы, подписаны действительным цифровым сертификатом, выданным SSL.com голландской компании Insight Digital B.V.
- GhostRedirector, которые скомпрометировали как минимум 65 серверов Windows образовательных, медицинских, страховых, транспортных, торговых и ИТ-организаций в нескольких странах , подписывали некоторые из своих вредоносов сертификатом,

выданным TrustAsia RSA Code Signing CA G3 разработчику (Shenzhen Diyuan Technology Co., Ltd.)

В обоих случаях из опубликованных статей неясно, как злоумышленникам удалось завладеть сертификатом.

Использование скомпрометированных почтовых ящиков

Последний из способов использования доверительных отношений, попавший в опубликованные в этом квартале технические статьи об атаках на промышленные организации, относится к эксплуатации доверия между людьми. Он же помогает и снизить вероятность обнаружения вредоносной активности некоторыми из автоматизированных средств защиты. Когда вы получаете письмо от известного вам («доверенного») контрагента, особенно, если оно отправлено в продолжение вашей с ним переписки, вы скорее всего, не задумываясь, откроете вложение, перейдете по ссылке или сделаете какое-то другое неосторожное действие, к которому вас подталкивает текст письма, ведь оно прошло автоматизированную проверку на корпоративном спам- и фишинг-фильтре и не содержит явных подозрительных признаков. Поэтому многие злоумышленники очень любят получать доступ к легитимным почтовым ящикам и часто используют их в своих последующих атаках. В одной из своих статей мы как-то раскрыли целую экосистему злоумышленников, действующих преимущественно таким методом.

- Paper Werewolf/GOFFEE в упомянутой выше вредоносной кампании отправляли российским и узбекским организациям электронное письмо от имени крупного научно-исследовательского института. При этом они использовали скомпрометированный электронный адрес, принадлежащий другой компании – поставщику мебели.
- APT-группа Head Mare/PhantomCore в масштабной кампании кибершпионажа против организаций России, включая промышленные, получали первичный доступ к сетям жертв фишинговыми рассылками. При этом злоумышленники использовали скомпрометированные почтовые ящики легитимных российских компаний.
- Группа Tomiris целенаправленно рассылала фишинговые письма российским государственным учреждениям, а также энергетическим, горнодобывающим и производственным предприятиям. Отправителями писем якобы были госслужащие Кыргызстана. В одном из таких писем использовался реальный электронный адрес, указанный на сайте регулятора Кыргызской Республики. По всей

видимости, этот адрес был ранее скомпрометирован для использования в атаках.

- ComicForm целенаправленно атакует российские компании в промышленном, финансовом, туристическом, биотехнологическом, исследовательском и торговом секторах, а также организации в Беларуси и Казахстане. Злоумышленники распространяют вредоносное ПО, рассылая фишинговые письма с электронных адресов, зарегистрированных в доменах верхнего уровня .ru, .by и .kz. Некоторые адреса, предположительно, были скомпрометированы.
- Группа UNK_FistBump атаковала организации, занимающиеся проектированием, производством и поставками изделий из полупроводников, фишинговыми письмами рекрутерам и сотрудникам HR-отделов, в которых злоумышленники представлялись выпускниками вуза, ищущими работу, при этом используя скомпрометированные почтовые ящики Национального университета Тайваня.

Безразличие и безалаберность

Ну и последняя и, возможно, самая вопиющая проблема информационной безопасности промышленных предприятий – недостаток внимания к ней со стороны ответственных сотрудников. В этом квартале исследователями опубликовано две статьи, которые особенно выразительно подсвечивают ее актуальность.

- Cisco Talos совместно с Федеральным бюро расследований опубликовали предупреждение об активности APT-группы, эксплуатирующей уязвимость CVE-2018-0171 (которой уже семь лет) в пограничных маршрутизаторах организаций, имеющих отношение к критической инфраструктуре.
- Исследователи Palo Alto Networks рассказали об атаках, в ходе которых эксплуатировалась критическая (с рейтингом CVSS 10.0) уязвимость CVE-2025-32433 в реализации сервера SSH в составе Open Telecom Platform, обнаруженная и исправленная в апреле 2025 года. Примечательно, что в общей сложности около 70% всех попыток эксплуатации (которых исследователи всего насчитали более 3000) пришлось на доступные из интернета специализированные файрволы, предназначенные для разграничения коммуникаций между ИТ и технологической сетями и, скорее всего, не рассчитанные на противодействие великому множеству угроз, которые могут достичь их из интернета.

Активность русскоязычных групп

Атаки RomCom

Киберкриминал

Целевой фишинг

Уязвимость нулевого дня

Бэкдор

Исследователи ESET обнаружили ранее неизвестную уязвимость в WinRAR, которую активно эксплуатирует группа RomCom (она же Storm-0978, Tropical Scorpius или UNC2596). Это уже как минимум третий зафиксированный случай, когда RomCom использует 0-день. Уязвимость, которой присвоили идентификатор CVE-2025-8088, позволяет обходить защитные решения за счет применения альтернативных потоков данных. После уведомления WinRAR оперативно выпустила исправленную версию 30 июля 2025 года.

Уязвимость позволяет злоумышленникам скрывать вредоносные файлы внутри архивов. Эти файлы незаметно запускаются в момент извлечения данных. В результате на скомпрометированные системы устанавливаются различные бэкдоры из арсенала RomCom, а именно специализированный вариант SnipBot, RustyClaw и агент Mythic. Данная кампания была направлена против финансовых, производственных, оборонных и логистических организаций в Европе и Канаде.

Атаки Static Tundra

APT

Эксплуатация сетевых устройств

Имплант прошивки

Cisco Talos совместно с Федеральным бюро расследований опубликовали предупреждение о кибершпионской активности прогосударственной группы, эксплуатирующей уязвимость в технологии Cisco Smart Install. Уязвимость CVE-2018-0171, которой уже семь лет, связана с некорректной проверкой ввода в уже не поддерживаемом функционале Cisco Smart Install программного обеспечения Cisco IOS и Cisco IOS XE. После анализа тактик, техник и процедур атакующих, а также списка пострадавших организаций исследователи Cisco Talos приписали эту активность группе Static Tundra и предположили, что она является подразделением APT-группы Energetic Bear (так же известной как Crouching Yeti, Berserk Bear и Dragonfly).

Кампания была направлена на устаревшие устройства, на которые больше не устанавливались обновления, и затронула организации в телекоммуникационном и производственном секторах, а также в сфере высшего образования по всему миру. Пользователям настоятельно рекомендуется установить исправление или, если это невозможно, отключить функцию Smart Install. По данным Cisco Talos, целью злоумышленников было похищение конфигурационных данных и получение постоянного доступа к уязвимым системам. Static Tundra давно

демонстрирует весьма изощренные методы работы: стоит вспомнить имплант прошивки SYNful Knock, появившийся еще в 2015 году, а также специальные SNMP-инструменты, позволяющие получать доступ к системам и оставаться незамеченными в течение многих лет.

Атаки Curly COMrades

Ранее неизвестный актор

Компрометация сайтов

Бэкдор

Исследователи Bitdefender описали активность вредоносного кластера, которую отслеживали с середины 2024 года, и раскрыли новую группу – Curly COMrades. Эта группа целенаправленно атакует важные организации в постсоветских странах. Среди ее целей – судебные и правительственные структуры Грузии, а также одна из энергетических компаний в Молдове. Основная задача Curly COMrades – получить долгосрочный доступ к сетям жертв и похитить учетные данные. Для этого злоумышленники применяют прокси-инструменты, такие как Resocks, SSH и Stunnel, чтобы создать несколько точек входа во внутренние сети. Затем они используют скрипт AtExec для удаленного выполнения команд. Злоумышленники внедряют новый бэкдор MucorAgent, для закрепления его в системе используют нетривиальную технику: перехватывают задачи планировщика, отвечающие за запуск NGEN (Native Image Generator) – оптимизатора производительности .NET-приложений, который периодически или при некоторых обстоятельствах (например, при обновлении .NET Framework) перекомпилирует код .NET в машинный. Для ретрансляторов трафика используются скомпрометированные легитимные сайты. В атаках злоумышленники стараются добраться до NTDS базы контроллеров домена – основного хранилища аутентификационных данных в Windows-инфраструктуре. Кроме того, они крадут дампы памяти LSASS на определенных системах, чтобы восстановить учетные данные активных пользователей.

