INSIGHTS

One Brightly Cyber

ONE TOKEN TO RULE THEM ALL

BY JAY BORDEN

Let's start by defining a token. It is a type of cookie that gives the user access to one application, or system, or service. A cookie is just a small text file that is stored on your device to provide information to what you want to access. A token is used to authenticate you and is given to your browser by the application, site, or system you want to access, after you prove you are authorized to be there. Your browser probably has a large collection of cookies from everything you have accessed over time.

Tokens have been a favorite target of hackers for years. They are associated with the browser and are one of the things info-stealers capture.

Why do cybercriminals want the access tokens? Simple, they provide access past all the authentication methods, past passwords, past MFA, past one-time tokens, past biometrics, past everything. This means if you change your password or get issued a new one-time token or other MFA it won't matter. The access token will still work and give the attacker access. Think of it like a bearer bond. Bearer bonds are redeemable by the person holding them. No other identification or proof of ownership is necessary. If you own bearer bonds and they are stolen you are out of luck. One reason they are not used much anymore.

The tokens have a life spam of anywhere from a few hours to a few days to a few weeks or possibly longer. The idea is you can re-access the applications, system, or site without having to go through a full log in.

Very convenient but also dangerous. That is why we always advise you to cancel your session tokens not just change your passwords if you get compromised.

The good thing about a token is it is only good for one site or one application, or one service.

ONE TOKEN TO RULE THEM ALL

CONTINUED

Well, that is true in most cases. Microsoft has introduced something they call the Primary Refresh Token that works for all their services that a person uses. It is part of Microsoft Entra, the new name for Microsoft Azure AD, (Active Directory).

When you access a Microsoft service or application you need to authenticate to it. Entra will look to see if you have registered with the system. If so, it will issue the Primary Refresh Token, PRT, to your device. The idea is that if you have the PRT, it will issue a token for any Microsoft service you are allowed to use without you needing to log into each one separately. Very similar to a Single Sign On for applications.

Convenient, yes, dangerous, very.

If a hacker gets hold of your PRT they can access all the services you do with no further authentication required.

The PRT has a life of 2 weeks except on Android where it is up to 90 days. That gives attackers plenty of time to steal your information and install malware, backdoors, ransomware, etc. before the PRT expires. Is it any wonder the PRT is desired by cybercriminals? Remember, whatever makes things easier for legitimate users also makes them easier for attackers.

If Lord of The Rings fans allow, this is the one token to rule them all. Whoever has it gets into everything.

I understand the want of convenience and not having to log in and authenticate to multiple services every day. But is it worth the risk? That’s for you to decide.

We aim to keep you informed about developments in cybersecurity, the good ones and the bad ones. As they say, forewarned is forearmed.

Stay safe.

Visit our site, onebrightlycyber.com to learn all the ways we help keep you safer.

Welcome to peace of mind.