

# 10,000 organisations targeted by phishing attack that bypasses multi-factor authentication



GRAHAM CLULEY ([HTTPS://WWW.TRIPWIRE.COM/STATE-OF-SECURITY/CONTRIBUTORS/GRAHAM-CLULEY/](https://www.tripwire.com/state-of-security/contributors/graham-cluley/))

FOLLOW @GCLULEY ([HTTPS://TWITTER.COM/GCLULEY](https://twitter.com/gcluley))

([HTTPS://WWW.TRIPWIRE.COM/STATE-OF-SECURITY/ARTICLES \(/STATE-OF-SECURITY/TOPICS/FEATURED/\)](https://www.tripwire.com/state-of-security/articles/))

OF-



[f](http://www.facebook.com/sharer.php?u=https://www.tripwire.com/state-of-security/featured/10000-organisations-targeted-by-phishing-attack-that-bypasses-multi-factor-authentication/) (<http://www.facebook.com/sharer.php?u=https://www.tripwire.com/state-of-security/featured/10000-organisations-targeted-by-phishing-attack-that-bypasses-multi-factor-authentication/>) [t](http://twitter.com/intent/tweet?url=https://www.tripwire.com/state-of-security/featured/10000-organisations-targeted-by-phishing-attack-that-bypasses-multi-factor-authentication/&text=10,000%20organisations%20targeted%20by%20phishing%20attack%20that%20bypasses%20multi-factor%20authentication&via=tripwireinc) (<http://twitter.com/intent/tweet?url=https://www.tripwire.com/state-of-security/featured/10000-organisations-targeted-by-phishing-attack-that-bypasses-multi-factor-authentication/&text=10,000 organisations targeted by phishing attack that bypasses multi-factor authentication&via=tripwireinc>) [in](http://www.linkedin.com/shareArticle?mini=true&url=https://www.tripwire.com/state-of-security/featured/10000-organisations-targeted-by-phishing-attack-that-bypasses-multi-factor-authentication/&text=10,000%20organisations%20targeted%20by%20phishing%20attack%20that%20bypasses%20multi-factor%20authentication) (<http://www.linkedin.com/shareArticle?mini=true&url=https://www.tripwire.com/state-of-security/featured/10000-organisations-targeted-by-phishing-attack-that-bypasses-multi-factor-authentication/&text=10,000 organisations targeted by phishing attack that bypasses multi-factor authentication>) [r](http://www.reddit.com/submit?url=https://www.tripwire.com/state-of-security/featured/10000-organisations-targeted-by-phishing-attack-that-bypasses-multi-factor-authentication/) (<http://www.reddit.com/submit?url=https://www.tripwire.com/state-of-security/featured/10000-organisations-targeted-by-phishing-attack-that-bypasses-multi-factor-authentication/>) [e](mailto:?subject=10,000%20organisations%20targeted%20by%20phishing%20attack%20that%20bypasses%20multi-factor%20authentication&body=https://www.tripwire.com/state-of-security/featured/10000-organisations-targeted-by-phishing-attack-that-bypasses-multi-factor-authentication/) (<mailto:?subject=10,000 organisations targeted by phishing attack that bypasses multi-factor authentication&body=https://www.tripwire.com/state-of-security/featured/10000-organisations-targeted-by-phishing-attack-that-bypasses-multi-factor-authentication/>)

Microsoft has shared details of a widespread phishing campaign that not only attempted to steal the passwords of targeted organisations, but was also capable of circumventing multi-factor authentication (MFA) defences.

The attackers used AiTM (Attacker-in-The-Middle) reverse-proxy sites to pose as Office 365, and then use them to log into the genuine site.

