Ngrok Platform Abused by Hackers to Deliver a New Wave of Phishing Attacks

cybleinc.com/2021/02/15/ngrok-platform-abused-by-hackers-to-deliver-a-new-wave-of-phishing-attacks/

February 16, 2021

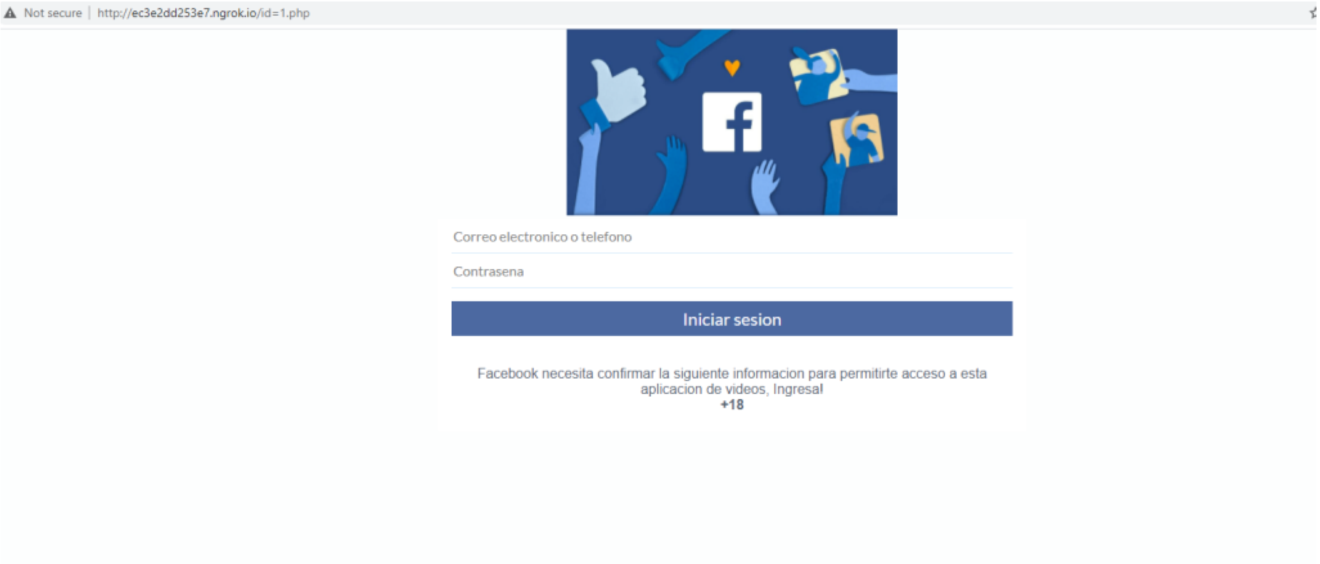
Cyble's research team has found an uptick in phishing campaigns targeting multiple organizations, including financial institutes, by abusing the **ngrok platform**, a secure and introspectable tunnel to the localhost.

About ngrok: ngrok is a cross-platform application used to expose a local development server to the internet, and it makes the locally hosted server appear to be hosted on a subdomain of ngrok(e.g., 4f421deb219c[.]ngrok[.]io) by creating a long-lived TCP tunnel to the localhost. The ngrok server software is self-hosted on a VPS or a dedicated server. It has the ability to bypass NAT mapping and Firewall restriction.

Multiple threat actors have abused the ngrok platform to gain unauthorized access to the target for delivering the additional payload, exfiltrating financial data such as credit/debit card information, and carrying out targeted phishing attacks.

The ngrok-based cyberattacks are harder to detect since they use random subdomains of ngrok.com, besides bypassing security devices like Firewall, thereby making it an active target for cybercriminals.

Sample phishing page –



Not secure | http://ec3e2dd253e7.ngrok.io/id=1.php

Correo electronico o telefono

Contrasena

Iniciar sesion

Facebook necesita confirmar la siguiente informacion para permitirte acceso a esta aplicacion de videos, Ingresa!
+18

History of ngrok-based attacks:

- In 2019, cybercriminals abused ngrok tunnelling hosted on AWS to deliver Lokibot.