Атаки, нацеленные на российские организации

Атаки UNG0901/Операция CargoTalon

Ранее неизвестный актор

Целевой фишинг

Бэкдор

Исследователи Seqrite Labs раскрыли кибершпионскую кампанию, получившую название «Операция CargoTalon», нацеленную на российские организации. Вредоносная активность с использованием бэкдора EAGLET была связана с кластером UNG0901 (Unknown Group 901). Жертвами стали сотрудники авиастроительного объединения, о чем свидетельствует вредоносный файл из электронной почты, обнаруженный в VirusTotal. Атаки начались с рассылки фишинговых писем с вложенным архивом

«Транспортная_накладная_ТТН_№391-44_от_26.06.2025.zip». Внутри архива находился LNK-файл, который с помощью PowerShell отображал поддельный XLS-документ и одновременно запускал через rundll32.exe файл EAGLET.

EAGLET предназначен для сбора системной информации, он устанавливает соединения с жестко закодированным удаленным сервером и выполняет команды на скомпрометированном компьютере. Имплант предоставляет доступ к командной строке, а также возможность загрузки и скачивания файлов. При этом точный характер вредоносного ПО следующего этапа остался невыясненным, поскольку на момент проведения исследования командный сервер был отключен.

Исследователи Seqrite Labs обнаружили аналогичную кампанию, нацеленную на российский военно-промышленный комплекс. В ней также применялся бэкдор EAGLET, а в качестве приманки в письме использовался архив «Договор_PH83_изменения.zip». Однако, в отличие от первой кампании, в этот раз имплант EAGLET не содержал файл-приманку.

Исследователи обратили внимание на ряд совпадений: обе кампании имели схожие цели, а код импланта оказался идентичен вредоносному ПО, которое использовала группа Head Mare. Эта группа, обнаруженная экспертами «Лаборатории Касперского», также атаковала русскоязычные организации. В частности, были выявлены функциональные сходства между EAGLET и PhantomDL – бэкдором, написанным на языке Go, с функцией shell и загрузки и скачивания файлов. Был также замечен схожий подход в названии файлов вложений фишинговых писем.

Атаки с использованием стилера Batavia

Ранее неизвестный актор

Целевой фишинг

Шпионское ПО

Эксперты «Лаборатории Касперского» сообщили об обнаружении ранее неизвестной программы-шпиона под названием Batavia. Этот вредонос активно используется в атаках на российские промышленные предприятия. Batavia состоит из VBS-скрипта и двух исполняемых файлов. Целенаправленная атака началась в июле 2024 года с рассылки электронных писем. Они содержали вредоносные ссылки, замаскированные под контракт, который просит скачать отправитель. После перехода по ссылке на компьютер жертвы загружался архив, внутри которого находился VBS-скрипт, зашифрованный проприетарным алгоритмом Microsoft. Скрипты назывались «договор-2025-5.vbe», «приложение.vbe», «договор.vbe». Скрипт запускал трехэтапное заражение компьютера с использованием двух исполняемых файлов. Первый, написанный на языке Delphi, собирает определенную информацию, включая различные системные журналы и офисные документы, найденные как на зараженном компьютере, так и на

съемных носителях. Более того, он периодически делает скриншоты, которые затем отправляет на командный сервер. Второй исполняемый файл, написанный на C++, обладает схожей шпионской функциональностью, но с расширенным списком собираемых типов файлов. Он также содержит две команды: одна предназначена для смены командного сервера, а другая – для загрузки и запуска дополнительных файлов.

Атаки Paper Werewolf/GOFFEE

APT

Целевой фишинг

Уязвимость нулевого дня

Исследователи BI.ZONE зафиксировали серию атак на российские и узбекские организации, проведенных группой Paper Werewolf/GOFFEE в июле и августе. Одной из мишеней стал российский производитель специализированного оборудования. Злоумышленники отправили электронное письмо от имени крупного научно-исследовательского института. При этом они использовали скомпрометированный электронный адрес, принадлежащий другой компании – поставщику мебели. Прикрепленный RAR-архив содержал документ-приманку якобы от одного из министерств и модифицированный исполняемый файл XPS Viewer, содержащий реверс-шелл.

В ходе этой атаки злоумышленники эксплуатировали уже известную уязвимость CVE-2025-6218 в WinRAR. Однако в последующих атаках, направленных против компаний в России и Узбекистане, они переключились на новую, на тот момент еще неописанную уязвимость нулевого дня CVE-2025-8088. Эта уязвимость, затрагивающая версии WinRAR вплоть до 7.12, также использована в операциях RomCom. Исследователи ESET, в свою очередь, отметили, что Paper Werewolf начала использовать CVE-2025-8088 на несколько дней позже RomCom.

Фишинговые письма, адресованные российским организациям, содержали архив, замаскированный под документ Министерства промышленности и торговли. А те, что рассылались узбекским организациям, – архив DON_AVIA_TRANS_RU.rar, который выдавался за документ от туристического агентства. Во всех этих вложениях скрывался вредоносный файл, эксплуатирующий уязвимость обхода каталога для записи фалов вне целевой папки. Загруженные таким образом вредоносные файлы представляли собой .NET-приложения, написанные на языке C#. Они скачивали вредоносную нагрузку в виде .NET-сборки с сервера и запускали ее в памяти. Стоит отметить, что незадолго до этих атак на одном из даркнет-форумов появился эксплойт для этой уязвимости, заявленный как рабочий.

Атаки PhantomCore

APT и киберкриминал

Целевой фишинг

Скомпрометированная легитимная электронная почта

Фишинговые сайты

ClickFix

Polyglot-файлы

Бэкдор

Исследователи Positive Technologies опубликовали отчет об APT-группе PhantomCore (известной также как Head Mare). В нем они обратили внимание на значительное расширение атакующего арсенала группы за последние полтора года, использованного в кибератаках на значимые российские организации.

В начале мая 2025 года исследователи обнаружили новую масштабную кампанию кибершпионажа против России. По их данным, к моменту публикации отчета PhantomCore уже получила доступ к 181 зараженному хосту. Первое заражение датируется 12 мая 2025 года, а пик кибератак пришелся на июнь, причем 56% всех заражений были зафиксированы 30 июня. В среднем группа оставалась в скомпрометированной сети 24 дня, а максимально – 78 дней. На момент публикации отчета 49 хостов все еще находились под контролем злоумышленников.

Первичный доступ к сетям жертв осуществляется посредством фишинговых писем, доставляющих бэкдоры. Эти письма содержат вредоносные файлы на различных языках, при этом злоумышленники используют скомпрометированные электронные адреса легитимных российских компаний. Арсенал группы весьма обширен и включает в себя бэкдор PhantomRAT, написанный на C++ бэкдор PhantomRShell, PowerShell-бэкдор PhantomTaskShell, написанный на Go стилер PhantomStealer, прокси-сервер для организации SSH-туннеля PhantomProxyLite, утилиту для восстановления паролей XenArmor All-In-One Password Recovery Pro, утилиты с открытым исходным кодом RClone и RSocx, а также средство удаленного администрирования MeshAgent.

Исследователи нашли фишинговый сайт группы, который был зарегистрирован на реальные данные гражданина России незадолго до раскрытия кампании кибершпионажа – в апреле. Этот сайт имитирует оригинальную HTML-верстку официального сайта Московского городского фонда обязательного медицинского страхования и предлагает посетителям, под предлогом прохождения поддельной капчи, вставить и выполнить содержимое буфера обмена в командной строке Windows – классический пример использования метода ClickFix.

Помимо этого, исследователи обнаружили обособленное подразделение группы, состоящее из менее квалифицированных специалистов. Это подразделение использует новый бэкдор PhantomGoShell, названный так, потому что он написан на языке Go и имеет сходства с PhatomRAT и PhantomRShell. Предполагается, что это подразделение было организовано одним из основных участников PhantomCore как своего рода

киберпреступный стартап. Вероятно, имея доступ к исходному коду инструментов группы, он привлек несколько хакеров-любителей из игровых и Discord-сообществ.

