Рекомендации по очистке компьютеров от вредоносных программ Windigo

Linux/Ebury

В ходе анализа зараженных систем было установлено, что для установки Linux/Ebury в систему атакующие использовали похищенные данные учетных записей с правами root в системе. Получив такие права, они без труда внедряли в систему вредоносный код. Антивирусное решение ESET NOD32 для Linux Desktop сможет обнаружить и удалить файлы вредоносной программы в системе, но на самом деле ситуация сложнее. Поскольку атакующие получали максимальные права в системе, могли установить бэкдор и модифицировать любые другие настройки ОС, а также загружать туда новые потенциально неизвестные вредоносные программы, мы рекомендуем полностью переустановить операционную систему и, если это возможно, удалить данные на дисках путем их форматирования. Также мы рекомендуем сменить аутентификационные данные учетных записей и никогда не использовать для них те пароли, которые применялись на момент обнаружения вредоносного кода в системе. Переустанавливать ОС и дистрибутивы ПО рекомендуется только из надежных и проверенных источников. Последнее особенно важно, поскольку, кроме кражи учетных данных, злоумышленники распространяли модули вредоносных программ через модифицированные легитимные бинарные дистрибутивы (напр., SSH).

Упомянутый вредоносный код способен красть аутентификационные данные не только зараженного сервера, но и тех компьютеров, на которые с этого сервера производится подключение (через SSH). Таким образом, злоумышленники расширяли свой список потенциальных жертв для дальнейшей компрометации. Ввиду этого факта мы также рекомендуем уведомить пользователей (клиентов SSH) о необходимости проверки компьютера на предмет вредоносного кода Windigo и сменить аутентификационные данные учетных записей этих компьютеров.

Linux/Cdorked

Рекомендации схожи с теми, которые даны для Linux/Ebury, и сводятся к полной переустановке ОС на скомпрометированном сервере из доверенного источника.

Linux/Onimiki

Рекомендации такие же, как и в случае с Linux/Ebury и Linux/Cdorked. Если нет возможности переустановить зараженный сервер, следующие шаги помогут минимально очистить систему:

- Убедитесь, что пользователь «named» не имеет доступа к shell (через /etc/passwd).

- Переустановите бинарный файл «named» (обычно находится в /usr/sbin/named) через ваш package manager.
- Перезапустите демон «named».

Perl/Calfbot

Рекомендуется полная переустановка ОС сервера дистрибутивом из доверенного источника. Если нет возможности переустановить зараженный сервер, следующие шаги помогут минимально очистить систему:

- Воспользуйтесь списком индикаторов компрометации системы Perl/Calfbot (IOC) для получения информации о том, какие user id и process id используются этим вредоносным кодом.
- Смените аутентификационные данные учетной записи (user id), под которой запущен процесс Perl/Calbot.
- Завершите процесс интерпретатора Perl (process id), который отвечает за исполнение вредоносных скриптов Perl/Calfbot.

Список индикаторов компрометации системы вышеупомянутыми вредоносными программами можно найти в нашем детальном отчете, посвященном операции Windigo.