Научная статья
doi: 10.29039/2312-7937-2024-1-101-106

ПОЗДЫШЕВ РОМАН СЕРГЕЕВИЧ
Нижегородская академия МВД России (Нижний Новгород, Россия)

rmanpzdyshev@rambler.ru

Активная деанонимизация личности преступника в сети Интернет с использованием canarytokens

Аннотация. В статье рассматривается возможность использования интернет-ресурса canarytokens.org для активной деанонимизации личности преступника в сети Интернет. В ходе исследования раскрыт принцип работы, а также сформулирован алгоритм формирования и направления токенов и анализа информации, получаемой после их срабатывания. Исследованы особенности работы canarytokens как в обычных условиях настройки пользовательского оборудования, так и при использовании средств повышения анонимности в компьютерной сети. Приведены авторские размышления о формах использования canarytokens в ходе расследования преступлений. В заключении сделаны выводы о преимуществах и недостатках рассмотренного метода установления личности пользователя сети Интернет. К первым относятся: оперативность получения информации даже в тех случаях, когда преступником используются интернет-ресурсы, находящиеся вне юрисдикции Российской Федерации; получение сведений не только об IP-адресе, но и о программно-аппаратных характеристиках используемого компьютерного устройства; возможность получения сведений, имеющих значение для уголовного дела, в случаях, когда преступником используется VPN-сервис. Недостатком является низкая эффективность при использовании преступником Tor-браузера.

Ключевые слова и словосочетания: деанонимизация, киберпреступления, IP-логгер, canarytokens, токен, ip-адрес, отпечаток браузера.

Для цитирования: *Поздышев Р.С. Активная деанонимизация личности преступника в сети Интернет с использованием canarytokens // Вестник ВИПК МВД России. – 2024. – № 1 (69). – С. 101-106; doi: 10.29039/2312-7937-2024-1-101-106*

POZDYSHEV ROMAN S.
Nizhny Novgorod academy of the Ministry of internal affairs of Russian Federation
(Nizhny Novgorod, Russia)

ACTIVE DEANONYMIZATION OF A CRIMINAL'S IDENTITY ON THE INTERNET USING CANARYTOKENS

Annotation. The article discusses the possibility of using the Internet resource canarytokens.org for active de-anonymization of the identity of a secure network on the Internet. A study of the features of setting up the work of canarytokens both in normal conditions of user equipment and when using means of increased anonymity in a computer network. The author's thoughts on the forms of using canarytokens during the investigation of crimes are given. In conclusion, outcomes are drawn about the advantages and disadvantages of the considered method of identifying an Internet user. The first include: the efficiency of obtaining information even in cases where the criminal uses Internet

resources that are outside the jurisdiction of the Russian Federation; obtaining information not only about the IP address, but also about the software and hardware characteristics of the computer device used; the ability to obtain information relevant to a criminal case in cases where a criminal uses a VPN service. The disadvantage is the low efficiency when a criminal uses the Tor browser.

Key words and word combinations: deanonymization, cybercrime, IP logger, canarytokens, token, ip address, browser fingerprint

For citation: *Pozdyshev R.S. Active deanonymization of a criminal's identity on the internet using canarytokens // Vestnik Advanced Training Institute of MIA of Russia. – 2024. – № 1 (69). – P. 101-106; doi: 10.29039/2312-7937-2024-1-101-106*

Внедрение информационно-телекоммуникационных технологий в жизнь людей, как и любое изменение, привносит не только положительный эффект, но имеет некоторые отрицательные последствия. Криминальный мир вооружается такими технологиями зачастую быстрее, чем их осваивают правоохранительные органы. Количество преступлений, совершаемых в Российской Федерации (далее – РФ) с использованием информационно-телекоммуникационных технологий (далее – ИТТ), ежегодно возрастает, а их способы становятся все более изощренными. В 2017 г. их число увеличилось на 37,4% (90 587); рост в 2018 г. – на 92,8% (174 674); в 2019 г. – на 68,5% (294 409); в 2020 г. – на 73,4% (510 396); в 2021 г. – на 1,4% (517 722); 2022 г. – на 0,8% (522 065); в 2023 г. – на 29,7% относительно аналогичного периода прошлого года (676 951) [1]. Преступность в сфере ИТТ занимает одну третью долю от всей преступности в стране. При этом следует заметить, что это данные официальной статистики, где учтены только зарегистрированные преступления.

