

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

The screenshot shows a Windows desktop with various icons on the taskbar and desktop. A browser window titled "Malicious activity" is open, showing network traffic for chrome.exe. The window includes a timeline, process details (ID 1036, Suspicious), and a warning section indicating the process modifies files in the Chrome extension folder.

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

This screenshot provides a detailed view of the ANY.RUN process analysis for chrome.exe (PID 1036). It shows the threat verdict as "Suspicious" (92 out of 100), a timeline of the process, and various threat categories such as "Warning" (Modifies files in Chrome extension folder), "Other" (Reads Internet Cache Settings, Reads the hosts file, Starts Microsoft Office Application), and "Info" (Application launched itself). The left sidebar shows navigation and reporting options.

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

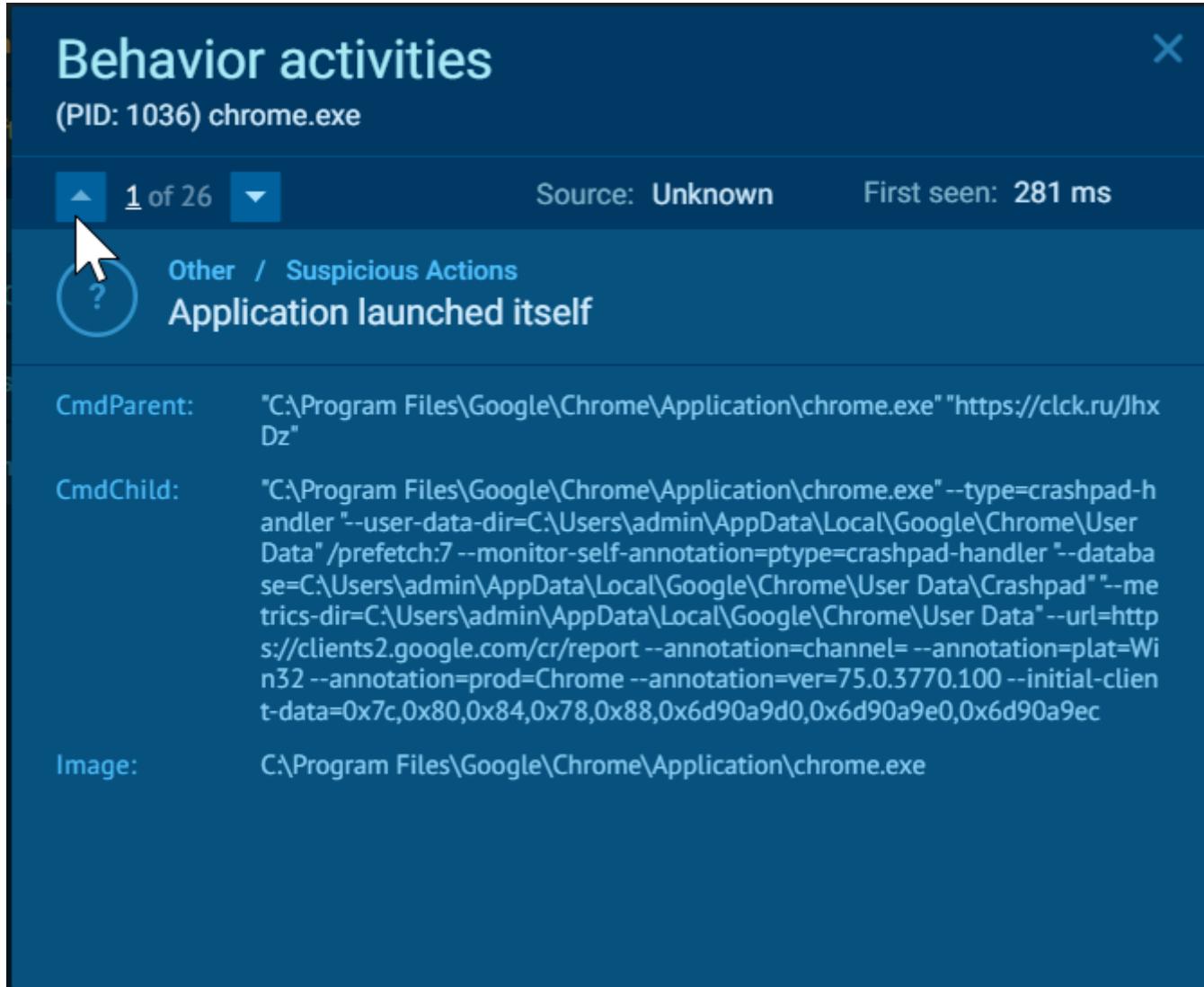
1 of 26 Source: Unknown First seen: 281 ms

