Arkose Labs

Threat Actor Dossier

Veiled Marble: Diverting Innocents Toward Hidden Exploits

OVERVIEW

Veiled Marble is a phishing-as-a-service (PhaaS) provider, making it part of a subset of CaaS providers, based on the ACTIR taxonomy. These threat actors do not carry out attacks themselves, but rather, they provide scammers with advanced tools to do so. It is not uncommon for the providers of these attack tools to have developed them for their own use first. Although ACTIR has no direct evidence, it is not hard to believe that Veiled Marble likewise created the toolkit to conduct its own attacks and has now pivoted to selling it to other fraudsters, which can be more profitable and less risky.

Phishing attacks are getting more sophisticated, and that is due in large part to Veiled Marble's creative techniques. By providing a toolkit that scammers can use to quickly and effectively launch attacks, it is part of a rising trend in the use of reverse proxies in phishing scams.

Here's how it works: A scammer sets up a reverse-proxy server between a user and a genuine website. The user believes that they are interacting directly with the legitimate site, but their requests are passing through to the attack server. See the diagram on page 9.

Since many websites now incorporate OTP/MFA authentication alongside login credentials, the old approach of simply creating fake websites is not enough to scam genuine users. To run successful phishing campaigns, today's scammers need to step up their strategy. A reverse proxy used in phishing attacks allows the scammer to steal a session cookie and compromise MFA whilst serving a complete 1:1 copy of the target website.

Increasingly Creative Attacks

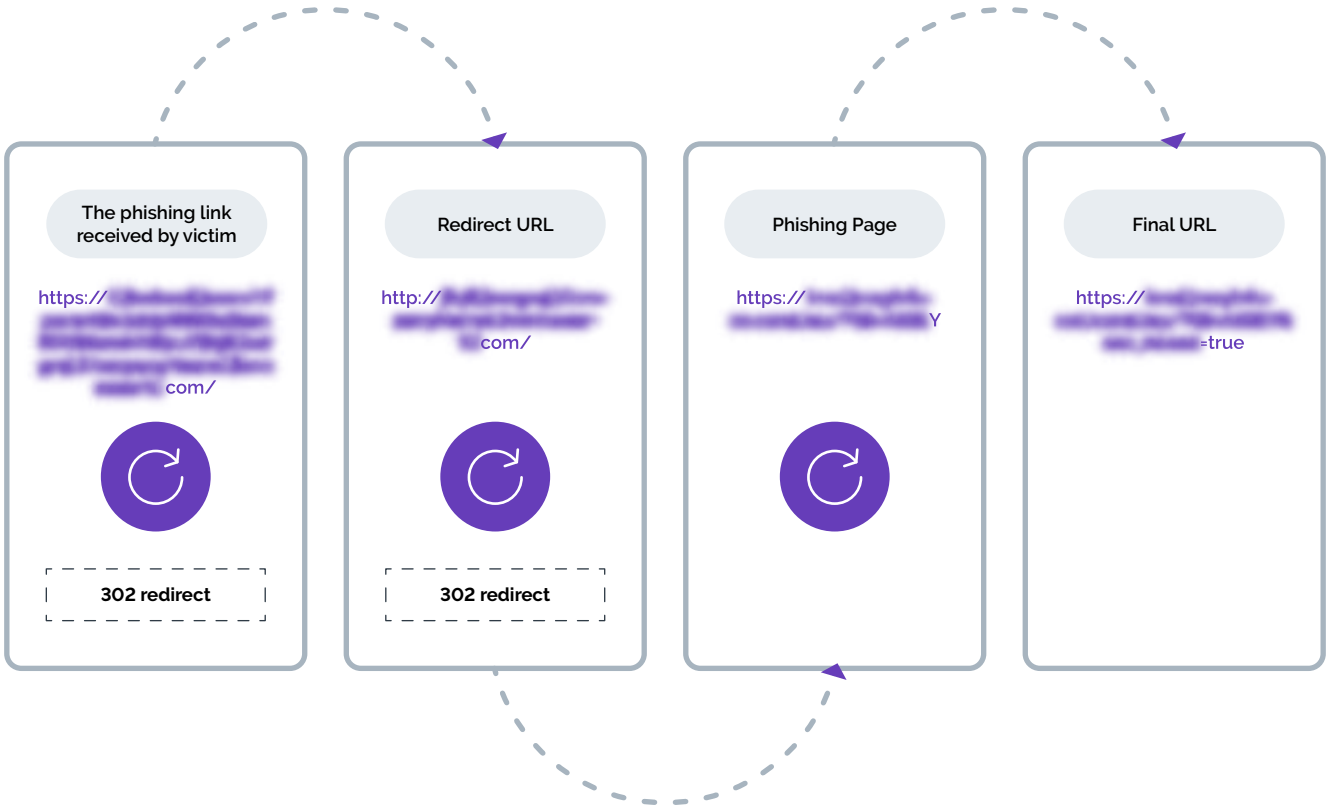
Many phishing tools are open source and allow scammers to set up reverse-proxy attacks. But Veiled Marble, which emerged in 2022, offers more features than other phishing libraries. With the platform that paid subscribers can access, the ready-to-use configurations make it easier for scammers to set up and launch their attacks. As a result, even amateurs can create and deploy sophisticated attacks in minutes.

