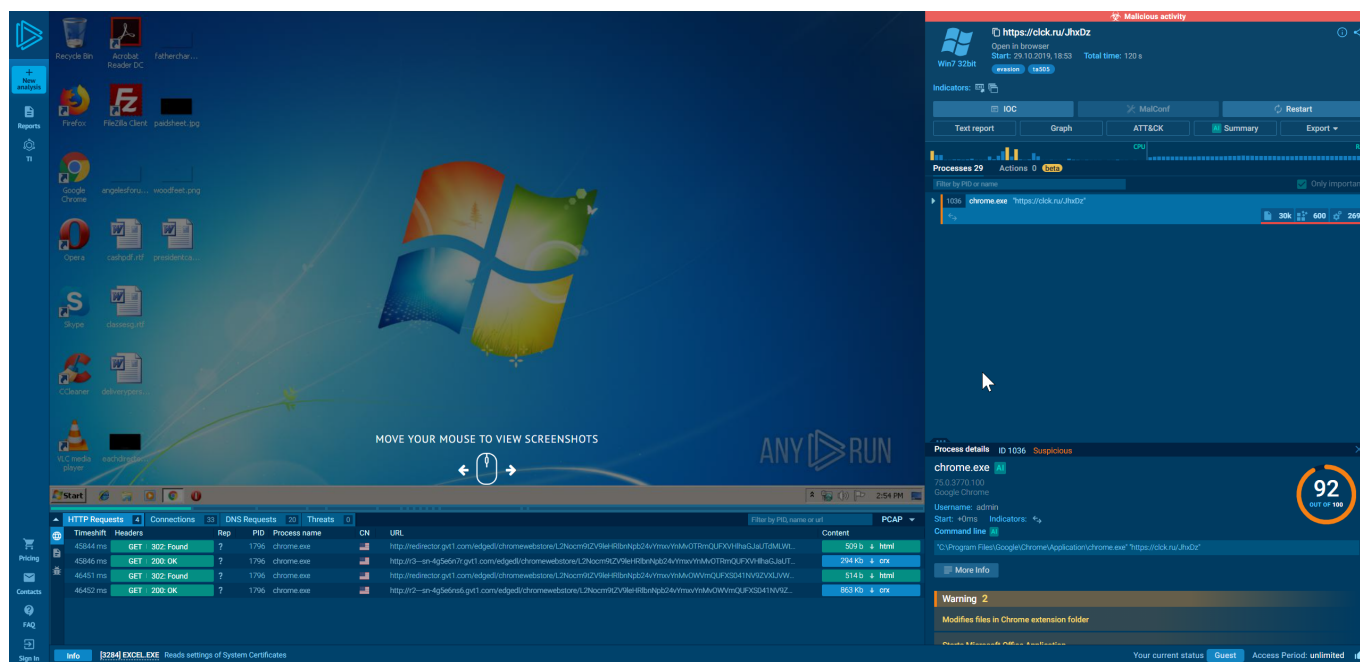


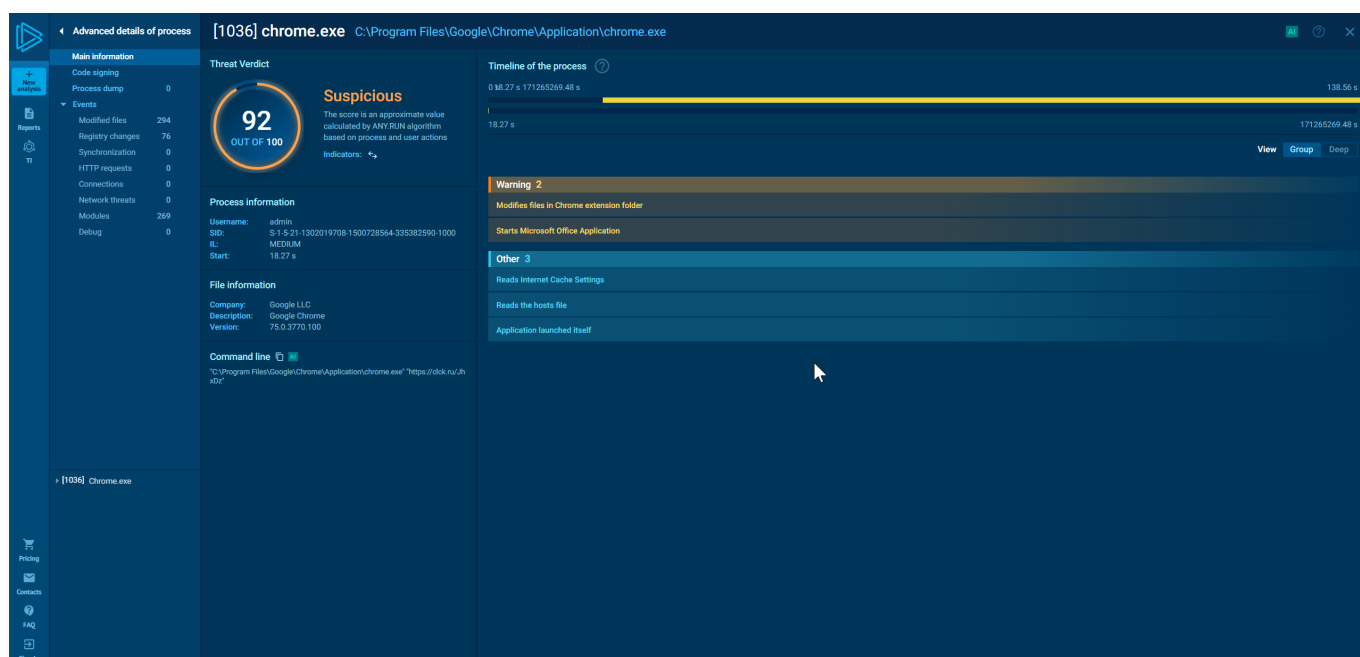
# Практическое задание №2: анализ отчета песочницы

Задание 1. Исходя из демонстрируемых действий с файлом укажите способ доставки и способ запуска полезной нагрузки на хосте (user или non-user).

В отчете мы видим уведомление о Malicious activity, которое начинается в процессе chrome.exe



Если открыть детальную информацию по данному процессу ("More info"), то мы увидим, что приложение было запущено без участия пользователя ("Other -> Application launched itself")



Дополнительно можем открыть более подробную информацию и увидеть, что chrome.exe (PID: 1036) запущен из командной строки с параметром "https://clck.ru/JhxDz" - т.е. внешней ссылкой (на

вредоносный ресурс)

# Behavior activities

(PID: 1036) chrome.exe

1 of 26 Source: Unknown First seen: 281 ms

Other / Suspicious Actions

## Application launched itself

CmdParent: "C:\Program Files\Google\Chrome\Application\chrome.exe" "https://clck.ru/Jhx Dz"

