

Беллерофонту такое и не снилось. Троян ChimeraWire накручивает популярность сайтов, искусно притворяясь человеком

 news.drweb.ru/show

December 8, 2025



[Подробнее](#)

Горячая лента угроз | «Горячие» новости | Все новости

[Скачать PDF](#)

8 декабря 2025 года

Введение

В ходе анализа одной из партнерских программ специалисты компании «Доктор Веб» обнаружили уникальное ВПО с функциональностью кликера, получившее наименование [Trojan.ChimeraWire](#). Оно работает на компьютерах под управлением ОС Windows и основано на проектах с открытым исходным кодом [zlsgo](#) и [Rod](#) для автоматизированного управления веб-сайтами и веб-приложениями.

[Trojan.ChimeraWire](#) позволяет злоумышленникам имитировать действия пользователей и накручивать поведенческий фактор веб-сайтов, искусственно поднимая их рейтинг в выдаче поисковых систем. Для этого вредоносная программа выполняет поиск нужных интернет-ресурсов в системах Google и Bing, после чего открывает их. Она также имитирует действия

пользователей, самостоятельно нажимая на ссылки на загруженных сайтах. Троян совершает все вредоносные действия через браузер Google Chrome, который он скачивает с определенного ресурса и запускает в скрытом режиме отладки по протоколу WebSocket.

[Trojan.ChimeraWire](#) попадает на компьютеры в результате работы нескольких вредоносных программ-загрузчиков. Они используют различные техники повышения привилегий на основе эксплуатации уязвимостей класса DLL Search Order Hijacking, а также антиотладочные приемы с целью избежать обнаружения. Наша антивирусная лаборатория отследила как минимум 2 цепочки заражения с их участием. В одной из них центральное место занимает вредоносный скрипт [Python.Downloader.208](#), а в другой — вредоносная программа [Trojan.DownLoader48.61444](#), которая по принципу работы схожа с [Python.Downloader.208](#) и фактически выступает его альтернативой.

В данном исследовании мы рассмотрим особенности [Trojan.ChimeraWire](#) и вредоносных программ, которые доставляют его на устройства пользователей.

Первая цепочка заражения



Схема, иллюстрирующая первую цепочку заражения

Первая цепочка начинается с трояна [Trojan.DownLoader48.54600](#). Он проверяет, не работает ли в искусственной среде, и завершает работу, если обнаруживает признаки виртуальной машины или режима отладки. Если таких признаков нет, троян скачивает с C2-сервера ZIP-архив python3.zip. В нем находится вредоносный Python-скрипт [Python.Downloader.208](#), а также необходимые для его работы вспомогательные файлы — в частности, вредоносная библиотека ISCSIEXE.dll ([Trojan.Starter.8377](#)). [Trojan.DownLoader48.54600](#) распаковывает архив и запускает скрипт. Тот является второй ступенью заражения и представляет собой загрузчик, который скачивает с C2-сервера следующую стадию.

Поведение [Python.Downloader.208](#) зависит от того, какими правами он обладает при запуске. Если скрипт запущен без прав администратора, он пытается их получить. Для этого извлеченный вместе с ним [Trojan.Starter.8377](#) копируется в каталог %LOCALAPPDATA%\Microsoft\WindowsApps. Кроме того, создается скрипт runs.vbs, который в дальнейшем будет использован для повторного запуска [Python.Downloader.208](#).

Далее [Python.Downloader.208](#) запускает системное приложение %SystemRoot%\SysWOW64\iscsicpl.exe. Из-за наличия в нем уязвимости класса DLL Search Order Hijacking оно автоматически загружает троянскую библиотеку ISCSIEXE.dll, имя которой совпадает с именем легитимного компонента ОС Windows.

В свою очередь, [Trojan.Starter.8377](#) запускает VBS-скрипт runs.vbs, и тот повторно исполняет [Python.Downloader.208](#) — уже с правами администратора.

При запуске с необходимыми привилегиями [Python.Downloader.208](#) скачивает с C2-сервера защищенный паролем архив onedrive.zip. В нем находится следующая стадия заражения — вредоносная программа [Trojan.DownLoader48.54318](#) в виде библиотеки с именем UpdateRingSettings.dll — и необходимые для ее работы вспомогательные файлы (например, легитимное приложение OneDrivePatcher.exe из ОС Windows с действительной цифровой подписью, относящееся к ПО OneDrive).