Атаки Cavalry Werewolf

APT

Целевой фишинг

Скомпрометированная легитимная электронная почта

Telegram как C2

RAT

Исследователи BI.ZONE с мая по август 2025 года отслеживали активность группы Cavalry Werewolf (известной также под именами YoroTrooper, SturgeonPhisher, Silent Lynx, Comrade Saiga, Tomiris и ShadowSilk). Эта группа целенаправленно рассылала фишинговые письма российским государственным учреждениям, а также энергетическим, горнодобывающим и производственным предприятиям. Отправителями писем якобы были госслужащие Кыргызстана. Примечательно, что в одном из таких писем использовался реальный электронный адрес, указанный на сайте регулятора Кыргызской Республики. По всей видимости, этот адрес был ранее скомпрометирован для использования в атаках.

В качестве вложения в фишинговых письмах находился RAR-архив с вредоносными программами FoalShell или StallionRAT, управление которыми осуществляется через Telegram. FoalShell представляет собой простые реверс-шеллы, написанные на языках Go, C++ и C#. Cavalry Werewolf использует их для выполнения произвольных команд в интерпретаторе командной строки cmd.exe на скомпрометированных хостах. StallionRAT – это трояны удаленного доступа, написанные на языках Go, PowerShell и Python. Они позволяют злоумышленникам выполнять произвольные команды, загружать дополнительные файлы и извлекать собранные данные.

География атак Cavalry Werewolf не ограничивается Россией и странами СНГ: обнаруженные файлы с названиями на арабском языке свидетельствуют о том, что группа также нацелена на ближневосточные государства. Кроме того, расследование выявило дополнительную информацию, указывающую на подготовку группой атак на Таджикистан и активное тестирование вредоносных программ, в частности AsyncRAT.

Атаки Hive0117

Киберкриминал

Целевой фишинг

Бэкдор

Исследователи F6 зафиксировали волну вредоносных рассылок от финансово-мотивированной группы Hive0117, которая активно использует DarkWatchman RAT с февраля 2022 года. В ходе этой масштабной кампании злоумышленники маскировались под реальные организации. Для своих фишинговых рассылок и инфраструктуры управления они зарегистрировали домены, имитирующие легитимные организации, причем нередко использовали эти домены повторно. Так, после нескольких месяцев затишья,

24 сентября 2025 года, исследователи F6 зафиксировали новую активность троянца DarkWatchman RAT. Напомним, в 2023 году он распространялся под видом архива с итогами фейкового тендера, якобы от Министерства обороны, и поддельными мобилизационными предписаниями. В этот раз злоумышленники атаковали компании, маскируясь под почтовую рассылку Федеральной службы судебных приставов.

Аналогичные рассылки были замечены в июне и июле. Однако для этих рассылок использовались домены 4ad74aab[.]cfd и 4ad74aab[.]xyz. Изучение списка получателей выявило, что целью группы Hive0117 являлись компании в России и Казахстане. Внушительный список из 51 потенциальной жертвы охватывал широкий спектр организаций: банки, торговые площадки, операторы связи, автосалоны, производственные, строительные и логистические компании, продуктовые ретейлеры, операторы лотерей, страховые и инвестиционные компании, топливно-энергетические компании, фармацевтические компании, научно-исследовательские институты, технопарки, операторы по обращению с отходами, туристические сервисы, фитнес-центры и ИТ-компании.

Атаки ComicForm

Целевой фишинг

Шпионское ПО

Исследователи F6 представили отчет о фишинговых атаках новой группы ComicForm. Этот актор, действующий минимум с апреля 2025 года, целенаправленно атакует российские компании в промышленном, финансовом, туристическом, биотехнологическом, исследовательском и торговом секторах, а также организации в Беларуси и Казахстане. Злоумышленники распространяют вредоносное ПО FormBook, предназначенное для кражи данных.

В частности, была выявлена фишинговая кампания, которая проводилась с мая по июнь 2025 года и была направлена против российских организаций. В ходе атаки злоумышленники рассылали письма с темами: Re: proforma invoice, Re: Bank Reconciliation report, Re: invoice and shipping documents, INvoice for Payment. Во вложении содержался скрытый загрузчик, который доставлял на компьютер жертвы стилер. Интересно, что в фишинговых письмах также была скрыта ссылка на анимированные GIF-изображения с супергероями. Эти картинки не выполняли никакой функциональной роли в атаке, а просто были частью кода. Именно эта любопытная деталь и дала актору название – ComicForm.

Группа рассылала фишинговые письма с электронных адресов, зарегистрированных в доменах верхнего уровня .ru, .by и .kz; некоторые адреса, предположительно, были скомпрометированы. Еще одной

отличительной чертой стало использование в качестве обратного адреса rivet_kz@, зарегистрированного в бесплатном российском почтовом сервисе.

Помимо вредоносных вложений, злоумышленники задействовали фишинговые страницы, имитирующие страницы авторизации в системе для работы с документами. После перехода по ссылке из электронного письма жертвы попадали на поддельные формы входа, откуда вводимые данные передавались на серверы атакующих.

Кластеры киберугроз, нацеленных на Россию и Беларусь

Киберкриминал

Хактивизм

APT

Эксперты «Лаборатории Касперского» проанализировали кампании с целями хактивизма, кибершпионажа и финансово-мотивированные атаки, рост активности которых с 2022 года был спровоцирован геополитической напряженностью. Отчет посвящен киберугрозам, исходящим от проукраинских группировок, с акцентом на их деятельность против России и Беларуси.

Исследование дает всестороннее понимание этих угроз, в нем описываются TTP (тактики, техники и процедуры), мотивы злоумышленников и их связь друг с другом. Все группы разделены на три кластера. Первый объединяет хактивистов и финансово-мотивированные группы, применяющие схожие TTP. Это Twelve, BlackJack, Crypt Ghouls, Head Mare и C.A.S. Во второй входят APT-группы, чьи TTP отличаются от хактивистских: Awaken Likho, Angry Likho, Mythic Likho, Librarian Likho, Cloud Atlas, GOFFEE и XDSpy. Третий включает группы хактивистов с уникальным почерком, для которых не было выявлено признаков активного взаимодействия с другими из описанных выше. Это Bo Team и «Киберпартизаны».

Южная Азия

Атаки APT36/Transparent Tribe

APT

Вредоносное ПО для Linux

Фишинговые сайты

Бэкдор

Исследователи Hunt.io проанализировали недавние кампании группы APT36 (она же Transparent Tribe). Изначально кампания была нацелена на объекты военно-промышленного комплекса Индии, но вскоре охватила среди прочего национальные железные дороги, инфраструктуру нефтегазовой отрасли, а также Министерство иностранных дел.

Злоумышленники использовали продвинутый фишинг, новые стратегии доставки вредоносного ПО и бэкдоры с механизмами закрепления в

системе. При атаках на системы на базе Linux злоумышленники использовали .desktop-файлы, которые маскировались под PDF-документы. Эти файлы запускали скрипты для скачивания вредоносного ПО и закрепления в системе с помощью cron. Было выявлено два сценария атаки: в первом случае использовался лишь один командный сервер, второй включает резервные серверы для отказоустойчивости. Бэкдор Poseidon, разработанный на платформе Mythic и написанный на Go, использовался для получения доступа и дальнейшего бокового перемещения.

Исследователи обнаружили более 100 фишинговых доменов. Многие из них имитировали сайты индийских правительственных организаций и хостились на AlexHost. Первые фишинговые домены для этой кампании были зарегистрированы в начале июля 2025 года, а к середине того же месяца инфраструктура уже активно развивалась. Такая динамика свидетельствует о непрерывном и активном ходе кампании.

