

# EvilProxy Phishing-as-a-Service with MFA Bypass Emerged in Dark Web

---

 [resecurity.com/blog/article/evilproxy-phishing-as-a-service-with-mfa-bypass-emerged-in-dark-web](https://resecurity.com/blog/article/evilproxy-phishing-as-a-service-with-mfa-bypass-emerged-in-dark-web)

[Back](#)

Cybercrime Intelligence

5 Sep 2022

MFA, Dark Web, Phishing, PhaaS, ATO, BEC, PyPi, supply chain

Following the recent Twilio hack leading to the leakage of 2FA (OTP) codes, cybercriminals continue to upgrade their attack arsenal to orchestrate advanced phishing campaigns targeting users worldwide. Resecurity has recently identified a new Phishing-as-a-Service (PhaaS) called **EvilProxy** advertised in the Dark Web. On some sources the alternative name is **Moloch**, which has some connection to a phishing-kit developed by several notable underground actors who targeted the financial institutions and e-commerce sector before.

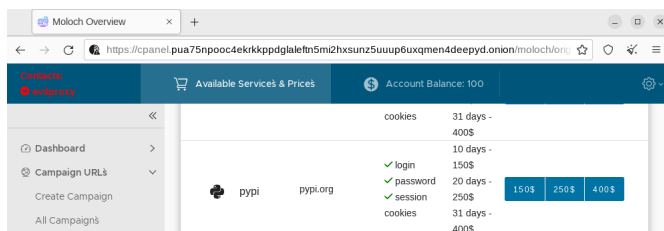
While the incident with Twilio is solely related to the supply chain, cybersecurity risks obviously lead to attacks against downstream targets, the productized underground service like EvilProxy enables threat actors to attack users with enabled MFA on the largest scale without the need to hack upstream services.

EvilProxy actors are using **Reverse Proxy** and **Cookie Injection** methods to bypass 2FA authentication – proxyfying victim's session. Previously such methods have been seen in targeted campaigns of APT and cyberespionage groups, however now these methods have been successfully productized in EvilProxy which highlights the significance of growth in attacks against online-services and MFA authorization mechanisms.

Based on the ongoing investigation surrounding the result of attacks against multiple employees from Fortune 500 companies, Resecurity was able to obtain substantial knowledge about EvilProxy including its structure, modules, functions, and the network infrastructure used to conduct malicious activity. Early occurrences of EvilProxy have been initially identified in connection to attacks against Google and MSFT customers who have **MFA enabled** on their accounts – either with **SMS** or **Application Token**.

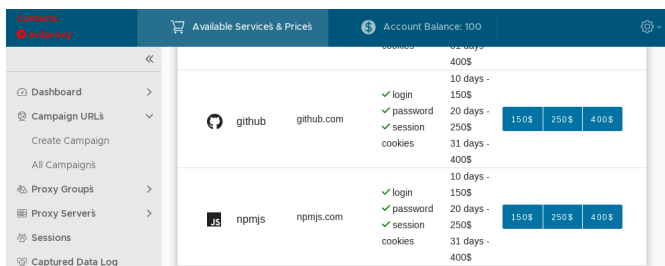
The first mention of EvilProxy was detected early May 2022, this is when the actors running it released a demonstration video detailing how it could be used to deliver advanced phishing links with the intention to compromise consumer accounts belonging to major brands such as **Apple, Facebook, GoDaddy, GitHub, Google, Dropbox, Instagram, Microsoft, Twitter, Yahoo, Yandex** and others.

Notably, EvilProxy also supports phishing attacks against **Python Package Index (PyPi)**:



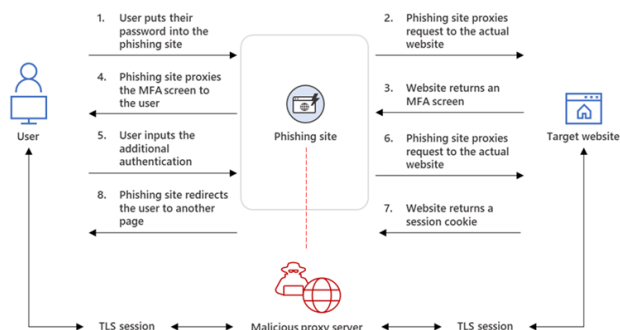
The official software repository for the Python language (Python Package Index (PyPI)) has been recently said (last week) that project contributors were subject to a phishing attack that attempted to trick them into divulging their account login credentials. The attack leveraged **JuiceStealer** (as the final payload after the initial compromise) and according to Resecurity's HUNTER team findings - related to EvilProxy actors who added this function not too long before the attack was conducted.