После распаковки архива [Python.Downloader.208](#) создает задачу в системном планировщике на запуск программы OneDrivePatcher.exe при старте системы. Далее он запускает это приложение. Из-за наличия в нем уязвимости DLL Search Order Hijacking оно автоматически загружает вредоносную библиотеку UpdateRingSettings.dll, имя которой совпадает с именем компонента ПО OneDrive.

Получив управление, [Trojan.DownLoader48.54318](#) проверяет, не работает ли он в искусственной среде. При обнаружении одного из признаков работы в виртуальной машине или в режиме отладки он прекращает работу.

Если такие признаки не обнаруживаются, троянская библиотека пытается скачать с C2-сервера полезную нагрузку, а также ключи шифрования для ее расшифровки.

Расшифрованная полезная нагрузка представляет собой ZLIB-контейнер, внутри которого находится шеллкод и исполняемый файл. После расшифровки контейнера [Trojan.DownLoader48.54318](#) пытается распаковать его. Если это не удастся, то троян самоуничтожается, а сам процесс завершает работу. В случае успеха управление передается шеллкоду, задача которого — разжать идущий вместе с ним исполняемый файл. Данный файл является последней стадией заражения — целевым трояном [Trojan.ChimeraWire](#).

Вторая цепочка заражения

Вторая цепочка начинается с вредоносной программы [Trojan.DownLoader48.61444](#). При запуске она проверяет наличие прав администратора и при их отсутствии пытается их получить. Троян использует технику Masquerade PEВ для обхода системы защиты, маскируясь под легитимный процесс explorer.exe.

Затем он вносит патч в копию системной библиотеки %SystemRoot%\System32\ATL.dll. Для этого [Trojan.DownLoader48.61444](#) считывает ее содержимое, добавляет в нее расшифрованный байт-код и путь до своего файла, после чего сохраняет модифицированную версию в виде файла dropper в той же директории, где он расположен. Далее троян инициализирует объекты COM-модели оболочки Windows для сервиса %SystemRoot%\System32\wbem и измененной библиотеки. Если инициализация проходит успешно, [Trojan.DownLoader48.61444](#) пытается получить права администратора через использование COM-интерфейса CMSTPLUA, эксплуатируя уязвимость, характерную для некоторых старых COM-интерфейсов.

В случае успеха модифицированная библиотека dropper копируется в каталог %SystemRoot%\System32\wbem в виде файла ATL.dll. После этого [Trojan.DownLoader48.61444](#) запускает системную оснастку управления WMI WmiMgmt.msc. В результате происходит эксплуатация уязвимости DLL Search Order Hijacking в системном приложении mmc.exe, которое автоматически загружает библиотеку %SystemRoot%\System32\wbem\ATL.dll с патчем. Она, в свою очередь, повторно запускает [Trojan.DownLoader48.61444](#), но уже с правами администратора.

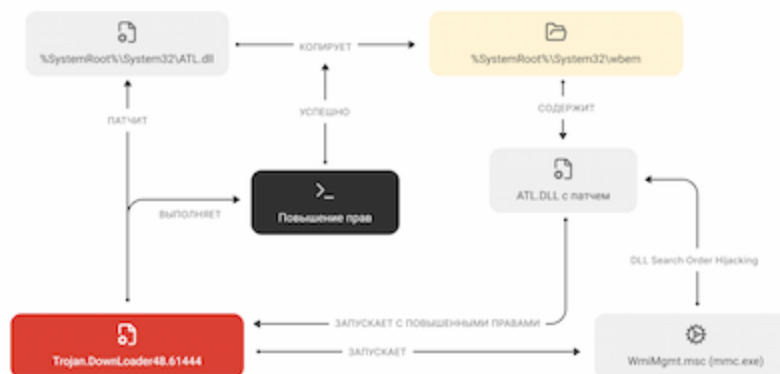


Схема работы [Trojan.DownLoader48.61444](#) при отсутствии прав администратора

При запуске от имени администратора [Trojan.DownLoader48.61444](#) исполняет несколько PowerShell-скриптов для скачивания полезной нагрузки с C2-сервера. Одним из загружаемых объектов является ZIP-архив one.zip. В нем находятся файлы, аналогичные

файлам из архива onedrive.zip из первой цепочки (в частности, легитимная программа OneDrivePatcher.exe и вредоносная библиотека UpdateRingSettings.dll — [Trojan.DownLoader48.54318](#)).

