

New phishing toolkit uses PWAs to steal login credentials

By [Lawrence Abrams](#)



June 12, 2024



01:35 PM



1

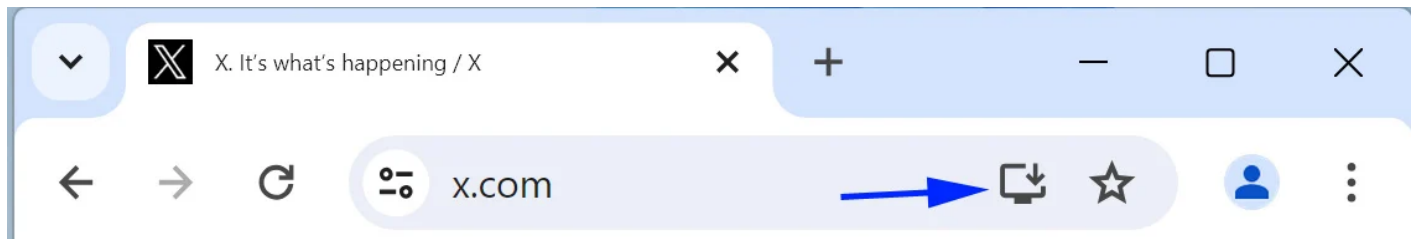


A new phishing kit has been released that allows red teamers and cybercriminals to create progressive web Apps (PWAs) that display convincing corporate login forms to steal credentials.

A PWA is a web-based app created using HTML, CSS, and JavaScript that can be installed from a website like a regular desktop application. Once installed, the operating system will create a PWA shortcut and add it to Add or Remove Programs in Windows and under the `/Users/<account>/Applications/` folder in macOS.

When launched, a progressive web app will run in the browser you installed it from but be displayed as a desktop application with all the standard browser controls hidden.

Many websites use a PWA to offer a desktop app experience, including X, Instagram, Facebook, and TikTok.



X prompting visitors to install its PWA

Source: BleepingComputer

Using PWAs to phish for credentials

A new phishing toolkit created by security researcher [mr.dox](#) demonstrates how to create PWA apps to display corporate login forms, even with a fake address bar showing the normal corporate login URL to make it look more convincing.

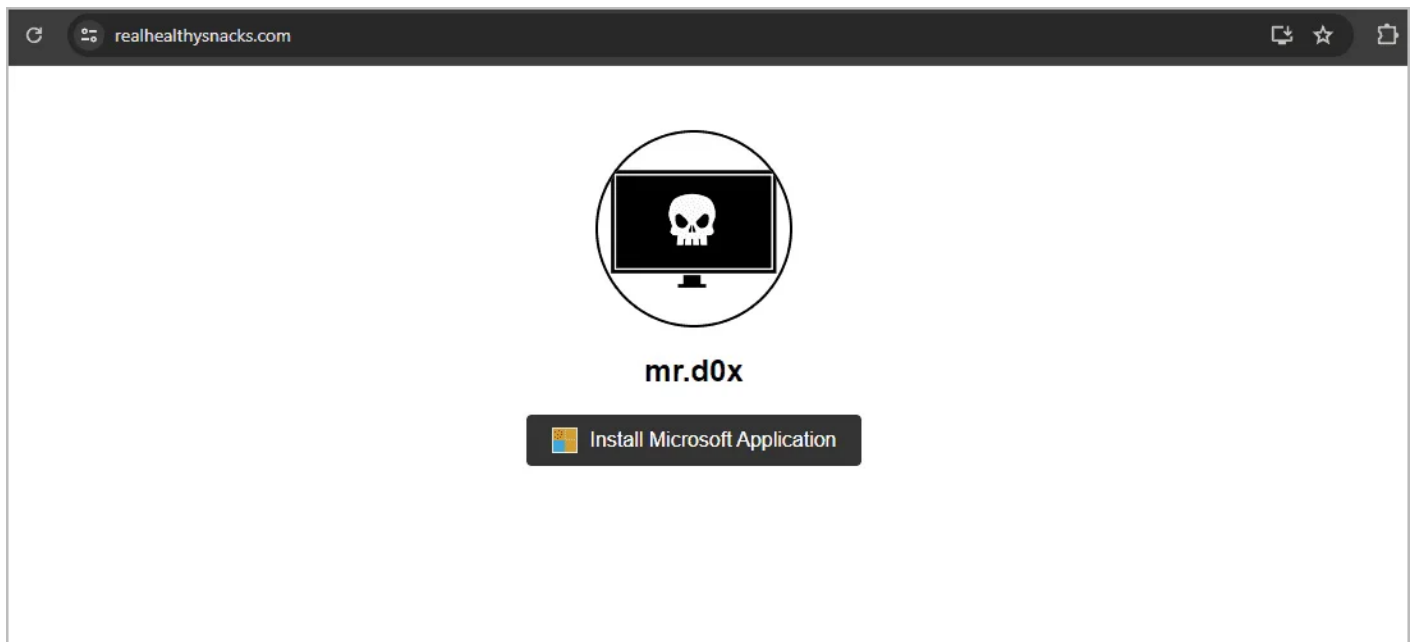
"PWAs integrate with the OS better (i.e. they have their own app icon, can push notifications) and therefore they can lead to higher engagement for websites," the researcher explains in a blog post about the new toolkit.

