АНАЛИЗ РАБОТЫ СЕТИ С ЛУКОВОЙ МАРШРУТИЗАЦИЕЙ В РАМКАХ ПОИСКА СКРЫТЫХ СЕРВИСОВ ПО ПРОДАЖЕ И ПОКУПКЕ ВРЕДОНОСНОГО ПРОГРАММНОГО КОДА ДЛЯ ВЗЛОМА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ВОЗДУШНОГО СУДНА

ANALYSIS OF ONION NETWORK IN THE SEARCH FOR HIDDEN SERVICES FOR THE SALE AND PURCHASE OF EXPLOITS TO BREAK INTO AVIATION SOFTWARE

K. Nikolaev

Summary. In the modern world, the problem of personal data protection is becoming more and more urgent, in connection with this, various anonymizers are gaining popularity, allowing them to hide their location on the network, VPN networks that allow you to connect from a certain country or even a city and an onion routing network. The main representative of networks with onion routing is the network The Onion Router. Monthly the number of active users of this network exceeds 3 million people, and the number of servers serving this network exceeds 8,000. [1] This article examines the network with onion routing The Onion Router, the principles of its operation and the principles of the operation of hidden services within this network. The article deals with the problem of searching for hidden services for hacking the software of aircraft with the help of the modified client of The Onion Router network. During the research, it was revealed the possibility of finding hidden services in TheOnionRouter network, including shops selling malicious code.

Keywords: The Onion Router, TOR, hidden service, onion routing, exploits, operation systems of aircraft.

Николаев Кирилл Андреевич
Аспирант, Московский государственный технический университет гражданской авиации, г. Москва, Россия
Kirill.a.nikolaev@yandex.ru

Аннотация. В современном мире становится все более актуальной проблема защиты персональных данных, в связи с этим все большую популярность приобретают различные анонимайзеры, позволяющие скрыть свое местоположение в сети, сети VPN, позволяющие подключиться из определенной страны или даже города и сети луковой маршрутизации. Главным представителем сетей с луковой маршрутизацией является сеть TheOnionRouter. Ежемесячно число активных пользователей данной сети превышает 3 млн. человек, а количество обслуживающих серверов данной сети превышает 8 тысяч. Данная статья рассматривает сеть с луковой маршрутизацией The Onion Router, принципы ее работы и принципы работы скрытых служб внутри этой сети. В статье рассматривается проблема поиска скрытых сервисов в данной сети, в частности сервисы для взлома программного обеспечения воздушных судов. В ходе исследования была выявлена возможность нахождения скрытых сервисов в сети TheOnionRouter, в том числе магазинов по продаже вредоносного кода.

Ключевые слова: The Onion Router, TOR, скрытые службы, луковая маршрутизация, эксплойты, программное обеспечение воздушного судна.

Введение

Авиационная отрасль предъявляет повышенные требования к программному обеспечению воздушных судов (ВС.), которое на данный момент управляет всеми функциями воздушных судов в воздухе и на земле. Операционные системы, работающие на воздушных судах, являются операционными системами реального времени, которые не допускают задержек времени реакции на прерывания и могут обеспечивать реализацию заданной частоты приема внешних данных и выдачи результатов.

Но даже в таких операционных системах с многоступенчатой разработкой и множественными проверками могут встречаться ошибки, которыми могут воспользоваться Злоумышленники для захвата воздушных судов или создания ошибок, возникновение которых может причинить ущерб отдельному воздушному судну или целому классу судов.[1, стр. 15]

В последнее время нашло применение использование луковой маршрутизации. Луковая маршрутизация — это технология, которая позволяет проводить через компьютерную сеть анонимный обмен информацией. Сообщения, передаваемые от отправителя к получателю, многократно шифруются и отсылаются через ряд сетевых узлов, которые называются луковыми маршрутизаторами. Каждый луковый маршрутизатор (узел) удаляет слой шифрования, чтобы открыть заголовок пакета, в котором находятся данные об адресе следующего узла и отослать на следующий адрес, где другой маршрутизатор делает то же самое, при этом у каждого маршрутизатора имеется ключ только к своему слою шифрования.

