Analyzing the RedTiger Malware Stealer

c-b.io/blog/redtiger_stealer/

March 16, 2025

Today we'll dive into a fresh malware stealer dubbed **RedTiger**, a sample targeting personal user data, particularly Discord tokens, browser-stored credentials, and gaming accounts. This stealer, like many others seen recently, heavily leverages Discord webhooks for Command & Control (C2).

SHA256: b8d1c0436023bf58ea7b0f530ea37ae67bac0e956d9c93376702b4832055e0fd

Distributed as: `Phantom X.exe`

Deobfuscated sample: https://github.com/cyb3rjerry/revengd-malware/tree/main/redtiger

How I found this sample

As usual, I grabbed this malware sample from tria.ge after spotting it flagged as malicious.

Initial Analysis

The sample is a Python-based malware script targeting Windows, easily recognizable from its initial imports:

> `os`, `socket`, `win32api`, and `requests`

This tells us immediately we're dealing with a Python-based Windows stealer, one that also directly interacts with web services and OS APIs.

Primary Capabilities

Here's a quick overview of its main functionalities:

- **Discord Token Theft**
- **Browser Data Exfiltration**
- **Roblox Session Stealing**
- **Comprehensive System Information Harvesting**

Discord Token Theft

The stealer systematically searches for Discord tokens in browser LevelDB files and decrypts them using Windows DPAPI. It then checks token validity by pinging Discord's own API, grabbing detailed user information, including:

- Username and discriminator
- Display Name
- User ID
- Email and phone number
- Nitro Status
- Payment methods and gift codes

All this stolen information is then beautifully packaged into a Discord embed and sent directly to the attacker's Discord webhook.

Browser Data Exfiltration

Similar to the previously analyzed BlankGrabber, this sample steals:

- Browser Passwords
- Cookies
- History and Download logs
- Credit card details stored in browsers

It scans numerous browsers, including Google Chrome, Microsoft Edge, Brave, Vivaldi, Firefox, and even niche browsers like Torch and Opera GX.

The malware cleverly handles Chrome's encrypted data by decrypting stored passwords, cookies, and credit card details using Windows APIs (`CryptUnprotectData`) and AES decryption methods.

Extracted data is written into neatly formatted files, zipped, and finally uploaded to Discord via webhook.

Roblox Cookie Stealing

Interestingly, the stealer explicitly targets Roblox user sessions by grabbing `.ROBLOSECURITY` cookies from multiple browsers. It gathers usernames, Robux balance, premium status, and other details, again sending this data directly back to Discord. This highlights an emerging trend targeting gamers and younger users, as we've seen previously with BlankGrabber.

System Reconnaissance

The malware also does a fairly comprehensive system enumeration including:

- Hostname, username, and display name
- Public and local IP addresses
- Geolocation data (country, city, latitude, longitude)
- ISP and organization information

- Detailed hardware specs (CPU, GPU, RAM)
- Drive storage status

All of these pieces are packed into a neatly organized Discord embed, making victim profiling trivial.

Prevention & Detection

Due to its aggressive data collection and direct interaction with Discord, this malware leaves a notable footprint:

- Suspicious webhook calls to Discord
- Unusual file accesses in browser directories
- High-frequency clipboard access and screen captures

A robust EDR solution should easily detect such behavior. Network defenders should pay close attention to outbound requests to Discord and data exfiltration behaviors, especially those targeting user session data.

Differences from BlankGrabber

While BlankGrabber focuses on a broad and somewhat indiscriminate approach to information extraction, including browser data, Discord tokens, and extensive VM detection to avoid analysis, this tool differentiates itself by:

1. **Targeted Functionality**: Unlike BlankGrabber, which aims to capture an extensive range of data including browser cookies, passwords, autofills, and extensive Discord interactions, this tool emphasizes specific extraction tasks tailored for precise requirements.

2. **Enhanced Stealth and Efficiency**: Rather than relying heavily on extensive virtual machine and sandbox detection like BlankGrabber (checking UUIDs, usernames, hosting status, etc.), this tool adopts a lighter, more streamlined approach to minimize detection risks and resource use.