According to Microsoft's detailed report on the campaign (<https://www.microsoft.com/security/blog/2019/05/01/office-365-attackers-use-aitm-phishing-sites-as-entry-point-to-further-financial-fraud/>), once hackers had broken into email inboxes via the use of stolen passwords and session cookies, they would exploit their access to launch Business Email Compromise (BEC) attacks

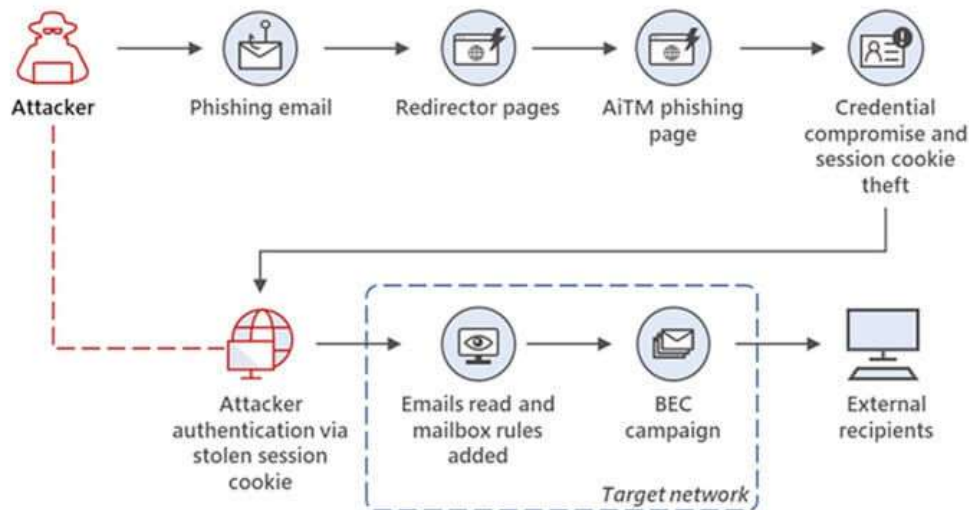
Welcome! Can I help you find relevant content while you research?

MFA

1

on other targets.

By creating rules on victims' email accounts, the attackers are able to then ensure that they are able to maintain access to incoming email even if a victim later changes their password.



(<https://3b6xlt3iddqmuq5vy2w0s5d3->

[wpengine.netdna-ssl.com/state-of-security/wp-content/uploads/sites/3/campaign.jpeg](https://wpengine.netdna-ssl.com/state-of-security/wp-content/uploads/sites/3/campaign.jpeg))

The global pandemic, and the resulting increase in staff working from home, has helped fuel a rise in the adoption of multi-factor authentication.

Cybercriminals, however, haven't thrown in the towel when faced with MFA-protected accounts. Accounts with MFA are certainly less trivial to break into than accounts which haven't hardened their security, but that doesn't mean that it's impossible.

Reverse-proxy phishing kits like Modlishka (<https://grahamcluley.com/automated-phishing-attack-tool-bypasses-2fa-protection/>), for instance, impersonate a login page, and ask unsuspecting users to enter their login credentials and MFA code. That collected data is then passed to the genuine website – granting the cybercriminal access to the site.

As more and more people recognise the benefits of MFA, we can expect a rise in the number of cybercriminals investing effort into bypassing MFA.

Microsoft's advice is that organisations should complement MFA with additional technology and best practices.

These include enabling conditional access policies (for instance, testing that logins are coming from trusted IP addresses and compliant devices), the deployment of anti-phishing defences at the email and web gateways, detection of unusual mailbox activity (such as the creation of suspicious inbox rules, and logins with unusual characteristics.)

More technical information about the attacks can be found in Microsoft's report (<https://www.microsoft.com/security/blog/2022/07/12/from-cookie-theft-to-bec-attackers-use-aitm-phishing-sites-as-entry-point-to-further-financial-fraud/>).

"While AiTM phishing attempts to circumvent MFA, it's important to underscore that MFA implementation remains an essential pillar in identity security," said Microsoft. "MFA is still very effective at stopping a wide variety of threats; its effectiveness is why AiTM phishing emerged in the first place."

Hear hear.