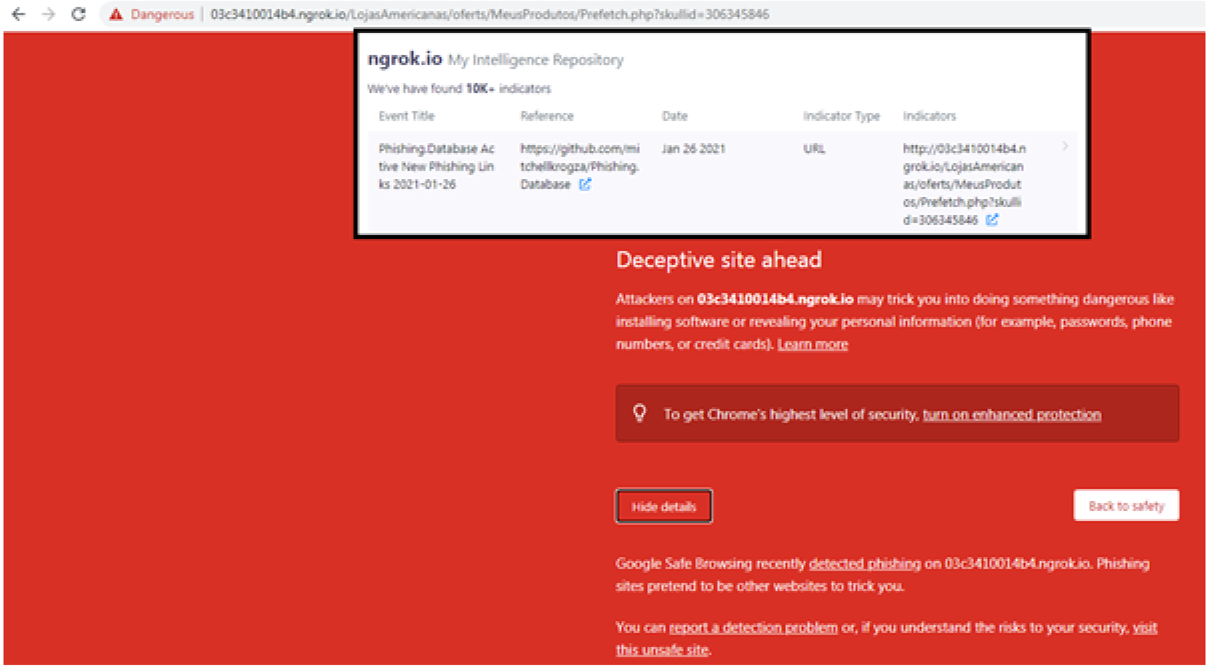
- Last year, the Fox Kitten APT group targeted the private and government sector in the U.S. The threat group was known for using ngrok to intrude on-premises BIG-IP devices.
- In September 2020, researchers identified the Pioneer kitten APT group, an Iran-based Threat group abusing the ngrok platform. The group was selling compromised corporate credentials on cybercrime forums.

Investigation:

Some of the new strains of malware / phishing campaign using ngrok tunnelling are:

- Njrat
- DarkComet
- Quasar RAT
- asynrat
- Nanocore RAT

Recently, Cyble found that cybercriminals are abusing ngrok.io to deliver phishing attacks. The image below showcases one of the phishing links captured in Cyble's Intelligence repository.



03c3410014b4.ngrok.io/LojasAmericanas/oferts/MeusProdutos/Prefetch.php?skullid=306345846

ngrok.io My Intelligence Repository

We've have found **10K+** indicators

Event Title	Reference	Date	Indicator Type	Indicators
Phishing.Database Active New Phishing Links 2021-01-26	https://github.com/mitchellkrogza/Phishing.Database	Jan 26 2021	URL	http://03c3410014b4.ngrok.io/LojasAmericanas/oferts/MeusProdutos/Prefetch.php?skullid=306345846

