VARONIS

ОФИЦИАЛЬНЫЙ ДОКУМЕНТ

Пять угроз при удаленной работе

и как от них защититься

Непрерывность бизнес-процессов **и угрозы безопасности**

В связи со стремительным ростом числа сотрудников, работающих удаленно, службы информационной безопасности вынуждены ослаблять меры защиты ради обеспечения бесперебойной работы своих предприятий. Количество VPN-устройств и серверов для работы с удаленными рабочими столами с выходом в интернет в последнее время резко увеличилось. Например, лишь за последний месяц их число выросло на 30%, и значительно возросло использование платформы Microsoft Teams. Такие факторы как смягчение политик безопасности и отмена строгих требований к использованию VPN, чтобы сотрудники имели возможность работать с файлами, почтой и приложениями из дома, могут представлять огромный риск для компаний.

Команда Varonis подготовила список из пяти наиболее распространенных рисков, а также рекомендации по их предотвращению.

1. **Взлом VPN путем перебора паролей**
2. **Фишинг**
3. **Атака через посредника (Man-in-the-Middle)**
4. **Вредоносные приложения Azure**
5. **Внутренние угрозы**

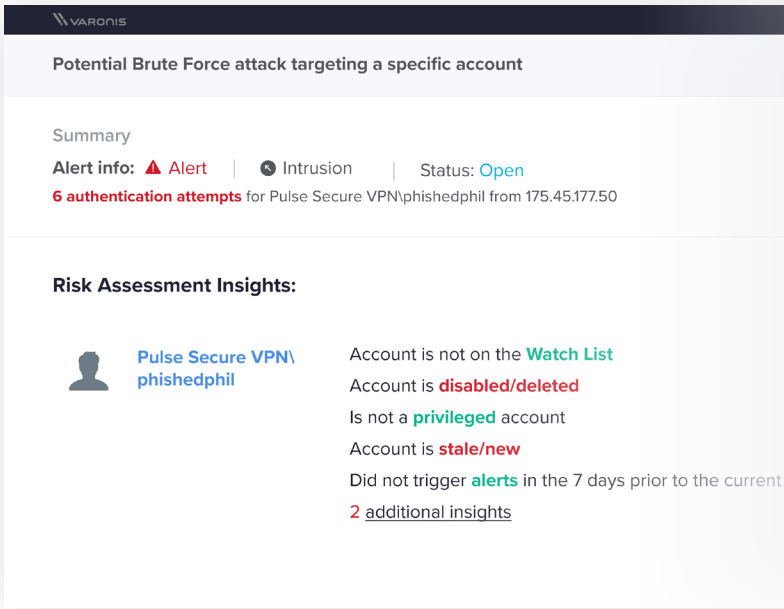
1 Взлом VPN путем перебора паролей

VPN часто является шлюзом для доступа к важным и конфиденциальным данным. С ростом количества сотрудников, работающих из дома, организации стали разрешать доступ через VPN значительно большему числу пользователей. Зная об этом, хакеры часто пытаются получить доступ к VPN путем полного перебора всех возможных вариантов паролей. Подобрав пароль к VPN, хакеры могут повышать свои права, изучать объекты в сети и использовать чужие учетные данные для хищения конфиденциальной информации.