Активность, связанная с Ближним Востоком

Атаки UNC1549

APT

Целевой фишинг

Бэкдор

C2, проксируемый через Azure

DLL sideloading

Сертификаты разработчика

Исследователи Prodaft отследили кибератаки группы Subtle Snail (также известной как UNC1549, Smoke Sandstorm, TA455 и Imperial Kitten), которая входит в состав сети Eclipsed Wasp (Charming Kitten). Группа активна по меньшей мере с июня 2022 года и в последнее время сфокусировалась на европейских телекоммуникационных, аэрокосмических и оборонных организациях. В ходе своей последней кампании Subtle Snail целенаправленно заразила 34 устройства в 11 организациях, используя социальную сеть LinkedIn. Злоумышленники выдавали себя за рекрутеров реальных компаний, чтобы установить контакт с конкретными специалистами, а затем скомпрометировать их компьютеры. На системы внедрялся бэкдор Minibike, который использует сервисы Azure в качестве прокси командного сервера, что позволяет ему избегать обнаружения.

Основная задача MiniBike – загрузка дополнительных компонентов в виде библиотек DLL. Злоумышленники развертывали различные модули DLL: кейлоггер, стилер для кражи данных из браузеров, стилер для кражи учетных данных Outlook/Winlogon.

Subtle Snail использует цифровую подпись для своих вредоносных программ как минимум с мая 2025 года. Согласно отчету Prodaft, все вредоносные бинарные файлы, задействованные в атаках группы, подписаны действительным цифровым сертификатом, выданным SSL.com голландской

компании Insight Digital B.V. Вредоносные DLL-файлы, разработанные злоумышленниками, каждый из которых реализует специализированную функцию и предназначается для конкретной жертвы, запускаются посредством сторонней загрузки DLL (DLL sideloading). Для бесшовного выполнения злоумышленники модифицируют легитимные DLL-файлы, редактируя их таблицы экспорта, в результате чего полученные файлы выглядят как легитимные, хотя и несут вредоносную функциональность.

Группа создает учетные записи электронной почты для поддержки своих фишинговых кампаний. Эти же аккаунты используются для создания облачных учетных записей, необходимых для управления прокси-серверами Azure и обеспечения фишинговой инфраструктуры. Злоумышленники покупают эти аккаунты под конкретные домены, которые будут использоваться для атак. В зависимости от цели, они создают, например, фейковое объявление о приеме на работу в формате PDF, которое выглядит так, будто отправлено, скажем, Telespazio. А для повышения шансов на успех покупают поддельный домен вроде telespazio-careers.com. Так, злоумышленники купили домен safrangroup-careers.com и выдавали себя за представителей Safran Group – французского конгломерата в сферах аэрокосмической промышленности, обороны и безопасности. Злоумышленники выбирают домены по одному и тому же принципу: они всегда содержат *-careers.com или *careers.com.

В то же время исследователи Check Point отследили продолжительную кампанию группы Nimbus Manticore, имеющую пересечения с операциями UNC1549, Smoke Sandstorm и Iranian Dream Job. Они отметили, что текущая кампания нацелена на оборонные, телекоммуникационные и авиационные предприятия. Недавняя активность Nimbus Manticore свидетельствует о повышенном внимании к Западной Европе, в частности к Дании, Швеции и Португалии. Злоумышленники маскируются под национальные и международные организации из указанных отраслей, применяя нетривиальные методы целевого фишинга. Они выдают себя за рекрутеров, а затем направляют жертв на фейковые карьерные порталы.

В центре этой кампании – сложно обфусцированный бэкдор MiniJunk и упрощенный стилер MiniBrowse в двух версиях: одна – для кражи учетных данных из браузеров Chrome, другая – для Edge. Анализ MiniJunk, проведенный исследователями Check Point, показал, что это значительно усовершенствованная версия Minibike. Новые возможности вредоносной программы включают загрузку вредоносных DLL-библиотек в WindowsDefender и другие уязвимые исполняемые файлы Microsoft посредством манипуляции параметром DllPath структуры RTL_USER_PROCESS_PARAMETERS, используемой в

недокументированном низкоуровневом NT API. Этот параметр определяет путь поиска DLL-библиотеки, если она не найдена в директории приложения. Злоумышленники Nimbus Manticore также подписывают свои вредоносные программы цифровой подписью, используя сертификаты от сервиса SSL.com, по крайней мере, с мая 2025 года. Основываясь на датах подписания и анализе образцов, подписанных этим сертификатом, исследователи определили, что они были сгенерированы злоумышленниками, выдающими себя за легитимные ИТ-организации в Европе.

Активность китайскоязычных групп

Атаки на полупроводниковую промышленность Тайваня

APT

Целевой фишинг

Скомпрометированная легитимная электронная почта

AitM

Бэкдор

С марта по июнь 2025 года исследователи Proofpoint отслеживали активность трех китайскоязычных акторов, которые проводили целенаправленные фишинговые кампании против полупроводниковой промышленности Тайваня. Вероятным мотивом во всех случаях был кибершпионаж. Цели этих атак варьировались в зависимости от специализации организаций, от производства, проектирования или тестирования полупроводников и интегральных схем, до более широкого списка организаций из числа поставщиков оборудования и услуг в этом секторе, а также финансовых и инвестиционных аналитиков, специализирующихся на тайваньском рынке полупроводников.

Группа UNK_FistBump атаковала организации, занимающиеся проектированием, производством и поставками изделий из полупроводников фишинговыми письмами, замаскированными под предложения о трудоустройстве. В результате на компьютеры жертв доставлялись Cobalt Strike или специальный бэкдор Voldemort. Злоумышленники представлялись выпускниками вуза, ищущими работу, при этом использовали скомпрометированные адреса электронной почты Национального университета Тайваня для рассылки фишинговых писем рекрутерам и сотрудникам HR-отделов.

Группа UNK_DropPitch, в свою очередь, проводила целевые фишинговые кампании против нескольких крупных инвестиционных банков. Злоумышленников интересовали конкретные финансовые аналитики, специализирующиеся на инвестициях в полупроводниковую и технологическую индустрии Тайваня. Фишинговые письма отправлялись с адреса злоумышленника, выдававшего себя за представителя финансово-инвестиционной компании, предлагающего сотрудничество конкретному

специалисту. В ходе операции также использовался специализированный бэкдор.

UNK_SparkyCarp использовала кастомный Adversary-in-the-Middle (AitM) фишинг-кит. Целью стала организация, которая уже пострадала от этого актора в ноябре 2024 года. Фишинговые письма маскировались под предупреждения о подозрительном входе в аккаунт и содержали ссылку на контролируемый злоумышленниками фишинговый сайт, предназначенный для кражи учетных данных.

Атаки UNC3886

APT

Уязвимость нулевого дня

Вредоносное ПО для Linux

LOTL

Бэкдор

Министр-координатор по вопросам национальной безопасности Сингапура 18 июля сделал заявление о «чрезвычайно изощренной угрозе», с которой столкнулась страна. Речь о группе UNC3886, нацеленной на критически важную инфраструктуру.

Впервые об активности этой группы сообщили в 2022 году, когда она атаковала ключевые службы Сингапура, создав серьезную угрозу для национальной безопасности страны. Исследователи Trend Micro проанализировали предыдущие атаки UNC3886. Тогда группа нацеливалась на критически важную инфраструктуру в США и Европе: правительственные организации, предприятия телекоммуникационной, технологической и оборонной отраслей.

Группа UNC3886 известна тем, что оперативно использует уязвимости нулевого дня в сетевом и виртуальном оборудовании, таком как VMware vCenter/ESXi, Fortinet FortiOS и Juniper Junos OS. В ее арсенале значатся кастомизированное ПО, включая TinyShell (инструмент удаленного доступа для скрытных операций), Reptile (руткит для Linux, используемый для сокрытия файлов, процессов и сетевой активности) и Medusa (еще один руткит для сокрытия вредоносных действий, специально разработанный под Linux). Это свидетельствует о способности группы разрабатывать и внедрять сложные инструменты, осуществлять многоуровневое закрепление в системе, использовать продвинутые методы уклонения от защиты. Группа также использует легитимные программы и функции, применяя тактику Living-off-the-Land (LOTL).

