1.   Рассказать что произошло ПК :

a.   Версия ОС - Win7SP1x64

b.   Какие пользователи есть в системе? - default, Администратор, Иванова, Общие, Романов

c.   Подключались ли какие-то устройства? - сканер, принтер, Net Card

d.   Какой пользователь получил файл и по какому каналу? -

e.   Как он его получил ? -

f.   Какой файл -

g.   Что за ВПО -

h.   Построить таймлайн файловой системы –

Операционная система исследуемого дампа Win7SP1x64. Файловая сисмема содержит пользователей: default, Администратор, Иванова, Общие, Романов.

Подключались устройства: USB Transcend, сканер, принтер, Net Card. Информация получена с помощью инструментария volatility 2.6 применялись плагины: imageinfo, pstree, hashdump, dlllist, hivelist, netscan. Пользователь Романов получил файл .exe архив название scan.pdf.exe фишинговое письмо с attachment в почтовый клиент Outlook на адрес [semen.romanov.1982@mail.ru](mailto:semen.romanov.1982@mail.ru). Контактируемые ip адреса 35.220.198.248, 93.184.221.240.

Начнем исследование с файла реестра **NTUSER.DAT** из каталога пользователя С:\Users\user\Романов**\NTUSER.DAT. Извлечем из него данные при помощи Autopsy 4.18.0. В** данном случае важно получить номер записи определенного файла.

exe файл 1С запускается из временной паки “Temp”, а также “AppData” скрыта от пользователей и рядом библиотека ntdll.dll вызывает подозрение.

1cv7s.exe pid: 2936

Command line : C:\Users\B5DA~1\AppData\Local\Temp\1C\1cv7s.exe

Note: use ldrmodules for listing DLLs in Wow64 processes

Base Size LoadCount Path

------------------ ------------------ ------------------ ----

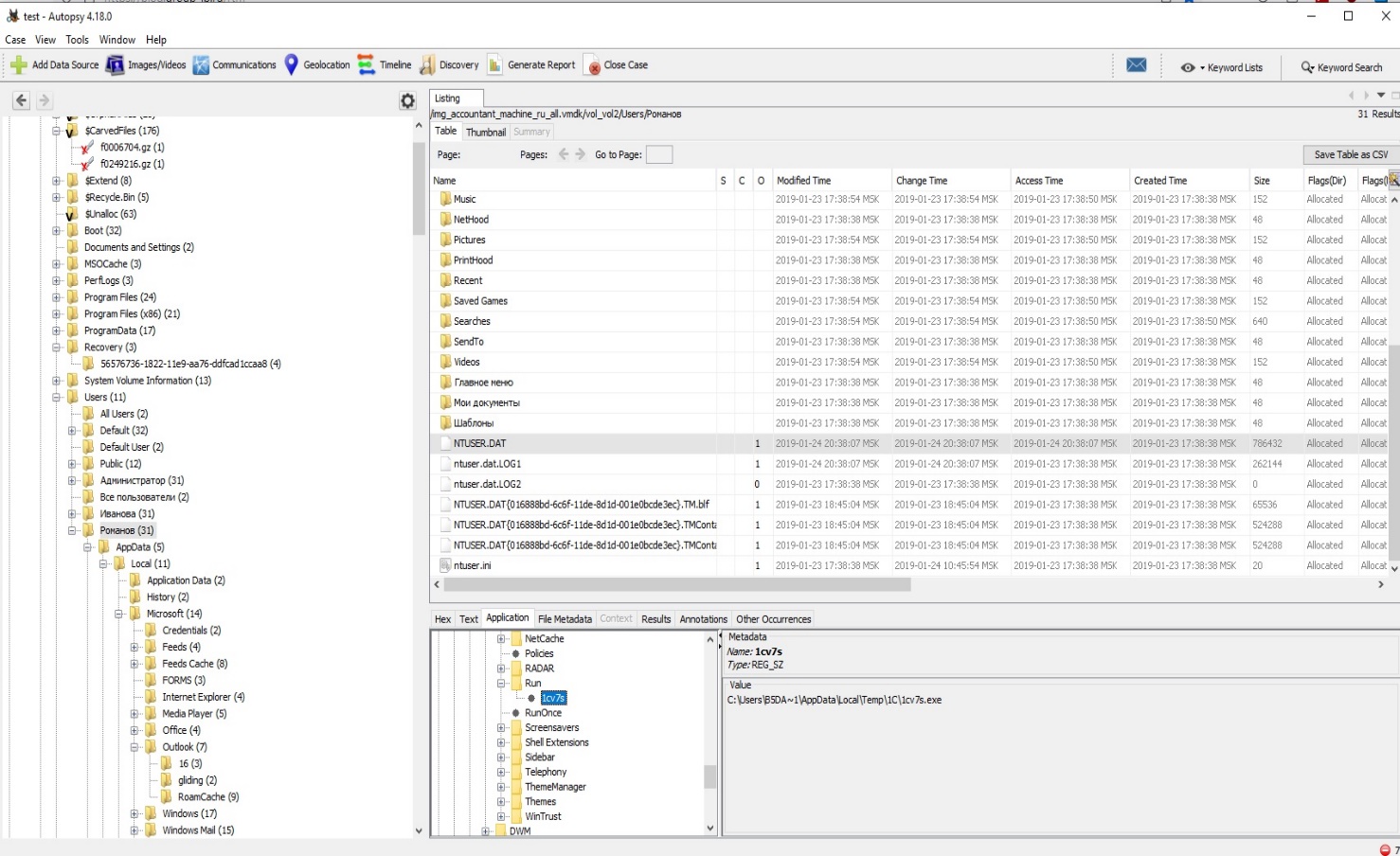
0x0000000000400000 0x16000 0xffff C:\Users\B5DA~1\AppData\Local\Temp\1C\1cv7s.exe

