University Targeted Credential Phishing Campaigns Use COVID-19, Omicron Themes

proofpoint.com/us/blog/threat-insight/university-targeted-credential-phishing-campaigns-use-covid-19-omicron-themes

December 2, 2021

Blog
Threat Insight
University Targeted Credential Phishing Campaigns Use COVID-19, Omicron Themes

December 07, 2021 Selena Larson and Jake G

Proofpoint researchers have identified an increase in email threats targeting mostly North American universities attempting to steal university login credentials. The threats typically leverage COVID-19 themes including testing information and the new Omicron variant.

Proofpoint observed COVID-19 themes impacting education institutions throughout the pandemic, but consistent, targeted credential theft campaigns using such lures targeting universities began in October 2021. Following the announcement of the new Omicron variant in late November, the threat actors began leveraging the new variant in credential theft campaigns.

Threat actors continue to use COVID-19 theme lures in campaigns targeting multiple industries and geographic areas. The threats specifically targeting universities is interesting due to the specificity in targeting and effort to mimic legitimate login portals. It is likely this activity will increase in the next two months as colleges and universities provide and require testing for students, faculty, and other workers traveling to and from campus during and after the holiday season, and as the Omicron variant emerges more widely.

We expect more threat actors will adopt COVID-19 themes given the introduction of the Omicron variant. This assessment is based on previously published research that identified COVID-19 themes making a resurgence in email campaigns

following the emergence of the Delta variant in August 2021.

Campaign Details

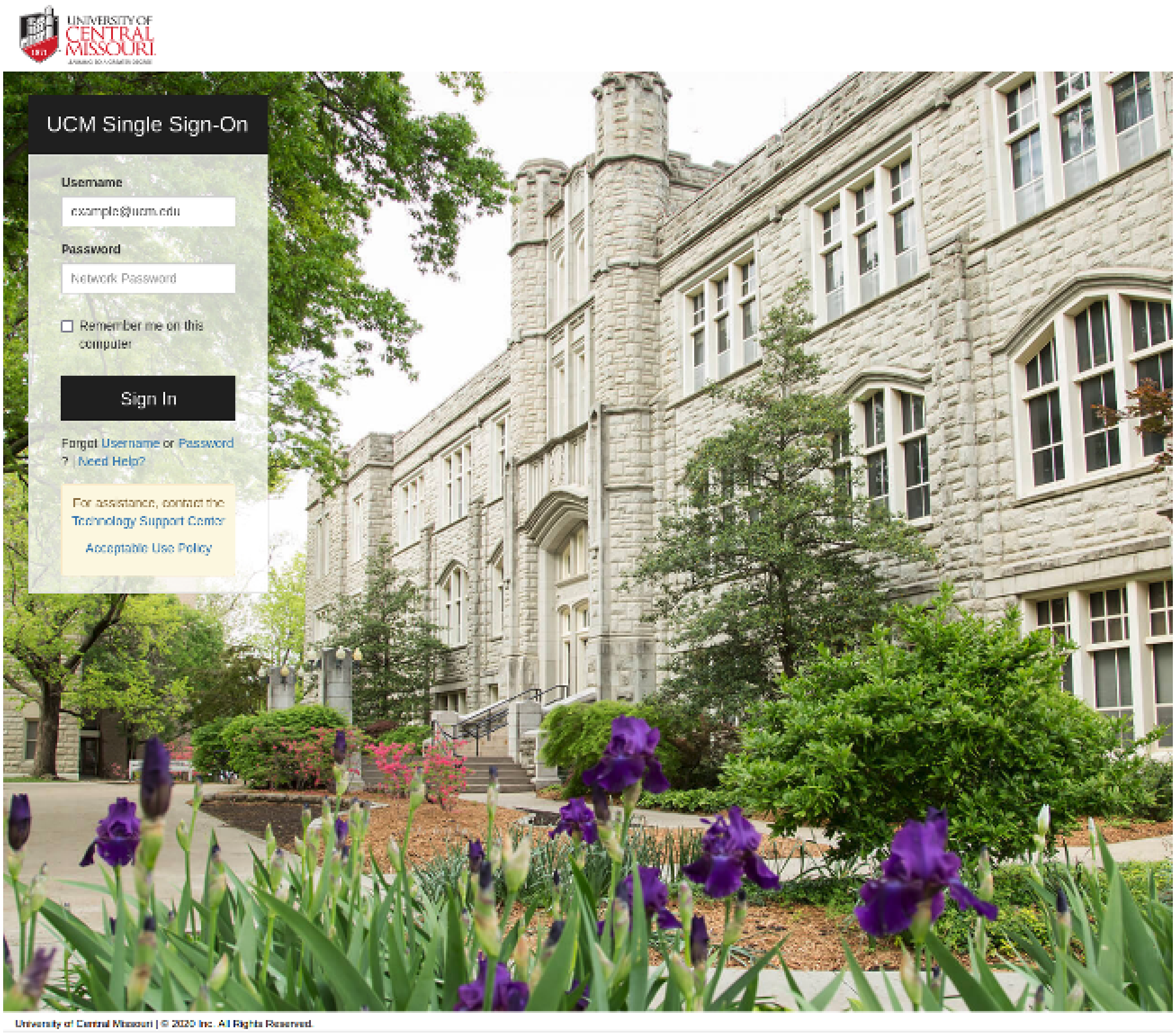
The COVID-19 themed campaigns including Omicron variant lures include thousands of messages targeted to dozens of universities in North America.

