Журнал Кибернновостей

vol. 6

birbank

Дорогой читатель,

Переходя во вторую половину 2025 года, количество киберинцидентов продолжает расти во всем мире. Искусственный интеллект играет значительную роль в этой меняющейся среде. С постоянно развивающимися киберугрозами оставаться информированным и бдительным остается лучшей защитой.

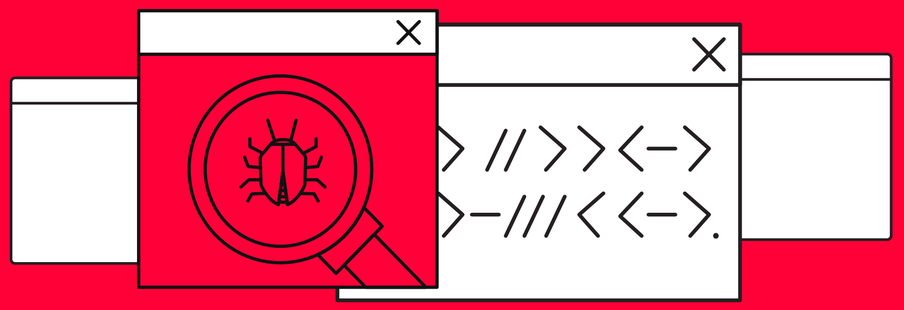
В этом выпуске мы представляем вам последние тенденции в области кибербезопасности и ключевые обновления, которые будут формировать предстоящий год.

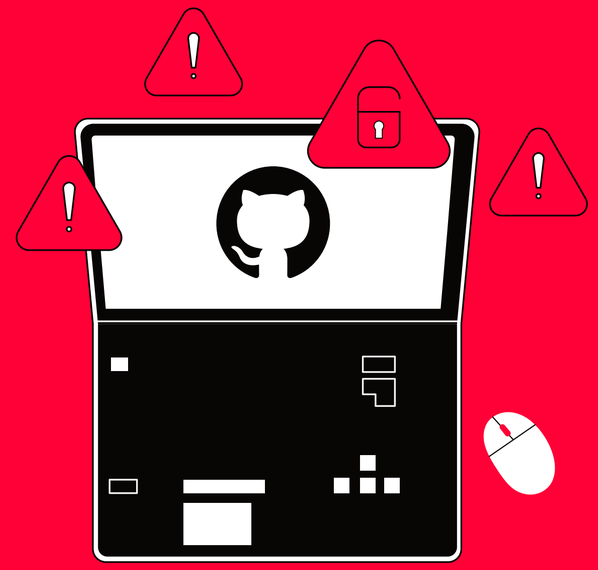
Давайте вместе исследуем динамику кибербезопасности 2025 года!

Microsoft предупреждает о кампании злонамеренной рекламы, затрагивающей **более миллион устройств**

Microsoft недавно сообщила подробности о масштабной кампании злонамеренной рекламы, затронувшей более 1 миллиона устройств по всему миру. Эта атака, впервые выявленная в декабре 2024 года, выглядит как продуманная попытка похитить личные и конфиденциальные данные пользователей.

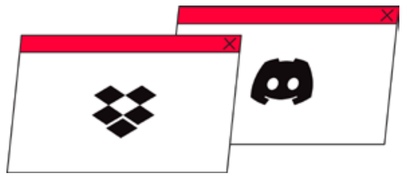
Отслеживаемая Microsoft под названием Storm-0408, эта кампания связана с группой, которая известна использованием таких методов, как фишинг, злонамеренная реклама и манипуляция результатами поисковых систем для распространения вредоносных программ. Их цель — получить несанкционированный доступ к устройствам и собрать ценную информацию.





Кампания началась с сомнительных сайтов для потоковой передачи, которые содержали вредоносные объявления. Эти объявления перенаправляли пользователей на промежуточный сайт, а затем на такие платформы, как GitHub и другие, где распространялось вредоносное ПО. Атака была нацелена как на личных пользователей, так и на бизнес, что делает её широкомасштабной угрозой.

Примечательной особенностью этой атаки стало использование GitHub для доставки первоначальной вредоносной загрузки. В отдельных случаях вредоносные файлы также размещались на таких платформах, как Discord и Dropbox. Microsoft предприняла меры, удалив скомпрометированные репозитории, хотя точное их количество не было раскрыто.