0x0000000077630000 0x1a9000 0xffff C:\Windows\SYSTEM32\ntdll.dll

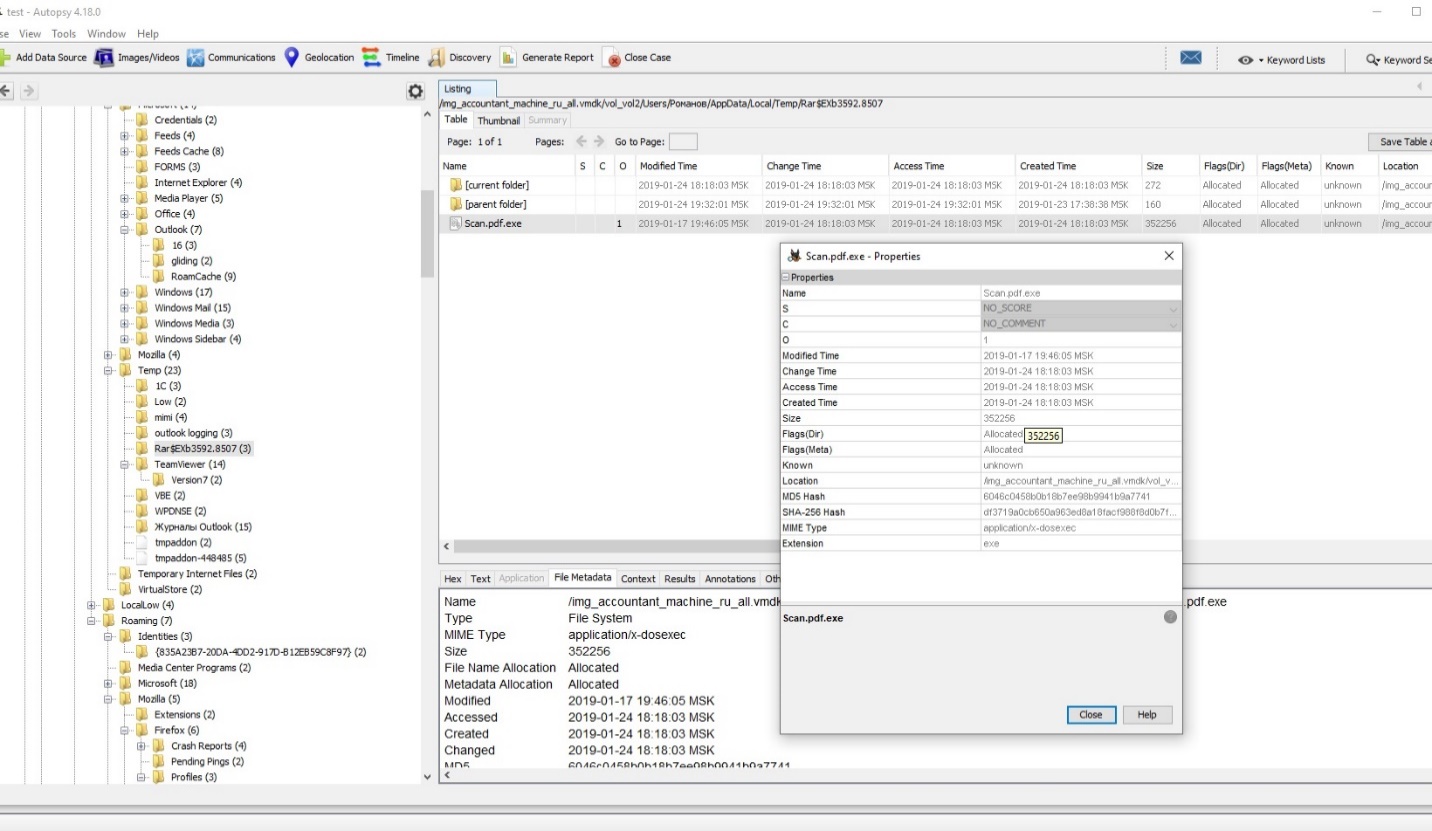
0x0000000075100000 0x3f000 0x3 C:\Windows\SYSTEM32\wow64.dll