Other / Suspicious Actions Application launched itself

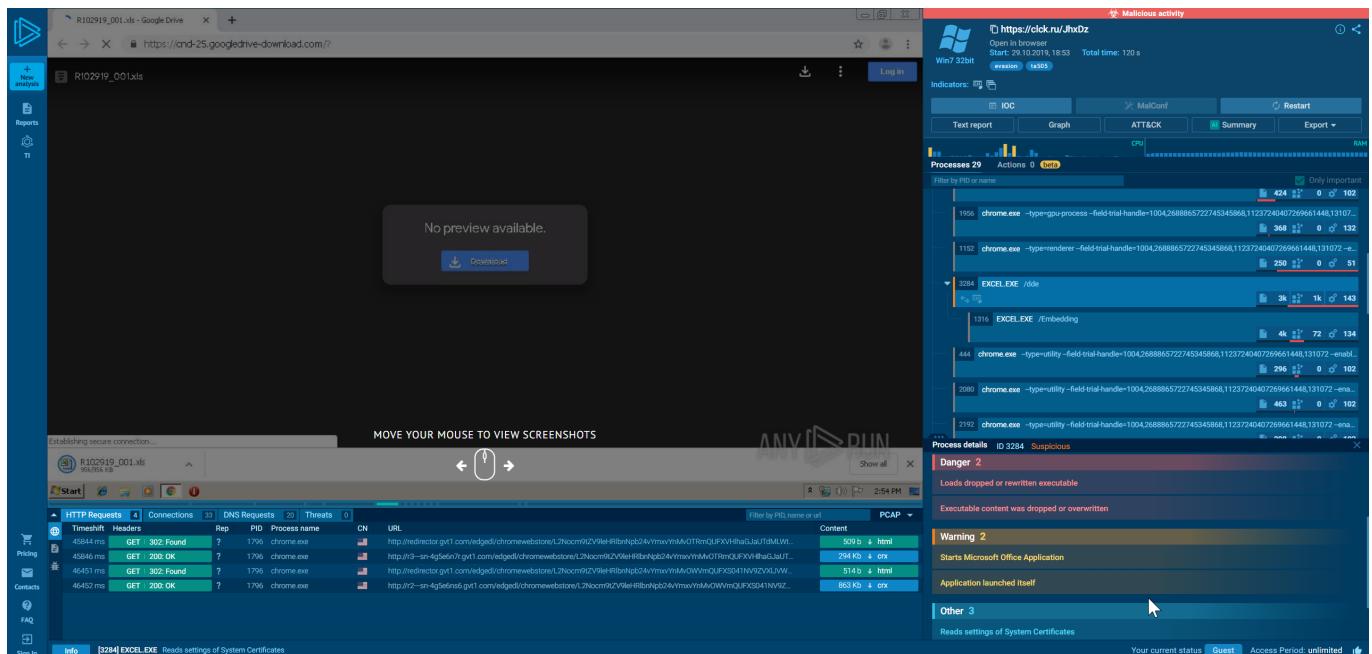
CmdParent: "C:\Program Files\Google\Chrome\Application\chrome.exe" "https://clck.ru/JhxDz"

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.



Malicious activity

R102919_001.xls - Google Drive

No preview available.

