Опубликовано на Швейцария: новости на русском языке (https://nashagazeta.ch)

Не платите выкуп! | Ne payez pas des rançons !

Author: Надежда Сикорская, Берн , 03.11.2025.

Photo © Bermix Studio/Unsplash

Такой совет дали гражданам Швейцарии Федеральная прокуратура (MPC), Федеральное полицейское управление (fedpol) и Федеральное управление по кибербезопасности (OFCS) в совместном коммюнике.

|

Voici le conseil donné aux habitants de la Suisse par le Ministère public de la Confédération (MPC), l'Office fédéral de la police (fedpol) etl'Office fédéral de la cybersécurité (OFCS) dans un communiqué commun.

Ne payez pas des rançons !

Совсем недавно три очень серьезные организации - Федеральная прокуратура (MPC), Федеральное полицейское управление (fedpol) и Федеральное управление по кибербезопасности (OFCS) – опубликовали совместное коммюнике, в котором сообщили о том, что в последние месяцы хакерская группа AKIRA активизировала свою деятельность в Швейцарии. Около 200 предприятий стали жертвами атак с использованием программ-вымогателей. Ущерб в настоящее время составляет несколько миллионов швейцарских франков, а в мировом масштабе – несколько сотен миллионов долларов.

С апреля 2024 года Федеральная прокуратура (MPC) ведет уголовное расследование, которое координируется Федеральным полицейским управлением (fedpol) в тесном сотрудничестве с Федеральным управлением по кибербезопасности (OFCS) и властями нескольких задействованных стран. Это уголовное дело против неизвестных лиц связано с несколькими атаками с использованием программ-вымогателей, совершенными в период с мая 2023 года по сентябрь 2025 года против швейцарских компаний. Эти атаки, ответственность за которые взяла на себя хакерская группировка под названием AKIRA, продолжаются и в последние месяцы стали еще более интенсивными. Власти отметили увеличение числа случаев, связанных с одним и тем же вымогательским ПО (от 4 до 5 в неделю, что является рекордным показателем для Швейцарии), что свидетельствует о высокой активности данной группы.

Федеральная прокуратура приняла на себя несколько кантональных уголовных дел, возбужденных в связи с этим явлением. Расследование в отношении неизвестных лиц по подозрению в хищении данных (ст. 143 УК), повреждении данных (ст. 144bis УК) и вымогательстве (ст. 156 УК), а также по подозрению в покушении на вымогательство (ст. 22 в сочетании со ст. 156 УК).

Группа AKIRA появилась в марте 2023 года и быстро стала предметом нескольких статей в специализированной прессе. Она действует с помощью специальных программ, разработанных специально для этой цели, и располагает международной ИТ-инфраструктурой, распределенной по нескольким странам. Она практикует то, что обычно называется двойным вымогательством, заключающимся в похищении данных жертвы перед их шифрованием. После шифрования данных жертва может только констатировать полную или частичную блокировку своей компьютерной сети, что делает деятельность пострадавшей компании потенциально невозможной. Если выкуп не будет выплачен в установленный срок, AKIRA не только не предоставит ключ дешифрования, позволяющий жертве вновь получить доступ к своим компьютерным данным, но и опубликует их в блоге, размещенном в даркнете. Этот блог называется DLS, что означает «Data Leak Site» (сайт утечки данных). Выкуп оплачивается в криптовалюте, чаще всего в биткойнах.

С учетом информации, собранной на данный момент в рамках текущего расследования, власти предполагают, что существует ряд несообщенных случаев. Это связано с тем, что жертвы этой группы, опасаясь за свою репутацию, платят требуемый выкуп и/или отказываются подавать жалобу. MPC, fedpol и OFCS подчеркивают, что подача жалоб позволяет расширить круг возможных направлений расследования и, следовательно, увеличить шансы на успех в борьбе с этими преступными группами. Власти напоминают, что не следует платить выкуп, поскольку это способствует финансированию деятельности преступников. Поэтому

рекомендуется проконсультироваться с властями, прежде чем предпринимать какие-либо действия в случае требования выкупа в связи с заражением вымогательским ПО.

