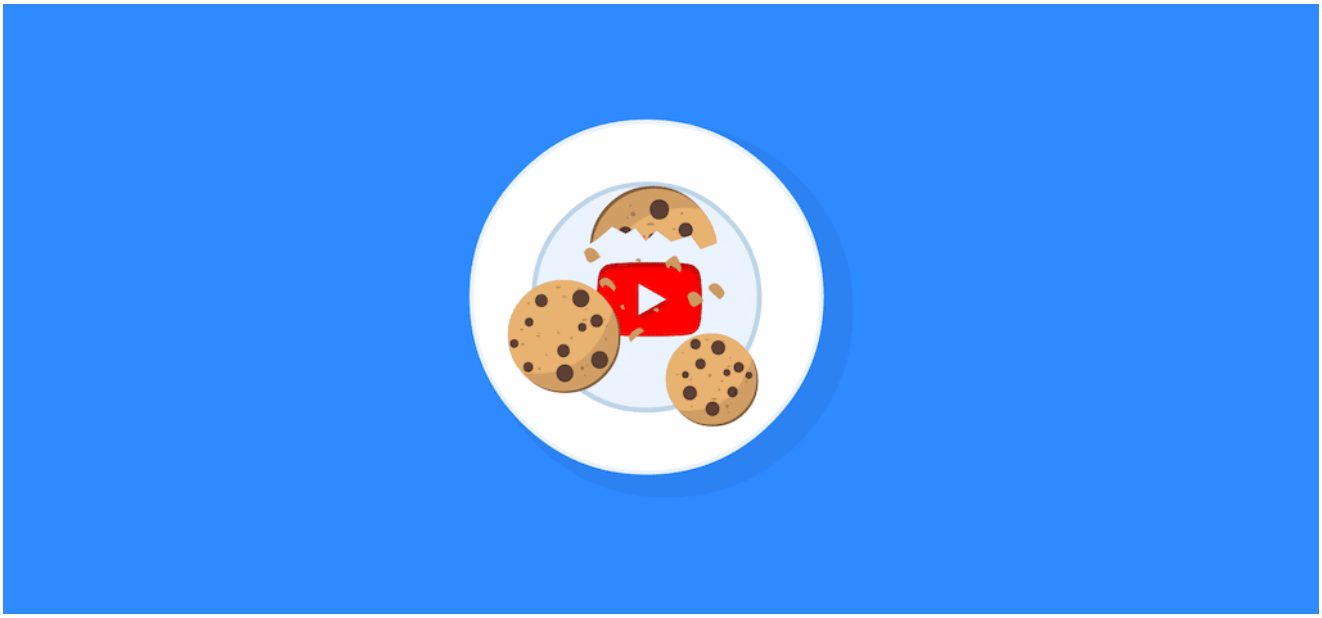
YTStealer Malware: “YouTube Cookies! Om Nom Nom Nom”

intezer.com/blog/research/ytstealer-malware-youtube-cookies/

June 29, 2022

Written by Joakim Kennedy - 29 June 2022



Get Free Account

Join Now

The Stage: The Dark Web Market for YouTube Account Access

In 2006, the term “data is the new oil” was coined. Ever since then, the value of data has just increased. We live in a world where many corporations collect data on users in an attempt to monetize it. This is not just limited to legitimate corporations; the same occurs on the Dark Web. With data, someone always wants to turn it into money. One thing that’s

interesting when it comes to the Dark Web is that a lot of these deals are not happening behind closed doors. Instead, they are sometimes advertised front and center on the forums.

These Dark Web forums have become their own small economies where threat actors specialize in specific services. This specialization has made it easier for these threat actors to monetize what they are good at. We see this, especially in the ransomware scene. There are specialized roles for people that gain access to organizations, steal and encrypt data for the double extortion effect, to ransom negotiators. Another hypothetical chain is: a threat actor sells malware to another that uses the malware to steal data from an organization. The data is sold to another that tries to convert the data into cash. As you move along this chain, the amount of money exchanged usually increases since each party wants to turn in a profit, but the risks also increase. At some point, one of these threat actors must interact with the real world to obtain the cash. This is when they are usually exposed, if they haven't already made other mistakes.

