

Achieve DORA Compliance with Uptycs: Securing Financial Services in the Cloud



THREATS

# KurayStealer: An Unscrupulous Actor Exploiting Discord Webhooks

July 01, 2022

Share [in](#) [f](#) [X](#)



Uptycs Threat Research



Now Available

# Gartner's 2024 CNAPP Market Guide

Achieve DORA Compliance with Uptycs: Securing Financial Services in the Cloud



Download report

Tags

Threats

*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.

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).

*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](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, 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).

*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).

*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.

Achieve DORA Compliance with Uptycs: Securing Financial Services in the Cloud



channel via webhooks (see Figure 5).

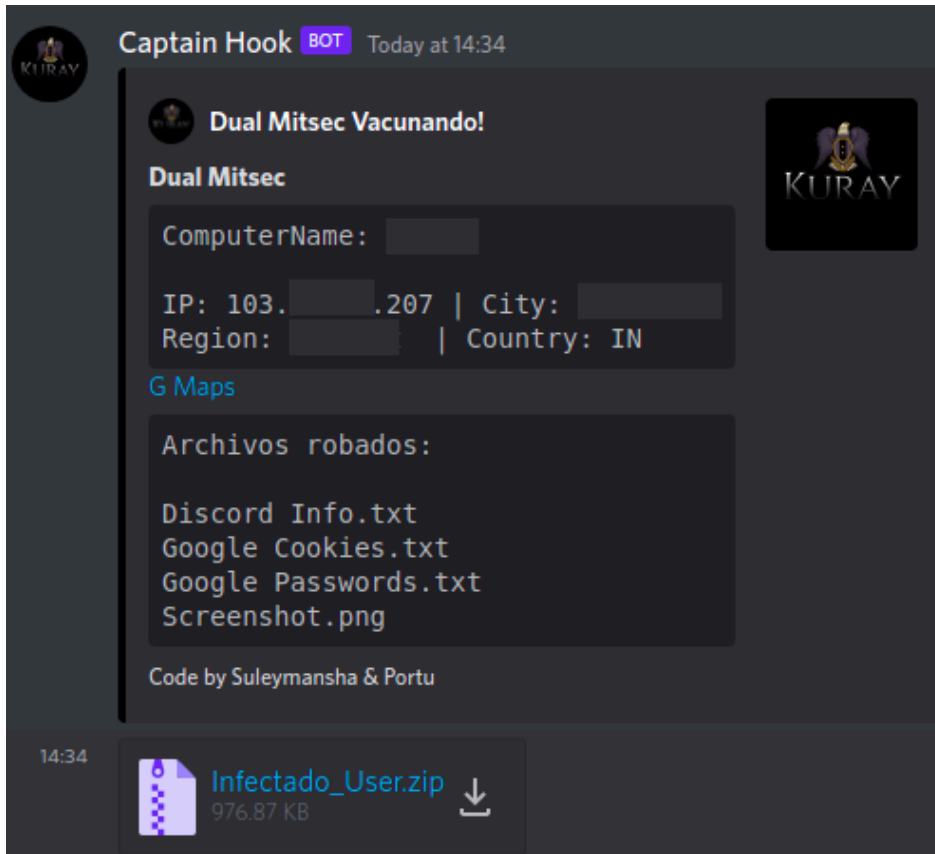


Figure 5: Credentials sent over Discord webhook

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

## 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](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.

We visited the YouTube link and identified the location of the user in Spain and found a video demonstrating KurayStealer (see Figure 8).

Alongside this, the shoppy profile link of “Portu” contained several other tools the author planned to create and their commercial offerings (see Figure 9).

*Figure 9: 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

Achieve DORA Compliance with Uptycs: Securing Financial Services in the Cloud



2c718fa780e7535f07 (c2.py)

2. 09844d550c91a834badeb1211383859214e65f93d54d6c  
b36161d58c84c49fab (DualMTS.py)

3. 30b61be0f8d2a8d32a38b8dfdc795acc0fac4c60efd045  
9cb3a5a8e7ddb2a1c0 (C2.exe)

**To Learn More About the Latest threat Research Conducted by the Uptycs Team, Check out Our Most Recent [Threat Bulletin](#).**

## Recommended Content

Analyzing Agent Tesla Malware:  
Unveiling WSHRAT as a Dropper

The Titan Stealer: Infamous  
Telegram Malware Campaign



Achieve DORA Compliance with Uptycs: Securing Financial Services in the Cloud



New Threat Detected: Inside Our  
Discovery of the Log4j Campaign...

## Stay in the loop

Get regular updates on all things Uptycs—from product updates to expert articles and much more

Achieve DORA Compliance with Uptycs: Securing Financial Services in the Cloud



in



CNAPP Hybrid Cloud Security

Platform  
Cloud Security Pricing

Solutions

Workload Protection  
Posture Management  
Vulnerability Management  
Container & Kubernetes Security  
Software Supply Chain  
File Integrity Monitoring  
Detection & Response  
Asset Management  
Compliance & Risk

By Platform

AWS  
Microsoft Azure  
Google Cloud

Integrations

Tools and Integrations

Why Uptycs

Why Choose Uptycs

About Us  
Case Studies  
Reviews

Compare Uptycs

Aqua  
Lacework  
Sysdig  
CrowdStrike

Resources

Resources

Analyst Reports  
Product Briefs  
Blog  
Video Hub  
Threat Research Report Team  
Whitepapers  
E-books  
~ . .

Achieve DORA Compliance with Uptycs: Securing Financial Services in the Cloud



Webinars and Events

Company

Careers

News

CSU

Support

## Partners

Partner Program

Upward Partner  
Program



Remote Access Trojan: Mitigating Infection...