0x00000000750a0000 0x5c000 0x1 C:\Windows\SYSTEM32\wow64win.dll

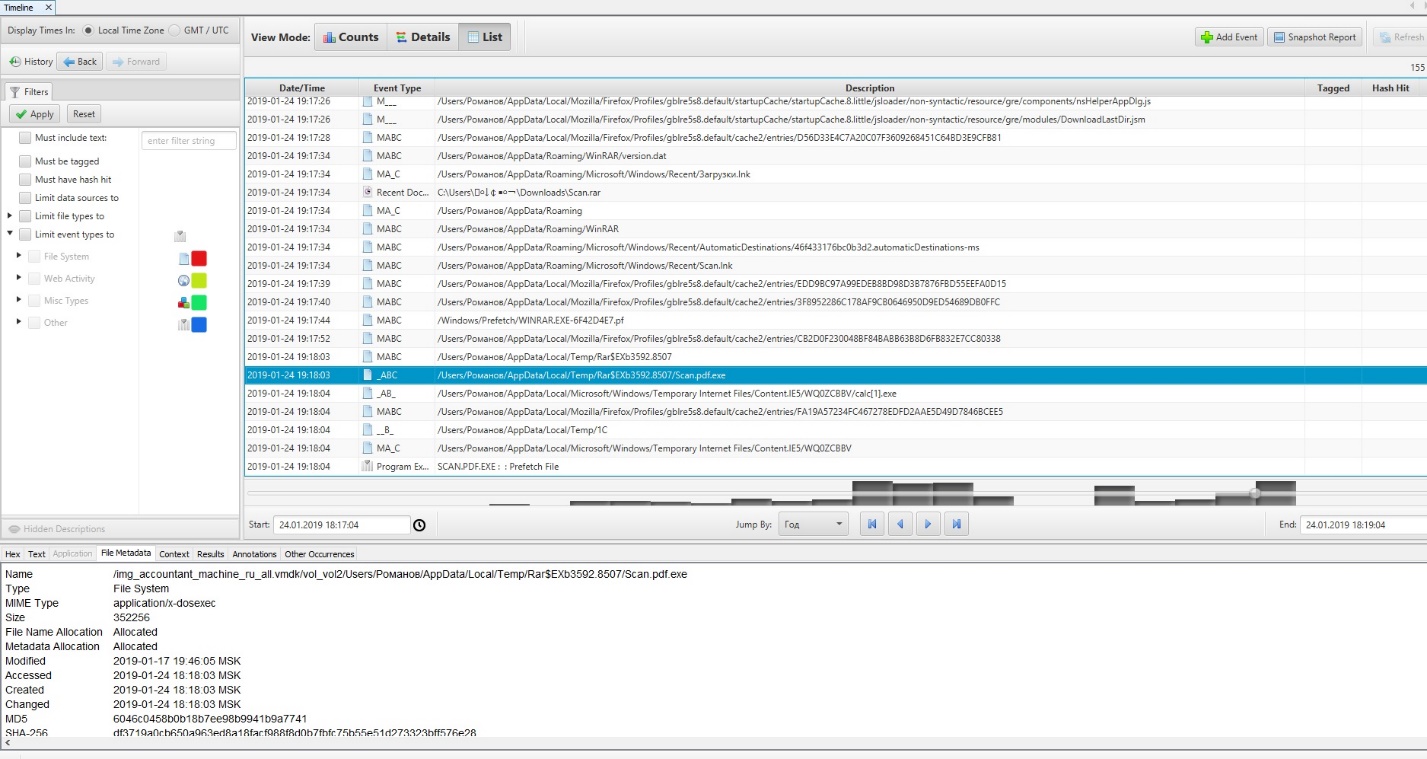
0x0000000075160000 0x8000 0x1 C:\Windows\SYSTEM32\wow64cpu.dll