In this blog post, we are describing a new malware that we have concluded is highly likely sold as a service on the Dark Web. **We have named the malware YTStealer because its sole objective is to steal authentication cookies from YouTube content creators.** In June 2020, IntSights released a report on a new trend that they observed. In this trend, threat actors were selling access to YouTube accounts. The goal of this write-up is to share one of the many methods threat actors are using to obtain these accounts.

One Stealer, One Goal

YTStealer is a malware whose objective is to steal YouTube authentication cookies. As a stealer, it operates like many other stealers. The first thing it does when it's executed is to perform some environment checks. This is to detect if the malware is being analyzed in a sandbox. The code that performs the checks comes from an open-source project hosted on GitHub called Chacal. Figure 1 shows a screenshot of the project's readme file. The framework is marketing itself for Red Teams and pen-testers. It provides anti-debugging, anti-memory analysis, and anti-VM functionality.

Chacal

Golang anti-vm framework for Red Team and Pentesters

Let Chacal hidde your malware in your assalt operation!

▾ Table of Contents

About The Project

Chacal is an anti-vm framework written in Golang in order to support Red Team and Pentesters in your assalts, in Windows environment!
!!I'm not responsible for your acts!!

Figure 1: Part of Chacal's README.

What sets YTStealer aside from other stealers sold on the Dark Web market is that it is solely focused on harvesting credentials for one single service instead of grabbing everything it can get ahold of. When it comes to the actual process, it is very similar to that seen in other stealers. The cookies are extracted from the browser's database files in the user's profile folder.

If YTStealer finds authentication cookies for YouTube, it does something interesting though. To validate the cookies and to grab more information about the YouTube user account, the malware starts one of the installed web browsers on the infected machine in headless mode and adds the cookie to its cookie store. By starting the web browser in headless mode, the malware can operate the browser as if the threat actor sat down on the computer without

the current user noticing anything. To control the browser, the malware uses a library called Rod. Rod provides a high-level interface to control browsers over the DevTools Protocol and markets itself as a tool for web automation and scraping.

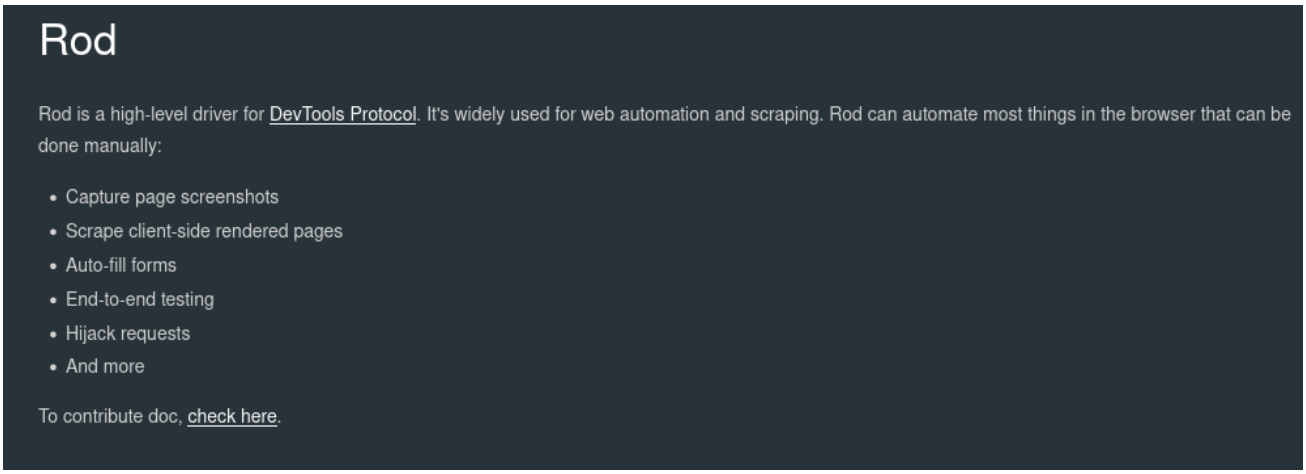


Figure 2: Screenshot of Rod's documentation describing the framework.