Атака разворачивается в нескольких этапах:

Этап 1:

Онлайн-платформа

Этап 2:

Вредоносная рекламная программа (adware)

Этап 3:

Вредоносный веб-сайт

Этап 4:

Зараженный пользователь

Эта кампания подчеркивает риски, связанные с злонамеренной рекламой, и показывает, как киберпреступники постоянно совершенствуют свои тактики. Это служит напоминанием для пользователей и организаций об усилении бдительности и улучшении мер кибербезопасности.

https://thehackernews.com/2025/03/microsoft-warns-of-malvertising.html

Обновления безопасности Microsoft за февраль 2025 года: **исправлены критические уязвимости**

Microsoft объявила, что в феврале было устранено 63 уязвимости безопасности. Хотя это обновление меньше по сравнению с основными исправлениями безопасности прошлого месяца, кажется, что критические проблемы безопасности все еще остаются.

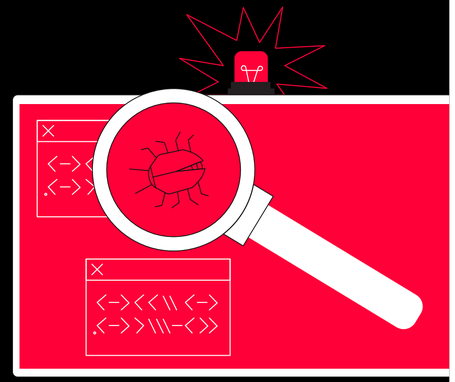
Две значительные уязвимости продолжают активно эксплуатироваться, что означает, что хакеры могут использовать их для атак на системы.

А именно:

- Одна позволяет киберпреступникам удалять файлы. Хотя утечка данных может быть маловероятной, удаление критических файлов может сделать услугу недоступной.

- Другая позволяет злоумышленникам получить полный системный уровень привилегий, что потенциально даёт им полный контроль над системой.

Microsoft
Patch Tuesday



Microsoft
Active Directory

Уязвимость Active Directory (AD): Критический риск

Другой уязвимый аспект связан с Active Directory (AD). AD это основная система, с помощью которой компании управляют пользователями и устройствами. Киберпреступники могут воспользоваться уязвимостью в протоколе LDAP, чтобы проникнуть в эту систему.

Каковы риски?

- Выполнение удаленного кода: Злоумышленники могут получить несанкционированный доступ, запуская вредоносный код.
- Повышение привилегий: Могут повысить свои права доступа от обычного пользователя до уровня администратора.
- Горизонтальное перемещение: Попав внутрь, злоумышленники могут продвигаться по сети, компроментируя другие системы.

Почему это важно?

AD управляет аутентификацией пользователей и контролем доступа в корпоративной сети.
Взлом может дать злоумышленникам неограниченный доступ к конфиденциальным данным компании. Хотя AD имеет решающее значение для управления идентификацией и доступом, это не система хранения данных. Данные обычно хранятся на выделенных серверах и в базах данных, но компроментация AD всё еще может быть шлюзом к широкомасштабным нарушениям безопасности.

В этом месяце исправления безопасности охватывают широкий спектр типов уязвимостей:

- **25 уязвимостей удаленного выполнения кода (RCE)**
- **20 уязвимостей повышения привилегий (EoP)**
- **9 уязвимостей отказа в обслуживании (DoS)**
- **5 уязвимостей подмены (Spoofing)**
- **2 уязвимости обхода средств безопасности (Security Feature Bypass)**
- **1 уязвимость раскрытия информации (Information Disclosure)**
- **1 уязвимость подделки данных (Tampering)**

В результате, несмотря на то, что февральское обновление Microsoft устраняет критические уязвимости, данные пробелы уже активно эксплуатируются, что представляет угрозу. Это служит предупреждением для компаний — не следует откладывать установку обновлений безопасности и необходимо как можно скорее принять меры для защиты своих систем.

https://thehackernews.com/2025/02/microsofts-patch-tuesday-fixes-63-flaws.html

Эти уязвимости позволяют киберпреступникам контролировать системы, удалять критические данные и распространяться внутри сети организации. Microsoft и CISA (Агентство по кибербезопасности и безопасности инфраструктуры США) призывают организации немедленно применить обновления против этих уязвимостей.

