flare

Criminal Hijacking: Profiling Threat Actors and Criminals Using Infostealer Logs

Criminal Hijacking: Profiling Threat Actors and Criminals Using Infostealer Logs

Eric Clay, November 2024

One of the great ironies of the infostealer ecosystem is that threat actors often unintentionally infect each other as part of their ongoing campaigns. Infostealer malware takes what is essentially a snapshot of the victim's computer, that includes all credentials and session cookies saved in the browser, along with basic information about the operating system, processes running, and in most cases a screenshot. Almost any executable file can contain an infostealer, and criminals frequently seed commonly cracked applications such as downloads for “Windows,” “Photoshop,” and “Adobe” with malware.

In some cases, however, threat actors may deliberately target other criminals by seeding illicit tools with infostealer malware. In these instances, the infostealer operator is intentionally infecting downstream criminals, which can provide valuable insights into how the infostealer ecosystem operates.

Flare has identified a malware campaign that ran during August and September of 2024. This campaign involved promoting a cracked version of “BLTools” across various cybercrime forums and marketplaces, that when downloaded, executed infostealer malware on the victims computer. This campaign is notable because BLTools is a type of software known as a “checker”, which is used exclusively by criminals. Checkers serve two primary functions in the criminal ecosystem, which include:

1. Enabling threat actors to test session cookies to determine if they work without invalidating them. Once valid session cookies are identified, threat actors can use an anti-detect browser to mimic the victim’s browser footprint and perform a session hijacking attack to gain direct access to web application accounts.
2. Identifying high-value credentials or crypto wallets in stealer logs. Threat actors can upload stealer logs obtained from public and private telegram channels to a checker, and select the “type” of session cookies and credentials they are interested in. We commonly see consumer bank accounts, Netflix accounts, and crypto exchanges as targets.

The result of this campaign is that Flare collected hundreds of infostealer logs containing criminal browser histories, saved credentials, operating systems, and other valuable data that gives us direct insight into criminal usage of logs. Since these users were downloading a checker, their primary aim was to perform session hijacking attacks against consumer accounts in order to monetize the illicit access in some way.

01

Threat actor seeds cracked version of the checker application BLTools with infostealer malware

02

The cracked checker is distributed on cybercrime forums such as Carders Market and Nulled

03

Cybercriminals who use stealer logs for account takeover download the cracked checker, infecting themselves with infostealer malware

04

Their data, including credentials, browser history, and session cookies are then distributed on Telegram

05

Flare collects the logs and is able to identify the TTPs the infected actors are using to compromise accounts

Cybercrime Definitions

Before we go any further, let's cover a few definitions in for the sake of clarity given the complexity of the topic:

- **Infostealer Malware:** Infostealer malware is a type of malicious software designed to capture and exfiltrate sensitive information from a victim's system, such as passwords, banking details, and other personal data. It typically operates stealthily, collecting data from web browsers, applications, or files.

- **Stealer Log:** A stealer log refers to the data logs generated by infostealer malware that contain the stolen information, such as credentials, browser history, and session tokens. These logs are often sold or shared in cybercrime forums.

- **Account Takeover:** Account takeover is a cyberattack where an attacker takes control of a valid user session by leveraging stolen credentials or session cookies, allowing them to impersonate the legitimate user and gain unauthorized access to the victim's account.

- **Session Replay Attacks:** In a session replay attack, a malicious actor captures valid data from a user session (e.g., authentication tokens) and replays it to a server to fraudulently gain access, essentially mimicking the original user's actions.

- **Cookies:** Cookies are small text files stored by web browsers that contain user session data, such as login information or session tokens. In attacks like session hijacking or replay attacks, stolen cookies can be used by attackers to impersonate legitimate users by gaining unauthorized access to active sessions.

In most cases, though not all, threat actors leveraged virtual machines (VMs) with VPNs, hacked remote desktop protocols (RDPs), and proxies to open, sift through stealer logs, and gain access to consumer accounts without leading back to them. In a few cases we were able to personally identify threat actors because they failed to use a VM or VPN/Proxy. When a criminal successfully compromised a consumer account, they would often save the credentials and session cookies of the compromised account to their browser's password management system.

