Задание

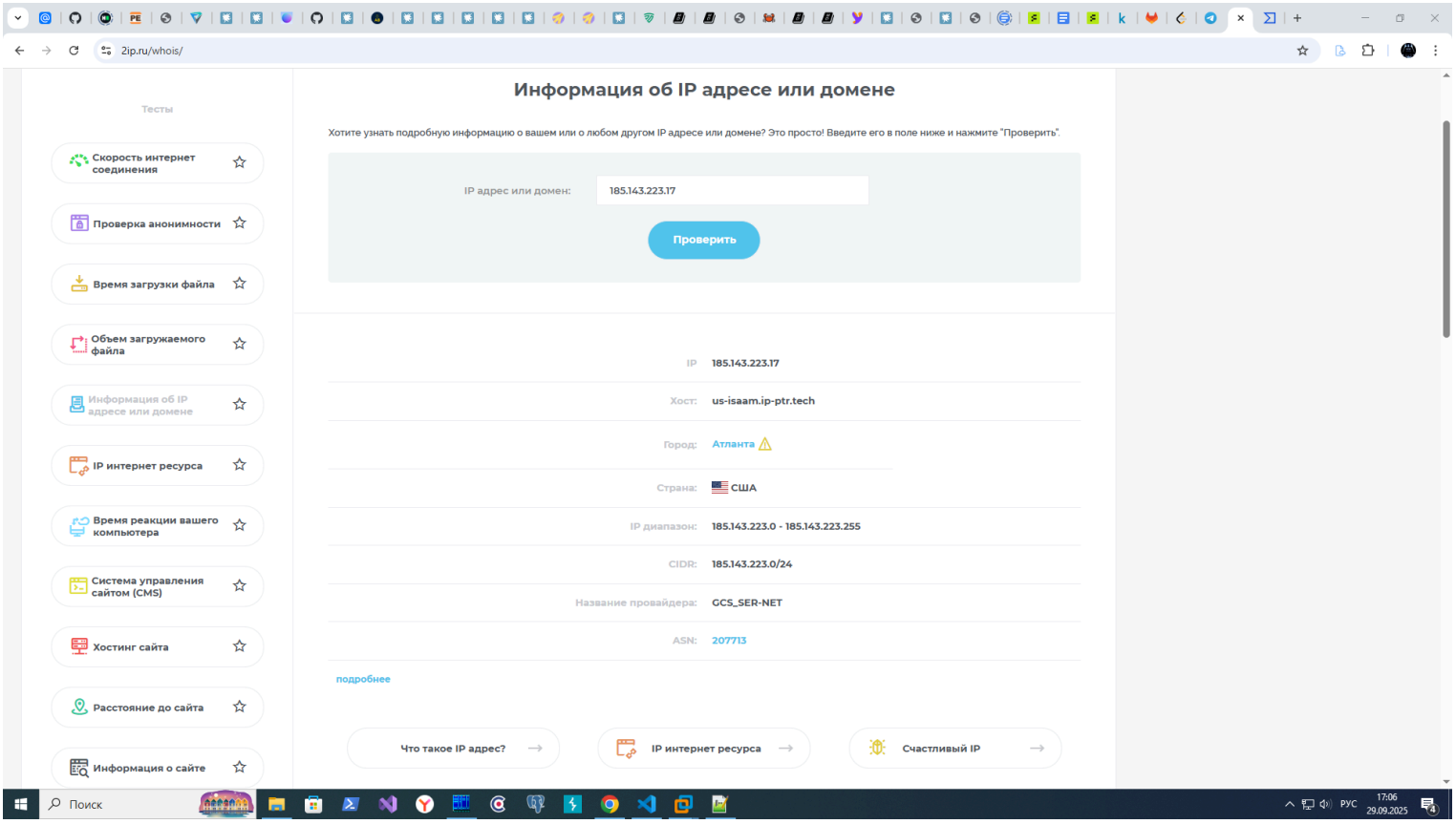
Фабула. Команда SOC обнаружила подозрительную активность в сети компании:

- Резкий рост исходящего трафика (2 ГБ за 5 минут) с рабочей станции бухгалтера.
- Попытки соединения с внешним IP (185.143.223.17) через порт 443