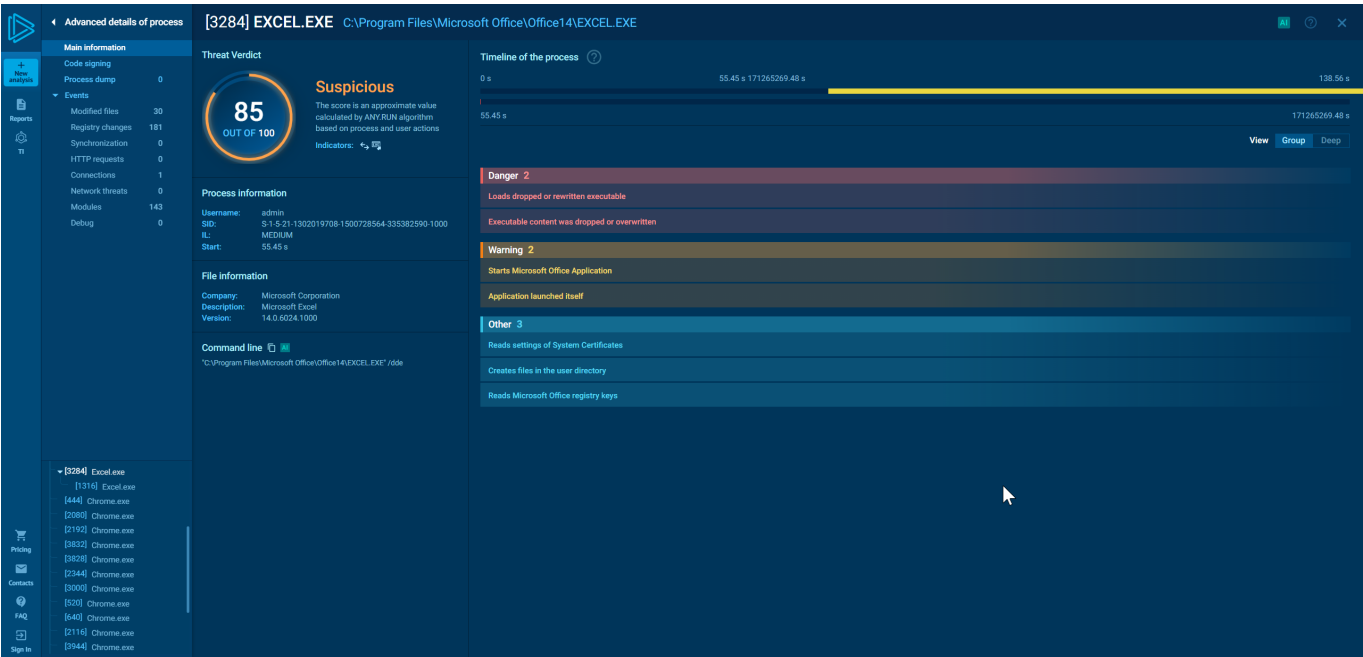
CmdChild: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=crashpad-handler --user-data-dir=C:\Users\admin\AppData\Local\Google\Chrome\User Data /prefetch:7 --monitor-self-annotation=ptype=crashpad-handler --database=C:\Users\admin\AppData\Local\Google\Chrome\User Data\Crashpad --metrics-dir=C:\Users\admin\AppData\Local\Google\Chrome\User Data --url=https://clients2.google.com/cr/report --annotation=channel= --annotation=plat=Win32 --annotation=prod=Chrome --annotation=ver=75.0.3770.100 --initial-client-data=0x7c,0x80,0x84,0x78,0x88,0x6d90a9d0,0x6d90a9e0,0x6d90a9ec

Image: C:\Program Files\Google\Chrome\Application\chrome.exe

Переход на указанную ссылку приводит к редиректу на скачивания вредоносного .xls файла из облачного хранилища и автоматического открытия данного файла в MS Excel.

The screenshot shows a Windows PC with a Google Drive download page open in a browser. The page displays a message "No preview available." and a "Download" button. Below the browser window, a Windows Security window is open, showing a list of processes. The list includes "chrome.exe" and "EXCEL.EXE". The "EXCEL.EXE" process is highlighted, and its details are shown on the right. The details include a warning that "Loads dropped or rewritten executable" and "Executable content was dropped or overwritten". The "Other" section shows "Application launched itself".

Дополнительная информация по процессу [3284] EXCEL.EXE C:\Program Files\Microsoft Office\Office14\EXCEL.EXE так же сообщает о том, что приложение было запущенно без участия пользователя (Warning: Application launched itself)



Таким образом, делаем вывод, что способ запуска полезной нагрузки на хосте **non-user**

Задание 2. Укажите полный путь исследуемого файла на диске.