Veiled Marble is distinguished by its ease of use. With a server and domain ready, an attacker could launch an attack from scratch in about an hour. If the goal is to set up multiple attacks, the process remains efficient. For example, if an attacker wants to create a new campaign and the system is already configured, the setup can be completed in just two minutes, resulting in a fully operational scheme ready to harvest credentials.

Many of these more refined phishing schemes are harder to spot than ever. For example, when attacking a global job search platform, Veiled Marble was used to send phishing emails with links to the platform's genuine ".com" domain. But there was a vulnerability to redirect back to its phishing site. These increasingly creative and sneaky attacks are a specialty of Veiled Marble, allowing scammers to defraud even vigilant users.

Veiled Marble TTPs

- Tactic 1: Open Redirects: A Very Effective Attack
    - Allows phishing attacks to exploit redirects in legitimate sites to create a false sense of security in the victim.
    - Technique:
        - Open redirection occurs when a trusted domain allows redirection to an untrusted external domain via url parameters. This flaw relies on a user's trust of the redirecting source, which in turn sends the victim to a phishing or compromised site.



- Tactic 2: MFA Compromise: Reverse-Proxy Phishing (Initial Access)
    - Veiled Marble acts as a reverse proxy, intercepting login requests between users and legitimate companies' websites.
    - Techniques:
        - Capturing credentials and session cookies in real time, allowing threat actors to bypass MFA.
        - Veiled Marble intercepts, relays MFA codes and obtains session cookies that allow attackers to access accounts.
    - Procedure: Phishing emails or links lead victims to fake login pages that replicate the real company's website.

- Tactic 3: Credential Harvesting (Persistence)
    - Technique: Storing harvested credentials for later use or sale on the dark web.
    - Procedure: Using Veiled Marble's user-friendly dashboard to automate credential collection, organization and export.

Veiled Marble empowers scammers to execute precise and efficient social engineering attacks designed to access users' credentials. By deploying tailored phishing campaigns aimed at high-value targets like executives or financial personnel (known as whaling) as well as general consumers, scammers use convincing emails, SMS (smishing) and even phone calls (vishing) to manipulate victims into disclosing sensitive login details. These attacks often exploit trust by mimicking familiar sources, leveraging personalized data to bypass user suspicion and enhance the likelihood of unauthorized access. Through a mix of digital and psychological tactics, Veiled Marble enables scammers to breach accounts with minimal detection.

IOC Domains and IPs Linked to Veiled Marble: 2024

ACTIR threat researchers have uncovered the following indicators of compromise.
Redirection domains:

- msdnmail[.]net
- [redacted][.]pro
- top-cyber[.]club
- rproxy[.]io
- login-live.rproxy[.]io
- gw1.usd0182738s80[.]click:9000
- gw2.usd0182738s80[.]click:9000
- cpanel.[redacted][.]pro
- cpanel.pua75npooc4ekrkkppdglaleftn5mi2hxsunz5uuup6uxqmen4deepyd[.]onion

Email IP sources:
147[.]78[.]47[.]250
185[.]158[.]251[.]169
194[.]76[.]226[.]166

To view a list of IOC domains and IPs linked to Veiled Marble in 2023, see the Appendix.

Example of Impact

The impact of tools such as Veiled Marble are far-reaching and used by scammers to kickstart other lucrative campaigns, such as business email compromise (BEC).

Earlier this year, threat actor group TA4903 engaged in persistent credential phishing by impersonating U.S. government entities and targeting various industries to gather corporate credentials. The group used Veiled Marble to launch email campaigns with PDF attachments, QR codes or links directing recipients to phishing sites. By leveraging Veiled Marble, TA4903 bypassed MFA and seized authentication tokens.

In 2023, the group broadened its tactics to mimic legitimate suppliers of its targeted companies. Using data from phishing and credential theft, TA4903 manipulated email threads with lookalike domains and spoofed reply-to addresses, leading to invoice fraud and payroll redirection.

Pricing

Veiled Marble recently changed its pricing model, which is subscription based. Prices now fluctuate according to how many days of access the buyer will have as follows:

10-day access	$150
20-day access	$250
31-day access	$400

Each subscription includes access to all of the Veiled Marble phishing services.

Veiled Marble accepts only the following cryptocurrency: Bitcoin, USDT, XMR and ETH. It rotates wallets for payments regularly and payments are withdrawn anonymously.

ACTIR estimates that Veiled Marble's minimum profit equals US$505,000.

> "Veiled Marble doesn't push many updates. It's extremely low maintenance and low cost to operate. Most of the costs are offloaded onto Veiled Marble buyers, such as the cost of the server, the domain and the proxies."
> **- ACTIR threat researcher**

Technology and Features

Veiled Marble offers phishing kits that attack companies including but not limited to:

Veiled Marble targets popular repositories like PYPI and NPMJS to launch attacks. Its goal is to phish owners of major code repositories used in other software. By compromising such accounts, Veiled Marble can distribute malicious code to any project relying on the affected repository—a significant threat to the software ecosystem.