Атака Lazarus Group на LinkedIn: **фальшивые предложения-ловушки о работе**

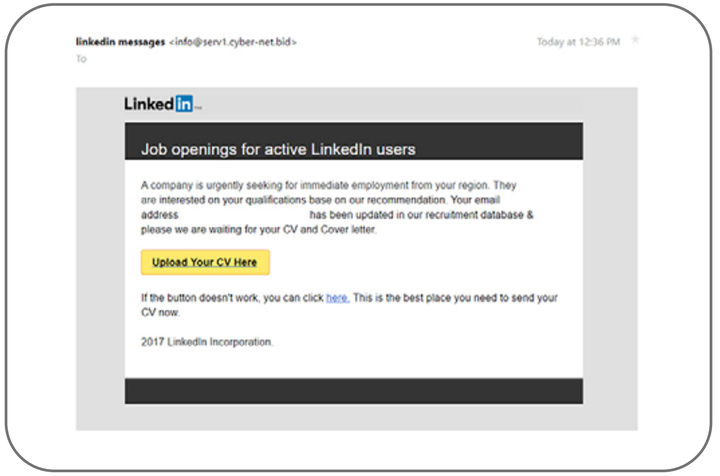
Группа киберпреступников Lazarus недавно активизировала свою кибершпионскую деятельность, используя платформу LinkedIn. Целью этой новой атаки являются сотрудники, работающие в финансовом и туристическом секторе. Группа пытается обмануть людей, предлагая фальшивые вакансии и тем самым загружая вредоносное ПО на их мобильные устройства.

Атака начинается в LinkedIn с сообщения, предназначенного для привлечения внимания и интереса, предлагая сотрудничество по проектам децентрализованных криптовалютных бирж. В сообщении предлагается удаленная работа с частичной занятостью и высокой заработной платой. Заинтересованных лиц просят отправить свои резюме или профили GitHub, что служит двойной цели: сбору личной информации и убеждению жертвы.

Такие атаки нацелены на кражу личной информации пользователя и компроментации их систем. Поэтому крайне важно избегать подозрительных предложений о работе и всегда оставаться бдительными.

После первоначального контакта жертвам отправляется проект через GitHub или Bitbucket. Эти файлы содержат скрытый код, который устанавливает вредоносное ПО на компьютеры. Это вредоносное ПО работает на операционных системах Windows, macOS и Linux. Основная цель - украсть информацию из криптовалютных аккаунтов в браузере жертвы. Вредоносное ПО создает “back door” (от англ. — «черный ход») на компьютере, позволяя киберпреступникам получить удалённый контроль.

https://socradar.io/lazarus-groups-cyber-espionage-involving-linkedin/



Сотни поддельных сайтов Reddit распространяют **вредоносное ПО Lumma Stealer**

Киберпреступник опубликовал почти 1000 поддельных сайтов, имитирующих популярные сайты, такие как Reddit и WeTransfer, заманивая пользователей для загрузки вредоносного ПО Lumma Stealer.

Эти поддельные сайты эксплуатируют бренд Reddit, инициируя фальшивое обсуждение на определенную тему. Человек, начинающий обсуждение, просит помощи в загрузке специального инструмента, другой делится ссылкой, загружая ее на WeTransfer, а третий выражает благодарность, делая всё это легитимным. Когда ничего не подозревающие пользователи нажимают на ссылку, они перенаправляются на поддельный сайт WeTransfer, где кнопка "Загрузить" запускает загрузку вредоносного ПО Lumma Stealer.

Угроза вредоносного ПО Lumma Stealer

Lumma Stealer продается киберпреступникам, которые распространяют его различными способами, такими как GitHub, через поддельные сайты и рекламу. Этот тип вредоносного ПО крадет сессионные токены для захвата паролей и учётных записей, хранящихся в браузерах пользователей. Украденные данные затем используются в сетевых атаках или социальной инженерии для получения конфиденциальной информации от компаний и частных лиц.

https://www.bleepingcomputer.com/news/security/hundreds-of-fake-reddit-sites-push-lumma-stealer-malware/

Все эти поддельные сайты на первый взгляд кажутся легитимными, имитируя название бренда и добавляя случайные числа и символы. Согласно расследованиям, был опубликован полный список страниц, участвующих в этой социальной инженерной атаке. В рамках этой кампании было обнаружено 529 поддельных сайтов Reddit и 407 поддельных сайтов WeTransfer.