Коллективное руководство по безопасности в отношении Salt Typhoon

APT

Эксплуатация сетевых устройств и общедоступных приложений

Trusted relationship

Ведомства из разных стран, включая Агентство национальной безопасности США и Агентство по кибербезопасности и защите инфраструктуры (CISA), совместно выпустили руководство по кибербезопасности с техническими подробностями о китайскоязычных APT-группах. Рекомендации опубликовали агентства США, Австралии, Канады, Новой Зеландии, Великобритании, Чехии, Финляндии, Германии, Италии, Японии, Нидерландов, Польши и Испании.

Описание вредоносной активности в документе частично пересекается с данными из отчетов других исследователей кибербезопасности, касающихся таких групп, как Salt Typhoon, OPERATOR PANDA, RedMike, UNC5807, GhostEmperor. Этот кластер был активен в США, Австралии, Канаде, Новой Зеландии, Великобритании и ряде других государств. Его активность авторы руководства связывают с несколькими китайскими компаниями, которые, как предполагается, предоставляют киберпродукты и услуги государственным организациям КНР.

Согласно документу, эти группы нацеливаются на информационные сети организаций из телекоммуникационного, правительственного, транспортного, военного и жилищного секторов разных стран. Основное внимание злоумышленников сосредоточено на ядрах сети крупных телекоммуникационных провайдеров, а также на пограничных маршрутизаторах провайдеров и клиентских организаций. Однако они также используют скомпрометированные устройства и доверенные отношения для компрометации сетей новых жертв. Группы часто конфигурируют маршрутизаторы для получения постоянного доступа к скомпрометированным сетям. Документ содержит подробную техническую информацию о первичном доступе, закреплении и горизонтальном перемещении в сети, сборе и извлечении данных. В нем также представлены разбор кейсов, руководство по обнаружению описанных угроз, индикаторы компрометации и рекомендуемые меры по смягчению последствий атак.

Атаки GhostRedirector

Ранее неизвестный актор

Эксплуатация общедоступных приложений

Бэкдор

Сертификат разработчика

Исследователи ESET обнаружили ранее неизвестного китайскоязычного актора GhostRedirector, который скомпрометировал как минимум 65 серверов Windows в нескольких странах, включая Бразилию, Таиланд и Вьетнам. Среди пострадавших оказались образовательные, медицинские, страховые, транспортные, торговые и ИТ-организации. Это позволило исследователям сделать вывод, что GhostRedirector не имеет конкретного регионального или отраслевого фокуса.

Злоумышленники, предположительно, выполняли SQL-инъекции в общедоступных приложениях для получения первичного доступа. Затем они внедряли вредоносные инструменты, в том числе написанные на языке C++ пассивный бэкдор Rungan, предназначенный для удаленного выполнения команд, и вредоносный модуль Internet Information Services под названием Gamshen, способный манипулировать поисковой выдачей Google в целях SEO-мошенничества в пользу онлайн-казино. Кроме того, в арсенале злоумышленников обнаружены кастомизированные утилиты для повышения привилегий на базе BadPotato и EfsPotato, многоцелевая DLL-библиотека Comdai и инструмент под названием Zunput для установки веб-шеллов. Злоумышленники задействовали сертификаты разработчика, создавали поддельные учетные записи администраторов и использовали такие инструменты, как GoToHTTP, для поддержания постоянного доступа к скомпрометированным системам.

Атаки RedNovember/TAG-100

APT

Эксплуатация сетевых устройств и общедоступных приложений

Бэкдор

Издание The Hacker News сообщило об активности группы TAG-100, которая теперь отслеживается как RedNovember. В период с июня 2024 года по июль 2025 года она атаковала периферийные устройства крупных организаций по всему миру, используя написанный на языке Go бэкдор Pantegana и популярный фреймворк Cobalt Strike.

Группа значительно расширила свою деятельность, атакуя как государственные, так и частные организации – космические и аэрокосмические предприятия, а также юридические фирмы. Было замечено, что RedNovember проводит разведку и компрометирует периферийные устройства. В их числе: SonicWall, Cisco ASA, F5 BIG-IP и Fortinet FortiGate, а также устройства, на которых установлены Outlook Web Access и Ivanti Connect Secure VPN. Активность группы демонстрирует ее способность комбинировать эксплойты и опенсорсные фреймворки для постэксплуатации. Это значительно упрощает задачу для не самых квалифицированных злоумышленников.

Исследователи выявили новых вероятных жертв RedNovember, среди которых Министерство иностранных дел одной из стран Центральной Азии, структура госбезопасности одной из стран Африки, правительственная организация в Европе и правительство одной из стран Юго-Восточной Азии. Кроме того, злоумышленники атаковали как минимум две компании, которые сотрудничают с Министерством обороны США, две американские нефтегазовые компании, европейского производителя двигателей и межправительственный орган по торговым отношениям в Юго-Восточной Азии. RedNovember фокусирует свою активность на странах с высокой геополитической напряженностью или же участвующих в военных конфликтах, представляющих стратегический интерес для Китая.

Атаки Naikon

APT

Бэкдор

DLL sideloading

Исследователи Cisco Talos обнаружили кампанию, начавшуюся в 2022 году и нацеленную на телекоммуникационный и производственный секторы в странах Центральной и Южной Азии и использующую новую версию вредоносной программы PlugX. По своей функциональности она похожа на бэкдоры RainyDay и Turian – использует те же легитимные приложения для DLL-sideloading и алгоритм XOR-RC4-RtlDecompressBuffer для шифрования и дешифрования вредоносной нагрузки. Конфигурация этой версии PlugX отличается от стандартной и напоминает структуру RainyDay. Это позволило исследователям с некоторой уверенностью отнести кампанию к китайскоязычной группе Naikon. Список жертв и технические характеристики атаки указывают на потенциальную связь Naikon с группой BackdoorDiplomacy. Вполне вероятно, что это одна и та же группа, либо обе используют инструментарий одного и того же поставщика.

Киберкриминал и прочее

Атаки Scattered Spider/UNC3944

Киберкриминал

Телефонные звонки

Шифровальщик

Исследователи Google Threat Intelligence Group сообщили об изощренной кампании финансово-мотивированной группы UNC3944 (известной также как 0ktapus, Octo Tempest и Scattered Spider). Атаки были нацелены на несколько отраслей, в том числе розничной торговли, авиационной и страхования. По данным исследователей, злоумышленники распространяли программы-вымогатели, а после требовали выкуп у ретейлеров из США. Довольно быстро кампания масштабировалась, и мишенями стали еще и транспортные и авиакомпании в Северной Америке.

Тактика группы остается неизменной: они используют не уязвимости программного обеспечения, а социальную инженерию – звонят по телефону в ИТ-поддержку компаний, представляясь штатными сотрудниками. После компрометации одной или нескольких учетных записей пользователей они получают контроль над доверенными административными системами и, получив доступ в Active Directory, компрометируют VMware vSphere. Это открывает злоумышленникам возможность для кражи данных виртуальных машин и развертывания на них программ-вымогателей непосредственно из гипервизора.

Вслед за публикацией Google Threat Intelligence Group последовали отчет Palo Alto Networks и рекомендации Агентства по кибербезопасности и защите инфраструктуры США (CISA) касательно Scattered Spider. В этих документах описаны TTP группы и предложены меры по усилению защиты. Также там указано, что в ходе недавних кампаний Scattered Spider применяла шифровальщик DragonForce.

Атаки с использованием Gunra

Киберкриминал

Вредоносное ПО для Linux

Шифровальщик

Исследователи Trend Micro проанализировали Linux-версию программы-вымогателя Gunra, которая обладает рядом любопытных особенностей. Среди них – возможность одновременного запуска до 100 потоков шифрования и поддержка частичного шифрования. Инструмент дает возможность злоумышленникам контролировать, какая часть каждого файла шифруется, и хранить ключи, зашифрованные с помощью криптографического алгоритма RSA, в отдельных файлах хранилища ключей.