**Editor's Note:** *The opinions expressed in this guest author article are solely those of the contributor, and do not necessarily reflect those of Tripwire, Inc.*

## SHARE THIS POST



([http://www.facebook.com/sharer.php?u=https://www.tripwire.com/state-of-security/featured/10000-organisations-targeted-by-phishing-attack-that-bypasses-multi-](http://www.facebook.com/sharer.php?u=https://www.tripwire.com/state-of-security/featured/10000-organisations-targeted-by-phishing-attack-that-bypasses-multi-factor-authentication/)

[factor-authentication/](http://www.facebook.com/sharer.php?u=https://www.tripwire.com/state-of-security/featured/10000-organisations-targeted-by-phishing-attack-that-bypasses-multi-factor-authentication/))



([http://twitter.com/intent/tweet?url=https://www.tripwire.com/state-of-security/featured/10000-organisations-targeted-by-phishing-attack-that-](http://twitter.com/intent/tweet?url=https://www.tripwire.com/state-of-security/featured/10000-organisations-targeted-by-phishing-attack-that-bypasses-multi-factor-authentication/&text=10,000%20organisations%20targeted%20by%20phishing%20attack%20that%20bypasses%20multi%20factor%20authentication/)


[bypasses-multi-factor-authentication/&text=10,000 organisations targeted by phishing attack that bypasses multi](http://twitter.com/intent/tweet?url=https://www.tripwire.com/state-of-security/featured/10000-organisations-targeted-by-phishing-attack-that-bypasses-multi-factor-authentication/&text=10,000%20organisations%20targeted%20by%20phishing%20attack%20that%20bypasses%20multi%20factor%20authentication/)

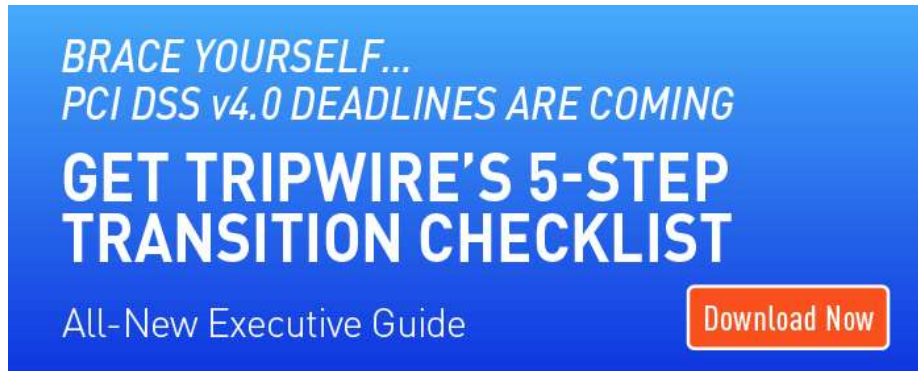
([http://www.linkedin.com/shareArticle?mini=true&url=https://www.tripwire.com/state-of-security/featured/10000-organisations-targeted-by-phishing-attack-that-](http://www.linkedin.com/shareArticle?mini=true&url=https://www.tripwire.com/state-of-security/featured/10000-organisations-targeted-by-phishing-attack-that-bypasses-multi-factor-authentication/&text=10,000%20organisations%20targeted%20by%20phishing%20attack%20that%20bypasses%20multi%20factor%20authentication/)

[factor-authentication/&text=10,000 organisations targeted by phishing attack that bypasses multi-factor authentication](http://www.linkedin.com/shareArticle?mini=true&url=https://www.tripwire.com/state-of-security/featured/10000-organisations-targeted-by-phishing-attack-that-bypasses-multi-factor-authentication/&text=10,000%20organisations%20targeted%20by%20phishing%20attack%20that%20bypasses%20multi%20factor%20authentication/)

Welcome! Can I help you find relevant content while you research?