Using the web browser, YTStealer navigates to YouTube's Studio page which allows content creators to manage their content. From YouTube studio, the malware grabs information about the user's channels. The data it grabs includes the channel name, how many subscribers it has, how old it is, if it is monetized, an official artist channel, and if the name has been verified. All the data is encrypted with a key that is unique for each sample and sends it together with a sample identifier to the command and control (C2) server located at the domain name youbot[.]solutions.

YTStealer doesn't discriminate about what credentials it steals, whether it's someone uploading Minecraft videos to share with a few friends or a channel like Mr. Beast with millions of subscribers. On the Dark Web, the "quality" of stolen account credentials influences the asking price, so access to more influential YouTube channels would command higher prices.

What is "YouBot Solutions"?

While investigating all the YTStealer samples that we have come across, we noticed that all shared the same build path. The path, shown below, looks like a path from an internal build service. The path also includes the domain name to which the stealer exfiltrates the stolen data.

```
/home/admin/web/youbot.solutions/public_html/Builder/Sources
```

This domain name was registered back in December 2021 and hosts a web server behind Cloudflare that returns an empty response. By using the domain name we identified an American corporation with the name of "YOUBOT SOLUTIONS LLC". The corporation was registered in New Mexico on March 8, 2022 (unfortunately, the State of New Mexico's corporation registry is not accessible outside of the US but the data can be obtained from

third party providers). Figure 2 shows a screenshot of a Google Business entry for a company with the same name and address as in the registry database. The company lists itself as a software company that “provides [sic] unique solutions for getting and monetizing targeted traffic”. The website provided in the listing points to youbot[.]solutions.