Одними из преимуществ ИТТ, привлекающих криминальные элементы, являются возможность дистанционного совершения преступлений и сокрытие реальной личности субъекта преступления за цифровой личностью. Таким образом, к основной сложности, с которой сталкиваются правоохранительные органы в данной сфере, следует отнести деанонимизацию пользователей компьютерных сетей. В данном контексте ключевой представляется информация об адресах устройств, связанных с пользователем, в сети Интернет (IP-адресах).

Базовые методы работы с подобной информацией достаточно давно усвоены сотрудниками органов внутренних дел РФ и заключаются в стандартном алгоритме истребования сведений: администратор интернет-ресурса – интернет-провайдер – конкретный пользователь. Данный алгоритм является реализацией пассивной формы деанонимизации, когда следователем исследуются уже оставленные следы и непосредственного взаимодействия с интересующим лицом не происходит. Такая форма является вполне эффективной, однако имеет свои недостатки. Во-первых, получение ответов от администратора интернет-ресурса и интернет-провайдера может занимать длительное время, как показывает практика, до нескольких месяцев. Во-вторых, в некоторых случаях могут возникать непреодолимые трудности, когда интернет-ресурс или интернет-провайдер находятся вне юрисдикции РФ. Вышеуказанных недостатков лишены активные формы деанонимизации, примерами которых являются использованием программ типа IP-логгер[1] или canarytokens[2]. IP-логгер позволяет подготовить URL-ссылку, в случае перехода по которой может быть установлен IP-адрес пользователя. Успешные случаи применения данного метода имеются в практике органов внутренних дел.

В производстве следственных подразделений ГСУ ГУ МВД России по Ставропольскому краю находилось уголовное дело № 12201070070020050, возбужденное 11 января 2022 г. по признакам преступления, предусмотренного ч. 2 ст. 207 Уголовного кодекса Российской Федерации, по факту поступления с электронного адреса kikolomanniu@protonmail.com на

[1]Например: https://iplogger.org/ru/; https://www.getnotify.com/; https://grabify.com и др.

[2] Canarytokens.org.

электронную почту ФСБ России сообщения о минировании здания МАОУ Гимназия № 24 в г. Ставрополе. В ходе расследования на вышеуказанный адрес электронной почты, используемый в преступных целях, была направлена ссылка, сформированная программой IP-логгер, по которой перешел преступник, тем самым раскрыв информацию о своем IP-адресе. Благодаря данным действиям к уголовной ответственности были привлечены два лица за совершение 27 аналогичных преступлений [2].

В ходе настоящего исследования проводились интервьюирование и анкетирование 96 сотрудников органов внутренних дел РФ, деятельность которых связана с раскрытием и расследованием преступлений, совершаемых с использованием информационно-телекоммуникационных технологий. Только 15 респондентов были осведомлены о возможностях программ типа IP-логгер и 3 – о canarytokens. При этом случаев использования canarytokens в оперативно-служебной деятельности не было установлено. В связи с данными обстоятельствами представляется небезынтересным рассмотрение функционала данного интернет-ресурса в разрезе противодействия преступности.

Canarytokens представляет собой веб-сервис или программное обеспечение, который формирует специальные интернет-ссылки или файлы для последующего их размещения на цифровом ресурсе любым способом: на веб-сайте, в сообщении мессенджера, в электронном письме и др. Когда пользователь переходит по такой ссылке или открывает файл с кодом, фиксируется его IP-адрес и информация в отношении программно-аппаратных характеристик используемого компьютерного устройства.

Шаг первый: создание токена (рис. 1). При создании токена нужно выбрать его тип. Им может быть URL-адрес веб-ресурса, файл Microsoft Office, PDF-документ, изображение, QR-код и др. Выбор типа зависит от обстоятельств, сложившихся в ходе расследования преступления. При этом целесообразно обеспечить, чтобы пользователь не осознал, что таким образом пытаются установить его личность. Это может быть изображение чека, направляемое преступнику в подтверждение осуществленной банковской транзакции, или ссылка на веб-сайт школы для заказа ложного сообщения о готовящемся террористическом акте. Далее необходимо указать адрес электронной почты, на который будет приходить информация о срабатывании токена.

