UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

# CYBER GUIDANCE ISSUE 0319

## 'GREATNESS' – PHISHING AS A SERVICE

**DATE ISSUED:** 15th May 2023

| | | | |
|---|---|---|---|
| IMPACT | LOW | MEDIUM | **HIGH** |
| EASE OF EXPLOIT | HARD | MEDIUM | **EASY** |

## OVERVIEW

Researchers at Cisco Talos have discovered a new phishing service called 'Greatness' designed explicitly to impersonate Microsoft 365 instances. It is an advanced Phishing as a Service (PhaaS) with capabilities such as Multi-Factor Authentication (MFA) bypass, IP filtering, and integration with Telegram bots.

## BREAKDOWN

The Phishing-as-a-Service (PhaaS) platform allows anyone with entry-level cybersecurity knowledge to create a phishing campaign attack and benefit that attack. The 'Greatness' Phishing-as-a-Service contains everything a "wannabe" threat actor needs to conduct a campaign successfully. To initiate an attack, the user of the services accesses the 'Greatness' admin panel using their API key and providing a list of target email addresses. The platform provides the server to host the phishing page and generate the HTML attachment. The phishing service sends the email with an HTML attachment to the victim. Once the victim clicks on the attachment, it automatically injects the target company logo and background image from the employer's Microsoft 365 login page. Greatness prefills the victim's email address to create a sense of legitimacy. The phishing platform acts as a proxy between the victim's browser and the actual Microsoft 365 login page, handling the authentication flow to obtain a valid session cookie for the target account. The attackers can use this session cookie to access a victim's email, files, and data in Microsoft 365 services. The stolen credentials could also be used to infiltrate corporate networks, leading to even more dangerous attacks, such as the deployment of ransomware. Researchers at Cisco Talos revealed that this campaign had seen a spike in activity. It targets organisations using Microsoft 365 in the United States, Canada, the U.K., Australia, and South Africa.

## REMEDIATION STEPS

- Security awareness training is essential for training employees on recognising and avoiding phishing threats.
- Implement multi-factor authentication (MFA) on all applications and services.
- Adopt a defence-in-depth strategy by implementing Next Generation endpoint security solutions such as email and web filtering to block the initial phishing email.

## REFERENCES & RESOURCES

Bleeping Computer https://www.bleepingcomputer.com/news/security/new-greatness-service-simplifies-microsoft-365-phishing-attacks/

Malwarebytes https://www.malwarebytes.com/blog/threat-intelligence/2023/05/fake-system-update-drops-new-highly-evasive-loader