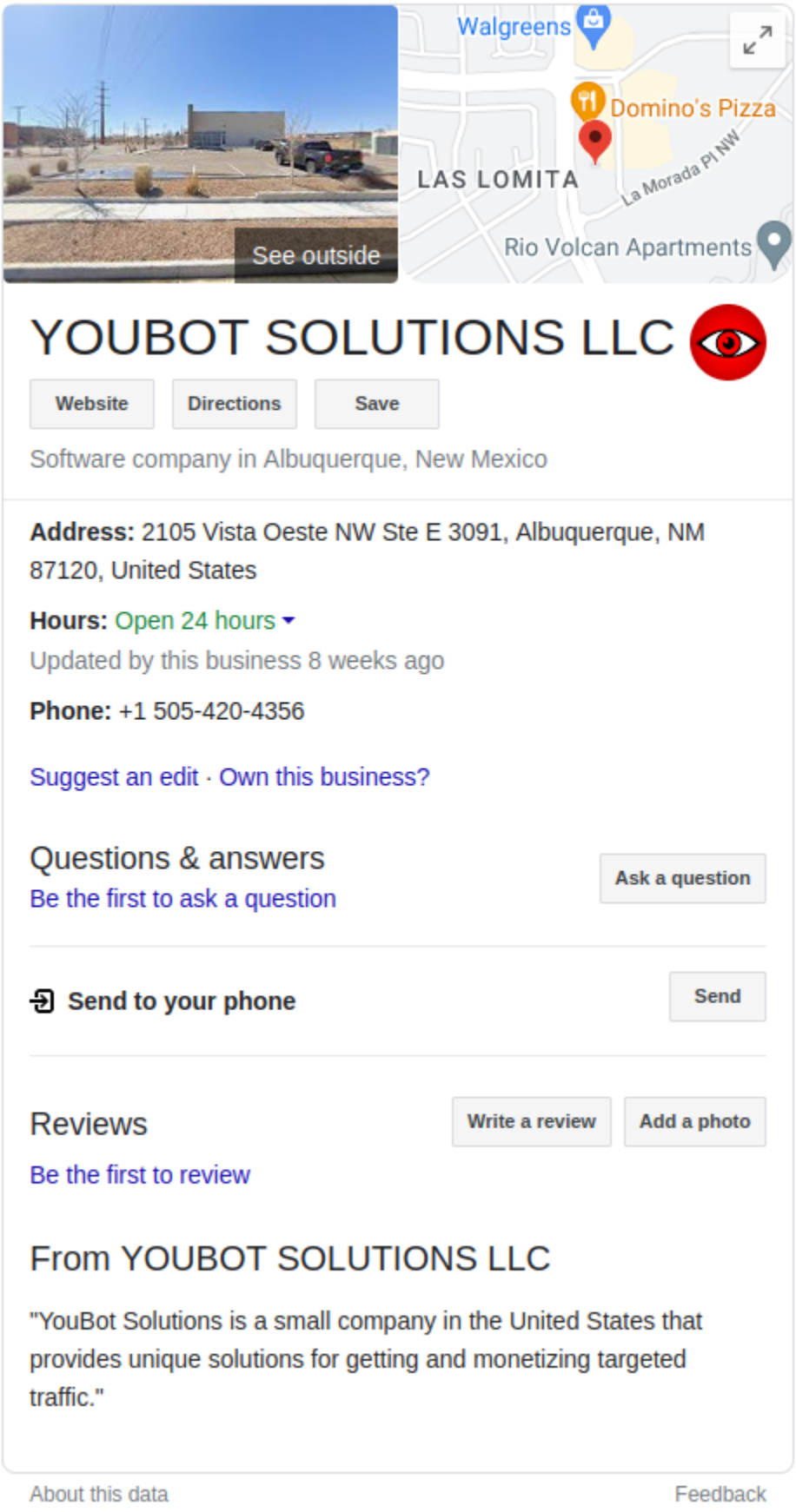


Figure 3: Google

Business listing for YOUBOT SOLUTIONS LLC.

The business listing has a logo of an eye in a red circle. A Google image search using the icon returned some results with the same image. All the results were under the domain aparat[.]com. Aparat is an Iranian video-sharing site that was founded in 2011. The image matched was used as a profile picture for a user on the site. Figure 4 shows the profile page of the user. The profile page provided a link to a Twitter account. Figure 5 shows a screenshot of the Twitter account.