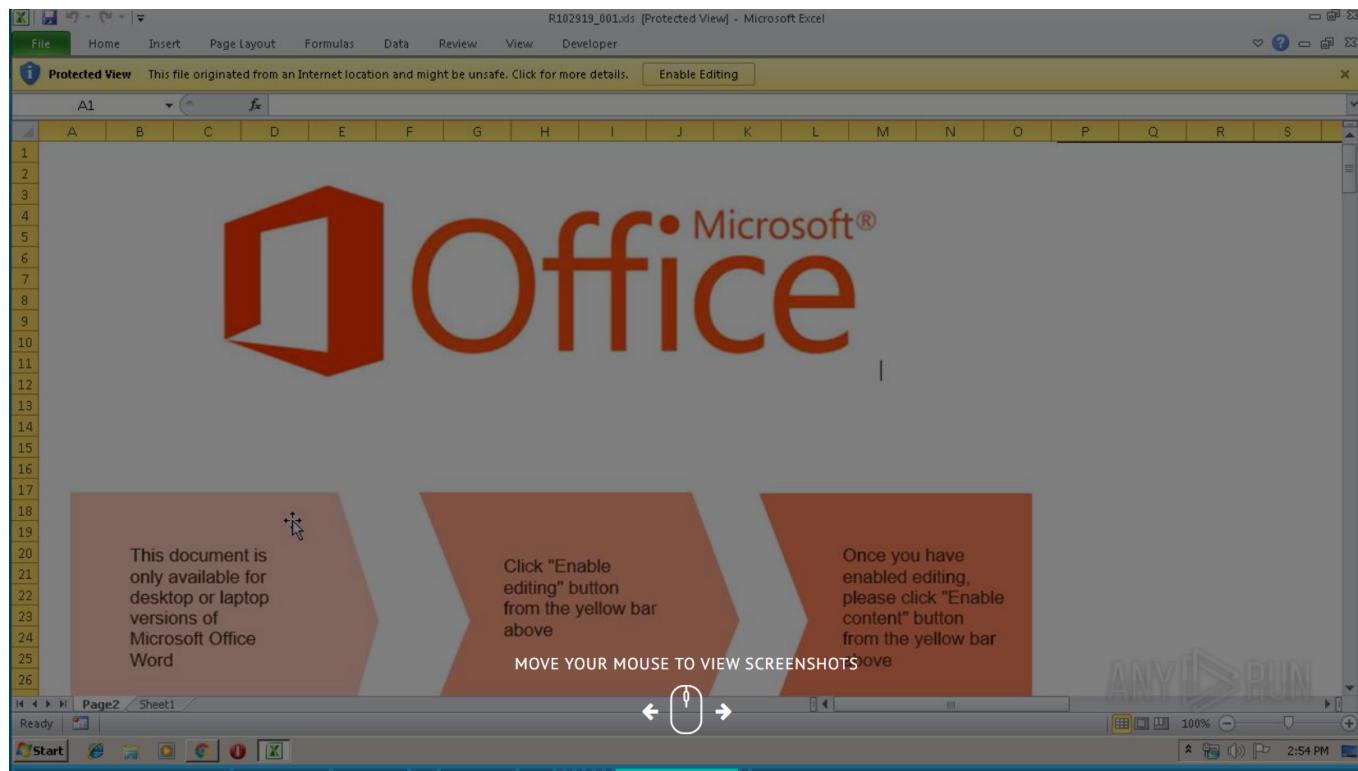
|          |              |        |   |
|----------|--------------|--------|---|
| +5318 ms | Delete Value | Item 1 | HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\File MRU<br>[F00000000][T01D56F99396E0A50][O00000000]*C:\Users\admin\Documents\test.xlsx       |
| +5318 ms | Write        | Item 1 | HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\File MRU<br>[F00000000][T01D58E68CF386420][O00000000]*C:\Users\admin\Downloads\R102919_001.xls |
| +5318 ms | Write        | Item 2 | HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\File MRU   |

Полный путь исследуемого файла на диске: C:\Users\admin\Downloads\R102919\_001.xls

Задание 3. На основе текстового отчета выпишите признаки вредоносного поведения файла.

Механизм атаки:

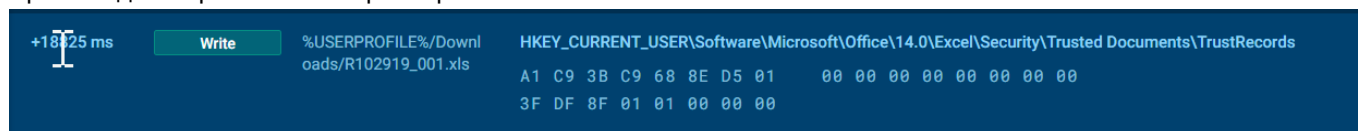
1. Первый файл (с Protected View):



Загружается автоматически через Chrome Excel открывает его в Protected View (безопасный режим) В Protected View макросы не выполняются, но этот файл может содержать механизм для обхода или триггер