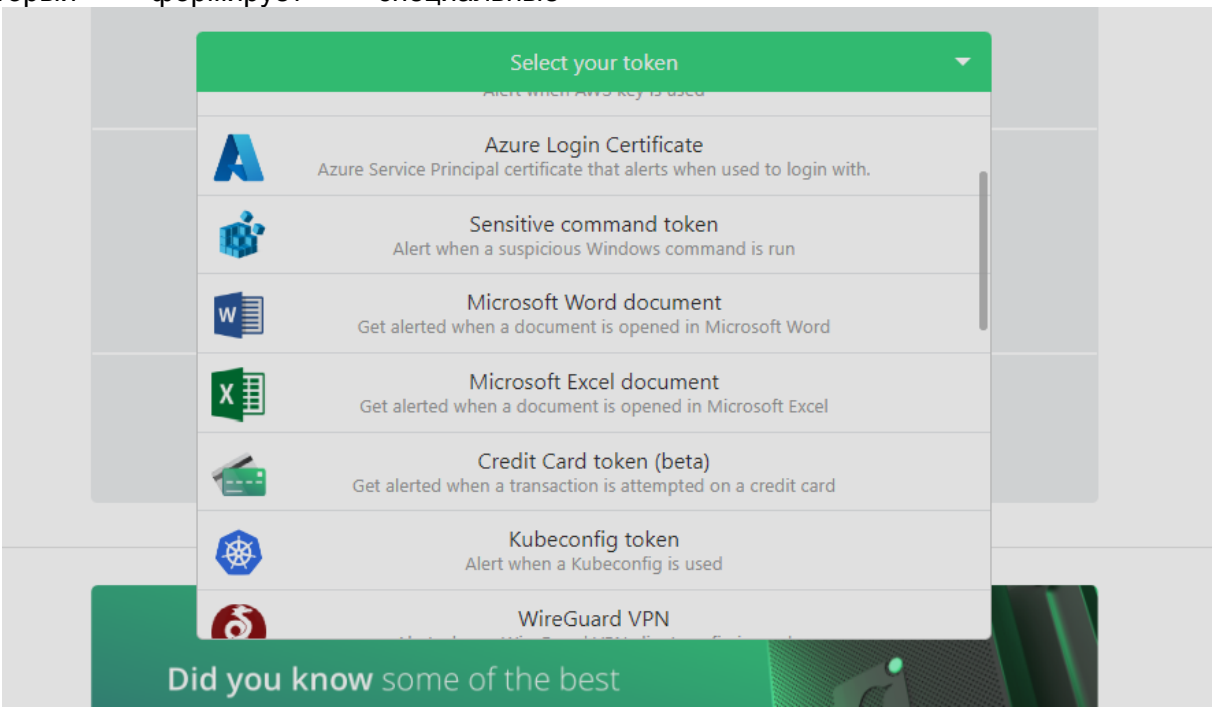
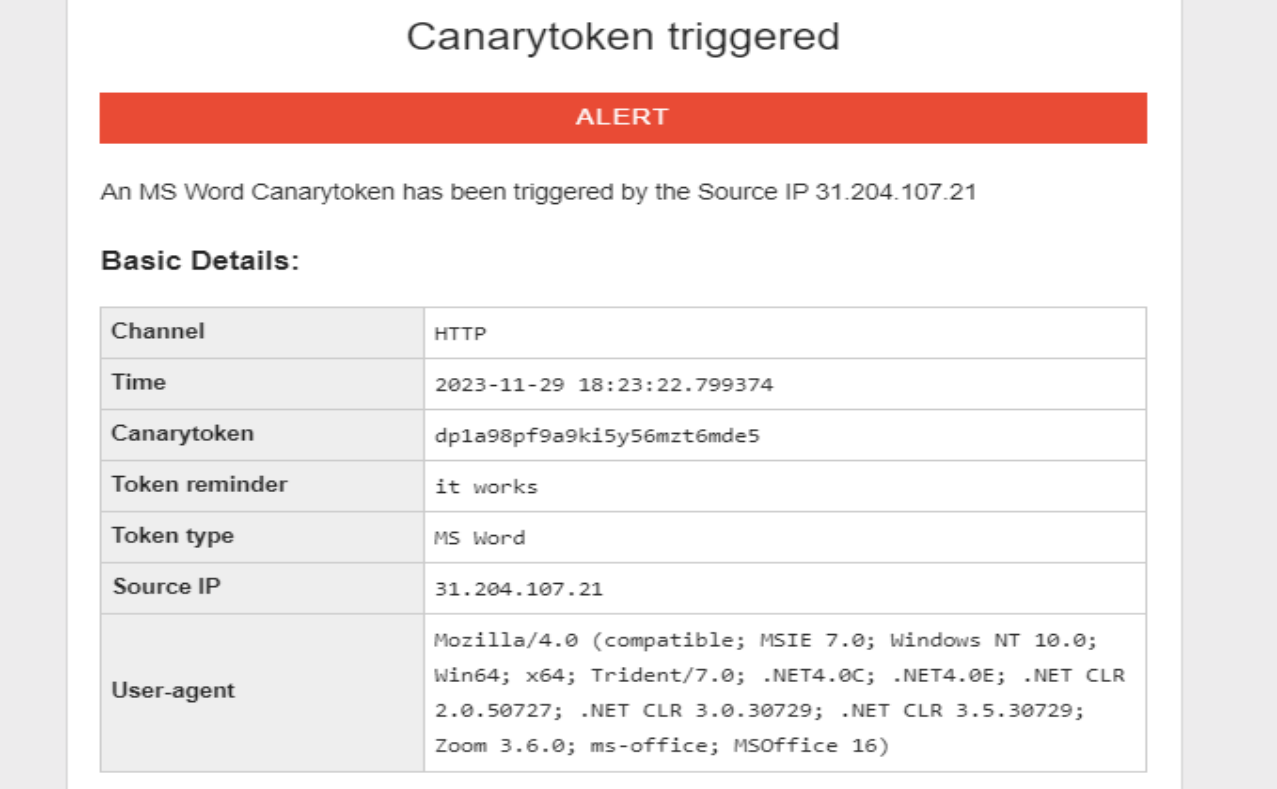