Attackers need to BYO a domain and server. Veiled Marble provides attackers with the full attack infrastructure that they need, like scripts, guides and storage (captured data and cookie logs), that are used to collect credentials and templates for creating fake emails and websites. Veiled Marble provides video tutorials, using either an AI-generated voice or no voice at all.

With an intuitive UX, detailed dashboards and configurations that are ready in one click, Veiled Marble walks attackers through the process of creating a phishing attack. The platform even offers bot protection on the domains that subscribers create.

> "Its UX is fantastic and makes it easy to navigate and use. It's very professional, which reflects the professionalism of the services and that it considers itself an actual business."
> **- ACTIR threat researcher**

Veiled Marble takes a pragmatic approach by off-loading risk onto its customers. When bad actors set up servers hosting phishing material, hosting providers typically shut down their entire accounts once the activity is detected. The same applies to domains—if a provider discovers or receives reports that a domain is being used for phishing, it will terminate the account and disable the domain. To avoid these disruptions, Veiled Marble structures its business model to transfer these risks to its clients.

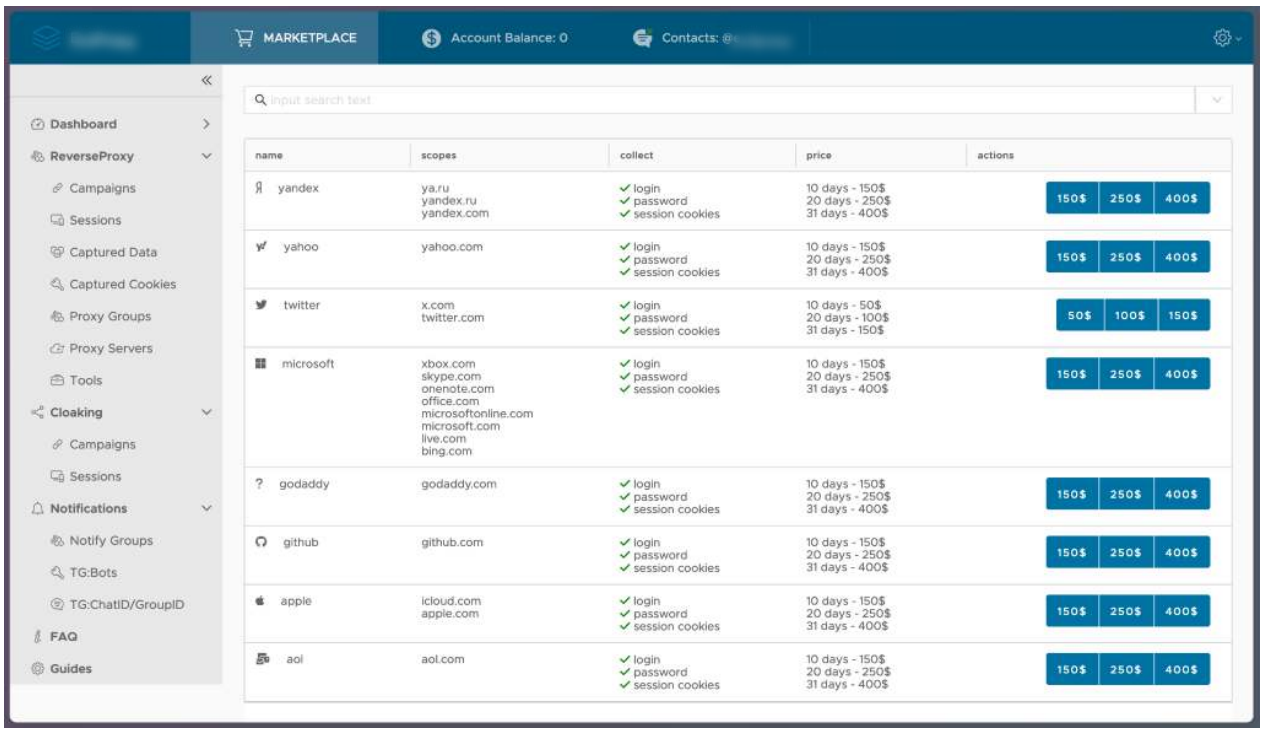


Image 1: This screenshot depicts the "Marketplace" for Veiled Marble. This is where attackers are able to purchase individual sites (or services as Veiled Marble calls them) to attack.

