IBM X-Force отчет 2023

Угрозы Информационной Безопасности в Облаке

Who is X-Force?

X-Force — это ориентированная на угрозы команда хакеров, специалистов реагирования, исследователей и аналитиков. Портфолио X-Force включает наступательные и оборонительные продукты и услуги, основанные на всестороннем обзоре угроз.

В эпоху непрекращающихся кибератак, всеобщей взаимосвязанности и растущих нормативных требований организациям необходим целенаправленный подход к обеспечению безопасности. Посредством тестирования на проникновение, управления уязвимостями и служб моделирования противников команда хакеров X-Force Red берет на себя роль субъектов угроз, которые находят уязвимости безопасности, подвергая риску ваши наиболее важные активы. Благодаря услугам по обеспечению готовности к инцидентам, их обнаружению и реагированию, а также услугам по управлению кризисами команда X-Force IR знает, где могут скрываться угрозы и как их остановить. Исследователи X-Force создают наступательные методы для обнаружения и предотвращения угроз, в то время как команда X-Force собирает и преобразует данные об угрозах в полезную информацию для снижения риска.

Благодаря глубокому пониманию того, как субъекты угроз думают, разрабатывают стратегии и наносят удары, команда X-Force может помочь предотвращать, обнаруживать, реагировать на инциденты и восстанавливаться после них, а также может помочь сосредоточиться на бизнес-приоритетах

Индекс аналитики угроз в облаке X-Force 2023

Команда IBM® X-Force® четвертый год выпускает отчет о ландшафте угроз в облаке, который публикуется, чтобы помочь клиентам и более широкому сообществу разработать стратегию облачной безопасности.

Для подготовки этого отчета команда X-Force проанализировала данные нескольких поставщиков облачных услуг (CSP), собранные в период с июня 2022 года по июнь 2023 года и полученные из следующих источников:

- Анализ угроз IBM X-Force
- Тесты на проникновение IBM X-Force Red
- Действия IBM X-Force по реагированию на инциденты (IR)
- Аналитика Red Hat®
- Анализ даркнета, проведенный командой X-Force, и данные отчета Cybersixgill.

Данные в отчете демонстрируют способы, с помощью которых команда следила за злоумышленниками, ставящими под угрозу облачную среду, и типы вредоносных действий, которые они осуществляют, находясь внутри облака. С данными, хранящимися в облаках связаны 82% утечек . По этой причине организациям необходимо научиться эффективно готовиться и реагировать на инциденты безопасности, связанные с их облачными средами.[1]

Индекс аналитики угроз в облаке X-Force 2023

Ключевые выводы

1. **Неправильное использование легитимных учетных данных вредит облачной среде**

   Данные X-Force IR показывают, что использование действительных учетных данных (T1078.004[2]) было наиболее распространенным вектором первоначального доступа в инцидентах безопасности облака, произошедших в 36% случаев.

   Команда X-Force обнаружила учетные данные в виде открытого текста, расположенные на конечных точках пользователей, в 33% случаев взаимодействия с облачными средами.

2. **Наблюдается рост проблем безопасности контейнеров**

   Команда X-Force Red сообщила о значительном росте использования пользовательских определений ресурсов в кластерах Kubernetes организаций, что может стать проблемой безопасности, если определение реализовано плохо или без соответствующего уровня процессов разработки, включающих безопасность.

Индекс аналитики угроз в облаке X-Force 2023

Ключевые выводы

3. **Уязвимости обнаруживаются и раскрываются все чаще**

   За отчетный период команда X-Force отследила 632 новых распространенных уязвимостей и воздействий (**C**ommon **V**ulnerabilities and **E**xposures - CVE), связанных с облаком. Эта цифра на **194%** больше, чем в предыдущем году.

4. **Последствия использования этих CVE различны**

   Более 40% CVE, обнаруженных за отчетный период, могли позволить злоумышленнику либо получить информацию (21%), либо получить доступ (20%).

5. **Облако по-прежнему остается популярным товаром в даркнете**

   В отчетный период учетные данные составляли почти 90% облачных активов, выставленных на продажу в даркнете.

   Средняя цена этих учетных данных составила 10,68 долларов США, что представляет собой незначительное снижение по сравнению с предыдущим отчетным периодом.

Индекс аналитики угроз в облаке X-Force 2023

Векторы начального доступа

Команда X-Force проанализировала все инциденты, связанные с облаком, за отчетный период и определила следующие наиболее распространенные векторы атак и отраслевые тенденции, влияющие на облачную инфраструктуру:

- **Использование действительных облачных учетных данных** было наиболее наблюдаемым вектором первоначального доступа в облачных средах: оно наблюдалось в 36% случаев, на которые отреагировала команда X-Force.
- **Эксплуатация общедоступных приложений** (T1190[3])наряду с фишинговыми и целевыми фишинговыми ссылками (T1566.002[4])заняла второе место, на долю которых приходится примерно 14% инцидентов.
- **СМИ и развлечения** лидировали во всех отраслях: на них пришлось 21% всех инцидентов, связанных с облаком, на которые команда X-Force отреагировала за отчетный период.
- Учитывая распределенный характер облачных вычислений, **каждый географический регион мира подвергается облачным атакам**. По данным X-Force IR, в Европе произошло 64% инцидентов, связанных с облаками, за ней следует Северная Америка с 29%. Данные Red Hat Insights еще раз подтверждают эти выводы: на европейские организации приходится 87% сканирований на вредоносное ПО, за ними следует Северная Америка с 12%.