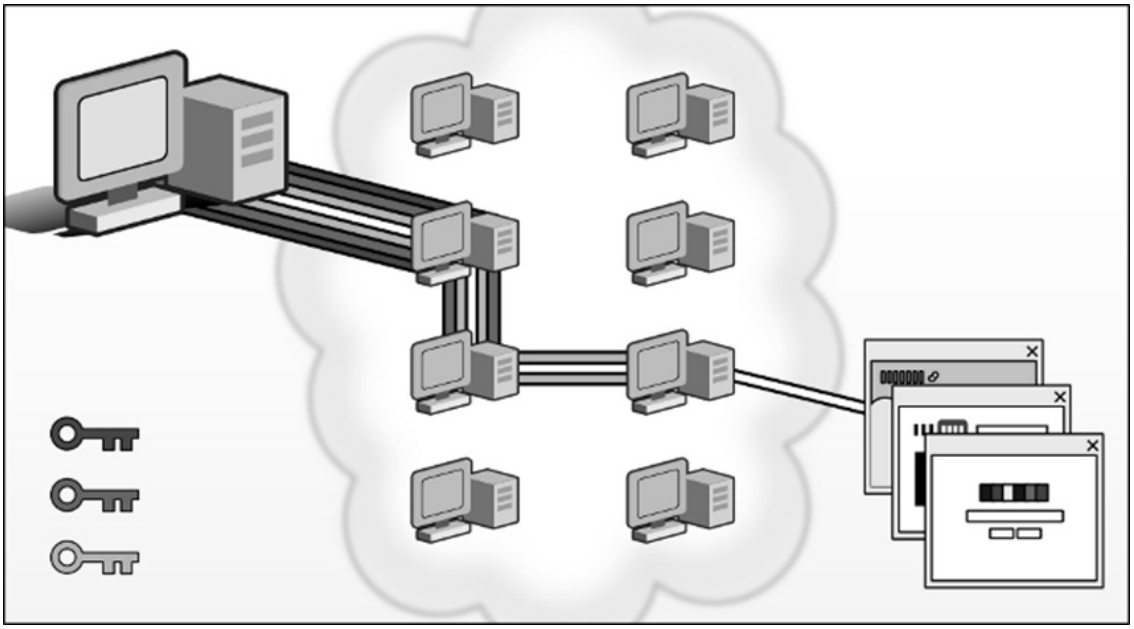

Рис. 1. Принцип работы сети TOR

Таким образом, никакие промежуточные узлы не могут узнать местонахождение отправителя и получателя и текст передаваемого сообщения.

Луковая маршрутизация была разработана в 90 годах в управлении перспективных исследовательских проектов Министерства обороны США. Тогда же было введено понятие луковой маршрутизации. [2]

Для луковой маршрутизации чаще всего используется свободно распространяемое программное обеспечение The Onion Router (TOR). Это открытое и свободно распространяемое программное обеспечение для реализации луковой маршрутизации второго поколения.

TOR — это сервис, который защищает анонимность участников сети, пока используется сеть Интернет. Эта сеть состоит из двух частей:

1. Сеть из компьютеров добровольцев, которые делают возможной работу этой сети. Эта система компьютеров работает в качестве прокси-серверов и позволяет устанавливать сетевое анонимное соединение, при этом данное соединение будет защищённым от прослушивания. Сеть рассматривается в качестве анонимной сети виртуальных туннелей, которые предоставляют передачу данных в зашифрованном виде. [3]

Программного обеспечения в виде браузера, который каждый пользователь сети может скачать и анонимно пользоваться глобальной сетью. При этом официальный браузер основан на базе браузера Firefox, в который уже встроен клиент сети TOR и различный дополнительный функционал для сохранения приватности участников сети. Также существуют различные веб браузеры от сторонних разработчиков под разные платформы, такие, как Linux, Android, IOS и другие. [4,5]

С помощью данной сети пользователи могут сохранять анонимность в Интернете при отправке различных сообщений, посещении сайтов, а также при работе с другими приложениями, использующими протокол TCP.