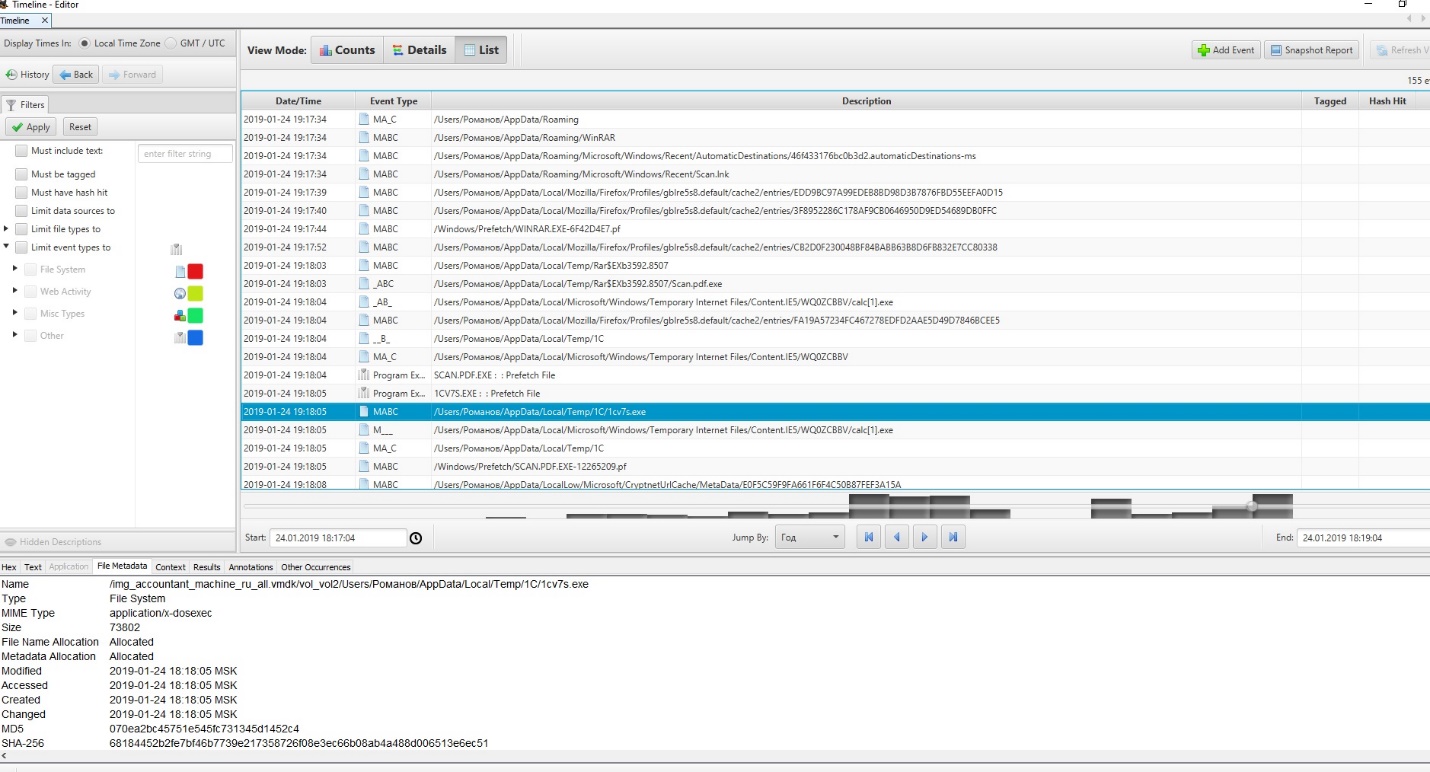


Видим, что при входе пользователя запускается файл 1cv7s.exe и scan.pdf.exe из не самого стандартного расположения.