Атака программ-вымогателей: группа Medusa требует до 15 миллионов долларов от жертв

С момента своего первого появления в январе 2023 года группа Medusa, занимающаяся программами-вымогателями, была связана почти с 400 атаками, количество которых увеличилось на 42% в период с 2023 по 2024 год. Только за первые два месяца 2025 года группе приписывают более 40 новых атак.

Medusa использует модель двойного вымогательства, сначала похищая данные у жертв, а затем

шифруя их системы. Эта тактика усиливает давление на организации, чтобы они выполнили требования о выкупе, так как отказ часто приводит к публикации украденных данных на сайте утечек принадлежащей группе.

С недавними нарушениями работы крупных групп программ-вымогателей (RaaS), таких как LockBit и BlackCat, Medusa стала ключевым игроком в ландшафте киберэксторсии. Другие группы программ-вымогателей, включая RansomHub (также известную как Greenbottle и Cyclops), Play (Balloonfly) и Qilin (Agenda, Stinkbug, Water Galura), также расширили свои операции

Требования о выкупе от Medusa сильно варьируются и составляют от 100 000 до 15 миллионов долларов. Группа в основном нацеливается на крупные организации, включая финансовые учреждения, государственные органы, некоммерческие организации и поставщиков медицинских услуг. Их атаки часто используют уязвимости в приложениях с публичным доступом, таких как Microsoft Exchange Server, для получения первоначального доступа.

Как и большинство групп программ-вымогателей, Medusa имеет финансовую мотивацию и не придерживается идеологических или политических взглядов, сосредотачиваясь исключительно на вымогательстве денег у высокоприоритетных целей в различных отраслях.

https://www.linkedin.com/pulse/medusa-ransomware-hits-40-victims-2025-demands-100k15m-ransom-mafic/

https://thehackernews.com/2025/03/medusa-ransomware-hits-40-victims-in.html

16 расширений Chrome были скомпрометированы, что подвергло **риску более 600 000 пользователей**

Недавняя кибератака скомпрометировала 16 расширений Chrome, подвергнув риску более 600 000 пользователей, чьи личные данные могли быть украдены.

Злоумышленники использовали изощренную фишинговую схему, нацеленную на разработчиков, создающих расширения для Chrome Web Store. Получив доступ, хакеры внедрили вредоносный код в легитимные расширения, что позволило им похищать конфиденциальные данные, такие как cookies и токены входа пользователей.

cyberhaven

27 декабря компания Cyberhaven сообщила, что одна из их собственных расширений стала жертвой атаки. Хакеры использовали это расширение для связи с внешним сервером, загрузки дополнительных вредоносных файлов и сбора данных пользователей.

Обзор угроз

Фишинговые электронные письма были оформлены так, чтобы выглядеть как сообщения от службы поддержки разработчиков Google Chrome Web Store. Они ложно предупреждали разработчиков о том, что их расширения могут быть удалены из-за нарушения политик, и просили их перейти по ссылке для решения проблемы. Эта ссылка вела на вредоносную страницу, которая предоставляла злоумышленникам доступ к вредоносному приложению под названием “Privacy Policy Extension”.

Эксперты теперь предупреждают, что расширения для браузеров, которые часто игнорируются, могут получать доступ к большому количеству конфиденциальной информации пользователей. “Многие организации даже не осознают, какие расширения установлены в их системах, и это делает их уязвимыми для таких атак,” — заявил Ор Эшед, генеральный директор LayerX Security.

Это является важным напоминанием о необходимости быть бдительным в вопросах безопасности расширений для браузеров и внимательно следить за устанавливаемыми расширениями.

https://www.linkedin.com/pulse/16-chrome-extensions-hacked-exposing-over-600000-users-data-6urvc/

birbank

Если у вас есть предложения или отзывы, пожалуйста, свяжитесь с нами по этому адресу электронной почты: cyberjournal@kapitalbank.az