Deceptive site ahead

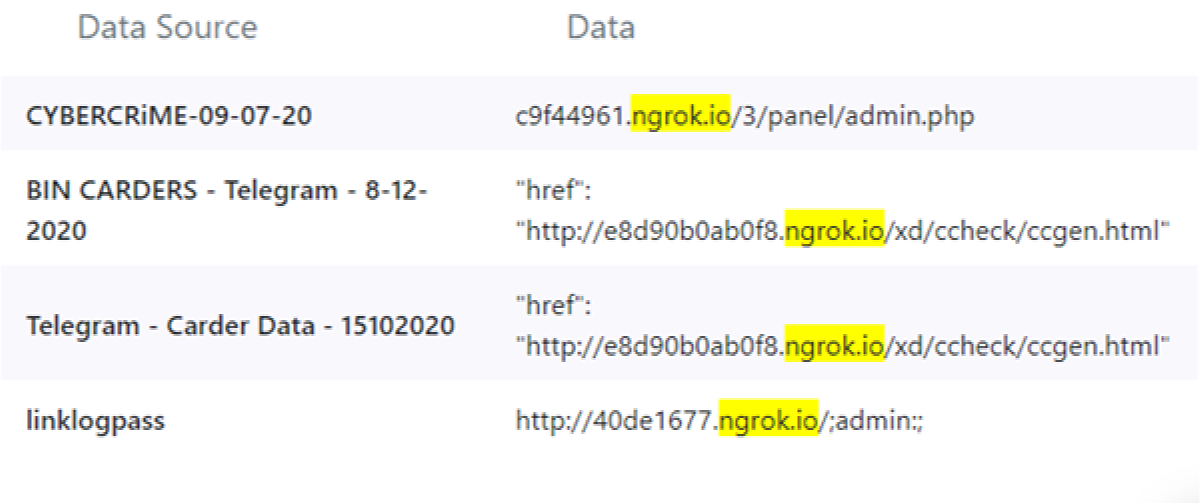
Attackers on **03c3410014b4.ngrok.io** may trick you into doing something dangerous like installing software or revealing your personal information (for example, passwords, phone numbers, or credit cards). Learn more

To get Chrome's highest level of security, turn on enhanced protection

Google Safe Browsing recently detected phishing on 03c3410014b4.ngrok.io. Phishing sites pretend to be other websites to trick you.

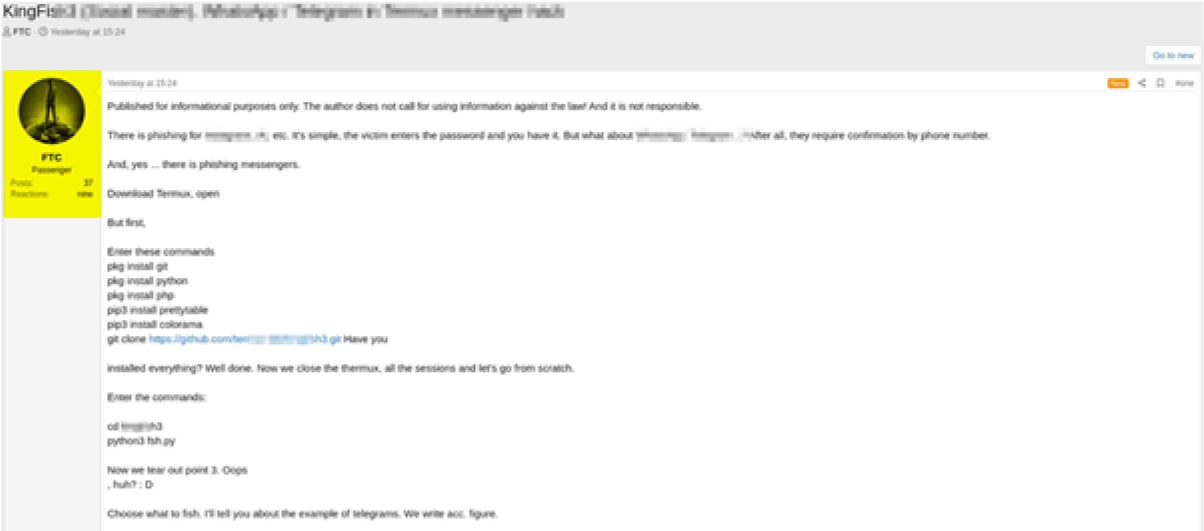
You can report a detection problem or, if you understand the risks to your security, visit this unsafe site.

Interestingly, we found multiple ngrok.io links used in darkweb markets/leaks and cybercrime forums by different threat actors such as BIN CARDERS, Telegram- carder data, and linlogpass. The leaks were captured by Cyble's Threat Intelligence platform, as shown in the below image.