[Trojan.DownLoader48.61444](#) распаковывает архив и в системном планировщике создает задачу на автозапуск OneDrivePatcher.exe при загрузке системы. Троян также непосредственно запускает это приложение. Так же, как и в первой цепочке, при запуске в OneDrivePatcher.exe происходит эксплуатация уязвимости DLL Search Order Hijacking и автоматическая загрузка троянской библиотеки UpdateRingSettings.dll. Далее цепочка заражения повторяет первый сценарий.

При этом [Trojan.DownLoader48.61444](#) скачивает и второй ZIP-архив: two.zip. В нем находится вредоносный скрипт [Python.Downloader.208](#) (update.py), а также файлы, необходимые для его запуска. Среди них — Guardian.exe — переименованный консольный интерпретатор языка Python pythonw.exe.

После распаковки архива [Trojan.DownLoader48.61444](#) создает в системном планировщике задачу на автозапуск Guardian.exe при загрузке системы. Кроме того, он непосредственно исполняет через это приложение вредоносный скрипт [Python.Downloader.208](#).

Частично дублируя первую цепочку заражения, злоумышленники, по всей видимости, стремились повысить вероятность успешной загрузки [Trojan.ChimeraWire](#) в целевые системы.

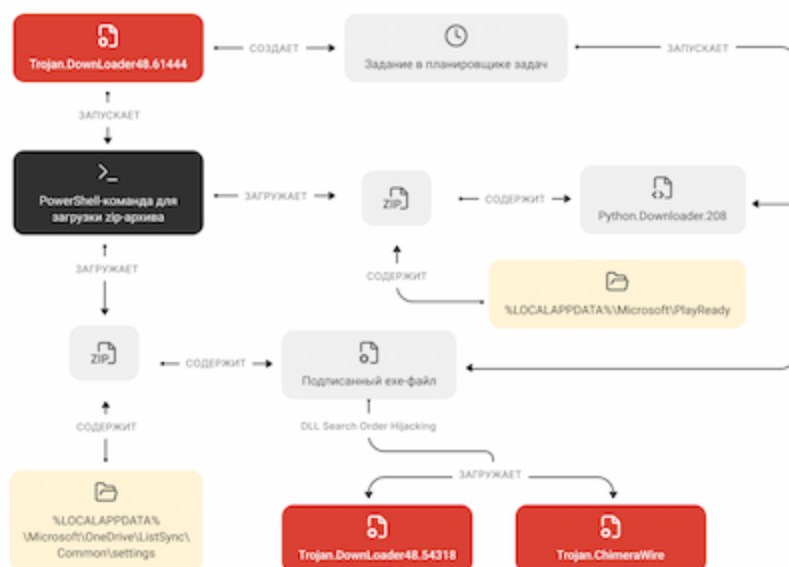
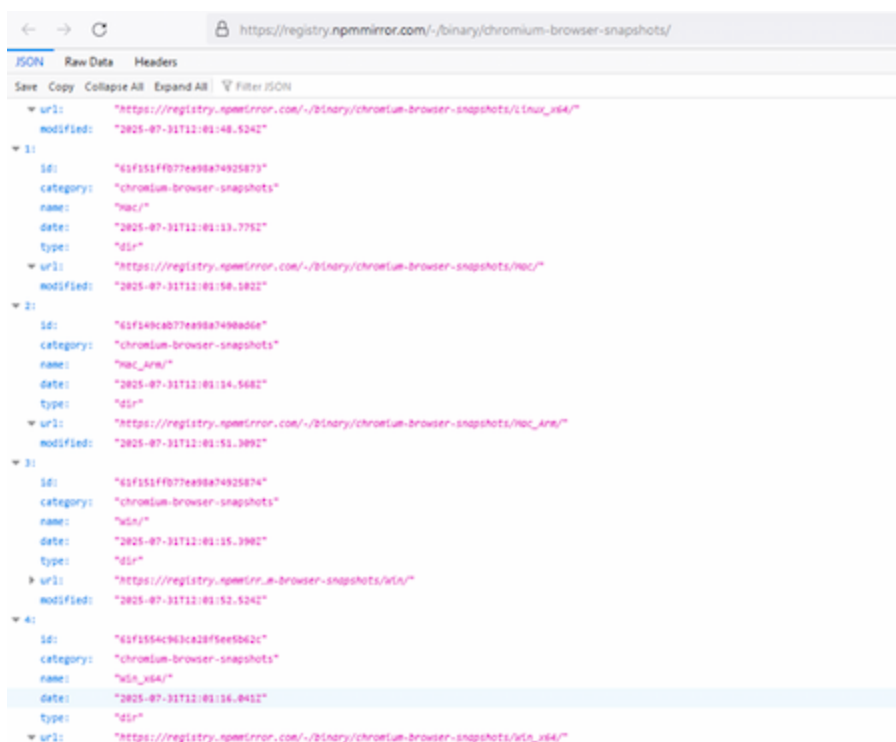