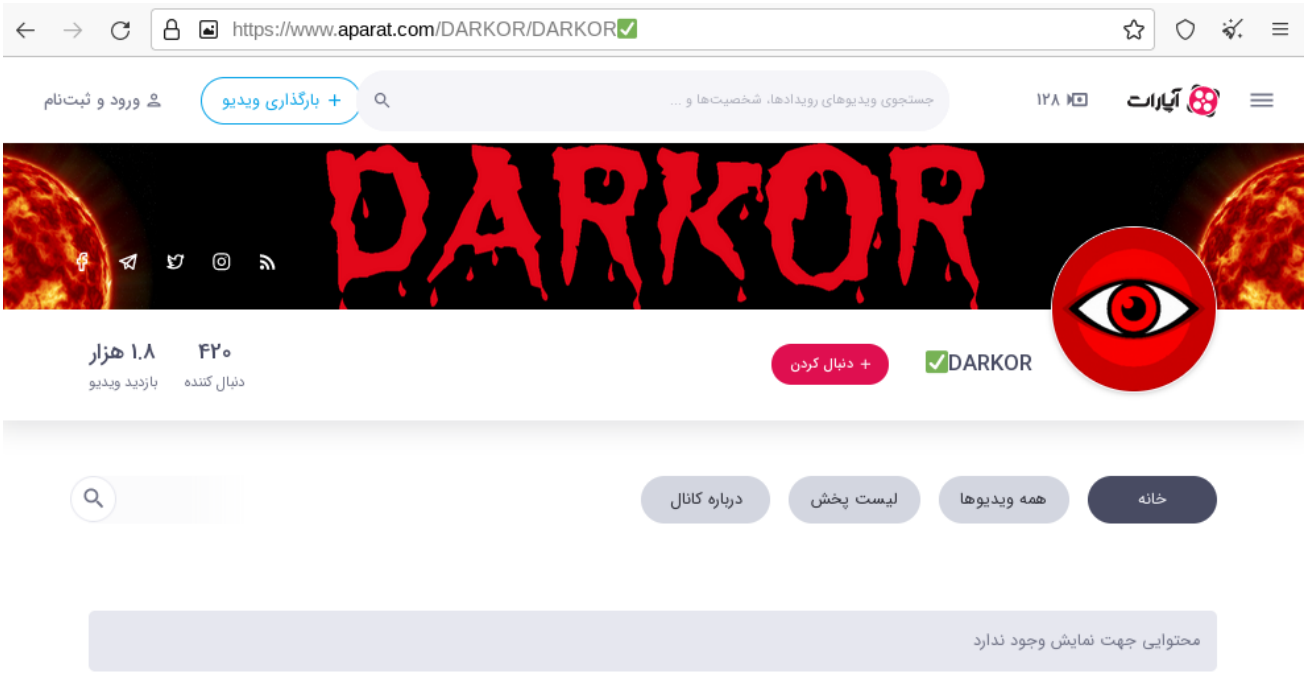


Figure 4: Screenshot of Aparat user account's profile page that uses YOUBOT SOLUTIONS LLC's "logo" as their profile image.

Figure 5: Twitter profile linked to in the Aparat user profile.

How Are Victims Targeted?

Given the optics of the infrastructure and that each sample has a unique identifier, it appears that YTStealer is sold as a service to other threat actors. With this in mind, we decided to look into if we could get a better understanding of who is targeted by this stealer. As it is designed to steal YouTube credentials, it's already clear that YouTube content creators are being targeted. Can we narrow the scope further?

We looked at files that either dropped or downloaded the YTStealer samples that we have collected. The first observation is that the majority of these files don't just drop YTStealer. The droppers also came loaded with other stealers, including RedLine and Vidar stealers. Of the different stealers used together with YTStealer, RedLine stealer was the highest count. Figure 6 shows the analysis of one of the files that drop both YTStealer and RedLine. One of the memory modules found has a lot of shared code with other RedLine stealer samples in our dataset.

