PROSPERNOT (PROSPERO-AS) The Little AS That Could. Part 1

oliverhough.io/prospernot-prospero-as-the-little-as-that-could-part-1/

17 October 2023

In this post, we will be taking a look at AS200593 (PROSPERO-AS). It is a place where I have come to call "PROSPERNOT" due to the sheer amount of criminal activity that exists in this /24.

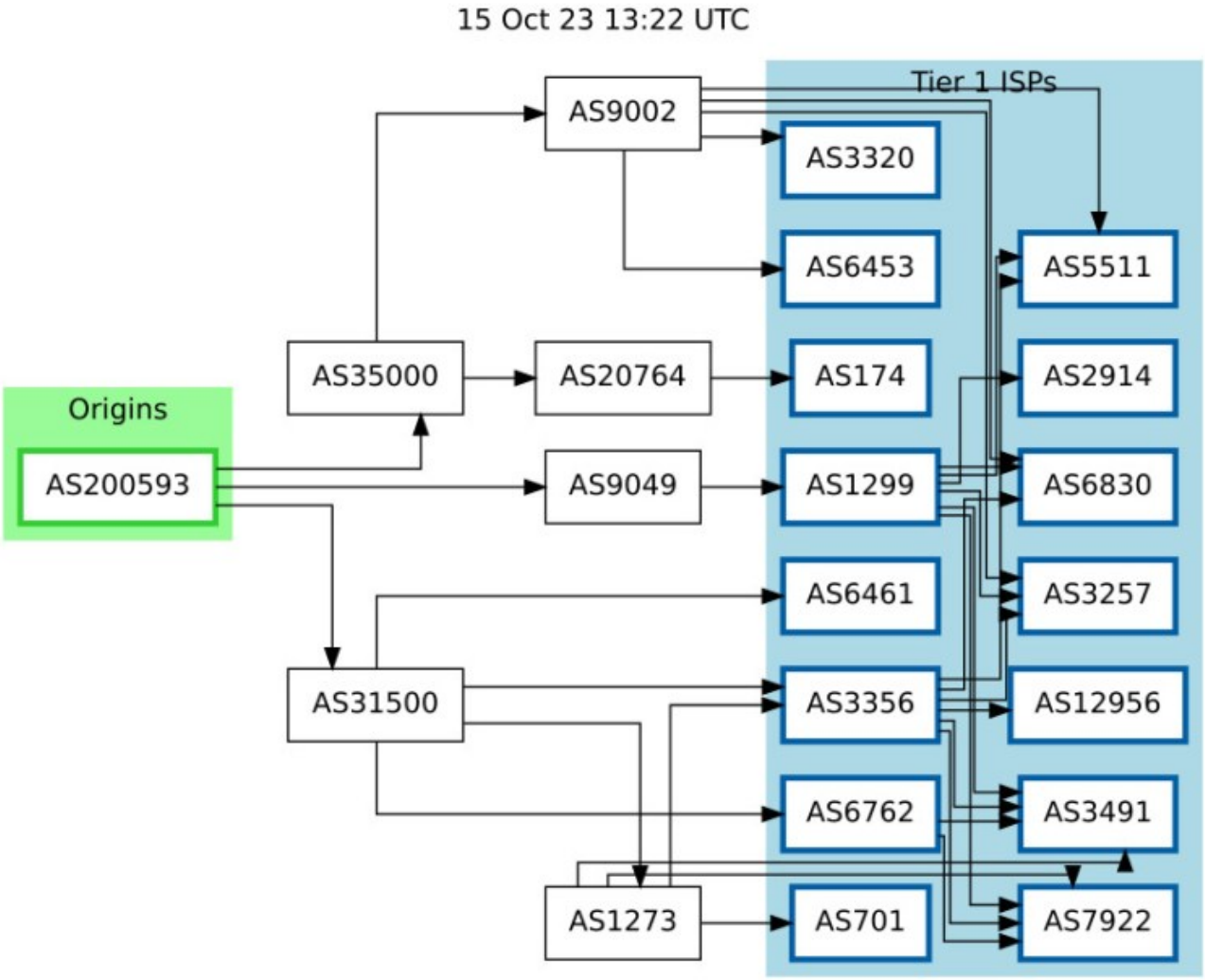


image from bgp.tools

Who is AS200593?