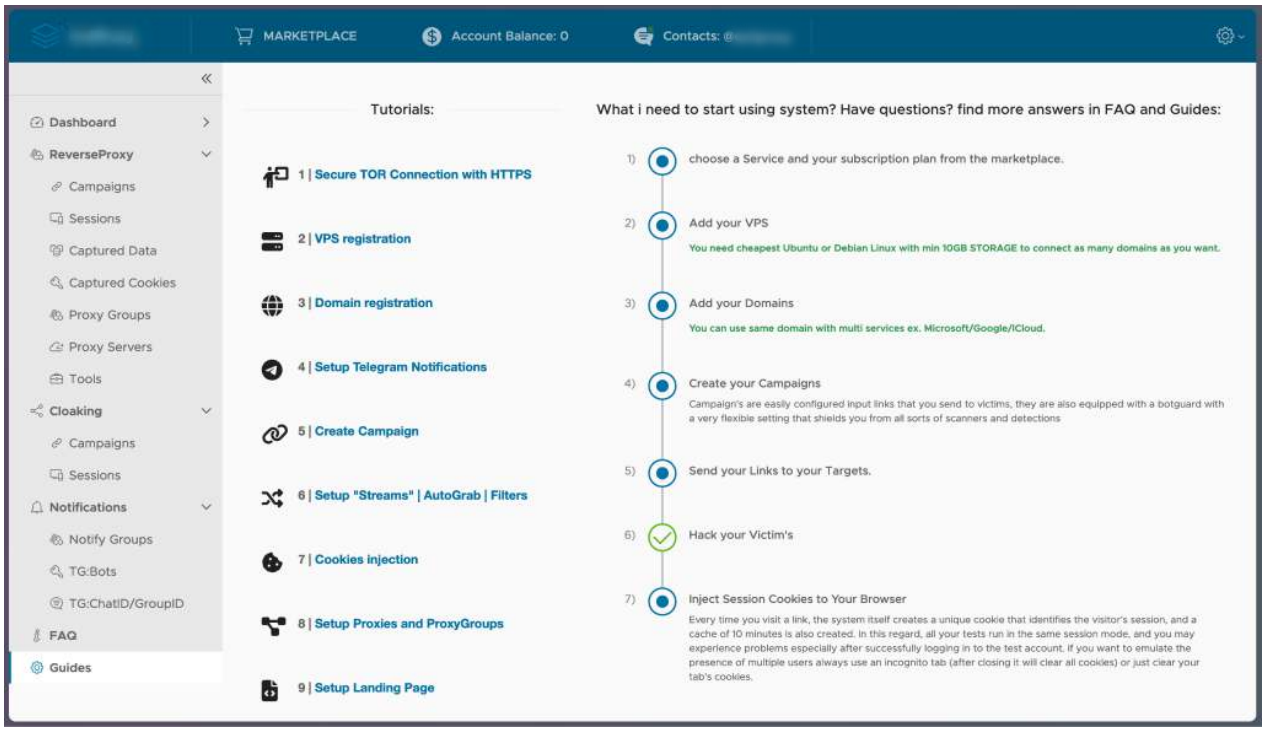


Image 2: Veiled Marble provides its customers with extensive guides and documentation on the setup procedure and phishing attacks. It even goes into detail with explanations on how to bypass Cloudflare and avoid browser-based phishing "red flags."

