ROBO6K

This week in Cyber Security

As many weeks can seem overwhelming, the need to stay up-to-date is increasingly more important. While it may have seemed like a somewhat slow week with not many major hacks being released, that does not mean that there were not any happening. The big one to note from this week is the release from Citrix regarding the Netscaler ADC and gateway servers coming under attack. Researchers determined that the attack affected Ips in many countries but the good news is the US has a low number of unique Ips listed as being exploited. Another notable release is the joint venture release from the FBI, CISA and NSA for the top exploited vulnerabilities of 2022. This brings up the idea for learning from your past and helping to prevent things in the future. Attacks like the Log4J after action report bring to light the need to not only fix the current production workspace but to also be aware when backups are to be rolled out and ensure that any security patch is then applied to those backups. If you think of this attack as a sine wave. The attacks peak quickly and then are patched but then as backups are used, the attacks begin to return. As time goes by the peak number of the attacks begins to lower but with proper data handling this could have been mitigated.

A preventative warning was issued by Cannon regarding disposal of old printers. Without proper disposal, the devices pose a risk of attackers gaining the Wi-Fi connection details. The risk varies between models but things like the SSID, password or network type along with other network related information is stored on the devices to allow them to connect. Without proper device clean up from these devices, attackers can then pull this information to allow them onto your network. This is a great example of ensuring policy for things like this are created and followed, whether in your organization or even at your home network.

Google publishes its annual 0-day vulnerability wrap up and begins to warn of n-day exploits becoming just as dangerous as 0-day attacks. The reason for this is that a patch is only good if applied to the device. While this is specific to the Android platform, this is very helpful in understanding the need for keeping up with patch management and ensuring devices stay within a set compliance. This is an example of more information that may be very important for your business but also for each user’s personal exposure. While companies may have a set schedule for releasing patches, it is also important to keep a look out for emergency security patches that can and will happen at any point as attacks are encountered.

Finally, lets take a quick look at the phishers exploit of SalesForce Email services. A 0-day vulnerability in the salesforce email servers has allowed attackers to launch a sophisticated phishing email using Facebook. Attackers are crafting targeted messages using the company’s domain AND infrastructure. The attack lures users to a rouge page that attempts to capture not only credentials but also the MFA mechanism used to allow access.

As we wrap up this week, other notable things are attacks affecting other countries. While these may not have a direct impact to you, it is important to always be aware of the things that are happening in the cyberespionage and cyberwar world as they may not always stay contained to those worlds. The importance of staying up with the current exploits and vulnerabilities is ever present and only you as the user can help mitigate these attacks.