AS200593, also known as PROSPERO-AS, was created in December 2022 and currently only has one net-block, which is 91.215.85.0/24. The AS was last updated in March 2023 and is assigned to an entity named PROSPERO OOO, which is based in Russia.

```
aut-num:        AS200593
as-name:        PROSPERO-AS
org:            ORG-PO83-RIPE
import:         from AS31500 accept ANY
export:         to AS31500 announce AS200593
import:         from AS35000 accept ANY
export:         to AS35000 announce AS200593
import:         from AS9049 accept ANY
export:         to AS9049 announce AS200593
admin-c:        ND7667-RIPE
tech-c:         ND7667-RIPE
status:         ASSIGNED
mnt-by:         RIPE-NCC-END-MNT
mnt-by:         PROSPERO-MNT
created:        2022-12-12T17:06:57Z
last-modified:  2023-03-23T10:58:42Z
source:         RIPE
abuse-email:    petr196721@yandex.ru
abuse-c:        AR69943-RIPE
abuse-org:      ORG-PO83-RIPE

organisation:   ORG-PO83-RIPE
org-name:       PROSPERO OOO
country:        RU
org-type:       LIR
address:        PR-CT SOLIDARITY, D. 12 K. 2 LITERA Z, KV. 167
address:        193312
address:        ST. PETERSBURG
address:        RUSSIAN FEDERATION
phone:          +79810357955
e-mail:         v.dmitriev-prospero@mail.ru
admin-c:        NA8053-RIPE
tech-c:         NA8053-RIPE
abuse-c:        AR69943-RIPE
mnt-ref:        PROSPERO-MNT
mnt-by:         RIPE-NCC-HM-MNT
mnt-by:         PROSPERO-MNT
created:        2023-03-01T10:22:15Z
last-modified:  2023-03-01T10:22:16Z
source:         RIPE
```

The rest of the AS WHOIS repeats the same physical address

```
address:        PR-CT SOLIDARITY, D. 12 K. 2 LITERA Z, KV. 167
address:        193312
address:        ST. PETERSBURG
address:        RUSSIAN FEDERATION
```

and telephone number

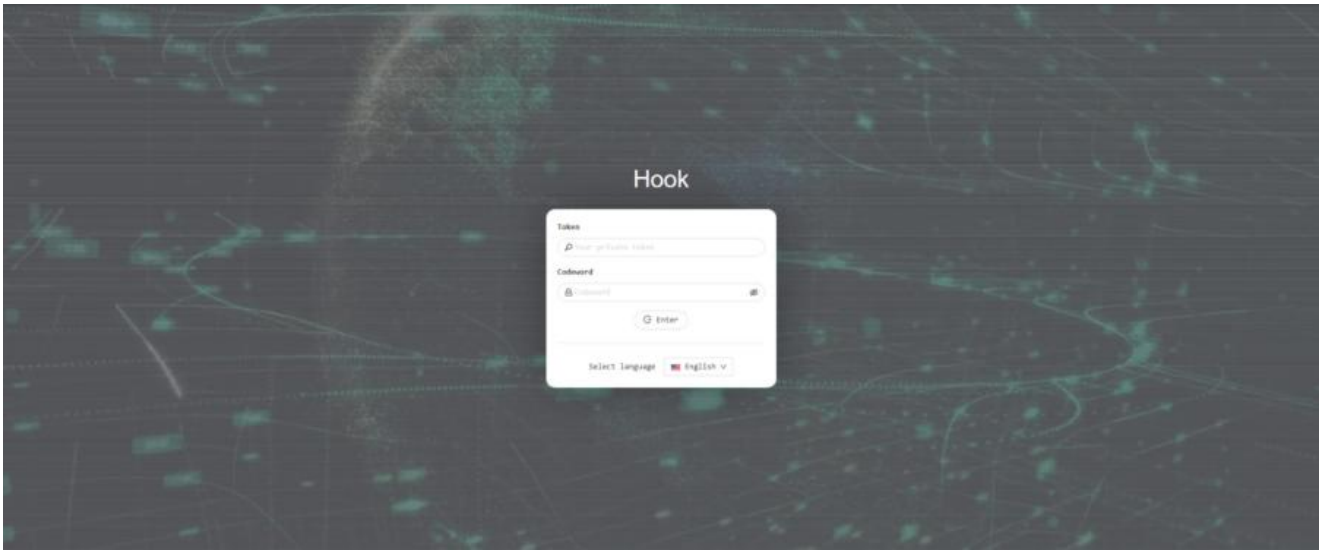
```
phone:          +79810357955
```

Though two different email addresses are provided, the first in 2022 and the 2nd in the 2023 update