Besides PyPi, the functionality of EvilProxy also supports **GitHub** and **npmjs** (widely used JavaScript Package Manager by over 11 million developers worldwide) enabling supply chain attacks via advanced phishing campaigns. It's highly likely the actors aim to target software developers and IT engineers to gain access to their repositories with the end goal to hack "**downstream**" targets. These tactics allow cybercriminals to capitalize on the end users insecurity who assume they're downloading software packages from secure resources and don't expect it to be compromised.



## How it works?

EvilProxy uses the “Reverse Proxy” principle. The reverse proxy concept is simple: the bad actors lead victims into a phishing page, use the reverse proxy to fetch all the legitimate content which the user expects including login pages - it sniffs their traffic as it passes through the proxy. This way they can harvest valid session cookies and bypass the need to authenticate with usernames, passwords and/or 2FA tokens.



Resecurity has acquired videos released by EvilProxy actors demonstrating how it can be used to steal the victim’s session and successfully go through Microsoft 2FA and Google e-mail services to gain access to the target account.

## Google 2FA

## Microsoft 2FA

EvilProxy is offered on a subscription base, when the end user (a cybercriminal) chooses a service of interest to target (e.g., Facebook or LinkedIn), the activation will be for a specific period of time (10, 20 or 31 days as per the plans description which was published by the actors on multiple Dark Web forums). One of the key actors - **John\_Malkovich**, acting as administrator to vet new customers. The service is represented on all major underground communities including **XSS**, **Exploit** and **Breached**.

[EvilProxy] Phishing as a Service / Фишинг как услуга  
by evilproxy - Monday, July 4, 2022 at 09:48 AM

July 4, 2022, 09:48 AM (This post was last modified: July 12, 2022, 07:03 AM by evilproxy)

**Reverse proxy**  
Our phishing pages are 100% identical

You get LOGIN, PASSWORD, COOKIES and more info about user

Мы можем помочь вам повысить устойчивость к фишинговым атакам. Фишинг как услуга (PhaaS) - это программа повышения осведомленности о безопасности для всех сотрудников организации.  
Наши симуляции фишинга поддерживаются программной платформой собственной разработки. В частности, наше бэкэнд-приложение предлагает полный набор функций, необходимых для проведения фишинговых кампаний.  
**Получите демоверсию совершенно бесплатно на 1 день!**

We can help you improve your resilience against phishing attacks. Phishing as a Service (PhaaS) is a security awareness program for all employees of the organization.  
Our phishing simulations are supported by an in-house developed software platform. In particular, our backend application offers the full set of functionalities required to conduct phishing campaigns:  
**Get a demo completely free 1 day!**

**+ Services:**

- google.com 10/20/31 days = 250/450/600\$ (Clickf)
- microsoft 10/20/31 days = 150/250/400\$ (Hotmail, CORP Remote SSO, ADPS) (Clickf)
- icloud.com 10/20/31 days = 150/250/400\$ (auto token/cookies refresh up to 2 days with internal tool)
- dropbox.com 10/20/31 days = 150/250/400\$ (also sign in with google)
- github.com 10/20/31 days = 150/250/400\$
- linkedin 10/20/31 days = 150/250/400\$
- yandex.ru 10/20/31 days = 150/250/400\$
- facebook.com 10/20/31 days = 150/250/400\$
- yahoo.com 10/20/31 days = 150/250/400\$
- twitter 10/20/31 days = 150/250/400\$
- wordpress.com 10/20/31 days = 150/250/400\$
- pypi.org 10/20/30 days = 150/250/400\$
- www.npmjs.com 10/20/30 days = 150/250/400\$
- rubygems.org 10/20/30 days = 150/250/400\$

**## Protection**

- **Bot Protection** Utilize a variety of algorithms for bot detection and the blocking of unwanted visitors to your resources.
- **Virtualization Detection** Protect your links, from vmware, vbox, and other virtualization.
- **Automation Detection** Protect your links, from headless browsers, selenium, phantom-JS and other automations.
- **Multi Stream** Streams help to manage traffic. You can send definite visitors to definite websites, landing pages, or prevent visitors from visiting some pages.