Сетевые узлы сети TOR

Рассмотрим подробнее сетевые узлы сети TOR. Анонимизация трафика обеспечивается за счёт использования распределённой сети серверов — узлов, что представлено на рис. 1.

Технология распределенной сети узлов обеспечивает защиту от анализа трафика, который ставит под угрозу не только анонимность в глобальной сети, но также конфиденциальность деловых контактов, коммерческих тайн и тайну связи в целом.

Сеть TOR работает с сетевыми уровнями onion-маршрутизаторов и позволяет обеспечивать анонимные исходящие соединения и анонимные скрытые службы. Рассмотрим более подробно виды узлов сети. Узлы сети TOR, также называемые маршрутизаторами или нодами, принимают трафик сети и посылают его далее. Существует несколько видов узлов сети TOR, к основным относят мосты, выходные и посреднические ноды.

Для обеспечения безопасности, весь трафик в сети TOR проходит минимум через три узла, перед тем как достигнуть точки назначения. Первые два узла являются посредническими, они только получают трафик и пересылают его дальше. Чем больше количество посреднических узлов, тем выше скорость и надежность сети TOR, при этом, трафик, проходя через данные узлы, не делает владельца данных узлов похожим на владельца источника данного трафика. Данные узлы говорят о своем присутствии всем пользователям сети, чтобы любой пользователь мог беспрепятственно подключаться к посредническому узлу. При этом даже если Злоумышленник подключиться к сети TOR для выполнения нелегитимных действий, сетевой адрес посреднической ноды не будет показываться как источник данных действий.

Выходная нода — это последний узел в сети TOR, который проходит трафик перед тем, как дойти до точки назначения. Выходные ноды также говорят о своем присутствии, так что их могут использовать любые пользователи данной сети. Поскольку трафик сети TOR выходит из этих узлов, адрес выходного узла интерпретируется как источник трафика. Если злоумышленник использует сеть TOR, именно выходные узлы берут на себя вину, поэтому люди, которые запускают выходные узлы, должны быть готовы к ответственности за передаваемую информацию через их ноды.

В качестве ретрансляторов сети TOR используются мосты, которые не публикуются публично как часть этой сети. Они являются инструментами для обхода цензуры в странах, которые регулярно блокируют адреса всех публично доступных узлов TOR.

Анализ работы скрытых веб-сервисов

Для обеспечения приватности владельцев веб-сервисов в сети TOR существуют скрытые службы (сервисы). Эти службы предоставляют своим пользователям возможность создавать собственные веб-приложения и электронные службы массовой информации, при этом не раскрывать информацию об их реальном местоположении и реальном сетевом адресе.[6]

TOR также предоставляет целый ряд других сервисов, например, сервисы публикаций и обмена сообщениями. Используя специальные технические узлы, называемые «точками рандеву», в сети TOR, пользователи могут подключаться к этим скрытым сервисам, не получая никакой информации о сетевом адресе друг друга. TOR обеспечивает анонимность для серверов веб-приложений, позволяя не допустить разглашения их местонахождения в сети Интернет при помощи определенных настроек для работы с сетью TOR.

Скрытые службы доступны только при использовании клиента TOR на стороне клиента. Сами скрытые службы доступны через специальные псевдо-домены верхнего уровня «.onion». Сеть TOR распознает эти домены и направляет информацию анонимно к скрытым службам, которые затем обрабатывают её посредством стандартного программного обеспечения, настроенного на прослушивание только непубличных (закрытых для внешнего доступа) интерфейсов.