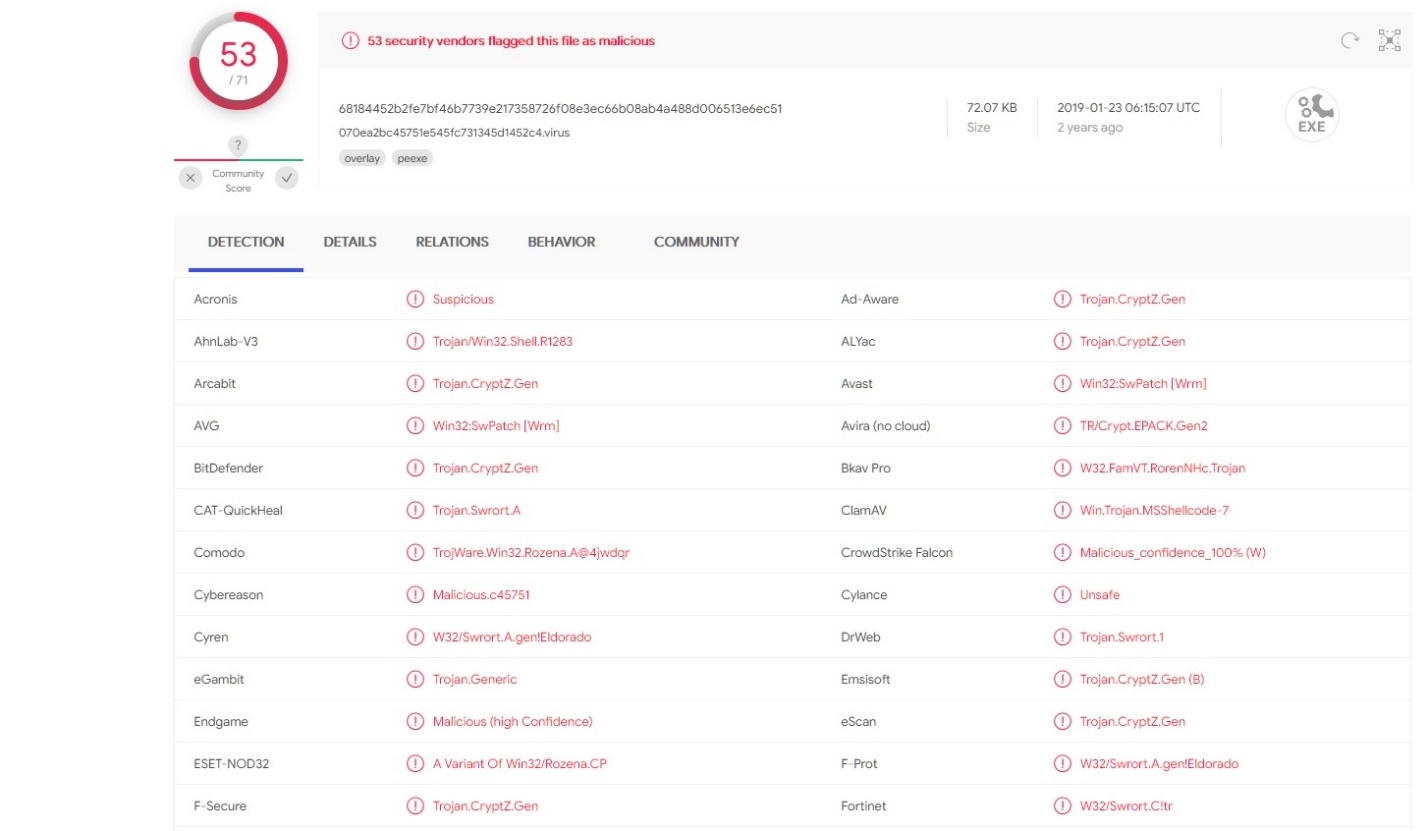
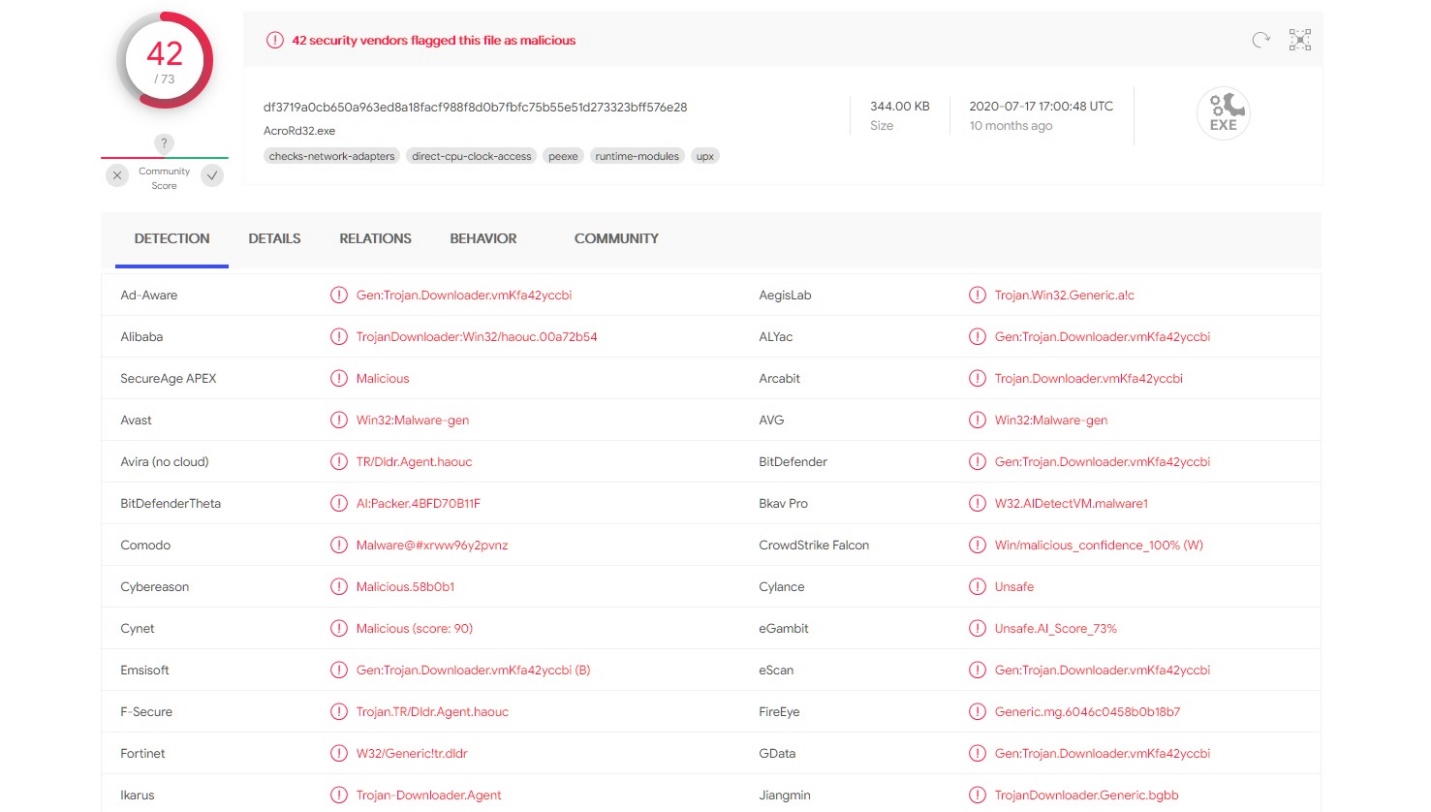