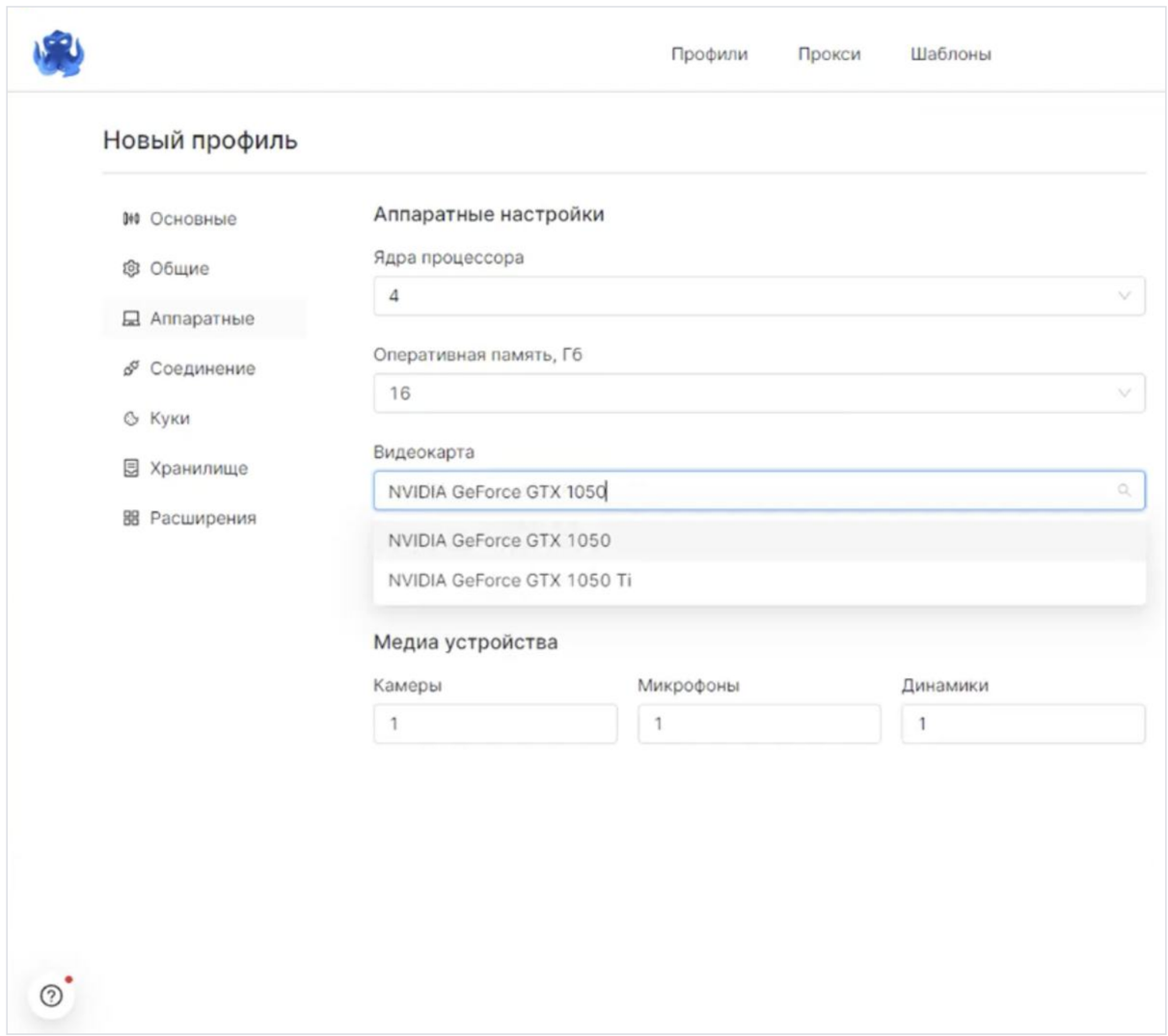
This article discusses how infostealer logs, complete with browser histories, screenshots, and saved credentials, can be used to profile criminals and, more specifically, to identify their tactics, techniques, and procedures (TTPs).

What makes this work particularly interesting is that we can use an exclusive dataset containing information on hundreds of criminals. This allows us not only to observe, broadly, how criminals use stealer log data but also to explore specific use cases within the infostealer malware ecosystem. Flare's research team reviewed hundreds of stealer logs associated with this campaign and selected representative logs that illustrate exactly how criminals leverage logs to get access to consumer accounts.

The sheer variety of use cases employed by threat actors was surprising. While some were expected—such as taking over financial service accounts and searching for crypto wallets—many were less obvious. These included taking over accounts with no clear monetary value, such as Facebook, Netflix, and other popular web applications.

