TLP:GREEN

PERSISTENT PHISHING CAMPAIGN

Release Date: September 23, 2021
TAMENGR-ADV-1330-09232021

Summary

On September 17, 2021, the Texas A&M Engineering Cyber Response Team (CRT) became aware of a widespread targeted phishing campaign by a persistent threat actor. This campaign is targeting higher education institutions with the goal of gaining access to those institutions' mail servers to engage in further phishing attacks internally and externally. CRT analysts assess that the primary goal of this campaign is to leverage trusted mail infrastructure to conduct phishing attacks against financial sector customers, however the group may additionally make use of gathered credentials for other operations. This actor has engaged in this activity since early 2017 and has engaged with nearly identical tradecraft over the past four years. They have recently proven their capability to bypass 2FA by prompting users to provide OTPs or approve requests.

Details

In this phishing campaign, the actor was successful in phishing and bypassing Two-Factor Authentication (2FA) against UNIVERSITY with upwards of 15 compromised user accounts. The actor used a consistent method to access these 2FA protected accounts. The actor harvested credentials and the DUO Mobile Passcode from USER. The actor immediately used USER's credentials and DUO Mobile Passcode to authenticate to UNIVERSITY's account management service. This allowed the actor to add a new device to USER's DUO profile for 2FA.

With an actor controlled device added for 2FA, the actor authenticates to Microsoft Office 365 using USER's credentials and a 2FA DUO push responded to on the actor controlled phone. The actor authenticates to the Exchange Outlook Web Application from the actor controlled phone. The actor then authenticates to UNIVERSITY's Virtual Open Access Lab environment using the DUO Mobile Passcode from the actor controlled phone. With this access, the actor downloaded mass mailing applications and began sending internal and external phishing emails.

Recommendations

- Allow only authenticated users to send mail via relays
- Prevent open relays by limiting mail to be sent from only your domains
- Ensure that 2FA is enabled for external applications

Victim Profile

This threat actor initially targets higher education institutions. This threat actor then utilizes the compromised higher education institutions to conduct aggressive phishing campaigns against additional higher education institutions and external entities, including organizations in the financial sector.

Indicators of Compromise

Value	Type	Context
metroplexhomeorganizer[.]com	domain	Tool Ingress Site
awesome-agent[.]com	domain	Credential Harvesting Site
bgbotanix[.]com	domain	Credential Harvesting Site
cesco-italia[.]com	domain	Credential Harvesting Site
medisolhealthcare[.]com	domain	Credential Harvesting Site
oyfresh[.]com	domain	Credential Harvesting Site
yumereal[.]com	domain	Credential Harvesting Site
xanfarin[.]com	domain	Credential Harvesting Site
51[.]81[.]169[.]225	ip	Attacker Infrastructure
192[.]119[.]111[.]254	ip	Attacker Infrastructure
51[.]79[.]8[.]129	ip	Attacker Infrastructure
195[.]148[.]239[.]162	ip	Attacker Infrastructure
173[.]186[.]194[.]203	ip	Attacker Infrastructure
96[.]71[.]52[.]249	ip	Attacker Infrastructure
40[.]124[.]181[.]191	ip	Attacker Infrastructure

73[.]172[.]196[.]88	ip	Attacker Infrastructure
COVID Test	mail_subject	Phishing Email Subject
eNotification	mail_subject	Phishing Email Subject
RE: Meeting	mail_subject	Phishing Email Subject

Tactics, Techniques, & Procedures

Actor tactics, techniques, and software are identified and documented using the MITRE ATT&CK technique knowledge base and framework.

Initial Access

ID	Technique	Context
T1566	Phishing	Sends various phishing lures to collect targeted credentials and spoof 2FA
T1078	Valid Accounts	Uses valid accounts to access target network and hosts
T1133	External Remote Services	Connects to target network via VPN and VDI using legitimate credentials

Persistence

ID	Technique	Context
T1136.001	Create Local Account	Creates local account disguised as a backup account with passwords “Arsenal1” and “1qaz”

Credential Access

ID	Technique	Context
T1110	Brute Force	Uses RDP Brute Force tool

Discovery

ID	Technique	Context
T1018	Remote System Discovery	Uses RDP Scanner for remote host discovery

Lateral Movement

ID	Technique	Context
T1021.001	Remote Services: Remote Desktop Protocol	Connects to other devices on the network using RDP

Command and Control

ID	Technique	Context
T1105	Ingress Tool Transfer	Downloads tools for mailing and scanning from file sharing sites, legitimate tool sites, and compromised staging sites

Tools

Name	Description	Context
Gammadyne Mailer	Mass mailing application	Used to send both internal and external phishing emails
Turbomailer	Mass mailing application	Used to send both internal and external phishing emails
Nodemailer	Mass mailing application	Used to send both internal and external phishing emails
Ncrack	Network authentication bruteforcer	Used to bruteforce RDP credentials

Related References

MITRE ATT&CK Technique IDs: https://attack.mitre.org/techniques/enterprise/