

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:

The screenshot shows a web browser window with the URL 2ip.ru/whois/. The page title is "Информация об IP адресе или домене". Below the title, there is a text input field containing "185.143.223.17" and a blue button labeled "Проверить". Below the input field, the following information is displayed:

IP	185.143.223.17
Хост	us-isaam.ip-ptr.tech
Город	Атланта ⚠
Страна	🇺🇸 США
IP диапазон	185.143.223.0 - 185.143.223.255
CIDR	185.143.223.0/24
Название провайдера	GCS_SER-NET
ASN	207713

Below the table, there is a link "подробнее". At the bottom of the page, there are three buttons: "Что такое IP адрес?", "IP интернет ресурса", and "Счастливым IP".

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

0 / 97
Community Score

No security vendors flagged this URL as malicious

http://185.143.223.17/
185.143.223.17

Last Analysis Date
5 months ago

DETECTION DETAILS COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Abusix	Clean	Acronis	Clean
ADMINUSLabs	Clean	AILabs (MONITORAPP)	Clean
AlienVault	Clean	Antiy-AVL	Clean
Artists Against 419	Clean	benkow.cc	Clean
BitDefender	Clean	BlockList	Clean
Blueliv	Clean	Certego	Clean
Chong Lua Dao	Clean	CINS Army	Clean
CMC Threat Intelligence	Clean	CRDF	Clean
Criminal IP	Clean	Cyble	Clean
CyRadar	Clean	desenmascara.me	Clean
DNS	Clean	DrWeb	Clean

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 попытки 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.).