**+ Information:**

- Advanced Session info (You get LOGIN, PASSWORD, COOKIES and more info about user).
- create unique browser fingerprints.

**+ Extra:**

- proxy manager (with futures like rotation, geo-adaptation).
- domain manager (add own domains with wildcard SSL [\*.\*mydomain.com] in minutes).
- Telegram Notifications

The payment for EvilProxy is organized manually via an operator on Telegram. Once the funds for the subscription are received, they will deposit to the account in customer portal hosted in TOR. The kit is available for \$400 per month in the Dark Web hosted in TOR network.

Bundle	Entry Schemes	Data Collected	Price
dropbox	dropbox.com	✓ login	10 days - 150\$
		✓ password	20 days - 250\$
		✓ session cookies	31 days - 400\$
rubygems	rubygems.org	✓ login	10 days - 150\$
		✓ password	20 days - 250\$
		✓ session cookies	31 days - 400\$
yandex	yandex.ru	✓ login	10 days - 150\$
		✓ password	20 days - 250\$
		✓ session cookies	31 days - 400\$
yahoo	yahoo.com	✓ login	10 days - 150\$
		✓ password	20 days - 250\$
		✓ session cookies	31 days - 400\$
microsoft	xbox.com skype.com onenote.com office.com microsoftonline.com microsoft.com live.com bing.com	✓ login	10 days - 150\$
		✓ password	20 days - 250\$
		✓ session cookies	31 days - 400\$
		✓ login	10 days - 150\$
		✓ session cookies	31 days - 400\$

The portal of EvilProxy contains multiple tutorials and interactive videos regarding the use of the service and configuration tips. Being frank – the bad actors did a great job in terms of the service usability, and configurability of new campaigns, traffic flows, and data collection.

**What I need to start using system?**

1. Add your VPS (You need cheapest VPS or Dedicated Line with min 10GB \$10/\$40).  
\*You need VPS to connect to many domains at a time.
2. Add your domains.
3. Pick your Service from Services and Prices.  
\*You can select from our ready-made services.
4. Create your Campaigns.  
\*Campaigns are ready-made phishing links that you need to select. They are also equipped with ready-made avatars, avatars and banners, which are updated with every update, making them look like real users of various browsers and devices.
5. Make your victims.
6. Hook Session Cookies to Your Browser.  
\*You can use our ready-made scripts to hook session cookies, which are updated with every update, making them look like real users of various browsers and devices. You can also use our ready-made scripts to hook session cookies, which are updated with every update, making them look like real users of various browsers and devices.

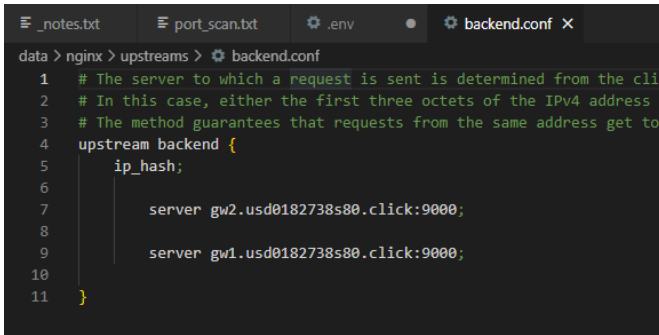
**COMMON QUESTIONS ABOUT SYSTEM:**

- What is the main idea of the reverse proxy?
- How can I stop VPS with content?
- What happens after the subscription ends?
- Why does it keep redirecting to the GoGuard URL?
- Why sometimes links in the same browser "do not work"?
- Why are my links landing not on host?