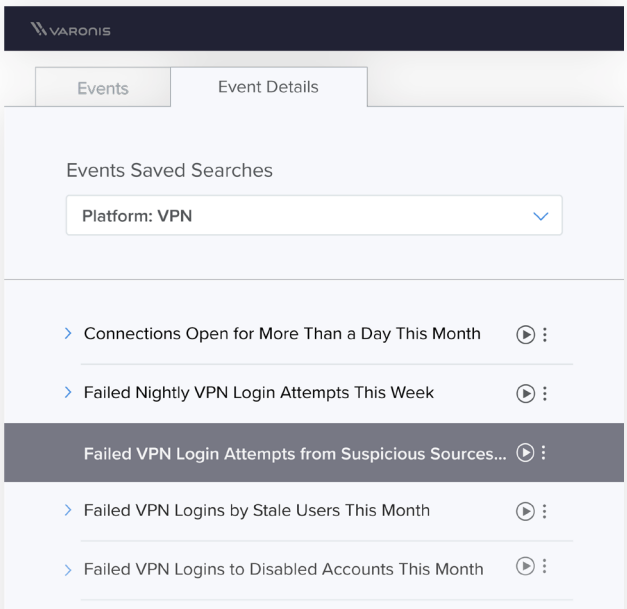
Но под угрозой *не только* VPN. Наша команда наблюдает скачкообразный рост случаев подбора паролей к Active Directory и веб-сервисам, использование которых в последнее время увеличилось. При этом одни организации отключают оповещения о превышении определенного количества неудачных попыток входа, а другие не следят за процессом аутентификации пользователей. К тому же, важно понимать, что далеко не все действия хакеров заметны и оставляют следы.

Чем может помочь Varonis

Встроенные модели угроз Varonis позволяют обнаружить аномальные попытки аутентификации в VPN и Active Directory: заполнение учетными данными, распыление паролей и брутфорс-атаки. Наши модели угроз учитывают больше контекста о событиях: каждое событие дополняется данными из Active Directory, веб-прокси и систем хранения, таких как SharePoint или OneDrive.



Вы также можете провести быстрый анализ VPN активности — и мы не имеем ввиду просмотр необработанных журнальных записей, а дополненные контекстом полноценные сведения о событиях. Затем эти сведения можно использовать для отчетности или обнаружения угроз:

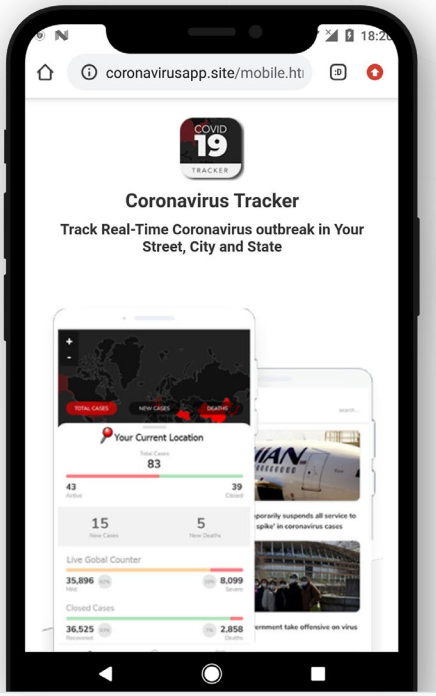


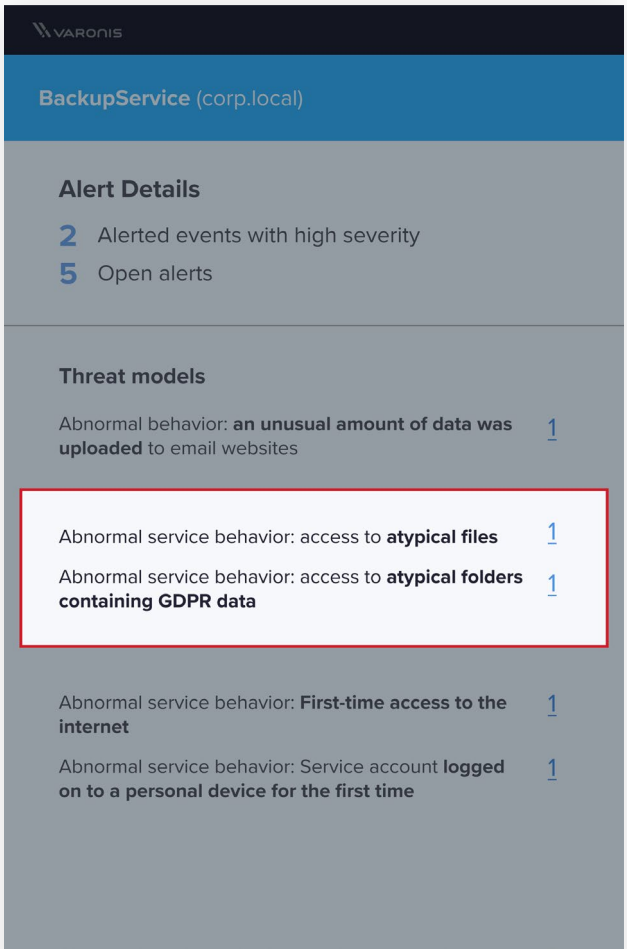
Подробный разбор атак методом перебора паролей в блоге Varonis