Хотя эти атаки с использованием программ-вымогателей, как правило, сложны, большинство из них можно предотвратить. Чаще всего входными воротами для таких атак являются не обновленные системы и удаленный доступ, такой как VPN (Virtual Private Network) и RDP (Remote Desktop Protocol), которые не защищены двухфакторной аутентификацией (2FA). Троянские программы, блокирующие данные (программы-вымогатели), могут нанести значительный ущерб, особенно если затронуты ваши резервные копии. В случае такого инцидента сохраняйте спокойствие и действуйте обдуманноВ случае инцидента сначала необходимо заблокировать все интернет-соединения (веб, электронная почта, удаленный доступ и VPN между сайтами), а затем немедленно проверить и защитить резервные копии. Системы также должны быть как можно скорее физически отключены от зараженной сети. Основная цель устранения инцидента — выявить путь заражения и предотвратить новое заражение. Власти рекомендуют во всех случаях подавать заявление в полицию.

При инциденте, связанном с программой-вымогателем, необходимо обратить внимание на следующие моменты:

Ограничение ущерба

Немедленно отключите зараженные системы от сети. Для этого отсоедините сетевой кабель от компьютера и отключите все беспроводные сетевые адаптеры.

Идентификация зараженных систем

Журналы (*logs*), с помощью которых можно, например, отследить доступ к сетевым дискам, могут помочь в идентификации зараженных систем. Метаданные зашифрованных данных также могут дать подсказки о зараженных системах, например, о пользовательских учетных записях, которые создали эти данные. Не забудьте также сохранить журналы.

Обнаружение

Журналы почтовых серверов, прокси-серверов и брандмауэров, а также возможного программного обеспечения безопасности позволяют определить масштабы заражения и обнаружить URL-адреса и IP-адреса злоумышленников. Заблокируйте эти URL-адреса и IP-адреса на внутреннем прокси-сервере или брандмауэре. Таким образом, вы предотвратите подключение к инфраструктуре злоумышленника. В случае заражения по электронной почте некоторые ссылки (URL-адреса и IP-адреса) иногда можно довольно легко прочитать либо непосредственно в электронном письме (гиперссылка), либо в приложении.

Уголовное заявление

Федеральное управление по кибербезопасности рекомендует во всех случаях подавать уголовное заявление. Заранее решите, хотите ли вы это сделать. Компетентным органом является кантональная полиция по месту вашего нахождения. Вы можете найти компетентный полицейский участок на веб-сайте «Suisse e-Police».

Полиция проконсультирует вас по дальнейшим действиям, в частности по вопросам общения с авторами атаки и поведения по отношению к ним. Обсудите целесообразность немедленного вмешательства полиции в качестве поддержки.

Криминалистическая экспертиза

Своевременно примите решение о проведении криминалистической экспертизы. Эта экспертиза важна, особенно если вы намерены подать заявление в полицию. В таком случае заранее проинформируйте об этом органы уголовного преследования и обсудите дальнейшие шаги (изучение вредоносного ПО, контрмеры и т. д.).

Было бы целесообразно, чтобы специализированный сотрудник или поставщик услуг сохранил буферную память и жесткие диски до любой попытки ремонта или перезапуска соответствующих систем, которые делают последующую криминалистическую экспертизу практически невозможной. Если в вашей компании нет необходимых специалистов, следует обратиться к эксперту.

Резервное копирование зашифрованных данных

Если резервные копии также были зашифрованы, рекомендуется сохранить и сделать резервную копию этих зашифрованных данных, чтобы впоследствии их можно было расшифровать, если будет найдено решение. В некоторых случаях органы безопасности и уголовного преследования в ходе своих расследований смогли получить доступ к ключам или найти методы расшифровки.