Индекс аналитики угроз в облаке X-Force 2023

Использование легитимных учетных данных

Злоумышленники, желающие проникнуть в сеть или глубже проникнуть в среду жертвы, часто делают это, используя легитимные учетные данные, обнаруженные во время атаки или собранные до нападения на конкретную жертву. В тех случаях, когда облачная инфраструктура является частью поверхности атаки, эти учетные данные могут использоваться для доступа к облачным ресурсам, не вызывая соответствующего уровня подозрений.

Команда X-Force обнаружила учетные данные в виде открытого текста, расположенные на конечных точках пользователей в 33% случаев взаимодействия с облачными средами. В частности, учетные данные сервисных учетных записей часто хранились на конечных точках, и многие из них имели завышенные привилегии (т.е. них было больше разрешений, чем им необходимо для выполнения своей работы или задачи). Скомпрометированные учетные данные стали причиной более трети инцидентов, связанных с облаком, которые наблюдала команда X-Force, что позволяет предположить, что предприятиям приходится сбалансировать потребности пользователей в доступе и риски безопасности. Организации могут извлечь выгоду из средств защиты личных данных на базе искусственного интеллекта, которые помогают детально выявлять поведенческие аномалии и проверять личность пользователей.

Индекс аналитики угроз в облаке X-Force 2023

Эксплуатация общедоступных приложений

Эксплуатация уязвимостей в общедоступных приложениях — это проверенный и надежный вектор доступа для злоумышленников как в облачных, так и в локальных средах. Организациям обычно сложнее управлять облачными приложениями из-за растущего числа приложений и сервисов, используемых в современной облачной или гибридной облачной среде. При неправильной реализации можно не заметить устаревшее приложение, работающее в облаке, или, что еще хуже, не заметить, что это приложение вообще используется.

В 2022 году уязвимость **Apache Log4j**[5] оказала значительное влияние на все отрасли из-за чрезвычайно широкого распространения библиотеки Log4j. Эту уязвимость, обнаруженную в декабре 2021 года, было легко использовать, что сделало ее популярным выбором для использования в своем наборе инструментов многими злоумышленниками. По этим причинам мы по-прежнему видим, что Log4j подвергается злоупотреблениям даже в 2023 году. В рамках партнерства с командой Red Hat Insights команда X-Force проанализировала файлы, связанные с фишинговой кампанией по электронной почте, которая включала вредоносные Bash-скрипты криптомайнинга, пытающиеся использовать Log4j. уязвимость в системах Linux®.

Индекс аналитики угроз в облаке X-Force 2023

Перехват легитимных прокси-сервисов (Proxyjacking)

Команда X-Force наблюдала, как злоумышленники устанавливали прокси-программы — законный инструмент сегментации сети — на ничего не подозревающие системы жертв, чтобы перепродать пропускную способность компьютеров жертв.

Исследования показывают, что кампания proxyjacking'а может принести злоумышленникам примерно 9,60 долларов США в течение 24 часов за один IP-адрес, а ее развертывание с помощью Log4j может принести 220 000 долларов США прибыли в месяц.[6]

Кроме того, proxyjacking может привести к тому, что жертвам придется платить крупные сборы облачным провайдерам из-за неожиданного увеличения веб-трафика. Proxyjacking труднее обнаружить, чем криптомайнинг, поскольку криптомайнинг можно обнаружить путем мониторинга использования ЦП.

Индекс аналитики угроз в облаке X-Force 2023

Не прекращающееся использование виртуальных сред

В соответствии с наблюдениями команды X-Force Агентство кибербезопасности и безопасности инфраструктуры (CISA) и ФБР выпустили в начале 2023 года совместную рекомендацию в ответ на продолжающуюся кампанию вымогателей, получившую название ESXiArgs.

Злоумышленники в этой кампании по вымогательству использовали уязвимости серверов VMware ESXi (CVE-2021-21974[7]) для получения доступа, развертывания программ-вымогателей и шифрования файлов на серверах ESXi, что потенциально делало виртуальные машины (ВМ) непригодными для использования.

Индекс аналитики угроз в облаке X-Force 2023

Семейства вредоносных программ и облачный хостинг файлов

Специалисты по обратному проектированию вредоносных программ X-Force заметили, что злоумышленники широко используют облачные службы хостинга файлов, такие как Dropbox, Microsoft OneDrive или Google Drive, для распространения вредоносного программного обеспечения, которое выглядит законным, в том числе:

- Банковский троян Grandoreiro, использующий Microsoft Azure.
- Бэкдор RokRAT с использованием OneDrive – ITG18, также известный как вредоносное ПО Yellow Garuda, использующий OneDrive, Dropbox и Google Drive.
- Бэкдор Marlin с использованием OneDrive
- Вредоносное ПО Graphite, использующее OneDrive.
- Общее вредоносное ПО, использующее OneDrive[8].

Индекс аналитики угроз в облаке X-Force 2023

Безопасность контейнеров

В этом году исследователи X-Force заметили значительный рост использования технологии пользовательских определений ресурсов Kubernetes Custom Resource Definition – CRD. (Подробнее см., например, https://habr.com/ru/companies/vk/articles/515138/).