Establishing secure connection... MOVE YOUR MOUSE TO VIEW SCREENSHOTS

HTTP Requests Connections DNS Requests Threats

| Timeshift | Headers | Rep | PID | Process name | CN | URL | Content |
|-----------|---------------|-----|------|--------------|----|--|--------------|
| 45840 ms | GET 302 Found | ? | 1796 | chrome.exe | | http://redactor.gvt1.com/edged/chromewebstore/L2Nocm9tZV9leRltbnNgbz4YmwsYmM0TRmQlUfXHlaGlsJtDUtW... | 509 b & HTML |
| 45840 ms | GET 200 OK | ? | 1796 | chrome.exe | | http://r3-sn-4g5e61.gvt1.com/edged/chromewebstore/L2Nocm9tZV9leRltbnNgbz4YmwsYmM0TRmQlUfXHlaGlsJtDUtW... | 514 b & HTML |
| 46451 ms | GET 302 Found | ? | 1796 | chrome.exe | | http://redactor.gvt1.com/edged/chromewebstore/L2Nocm9tZV9leRltbnNgbz4YmwsYmM0TRmQlUfXHlaGlsJtDUtW... | 863 b & HTML |
| 46452 ms | GET 200 OK | ? | 1796 | chrome.exe | | http://r2-sn-4g5e61.gvt1.com/edged/chromewebstore/L2Nocm9tZV9leRltbnNgbz4YmwsYmM0TRmQlUfXHlaGlsJtDUtW... | |

Process details ID 3284 Suspicious

Danger 2 Loads dropped or rewritten executable

Executable content was dropped or overwritten

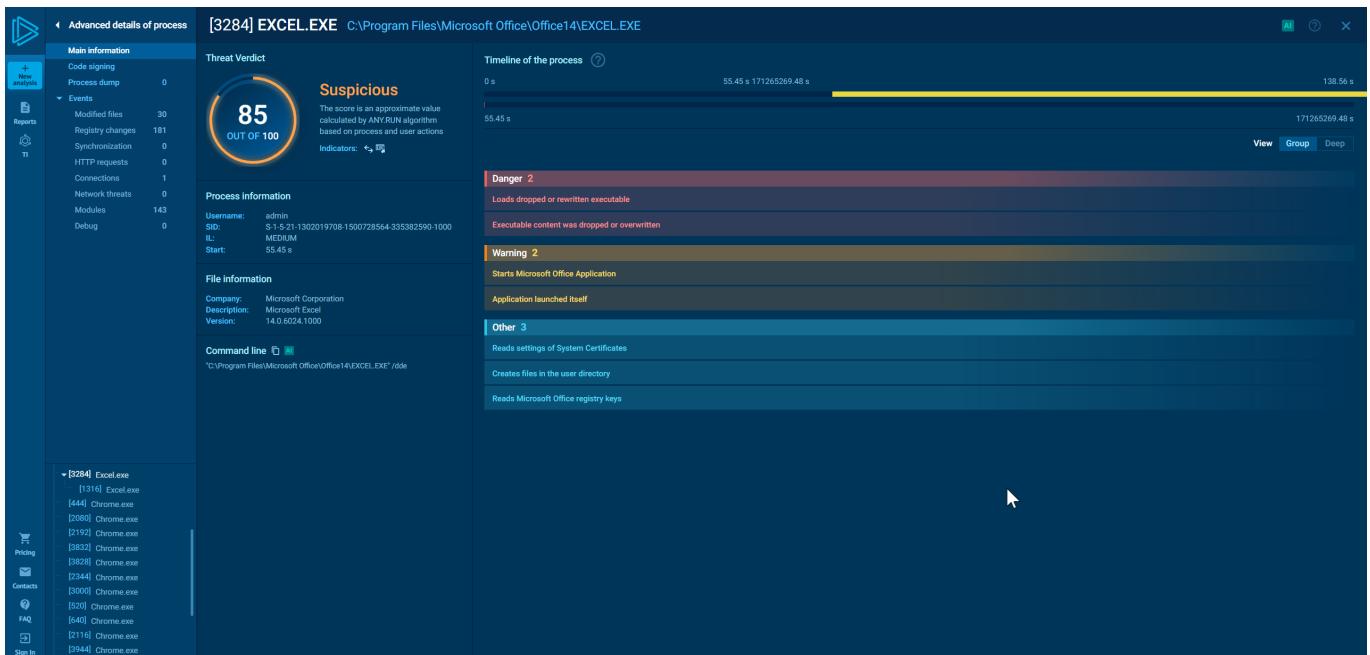
Warning 2 Starts Microsoft Office Application

Application launched itself

Other 3 Reads settings of System Certificates

Your current status Guest Access Period: unlimited

Дополнительная информация по процессу [3284] EXCEL.EXE C:\Program Files\Microsoft Office\Office14\EXCEL.EXE так же сообщает о том, что приложение было запущено 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.