The Broad Attack Pattern

Before we dive into specific examples, let's begin by discussing exactly what criminals are doing with infostealer logs in broad strokes. Web applications don't just rely on session cookies and credentials in order to successfully authenticate users. In most cases they will also look at the "fingerprint" of the browser to identify key details about the user that can be used for additional validation. The combination of infostealer malware, anti-detect browsers, and checkers represent a multi-pronged approach to defeating these controls.

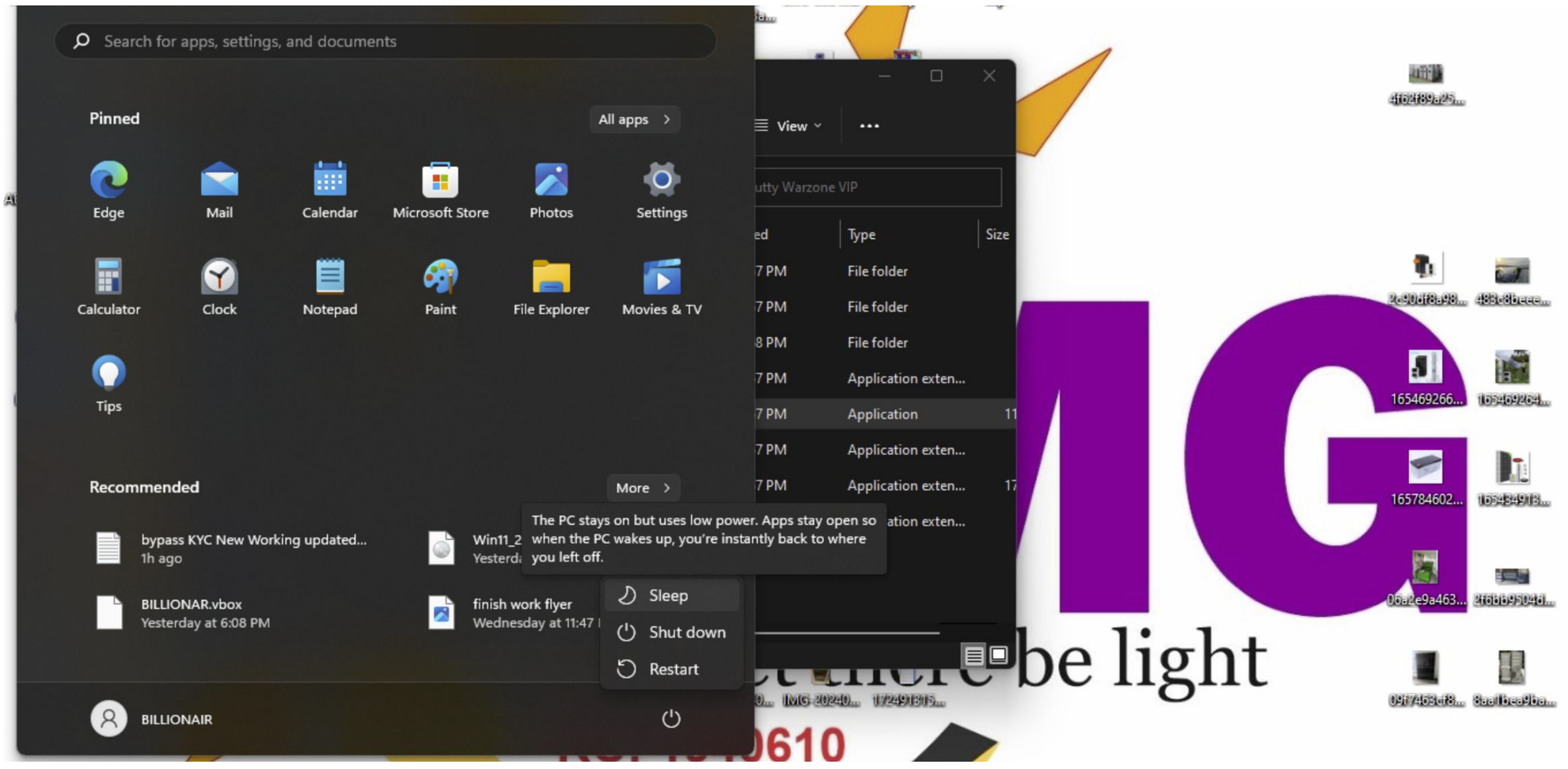


Anti-detect browser that enables the user to replay session cookies while also mimicking key details from the victim's computer to bypass anti-fraud mechanisms

The infostealer grabs all of the credentials, session cookies, key operating system data, hardware information, and the browser fingerprint from the host. These logs are then typically distributed in Telegram. A criminal downloads free stealer logs or purchases them in a private channel. They then use a checker which enables the actor to rapidly identify valid session cookies for services that they want to compromise (e.g. financial services accounts, streaming platforms, and crypto exchanges) by running it on top of hundreds of stealer logs.