Data Source	Data
CYBERCRiME-09-07-20	c9f44961.ngrok.io/3/panel/admin.php
BIN CARDERS - Telegram - 8-12-2020	"href": "http://e8d90b0ab0f8.ngrok.io/xd/ccheck/ccgen.html"
Telegram - Carder Data - 15102020	"href": "http://e8d90b0ab0f8.ngrok.io/xd/ccheck/ccgen.html"
linklogpass	http://40de1677.ngrok.io/;admin:;

Cyble research team also came across a post in a cybercrime forum about a phishing tool kit, “KingFish3 (Social master). The image below showcases the threat actor’s post about the phishing tool in the cybercrime forum. The threat actor also shared the Github link to the phishing tool, which abuses ngrok.



KingFis[redacted]

Published for informational purposes only. The author does not call for using information against the law! And it is not responsible.

There is phishing for [redacted] etc. It's simple, the victim enters the password and you have it. But what about [redacted] After all, they require confirmation by phone number.

And, yes ... there is phishing messengers.

Download Termux, open

But first,

Enter these commands

```
pkg install git
pkg install python
pkg install php
pip3 install prettytable
pip3 install colorama
git clone https://github.com/ter[redacted]h3.git Have you
```

installed everything? Well done. Now we close the thermux, all the sessions and let's go from scratch.

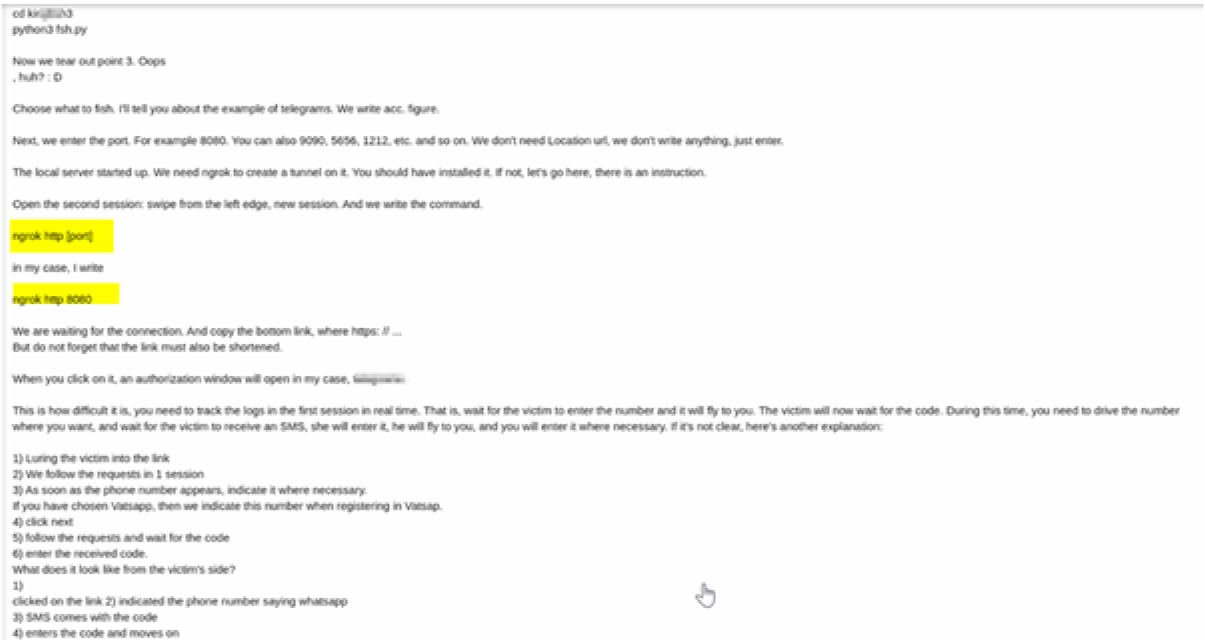
Enter the commands:

```
cd [redacted]h3
python3 fish.py
```

Now we tear out point 3. Oops
, huh? : D

Choose what to fish. I'll tell you about the example of telegrams. We write acc. figure.

The actor described the usage of tools as shown in the following image, thereby showcasing more information about how the ngrok tunnel is being used to carry out successful phishing attacks.



cd kir[redacted]h3
python3 fish.py

Now we tear out point 3. Oops
, huh? : D

Choose what to fish. I'll tell you about the example of telegrams. We write acc. figure.

