Devious phishing method bypasses MFA using remote access software

By **Lawrence Abrams (https://www.bleepingcomputer.com/author/lawrence-abrams/)** February 22, 2022 04:57 PM 1

A devious, new phishing technique allows adversaries to bypass multi- authentication (MFA) by secretly having victims log into their

One of the biggest obstacles to successful phishing attacks is bypassing multi-factor authentication (MFA) configured on the targeted victim's email accounts.

Even if threat actors can convince users to enter their credentials on a phishing site, if MFA protects the account, fully compromising the account still requires the one-time passcode sent to the victim.

To gain access to a target's MFA-protected accounts, phishing kits have been updated to use reverse proxies or other methods to collect MFA codes from unwitting victims.

However, companies are catching on to this method and have begun introducing security measures that block logins or deactivate accounts when reverse proxies are detected

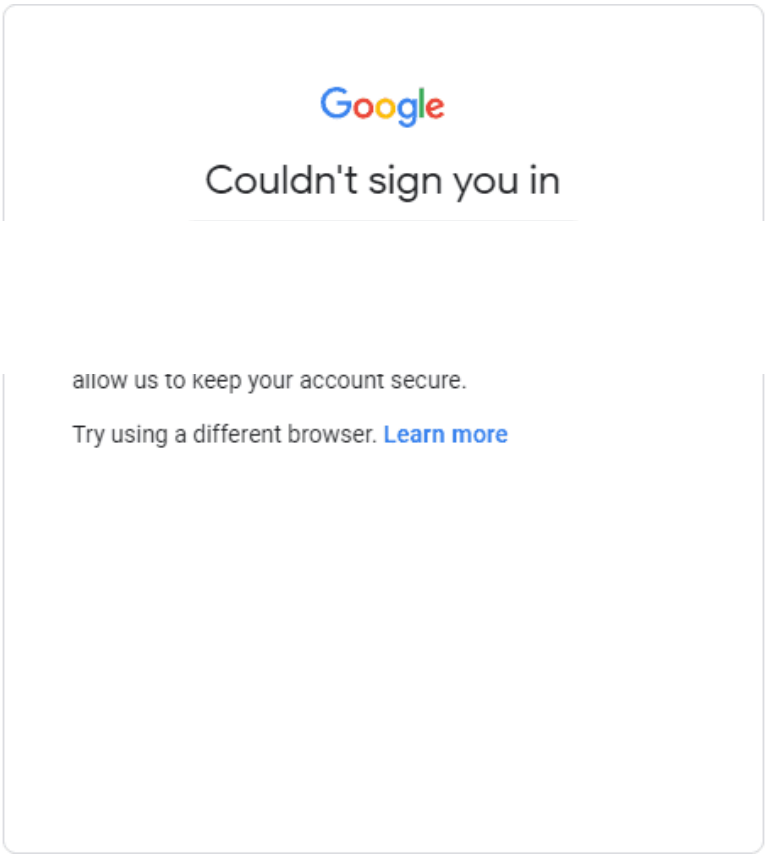
VNC to the rescue

While conducting a penetration test for a customer, security researcher mr.dox attempted to create a phishing attack on the client's employees to gain corporate account credentials.

As the accounts were all configured with MFA, mr.dox set up a phishing attack using the Evilginx2 (https://github.com/kgretzky/evilginx2) attack framework that acts as a reverse proxy to steal credentials and MFA codes.

When conducting the test, the researcher found that Google prevented logins when detecting reverse proxies or man-in-the-middle (MiTM) attacks.

these types of attacks.



Google Chrome logon blocking MiTM attacks
Source: mr.d0x

The researcher also told BleepingComputer that websites, such as LinkedIn, detect man-in-the-middle (MiTM) attacks and deactivate accounts after successful login (http://github.com/kgretzky/evilginx2/issues/697)s.

To overcome this obstacle, mr.d0x came up with a devious new phishing technique that uses the noVNC remote access software and browsers running in kiosk mode to display email login prompts running on the attacker's server but shown in the victim's browser.