"The issue with PWAs is that manipulating the UI for phishing purposes is possible as we'll explore in this blog."

While the new phishing templates will require some convincing to get a user to install the PWA, there are scenarios where it may be easier to do so.

It's common for threat actors to create websites designed to distribute programs that install malware, as we saw in the past with [fake NordVPN](#) and [ProtonVPN sites](#) and [fake Windows PC cleaners](#).

In a similar manner, a threat actor can create sites promoting fake software or remote management tools that include a button to install their software, as shown below.



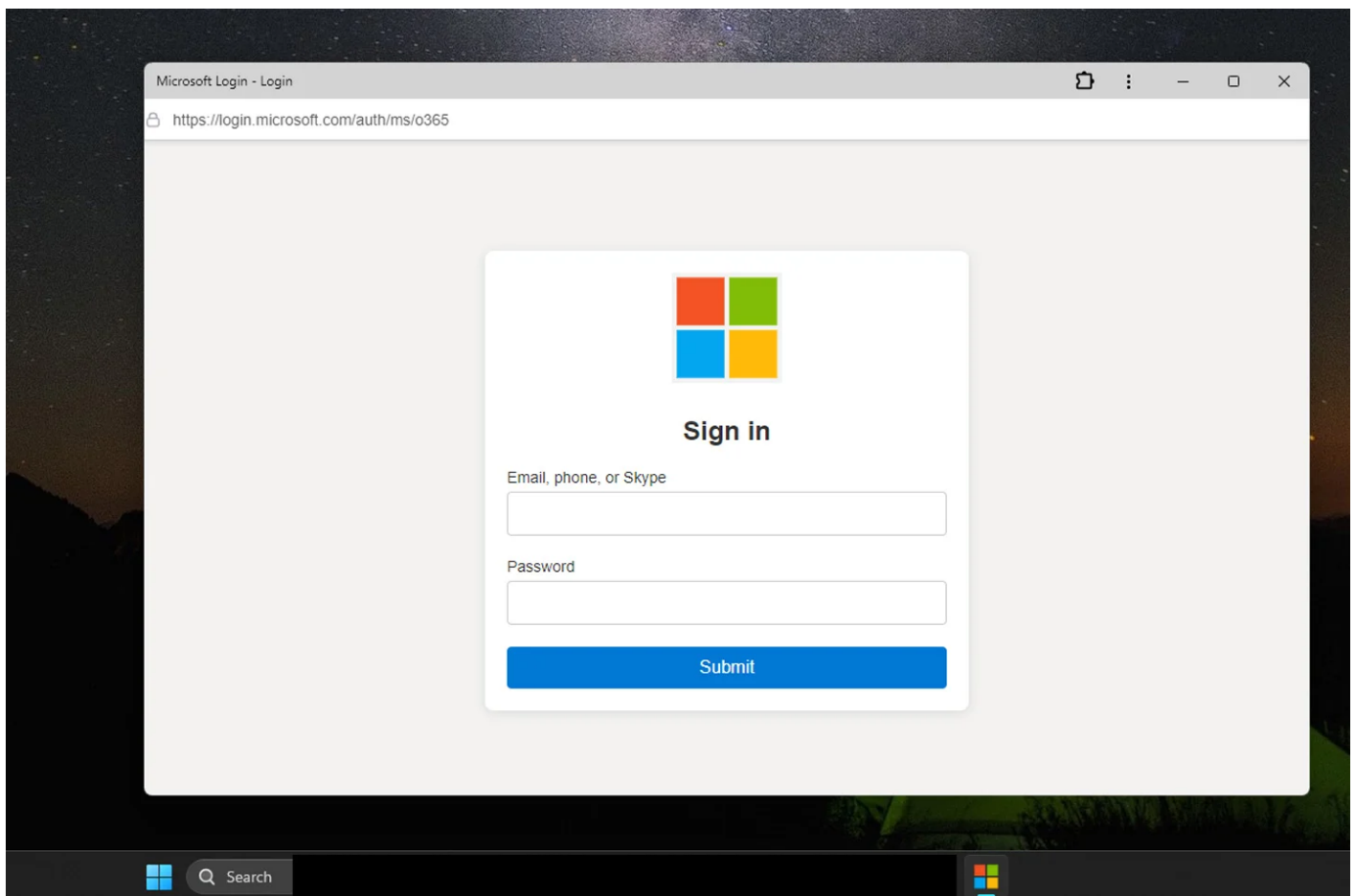
Website created to push the malicious PWA