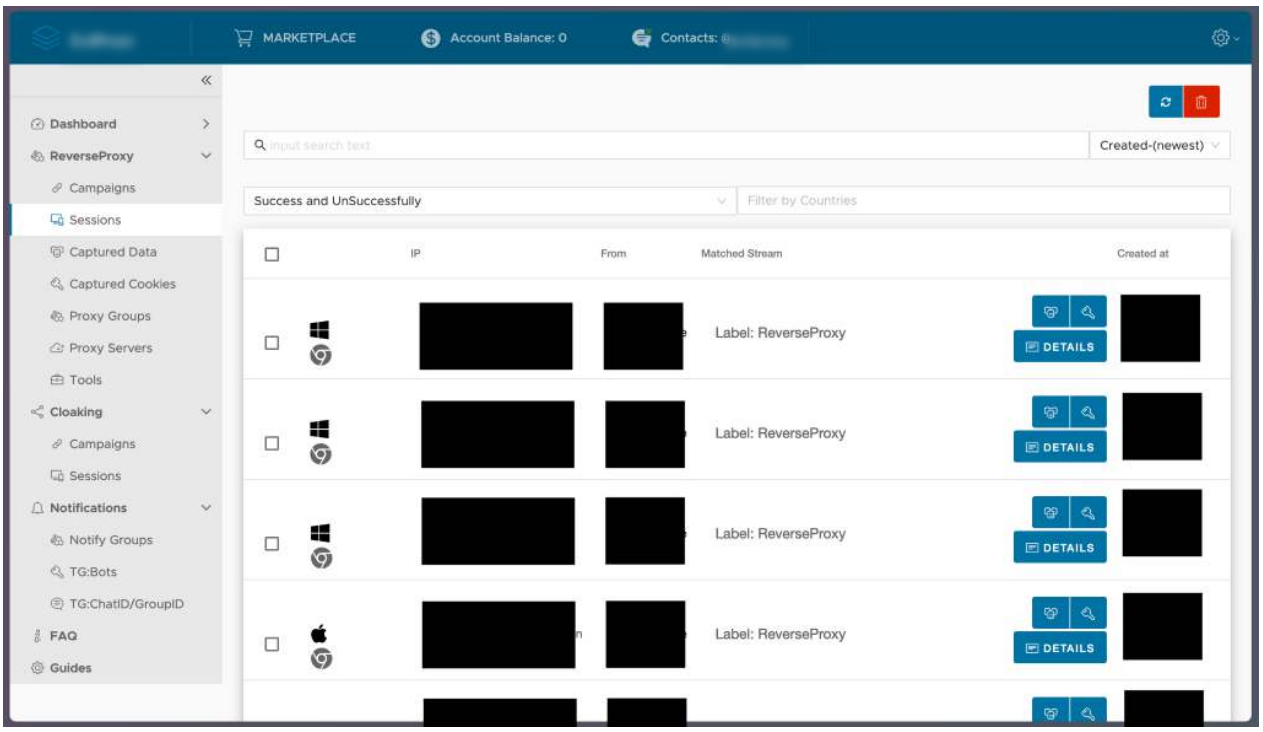


Image 3: An obfuscated screenshot of the "Successful Sessions" tab. This page shows all sessions that have browsed the phishing campaign created by Veiled Marble; it lists all details about the session such as fingerprint data, location, IP and more.

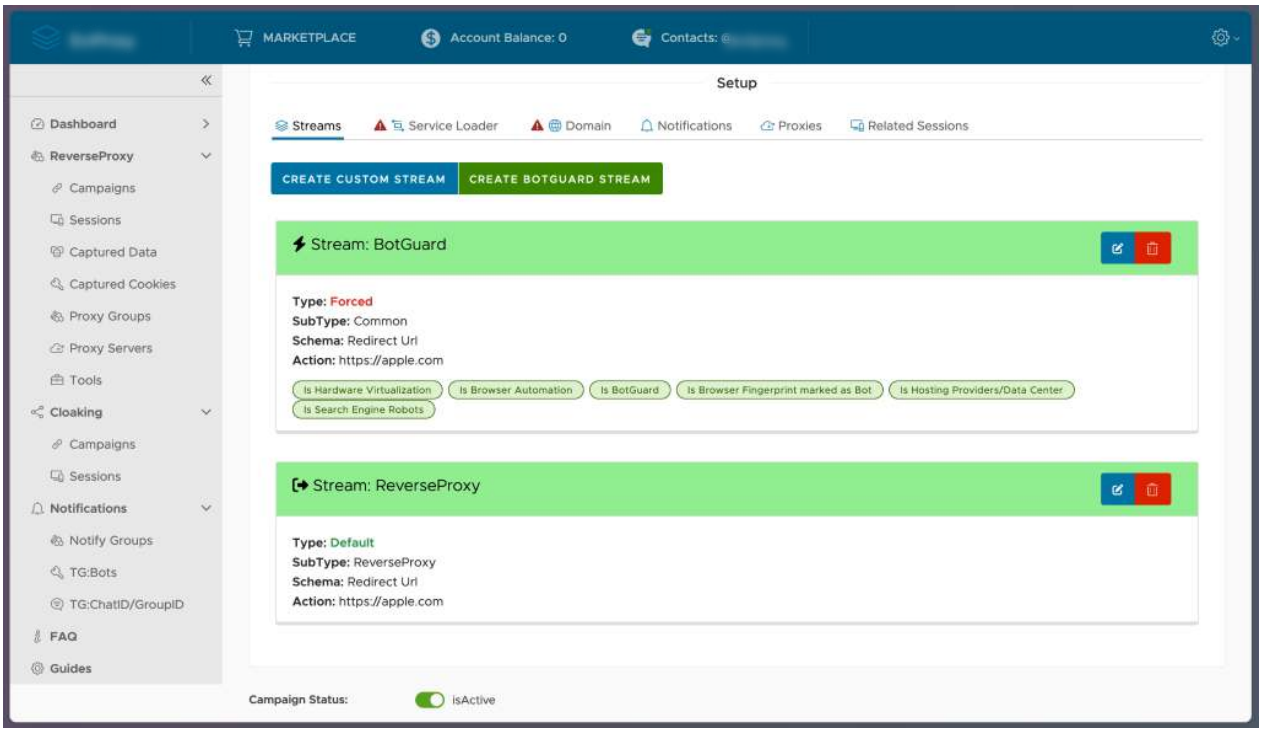


*Image 4: This is the configuration page for setting up a phishing campaign. It's an extremely easy process that involves selecting the service (site to attack), which phishing domain to use and any Telegram channels for the notifications. Veiled Marble offers a unique feature that causes any non-phishing target (search engines, security gateway scanners, automated phishing detection) **to see the REAL site, not the phishing site.***

