Week of November 27

As we make it closer to the end of the year, it is important to remember that attackers will never rest. This is why it is important to continue to stay up with everything going on in the world of Cyber Security. A few of the bigger things to note from this week include Zero-days, scalable phishing and the widening impact of attacks.

We will start off by looking at zero-days released by two major companies, Google and Apple. With the release of the newest Zero-Day, Google has now patched a total of 7 high severity Zero-Day attacks so far this year. Google's TAG has confirmed that the newest attack has been actively exploited in the wild but has not released much more information regarding CVE-2023-6345. Switching focus to Apple, the company has released an emergency security update to address an out-of-bounds read flaw and a memory corruption bug. The first can allow attackers to gain access to sensitive data and the second allows for arbitrary code execution. These two exploits bring the total number of Zero-Days for the company to 20 for the year so far. I highlight this as many people think that just having an Apple device means that they are secure. Keeping every device and software updated will be the first line to ensure the best protection no matter the device or service/application.

Understanding that the criminal world can function similar to the legitimate business world can help you to understand the scope and threat they can pose. One such example it the threat actors behind the Telegram bot Telekopye. Codenamed Neanderthals, the group acts similar to a legitimate business with members having distinct tasks and a structure. The botnet is able to perform many of the tasks involved in a phishing campaign like creating phishing websites, crafting emails or SMS messages and much more. The scam-as-a-service is similar to Classiscam, which has netted $64.5 million dollars. Keep in mind that this is just one example of a criminal organization with a focus on one area. Many of the ransomware "gangs" will have a similar structure with distinct separation of duties for each member.

Finally, lets take a look at how the scope of an attack can change, showing us the importance of keeping up with the systems that are in use and following releases from breaches. Disclosed in September, Okta initially insisted that only 1% of clients where impacted by the breach. In a release on November 29, CSO, David Bradbury announced that the impact of the data breach has increased to 100% of its customer base. The attackers were able to run and export a report containing every company name, contact information, user name, role description as well as "other" data. Seeing the jump from 1% to 100% of Okta customers is a clear reason to keep up with security incidents as just because a patch or announcement has been released, the scope or attack vector could be changed.

Whether it is a zero-day exploit, understanding how the attackers think and keeping up with releases for changes or updates is extremely important. Knowing that the world of technology is forever changing and doing your part by staying updated with the news will only help in keeping you at the forefront of the industry. The moment that you stop learning will be the beginning of your downfall within technology.

Caleb Leggett

Technical Specialist