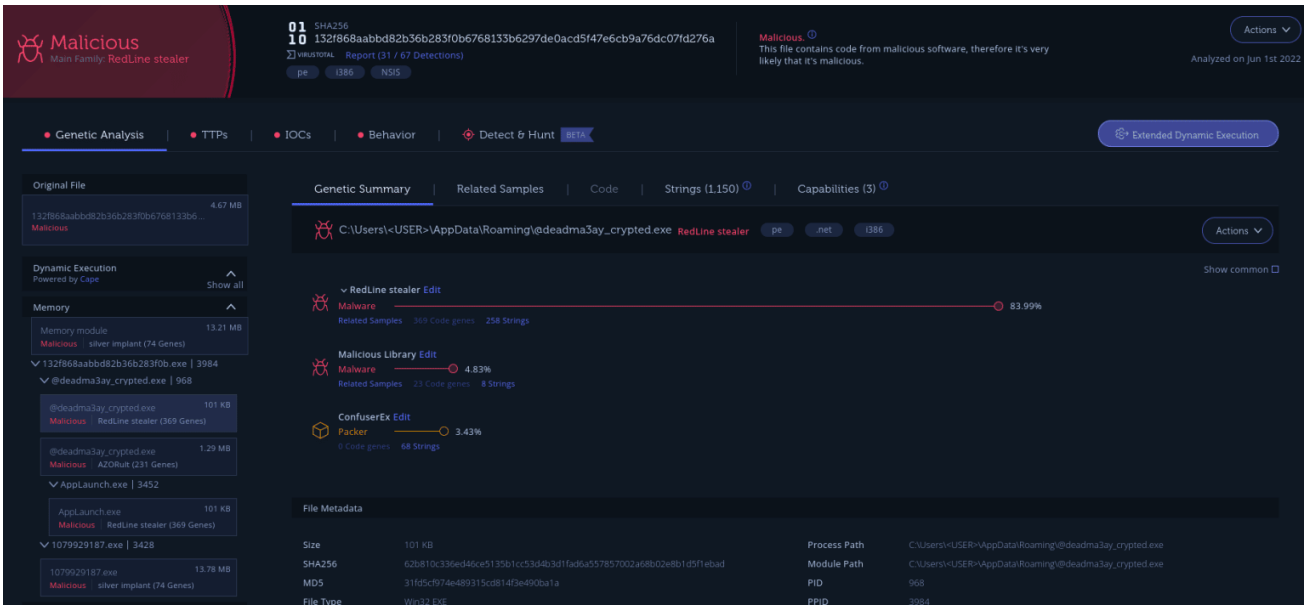


Figure 6: Intezer Analyze result for one of the malware dropping YTStealer together with RedLine stealer.

A lot of these files are disguised as installers for tools or legitimate software. With it targeting content creators, we would expect some of the names to overlap with tools or software used by the intended targets. Grouping the names, we do see some overlap.

One of the groups is “Digital, Image, and Video software”. We found fake installers for OBS Studio, an open-source streaming software. Additionally, we identified a few video editing software installers which included Adobe Premiere Pro, Filmora, and HitFilm Express. In the audio category, we identified fake installers for digital audio workstation (DAW) applications and plugins. This included the DAWs Ableton Live 11 Suite and FL Studio. The plugins included the infamous Antares Auto-Tune Pro, but also Valhalla DSP, FabFilter Total, and Xfer Serum.

The second group is what we call “Game mods and cheats”. The games match popular games used by streamers and content creators. We identified fake installers for the FiveM Grand Theft Auto V mod, different “hacks” for Roblox, and cheats for Counter-Strike Go, and Call of Duty. A variant of the Valorant hack reported on by AhnLab earlier was also discovered. Valorant “gamers” were also targeted by a “Skin Changer”.

Another group of tools that can be classified as adjacent to games is driver tools. Gamers usually would like to squeeze the very last drop of performance out of their gaming rigs. One way of doing this is to “ensure you are using updated drivers and that they are tuned correctly”. In this group, we found fake installers for tools such as “Driver Booster” and “Driver Easy”.

The last group is for other software and “cracks”. Here we identified anything from fake installers for security products, such as Norton Security and Malwarebytes to “token generators” and “cracks” for services such as Discord Nitro, Stepn, and Spotify Premium.

The overwhelming part of these fake installers are for pirated versions of the software, but we also see some fake installers for game mods. This finding should further stress the importance of only obtaining software from trusted sources. Only obtain software directly from the vendor or “modding” group.

Lessons Learned

Someone always has a way of monetizing data. When it comes to stolen YouTube authentication data, we haven’t analyzed how it’s being monetized in the next step of the chain. One potential option could be to defraud the subscribers of channels. When it comes to how this malware is infecting the victims, we can see a trend. Most of the fake installers used were for cracked versions of legitimate software. We also saw fake installers for mods and cheats for games. When it comes to how to protect yourself, the classic security practice should be applied. Only use software from trusted sources.

Indicators of Compromise

IoCs can be found on GitHub here.

Joakim Kennedy
Dr. Joakim Kennedy is a Security Researcher analyzing malware and tracking threat actors on a daily basis. For the last few years, Joakim has been researching malware written in Go. To make the analysis easier he has written the Go Reverse Engineering Toolkit (github.com/goretk), an open-source toolkit for analysis of Go binaries.