Рис. 1. *Выбор типа canarytokens*

Шаг второй: направление токена. Способ направления токена зависит от следственной ситуации и от того, по каким средствам связи осуществляется коммуникация с преступником. Зачастую это может быть электронная почта, мессенджер, социальная сеть или SMS-сообщение. Перед направлением ссылки преступнику следует ее протестировать на устройствах, находящихся в пользовании инициатора этой процедуры. Некоторые особенности могут быть обнаружены при использовании мессенджеров и социальных сетей. В ряде случаев, когда в качестве токена выступает не файл, а интернет-ссылка, мессенджер автоматически проверяет поступившую ссылку и получивший ее пользователь увидит не только ее текстовое наименование, но и эмблему веб-сайта, на котором она была создана, например canarytokens.org. Это будет выглядеть подозрительно и существенно снижать вероятность срабатывания токена.

Шаг третий: анализ полученной информации (рис. 2, 3). В случае срабатывания токена орган следствия может получить не только IP-адрес пользователя, но и иную информацию, имеющую значение для уголовного дела. В информации присутствуют наименование интернет-провайдера, страна и предполагаемый населенный пункт места нахождения пользователя. Информация о населенном пункте может быть не точной, поскольку она относится к интернет-провайдеру, который может распределять IP-адреса на территории нескольких регионов. Эти сведения будут соответствовать действительности, только если интернет-провайдер работает на территории одной административно-территориальной единицы. В информации о срабатывании токена также будут содержаться сведения о часовом поясе, дате, времени и установленном языке на компьютерном устройстве. Важное значение будут иметь программно-аппаратные характеристики данного устройства пользователя. К ним относятся: размер экрана, марка и модель графического процессора, операционная система, веб-браузер и его версия, а также пользовательский агент (useragent) – идентификационная строка клиентского оборудования. Кроме того, могут содержаться сведения о наличии сенсорного дисплея, установленном в веб-браузере блокировщике рекламы, работе в режиме инкогнито и др. Объем и качество полученной информации зависят от типа токена и уровня приватности компьютерного устройства пользователя. Например, при направлении токена – файла MicrosoftWord – может быть получена информация о наименовании и версии программы, с помощью которой пользователь открыл файл на своем устройстве. А при направлении токена – URL-ссылки – может быть получена информация о размерах экрана устройства, наименовании и версии браузера, установленных расширениях.



