WE MAKE CYBER SIMPLE

BROWSERS – RISKIER THAN YOU MAY THINK

Browsers for often taken for granted and not considered as cybersecurity risks. This is a mistake.

One reason is that seemingly there are a number of browsers, Chrome, Edge, Opera, Safari, Internet Explorer, Firefox, QQ, Brave and a few more. But almost all are based upon two browser engines, the underlying technology, Chromium and Mozilla Firefox. A few, like Safari, are developed by a company and use their own engine, for Safari, it is Apple.

This means that if cybercriminals find a vulnerability in even one of those two engines, they get access to many browser users.

Vulnerabilities were found in both engines over the last 12 months.

Chrome has three zero-day vulnerabilities in 2022 so far and Mozilla has four. A zero-day means the vulnerability has been discovered but not patched or corrected yet. Cybercriminals love zero-days because they are available for them to exploit.

Remember the browsers and the vulnerabilities are not the final target. It is the way to the prizes, credentials and system access to install more malware or ransomware. Some of these vulnerabilities were very serious including the ability to do remote code execution and gain administrative rights to the system, allowing the attacker to install software or execute programs.

Attackers exploit these in a number of ways depending upon the specific vulnerability. The vulnerability itself may allow cybercriminals to install and run malware if a compromised site is visited.

In other cases, the vulnerability is tied to phishing emails. In fact, Cisco's 2021 Cybersecurity Threat Trend Report attributed 90% of breaches to phishing. That is why we say never click a link in an email.

If that link is clicked, and it often is, it takes the user to a compromised or fake site that downloads and installs malware often by exploiting browser vulnerabilities. That installed malware will often download other malware giving the cybercriminals broader access to the systems and information and providing a "backup" in case their first means of access is discovered and closed.

How do you avoid these issues? Using a multi-pronged approach. First keep your browsers up to date. Second, limit the plugins that can be installed to known ones that have been tested. Third, do not allow browsers to be installed in a way that makes them invisible to the IT team and monitoring.

And last but certainly not least is educate everyone. At all levels. And instill in them that protecting information is everyone's job. Everyone regardless of level or role. Remember 90% of the breaches are due to phishing. The best way to protect against this is educating people to recognize phishing emails and not click on them. We can help.

Ready to take the next steps? Contact onebrightlycyber at info@onebrightlycyber.com or call (888) 773-1920.