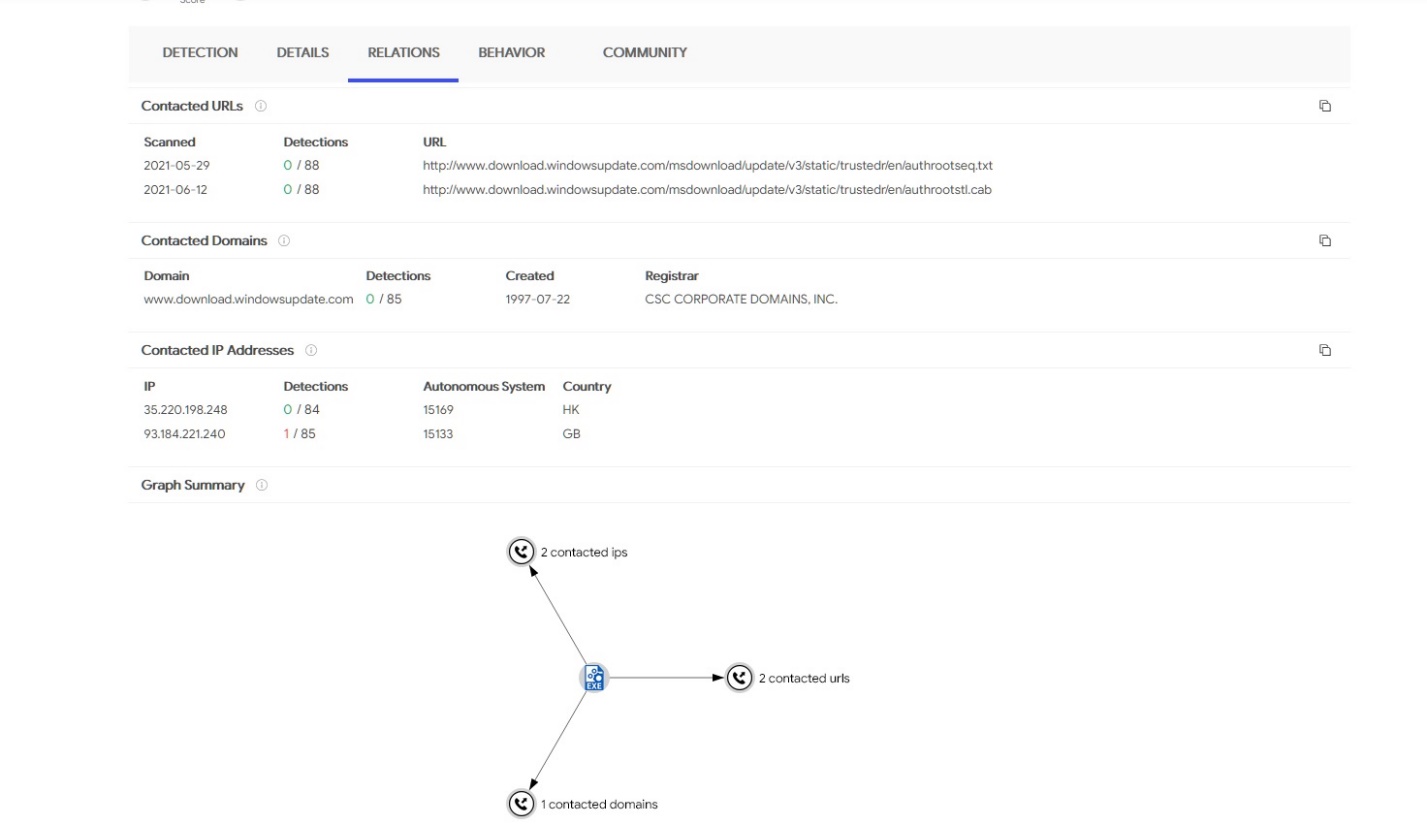
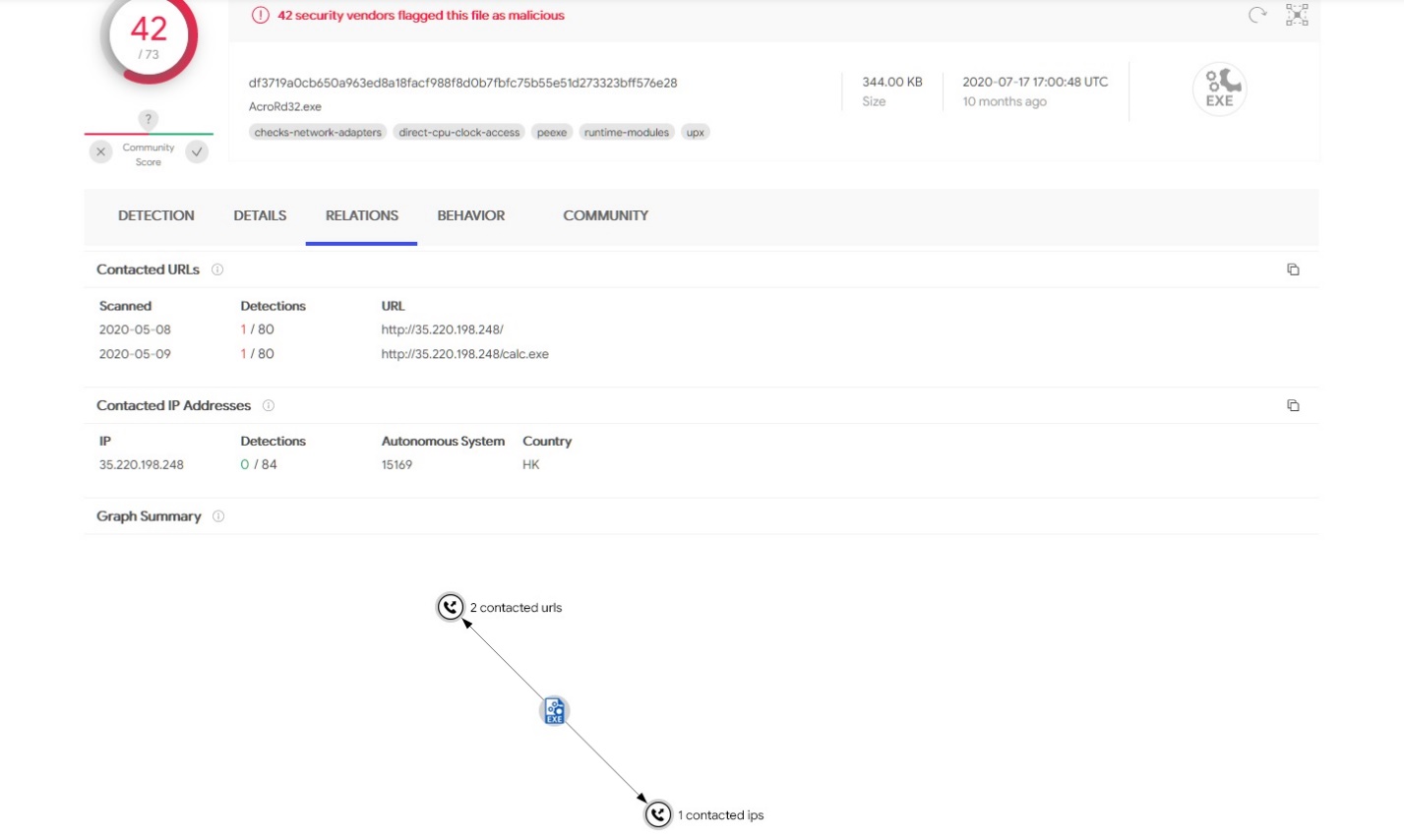
Таймлайн будет включать события файловой системы.