## 2. Второй этап (изменение реестра):

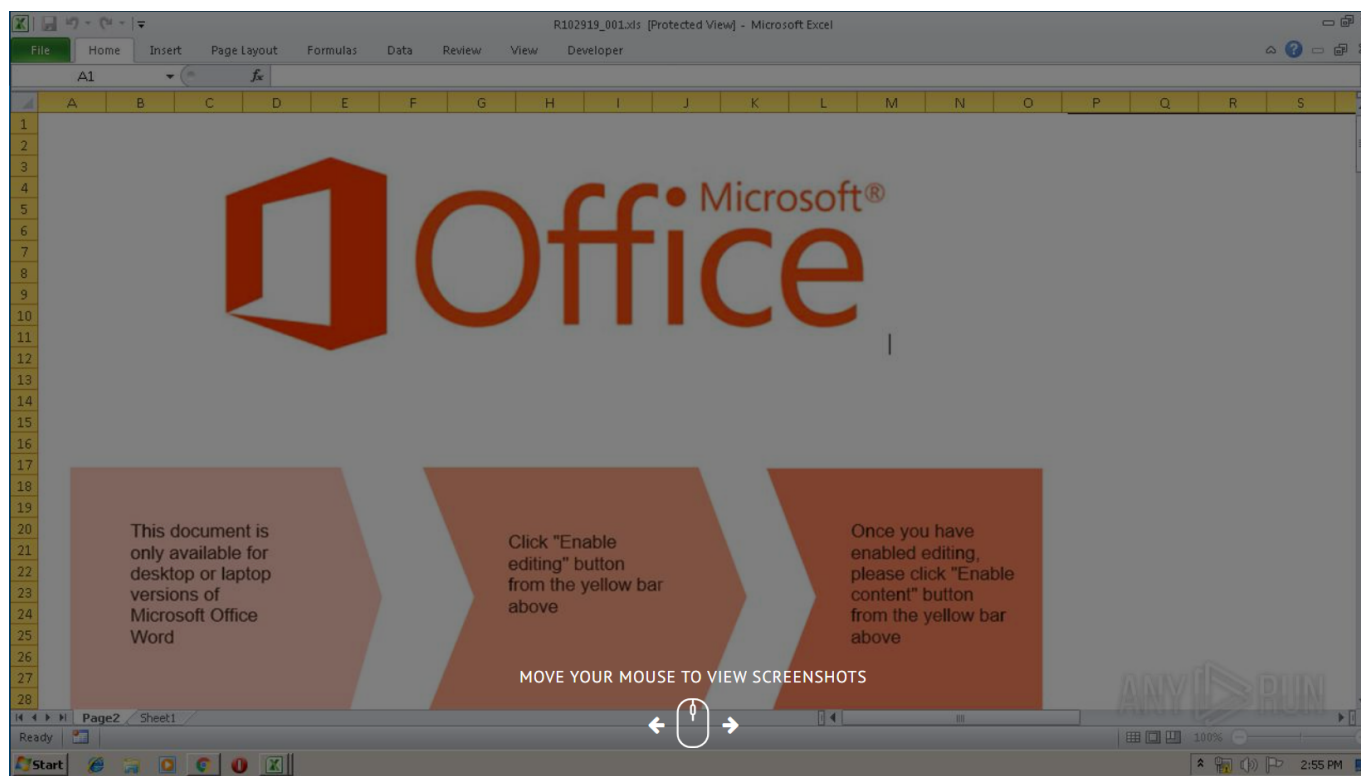
После выполнения макросов Excel автоматически записывает файл в Trusted Documents. Это происходит через запись в реестр