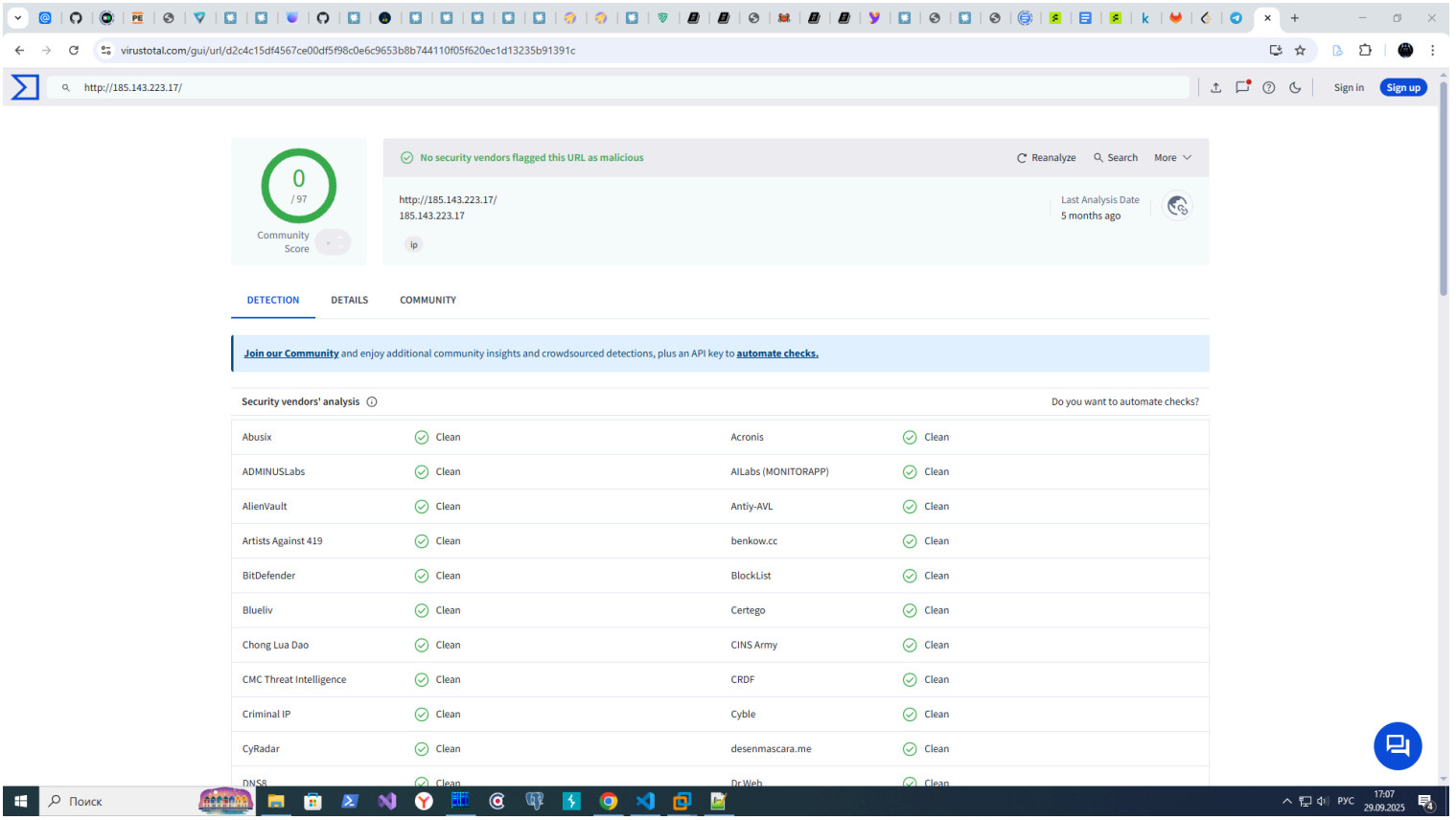
Гипотезы

Прежде, чем выдвигать гипотезы, я сделаю пару небольших проверок.

1. Получаю информацию о внешнем IP адресе - видно, что данный IP адрес выдан устройству на территории США и не принадлежит известному (публичному) сервису:



2. Проверяю внешний IP адрес на VirusTotal - информации об известной вредоносной активности с этого внешнего IP адреса нет.