Next, we enter the port. For example 8080. You can also 9090, 5656, 1212, etc. and so on. We don't need Location url, we don't write anything, just enter.

The local server started up. We need ngrok to create a tunnel on it. You should have installed it. If not, let's go here, there is an instruction.

Open the second session: swipe from the left edge, new session. And we write the command.

ngrok http [port]

in my case, I write

ngrok http 8080

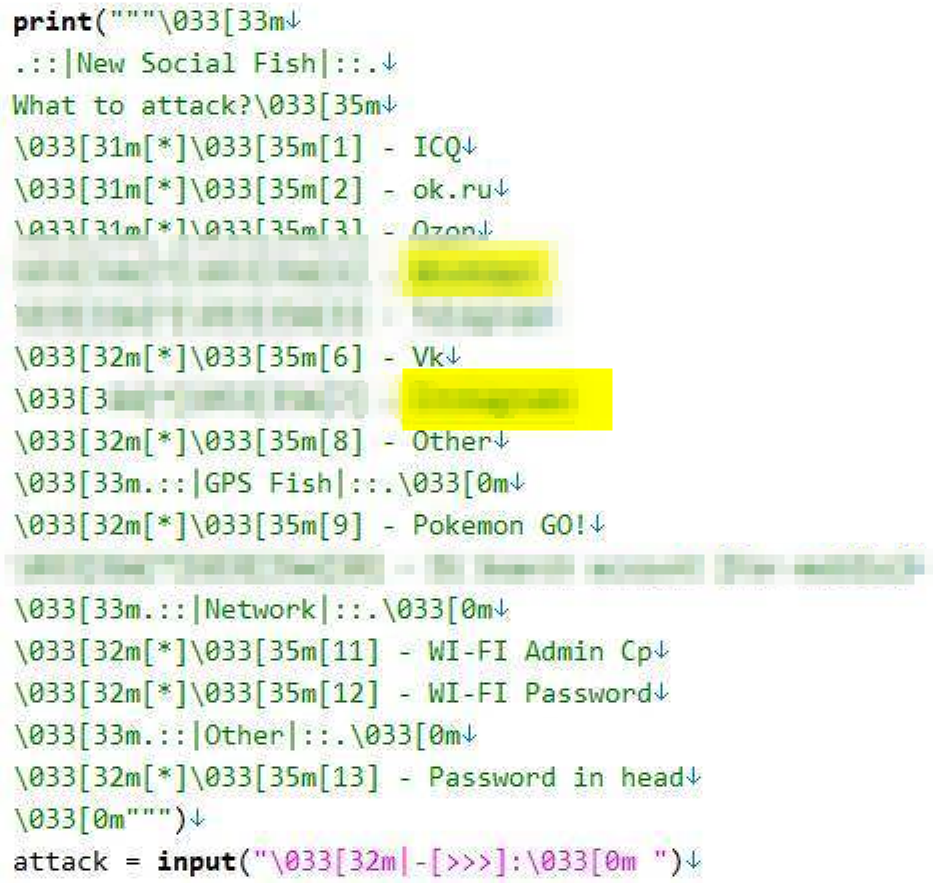
We are waiting for the connection. And copy the bottom link, where https: // ...
But do not forget that the link must also be shortened.

When you click on it, an authorization window will open in my case, [redacted]

This is how difficult it is, you need to track the logs in the first session in real time. That is, wait for the victim to enter the number and it will fly to you. The victim will now wait for the code. During this time, you need to drive the number where you want, and wait for the victim to receive an SMS, she will enter it, he will fly to you, and you will enter it where necessary. If it's not clear, here's another explanation:

1) Luring the victim into the link
2) We follow the requests in 1 session
3) As soon as the phone number appears, indicate it where necessary.
If you have chosen Vatsapp, then we indicate this number when registering in Vatsap.
4) click next
5) follow the requests and wait for the code
6) enter the received code.
What does it look like from the victim's side?
1)
clicked on the link 2) indicated the phone number saying whatsapp
3) SMS comes with the code
4) enters the code and moves on