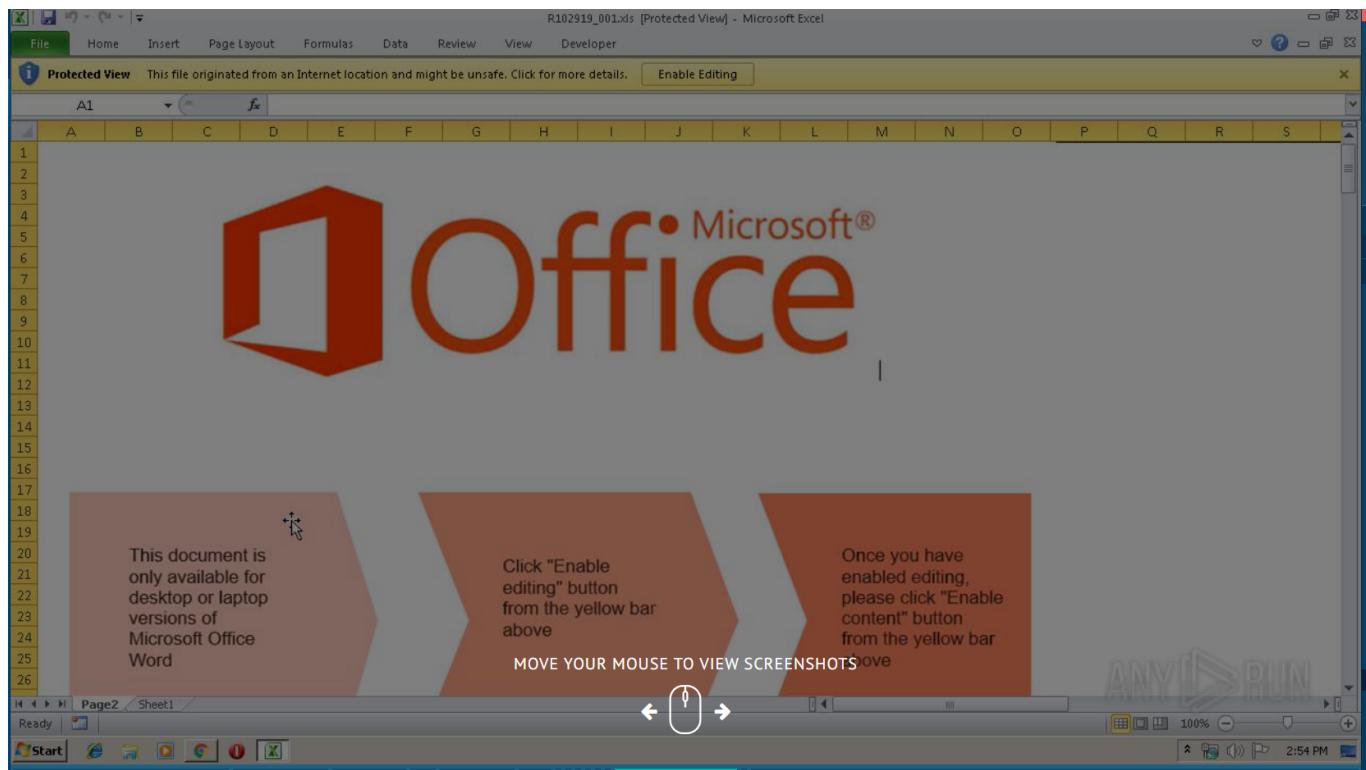
| | | | |
|----------|--------------|--------|---|
| +5318 ms | Delete Value | Item 1 | HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\File MRU [F0000000][T01D56F99396E0A50][00000000]*C:\Users\admin\Documents\test.xls |
| +5318 ms | Write | Item 1 | HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\File MRU [F0000000][T01D58E68CF386420][00000000]*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):