Canarytoken triggered

ALERT

An MS Word Canarytoken has been triggered by the Source IP 31.204.107.21

Basic Details:

Channel	HTTP
Time	2023-11-29 18:23:22.799374
Canarytoken	dp1a98pf9a9ki5y56mzt6mde5
Token reminder	it works
Token type	MS Word
Source IP	31.204.107.21
User-agent	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729; Zoom 3.6.0; ms-office; MSOffice 16)

Рис. 2. *Пример информации, полученной при срабатывании токена*

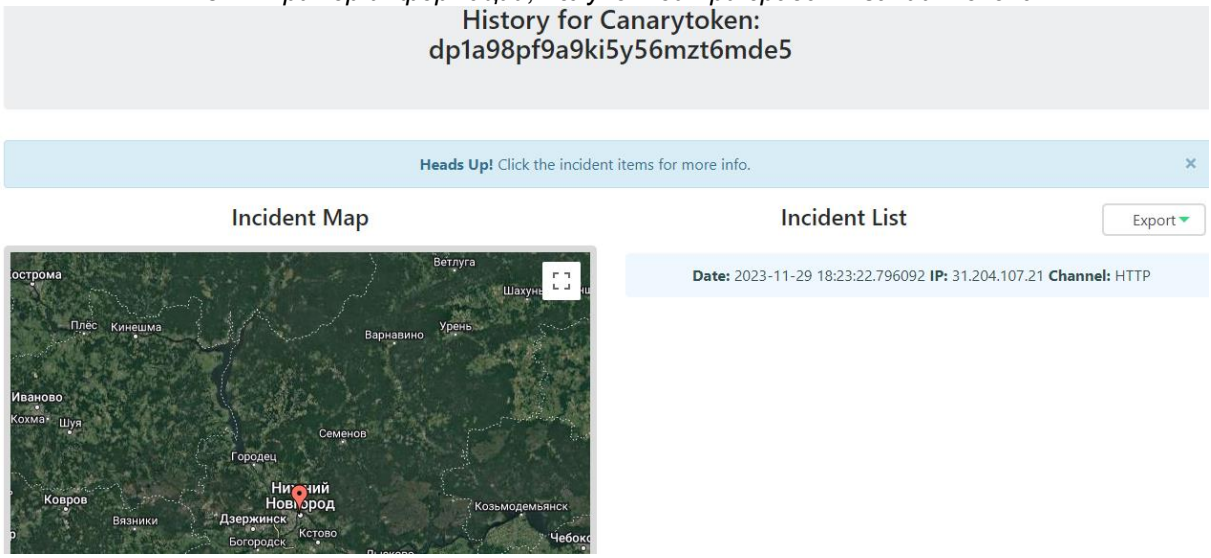


Рис. 3. *Пример информации, полученной при срабатывании токена*

Шаг четвертый: работа с полученной информацией. Процессуальные действия по установлению личности пользователя по IP-адресу неоднократно рассматривались в учебной и научной литературе [3], поэтому в рамках настоящей статьи акцент сделан на работу с иной вышеуказанной информацией. Пользовательский агент может быть представлен в следующем виде: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, likeGecko) Chrome/116.0.5845.967 YaBrowser/23.9.1.967 Yowser/2.5 Safari/537.36. При использовании открытых источников, например https://useragents.io, по пользовательскому агенту можно провести парсинг и получить информацию о наименовании и версии веб-браузера, операционной системе и ее битности, типе компьютерного устройства (смартфон, планшет, компьютер и др.), включении Javascript, CSS, Cookiesи др. Данная информация может быть использована для разработки криминалистических версий, для установления личности пользователя наравне с IP-адресом. Такие сведения называются цифровыми отпечатками или отпечатками браузера (BrowserFingerprints). Они передаются веб-браузером при каждом обращении на веб-сайт для того, чтобы он адаптировал свое содержимое под требования устройства пользователя. Отпечатки браузера используются администраторами веб-сайта в целях настройки рекламы для идентификации пользователей и работают даже в тех случаях, когда cookie-файлы отключены [4, с. 50-53].