VNC is a remote access software that allows remote users to connect to

However, a program called noVNC allows users to connect to a VNC server directly from within a browser by simply clicking a link, which is when the researcher's new phishing technique comes into play.

"So how do we use noVNC to steal credentials & bypass 2FA? Setup a server with noVNC, run Firefox (or any other browser) in kiosk mode and head to the website you'd like the user to authenticate to (e.g. accounts.google.com)," explains a new report by mr.d0x.

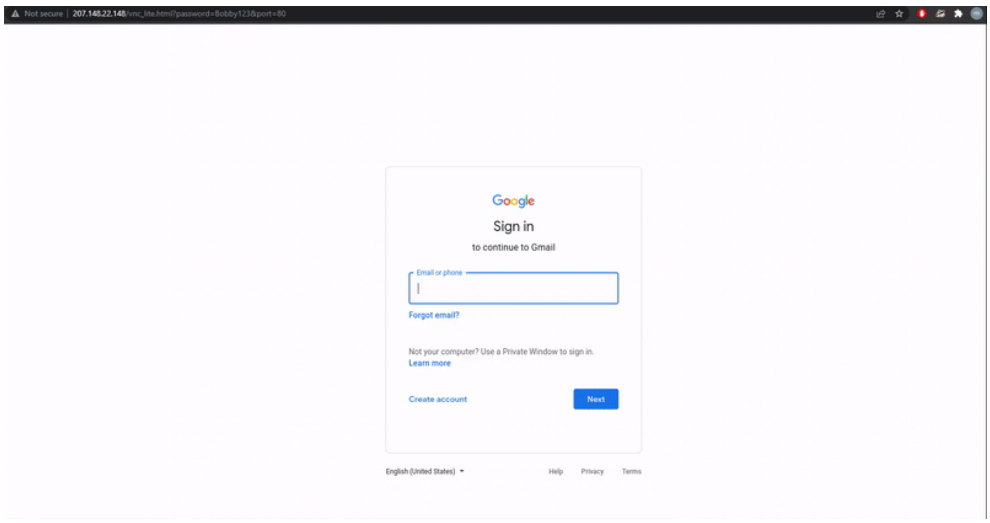
Send the link to the target user and when the user clicks the URL they'll be accessing the VNC session without realizing. And because you've already setup Firefox in kiosk mode all the user will see is a web page, as expected."

Using this configuration, a threat actor can send out targeted spear-phishing emails that contain links that automatically launch the target's browser and log into the attacker's remote VNC server.

These links are highly customizable and allow the attacker to create links that don't look like suspicious VNC login URLs, such as the ones below:

```
Example[.]com/index.html?id=VNCPASSWORD
Example[.]com/auth/login?name=password
```

As the attacker's VNC server is configured to run a browser in kiosk mode, which runs the browser in full-screen mode, when the victim clicks on a link they will simply see a login screen for the targeted email service and login as normal.



Demonstration of the VNC phishing technique
Source: mr.d0x

However, as the login prompt is actually being displayed by the attacker's VNC server, all login attempts will happen directly on the remote server

Even more dangerous, this technique will bypass MFA as the user will enter the one-time passcode directly on the attacker's server, authorizing the device for future login attempts.

> "Since it's my server I can have many tricks up my sleeve, for example say I have burp suite or any other HTTP proxy attached to
>
> Another alternative could be I inject JS into the browser before sending the phishing link. When the user begins using the browser it runs my JS.Theres many more options because at the end of the day the user authenticates onto your server."
>
> *mr.dox*

If the attack were being used on a limited basis to target only a few people, simply logging into their email account over the attacker's VNC session would authorize the device to connect to the account in the future.

As VNC allows multiple people to monitor the same session, an attacker could disconnect the victim's session after the account was logged in and connect to the same session later to access the account and all its email.

While this attack has not been seen used in real-world attacks, the researcher told BleepingComputer that he believes attackers will use it in the future.

As for how to protect yourself from these types of attacks, all the phishing advice remains the same: do not click on URLs from unknown senders, inspect embedded links for unusual domains, and treat all email as suspicious, especially when it prompts you to login to your account.