Ключевые детали:

1. Резкий рост исходящего трафика (2 ГБ за 5 минут) с рабочей станции бухгалтера означает, что некий процесс передает какую-то достаточно большую информацию с рабочей станции бухгалтера на удаленный компьютер.
2. Попытки соединения с внешним IP (185.143.223.17) через порт 443. Порт 443 - это порт по умолчанию для HTTPS. Так как в современном мире подавляющее число web ресурсов использует по умолчанию HTTPS, то можно предположить, что соединения скорее всего осуществлялись либо с некоторым web-сайтом, либо с некоторым REST API сервисом.
3. У нас нет информации о том, на какой IP адрес (адреса) происходит передача данных.
4. У нас нет информации о том, были ли попытки соединения с внешним IP (185.143.223.17) через порт 443 успешными или нет.
5. У нас вообще нет информации о том связаны ли эти два события между собой или нет? Были ли попытки соединения с внешним IP (185.143.223.17) через порт 443 осуществлены с рабочей станции бухгалтера или нет.

Попробуем выдвинуть несколько гипотез:

1. С рабочей станции бухгалтера происходила некоторая активность, связанная с работой.
2. С рабочей станции бухгалтера происходила некоторая активность, не связанная с работой, но и не связанная с передачей каких-либо конфиденциальных данных (например, с рабочей станции бухгалтера происходила загрузка архива личных фотографий на некоторый файлообменник).

3. С рабочей станцией бухгалтера происходила передача конфиденциальной информации, либо с помощью инсайдера (внутреннего нарушителя), либо с применением вредоносного ПО (внешнего нарушителя).
4. Попытки соединения с внешним IP (185.143.223.17) через порт 443 осуществлялись для некоторой, не связанной с работой активностью без передачи конфиденциальной информации.
5. Попытки соединения с внешним IP (185.143.223.17) через порт 443 являются некоторой зловредной активностью - например, это попытки соединения вредоносного ПО с C2 сервером.

Способы проверки гипотез:
1. Проверить логи, связанные с установлением сетевых подключений и выяснить адрес назначения исходящего трафика; проверить на рабочей станции бухгалтера, какие данные передавались; опросить бухгалтера и/или его начальника на предмет активности перед и во время возникновения большого исходящего трафика. Это даст нам понимание, что исходящий трафик связан с рабочей активностью.
2. Проверить логи, связанные с установлением сетевых подключений и выяснить адрес назначения исходящего трафика; проверить на рабочей станции бухгалтера, какие данные передавались; проверить логи DLP системы; опросить бухгалтера на предмет активности перед и во время возникновения большого исходящего трафика. Это даст нам понимание, что исходящий трафик хоть и не связан с рабочей активностью, но не приводит к передаче каких-либо конфиденциальных данных.
3. Проверить логи, связанные с установлением сетевых подключений и выяснить адрес назначения исходящего трафика; проверить на рабочей станции бухгалтера, какие данные передавались; проверить логи DLP системы; проверить рабочую станцию бухгалтера на наличие вредоносного ПО; снять образы памяти и диска. Это даст нам понимание того, что произошла утечка конфиденциальной информации. Анализ памяти и диска поможет установить нам вектор атаки: была ли атака инициирована с помощью внутреннего нарушителя (с помощью инсайдера) или же с помощью одной из техник внешнего нарушителя (фишинг и т.п.).
4. Проверить логи, связанные с установлением сетевых подключений и выяснить с какой рабочей станции осуществлялись попытки соединения с внешним IP (185.143.223.17) через порт 443; собрать больше информации о ресурсе с этим внешним IP (185.143.223.17); проверить (в случае наличия успешных попыток соединения) на рабочей станции, с которой осуществлялись попытки соединения, что происходило после установления соединения (как происходило взаимодействие с этим внешним ресурсом); проверить логи DLP системы; опросить владельца (работника) этой рабочей станции на предмет его не рабочей активности. Это даст нам понимание, для чего осуществлялась данная активность с внешним ресурсом - что она хоть и не связана с работой, но не привела к передачи конфиденциальных данных и/или заражению рабочей станции вредоносным ПО.
5. Проверить логи, связанные с установлением сетевых подключений и выяснить с какой рабочей станции осуществлялись попытки соединения с внешним IP (185.143.223.17) через порт 443; собрать больше информации о ресурсе с этим внешним IP (185.143.223.17); снять и проанализировать образы памяти и диска, чтобы понимать, каким процессом и пользователем осуществлялись попытки соединения с внешним ресурсом, как происходило взаимодействие с этим внешним ресурсом и какие данные были переданы (в случае, если попытуи соединения были успешны),