Then the actor uses an anti-detect browser to impersonate the user's browser fingerprint based on details found in the stealer log to successfully replay the session cookies and facilitate an account takeover attack. Once in, the actor changes key profile information such as email, password, and two-factor authentication (2FA) to authentication mechanisms that they control, then transfers money or resell the account in a different part of the ecosystem.

This approach is enabled by the fact that infostealers are **big business**. Threat actors have no trouble finding stealer logs - there are millions being distributed monthly on Telegram.



Infection Date: September 5, 2024

Possibly Relevant Tools: Telegram, BLTools

Location: Nigeria

VM/Proxy: No

Infostealer Screenshot, Sep 5, 2024, BLTools Campaign. Note that presence of the"Bypass KYC New working Updated" file saved on the host[1]

This user is a perfect example of a typical infostealer use case. They have been infected by downloading BLTools (almost certainly based on campaign details), and even a cursory glance at their profile reveals that their motive is direct access to financial services accounts. Based on the IP address and other data on the computer, we can place the user in Nigeria. The following URLs had saved credentials in their browser:

- coinbase (crypto exchange)
- oi.huidclaims.ui.hawaii.gov (government claims site)
- 53.com (banking)
- patriotsoftware (business payroll)
- found.com (small business banking)

[1]KYC stands for "know your customer" essentially financial institutions need to gather evidence to affirmatively provide identity. KYC is required by law for banking and financial institutions to prevent money laundering and theft.

Interestingly, if we look more closely at the browser history, we can see that they seem to have had some success. In fact, their browser history contained a real example of the actor taking over a consumer Bank of America account through session hijacking. Reviewing the criminals browser history we can see:

https://secure.bankofamerica.com/**login/sign-in**
https://secure.bankofamerica.com/**login/sign-in/signOnSuccessRedirect**
https://secure.bankofamerica.com/**myaccounts/signin/signIn**
https://secure.bankofamerica.com/**myaccounts/brain/redirect**
https://secure.bankofamerica.com/**myaccounts/accounts-transfer**
https://transfers.bankofamerica.com/**jsp/bofa/account_add**
https://transfers.bankofamerica.com/**jsp/bofa/ft_overview**
https://transfers.bankofamerica.com/**jsp/bofa/make_transfer**
https://secure.bankofamerica.com/**myaccounts/signoff/signoff-default**

- The threat actor accessed Bank of America's login page, successfully logged in, and viewed account details through the "Accounts Overview" page. This suggests the actor has access to online banking credentials or session cookies found in infostealer logs.