Схема работы [Trojan.DownLoader48.61444](#) с правами администратора

Trojan.ChimeraWire

[Trojan.ChimeraWire](#) получил свое имя на основе сочетания слов «chimera» (в переводе с англ. «химера» — мифическое существо с частями тел нескольких животных) и «wire» (в переводе с англ. «провод»). Слово «chimera» описывает гибридную природу применяемых злоумышленниками методик: использование троянов-загрузчиков, написанных на разных языках, а также антиотладочные техники и эскалация привилегий в процессе заражения. Кроме того, оно отражает то, что троян представляет собой комбинацию различных фреймворков, плагинов и легального ПО, через которое осуществляется скрытое управление трафиком. Отсюда вытекает второе слово «wire»: оно отсылает к невидимой и вредоносной работе трояна с сетью.

Попадая на целевой компьютер, [Trojan.ChimeraWire](#) скачивает со стороннего сайта ZIP-архив chrome-win.zip с браузером Google Chrome для ОС Windows. Отметим, что на этом ресурсе также хранятся архивы со сборками Google Chrome и для других систем, таких как Linux и macOS — в том числе для различных аппаратных платформ.



Сайт с различными сборками браузера Google Chrome, откуда троян загружает необходимый архив

После скачивания браузера [Trojan.ChimeraWire](#) пытается незаметно установить в него расширения NopeCHA и Buster, предназначенные для автоматизированного распознавания капчи (CAPTCHA). Данные расширения будут в дальнейшем использоваться трояном в процессе его работы.

Далее он запускает браузер в режиме отладки без видимого окна, что позволяет выполнять вредоносную деятельность, не привлекая внимания пользователя. После этого происходит подключение к выбранному автоматически порту отладки по протоколу WebSocket.