Доменные имена в зоне.onion генерируются на основе открытого ключа сервера и состоят из 16 цифр или букв латинского алфавита. Возможносозданиепроизвольногоименипripомощистороннегопрограммногообеспечения.

У скрытых сервисов TOR есть свои собственные каталоги сайтов, которые, однако, не имеют в своих каталогах все адреса сети. Также некоторые популярные сайты имеют свои зеркала среди скрытых сервисов, например, Facebook и другие. [7]

Кроме того, существуют специальные мосты для доступа к скрытым службам непосредственно из глобальной сети Интернет, а также для посещения других анонимных сетей через TOR.

Также следует отметить тот факт, что существует возможность скрытых служб TOR размещаться за фаерволом или при использовании технологии NAT, не требуя при этом обязательного наличия публичного сетевого адреса.[7]

По оценкам экспертов количество скрытых сервисов TOR по состоянию на ноябрь 2017 года оценивается в 40000–50000 сайтов.[8]

Исследование возможности поиска определенных скрытых сервисов в сети TOR

В ходе проведения анализа сети TOR, было выявлено, что существуют специальные посреднические ноды в данной сети, имеющие информацию о скрытых сервисах. Данные ноды имеют флаг HSDir и сохраняют необходимую информацию в своей памяти. [9]

В ходе исследования была запущена посредническая нода сети TOR с измененным кодом клиента данной сети[10], что дает возможность перехватывать запросы клиентов на соединение со скрытыми сетевыми сервисами и сохранять данную информацию в лог-файл клиента. Впоследствии после недели непрерывной работы данная нода была выключена.