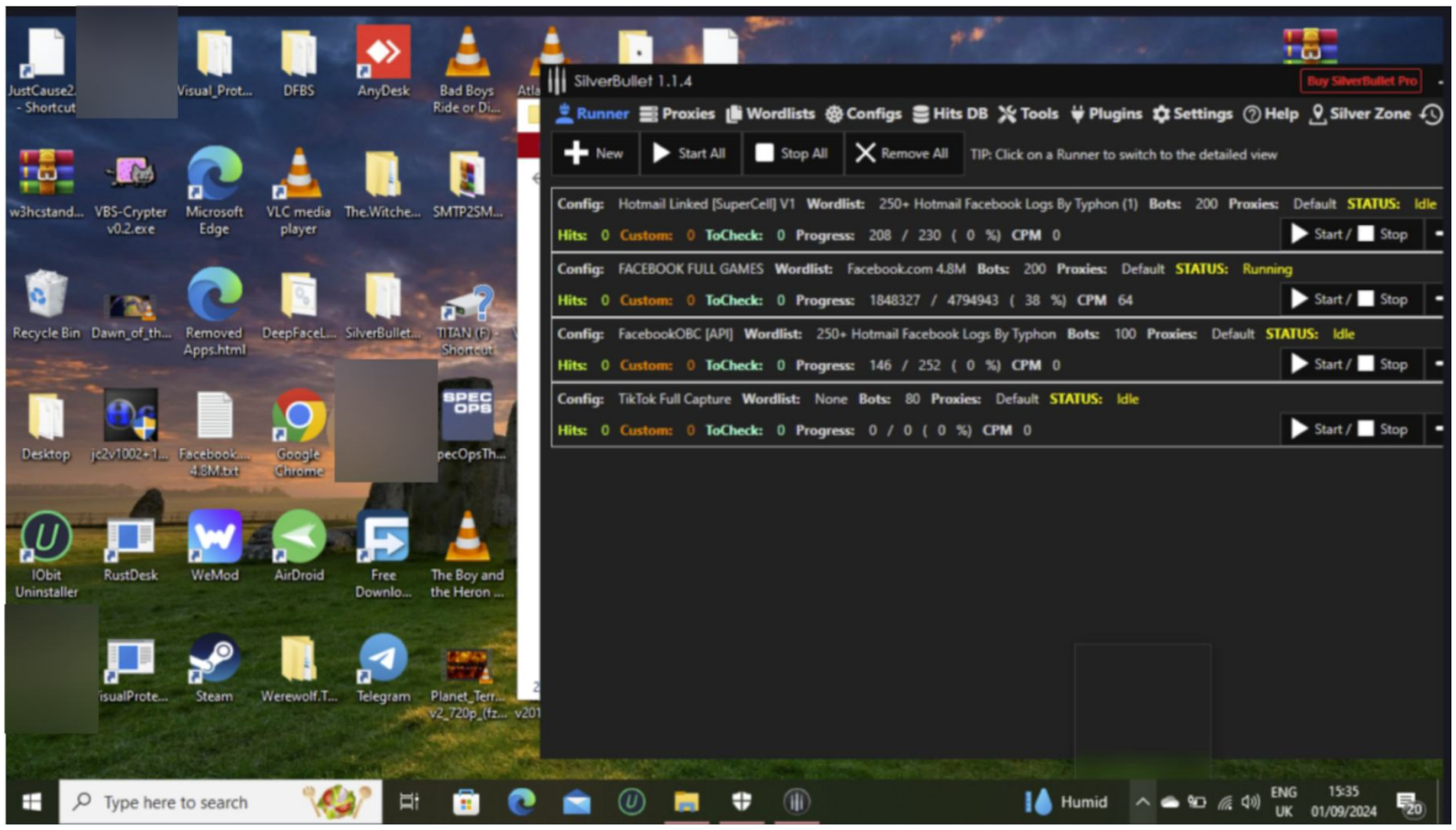
- The individual accessed the "Transfers to Other Banks" feature, possibly with the intent to transfer funds to external accounts. The URL paths, particularly those mentioning "interbankTransfersSA" and "cashedge," suggest an attempt to move money between different financial institutions, potentially to accounts the threat actor controls or to launder funds.

- These URLs show the threat actor navigating through pages to validate emails, add new external accounts, and manage accounts for transfer purposes. This step is essential in linking external bank accounts to facilitate fraudulent transfers.

- The actor likely proceeded to make transfers to either domestic or international accounts. The final URL indicates that the system was used to initiate and manage financial transfers.

- After completing their activities, the actor signs off from the account.

This instance is a common example of how threat actors use infostealer logs, searching for easily accessible financial credentials, gaining access, and transferring money to an account that the actor can use to further forward the illicitly gained funds on.



Our next actor is quite interesting. Whereas many criminals are specifically seeking bank logins, crypto wallets and other data this actor is very focused on compromising Facebook, Whatsapp, and Tiktok.

This users browser history includes:

- Hundreds of attempts to log into Facebook accounts and includes visiting Facebook dating groups in the browser history, likely from stolen accounts
- Dozens of saved Facebook credentials, each for a different user
- Dating sites and WhatsApp accounts
- An Africa based cryptocurrency exchange