Source: mr.d0x

When the visitor clicks on the install button, the browser will install the PWA and add it to the operating system, with Windows prompting as to whether you want to create a shortcut on the Taskbar.

When the PWA automatically launches, though, it will prompt the user to enter their credentials to log in, whether those are, for example, for a VPN product, Microsoft, AWS, or online store credentials.

This technique stands out because mr.d0x illustrates how you can integrate a fake address bar containing a fake URL in the PWA, similar to how it was done in the [Browser-in-the-Browser technique](#). This will cause the login form to appear more legitimate to the target.



PWA showing a fake Microsoft login form

Source: mr.d0x

The researcher has released the PWA phishing templates [on GitHub](#), allowing anyone to test or modify them for their own scenarios.

“

"Users that don't use PWAs often may be more susceptible to this technique as they might be unaware that PWAs should not have a URL bar. Even though Chrome appears to have taken measures against this by periodically showing the real domain in the title bar, I think people's habits of "checking the URL" will render that measure less useful.

Additionally, how many security awareness programs today mention PWA phishing? I can only speak from personal experience and I haven't seen companies mention this in their training. The lack of familiarity with PWA and the danger they can potentially pose might make this technique more effective.

I can see this technique being used by attackers to request users to install a software and then in the PWA window the phishing

happens. This was demonstrated in the demo video I provided.

Finally, one thing to keep in mind is that Windows actively prompts the user to pin the PWA to the task bar. The next time the window is opened it will automatically open the URL mentioned in the "start_url" parameter in the manifest file. This may cause the user to pin the PWA and use it more than once, providing the attacker with more results."

❖ mr.dox told BleepingComputer



The researcher is known for his previous phishing toolkits that display [fake file archivers in the browser](#), [use VNC to bypass MFA](#), and the notorious Browser in the Browser templates, which have been abused by [ransomware gangs](#) and to [steal Steam credentials](#).

While this new PWA phishing method will require more convincing to get targets to install the app, it won't be surprising if we find threat actors utilizing this technique at some point in the future.

Unfortunately, no existing group policies can prevent the installation of progressive web apps, with existing policies only allowing you to ban specific extension IDs or access to specific URLs.

In 2018, researchers from the Korea Advanced Institute of Science & Technology (KAIST) [released a paper](#) investigating progressive web apps and their potential security risks.

A demonstration of the PWA phishing kit can be seen below.

CREDENTIAL THEFT

CREDENTIALS

PHISHING

PROGRESSIVE WEB APP

PWA

TOOLKIT





LAWRENCE ABRAMS

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

[< PREVIOUS ARTICLE](#)[NEXT ARTICLE >](#)

Comments



Hmm888 - 4 hours ago



There are free applications on the web (not dark or deep web) which allow users to easily view Chrome or other browser passwords and log-ins which is a "bug" never patched.