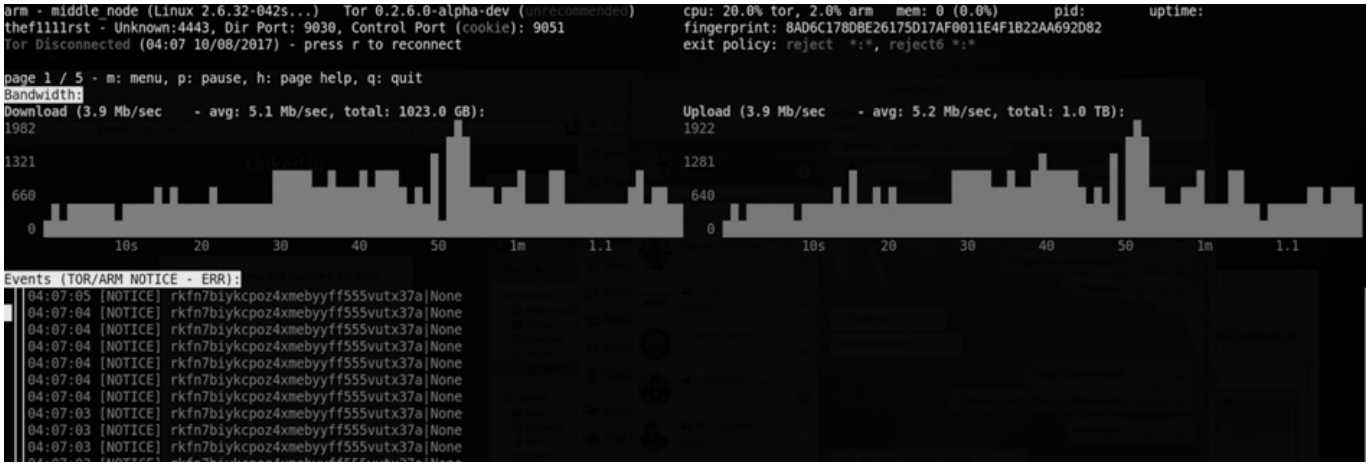

Рис. 2. Графики загрузки трафика в реальном времени

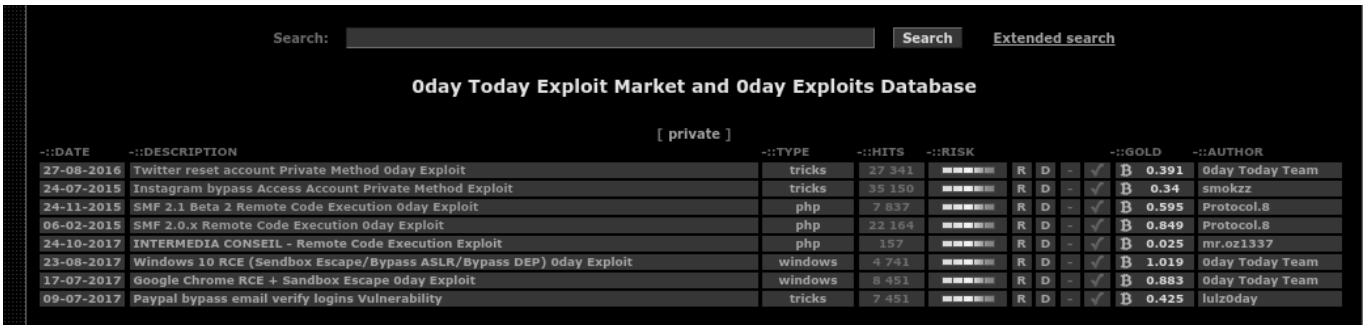

Рис. 3. Найденный скрытый сервис для покупки эксплойтов

Для анализа работы ноды была установлена программа TOR-arm, позволяющая в реальном времени отслеживать графики загрузки трафика и запросов на установление соединения со скрытыми сетевыми сервисами, что представлено на рис. 2.

В ходе работ были получены около 3.5 миллионов запросов на установление соединения со скрытыми сервисами. При этом следует отметить тот факт, что в связи с технологическими особенностями работы сети TOR, в каждый момент времени вероятность получения запроса от клиента для получения запроса к скрытому сервису только 6/n, где n — общее количество узлов сети TOR, имеющих флаг HSDIR.[11]

Из данных запросов удалось установить около 35 тысяч запросов до имени скрытых сетевых сервисов, и при этом было обнаружено только 864 уникальных адреса в скрытой сети TOR.

В процессе идентификации данных сетевых сервисов была написана программа на языке Python, которая подключалась к скрытым веб-приложениям и запрашивала у них заголовок главной страницы для определения наличия веб-приложений на данном скрытом сервисе. [Приложение 1]

С помощью данной программы были проиндексированы все найденные скрытые сервисы, а также было найдено большое количество веб-приложений, в том числе продающих запрещенные вещества, сайты с возможностью покупки паспорта или оружия, а также веб-приложения для покупки эксплойтов для различных операционных систем, что показано на рисунке 3.

На данном сайте не было обнаружено эксплойтов для авиационного программного обеспечения, но стоит обратить внимание на малое количество времени работы ноды, созданной для данной научной работы.

Заключение

Луковая маршрутизация — это технология анонимного обмена информацией через компьютерную сеть. TOR — анонимная сеть виртуальных туннелей, предо-

ставляющая передачу данных в зашифрованном виде и использующая луковую маршрутизацию.

Скрытые сервисы TOR предоставляют своим пользователям возможность создавать собственные веб-приложения и электронные СМИ, не раскрывая при этом информацию об их реальном местоположении. Данные скрытые сервисы могут содержать различную информацию, в том числе исходный код эксплойтов для авиационного программного обеспечения.

С помощью измененного кода клиента сети TOR удалось поднять узел, который может документировать адреса скрытых сервисов, что может дать возможность искать скрытые веб-приложения для продажи эксплойтов, которые могут использоваться для взлома авиационного программного обеспечения.