Все большее число организаций имеют больше возможностей и желания создавать собственные ресурсы в своих кластерах Kubernetes. Они часто делают это без обычного процесса разработки приложений, обеспечивающего безопасность, поскольку используют внутренние интерфейсы программирования приложений (API).

Этот процесс открывает новые возможности в кластерах Kubernetes. Некоторые CRD представляют собой готовые решения, которые пользуются широкой поддержкой, в то время как другие представляют собой компоненты, требующие меньших усилий, изготовленные собственными силами или при минимальной поддержке со стороны сообщества. Эксплуатация этих CRD может быть исключительно простой или исключительно сложной.

Индекс аналитики угроз в облаке X-Force 2023

Целенаправленные действия: Майнинг, Инструменты удаленного доступа (RAT) и боты

Хотя облачные среды подвергались попыткам вымогательства данных, большая часть активности угроз за анализируемый период, судя по всему, была сконцентрирована на использовании скомпрометированного доступа к облачным ресурсам для майнинга криптовалют. Подобно тенденции, отмеченной в прошлогоднем отчете, в 2023 году команда X-Force наблюдала, как криптомайнер XMRig был развернут на машинах с Linux и в облачных экземплярах. XMRig используется в качестве основной полезной нагрузки для майнинга криптовалюты Monero.

Преступников облачные платформы привлекают, вероятно, по следующим причинам:

1. Криптомайнинг требует больших ресурсов и является дорогостоящим. Воспользовавшись скомпрометированной инфраструктурой, злоумышленники могут переложить расходы на жертву.
2. Злоумышленники рассчитывают на то, что облачные ресурсы подвергаются менее тщательному и бдительному мониторингу по сравнению с локальными ресурсами, что позволит майнинговым вредоносным программам работать дольше, прежде чем они будут обнаружены и удалены.
3. Такие уязвимости в интернет-инфраструктуре Log4j, позволили злоумышленникам сканировать, эксплуатировать и развертывать криптомайнеры в больших масштабах.

Индекс аналитики угроз в облаке X-Force 2023

Целенаправленные действия: Майнинг, Инструменты удаленного доступа (RAT) и боты

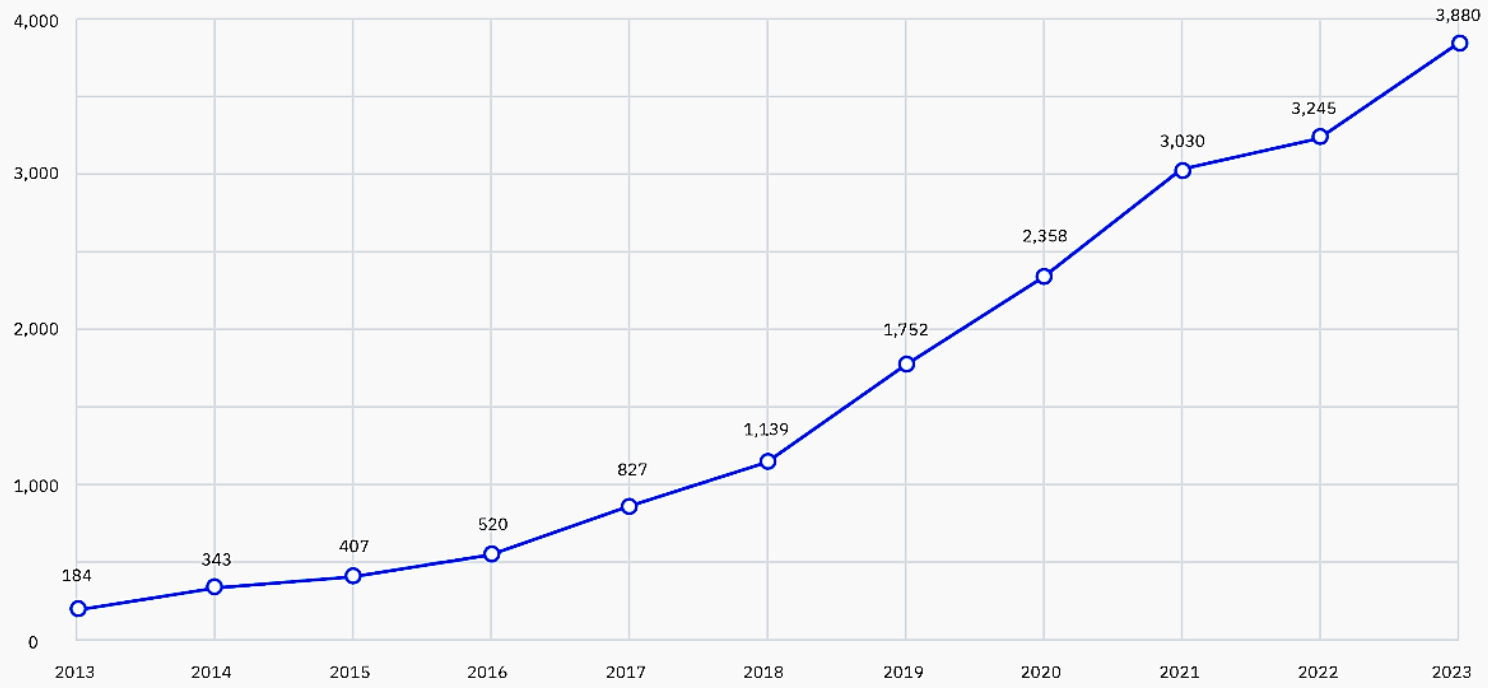
Chaos RAT: команда X-Force также наблюдала, как инструмент удаленного администрирования Chaos (Trojan.Linux.CHAOSRAT) развертывается в качестве инструмента удаленного доступа (RAT). Функции Chaos RAT включают загрузку, загрузку и удаление файлов обратной оболочки; скриншоты; сбор информации об операционной системе; выключение и перезапуск хоста; и открытие URL-адресов. Этот RAT демонстрирует сложность и эволюцию облачных угроз.

