# New 'EvilProxy' phishing tool

**A new phishing tool which bypasses MFA, is causing a spike in BEC cases.**

## What is the threat?

QBE's claims team and S-RM's Incident Response team have recently observed a significant increase in the number of Business Email Compromise ('BEC') cases ending in attempted payment fraud.

Most of the cases we have worked on appear to be linked to a global phishing campaign using a new tool – called EvilProxy – used to bypass most forms of multi-factor authentication ('MFA') and compromise user accounts.

**There is a high risk that organisations will fall victim to this new BEC attack method, if existing defences are not fine-tuned:**

- EvilProxy bypasses most forms of MFA, which many organisations rely on as their primary defence against account compromise.
- Current campaigns are using previously compromised accounts to send out further phishing emails, which means recipients are receiving convincing phishing emails from people they trust.
- Phishing landing pages are more convincing than ever.
- Certain industries and sectors are being heavily targeted – legal, insurance, real estate and financial services.

So far, the attacks using EvilProxy that we have observed have all had the end goal of payment fraud (rather than data exfiltration or as a starting point for broader attacks). This is a trend we expect to continue short-term; however, we are monitoring campaigns closely for any changes in behaviour.

## How does EvilProxy work?

EvilProxy is a powerful adversary-in-the-middle (AiTM) attack framework which is being offered as a cheap, easy to use service on the dark web amongst cybercriminals.

Threat actors are using EvilProxy to craft targeted phishing emails that include links to customised phishing websites, which are designed to look like legitimate sign-in pages for services like Google Workspace and Microsoft 365. These phishing websites then redirect – or 'proxy' – traffic from the user to legitimate login sites, allowing the threat actor to intercept user credentials, validate session cookies and effectively sit in the middle of the MFA process.

This proxy attack framework is not a new technique: sophisticated threat actors have previously used similar tools to bypass MFA protections since as early as 2018. However, EvilProxy differs from these earlier frameworks, as it is much easier to set up, provides a wealth of in-depth training and instructional videos, has a user-friendly interface, and offers a much wider library of fake phishing websites for well-known platforms such as Apple iCloud, Facebook, GoDaddy, GitHub, Google, Dropbox, Instagram, Microsoft, Twitter, Yahoo, and Yandex.

QBE | S-RM

## How can you defend yourself?

In order to defend against AiTM attacks, organisations must complement their traditional MFA protections with a variety of different security measures, some of which are outlined below.

- **Conditional Access Policies and alternative MFA methods:** The best way to defend against EvilProxy attacks is to configure conditional access policies to deny access to untrusted devices from untrusted IP ranges and geographic locations. It is also recommended that organisations use hardware token MFA methods (FIDO2 security keys) and enable password-less authentication methods.
- **Security Operation Centres:** It is vital that security operation centres closely monitor alerts generated by their security tools for known indicators of EvilProxy, such as suspicious user sign-ins and unusual mailbox activity.
- **Email Security Software:** Organisations should invest in advanced software solutions that monitor and scan incoming emails for malicious websites, including those used in EvilProxy phishing campaigns.
- **Phishing Awareness Campaigns:** As always, it is important for organisations to run regular phishing awareness campaigns to increase the likelihood that employees spot malicious links before opening them and know how to report them to the security team.

It is important to note that none of the current solutions is a silver bullet, and EvilProxy could continue to pose a significant threat even after implementing the mitigations above.

## What should you do following an EvilProxy attack?

Should your organisation fall victim to an EvilProxy phishing attack, SRM recommend immediately enforcing **password resets** for all compromised accounts. SRM also recommend revoking the users' sessions in Microsoft 365 or whichever platform is affected, and across all devices.

In addition to enforcing password resets, it is recommended that compromised organisations conduct a more **in-depth forensic investigation** of their platforms to assess the point of entry, the scope of the threat actor's access to the victim's network, and the actions taken by the attacker once inside such as changes to MFA configurations, the creation of new mailbox rules, and the deletion of emails containing malicious files to name a few.


## Acknowledgements

We thank S-RM for their review and contributions to this threat notice.

S-RM is a global cyber security and intelligence consultancy. Find out more at **s-rminform.com**



**Contacts:**

**William Finley**
Senior Cyber Underwriter
**william.finley@uk.qbe.com**

**David Warr**
Cyber Portfolio Manager
**david.warr@uk.qbe.com**

**QBE European Operations**
30 Fenchurch Street
London EC3M 3BD
tel +44 (0)20 7105 4000
**QBEeurope.com**




476862/2302