2 Фишинг

Фишинг — это один из самых популярных способов, используемый киберпреступниками для проникновения на устройства своих жертв, и, учитывая жажду информации у современного общества, этот способ крайне эффективен. В поле нашего зрения попало **несколько псевдокампаний, посвященных коронавирусу,** которые заманивали пользователей почтовыми рассылками о пожертвованиях, медикаментах и вакцинах.

Нажатие на ссылки в фишинговых электронных письмах и открытие зараженных вложений может привести к установке на ваше устройство вредоносных программ, с помощью которых злоумышленник сможет установить контроль и управление над вашим устройством, заражать другие устройства в вашей сети, внедрять программы-вымогатели или похищать данные. Сотрудники, использующие для доступа к корпоративным ресурсам своиличные устройства, особенно уязвимы для **атак с помощью скрытой загрузки**.





Чем может помочь Varonis

Varonis обнаруживает сетевую активность, похожую на попытки установить контроль и управление, не только путем поиска подключений к известным опасным IP-адресам и доменам, но и с помощью глубокого анализа трафика DNS и веб-прокси. Это позволяет обнаруживать вредоносные программы, которые маскируют передаваемые данные в трафике HTTP или DNS.

В дополнение к обнаружению вредоносных программ, модели угроз Varonis часто находят взломанного пользователя путем анализа отклонений в доступе к файлам и электронной почте.

Скачайте наш буклет о фишинге

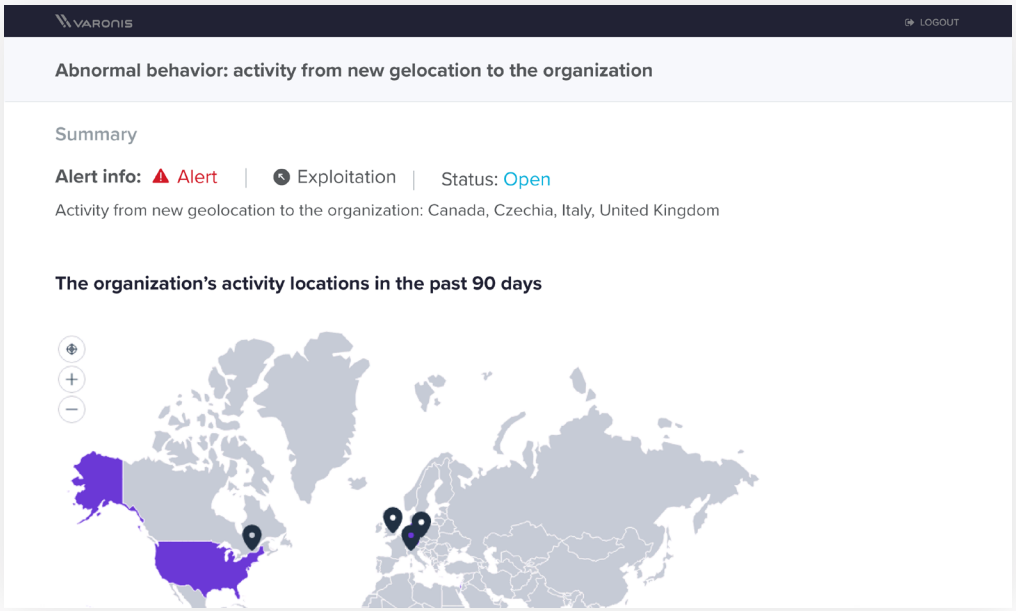
VARONIS

3 Атака через посредника (Man-in-the-Middle)