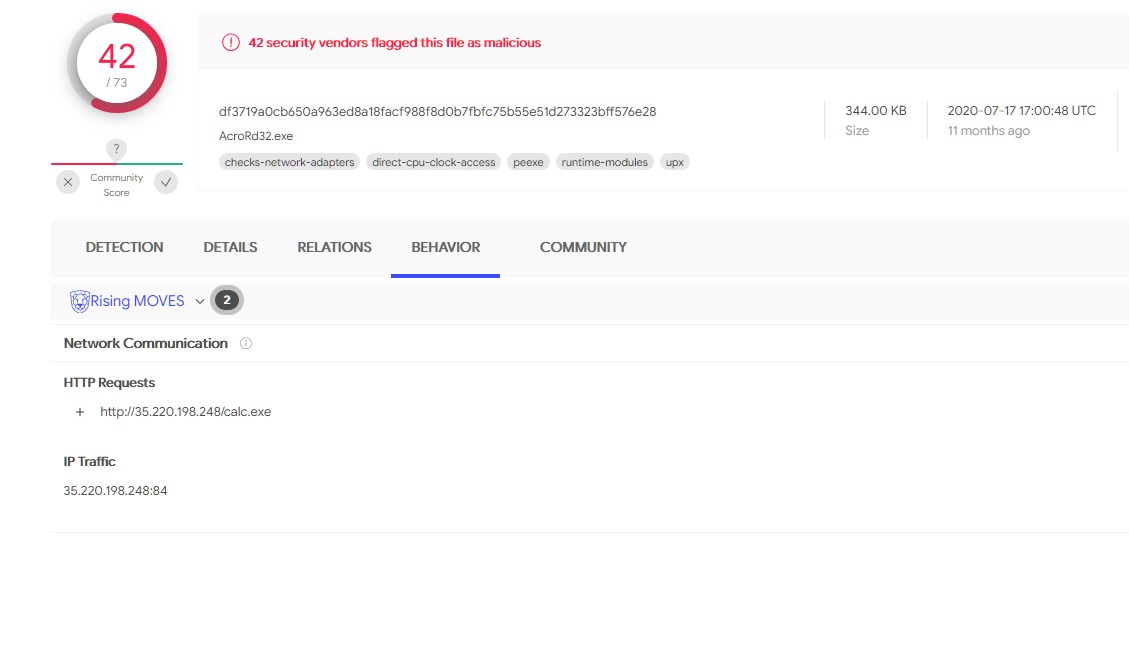
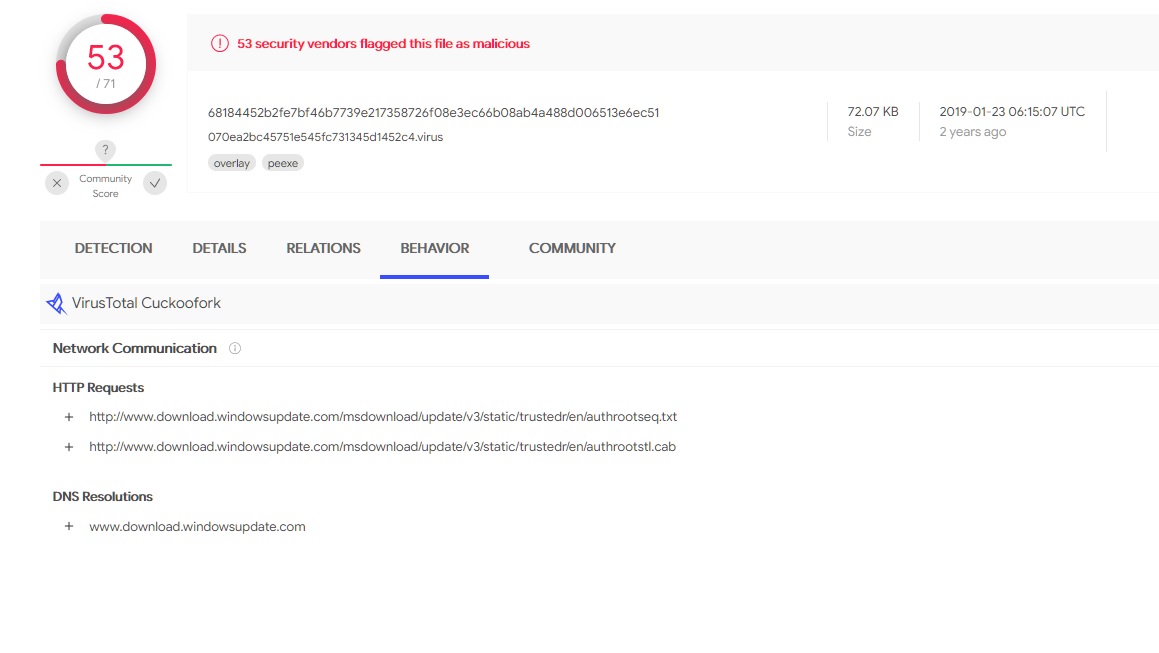
По контрольной сумме ищем на VirusTotal и сразу несколько антивирусных продуктов детектируют как Trojan.