Вслед за этим троян переходит к получению заданий. Он отправляет запрос на C2-сервер и получает в ответ base64-строку, в которой скрыта зашифрованная алгоритмом AES-GCM конфигурация в формате JSON.

```
[{"\u0434\u0435\u0439\u0441\u0442\u0432\u0438\u0435": "\u0434\u043e\u0436\u0434\u0430\u0442\u044c", "\u0441\u0432\u0435\u0434\u0435\u043d\u0438\u0435": "\u0434\u043e\u0436\u0434\u0430\u0442\u044c 5000-20000 \u0441\u0435\u043a\u0443\u043d\u0434", "\u0434\u043e\u0436\u0434\u0430\u0442\u0435\u043b\u044c\u043d\u043e\u0435 \u0432\u0440\u0435\u043c\u044f": "1-5"}, {"\u0434\u0435\u0439\u0441\u0442\u0432\u0438\u0435": "google", "\u043a\u043b\u044e\u0447\u0435\u0432\u044b\u0435 \u0441\u043b\u043e\u0432\u0430": ["plus size swimwear", "plus size dresses", "plus size bathing suits", "plus size swimsuits"], "\u043c\u0430\u043a\u0441\u0438\u043c\u0430\u043b\u044c\u043d\u043e\u0435 \u043a\u043e\u043b\u0438\u0447\u0435\u0441\u0442\u0432\u043e \u043f\u043e\u043b\u0435\u0447\u0435\u043d\u0438\u044f": 10, "\u0432\u0440\u0435\u043c\u044f \u0441\u043b\u0443\u0447\u0430\u0439\u043d\u043e\u0433\u043e \u043a\u043b\u0438\u043a\u0430": ["1:30", "2:10"], "\u0432\u0440\u0435\u043c\u044f \u043e\u0436\u0438\u0434\u0430\u043d\u0438\u044f \u0434\u043e \u0432\u0435\u0434\u0435\u043d\u0438\u044f \u0432\u0435\u0431-\u0441\u0442\u0440\u0430\u043d\u0438\u0446\u044b": ["380", "500"], "\u0441\u0432\u044f\u0437\u0430\u043d\u043d\u044b\u0435 \u0441\u0441\u044b\u043b\u043a\u0438": ["*bloomchic[.]com/*"]}, {"\u0434\u0435\u0439\u0441\u0442\u0432\u0438\u0435": "google", "\u043a\u043b\u044e\u0447\u0435\u0432\u044b\u0435 \u0441\u043b\u043e\u0432\u0430": ["Semi Auto Hot Foil Stamping Machine", "hot stamping machine", "automatic silk screen press", "best silk screen machine"], "\u043c\u0430\u043a\u0441\u0438\u043c\u0430\u043b\u044c\u043d\u043e\u0435 \u043a\u043e\u043b\u0438\u0447\u0435\u0441\u0442\u0432\u043e \u043f\u043e\u043b\u0435\u0447\u0435\u043d\u0438\u044f": 10, "\u0432\u0440\u0435\u043c\u044f \u0441\u043b\u0443\u0447\u0430\u0439\u043d\u043e\u0433\u043e \u043a\u043b\u0438\u043a\u0430": ["1:60", "2:40"], "\u0432\u0440\u0435\u043c\u044f \u043e\u0436\u0438\u0434\u0430\u043d\u0438\u044f \u0434\u043e \u0432\u0435\u0434\u0435\u043d\u0438\u044f \u0432\u0435\u0431-\u0441\u0442\u0440\u0430\u043d\u0438\u0446\u044b": ["360", "510"], "\u0441\u0432\u044f\u0437\u0430\u043d\u043d\u044b\u0435 \u0441\u0441\u044b\u043b\u043a\u0438": ["*.[.]cn-superfine[.]com/*"]}, {"\u0434\u0435\u0439\u0441\u0442\u0432\u0438\u0435": "google", "\u043a\u043b\u044e\u0447\u0435\u0432\u044b\u0435 \u0441\u043b\u043e\u0432\u0430": ["plus size summer dresses", "plus size swim", "plus size women's clothing", "plus size clothes", "plus size swimwear for women"], "\u043c\u0430\u043a\u0441\u0438\u043c\u0430\u043b\u044c\u043d\u043e\u0435 \u043a\u043e\u043b\u0438\u0447\u0435\u0441\u0442\u0432\u043e \u043f\u043e\u043b\u0435\u0447\u0435\u043d\u0438\u044f": 