Группа вымогателей Gunra впервые была обнаружена в апреле 2025 года в ходе кампании, нацеленной на системы на базе Windows. В ходе своих атак она использовала методы, отсылающие к известной группе Conti. На сайте утечек утверждается, что Gunra успешно атаковала предприятия в Бразилии, Японии, Канаде, Турции и США. Среди пострадавших отраслей называются производство, юриспруденция и консалтинг, здравоохранение, ИТ и сельское хозяйство. Исследователи Trend Micro, в свою очередь, зафиксировали активность Gunra на предприятиях в Турции, США, Южной Корее и на Тайване. Данные Trend Micro указывают на то, что вымогатели пытались атаковать правительственные организации, а также медицинские, производственные и транспортные компании.

Атаки TGR-CRI-0045/Gold Melody

Киберкриминал

Брокеры начального доступа

Эксплуатация Machine Keys

Десериализация ASP.NET View State

Исследователи Unit 42 раскрыли кампанию брокера начального доступа, в ходе которой злоумышленники использовали похищенные криптографические ключи с сайтов на базе ASP.NET для получения доступа к целевым организациям. Эта техника известна с 2014 года как «Десериализация Viewstate» и эксплуатировалась в атаках на различные ASP.NET-сервисы, использующие технологию сериализации, проблему безопасности которой Microsoft пометили как «Won't Fix». Вредоносное ПО запускалось непосредственно в памяти сервера, что сводило к минимуму их присутствие на диске и практически не оставляло криминалистических артефактов, значительно усложняя обнаружение. Инструментарий группы, по-видимому, находится на стадии разработки. Первые признаки эксплуатации и внедрения этих инструментов были замечены в октябре 2024 года, а в период с конца января по март 2025 года активность значительно увеличилась. В это же время развертывались инструменты для постэксплуатации: сканеры портов с открытым исходным кодом и кастомизированные утилиты для закрепления и повышения привилегий.

Исследователи отслеживают этого актора как временную группу TGR-CRI-0045 и с некоторой степенью уверенности связывают его с Gold Melody (она же UNC961, Prophet Spider). Группа, как отмечается, придерживается авантюрного подхода и атакует организации в Европе и США в следующих отраслях: финансовые услуги, производство, оптовая и розничная торговля, высокие технологии, транспорт и логистика.

Атаки GLOBAL GROUP

Киберкриминал

RaaS

ИИ-чат-боты

Эксплуатация общедоступных приложений

Шифровальщик

Исследователи EclecticIQ сообщают о появлении новой программы-вымогателя как услуге (Ransomware as a Service, RaaS). За ней стоит GLOBAL GROUP, применяющая продвинутые ИИ-технологии для проведения атак против широкого круга компаний. По состоянию на 14 июля 2025 года жертвами группы стали 17 организаций в США, Великобритании, Австралии и Бразилии. Атаки затронули различные секторы, включая здравоохранение, производство нефтегазового оборудования, промышленной техники и высокоточных деталей, механизмов и систем, ремонт автомобилей и аутсорсинг бизнес-процессов.

Группа прибегает к услугам брокеров начального доступа для распространения программ-вымогателей. Она получает доступ к уязвимым периферийным VPN-устройствам, например Cisco, Fortinet и Palo Alto Networks, а также использует брутфорс-инструменты для взлома аккаунтов к порталам Microsoft Outlook и RDWeb. Платформа RaaS включает портал

для переговоров и партнерскую панель, которые позволяют злоумышленникам выбирать жертв, создавать вредоносные программы-вымогатели для VMware ESXi, NAS, BSD и Windows, а также удаленно отслеживать ход операций. Особого внимания заслуживает использование GLOBAL GROUP автоматизированной системы, основанной на чат-ботах с искусственным интеллектом, для ведения переговоров о выкупе. Эта функция позволяет операторам, не владеющим английским языком, более эффективно взаимодействовать с жертвами.

Исследователи EclecticIQ с некоторой уверенностью считают, что GLOBAL GROUP была создана в рамках ребрендинга операции BlackLock RaaS. Анализ образцов программы-вымогателя GLOBAL показывает, что это кастомизированный вариант шифровальщика Mamona. В отличие от базовой версии Mamona, GLOBAL имеет дополнительный функционал для автоматической установки в рамках домена. Он использует SMB-соединения и вредоносный Windows Service для более масштабного развертывания. Аналитики EclecticIQ также обнаружили, что в операциях ныне несуществующей группы вымогателей Mamona RIP, а также GLOBAL GROUP использовался один и тот же российский VPS-провайдер IpServer, что указывает на возможную связь между ними.

Атаки с использованием Charon

Киберкриминал

DLL sideloading

Шифровальщик

Исследователи Trend Micro выявили новое семейство программ-вымогателей Charon, которые были задействованы в ходе целенаправленной атаки на государственный сектор и авиационную промышленность на Ближнем Востоке. Злоумышленники применили метод DLL sideloading, который оказался поразительно схожим с тактикой, ранее описанной в кампаниях Earth Baxia. Эти кампании, как известно, исторически были нацелены на правительственные организации.

В цепочке атак использовался легитимный файл браузера Edge.exe (изначально именовавшийся cookie_exporter.exe). Уязвимость в нем использовалась для загрузки вредоносной библиотеки msedge.dll (названной SWORDLDR), которая затем активизировала полезную нагрузку программы-вымогателя Charon.

Несмотря на то, что исследователи выявили технические сходства – в частности, в качестве инструмента для развертывания зашифрованного шелл-кода используется тот же уязвимый исполняемый файл, в который загружается вредоносная DLL-библиотека, – они не могут однозначно приписать эту атаку группе Earth Baxia. Подобные методы могут указывать как на прямое участие Earth Baxia, так и на попытку маскировки или же на разработку схожей тактики другой группой.

Важно отметить, что в требовании о выкупе вымогатели конкретно упомянули название организации-жертвы. Это подтверждает, что атака носила целенаправленный, а не случайный характер. Этот инцидент наглядно демонстрирует тревожную тенденцию: вымогатели все чаще применяют сложные методы, присущие APT-группам. Сюда входят DLL sideloading, внедрение процессов и использование техник обхода EDR-решений.

Предупреждение CISA о группе вымогателей Interlock

Киберкриминал

Скомпрометированные сайты

Drive-by атака

ClickFix

Вредоносное ПО для Linux

RAT

Агентство по кибербезопасности и защите инфраструктуры США (CISA), Федеральное бюро расследований, Министерство здравоохранения и социальных служб США и Международный центр обмена информацией и анализа (MS-ISAC) 22 июля опубликовали рекомендации по кибербезопасности, в которых приводятся индикаторы компрометации и TTP группы вымогателей Interlock, выявленные в ходе недавних расследований ФБР.

Группа Interlock получила известность в конце сентября 2024 года, когда атаковала различные коммерческие предприятия и критически важные объекты инфраструктуры в Северной Америке и Европе. ФБР заявило, что

эти злоумышленники исповедуют оппортунистический подход при выборе своих жертв, исходя из своих возможностей, и действуют исключительно с целью вымогательства.

Interlock создала программы-вымогатели для операционных систем Windows и Linux. Эти вредоносы шифровали виртуальные машины на базе обеих операционных систем. ФБР зафиксировало, как злоумышленники получали первичный доступ посредством атак Drive-by Download, используя скомпрометированные легитимных сайты. Это довольно нетипичный подход для вымогателей. Interlock маскировала вредоносное ПО под популярные защитные программы или обновления для Google Chrome или Microsoft Edge, чтобы заставить пользователей запустить RAT на своих системах. Другим способом получения первичного доступа являлся метод социальной инженерии ClickFix. После они задействовали различные методы разведки, получения учетных данных и горизонтального перемещения на другие системы в сети жертвы.

