Рекомендации по предотвращению или нивелированию целевой атаки на сеть ViPNet

1. Для предотвращения или нивелирования атаки на сеть ViPNet необходимо обновить ПК ViPNet Client 4 до версий:
   - 4.5.3 (сборка 65211) и выше;
   - 4.5.5 (сборка 24749) и выше

   только на узлах с установленным управляющим ПО (ViPNet Administrator или ViPNet Policy Manager). **Обратите внимание!** Что потребителю в сети ViPNet необходимо установить доработанные версии ПК ViPNet Client 4 точечно только на 1-2 узлах сети с установленным управляющим ПО.

2. Обновление на всех узлах сети ПК ViPNet Client версии 4.5.* не требуется. На остальных узлах ViPNet сети необходимо только убедиться, что не эксплуатируется ПК ViPNet Client ниже версий 4.5.3.65160 (сертифицированная) и 4.5.5.23984 (официальная) – предыдущие версии ViPNet Client от 2025г. не подвержены новому вектору целевой атаки без предварительной компрометации узла с управляющим ПО.

3. Для ПАК ViPNet 4 поколения, если на них установлены актуальные прошивки (от 2025 г.), не требуются дополнительные меры для нивелирования уязвимости, помимо установки и доработанного обновления ViPNet Client версии 4.5 на хост с управляющим ПО и дальнейшего обновления доработанных прошивок ПАК 4 поколения (ViPNet Coordinator HW 4, ViPNet Coordinator IG 4, ViPNet xFirewall 5 и ViPNet xFirewall xF65000).
   Продолжение многоэтапной целевой атаки, используя новый вектор атаки без предварительной компрометации узла с управляющим ПО, невозможно.

4. Если новый вектор атаки был проэксплуатирован, и компрометация узла с установленным управляющим ПО подтверждена, рекомендуется проведение смены мастер-ключей.

Так же, обращаем ваше внимание, что необходимо использовать только рекомендации компании «ИнфоТеКС» как производителя:

- по применению компенсирующим мер;
- мер для устранения инцидента, если такой случился.

Не используйте непроверенные и не подтвержденные производителем рекомендации, предоставляемые сторонними организациями. Выполнение некорректных рекомендаций может привести к потере управления ViPNet сетью! При этом данные действия не требуются для нивелирования возможного или случившегося инцидента.

Системные рекомендации повышения безопасности ViPNet-сети

Помимо установки доработанных обновлений продуктов ViPNet в соответствии с вышеприведенными рекомендациями, так же следует придерживаться следующих рекомендаций:

1. Выявление компрометации сети:

Если ваша сеть связана с другими защищенными сетями, за администрирование которых Вы не отвечаете и не можете гарантировать выполнение по отношению к ним вышеуказанных требований, следует убедиться в отсутствии признаков заражения на узлах своей сети, используя YARA-правила в соответствии с инструкцией их применения.

Для выявления дополнительных признаков компрометации следует выполнять меры противодействия угрозе, приведенные в бюллетене информационной безопасности, выпущенного АО «Перспективный мониторинг».
При наличии указанных признаков, а также при обнаружении подозрительной сетевой активности с узлов ViPNet на Координаторы и другие элементы инфраструктуры организации, **незамедлительно обращайтесь в службу технического сопровождения ИнфоТеКС**.

2. Выполнение правил пользования:

Необходимо убедиться в выполнении требований эксплуатационной документации и правил пользования продуктов ViPNet на всех узлах защищенной сети ViPNet. Отдельно необходимо обратить внимание:

- на актуальность версий установленных продуктов ViPNet;
- на отсутствие полномочий администратора у пользователей, работающих на узлах сети ViPNet;
- особенно на отсутствие полномочий администратора у пользователей, работающих на узлах сети ViPNet с установленным управляющим ПО;
- на выполнении правил пользования управляющим ПО ViPNet;
- на наличие свежих обновлений установленного антивирусного ПО;

3. Конфигурирование мониторинга сети:

Для повышения системной безопасности защищенной сети рекомендуется настроить постоянный мониторинг указанных далее направлений. Результаты мониторинга необходимо оперативно отслеживать, выстроив для этого в организации систему реагирования.

Рекомендуемые направления для мониторинга хостов с установленным управляющим ПО ViPNet:

1. Настроить мониторинг целостности среды исполнения и оперативно отслеживать результаты контроля его целостности.
2. Настроить мониторинг подключений администраторов хоста. Отдельно необходимо мониторить удаленные подключения, обращая особое внимание на удаленные подключения пользователей с правами администратора.
3. Настроить расширенную телеметрию хостов, для ОС Windows для этого можно использовать встроенные средства – ETW, SACL и Sysmon для получения максимально подробного аудита системы. Рекомендуется настраивать циклический режим записи с фиксированным размером файла, чтобы трассировка не переполнила диск, и запускать сессии с флагом автозапуска при старте системы.

   В конфигурации Sysmon необходимо отслеживать создание процессов из каталога установки ViPNet Client - по умолчанию для ViPNet Client 4 это «C:\Program Files (x86)\InfoTeCS\ViPNet Client» или «C:\Program Files\InfoTeCS\ViPNet Client», а так же из рабочих директорий «C:\ProgramData\InfoTeCS» и «C:\Program Files\Common Files\InfoTeCS». Так же рекомендуется включить мониторинг сетевых соединений от процессов ViPNet Client.

   Для обогащения телеметрии Sysmon так же следует сконфигурировать SACL. В нем необходимо указать условия, при которых будут генерироваться события безопасности. Перед наложением SACL необходимо сначала включить глобальный аудит объектов в категории «File System» и «Registry». Для директорий установки и работы ViPNet Client, ключей реестра

«HKLM\SOFTWARE\WOW6432Node\InfoTeCS» и «HKLM\SOFTWARE\InfoTeCS» необходимо добавить аудит на чтение, запись и удаление.

Для ETW включите провайдер «Kernel-Process» для контроля цепочки запуска процессов, «Threat-Intelligence» для мониторинга чтения памяти процессов и «Kernel-Registry» для аудита любых операций с реестром.