Приложение 1. Программный код на языке Python

```
import socks, socket
from lxml import html
from urllib2 import URLError, urlopen
def create_connection(address, timeout=20000, source_address=None):
sock = socks.socksocket(); sock.connect(address)
return sock
def get_title(url):
try:
contents = urlopen(url).read(); tree = html.fromstring(contents)
title = str(tree.xpath('//title/text()'))
title=title[title.find(«'»)+1: title.rfind(«'»)].replace(r»\u»,»»).replace(r»\n»,»»)
except:
title=»NULL_TRUEOAZ»
return title
f=open('onion_domains_new')
socks.setdefaultproxy(socks.PROXY_TYPE_SOCKS5, «127.0.0.1», 9050, True)
socket.socket = socks.socksocket; socket.create_connection = create_connection
a=[]; print («I work, this is ok»); num=0
for line in f:
file_title = open('onion_with_title', 'a'); b=[]
url =»http://» + line[line.rfind(««)+1:]; url = url.strip()
number = line[: line.rfind(««)].replace(««,»»); title=get_title(url)
if title!=»NULL_TRUEOAZ»:
if num!=0: print «Don't answer «+str(num)+ « sites»
num=0; b=[url, title, number]
string = url + « get title « + str(title) + « and has « + number + « numbers of requests»
print string
else:
b=[url,»Don't answer», number]
string = url + « don't answer and has « + number + « numbers of requests»; num+=1
a.append(b); file_title.write(str(b)+»\n»); file_title.close()
```

ЛИТЕРАТУРА

1. ГОСТ Р. 51904–2002. Программное обеспечение встроенных систем. Общие требования к разработке и документированию.— Москва: Изд-во стандартов, 2005.— 67 с.
2. Reed M. G., Sylverson P. F., Goldschlag D. M. (1998) «Anonymous connections and onion routing», IEEE Journal on Selected Areas in Communications, 16(4):482–494
3. Servers — Tor Metrics // TorMetrics URL: https://metrics.torproject.org/networksize.html (дата обращения: 05.02.2018).
4. Onion Browser: Tor for iPhone and iPad // Mike Tigas URL: https://mike.tig.as/onionbrowser/ (дата обращения: 05.02.2018).
5. Tor Browser — anonymous browser from the official developer — TorBro URL: https://torbro.com/ (дата обращения: 05.02.2018).
6. TOR: Hidden Service Protocol // TOR Project URL: https://www.TORproject.org/docs/hidden-services.html.en (дата обращения: 27.10.2017).
7. Deep Web DirecTORies and Search Engines — The Hidden Wiki // The Hiddenwiki.net URL: http://www.thehiddenwiki.net/deep-web-direcTORies-search-engines/ (дата обращения: 27.10.2017).
8. TORHiddenService как техника NatTraversal // Информационный портал по безопасности SecurityCorpURL: http://www.security-corp.org/administration/sys_admin/22764-TOR-hidden-service-kak-tehnika-nat-traversal.html (дата обращения: 27.10.2017)
9. Onion Services — Tor Metrics // TorMetrics URL: https://metrics.torproject.org/hidserv-dir-onions-seen.html (дата обращения: 05.02.2018).
10. Hstools/rend-spec.txt at master · FiloSottile/hstools · GitHub // GitHub URL: https://github.com/FiloSottile/hstools/blob/master/misc/rend-spec.txt (дата обращения: 05.02.2018). Onion Services — TOR Metrics // TOR metrics URL: https://metrics.TORproject.org/hidserv-dir-onions-seen.html (дата обращения: 30.10.2017).
11. MoniTORing 'DNS' inside the TOR network // 0x3a — Security Specialist and programmer by trade URL: https://blog.0x3a.com/post/153468210759/moniTORing-dns-inside-the-TOR-network (дата обращения: 27.10.2017).
12. Rend-spec-v3.txt — torspec — Tor's protocol specifications // gitweb.torproject.org URL: https://gitweb.torproject.org/torspec.git/tree/rend-spec-v3.txt (дата обращения: 05.02.2018).

© Николаев Кирилл Андреевич (Kirill.a.nikolaev@yandex.ru).

Журнал «Современная наука: актуальные проблемы теории и практики»