KeyBot: исследователи X-Force наблюдали и анализировали KeyBot, сканер, написанный на Python, который используется для сканирования списка доменов на предмет ключей, связанных с различными сервисами, включая облачные приложения. Этот конкретный штамм вредоносного ПО был замечен нацеленным на серверы Amazon Web Services (AWS). Действия, выполняемые в системе, включали удаление файлов, механизмы сохранения, детали выполнения процессов и сетевые коммуникации.

.

Индекс аналитики угроз в облаке X-Force 2023

Уязвимости облака: восходящая траектория



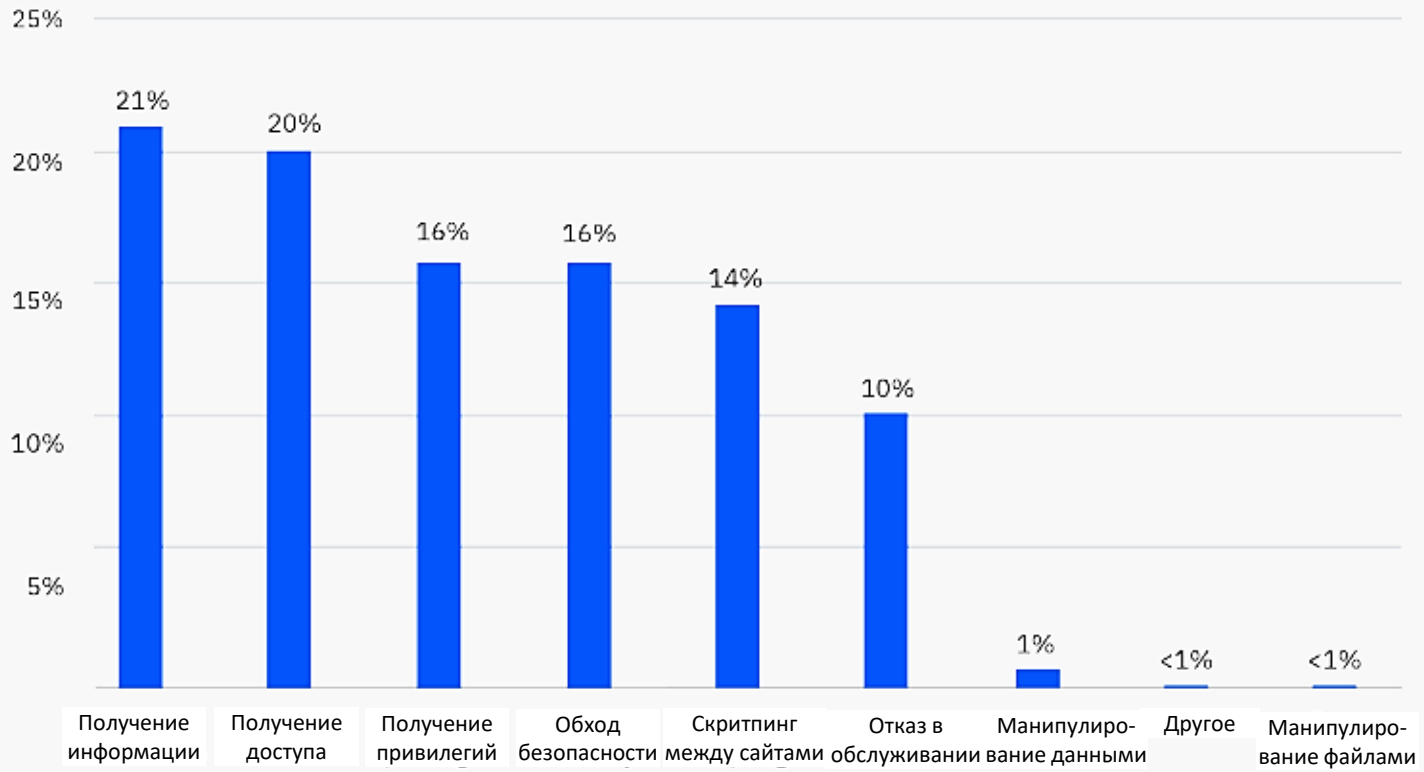
Общее количество облачных уязвимостей, отслеживаемых X-Force Red Vulnerability Management Service составляет около 3900.

Число отслеживаемых облачных уязвимостей за последнее десятилетие выросло в геометрической прогрессии и удвоилось по сравнению с 2019 годом.