Атаки с использованием Warlock

Киберкриминал

Эксплуатация общедоступных приложений

LOTL

Шифровальщик

Исследователи Trend Micro обнаружили волну атак группы вымогателей Warlock. В качестве средства первичного доступа злоумышленники использовали свежие уязвимости серверов Microsoft SharePoint, загружая на них веб-шеллы для разведки и кражи учетных данных. Согласно более ранним отчетам, география жертв Warlock охватывает Северную Америку, Европу, Азию и Африку. Группа атаковала организации в различных отраслях, включая критическую инфраструктуру. Всего через несколько дней после своего первого публичного заявления Warlock объявила о как минимум 16 успешных атаках, примерно половина из которых была направлена против правительственных учреждений в Португалии, Хорватии и Турции. В числе других пострадавших оказались организации из финансового и производственного секторов. Внутри скомпрометированной инфраструктуры злоумышленники крадут учетные данные, продвигаются по сети и разворачивают шифровальщики, используя групповые политики, встроенные средства Windows и кастомизированное вредоносное ПО. Зашифрованные файлы получают расширение .x2anylock, а похищенные данные извлекаются с помощью утилиты RClone.

Атаки Crypto24

Киберкриминал

Google Drive

LOTL

BYOVD

Шифровальщик

Исследователи Trend Micro обнаружили группу вымогателей Crypto24. Она атакует организации в Азии, Европе и США преимущественно из сфер финансовых услуг, индустрии развлечений, производственно-технологического сектора. Группа использует легитимные инструменты, такие как PsExec и AnyDesk, наряду со специально разработанными вредоносными программами. В ее арсенал входят кейлоггер, который осуществляет вывод данных через Google Диск, и кастомизированная версия инструмента RealBlindingEDR, предназначенного для отключения защитных решений, по всей видимости, использующего для этого новые или неизвестные уязвимые драйверы.

Для закрепления в системе злоумышленники создавали привилегированную учетную запись и задачи планировщика, которые интегрировали вредоносные действия в обычные операции системы. Для обхода ограничений контроля учетных записей пользователей (User Account Control) Crypto24 эксплуатирует COM-интерфейс CMSTPLUA. Анализ показал, что злоумышленники действуют очень скоординировано, часто начиная атаки в нерабочее время, чтобы избежать обнаружения и добиться максимального эффекта.

Атаки The Gentlemen

Ранее неизвестный актор

Двойное вымогательство

BYOVD

Шифровальщик

Исследователи Trend Micro проанализировали новую кампанию ранее неизвестной группы вымогателей The Gentlemen. Группа продемонстрировала расширенные возможности по взлому крупных организаций. Для обхода защитных решений The Gentlemen использует легитимный драйвер и специально разработанные противо-антивирусные утилиты, манипулируют групповыми политиками, компрометируют привилегированные учетные записи и эксфильтруют данные через зашифрованные каналы. Атаки группы затронули множество отраслей, включая производство, строительство, здравоохранение и страхование, как минимум в 17 странах. Кроме того, The Gentlemen разработала программу-вымогатель, которая использует привилегированные доменные учетные записи, и различные методы для обхода мер кибербезопасности.

Атаки DireWolf

Киберкриминал

Двойное вымогательство

Предотвращение возможности восстановления

Шифровальщик

Исследователи AhnLab описали деятельность группы вымогателей DireWolf. Эта группа появилась в мае 2025 года и с тех пор атакует компании по всему миру, преимущественно из производственной, ИТ, строительной и финансовой отраслей. Она применяет тактику двойного вымогательства: сначала шифрует данные, а затем угрожает опубликовать их. DireWolf уже скомпрометировала 16 организаций в 16 регионах.

Для шифрования данных злоумышленники используют стойкие криптографические алгоритмы – обмен ключей Диффи – Хеллмана на основе эллиптической кривой Curve25519 и потоковое шифрование ChaCha20. В процессе шифрования для каждого файла генерируется случайный сеансовый ключ, который затем используется для формирования ключа шифрования. Зашифрованные файлы получают расширение .direwolf, а используемая система шифрования устойчива к известным доступным методам дешифрования. DireWolf также применяет методы, затрудняющие восстановление данных и анализ, – они завершают процессы резервного копирования, удаляют журналы событий и отключают средства восстановления данных. После завершения процесса шифрования вредоносная программа удаляет свой исполняемый файл и пытается перезагрузить компьютер. Это значительно снижает шансы на успешное проведение криминалистического анализа и восстановление самого вредоносного ПО.

Атаки с использованием уязвимости ToolShell

Ранее неизвестный актор

Эксплуатация общедоступных приложений

Несколько компаний по обеспечению безопасности и национальных центров реагирования на инциденты опубликовали 19 и 20 июля 2025 года предупреждения об активной эксплуатации уязвимостей серверов SharePoint. Атака с использованием цепочки из двух уязвимостей – CVE-2025-49704 и CVE-2025-49706, получившей название ToolShell, не требует аутентификации и дает полный контроль над уязвимым сервером.

Параллельно, в те же даты Microsoft выпустила срочные внеочередные исправления для уязвимостей CVE-2025-53770 и CVE-2025-53771. Эти патчи предназначались для устранения недостатков в предыдущих исправлениях для CVE-2025-49704 и CVE-2025-49706. По утверждению исследователей, для обхода первоначально выпущенных Microsoft исправлений в коде эксплойта достаточно было поменять всего один байт. Выпуск этих новых, «правильных» обновлений привел к путанице по поводу того, какие именно уязвимости эксплуатируют атакующие и используют ли они эксплойты нулевого дня.

Продукты Kaspersky регулярно обнаруживали и блокировали вредоносную активность, связанную с этими атаками, что позволило собрать статистику о сроках и масштабах этой кампании. Так, в отчете «Лаборатории Касперского» подробно описывается механика эксплуатации ToolShell. Эксперты демонстрируют, как вредоносная нагрузка может быть внедрена без какой-либо аутентификации, акцентируя внимание на механизме обхода защитных решений. Согласно статистике «Лаборатории Касперского», широкомасштабная эксплуатация началась 18 июля 2025 года. Злоумышленники нацелились на серверы в Египте, Иордании, России, Вьетнаме и Замбии. Атаки затронули организации из правительственного, финансового и производственного секторов, а также лесного и сельского хозяйства.

Атаки с использованием уязвимости CVE-2025-32433

Ранее неизвестный актор

Эксплуатация общедоступных приложений

Исследователи Palo Alto Networks сообщили об атаках, в ходе которых эксплуатировалась критическая уязвимость, обнаруженная и исправленная в апреле 2025 года. Она затрагивает Open Telecom Platform – платформу с набором библиотек и шаблонов проектирования для построения приложений на языке программирования Erlang – до версий OTP-27.3.3, OTP-26.2.5.11 и OTP-25.3.2.20.

Уязвимость CVE-2025-32433 с рейтингом CVSS 10.0 позволяет злоумышленникам получить несанкционированный доступ к системе и выполнять произвольные команды без ввода действительных учетных данных, манипулируя данными при коммуникации со встроеннным SSH-сервером. Исследователи отметили, что в технологических средах и сетях 5G OTP используется из-за ее отказоустойчивости и масштабируемости, необходимых для систем высокой доступности с минимальным временем простоя, а удаленные команды часто выполняются с помощью встроенного SSH-сервера.

Исследователи предоставили анализ вредоносной нагрузки, распределение поверхности атаки (распространенности подключенных к интернету уязвимых устройств) и попыток их атак по географии, времени, отрасли, а также распределение атакованных устройств между ИТ- и ОТ-инфраструктурами. Примечательно, что значительное количество ОТ-сетевых экранов оказалось уязвимым и подключенным к интернету. В общей сложности около 70% всех попыток эксплуатации пришлось именно на доступные из интернета ОТ-файрволы.

Исследователи также обратили внимание, что сильнее всего пострадала образовательная отрасль, что ОТ-файрволы в здравоохранении, сельском

хозяйстве, СМИ и индустрии развлечений, а также в высокотехнологичных отраслях были атакованы диспропорционально часто – до 85% всех попыток эксплуатации в этих индустриях пришлось именно на пограничные устройства технологической сети.

В то же время системы OT- и ИТ-сетей в таких секторах, как производство, оптовая и розничная торговля, а также финансовые услуги, были атакованы со сравнимой частотой, что свидетельствует, по мнению исследователей, о необходимости комплексных мер защиты для организаций этих секторов.

Атак же на технологические сети коммунальных, энергетических, горнодобывающих, аэрокосмических и оборонных предприятий зафиксировано не было. Palo Alto Networks, однако, рассматривает это как потенциальное свидетельство слабости механизмов обнаружения атак на предприятиях данных секторов или задержки в выборе атакующими целей из их числа.