С ростом количества людей, работающих из дома, продукты, предназначенные для совместной работы и повышения продуктивности, стали использоваться намного чаще. Многие пользователи получают доступ к этим приложениям впервые. Хакеры тоже могут получить доступ к этим приложениям, создавая **поддельные веб-страницы** и обманом заставляя пользователей вводить там свои учетные данные. Даже наличие многофакторной аутентификации не гарантирует защиту от этих уловок. Узнав логин и пароль пользователя, злоумышленник может получить доступ к настоящему приложению.

Чем может помочь Varonis

В приведенной ниже записи аналитики Varonis наглядно демонстрируют, как злоумышленники осуществляют свои атаки. Затем наши специалисты изучают оповещения, срабатывающие на платформе Varonis, на каждом этапе атаки: начиная с первого посещения поддельной страницы и попытки хакером войти с нестандартного местоположения, и заканчивая активностью после вторжения.



Посмотрите применение «атаки через посредника» для пользователя Office 365 с активированной многофакторной аутентификацией

4 Вредоносные приложения Azure

Для людей, впервые работающих удаленно, многие приложения и процессы могут быть незнакомыми. Злоумышленники вкладывают вредоносные приложения Azure в свои фишинговые рассылки и просят пользователей предоставить доступ к их данным в Microsoft Teams и Office 365. Как только пользователь сделает это, киберпреступник получает доступ ко всем файлам и почте, доступным этому пользователю.

Чем может помочь Varonis

Varonis может отслеживать запросы приложений Azure на предоставление разрешений и, таким образом, с самого начала обнаруживать признаки атак. Кроме того, Varonis собирает, анализирует и категоризирует все события в Office 365 для каждого элемента. Как только вредоносная программа начинает выдавать себя за легитимного пользователя, отправляя электронные письма и загружая файлы, срабатывают поведенческие модели угроз Varonis, и вы получаете оповещение.

Ознакомьтесь с полным анализом атаки в блоге Varonis

VARONIS

5 Внутренние угрозы

Сейчас, когда большинство сотрудников выполняют работу удаленно, они часто получают доступ к целым массивам конфиденциальной информации и загружают ее на свои личные устройства. И даже если они делают это из благих побуждений, такие действия подвергают организацию значительному риску. Для организации важно понимать, что происходит с ее конфиденциальными данными.