After activation, the operator will be asked to provide SSH credentials to further deploy a Docker container and a set of scripts. This approach has also been used in other [Phaas service called "Frappo"](#) which was identified by Resecurity this year. The automated installer has a reference to a user "Olf Dobs" (ksh8h297aydO) on Gitlab:

```
apt update -qqy && apt dist-upgrade --no-install-recommends --no-install-suggests -o Dpkg::options::="--force-confdef" -y \ && apt install --no-install-recommends --no-install-suggests -y git \ && rm -rf /srv/control-agent && git clone --recurse-submodules https://gitlab.com/ksh8h297ayd0/docker-control-agent.git /srv/control-agent \ && cd /srv/control-agent && chmod +x ./install.sh \ && /srv/control-agent/install.sh '[license_key]' ===*==
```

After a successful deployment, the scripts will forward the traffic from the victims via 2 gateways defined as "upstream":



```
data > nginx > upstreams > backend.conf
1 # The server to which a request is sent is determined from the cli
2 # In this case, either the first three octets of the IPv4 address o
3 # The method guarantees that requests from the same address get to
4 upstream backend {
5     ip_hash;
6
7     server gw2.usd0182738s80.click:9000;
8
9     server gw1.usd0182738s80.click:9000;
10
11 }
```

Based on further analysis, we identified some of the domain names used for phishing campaigns. The bad actors register similar (by spelling) domains with the intention of masking them under legitimate online-services.

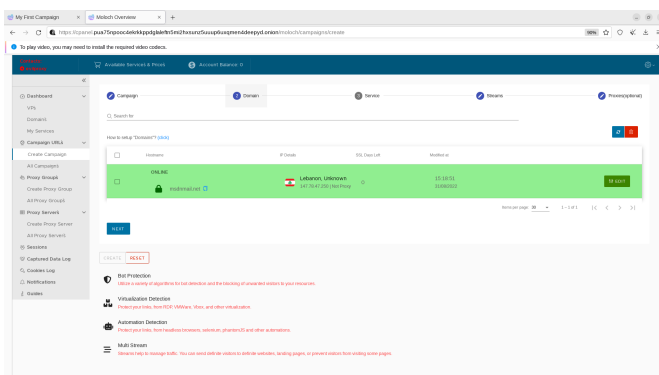
Some of the links generated by EvilProxy to impersonate Microsoft E-Mail services are provided below:

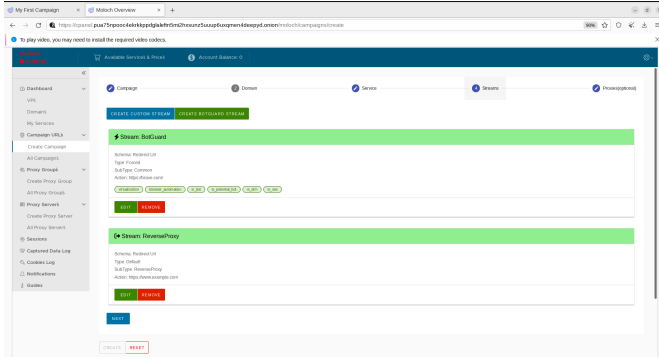
### Login Phishing URL

```
https://lmo.msdnmail[.]net/common/oauth2/v2.0/authorize?client_id=4765445b-32c6-49b0-83e6-1d93765276ca&redirect_uri=https%3A%2Fopenid%20profile%20https%3A%2F%2Fwwwofc.msdnmail.net%2Fv2%2FofficeHome.All&response_mode=form_post&nonce=637975588496970710.Zjg3YzFkMmEtYTUxYy00NDliLWEZyZAtMTExZTliNjBkY2ZkY2U3NmZMDMtZWNhZC00ZWFlWE5YjMtYzgzZTFjM2E1ZDdl&ui_locales=en-US&mkt=en-US&state=jHi-CP0Nu40FHIxklcT1adstnCwbwJwXQWTxNSSsw-23qiXK-6EzyYoAyNZ6rHuHwsIYSKRp99F-bqPqhN4JVCnT4-3MQIDvdTKapKarcqaMF16_xv2_3D0KfqbQ070yKGBG1wxFQ6Mzt9CwUsz2zdgCB4jFux2BhZQwcj-WumSBz0VQs5VePV-wz00E8rDxEXFQdlv-AT29EwdG77AmGwinyf3yQXSZTHJyo8s-IWSHoly3Kbturwnc87sDC3uwEn6VDIjKbbaJ-c-WOzrg&x-client-SKU=ID_NETSTANDARD2_0&x-client-ver=6.16.0.0
```

### Post-Authorization URL

```
https://473126b6-bf9a-4a96-8111-fb04f6631ad8-571c4b21.msdnmail[.]net/mail/?realm=[victim_domain]&exsvurl=1&ll-cc=1033&modurl=0&JitExp=1&url=%2Fowa%2F%3Frealm%253d%2526exsvurl%253d1%252611-cc%253d1033%2526modurl%253d0%2526login_hint%253[victim_email]%252540[victim_domain]
```