Новые CVE, отслеживаемые за последнее десятилетие, имеют тенденцию к росту.[9] Несмотря на спад в 2022 году, в 2023 году наблюдали 632 новых CVE

Индекс аналитики угроз в облаке X-Force 2023

Уязвимости облака: классификация новых CVE



Команда X-Force классифициро-вала новые CVE в соответствии с их потенциальным воздействием. Получение, доступа и привилегий — это три основных последствия CVE, обнаруженных в течение отчетного периода.

CVE часто используют в качестве первоначального вектора доступа. для достижения конечной цели, включать развертывание крипто-майнеров, программ-вымогателей и других типов вредоносов.

Получение информации – это CVE воздействие номер один

Индекс аналитики угроз в облаке X-Force 2023

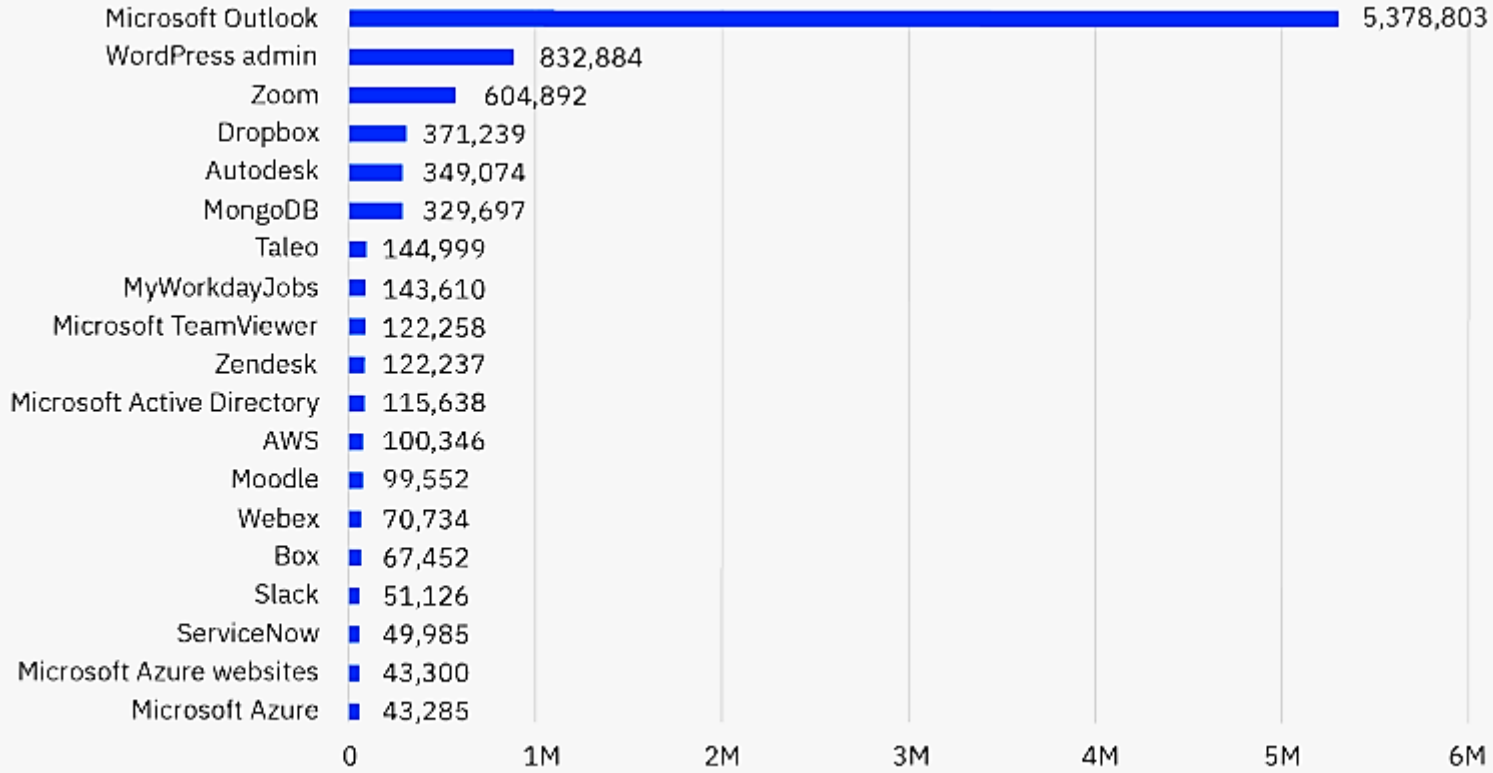
Облако и даркнет

Для отчета за 2023 год исследователи X-Force проанализировали данные в сотрудничестве с Cybersixgill, чтобы получить представление о том, как облачная инфраструктура используется на торговых площадках даркнета. Для проведения этого анализа были собраны данные с различных темных форумов и извлечены некоторые ключевые идеи и выводы из этих наблюдений. Следующий анализ основан на исследовании даркнета командой X-Force с июня 2022 по июнь 2023 года.

Злоумышленники часто продают или запрашивают скомпрометированные учетные данные некоторых из самых популярных облачных решений «программное обеспечение как услуга» (SaaS). Это дает им самый широкий уровень доступа с заданным набором имен пользователей и паролей. Исследование показывает, что Microsoft Outlook был, несомненно, наиболее упоминаемым SaaS-решением в дискуссиях на рынке даркнета, за ним следовали WordPress и Zoom.