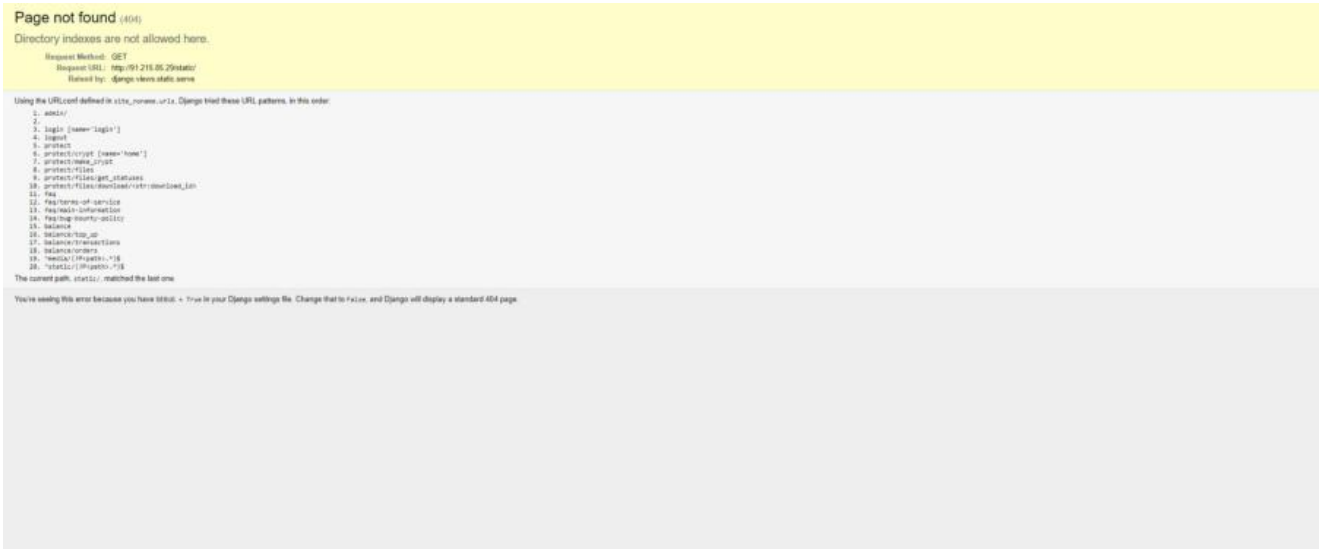
```
e-mail:         petr196721@yandex.ru
e-mail:         v.dmitriev-prospero@mail.ru
```

So, What's Going On?

The short answer to this question: what isn't going on? Over the past few weeks while monitoring AS200593, I've seen at least one Android malware control panel, a half-finished "shop" which seemed designed to sell data dumps, and an in-development ransomware blog. Predominantly, the focus of this post is phishing campaigns targeting numerous banks.