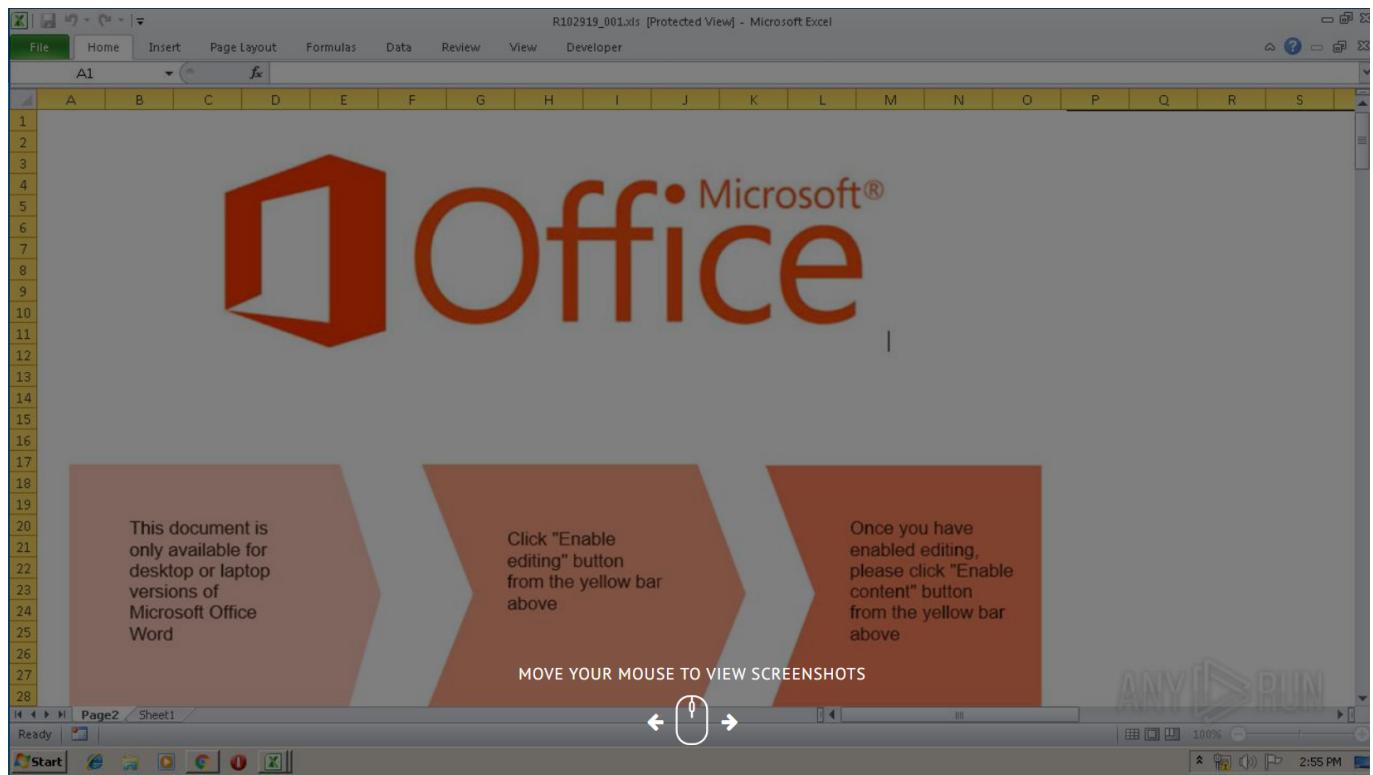
После выполнения макросов Excel автоматически записывает файл в Trusted Documents. Это происходит через запись в реестр

A screenshot of a debugger showing a write operation to the registry. The operation is labeled "Write" and the path is "%USERPROFILE%\Downloads\R102919_001.xls". The destination key is "HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Security\Trusted Documents\TrustRecords". The data being written is binary: A1 C9 3B C9 68 8E D5 01 00 00 00 00 00 00 00 00 3F DF 8F 01 01 00 00 00.