Infection Date: September 1, 2024

Possibly Relevant Tools: Telegram, SilverBullet, DeepFace

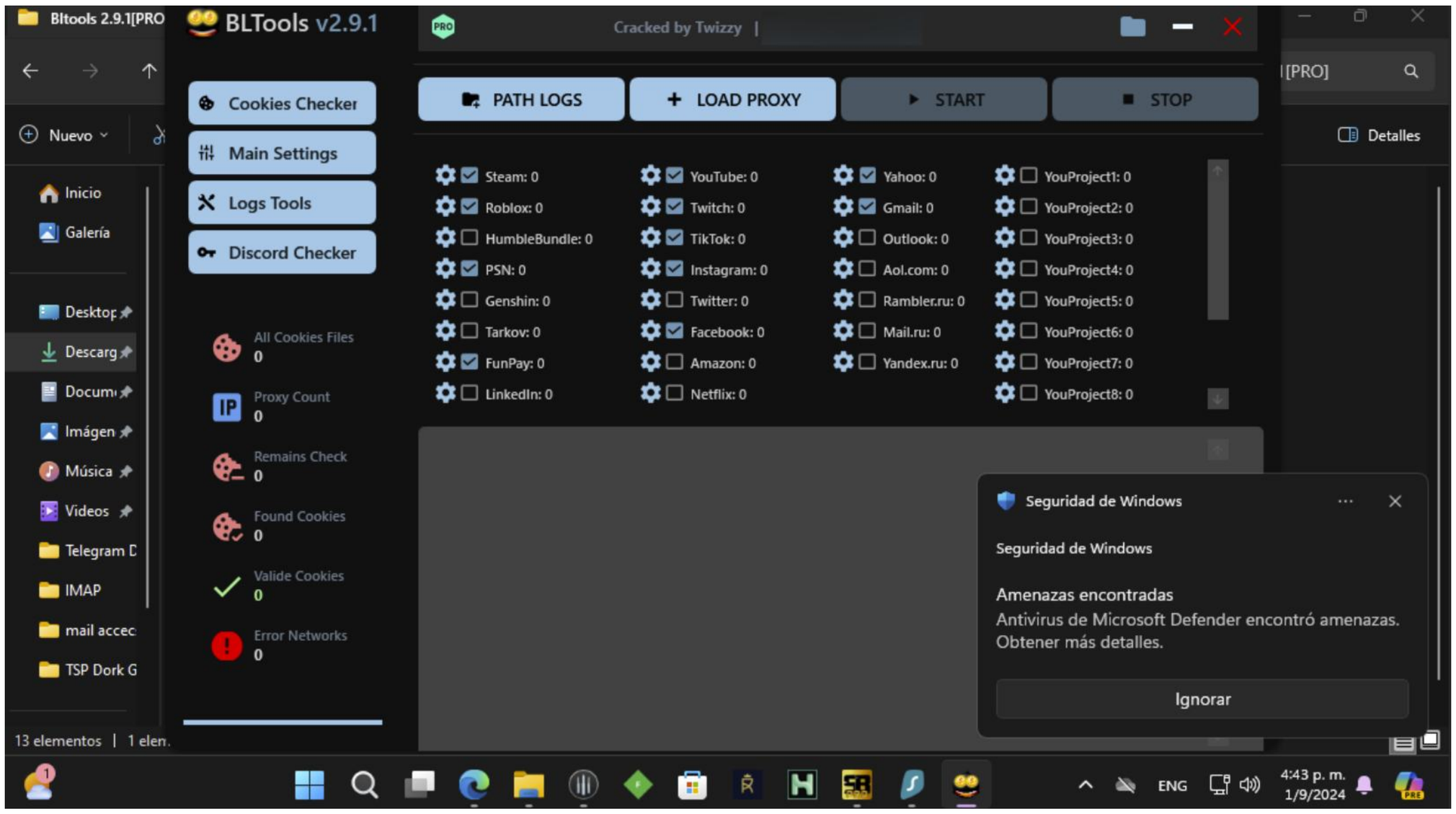
Location: Nigeria

VM/Proxy: No

Additionally reviewing the screenshot from the threat actor's desktop, it appears that this actor has multiple potentially AI-generated pictures for WhatsApp and Facebook accounts. Based on this data it isn't possible to definitively state what the actor is involved in but based on browser history we identified the following as a (highly speculative) potential workflow.

- Leverage combolists and SilverBullet to gain access to Facebook and Whatsapp accounts.
- After gaining access the actor visits the compromised users Facebook profile settings to review and possibly change account information. This is a crucial step in gaining control over the compromised accounts. By visiting the notification setting, they can alter alerts to prevent the original user from being notified of suspicious activity, such as a login from an unfamiliar location.
- Next, the attacker focuses on the Login Alerts page and Saved Logins, ensuring they can access the account in the future and monitor any other logins that might signal the original owner noticing suspicious behavior. The attacker might check for device-based logins, which would make future logins easier without needing to re-enter credentials.
- The attacker repeatedly accesses Facebook's password recovery and login help pages. This activity likely indicates an attempt to reset passwords and lock the original owners out of their accounts. By gaining control over password reset procedures, the attacker ensures continuous access and control over the compromised accounts.
- Accessing WhatsApp suggests that the attacker might be using compromised Facebook accounts to target or impersonate victims on WhatsApp. Because Facebook and WhatsApp accounts are often linked, this could expand the attacker's reach, allowing them to communicate directly with contacts of the compromised accounts.
- The attacker replaces WhatsApp information with fake information and photos, likely created with generative AI in order to lure victims into a romance scam where they are either blackmailed or scammed for money.