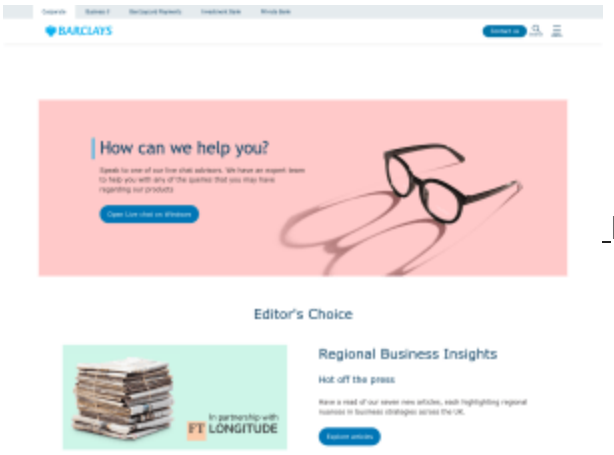
HookBot Android malware panel



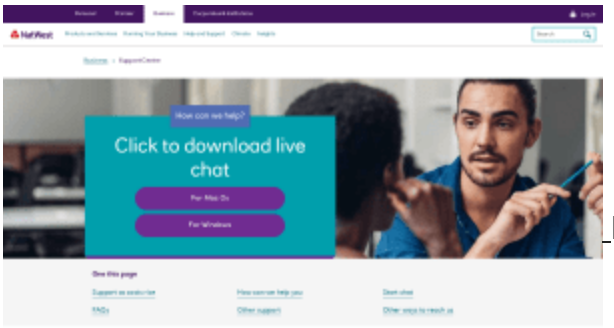
Unknown shop in development

AnyDesk

The first phishing campaign I observed on AS200593 emulated various different banks and crypto wallet providers, although the aim appeared to be the same in all cases – to deliver an AnyDesk binary. AnyDesk is a legitimate piece of software that is often used for remote technical support. It functions similarly to other popular remote control tools; the user installs the client application and inputs a code that grants access to their computer (in this case, to the attacker).



_Barclays bank



_Natwest bank

_Ledger hardware wallet

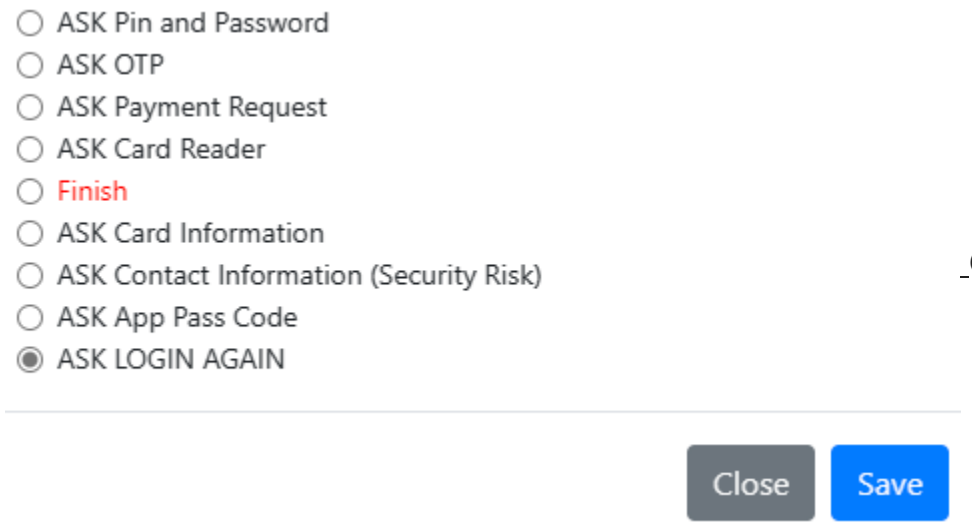
Each page is a single clone of the target brand with a link to open a live chat session. Clicking the link prompts the victim to download an AnyDesk binary for either Microsoft Windows or Apple MacOS. The Windows binary appears to be a legitimate AnyDesk client, as can be seen on VirusTotal (SHA256: 8cd552392bb25546ba58e73d63c4b7c290188ca1060f96c8abf641ae9f5a8383). Considering that the AnyDesk client requires the victim to enter a code to allow access to the attacker, the attacker must also be using another communication channel.

Operator Driven Phishing Kits

T-mobile
AU Gov
Barclays
Santander
Halifax
Natwest
ANZ Bank
Commonwealth Bank

The second type of phishing kit that I found on AS200593 is a modern take on a regular credential stealing phishing kit. Operator-driven phishing kits allow the attacker to manipulate the flow of a phish in real-time.

These kits function by first presenting a login page, which captures the victim's username and password. As the authentication flow of banking portals is often more complex, attackers need more real-time information such as 2FA codes. Operator-driven kits allow attackers to "push" victims to certain pages to harvest details in real time. A simplified authentication flow can illustrate how these kits work. The attacker captures the victim's username and password and starts the authentication process on the real banking portal. The portal then asks for an SMS 2FA code, which is already sent to the victim by the bank. The attacker then pushes the 2FA capture page to the victim. Once the code arrives on the victim's phone, they enter the code into the phishing page, which the attacker uses to sign in as the victim. The attacker controls the flow of the phish in real-time, and anything prompted in the real portal can be requested without worrying about codes expiring.



_Operator menu inside the admin section of an operator driven phishing kit

That's it for Part 1! In the next part, we will look at some of the malware panels I've observed and take a peek inside the source code of an operator-driven phishing kit that I picked up from AS200593 recently.