какие действия в системе происходили до попыток соединения. Это все даст нам понимание, что попытки соединения являются частью некоторой зловредной активности, а также позволят определить изначальный вектор атаки: была ли атака инициирована с помощью внутреннего нарушителя (с помощью инсайдера) или же с помощью одной из техник внешнего нарушителя (фишинг и т.п.).

Задание

Фабула. В сети обнаружено неизвестное устройство:

- В системе контроля доступа появилось неизвестное устройство с MAC-адресом 00:1A:3F:4B:66:6D

Устройство подключилось к Wi-Fi и пытается сканировать сетевые папки.

Гипотезы

Ключевые детали:
1. В сети появилось неизвестное устройство, которое подключилось к сети через Wi-Fi.
2. На данном устройстве запущено некоторое ПО (не обязательно вредоносное - это может быть, например, тот же nmap), которое сканирует сетевые папки.
3. Мы не знаем, через конкретно какую точку доступа подключилось данное неизвестное устройство и к какой именно сети подключилось (к гостевой или нет)?
4. Мы также не знаем, была ли зафиксирована какая-либо еще активность с данного устройства.

Попробуем выдвинуть несколько гипотез:
1. Данное устройство было использовано отделом ИБ для тестирования существующей инфраструктуры на возможность проникновения.
2. Данное устройство было подключено кем то из системных администраторов для выполнения своих обязанностей, но информацию о нем не успели/забыли внести в систему контроля доступом. Сканирование сетевых папок - это одна из рабочих активностей (например, в целях проведения инвентаризации) сотрудника, которому принадлежит устройство.
3. Данное устройство является личным устройством одного из сотрудников, которое он принес и подключил к корпоративной сети для совершения некоторых противоправных действий (внутренний нарушитель). Попытка сканирования сетевых папок - это как раз начало таких противоправных действий (разведка).
4. Данное устройство принадлежит лицу, не являющемуся сотрудником (внешний нарушитель), которое подключилось либо к гостевой Wi-Fi сети (если у ней нет пароля или есть известный пароль), либо к основной Wi-Fi сети (с помощью подбора/взлома пароля) для совершения некоторых противоправных действий. Попытка сканирования сетевых папок - это как раз начало таких противоправных действий (разведка).

Способы проверки гипотез:
1. Обратиться в отдел ИБ по поводу проведения ими тестирования существующей инфраструктуры на возможность проникновения. Это даст нам понимание, что данная активность в сети является законной и по этому поводу не следует беспокоиться.
2. Обратиться в отдел ИТ (к системным администраторам) с вопросом о подключении ими нового устройства. Это даст нам понимание, что появление нового устройства в Wi-Fi сети и его активность являются законными.
3. Локализовать точку подключения неизвестного устройства и попытаться найти его физически. В случае удачи - снять с него снять образы памяти и диска. В случае неудачи - заблокировать его, а также запретить возможность подключения к не гостевой сети Wi-Fi неизвестных устройств. Это даст нам возможность в лучшем

случае информацию о намерениях и используемых средствах, а в худшем случае - устройство, с которого начинается потенциальная атака будет заблокировано.
4. Локализовать точку подключения неизвестного устройства и попытаться найти его физически. В случае удачи будет известна личность атакующего (внешнего нарушителя) - эту информацию можно будет передать правоохранительным органам. В случае неудачи - заблокировать его. Также, если злоумышленник подключался к основной Wi-Fi сети (с помощью подбора/взлома пароля), то необходимо запретить возможность подключения к не гостевой сети Wi-Fi неизвестных устройств, а также поменять пароль на подключение на более стойкий (т.к. существующий пароль уже не надежен). Это даст нам в лучшем случае информацию о злоумышленнике (например, его фотографию), а в худшем случае - устройство, с которого начинается потенциальная атака будет заблокировано.