The phishing emails contain attachments or URLs for pages intended to harvest credentials for university accounts. The landing pages typically imitate the university's official login portal, although some campaigns feature generic Office 365 login portals. In some cases, such as the Omicron variant lures, victims are redirected to a legitimate university communication after credentials are harvested. Proofpoint observed this threat actor pivot from Delta variant themed email lures to Omicron themes following the announcement of the new variant.

Emails with URLs use subjects such as:

Attention Required - Information Regarding COVID-19 Omicron Variant - November 29

With a link to a spoofed landing page such as:



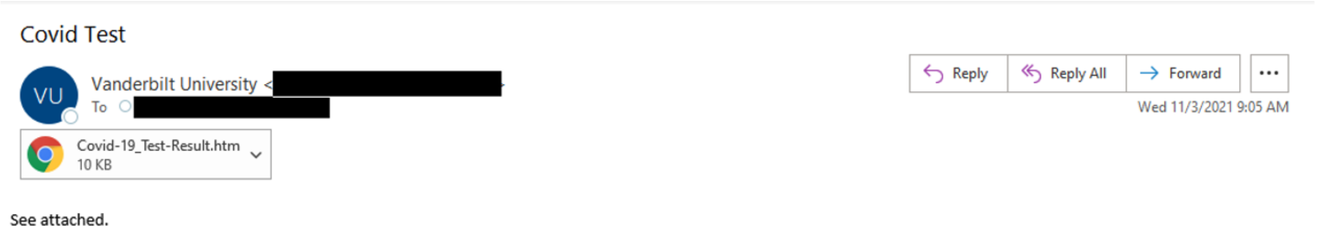
UNIVERSITY OF CENTRAL MISSOURI
UCM Single Sign-On
Username
example@ucm.edu
Password
Network Password
□ Remember me on this computer
Sign In
Forgot Username or Password ? | Need Help?
Acceptable Use Policy

For assistance, contact the Technology Support Center

University of Central Missouri | © 2020 Inc. All Rights Reserved.

Figure 1: Spoofed login page for the University of Central Missouri.

Messages distributing attachments included subject lines such as "Covid Test".



Covid Test

VU Vanderbilt University <[redacted]

To [redacted]