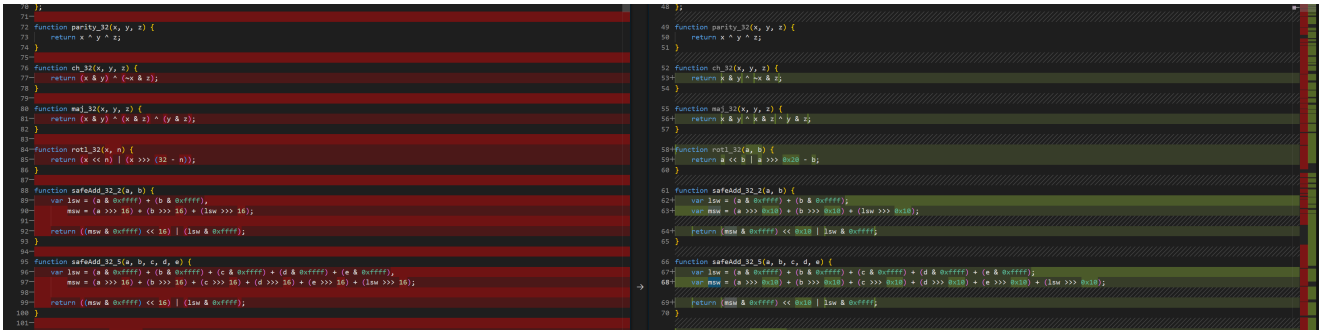
3. **Customization and Modularity**: This tool provides modular components, allowing users greater flexibility in configuring and selecting only relevant features, whereas BlankGrabber is designed as a monolithic solution with less configurability.

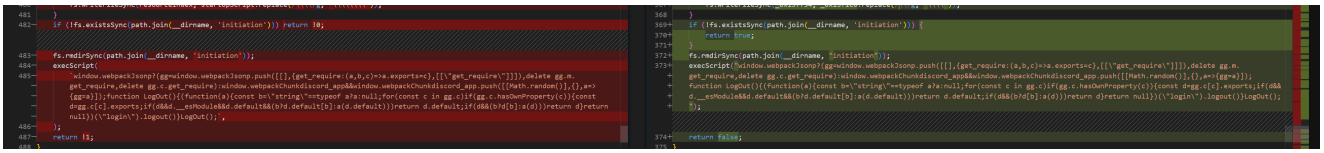
4. **Security and Ethical Standards**: While BlankGrabber utilizes aggressive techniques such as disabling Windows Defender and injecting scripts into Discord, this tool maintains stricter boundaries aimed at legitimate use-cases, focusing on operational transparency and compliance.

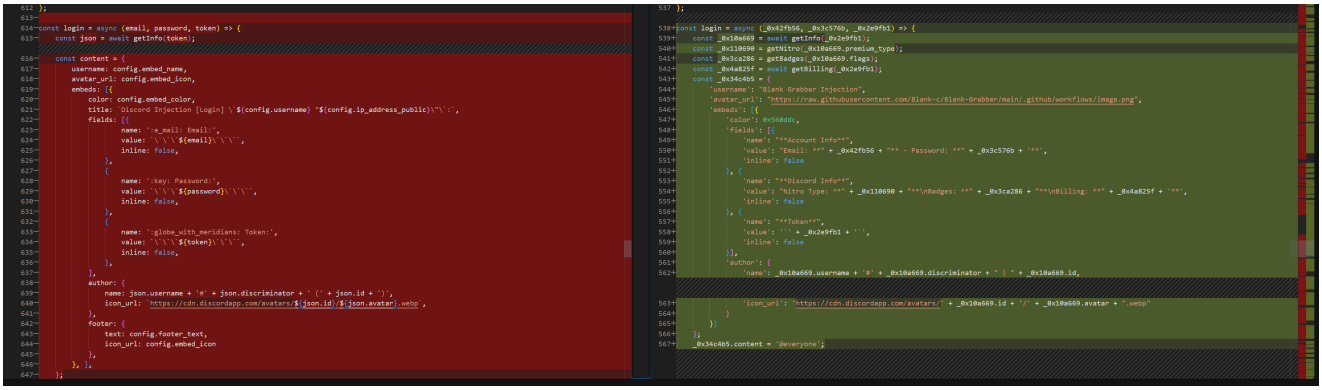
By clearly defining these distinctions, users can appreciate the strategic choices in efficiency, stealth, configurability, and ethical considerations that set this tool apart from BlankGrabber.

Discord code injection

Among all the similarities with BlankGrabber, the one that strikes the most is the code that's injected within the Discord app. Both scripts are **nearly** identical although we notice that the code used by RedTiger seems to have regressed on. The Discord JS file from BlankGrabber offered finer grained metadata collection on the victim's account.







Conclusion

RedTiger is yet another example of the ever-popular Discord-based stealers targeting younger demographics. It shows the commonalities we often see in post-compromise malware today: straightforward, noisy, and surprisingly easy to analyze.

Overall, I'd rate this malware about a **3.1/10**. While it's slightly more sophisticated than the BlankGrabber, it remains fairly easy to catch with modern security tooling.

References

Original C2 code: https://github.com/cyb3rjerry/RedTiger-Tools/tree/main