Переустановка затронутых систем

Перед началом восстановления данных необходимо переустановить зараженные системы. Используемая операционная система должна быть получена с надежного носителя данных.

При определенных условиях можно полностью или частично восстановить данные даже при отсутствии резервных копий. Дешифрование иногда возможно, если:

- вымогательское ПО не зашифровало или не удалило моментальные снимки (*shadow copies*) в Windows;
- существуют моментальные снимки виртуальных машин или предыдущие версии файлов в облачных сервисах;
- возможно криминалистическое восстановление удаленных файлов;
- функция шифрования вымогательского ПО содержит ошибки или известен ключ дешифрования.

Сайт https://www.nomoreransom.org содержит советы по идентификации вредоносного ПО и предлагает возможность загрузить уже известные ключи. Nomoreransom.org — это совместный проект полиции Нидерландов и Европола, в котором также участвует Швейцарская Конфедерация.

Что касается выкупа, который обычно требуют злоумышленники, то компетентные органы советуют его не платить, поясняя, что нет никакой гарантии, что преступники не опубликуют данные или не извлекут из них другую выгоду после уплаты выкупа. Кроме того, любой успешный шантаж побуждает злоумышленников продолжать свои действия, финансирует развитие атак и способствует их распространению. Если вы все же намерены заплатить выкуп, то настоятельно

рекомендуется обсудить эти действия с кантональной полицией.

В прошлый четверг три очень серьезные организации - Федеральная прокуратура (MPC), Федеральное полицейское управление (fedpol) и Федеральное управление по кибербезопасности (OFCS) – опубликовали совместное коммюнике, в котором сообщили о том, что в последние месяцы хакерская группа AKIRA активизировала свою деятельность в Швейцарии. Около 200 предприятий стали жертвами атак с использованием программ-вымогателей. Ущерб в настоящее время составляет несколько миллионов швейцарских франков, а в мировом масштабе – несколько сотен миллионов долларов.

С апреля 2024 года Федеральная прокуратура (MPC) ведет уголовное расследование, которое координируется Федеральным полицейским управлением (fedpol) в тесном сотрудничестве с Федеральным управлением по кибербезопасности (OFCS) и властями нескольких задействованных стран. Это уголовное дело против неизвестных лиц связано с несколькими атаками с использованием программ-вымогателей, совершенными в период с мая 2023 года по сентябрь 2025 года против швейцарских компаний. Эти атаки, ответственность за которые взяла на себя хакерская группировка под названием AKIRA, продолжаются и в последние месяцы стали еще более интенсивными. Власти отметили увеличение числа случаев, связанных с одним и тем же вымогательским ПО (от 4 до 5 в неделю, что является рекордным показателем для Швейцарии), что свидетельствует о высокой активности данной группы.

Федеральная прокуратура приняла на себя несколько кантональных уголовных дел, возбужденных в связи с этим явлением. Расследование в отношении неизвестных лиц по подозрению в хищении данных (ст. 143 УК), повреждении данных (ст. 144bis УК) и вымогательстве (ст. 156 УК), а также по подозрению в покушении на вымогательство (ст. 22 в сочетании со ст. 156 УК).

Группа AKIRA появилась в марте 2023 года и быстро стала предметом нескольких статей в специализированной прессе. Она действует с помощью специальных программ, разработанных специально для этой цели, и располагает международной ИТ-инфраструктурой, распределенной по нескольким странам. Она практикует то, что обычно называется двойным вымогательством, заключающимся в похищении данных жертвы перед их шифрованием. После шифрования данных жертва может только констатировать полную или частичную блокировку своей компьютерной сети, что делает деятельность пострадавшей компании потенциально невозможной. Если выкуп не будет выплачен в установленный срок, AKIRA не только не предоставит ключ дешифрования, позволяющий жертве вновь получить доступ к своим компьютерным данным, но и опубликует их в блоге, размещенном в даркнете. Этот блог называется DLS, что означает «Data Leak Site» (сайт утечки данных). Выкуп оплачивается в криптовалюте, чаще всего в биткойнах.