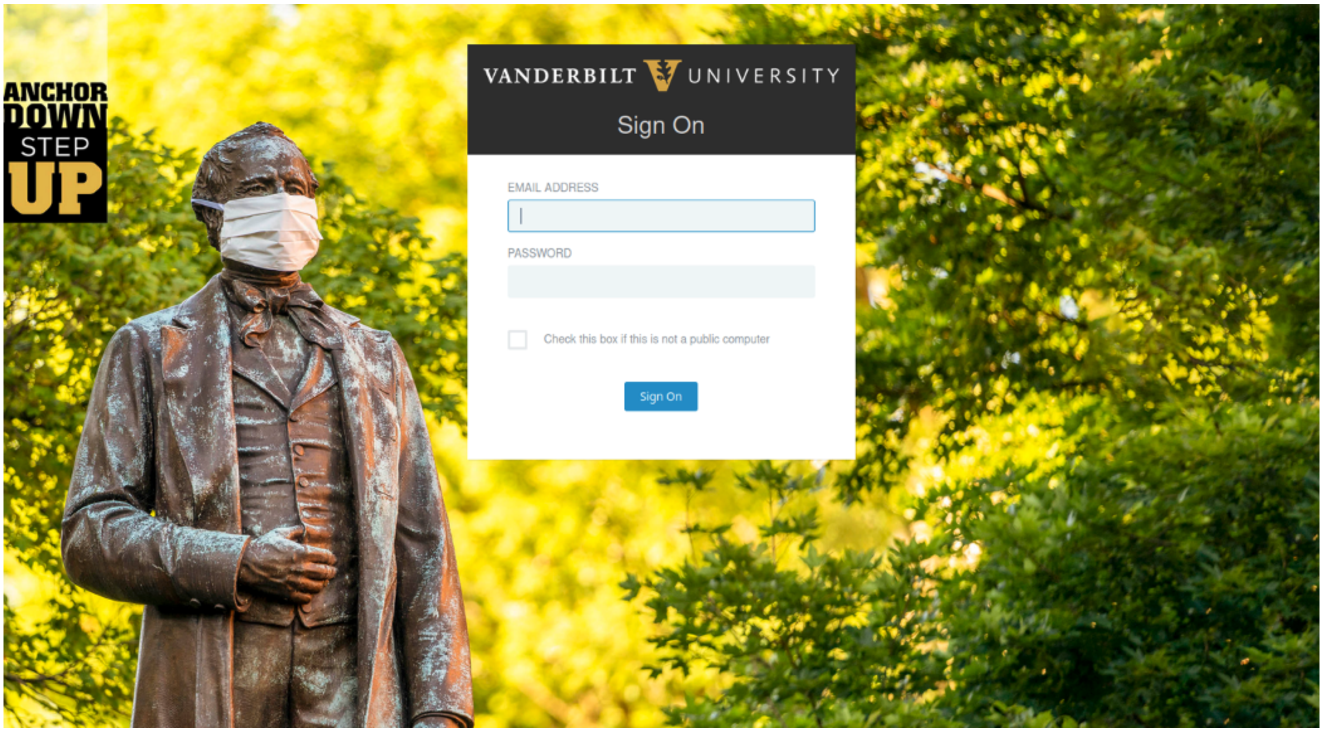
Covid-19_Test-Result.htm
10 KB

Wed 11/3/2021 9:05 AM

See attached.

Figure 2: HTM attachment leading to a credential capture webpage.

The attachments lead to a university themed email credential theft webpage.



VANDERBILT UNIVERSITY

Sign On

EMAIL ADDRESS

PASSWORD

□ Check this box if this is not a public computer

Figure 3: Credential theft webpage spoofing Vanderbilt University.

Proofpoint has identified multiple threat clusters using COVID-19 themes to target universities using different tactics, techniques, and procedures (TTPs). In addition to multiple delivery methods – Proofpoint has observed both URL and attachments in campaigns – activity clusters use different sender and hosting methods to distribute credential theft campaigns.