10, "\u0432\u0440\u0435\u043c\u044f \u0441\u043b\u0443\u0447\u0430\u0439\u043d\u043e\u0433\u043e \u043a\u043b\u0438\u043a\u0430": ["1:60", "2:40"], "\u0432\u0440\u0435\u043c\u044f \u043e\u0436\u0438\u0434\u0430\u043d\u0438\u044f \u0434\u043e \u0432\u0435\u0434\u0435\u043d\u0438\u044f \u0432\u0435\u0431-\u0441\u0442\u0440\u0430\u043d\u0438\u0446\u044b": ["390", "530"], "\u0441\u0432\u044f\u0437\u0430\u043d\u043d\u044b\u0435 \u0441\u0441\u044b\u043b\u043a\u0438": ["*bloomchic[.]com/*"]}, {"\u0434\u0435\u0439\u0441\u0442\u0432\u0438\u0435": "google", "\u043a\u043b\u044e\u0447\u0435\u0432\u044b\u0435 \u0441\u043b\u043e\u0432\u0430": ["silk screen printing machine automatic", "cosmetics printing machines", "hot foil stamping equipment"], "\u043c\u0430\u043a\u0441\u0438\u043c\u0430\u043b\u044c\u043d\u043e\u0435 \u043a\u043e\u043b\u0438\u0447\u0435\u0441\u0442\u0432\u043e \u043f\u043e\u043b\u0435\u0447\u0435\u043d\u0438\u044f": 10, "\u0432\u0440\u0435\u043c\u044f \u0441\u043b\u0443\u0447\u0430\u0439\u043d\u043e\u0433\u043e \u043a\u043b\u0438\u043a\u0430": ["2:70", "3:30"], "\u0432\u0440\u0435\u043c\u044f \u043e\u0436\u0438\u0434\u0430\u043d\u0438\u044f \u0434\u043e \u0432\u0435\u0434\u0435\u043d\u0438\u044f \u0432\u0435\u0431-\u0441\u0442\u0440\u0430\u043d\u0438\u0446\u044b": ["330", "500"], "\u0441\u0432\u044f\u0437\u0430\u043d\u043d\u044b\u0435 \u0441\u0441\u044b\u043b\u043a\u0438": ["*www[.]cn-superfine[.]com/*"]}, {"\u0434\u0435\u0439\u0441\u0442\u0432\u0438\u0435": "google", "\u043a\u043b\u044e\u0447\u0435\u0432\u044b\u0435 \u0441\u043b\u043e\u0432\u0430": ["low cost business ideas", "low risk business ideas", "low cost business opportunities", "low risk businesses", "low cost business to start", "low-cost business ideas with high", "business low cost"], "\u043c\u0430\u043a\u0441\u0438\u043c\u0430\u043b\u044c\u043d\u043e\u0435 \u043a\u043e\u043b\u0438\u0447\u0435\u0441\u0442\u0432\u043e \u043f\u043e\u043b\u0435\u0447\u0435\u043d\u0438\u044f": 10, "\u0432\u0440\u0435\u043c\u044f \u0441\u043b\u0443\u0447\u0430\u0439\u043d\u043e\u0433\u043e \u043a\u043b\u0438\u043a\u0430": ["0:30", "1:10"], "\u0432\u0440\u0435\u043c\u044f \u043e\u0436\u0438\u0434\u0430\u043d\u0438\u044f \u0434\u043e \u0432\u0435\u0434\u0435\u043d\u0438\u044f \u0432\u0435\u0431-\u0441\u0442\u0440\u0430\u043d\u0438\u0446\u044b": ["320", "600"], "\u0441\u0432\u044f\u0437\u0430\u043d\u043d\u044b\u0435 \u0441\u0441\u044b\u043b\u043a\u0438": ["*businessideashunter[.]com/*"]}, {"\u0434\u0435\u0439\u0441\u0442\u0432\u0438\u0435": "\u0434\u043e\u0436\u0434\u0430\u0442\u044c", "\u0441\u0432\u0435\u0434\u0435\u043d\u0438\u0435": "\u0441\u043b\u0443\u0447\u0430\u0439\u043d\u043e\u0435 \u0434\u043e\u0436\u0434\u0430\u0442\u044c 10000 - 60000 \u0441\u0435\u043a\u0443\u043d\u0434", "\u0434\u043e\u0436\u0434\u0430\u0442\u0435\u043b\u044c\u043d\u043e\u0435 \u0432\u0440\u0435\u043c\u044f": "480,1400"}]
```