С учетом информации, собранной на данный момент в рамках текущего расследования, власти предполагают, что существует ряд несообщенных случаев. Это связано с тем, что жертвы этой группы, опасаясь за свою репутацию, платят требуемый выкуп и/или отказываются подавать жалобу. MPC, fedpol и OFCS подчеркивают, что подача жалоб позволяет расширить круг возможных направлений расследования и, следовательно, увеличить шансы на успех в борьбе с этими преступными группами. Власти напоминают, что не следует платить выкуп, поскольку это способствует финансированию деятельности преступников. Поэтому

рекомендуется проконсультироваться с властями, прежде чем предпринимать какие-либо действия в случае требования выкупа в связи с заражением вымогательским ПО.

Хотя эти атаки с использованием программ-вымогателей, как правило, сложны, большинство из них можно предотвратить. Чаще всего входными воротами для таких атак являются не обновленные системы и удаленный доступ, такой как VPN (Virtual Private Network) и RDP (Remote Desktop Protocol), которые не защищены двухфакторной аутентификацией (2FA). Троянские программы, блокирующие данные (программы-вымогатели), могут нанести значительный ущерб, особенно если затронуты ваши резервные копии. В случае такого инцидента сохраняйте спокойствие и действуйте обдуманноВ случае инцидента сначала необходимо заблокировать все интернет-соединения (веб, электронная почта, удаленный доступ и VPN между сайтами), а затем немедленно проверить и защитить резервные копии. Системы также должны быть как можно скорее физически отключены от зараженной сети. Основная цель устранения инцидента — выявить путь заражения и предотвратить новое заражение. Власти рекомендуют во всех случаях подавать заявление в полицию

При инциденте, связанном с программой-вымогателем, необходимо обратить внимание на следующие моменты:

Ограничение ущерба

Немедленно отключите зараженные системы от сети. Для этого отсоедините сетевой кабель от компьютера и отключите все беспроводные сетевые адаптеры.

Идентификация зараженных систем

Журналы (*logs*), с помощью которых можно, например, отследить доступ к сетевым дискам, могут помочь в идентификации зараженных систем. Метаданные зашифрованных данных также могут дать подсказки о зараженных системах, например, о пользовательских учетных записях, которые создали эти данные. Не забудьте также сохранить журналы.

Обнаружение

Журналы почтовых серверов, прокси-серверов и брандмауэров, а также возможного программного обеспечения безопасности позволяют определить масштабы заражения и обнаружить URL-адреса и IP-адреса злоумышленников. Заблокируйте эти URL-адреса и IP-адреса на внутреннем прокси-сервере или брандмауэре. Таким образом, вы предотвратите подключение к инфраструктуре злоумышленника. В случае заражения по электронной почте некоторые ссылки (URL-адреса и IP-адреса) иногда можно довольно легко прочитать либо непосредственно в электронном письме (гиперссылка), либо в приложении.

Уголовное заявление

Федеральное управление по кибербезопасности рекомендует во всех случаях подавать уголовное заявление. Заранее решите, хотите ли вы это сделать. Компетентным органом является кантональная полиция по месту вашего нахождения. Вы можете найти компетентный полицейский участок на веб-сайте «Suisse e-Police».

Полиция проконсультирует вас по дальнейшим действиям, в частности по вопросам общения с авторами атаки и поведения по отношению к ним. Обсудите целесообразность немедленного вмешательства полиции в качестве поддержки.

Криминалистическая экспертиза

Своевременно примите решение о проведении криминалистической экспертизы. Эта экспертиза важна, особенно если вы намерены подать заявление в полицию. В таком случае заранее проинформируйте об этом органы уголовного преследования и обсудите дальнейшие шаги (изучение вредоносного ПО, контрмеры и т. д.).