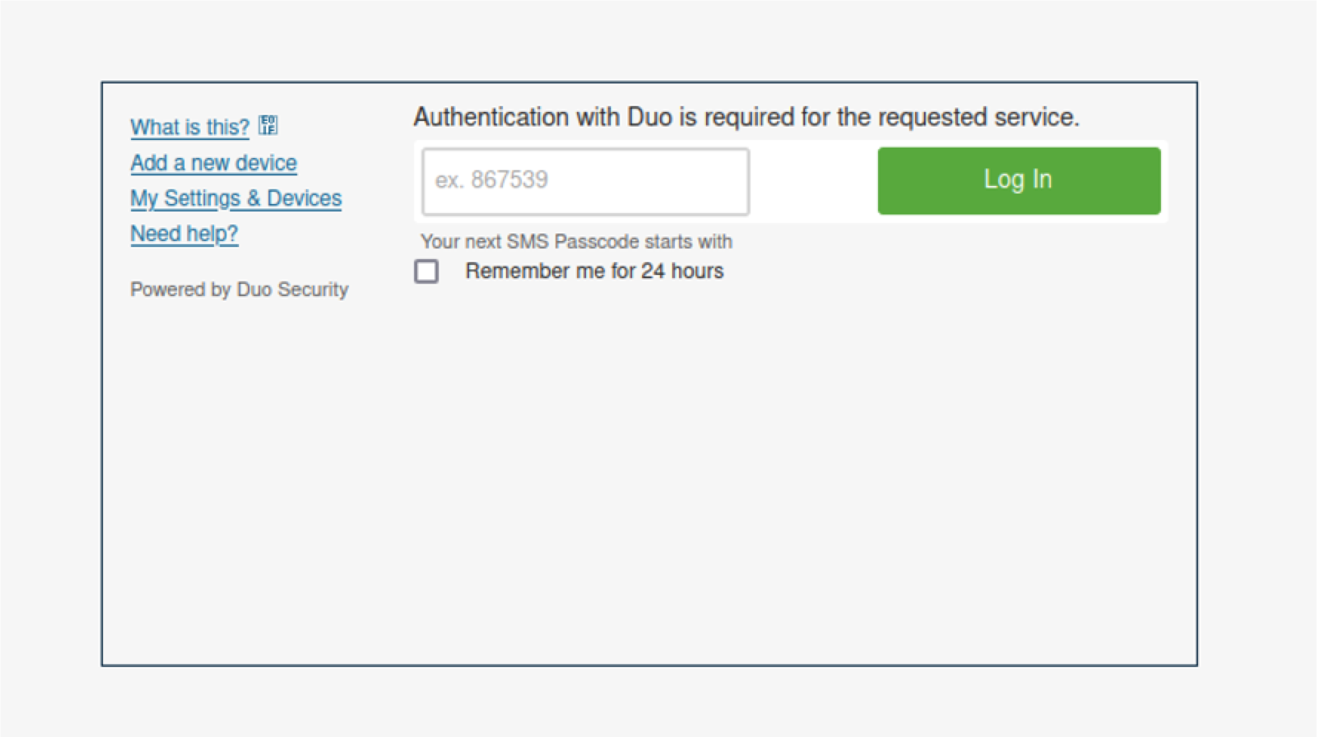
In the Omicron variant campaign, threat actors leverage actor-controlled infrastructure to host credential theft webpages using similar domain naming patterns. These include:

- sso[.]ucmo[.]edu[.]boring[.]cf/Covid19/authenticationedpoint.html
- sso2[.]astate[.]edu[.]boring[.]cf/login/authenticationedpoint.html

Attachment-based campaigns have leveraged legitimate but compromised WordPress websites to host credential capture webpages, including:

- hfbcbiblestudy[.]org/demo1/includes/jah/[university]/auth[.]php
- afr-tours[.]co[.]za/includes/css/js/edu/web/etc/login[.]php
- traveloaid[.]com/css/js/[university]/auth[.]php

In some campaigns, threat actors attempted to steal multifactor authentication (MFA) credentials, spoofing MFA providers such as Duo. Stealing MFA tokens enables the attacker to bypass the second layer of security designed to keep out threat actors who already know a victim’s username and password.



Authentication with Duo is required for the requested service.

Your next SMS Passcode starts with

□ Remember me for 24 hours

Figure 4: Duo MFA credential theft landing page.

While many messages are sent via spoofed senders, Proofpoint has observed threat actors leveraging legitimate, compromised university accounts to send COVID-19 themed threats. It is likely the threat actors are stealing credentials from universities and using compromised mailboxes to send the same threats to other universities.

Proofpoint does not attribute this activity to a known actor or threat group, and the ultimate objective of the threat actors is currently unknown.

Indicators of Compromise

Indicator	Description
hfbcbiblestudy[.]org/demo1/includes/jah/[university]/auth[.]php	Credential Theft URL

afr-tours[.]co[.]za/includes/css/js/edu/web/etc/login[.]php	Credential Theft URL
traveloaid[.]com/css/js/[university]/auth[.]php	Credential Theft URL
traveloaid[.]com/css/js/[university]/auth[.]php	Credential Theft URL
offthewallgraffiti[.]org/[university]/auth[.]php	Credential Theft URL
traveloaid[.]com/css/js/[university]/auth[.]php	Credential Theft URL
sso[.]ucmo[.]edu[.]boring[.]cf/Covid19/authenticationedpoint.html	Credential Theft URL
sso2[.]astate[.]edu[.]boring[.]cf/login/authenticationedpoint.html	Credential Theft URL
242smarthome[.]com/[university]/auth.php	Credential Theft URL
jass-butz[.]at/xx/main/main.php	Credential Theft URL
Bluecollarsubs[.]com/main/ main.php	Credential Theft URL

Subscribe to the Proofpoint Blog