Как видно на иллюстрации, некоторое антивирусное ПО детектирует наш файл довольно определенно – мы имеем дело с RTM.

Сетевые индикаторы компрометации в вкладке Behavior



Наиболее вероятным вектором заражения является фишинговое письмо. В данном случае пользователь Романов использовал Microsoft Outlook адрес semen.romanov.1982@mail.ru.

1. С помощью API сервиса https://censys.io найти и вывести все IP-

адреса из сети 217.175.16.0/23 на которых доступен https.

Отображение сделать в удобочитаемом виде. Желательно, для

решения задачи использовать Python.

2. У вас есть разнородная ИТ-инфраструктура из нескольких тысяч

машин, коммутаторов, контроллеров. Ваша задача — научиться

выявлять в логах этих машин, коммутаторах события безопасности.

Как вы будете проектировать такую систему? На какие события

будете смотреть?

Диапазон ip адресов (192.168.1.1 TO 192.168.1.22)

С помощью API сервиса Censys

(ip:[192.168.1.1 TO 192.168.1.22]) AND protocols: "443/https"

Для разнородной ИТ-инфраструктуры из нескольких тысяч машин, коммутаторов, контроллеров требуется сервер логирования VMware NSX Data Center

Такие события как:

События входа и выхода,

Изменение аккаунта, Изменение пароля,

Запуск и прекращение работы сервисов

Трафик, заблокированный файерволом,

Объем трафика,

Использование каналов и протоколов,

Обнаружение атаки,

Изменение аккаунта,

Доступ администратора,

Чрезмерные попытки доступа,

Сообщения об остановке/запуске/сбое веб-службы,

Доступ к расширениям, которые вы не устанавливали, код ошибки 200 (успешный запрос) на файлах, которые не принадлежат вам,

Ошибка аутентификации: Код ошибки 401,403, Неверный запрос: Код ошибки 400, Внутренняя ошибка сервера: Код ошибки 500

Перебор пользователей и групп (события 4798 и 4799).

Создание локальной учётной записи и изменения в локальных группах (события 4720, 4722–4726, 4738, 4740, 4767, 4780, 4781, 4794, 5376 и 5377).

Попытки входа с локальной учётной записью (событие 4624)

Попытка входа с заданной учётной записью (событие 4648)

Изменения конфигурации файрволла (события 4944-4958)

Подключение устройств Plug’n’play (событие 6416 и только для WIndows 10).

Изменения в системном реестре (ID события 12-14)