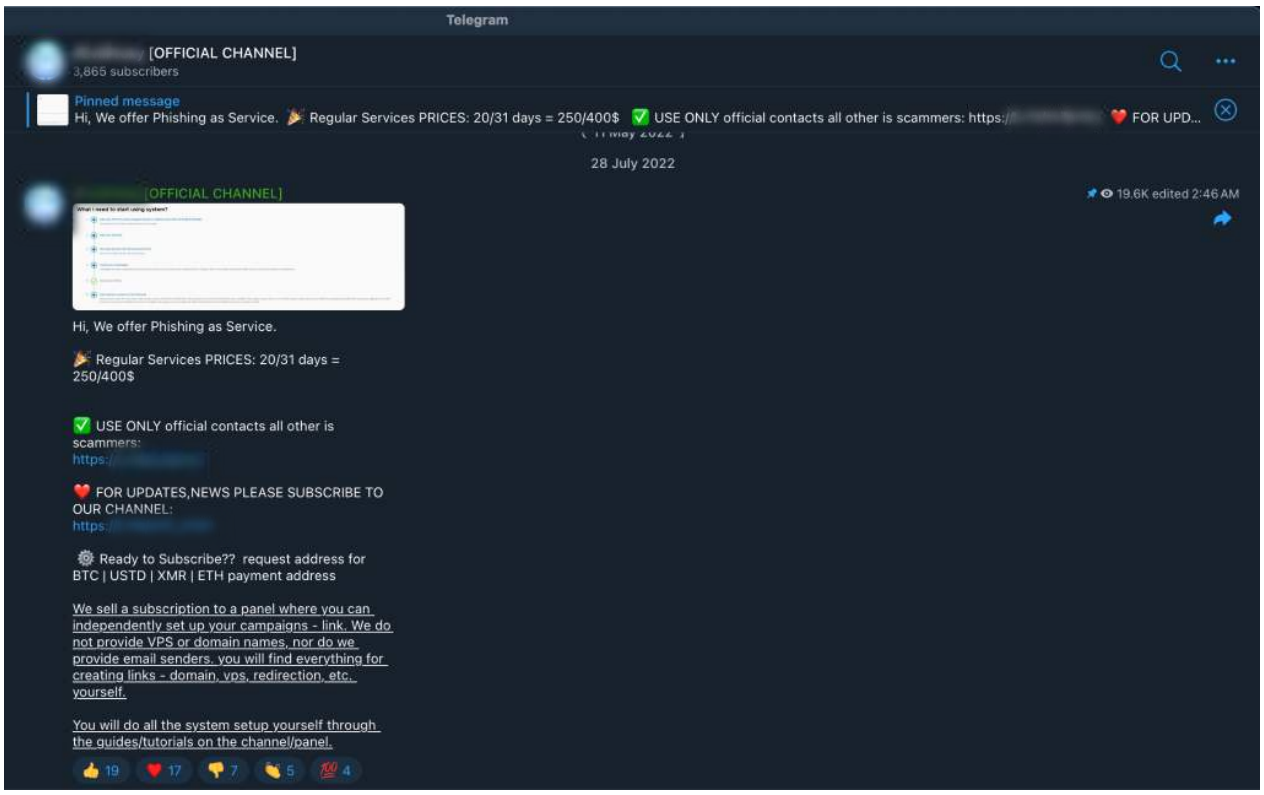


Image 5: Veiled Marble's Telegram channel has over 3,865 subscribers. Ironically, numerous other Telegram servers are pretending to be this one and scamming unsuspecting attackers. Payments are accepted via crypto and the dashboard is set up within 24 hours with full access.

Monitoring and Analysis

Multiple phishing libraries exist. Reports show that phishing continues to increase, with 3.5 billion spam emails sent daily.

ACTIR is actively monitoring reverse-proxy phishing attacks, MFA compromise trends and tracking updates to the key functionality available to Veiled Marble subscribers. New survey data shows that 57% of enterprises are concerned about these attacks, which so easily bypass MFA.

Abatement

Arkose Phishing Protection detects and blocks reverse-proxy phishing attack campaigns, protecting users by preventing the interception of MFA/2FA codes. It's a way for businesses to detect phishing attacks in real time and manage phishing detection rulesets.

