INSIGHTS

Cyber made simple.

one brightly cyber

ANOTHER WAY TO DO CYBER SECURITY

BY JAY BORDEN

Cyberattackers aim to steal private information and download malware and ransomware. They do this in multiple ways. A common one is by getting users to click links in phishing emails that go to infected sites where credentials are stolen. Another way is to exploit a software vulnerability to install malware infecting a system or encrypting everything with ransomware. Phishing emails are an effective technique as they evade security tools because they have no malware in them.

Regardless of the method of compromise, when you discover that an attack has been successful the first thing to do is change the password. This is essential as the attacker probably has your password allowing them into your account or accounts and access to that data and information.

In the case of business systems, this can be devastating. The attacker can exfiltrate, or steal, information such as customer names, contact information, bank accounts, credit cards, email addresses, and more.

If the malware is pervasive then it is advisable to reimage the system, meaning to reload the operating system, applications, and company specific software. Reimaging the system should get rid of any malware.

Nothing wrong with that. It just doesn't go far enough. Today, attackers steal more than credentials and information. They install infostealers that capture credentials and session cookies. If attackers have a session cookie, a changed password will not keep them out of applications and data. Nor will a reimaged system.

Why? Session cookies provide direct access without needing a username or password. The access they provide is post login and even post Multi-factor Authentication, MFA. So complex passwords and MFA won't stop cybercriminals who have your session cookies.

onebrightlycyber.com
(888) 773-1920

ANOTHER WAY TO DO CYBER SECURITY

CONTINUED

Even if the system is reimaged and all malware removed, the session cookies still work. Once in the application they will steal more information, attempt to get into other systems and maybe put ransomware on as many systems as they can.

So, what did changing the password and reimaging the system do? Only provide a false sense of security.

Unless the session cookies are disabled you haven't even slowed the attackers down.

Google is working on this issue with a new initiative named Device Bound Session Credentials (DBSC).

DBSC will tie the session specifically to the device. When a new session is started DBSC identifies the browser being used. It creates a public/private key pair that will be stored on the computer by the operating system in a secure way.

If the session cookie is captured by cybercriminals who attempt to use it, it will not work. Since attackers will be on a different device, DBSC will not authenticate the session. This effectively makes stolen session cookies useless.

Google plans to make this an open standard to allow all to employ it.

Until this work is completed and in use by different vendors, do not stop at just changing passwords and reimaging devices. Invalidate all session cookies when any information is compromised or even suspected of being compromised.

Staying safe is a full time job. Cybercriminals are relentless in attacking, you must be equally relentless in protecting yourself.

To learn all the ways we can help make your company and family safer, visit onebrightlycyber.com, contact OneBrightlyCyber at info@onebrightlycyber.com, or call (888) 773-1920.