This is a stark example of how combolists, credentials and stealer logs may have many different use-cases beyond simple financial fraud.



Infection Date: September 1, 2024

Possibly Relevant Tools: Telegram, BLTools, VPNCity, MegaNZ, SilverBullet

Cybercrime Forums: Cracked, Nulled, Cracked Org, CardingForum, Breachforums, CrackingPro, Niflheim, ASCarding, NulledBB

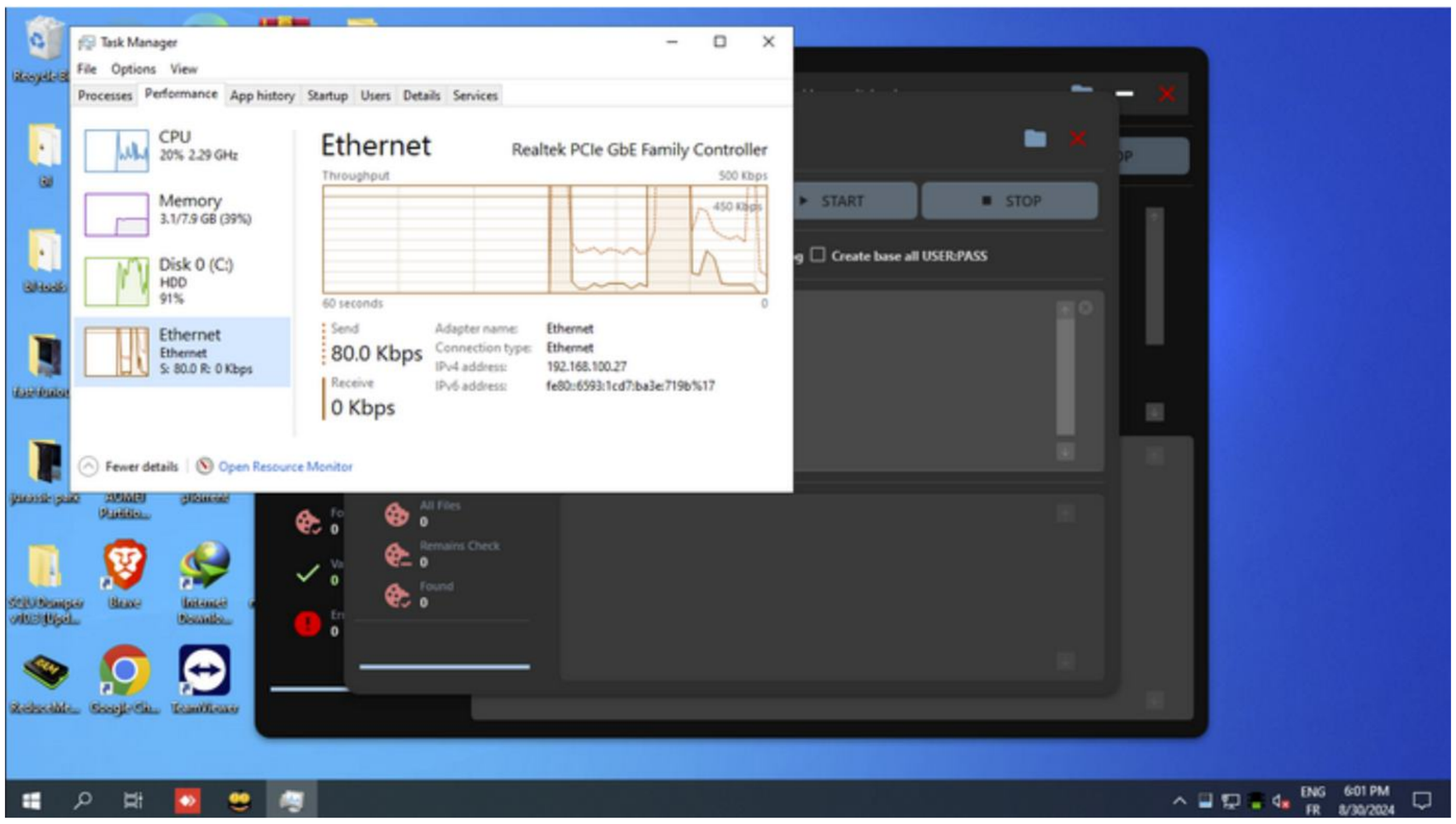
Location: Based on browser history we were able to locate this user to the Dominican Republic

