

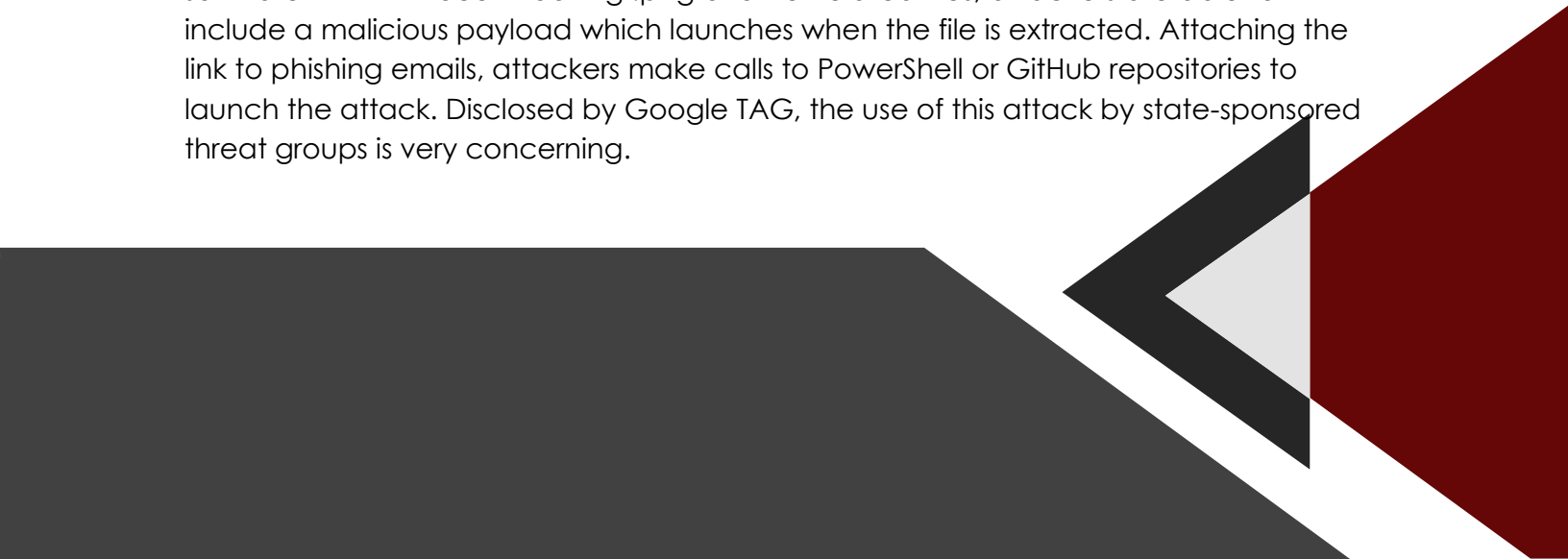



October 16-20

It's that time again! A week filled with vulnerabilities, state-sponsored attacks and rumor debunking, it was a busy week in Cyber. Let's take a quick look through a few of the highlights. Remember that this should not be your only area of information for what is going on in Cyber and if you want help finding sources, please do not hesitate to reach out.

Citrix and Cisco have been disclosing more information on the latest vulnerabilities. While the Citrix vulnerability has been patched, Mandiant has released research showing that the vulnerability has been actively exploited in the wild since late August. The biggest concern with this flaw is that it allows attackers access to the AAA services. The ability to access this information allows attackers to hijack authenticated sessions. While there is a patch available, Citrix also discloses ways to close the vector if patching is not an option in the near term. Unfortunately for Cisco, the current backdoor zero-day does not have a patch currently. With an estimated 40,000 devices vulnerable, this is a huge attack surface for threat actors to go after. The good news on this one is that it only affects the Web GUI, which for a strong security posture, should never be used for network appliances. Unfortunately, the threat is persistent even after a device reboot.

The fear of being targeted by state sponsored attackers can be a scary thing as they tend to have almost unlimited resources. Backed by Russia and China, attackers have been targeting the WinRAR flaw to spread malicious software. By packaging the software within innocent looking .png or other related files, attackers are able to include a malicious payload which launches when the file is extracted. Attaching the link to phishing emails, attackers make calls to PowerShell or GitHub repositories to launch the attack. Disclosed by Google TAG, the use of this attack by state-sponsored threat groups is very concerning.





The importance of due diligence when vulnerabilities are released becomes evident with the suspected Zero-Day that came out affecting Signal. This brings up a good time to talk about the difference between information and intelligence. While gathering information is extremely important, analyzing that information and determining the value, impact and mitigation steps, if necessary, turns that information into intelligence. Luckily for Signal, they were able to debunk the rumors of a suspected backdoor.

While there is always more to know within the world of Cyber security, taking the time to do research is extremely important. Knowing when patches become available and applying those patches are your first line of the Blue Team tactics and can help to prevent the eventuality of an attack. Remember, you are the protectors of the uninitiated and they rely on us to help keep them safe.

Caleb Leggett