Индекс аналитики угроз в облаке X-Force 2023

Облако и даркнет: Наиболее упоминаемые SaaS-решения в даркнете



Понимание того, какой тип доступа к облаку продают злоумышленники, может помочь понять, как им удалось скомпрометировать учетные записи. На рисунке показаны наиболее распространенные типы продаваемого доступа к облаку, согласно анализу X-Force

Индекс аналитики угроз в облаке X-Force 2023

Облако и даркнет: Продаваемые типы доступа

Учетные данные: этот доступ к облаку включает комбинации имени пользователя и пароля для учетных записей облака. Учетные данные также могут включать в себя различную дополнительную информацию об хосте, относящуюся к зараженной системе. В большинстве случаев этот доступ к облаку включает в себя версию операционной системы, IP-адрес и другие данные, захваченные различными вредоносными программами, крадущими информацию, например, дополнительные учетные данные для других служб. В 2023 году наблюдалось небольшое снижение цен на учетные данные: с 11,74 доллара США в 2022 году до 10,68 доллара США в отчете за этот год.

Электронная почта: В форме простого протокола передачи почты (SMTP) учетные записи электронной почты позволяют злоумышленникам рассылать спам и фишинговые электронные письма. Настройки, специфичные для учетной записи, например, сколько ежедневных сообщений электронной почты можно отправлять, могут повлиять на цену продажи.

Shell или SSH: SSH — это протокол, который позволяет авторизованным пользователям открывать удаленные оболочки на других компьютерах. Доступ к оболочке, скорее всего, указывает на возможность инициировать обратное соединение с оболочкой на целевом ресурсе.

Индекс аналитики угроз в облаке X-Force 2023

Облако и даркнет: Продаваемые типы доступа

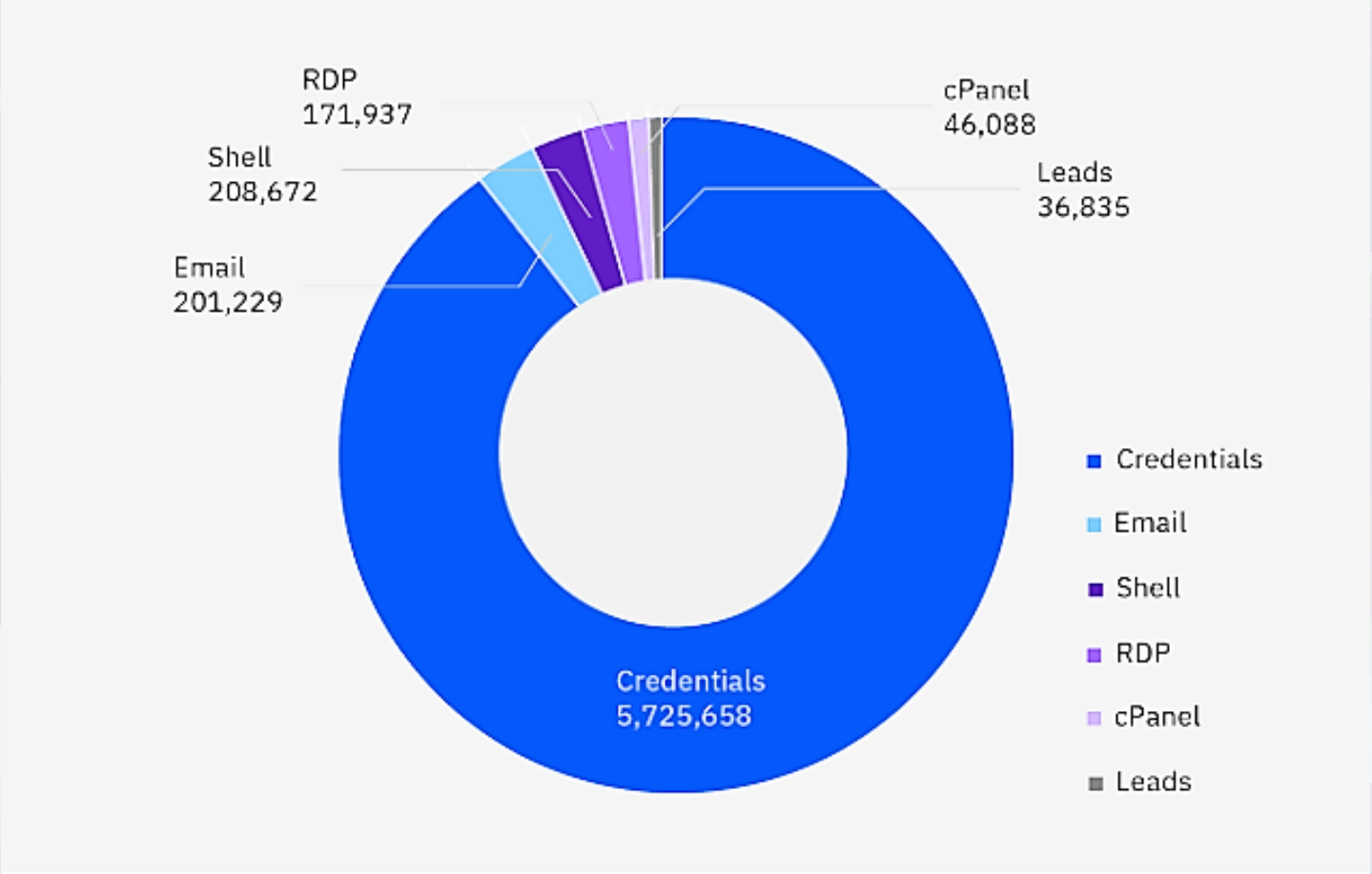
Протокол удаленного рабочего стола (RDP): RDP представляет учетные данные для систем под управлением Microsoft Windows, работающих на облачном ресурсе. Определенные факторы, такие как доступные ресурсы, могут влиять на воспринимаемую ценность счета. Например, система с большим объемом оперативной памяти и вычислительными возможностями обычно требует более высокой цены, чем система с меньшим количеством ресурсов. Наблюдался скачок цен на доступ по RDP с 7,98 долларов США за доступ в 2022 году до 10,67 долларов США в 2023 году.