## 3. Третий этап (персистентность):

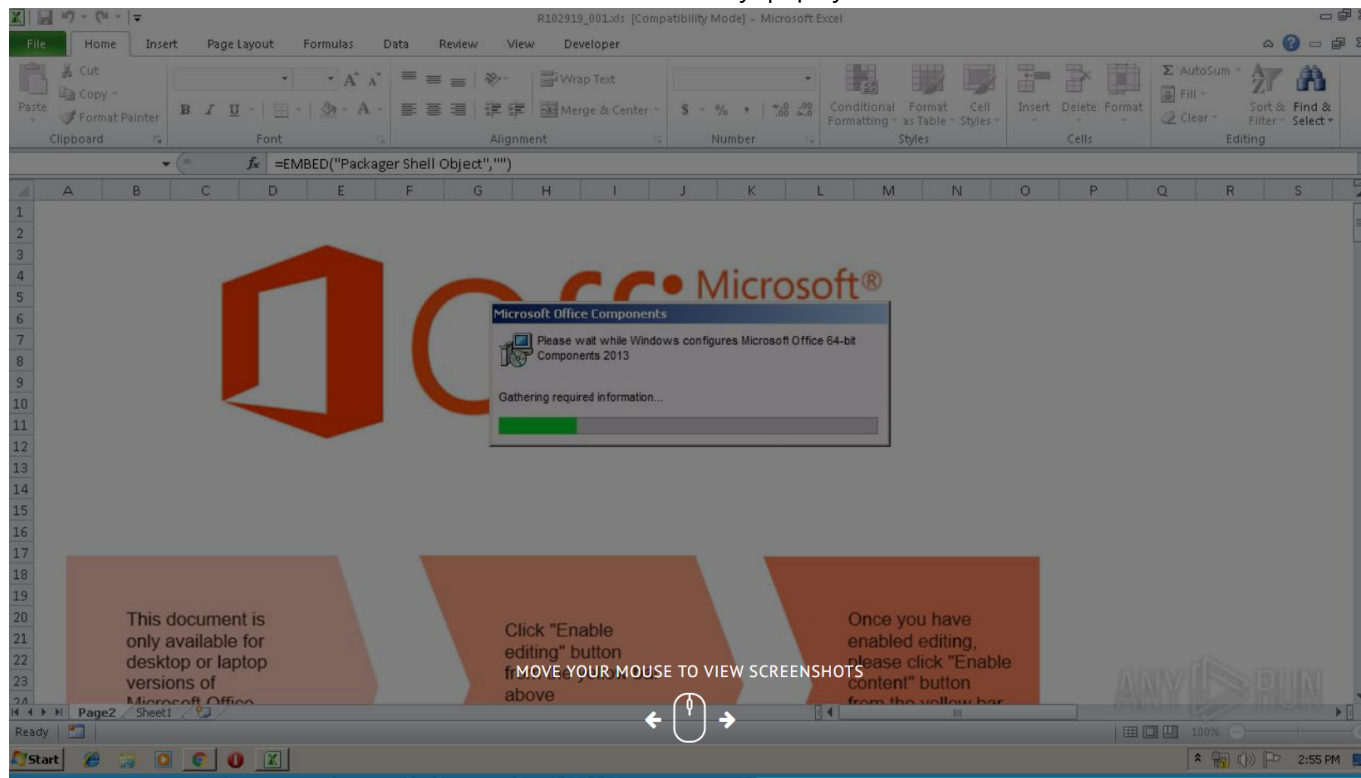
Файл теперь в списке доверенных. При следующем открытии (видно что открыто 2 экземпляра файла) - макросы будут выполняться автоматически, без предупреждений - это обеспечивает персистентность

атаки.



#### 4. Финальный файл с EMBED:

Это тот же второй файл или результат обработки. Формула EMBED("Packager Shell Object","") уже готова к выполнению. Файл больше не в Protected View, поэтому формула может выполняться.



Это двухэтапная атака:

Первый файл — обход Protected View и запуск второго этапа. Второй файл — содержит EMBED и выполняется без ограничений. Вероятно, первый файл использует внешние ссылки или DDE для

автоматической загрузки и открытия второго файла, минуя Protected View. Это объясняет, почему в итоге виден только один файл с формулой EMBED — второй файл заменил первый или это тот же файл, открытый другим способом. Признак вредоносного поведения: Автоматическое открытие второго файла без участия пользователя и обход Protected View.

EMBED("Packager Shell Object","") — альтернатива DDE для обхода защиты макросов. Используется для автоматического запуска кода без предупреждений о макросах, что часто является частью многоэтапной атаки.