1 ti-

url=<https://www.tripwire.com/state-of-security/featured/10000-organisations-targeted-by-phishing-attack-that-bypasses-multi-factor-authentication/>)  (mailto:?subject=10,000 organisations targeted by phishing attack that bypasses multi-factor authentication&body=<https://www.tripwire.com/state-of-security/featured/10000-organisations-targeted-by-phishing-attack-that-bypasses-multi-factor-authentication/>)



*BRACE YOURSELF...*  
*PCI DSS v4.0 DEADLINES ARE COMING*  
**GET TRIPWIRE'S 5-STEP  
TRANSITION CHECKLIST**  
All-New Executive Guide [Download Now](#)

(<https://www.tripwire.com/solutions/compliance-solutions/pci->

[dss-compliance/essential-pci-dss-40-transition-checklist/?utm\\_source=sos&utm\\_medium=bottombanner&utm\\_campaign=CISGuide](https://www.tripwire.com/solutions/compliance-solutions/pci-dss-compliance/essential-pci-dss-40-transition-checklist/?utm_source=sos&utm_medium=bottombanner&utm_campaign=CISGuide))



**NAVIGATING  
INDUSTRIAL  
CYBERSECURITY**  
[Download Now](#)

(<https://resources.tripwire.com/state-of-security-guide-to-industrial-cybersecurity>)



Join over 20,000 IT  
security pros who get our  
top stories delivered to  
their inbox every week!  
[tripwire](#) [SUBSCRIBE](#)

(<https://info.tripwire.com/state-of-security-subscription-center>)

## RECENT POSTS


10,000 organisations targeted by phishing attack that bypasses multi-factor authentication >

What Is GitOps and How Will it Impact Digital Forensics? >

Defense in Depth to minimize the impact of ransomware attacks >

The Great Cybersecurity Resignation >

VERT Threat Alert: July 2022 Patch Tuesday Analysis >

 Welcome! Can I help you find relevant content while you research?

1

[File Integrity Monitoring \(FIM\): Your Friendly Network Detective Control >](#)

[Defending Aircraft Networks Against Cybersecurity Breaches >](#)

[Using DevSecOps for Efficient IT Security >](#)

[Lockdown Mode: Apple to protect users from targeted spyware attacks >](#)

[PCI 4.0: The wider meanings of the new Standard >](#)



([https://www.tripwire.com/misc/executives-guide-cis-controls-register?](https://www.tripwire.com/misc/executives-guide-cis-controls-register?utm_source=stateofsecurity&utm_medium=blog)

)

## TOPICS

[ICS Security \(/state-of-security/topics/ics-security/\)](/state-of-security/topics/ics-security/)

[Cloud \(/state-of-security/topics/security-data-protection/cloud/\)](/state-of-security/topics/security-data-protection/cloud/)

[IT Security and Data Protection \(/state-of-security/topics/security-data-protection/\)](/state-of-security/topics/security-data-protection/)

[Latest Security News \(/state-of-security/topics/tripwire-news/\)](/state-of-security/topics/tripwire-news/)

[Regulatory Compliance \(/state-of-security/topics/regulatory-compliance/\)](/state-of-security/topics/regulatory-compliance/)

[Government \(/state-of-security/topics/government/\)](/state-of-security/topics/government/)

[Vulnerability Management \(/state-of-security/topics/vulnerability-management/\)](/state-of-security/topics/vulnerability-management/)

## ABOUT

[About \(/state-of-security/about/\)](/state-of-security/about/)

[Contributors \(/state-of-security/contributors/\)](/state-of-security/contributors/)

[Write for us \(/state-of-security/about/contact-us/\)](/state-of-security/about/contact-us/)

[Privacy Policy \(/legal/privacy/\)](/legal/privacy/)

[Tripwire.com \(/\)](/)

## CONTACT US

US Headquarters

308 SW 2nd Ave Suite 400

Portland, OR 97204

(<https://www.google.com/maps/place/Tripwire/@45.5201564,-122.673347,19z/data=!3m1!4b1!4m5!3m4!1s0x54950a0fb0c4e8f1:0x5e346d3964f079a2!8m2!3d45.5201555!4d-122.6727998>)

Direct: 503.276.7500 (tel:5032767500)


[International Offices \(/contact/\)](/contact/)

## SEARCH



Welcome! Can I help you find relevant content while you research?

1

 Welcome! Can I help you find relevant content while you research?

1