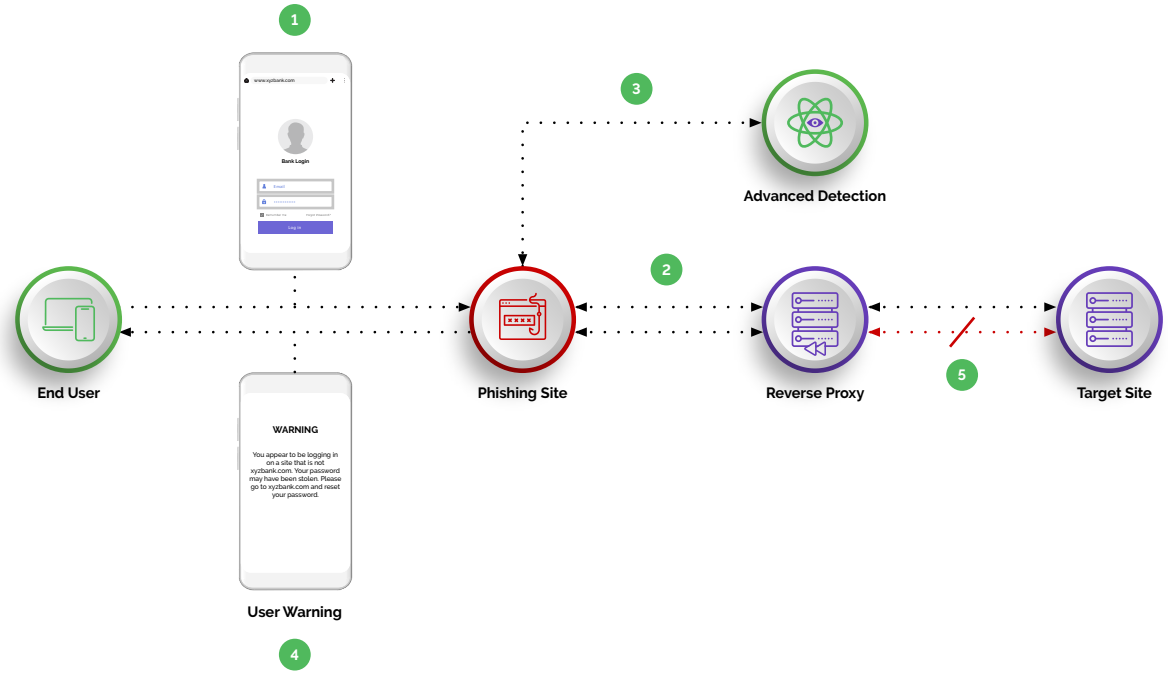


Diagram 1: How reserve-proxy phishing attacks work.

When ACTIR conducted an analysis of requests seen on three login endpoints, the threat researchers observed about 90,000 suspicious sessions originating from 1,400 domains. Of the 1,400 suspicious domains, ACTIR picked a sample of 250 domains for further analysis. Of those 250 domains, 49 were created in less than 60 days, which means they were likely created for attack purposes; 191 domains were short-lived and soon disappeared.

The team also observed that out of the 250, only 10 were marked as suspicious by traditional phishing detection/scanning methods. So, if protections hadn't been deployed, 240 suspicious domains would have gone unnoticed and would have been free to do harm to businesses and consumers.

Analyzed the data gathered from 3 login flows for a period of 30 days.

Suspicious Sessions	~90,000
Top-level Domain	~1400

Analysis on a sample size of 250 domains.

Signals of Malicious Intent

Domain age less than 60 days (206 domains analyzed)	49
Short life websites/URLs (250 domains analyzed)	191

Compared to Static Detection Methods

Domains detected by Transparency Report (250 domains analyzed)	10

Image 6: Impact of reverse-proxy phishing attacks.

Interesting Twist

When researching Veiled Marble, it became clear that other bad actors had actually created Telegram sites that impersonated Veiled Marble. The intention was to trick other fraudsters into thinking they were paying for Veiled Marble, when in fact they were paying the other bad actors. Truly there is no honor among thieves. This observation also reveals the popularity and effectiveness of Veiled Marble.

Conclusion

Veiled Marble is one of the most advanced PHaaS actors operating on the dark web today. It takes the following three steps to obfuscate its identity:

1. The service has been built on the dark web onion router.

2. It leverages a unique code name that is used only on Telegram and not in any other forum.

3. It doesn't advertise publicly on the clear net. Sometimes bad actors will advertise their services on hack forums to try and get business, whereas Veiled Marble has focused on creating an outstanding "product" that is easy to use and highly effective. As a result, its popularity and word-of-mouth drive its illicit "customer acquisition" strategy, thus business growth.

Veiled Marble is a formidable foe that is user-friendly enough to allow even inexperienced scammers to set up campaigns that are hard for users to catch and businesses to stop. Most global enterprises rely on security gateways to scan emails for reverse-proxy attacks, but Veiled Marble has rendered these defenses ineffective.

Gateways can no longer reliably detect and block such attacks, pushing enterprises to adopt modern protections. ACTIR has observed that when modern defenses thwart Veiled Marble's attacks or make attacks cost-prohibitive, it removes the targeted company's domains and brand name from its dashboard, thus eliminating the company's vulnerability to these specific phishing attacks. This removal appears to be indefinite, signaling Veiled Marble's strategic shift away from resistant targets.

> "Veiled Marble doesn't appear to actively bypass phishing protections. Instead, it removes the targeted brand from its support once phishing defenses are implemented on the brand's site."
> **- ACTIR threat researcher**

Given Veiled Marble's lengthy list of supported companies, most if not all digital consumers are in this threat actor's path of harm. It's now critical that businesses step up their phishing prevention strategies to protect their websites from being the latest target of attackers using Veiled Marble.

> "Veiled Marble has streamlined the process for attackers to set up malicious websites for phishing consumers and conducting BEC."
> **- ACTIR threat researcher**

Recommendations

1. Implement Day-One Security Training for High-Privilege Employees

New employees with deep access privileges are prime targets for adversaries like Veiled Marble, which exploit human error to infiltrate systems. Tailored onboarding security training should educate these employees on recognizing phishing attempts, securing credentials and following best practices to avoid targeted attacks.

Why it matters: Providing robust security awareness training from day one reduces the risk of human vulnerabilities, creating a strong first line of defense against advanced threats.

2. Deploy Intelligent Bot Management to Detect Reverse-Proxy Behavior

Adversaries like Veiled Marble use reverse-proxy phishing to intercept authentication tokens and credentials in real time. Detect this behavior by implementing advanced telemetry and behavioral analytics to identify anomalies such as unusual session replays or token usage patterns.