cPanel, также известный как WebHost Manager (WHM): WHM — это инструмент административного доступа, который позволяет пользователям управлять внутренней частью учетных записей cPanel. cPanel — это графический интерфейс на базе Linux, который позволяет пользователю управлять сервером.

Leads: Lead – это список адресов электронной почты, который злоумышленники могут использовать для рассылки спама и фишинговых кампаний, и который обычно продаётся как есть. Злоумышленники используют многочисленные торговые площадки и форумы для рекламы товаров, выставленных на продажу в даркнете. Анализ публикаций с июня 2022 года по июнь 2023 года позволил извлечь информацию о ценах с различных торговых площадок даркнета.

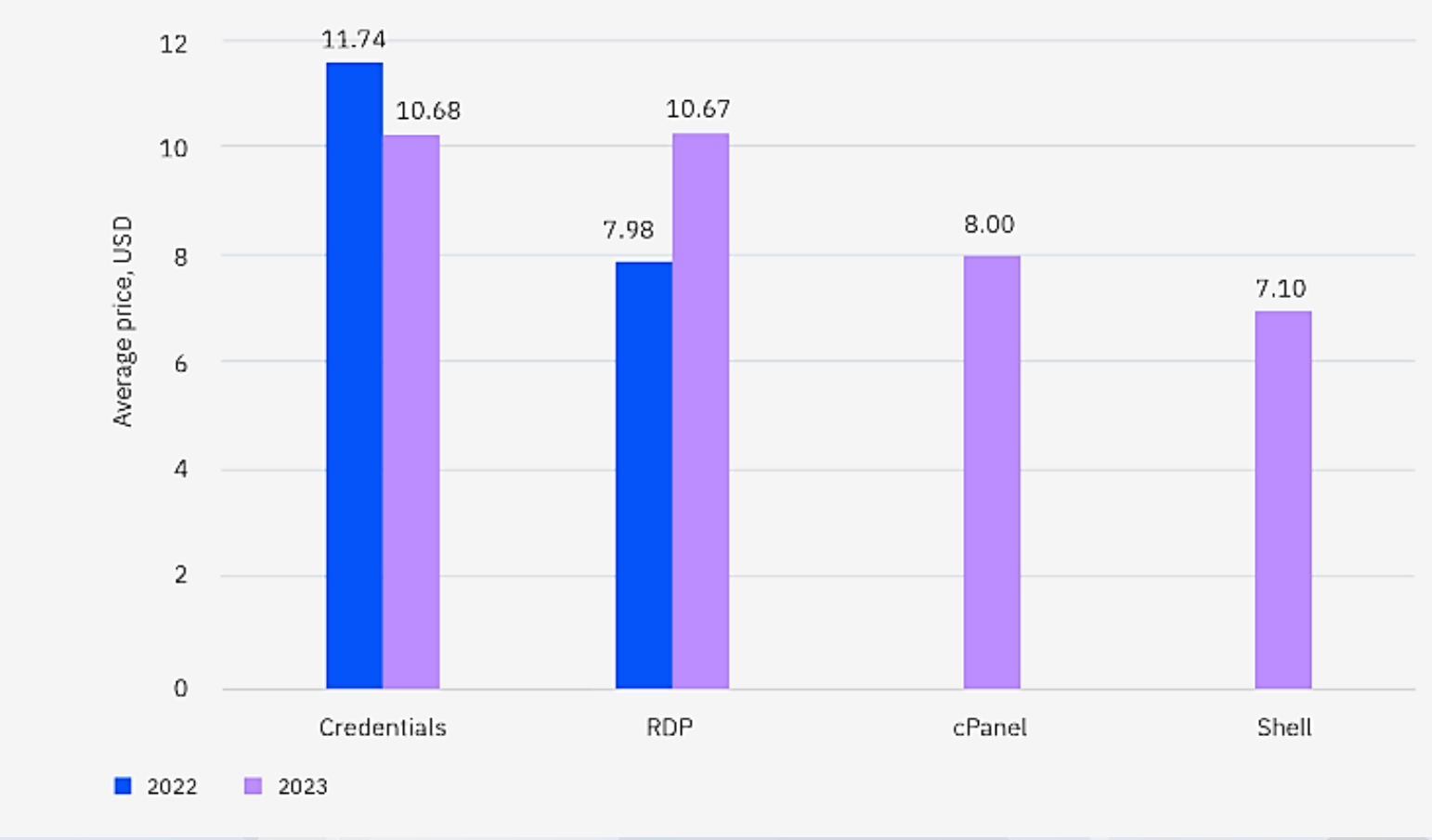
Индекс аналитики угроз в облаке X-Force 2023

Облако и даркнет: Число продаж по типам доступа



Индекс аналитики угроз в облаке X-Force 2023

Облако и даркнет: Цены на взломанные облачные учетные записи



Индекс аналитики угроз в облаке X-Force 2023

Распределение инцидентов по отраслям промышленности и географии

Хотя организации во всех отраслях и регионах подвержены одним и тем же облачным уязвимостям и рискам, с прошлого года команда X-Force стала свидетелем того, что больше всего инцидентов, связанных с облачными технологиями, произошло в сфере СМИ и развлечений — на их долю приходится 21% случаев.