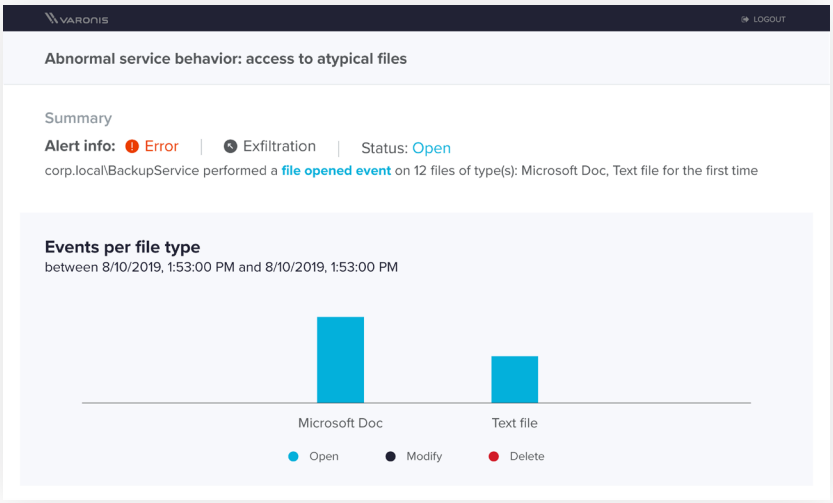
Чем может помочь Varonis

Varonis обнаруживает внутренние угрозы, сначала определяя, где находятся конфиденциальные данные в организации, а затем изучая, как пользователи обычно взаимодействуют с этими данными. Varonis определяет стандартное поведение пользователей при доступе к данным и отслеживает операции с файлами, дополняя эти сведения данными о VPN, DNS и прокси. Varonis определяет, когда пользователи скачивают большие объемы данных или получают доступ к конфиденциальной информации, с которой они обычно не взаимодействуют, а затем предоставляет подробный отчет, к каким файлам обращались пользователи.

Вот пример учетной записи BackupService, к которой имеет законный доступ системный администратор. Инсайдер использовал резервную учетную запись для доступа к конфиденциальной информации и сокрытия следов своей деятельности, что привело к срабатыванию политики поведенческого анализа.

Вот как мы обнаружили угрозу:

- Данная служебная учетная запись **обычно не работает с документами Word** (операция доступа к файлам).
- Доступ к службе BackupService был получен **с личного устройства системного администратора** (Active Directory).
- Затем **служба впервые подключилась к интернету** (веб-прокси).



Эти события в сочетании с аномальным доступом к файлам позволили Varonis достоверно обнаружить внутреннюю угрозу.

Посмотрите наш мастер-класс по реагированию на инциденты

Мы здесь, чтобы помочь

Varonis предлагает перечень бесплатных сервисов и расширенных пробных лицензий, призванных помочь вам в решении проблем и защите от угроз, связанных с удаленной работой ваших сотрудников. Если вам что-нибудь понадобится, **свяжитесь с нами**, и мы сделаем все, что в наших силах, чтобы решить вашу задачу.

Помощь в расследовании и реагировании на инциденты

Призвана помочь вам в расследовании каких-либо подозрительных событий и действий, даже если они не относятся к Varonis.

Безопасность Microsoft Teams и Office 365

Защитите ваши данные в Microsoft Teams и Office 365 от доступа посторонних лиц.

Мониторинг VPN, DNS и веб-прокси

Бесплатные лицензии Edge помогут вам обнаруживать кражу данных, определять людей, использующих RDP нестандартным способом (с Active Directory), и многое другое. Это особенно актуально в условиях, когда все большее количество людей работает удаленно.

Мониторинг Active Directory

Бесплатные лицензии DatAlert помогут вам определить подозрительную активность при авторизации, например, подключение учетной записи администратора к большему количеству устройств, чем обычно.

ЗАПЛАНИРУЙТЕ КОНСУЛЬТАЦИЮ С НАШЕЙ КОМАНДОЙ

О КОМПАНИИ VARONIS

Varonis — разработчик решений по кибербезопасности, основанных на поведенческом анализе пользователей и защите корпоративных данных от внутренних угроз и кибератак.Varonis специализируется на защите корпоративных данных, хранящихся как локально, так и в облаке. Мы защищаем критически важные файлы и электронную почту, персональные данные, финансовую информацию, стратегические планы, а также другие виды интеллектуальной собственности.

Платформа кибербезопасности Varonis обнаруживает внутрисистемные угрозы и кибератаки, анализируя данные, действия учетных записей и поведение пользователей. Платформа предотвращает и ограничивает чрезвычайные ситуации, блокируя критически важные и устаревшие данные, а также эффективно поддерживает безопасность с помощью автоматизации. Varonis ориентируется на защиту данных и решает многие задачи, включая управление, соответствие, классификацию и анализ угроз. Наша компания начала свою деятельность в 2005 году и имеет тысячи клиентов по всему миру, включая отраслевых лидеров в таких направлениях, как технологии, потребительские товары, розничная торговля, финансовые услуги, здравоохранение, производство, энергетика, медиа и образование.