Исследователи настоятельно рекомендуют оперативно применять актуальные исправления безопасности, обновлять сигнатуры в системах предотвращения вторжений и всесторонне использовать средства мониторинга. Если немедленная установка исправлений невозможна, рекомендуется отключить SSH-сервер или ограничить доступ с помощью правил брандмауэра.

Атаки с использованием бэкдора PipeMagic

Шифровальщик

Уязвимость нулевого дня

DLL hijacking

Бэкдор

В апреле 2025 года Microsoft исправила в своих продуктах 121 уязвимость. По данным компании, на момент выпуска патчей только одна из них – CVE-2025-29824 – эксплуатировалась в реальных атаках. Эксплойт к этой уязвимости запускала вредоносная программа PipeMagic, которую исследователи «Лаборатории Касперского» впервые обнаружили в декабре 2022 года в ходе исследования вредоносной кампании с применением программы-вымогателя RansomExx. Тогда жертвами стали промышленные предприятия в Юго-Восточной Азии. Загрузчиком бэкдора служила троянизированная версия Rufus – утилиты для форматирования USB-накопителей.

В сентябре 2024 года исследователи «Лаборатории Касперского» вновь обнаружили PipeMagic в атаках на организации на Ближнем Востоке. На этот раз злоумышленники изменили тактику: вместо эксплуатации уязвимости для получения первичного доступа они использовали в качестве приманки поддельный клиент ChatGPT. Приложение было написано на языке Rust с использованием двух фреймворков: Tauri для рендеринга графических приложений и Tokio для асинхронной обработки событий. Примечательно,

что поддельное приложение не имело пользовательских функций и при запуске просто отображало пустой экран. Эксперты отметили, что это была та же версия PipeMagic, что и в 2022 году.

В 2025 году решения Kaspersky предотвратили заражение этим бэкдором организаций в Бразилии и Саудовской Аравии. В ходе совместного расследования с BI. ZONE исследователи «Лаборатории Касперского» проследили эволюцию PipeMagic с момента ее первого обнаружения в 2022 году до новых инцидентов в 2025 году. Они выявили ключевые изменения в тактике ее операторов и предоставили анализ модулей вредоноса, включая модуль асинхронной коммуникации, загрузчик и инжектор. Помимо загрузчика в виде поддельного клиента ChatGPT использовался загрузчик в виде файла формата Microsoft Help Index File, который вместо кода чтения данных контейнеров .mshi содержал код на C#, выполняющий расшифровку и шелл-код, который извлекает из себя и запускает на выполнение код конечного вредоноса. Третий вариант загрузчика использовал технику DLL hijacking, где в легитимный исполняемый файл обновления Google Chrome загружалась вредоносная библиотека. Вредоносный код содержался в функции DllMain. Злоумышленники использовали тот факт, что управление DllMain передается в любом случае – для инициализации внутренних структур данных библиотеки. Исследователи BI.ZONE, в свою очередь, провели технический анализ самой уязвимости CVE-2025-29824. В тот же день Microsoft Threat Intelligence опубликовала собственный анализ архитектуры PipeMagic и дополнительных функций этого ПО, включая выделенный сетевой модуль.

Атаки с использованием UpCrypter

Киберкриминал

Целевой фишинг

Бэкдор

RAT

Исследователи Fortinet Labs обнаружили крупномасштабную кампанию, нацеленную на организации из различных секторов. Основной удар пришелся на производство, ИТ, здравоохранение, строительство, розничную торговлю и индустрию гостеприимства.

Злоумышленники используют различные сценарии социальной инженерии, чтобы заманить пользователей на достоверно выглядящие фишинговые страницы. Для этого они рассылают электронные письма с темами, которые «требуют немедленного внимания», например, о якобы голосовых сообщениях о пропущенных телефонных звонках, заказах на покупку и т. д. Злоумышленники персонализируют эти страницы, используя электронный адрес и логотип организации-жертвы, чтобы они выглядели правдоподобно. Цепочка атаки начинается с небольшого обфусцированного скрипта, который перенаправляет жертв на поддельный сайт. Эти страницы призваны побудить получателей загрузить вредоносные JavaScript-файлы. В свою

очередь, эти файлы загружают UpCrypter – вредоносное ПО, которое в итоге внедряет различные средства удаленного доступа (RAT). Среди обнаруженных образцов вредоносной нагрузки были PureHVNC, DCRat и Babylon RAT.

Атаки EvilAI

Ранее неизвестный актор

Код, написанный ИИ

Маскировка под ИИ-инструментарий для повышения производительности

Бэкдор

Исследователи Trend Micro выявили новую вредоносную кампанию EvilAI. В данном случае вредоносное ПО маскируется под легитимные инструменты повышения производительности на основе технологии искусственного интеллекта, с профессионально выглядящими интерфейсами и действительными цифровыми подписями. Согласно телеметрическим данным Trend Research, случаи заражения EvilAI были зафиксированы по всему миру, оказав значительное влияние на Европу, Америку, Азию, Ближний Восток и Африку. В первую очередь пострадали производственные, правительственные и медицинские организации.

Код вредоносной программы создавался с использованием больших лингвистических моделей для придания ему вида безобидного и легитимного. Вредонос крадет конфиденциальные данные браузера и поддерживает зашифрованную AES связь с командными серверами. Для закрепления в системе EvilAI создает задачи планировщика, записи о ключах Registry Run и вредоносные ярлыки. Функциональность бэкдора включает загрузку файлов с помощью специального загрузчика, операции записи файлов, операции с реестром и выполнения процессов. Для обхода детектирования EvilAI пытается сделать так, чтобы вредоносное ПО со всех сторон выглядело легитимным. Он использует правдоподобные имена файлов и незаметно выполняет вредоносный JavaScript с помощью Node.js. Наряду с другими методами обфускации и препятствия анализу вредонос использует 32-битное хеширование MurmurHash3 для создания непредсказуемого потока управления с циклами, которые при статическом анализе кажутся потенциально бесконечными. Вредоносная программа обеспечивает продолжительный доступ, создавая задачу планировщика Windows, и, обрабатывая структурированные команды от сервера управления, поддерживает с ним непрерывную автономную связь.

Атаки с использованием DarkCloud

Киберкриминал

Целевой фишинг

Шпионское ПО

В сентябре 2025 года исследователи ESentire обнаружили фишинговую кампанию против одной производственной организации, в ходе которой была предпринята попытка доставить стилер DarkCloud. Фишинговое письмо, отправленное на адрес клиентской службы поддержки Zendesk, содержало вредоносный ZIP-архив с образцом DarkCloud внутри. Само

письмо имитировало обычную финансовую переписку с банком с соответствующей темой. DarkCloud претерпел множество обновлений: так, стаб (часть вредоноса, не имеющая вредоносной функциональности, которая обеспечивает расшифровку полезной нагрузки) полностью переписан на VB6, строки зашифрованы, внесены изменения, нацеленные на обход детектирования. Функциональность вредоноса включает кражу различной конфиденциальной информации, а именно паролей браузера, данных кредитных карт и криптовалютных кошельков, нажатий клавиш, учетных данных FTP. Похищенные данные передаются на контролируемые злоумышленниками конечные точки, включая Telegram, FTP, SMTP и веб-панель. В этой конкретной кампании использовалась не самая новая версия DarkCloud, 3.2, которая была выпущена ранее в 2025 году.

Центр реагирования на инциденты информационной безопасности промышленных инфраструктур «Лаборатории Касперского» (Kaspersky ICS CERT) — глобальный проект «Лаборатории Касперского», направленный на координацию усилий производителей систем автоматизации, владельцев и операторов промышленных объектов, а также исследователей ИТ-безопасности для защиты промышленных предприятий от кибератак. Kaspersky ICS CERT направляет свои усилия в первую очередь на выявление потенциальных и существующих угроз, нацеленных на системы промышленной автоматизации и промышленный интернет вещей.

Kaspersky ICS CERT ics-cert@kaspersky.com