Согласно третьему ежегодному индексу корпоративных облаков Nutanix, индустрия СМИ и развлечений «лидирует в эксклюзивном использовании нескольких общедоступных облачных сервисов и опережает в развертывании гиперконвергентной инфраструктуры (HCI)».[10] Такая агрессивная стратегия внедрения облака может способствовать высокому рейтингу инцидентов, учитывая, что для атак доступно больше целей

Кроме того, на Европу пришлось 64% инцидентов, на которые отреагировала команда X-Force, что также может быть результатом интенсивного использования облачных технологий в этом регионе. Согласно отчету Forrester «Состояние европейских облачных технологий, 2022 год», 87% европейских предприятий используют несколько общедоступных облачных платформ[11]. Этот процент соответствует множеству потенциальных целей.

Индекс аналитики угроз в облаке X-Force 2023

Рекомендации и лучшие практики

1. Используйте подход стратегии безопасности с нулевым доверием, включающий реализацию многофакторной аутентификации (MFA) и принцип наименьших привилегий.
2. Внедряйте передовые методы активации и деактивации устройств и служб, включающие сканирование и исправление уязвимостей на протяжении всего жизненного цикла системы, в том числе:
   - управление идентификацией и доступом (Identity and Access Management - IAM), для уменьшения зависимости от комбинаций имени пользователя и пароля и борьбы с кражей учетных данных
   - проверка цифровой идентификации и поведения, их легитимности для интеллектуальной аутентификации с использование возможностей искусственного интеллекта.
   - автоматизация управлением привилегиями группы безопасности и созданием новых пользователей с минимальными привилегиями по умолчанию.
3. По возможности используйте открытый и интегрированный подход к безопасности, чтобы устанавливать безопасные соединения и передавать данные безопасности между точками, которые находятся во фрагментированных облачных средах. Приоритет отдавайте использованию платформ безопасности, опирающихся на открытые технологии и обеспечивающих тесную интеграцию между инструментами для создания централизованной панели управления.

.

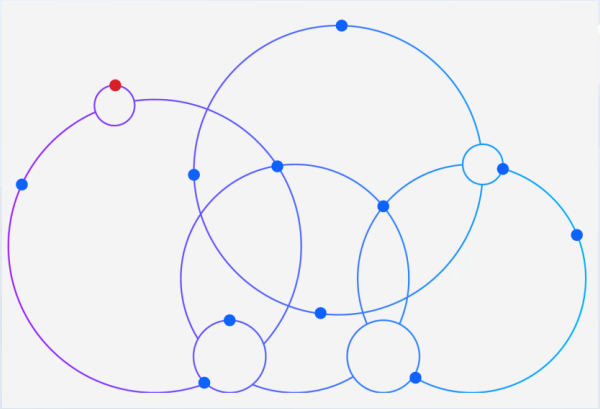
Индекс аналитики угроз в облаке X-Force 2023

Ссылки:

1. Cost of a Data Breach Report 2023, Ponemon Institute and IBM Security®, July 2023.
2. Valid Accounts: Cloud Accounts, MITRE ATT&CK, 21 March 2023.
3. Exploit Public-Facing Application, MITRE ATT&CK, 14 April 2023.
4. Phishing: Spearphishing Link, MITRE ATT&CK, 11 April 2023.
5. Log4j - Initial Access to the Cloud, Palo Alto Networks, Inc., 21 March 2022.
6. Proxyjacking has Entered the Chat, Sysdig, Inc., 4 April 2023.
7. CVE-2021-21974, The MITRE Corporation, 4 January 2021.
8. К общим вредоносным программам относятся загружающие (loaders) и выгружающие (downloaders) программы, которые явно не привязаны к одному конкретному семейству вредоносных программ..
9. Команда X-Force использует многогранный алгоритм ранжирования для определения приоритетов и оценки серьезности уязвимостей с помощью оценки риска, в которой используются такие факторы, как простота использования, уровень предоставленного доступа и влияние на затронутую систему. Эта информация вставляется в формулу риска, которая оценивает угрозу на основе общей системы оценки уязвимостей (CVSS), потенциального возможного ущерба, сложности и полезности для злоумышленника.
10. Cloud Migration a Top Priority for Media and Entertainment Industry, Spiceworks Inc., 9 November 2021.
11. Cloud Usage Is Alive And Well In The European Cloud Market, Forrester, 19 July 2022.

.

IBM X-Force Cloud Threat Landscape Report 2023



Благодарю за внимание!

Ронжин В.В.
Для группы компаний «Nihol»
Октябрь 2023г.