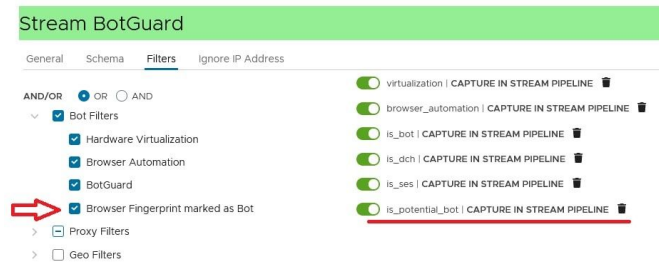




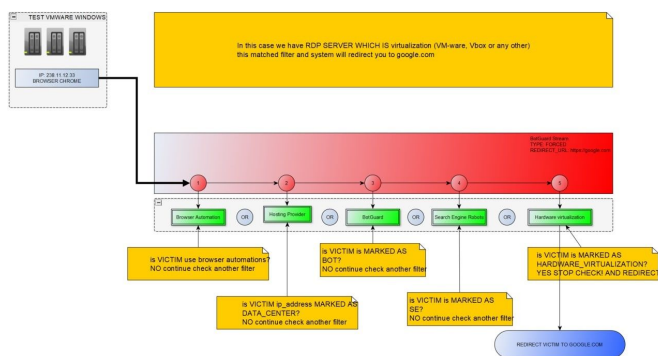
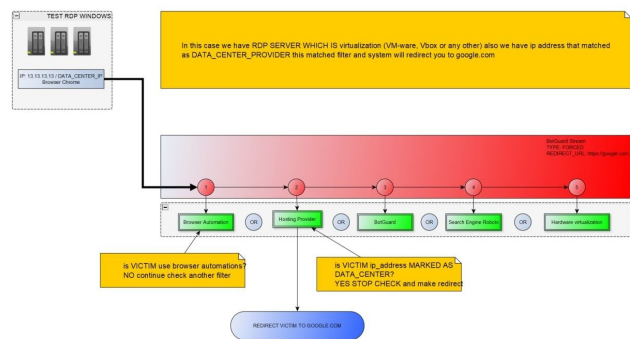
The bad actors are using multiple techniques and approaches to recognize victims and to protect the phishing-kit code from being detected. Like fraud prevention and cyber threat intelligence (CTI) solutions, they aggregate data about known **VPN services**, **Proxies**, **TOR exit nodes** and other hosts which may be used for IP reputation analysis (of potential victims). In the case they suspect a bot or researcher, they drop the connection or redirect it to a specific host (for example, 'brave.com').



Another approach which has been identified is based on fingerprints.



The bad actors are especially diligent when it comes to detecting possible virtual machines, typically used by security analysts to research malicious content and clients connecting via RDP (Remote Desktop Protocol):



## Significance

While the sale of EvilProxy requires vetting, cybercriminals now have a cost-effective and scalable solution to perform advanced phishing attacks to compromise consumers of popular online services with enabled MFA. The appearance of such services in Dark Web will lead to a significant increase in ATO/BEC activity and cyberattacks targeting the identity of the end users, where MFA may be easily bypassed with the help of tools like EvilProxy.

## IOC:

Resecurity's HUNTER team collected the following domain names and URLs related to the EvilProxy infrastructure. Some of these hosts were mapped as a result of post-incident response engagement with the affected victims from Fortune 500 companies and consumers of popular online-services. While the operations of bad actors are extremely dynamic, the information about these hosts may help cybersecurity researchers and incident responders detect and attribute possible malicious activity to EvilProxy when investigating incidents affecting MFA (2FA).

- 147[.]78[.]47[.]250
- 185[.]158[.]251[.]169
- 194[.]76[.]226[.]166
- msdnmail[.]net
- evilproxy[.]pro
- top-cyber[.]club
- rproxy[.]io
- login-live.rproxy[.]io
- gw1.usd0182738s80[.]click:9000
- gw2.usd0182738s80[.]click:9000
- cpanel.evilproxy[.]pro
- cpanel.pua75npoc4ekrkkppdglaleftn5mi2hxsunz5uuup6uxqmen4deepydf[.]onion