Пример конфигурации, которую трояну передает C2-сервер

В ней находятся задания и связанные с ними параметры:

- целевая поисковая система (поддерживаются системы Google и Bing);
- ключевые фразы для поиска сайтов в заданной поисковой системе и их последующего открытия;
- максимальное количество последовательных переходов по веб-страницам;
- случайные распределения для выполнения автоматических кликов на веб-страницах;
- время ожидания загрузки страниц;
- целевые домены.

Для дополнительной имитации деятельности реального человека и обхода систем, отслеживающих постоянную активность, в конфигурации также предусмотрены параметры, отвечающие за паузы между сессиями работы.

Имитация кликов мышью пользователем

[Trojan.ChimeraWire](#) способен выполнять клики следующих видов:

- для навигации по поисковой выдаче;

- для открытия найденных релевантных ссылок в новых фоновых вкладках.

Вначале [Trojan.ChimeraWire](#) через нужную поисковую систему выполняет поиск сайтов по доменам и ключевым фразам, указанным в конфигурации. Далее он открывает полученные в поисковой выдаче сайты и находит на них все HTML-элементы, которые определяют гиперссылки. Троян помещает их в массив данных и перемешивает его, чтобы объекты в нем располагались в последовательности, отличной от последовательности на веб-странице. Это делается для обхода антибот-защиты сайтов, которая может отслеживать порядок нажатий.

Затем [Trojan.ChimeraWire](#) проверяет, работоспособны ли найденные ссылки и совпадают ли строки в них с заданным шаблоном из конфигурации, после чего подсчитывает общее количество совпадений. Дальнейшие действия трояна зависят от получившегося числа.

Если на странице было выявлено достаточное количество подходящих ссылок, [Trojan.ChimeraWire](#) сканирует страницу и сортирует найденные ссылки по релевантности (наиболее соответствующие ключевым словам ссылки идут первыми). После этого выполняется клик по одной или нескольким подходящим ссылкам.

Если же совпадений с заданным шаблоном недостаточно или их нет вовсе, вредоносная программа использует алгоритм с вероятностной моделью поведения, который максимально имитирует действия настоящего пользователя. На основе параметров из конфигурации при помощи взвешенного случайного распределения [Trojan.ChimeraWire](#) определяет количество ссылок, по которым необходимо перейти. Например, распределение ["1:90", "2:10"] означает, что [Trojan.ChimeraWire](#) кликнет 1 ссылку с вероятностью 90%, и 2 ссылки — с вероятностью 20%. Таким образом, с большой долей вероятности вредоносная программа должна перейти по одной ссылке. Троян случайным образом выбирает ссылку из составленного ранее массива и выполняет клик.

После каждого перехода по ссылке из поисковой выдачи и выполнения кликов на загружаемой странице троян, в зависимости от задачи, возвращается на предыдущую вкладку или переходит к следующей. Алгоритм действий повторяется до тех пор, пока не будет исчерпан лимит по кликам для целевых веб-сайтов.

Ниже представлены примеры сайтов, параметры для взаимодействия с которыми поступали трояну в заданиях от C2-сервера:



