1. Вирусные аналитики сообщают об обнаружении новой угрозы для NAS-устройств. Выявлены несколько случаев поражения сетевых хранилищ вредоносным вирусом-вымогателем.

Уязвимы перед новой угрозой любые сетевые устройства хранения, работающие на базе Linux. Вирус проникает на NAS-устройства под видом сервисного обновления, устанавливая себя в корень сетевого диска и, шифруя всю находящуюся на нём информацию. Несколько десятков, пострадавших от атак, пользователей сообщили, что на заражённом устройстве доступным остаётся только один текстовый документ с требованием выкупа. Пользователям предлагается получить ключ для расшифровки данных в обмен на сумму в 1 биткоин, перечисленную на счёт, указанный в текстовом документе. В действительности, пользователи не получают доступ к данным в хранилище даже после перечисления указанной суммы. В вирус встроен алгоритм самоуничтожения через заданное время, вследствие чего вредоносный файл удаляет себя и всю информацию на хранилище.

Экспертам удалось понять принцип проникновения вируса на сетевые хранилища. Как было упомянуто выше, шифровальщик попадает на сетевое устройство, подменяя DNS-адрес сервера на адрес официального канала обновлений, таким образом заставляя устройство думать, что обновление поступило из официального источника. После проникновения в хранилище, вирус пытается получить пароль администратора, запуская кейлоггер. В случае неудачи, он начинает шифровать имеющиеся данные и требовать выкуп.

Вымогатель заточен под устройства, работающие под операционной системой Linux, однако, не стоит забывать об осторожности, даже если вы пользуетесь иной ОС. Самый простой и надёжный способ обезопасить себя от подобных атак – изолировать сетевое устройство от всемирной паутины. Также рекомендуется отключить любые автоматические обновления и, при необходимости, устанавливать их только вручную, предварительно проверяя пакет установки на вирусы.

2. Вопросы вирусному аналитику:

- Каким образом троянец похищает пароли?
- Как проникает?
- Защищает ли соединение по HTTPS?
- Как выявить факт проникновения? Как проверить?
- Как обезопасить себя от угрозы?

3. Краткая аннотация на английском.

A new threat detected for NAS-devices. Analytics report.

Several network storage customers have been affected by a new ransomware virus.

Vulnerability found in Linux-based systems of network storage devices allows hackers to get access to information stored inside. Reportedly, more than twenty users have been affected by this attack. The virus masks itself as a service update for a NAS-device, that is installed into the root of the storage and attempts to launch a keylogger in order to receive the administrator password. Simultaneously with those attempts, the virus begins encoding all the information located on the network drive. The user is left with access to only a .txt file containing a ransom demand in the amount of 1 bitcoin. The virus also contains a self-destruct algorithm that erases itself and all the stored data.