Было бы целесообразно, чтобы специализированный сотрудник или поставщик услуг сохранил буферную память и жесткие диски до любой попытки ремонта или перезапуска соответствующих систем, которые делают последующую криминалистическую экспертизу практически невозможной. Если в вашей компании нет необходимых специалистов, следует обратиться к эксперту.

Резервное копирование зашифрованных данных

Если резервные копии также были зашифрованы, рекомендуется сохранить и сделать резервную копию этих зашифрованных данных, чтобы впоследствии их можно было расшифровать, если будет найдено решение. В некоторых случаях органы безопасности и уголовного преследования в ходе своих расследований смогли получить доступ к ключам или найти методы расшифровки.

Переустановка затронутых систем

Перед началом восстановления данных необходимо переустановить зараженные системы. Используемая операционная система должна быть получена с надежного носителя данных.

При определенных условиях можно полностью или частично восстановить данные даже при отсутствии резервных копий. Дешифрование иногда возможно, если:

- вымогательское ПО не зашифровало или не удалило моментальные снимки (*shadow copies*) в Windows;
- существуют моментальные снимки виртуальных машин или предыдущие версии файлов в облачных сервисах;
- возможно криминалистическое восстановление удаленных файлов;
- функция шифрования вымогательского ПО содержит ошибки или известен ключ дешифрования.

Сайт https://www.nomoreransom.org содержит советы по идентификации вредоносного ПО и предлагает возможность загрузить уже известные ключи. Nomoreransom.org — это совместный проект полиции Нидерландов и Европола, в котором также участвует Швейцарская Конфедерация.

Что касается выкупа, который обычно требуют злоумышленники, то компетентные органы советуют его не платить, поясняя, что нет никакой гарантии, что преступники не опубликуют данные или не извлекут из них другую выгоду после уплаты выкупа. Кроме того, любой успешный шантаж побуждает злоумышленников продолжать свои действия, финансирует развитие атак и способствует их распространению. Если вы все же намерены заплатить выкуп, то настоятельно

рекомендуется обсудить эти действия с кантональной полицией.

PS. И еще одна новость в тему, не такая масштабная, но все же крайне неприятная, если она коснется кого-то из нас. Мы уже рассказывали об уловках мошенников, «работающих» со швейцарской системой мгновенных платежей Twint. Увы, они не стоят на месте. Новый метод вымогательства, о котором предупреждает Федеральное ведомство по кибербезопасности, нацелен на пользователей Twint, еще толком не проснувшихся: запросы на деньги, замаскированные под возврат средств, с самого утра.

Происходит это так. Ранним утром – динь! Это уведомление от Twint: «Вот деньги, которые я тебе должен». Человек вспоминает: накануне он выходил с друзьями, каждый платил за свой заказ. Ничего удивительного, думает он, что ему возвращают часть денег. Спросонья он нажимает на кнопку. И … с его счета списываются деньги.

В большинстве случаев эти мошенничества касаются небольших сумм, часто менее 100 франков, типичных для друзей. OFCS уже давно следит за различными попытками мошенничества, связанными с Twint и напоминает о нескольких простых правилах, которые помогут защитить себя. Во-первых, получение платежа через Twint происходит автоматически, без необходимости что-то нажимать или подтверждать. Во-вторых, всегда внимательно проверяйте запросы на оплату – сумму, получателя и характер транзакции.

кибербезопасность Швейцарии
киберпреступность в швейцарии

Надежда Сикорская
Nadia Sikorsky
Rédactrice, NashaGazeta.ch

Статьи по теме
Швейцарская атака на «хакеров»
Швейцария под прицелом хакеров
Швейцария экстрадировала в США российского хакера, которому грозят 142 года тюрьмы
Швейцарская разведка к кибератаке готова?
Кибератака затронула федеральные учреждения Швейцарии