3. Третий этап (персистентность):

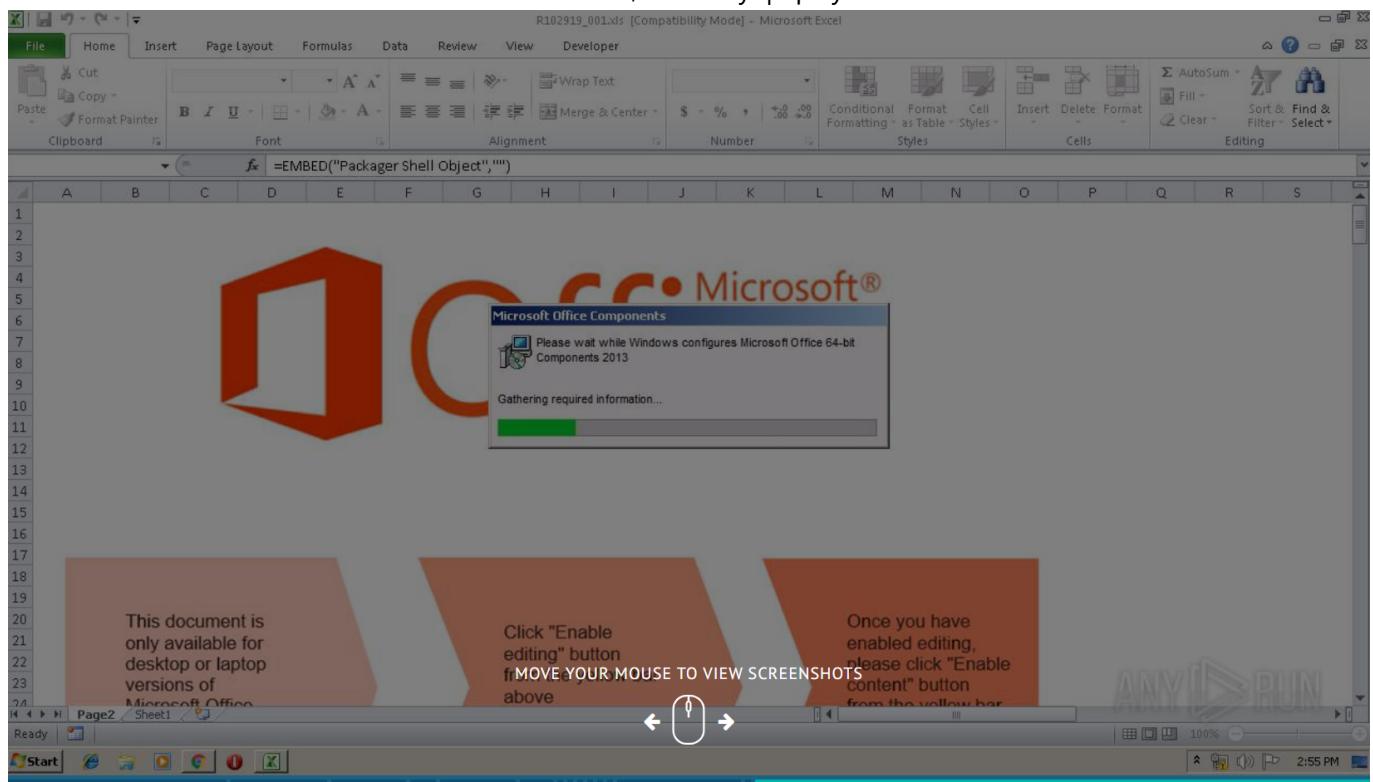
Файл теперь в списке доверенных. При следующем открытии (видно что открыто 2 экземпляра файла) - макросы будут выполнятся автоматически, без предупреждений - это обеспечивает персистентность

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 выполниться



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.