VM/Proxy: VM No, VPN yes

Our next victim has also downloaded a cracked version of BLTools and is in the process of actively configuring it to search for high-value credentials and session cookies. Interestingly, while a full review of this user's browser history and saved credentials does personally identify them, we didn’t detect any attempts to actively gain unauthorized access to computer systems despite a plethora of tooling and research (and credentials saved) on their computer.

It is possible that this criminal uses another system to actively try credentials, an incognito browser, or was just beginning their life of crime after months of careful research and planning.

More than 400 personal credentials are saved to the computer in addition to credentials used for criminal activity, including to adult sites, Facebook, and other mainstream sites, all with the user and their significant other's real name in the saved email addresses.



Infection Date: September 1, 2024

Possibly Relevant Tools: Telegram, BLTools, ExpressVPN

Location: Morocco

VM/Proxy: VM Yes, VPN Yes

With this user we have an entirely different and new primary use case for stealer logs. Rather than focus on financial accounts, crypto wallets, or Facebook accounts this user seems intent on a substantially different use of the data: namely stealing Netflix and Spotify accounts. Now a reasonable observer may question why a threat actor would choose to focus on Netflix accounts in a stealer log given the increased difficulty in monetization.

Financial accounts are tough; banks, crypto exchanges, and other financial services organizations spend millions of dollars on sophisticated anti-fraud systems and often mandate 2FA for their online banking customers.

https://www.netflix.com/login
https://www.onbuy.click/index.html
https://www.netflix.com/signup/regform
https://app.hotspotshield.com/sign-in
https://shahid.mbc.net/ar/widgets/login-password
https://www.netflix.com/ma-fr/login
https://www.netflix.com/ma-fr/Login
https://www.netflix.com/ma-fr/login
https://www.netflix.com/ma-fr/login
https://www.netflix.com/ma-fr/login
https://www.netflix.com/ma-fr/login
https://www.netflix.com/ma-fr/login
https://accounts.google.com/v3/signin/challenge/pwd
https://www.netflix.com/ma-fr/login
https://www.netflix.com/ma-fr/login
https://www.netflix.com/ma-fr/login

This means that to successfully make significant money off of financial fraud requires some degree of technical skills, along with large amounts of time to identify working TTP's and defeat anti-fraud mechanisms. Conversely Netflix and Spotify accounts are almost the polar opposite. These accounts often have 2FA optionally, but do not mandate it for customers.

This makes them an easy target, particularly for low sophistication threat actors. Netflix and Spotify accounts can be sold on the cybercrime ecosystem for $10-$20 on forums such as Cracked and Nulled to other low sophistication actors.

In this specific case based on the saved credentials it appears that once the actor gained access to a Netflix account, they would change the username to a variation of client.netflixnumber@Hotmail.com along with a password change, that also usually included Netflix.

These accounts could then be easily sold in the cybercrime ecosystem.

Concluding Thoughts

Cybercrime is sophisticated. Notice in each of our examples actors used numerous different free and paid services to aid in their process, including legitimate services such as VPNs and file sharing sites. Threat actors utilize info stealers in a variety of ways - all in the pursuit of profits but the path to get to profits is different in each case.

In each and every step there is a complex ecosystem that supports criminal activity. If a user had to design, distribute, and harvest the results from their own malware cybercrime would be forced to operate on a dramatically smaller scale. But, the same economics principles that have enabled our modern society also apply to cybercrime - role specialization, economies of scale, and monthly subscriptions power a multi billion dollar criminal ecosystem that has roots around the world.

About Flare

The Flare Threat Exposure Management (TEM) solution empowers organizations to proactively detect, prioritize, and mitigate the types of exposures commonly exploited by threat actors. Our platform automatically scans the clear & dark web and prominent threat actor communities 24/7 to discover unknown events, prioritize risks, and deliver actionable intelligence you can use instantly to improve security.

Flare integrates into your security program in 30 minutes and often replaces several SaaS and open source tools. Learn more by signing up for our free trial.

Want to learn more about better protecting your digital assets with Flare?

Sign Up for a Free Trial

flare.io

hello@flare.io

Gartner Peer Insights™ 4.9 ★ ★ ★ ★ ★