The post contains step-by-step instructions on how to use the publicly available GitHub code. The image below shows the output of the phishing tools along with the applications targeted.



```
print("""\033[33m↓
.::|New Social Fish|::.↓
What to attack?\033[35m↓
\033[31m[*]\033[35m[1] - ICQ↓
\033[31m[*]\033[35m[2] - ok.ru↓
\033[31m[*]\033[35m[3] - Ozon↓
[redacted]
[redacted]
\033[32m[*]\033[35m[6] - Vk↓
\033[3[redacted]
\033[32m[*]\033[35m[8] - Other↓
\033[33m.::|GPS Fish|::.\033[0m↓
\033[32m[*]\033[35m[9] - Pokemon GO!↓
[redacted]
\033[33m.::|Network|::.\033[0m↓
\033[32m[*]\033[35m[11] - WI-FI Admin Cp↓
\033[32m[*]\033[35m[12] - WI-FI Password↓
\033[33m.::|Other|::.\033[0m↓
\033[32m[*]\033[35m[13] - Password in head↓
\033[0m""")↓
attack = input("\033[32m|-[>>>]:\033[0m ")↓
```

Based on further investigation and analysis of the phishing tool, we were able to identify precisely how the cybercriminals abuse the ngrok tunnels to carry out phishing attacks towards multiple organizations. Here are the steps based on our analysis.

1. The tool creates a tunnel using ngrok to the chosen phishing URL with the specified port.
2. The hacker tracks real-time logs in the first session and waits for the victims to enter their phone number.
3. The hacker then logs into the affected application's official site with the harvested credentials and generates an OTP (2FA).
4. Victims then enter the received OTP in the phishing site, which the hacker captures.
5. Finally, the hacker gains access to the victims' official account using the OTP(2FA).

The following are some of the ngrok based phishing Indicators of Compromise (IOCs) – this list is not exhaustive:

4f421deb219c[.]ngrok[.]io	64bdaf63996c[.]ngrok[.]io
fd4a5b0113b7[.]ngrok[.]io	7f37e07fc0f9[.]ngrok[.]io
8c8a73773aef[.]ngrok[.]io	ed23321e00e2[.]ngrok[.]io
9be055fae612[.]ngrok[.]io	232fa25e1abe[.]ngrok[.]io
b36a3cf2dc0f[.]ngrok[.]io	1b96bd67151a[.]ngrok[.]io
2106ef42b27b[.]ngrok[.]io	98de9202cf1d[.]ngrok[.]io
c1df5c5c340e[.]ngrok[.]io	8e3d3f5d9ca3[.]ngrok[.]io
fc6cbeaa8cbb[.]ngrok[.]io	9d448ee31851[.]ngrok[.]io
fe7544eeda51[.]ngrok[.]io	3b6859c00864[.]ngrok[.]io
dcf4820d88b8[.]ngrok[.]io	4a826717681a[.]ngrok[.]io
f7e82c8b73a6[.]ngrok[.]io	bd69091[.]**ngrok[.]io**

How to report these malicious URLs for takedowns: It's quite straightforward, just drop a note at contact@ngrok.com.

Our Recommendations:

- Users of ngrok and other tunnelling services are advised to obtain authorization from their information security teams.
- It is advised to password-protect their tunnel access and enable IP whitelisting to restrict access to only trusted IP addresses.
- Turn on the automatic software update feature on your computer, mobile, and other connected devices wherever possible and pragmatic.
- Regularly monitor your financial transactions, and if you notice any suspicious activity, contact your bank immediately.

- Use a reputed anti-virus and Internet security software package on your connected devices, including PC, laptop, and mobile.
- People concerned about their exposure to the Dark web can register at AmiBreached.com to ascertain their exposure.
- Refrain from opening untrusted links and email attachments without verifying their authenticity.

About Cyble

Cyble is a global threat intelligence SaaS provider that helps enterprises protect themselves from cybercrimes and exposure in the darkweb. Cyble's prime focus is to provide organizations with real-time visibility into their digital risk footprint. Backed by Y Combinator as part of the 2021 winter cohort, Cyble has also been recognized by Forbes as one of the top 20 Best Cybersecurity Startups To Watch In 2020. Headquartered in Alpharetta, Georgia, and with offices in Australia, Singapore, and India, Cyble has a global presence. To learn more about Cyble, visit www.cyble.com.