Интересным в рамках рассматриваемой темы представляются особенности работы canarytokens в случаях, когда преступником используются такие популярные средства повышения анонимности в сети, как VPN-сервисы и Tor-браузер [4, с. 50-53]. В ходе исследования проведены эксперименты, которые привели к следующим результатам. При использовании VPN-сервиса при срабатывании токена можно получить IP-адрес данного сервиса, а не самого пользователя, но остальная информация передается в соответствующем действительности виде. В таких случаях сведения об отпечатках браузера имеют повышенное значение. При использовании Tor-браузера IP-логгер получает значительно меньше информации. В таких случаях может быть установлен IP-адрес выходной ноды сети Tor и факт использования данной сети, что, очевидно, является недостаточным для эффективной работы с отпечатками браузера.

Рассмотрев технические особенности функционирования canarytokens, следует затронуть процессуальные аспекты их использования в расследовании преступлений. Поскольку этот метод активной деанонимизации личности преступника является относительно новым в арсенале правоохранительных органов и редким в использовании, однозначная практика его применения еще не

сформирована. Представляется, что в данном контексте есть два направления.

Первое направление – использование инструментария органа дознания. В данном случае следователь дает поручение о производстве оперативно-розыскных мероприятий, результаты которых в последующем предоставляются в орган предварительного следствия.

Второе направление – производство следственных действий. Стоит повторится, что данный вопрос является дискуссионным, однако представляется возможным использование данного метода в рамках осмотра или следственного эксперимента. В этом случае целесообразно привлекать специалиста, которого в последующем необходимо допрашивать с выяснением механизма работы canarytokens для подтверждения достоверности полученных доказательств.

Оба варианта имеют право на существование и выбор конкретного из них зависит от множества факторов: уровня подготовки следователя и сотрудника органа дознания, наличия специалиста, позиции прокуратуры и др.

Резюмируя изложенное, следует заключить, что canarytokens служит эффективным средством активной деанонимизации личности преступника в сети Интернет. Преимуществами являются: оперативность получения информации даже в тех случаях, когда преступником используются интернет-ресурсы, находящиеся вне юрисдикции РФ; получение сведений не только об IP-адресе, но и о программно-аппаратных характеристиках используемого компьютерного устройства; возможность получения сведений, имеющих значение для уголовного дела, в случаях, когда преступником используется VPN-сервис. К недостаткам можно отнести низкую эффективность при использовании преступником Tor-браузера. Однако следует заметить, что это все же является в большей степени не отрицательной характеристикой IP-логгера, а особенностью работы вышеуказанного веб-браузера и сети Tor.

1. Состояние преступности [Электронный ресурс] // URL: https://мвд.рф/reports (дата обращения: 13.02.2024).
2. О направлении информации о положительном опыте: письмо Следственного департамента МВД России от 5 июня 2023 г. № 17/1-18806.
3. Расследование преступлений в сфере компьютерной информации и иных преступлений, совершаемых с использованием информационно-телекоммуникационных технологий: учеб. пособие / Р.С. Поздышев, А.Е. Васильев, А.Г. Саакян [и др.]. – Н. Новгород: Нижегородская академия МВД России, 2023.
4. Поздышев Р.С. Деанонимизация личности преступника в сети Интернет // Вестник Уральского юридического института МВД России. 2022. № 2 (34).

Информация об авторе:

Р.С. Поздышев, *заместитель начальника кафедры предварительного расследования, кандидат юридических наук*

About the author:

R.S. Pozdyshev*, deputy chief of the chair of preliminary investigation, candidate of law science*

Статья поступила в редакцию 15.02.2024