Shenfe

The World's No.1 Trade Fair for Plastics and Rubber

2025 8-15 October Düsseldorf, Germany

Hall 04 4C58

Featured Products

8-25MM Three Color Ink Printing Machine For Cosmetic Pen Barrels

Automatic Varnishing High Speed Screen Printing Machine For 30mm Tube

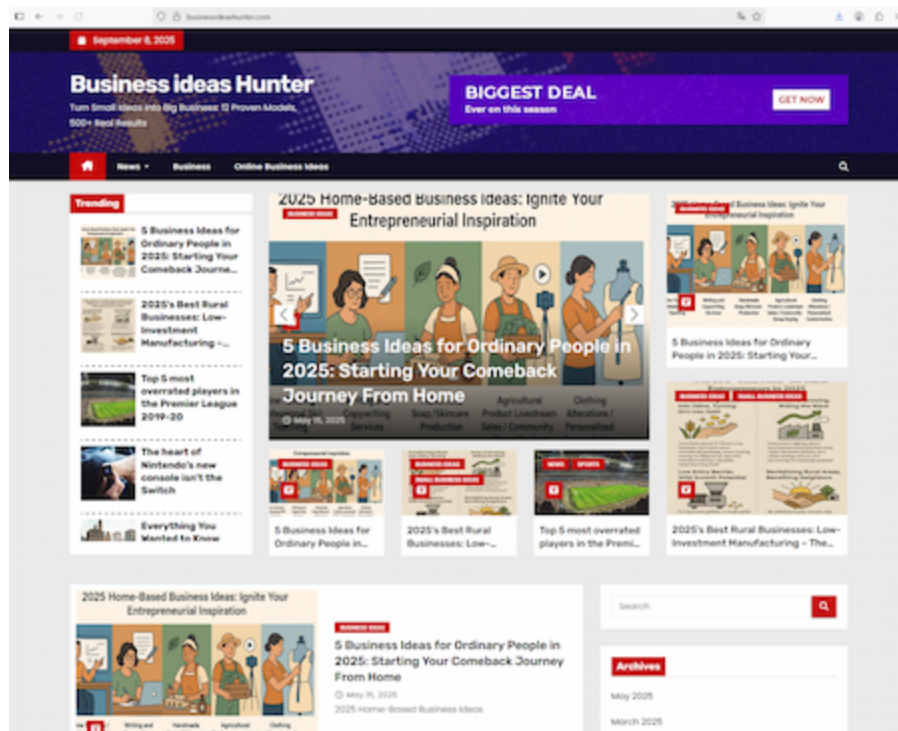
Chat Now

Chat Now

shenfe

Good day, what product are you looking for?

Type a message



Подробные технические описания трояна **ChimeraWire** и вредоносных программ, участвующих в его загрузке, находятся в PDF-версии исследования и в вирусной библиотеке компании «Доктор Веб».

Подробнее о [Trojan.ChimeraWire](#)

Подробнее о [Trojan.DownLoader48.54600](#)

Подробнее о [Trojan.Starter.8377](#)

Подробнее о [Python.Downloader.208](#)

Подробнее о [Trojan.DownLoader48.54318](#)

Подробнее о [Trojan.DownLoader48.61444](#)

Заключение

В настоящее время вредоносная деятельность [Trojan.ChimeraWire](#) фактически сводится к выполнению относительно простых задач кликера по накрутке популярности веб-сайтов. Вместе с тем, функциональные возможности лежащих в его основе утилит позволяют трояну решать более широкий спектр задач — в том числе совершать автоматизированные действия под видом активности настоящих пользователей. Так, с его помощью злоумышленники могут заполнять веб-формы — например, на сайтах, проводящих опросы в рекламных целях. Кроме того, они могут использовать его для считывания содержимого веб-страниц и создания их скриншотов — как с целью кибершпионажа, так и для автоматического сбора информации для наполнения различных баз данных (например, с почтовыми адресами, номерами телефонов и т. п.).

Таким образом, в будущем возможно появление новых версий [Trojan.ChimeraWire](#), где эти и другие функции будут реализованы в полной мере. Специалисты компании «Доктор Веб» продолжают следить за развитием этого трояна.

MITRE ATT&CK®

Мы проанализировали [Trojan.ChimeraWire](#) по фреймворку MITRE ATT&CK®, который представляет собой матрицу с описанием тактик и техник киберпреступников, атакующих информационные системы. В результате были выявлены следующие ключевые техники:

Этап	Техника
Выполнение	Выполнение с участием пользователя (T1204) Вредоносный файл (T1204.002) Вредоносная библиотека (T1204.005) PowerShell (T1059.001) Командная оболочка Windows (T1059.003) Visual Basic (T1059.005) Python (T1059.006) Планировщик заданий Windows (T1053.005)
Закрепление	Ключи запуска в реестре Windows / Каталог автозагрузки (T1547.001) Запланированная задача / задание (T1053)
Повышение привилегий	Перехват потока исполнения: перехват поиска DLL (T1574.001) Обход контроля учетных записей (T1548.002)
Предотвращение обнаружения	Зашифрованный / закодированный файл (T1027.013) Уклонение от отладки (T1622) Скрытое окно (T1564.003) Исключения для файла или пути (T1564.012) Деобфускация / декодирование файлов или данных (T1140) Перехват потока исполнения: перехват поиска DLL (T1574.001)
Организация управления	Двусторонняя связь (T1102.002) Веб-протоколы (T1071.001)

[Индикаторы компрометации](#)

0

Последние новости [Все новости](#)

Горячая лента угроз

[Читать](#)

Черная пятница: скидка 40% на комплексную защиту Dr.Web

Об акциях

[Читать](#)

Dr.Web CureIt! теперь видит то, что пытается скрыть вредоносное программное обеспечение

Об обновлениях | О продуктах Dr.Web

[Читать](#)