Why it matters: Reverse-proxy phishing bypasses traditional defenses. Intelligent bot management solutions disrupt these tactics at the session level, ensuring secure authentication and reducing risk.

3. Leverage Adaptive Challenges to Neutralize Open Redirect Exploits

Threat actors often exploit open redirects on trusted domains to redirect users to phishing sites. Adaptive challenges can identify traffic anomalies and impose friction only on suspicious users, preventing these attacks without disrupting legitimate activity.

Why it matters: Adaptive challenges strike a balance between strong security and seamless user experience, protecting businesses from reputational harm caused by open redirect vulnerabilities.

4. Strengthen Multi-Factor Authentication (MFA) with Real-Time Risk Assessments

Veiled Marble circumvents MFA by phishing tokens through man-in-the-middle attacks. Enhancing MFA with dynamic risk assessments ensures token integrity by flagging intercepted or manipulated sessions in real time.

Why it matters: Protecting the integrity of MFA safeguards account security at scale, which is essential for businesses managing sensitive user data.

5. Harness a Cross-Industry Risk Intelligence Network for Proactive Defense

Evolving tactics like those employed by Veiled Marble demand insights beyond individual industries. A cross-industry risk intelligence network provides real-time threat data, helping businesses stay ahead of adversaries by identifying and neutralizing attack patterns early.

Why it matters: Leveraging global threat intelligence enables proactive defenses, offering comprehensive protection against sophisticated attacks.

6. Rely on SOC Support for Threat Monitoring and Incident Response

A 24/7/365 Security Operations Center (SOC) provides critical customer support, offering real-time threat monitoring, incident response and expert guidance to combat adversaries like Veiled Marble. Access to tailored solutions ensures businesses can address threats effectively and efficiently.

Why it matters: SOC-backed support from vendor partners helps businesses quickly adapt to evolving threats, minimize downtime and maintain seamless security operations for end users.

About ACTIR

Arkose Cyber Threat Intelligence Research (ACTIR) unit is a dedicated and specialized counterintelligence team embedded in Arkose Labs. Composed of full-time experts in cyber threat analysis, digital forensics and cybersecurity operations, ACTIR's primary mission is to identify, assess and neutralize sophisticated cyber threats. By leveraging cutting-edge technologies and methodologies, ACTIR provides actionable intelligence and orchestrates coordinated responses to mitigate threats posed by entities like Greasy Opal and Veiled Marble. Recently it partnered with Microsoft DCU and law enforcement to disrupt Vietnamese threat actor group Storm-1152. Through collaboration with Arkose Labs' award-winning SOC, ACTIR plays a pivotal role in enhancing the cybersecurity posture and ensuring the integrity of the digital infrastructure of Fortune 500, category-leading enterprises and trailblazing businesses. Access ACTIR's threat research taxonomy.

Contact ACTIR to discuss these insights: actir@arkoselabs.com

Appendix

IOC domains and IPs linked to Veiled Marble in 2023

Redirection domains:

01-net[.]com
837[.]best abbotsfordbc[.]com
ae-lrmed[.]com
andrealynnsanders[.]com
bdowh[.]com
cad-3[.]com
cdjcfc[.]com
chiromaflo[.]com
cmzo-eu[.]cz concur[.]bond concurcloud[.]us
concursolution[.]us concursolutions[.]info cualn[.]com
d8z[.]net
dealemd[.]com
dl2b[.]com
dsa-erie[.]com
dse[.]best dse[.]buzz dsena[.]net e-csg[.]com
etrax[.]eu
farmacgroup[.]ca faxphoto[.]com
fdh[.]aero
finsw[.]com
fortnelsonbc[.]com
g3u[.]eu
greatbayservices[.]com
Gwcea[.]com
indevsys[.]com
inteproinc[.]com
jxh[.]us
k4a[.]eu
kayakingbc[.]com
kirklandellis[.]net
kofisch[.]com
ld3[.]eu
mde45[.]com
mjdac[.]com
n4q[.]net na-7[.]com
na3[.]wiki
nilyn[.]us
p1q[.]eu
pagetome[.]com
parsfn[.]com
pbcinvestment[.]com
Phillipsoc[.]com
pwsarch[.]com
re5[.]eu
sloanecarpet[.]com
ssidaignostica[.]com
tallwind[.]com[.]tr
ukbarrister[.]com
utnets[.]com
uv-pm[.]com
vleonard[.]com
wattsmed[.]com
whoyiz[.]com
wj-asys[.]com
wmbr[.]us
Wwgstaff[.]com
xp1[.]us
xstpl[.]com

Email IP sources:

154.29.75[.]192
185.241.52[.]781
185.250.243[.]176
185.250.243[.]38
198.44.132[.]249
212.224.107[.]12
45.8.191[.]151
45.8.191[.]17
74.208.49[.]213
77.91.84[.]52
78.153.130[.]178
87.120.37[.]47
104.183.206[.]97
172.102.23[.]21
191.96.227[.]102
90.92.138[.]71