

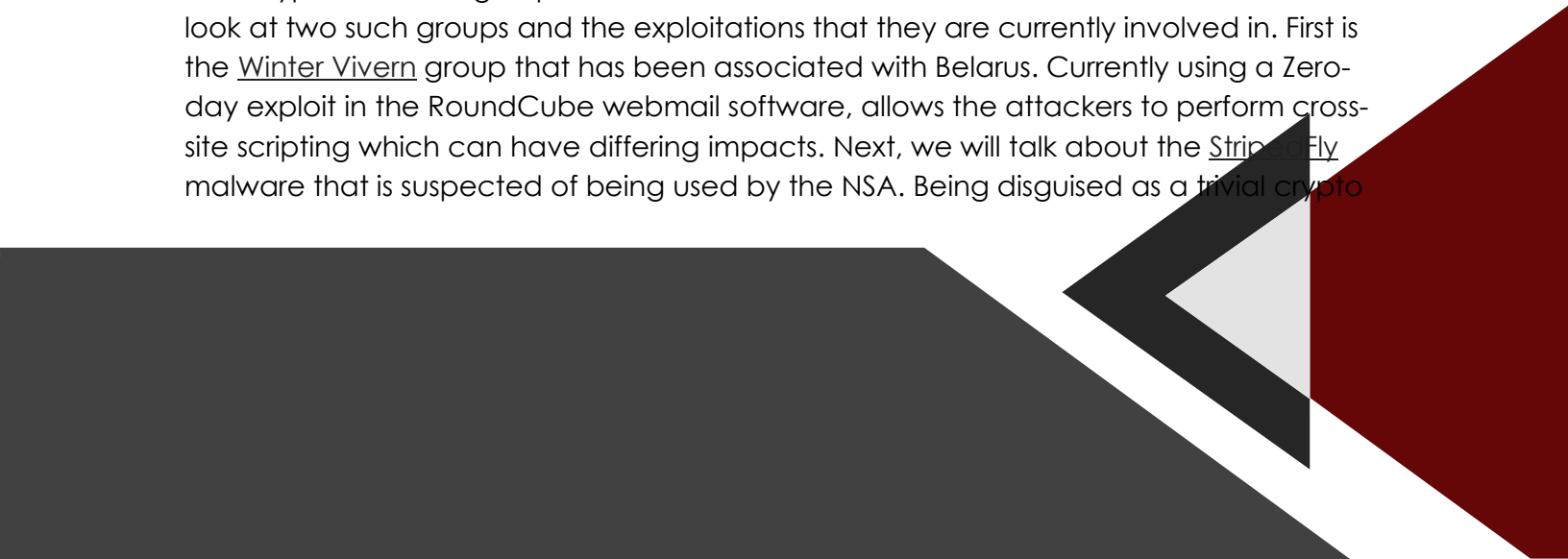
Caleb Leggett
IT Technical Specialist


October 23-27

Welcome to another addition to this week in Cyber. As we take a brief look into the issues that have come up, it is always worth noting the need to stay vigilant and never stop learning. Let's look at the idea of the PoC, Nation-backed threats and advances in the Vishing world.

While not every vulnerability is found by bad actors, it is important to stay up to date with these releases. The main reason that it is important to stay current with these types of releases is that the threat actors most definitely are. While many PoC or Proof of Concept vulnerabilities are released with relevant patching, the release gives attackers the knowledge of a new tactic. The most recent, found by [James Horseman](#) of Horizon3.ai, affects VMWare and Citrix virtual machines. The release is not a new vulnerability but a way to bypass a previous patch to a vulnerability. This just highlights the fact that attackers and defenders are ever in the cat and mouse game of getting in, blocking and finding a new way in. The flaw allows for RCE and is tracked through three different CVE with a score of 8.1-9.6 in severity.

The threat of Nation-backed threat actors is a very important topic to be aware of as these types of threat groups have almost unlimited funds and resources. Let's take a look at two such groups and the exploitations that they are currently involved in. First is the [Winter Vibern](#) group that has been associated with Belarus. Currently using a Zero-day exploit in the RoundCube webmail software, allows the attackers to perform cross-site scripting which can have differing impacts. Next, we will talk about the [Strip-Fly](#) malware that is suspected of being used by the NSA. Being disguised as a trivial crypto





miner, the malware is starting to appear to be a sophisticated spy platform for gathering information. The falw, originally released in 2016, has now been determined to be a much more sophisticated malware that not only pulls data from infected devices but also includes an update module that allows the attackers to update the malware with Windows updates. It is suspected that more than a Million victims have been infected at this point.

As the world of Cyber security is an ever-changing landscape and new attack types are always popping up. As we take a brief glimpse into the advances in Vishing attacks, it is important to understand mitigation. The days of the phone calls with broken English and poor grammar may be coming to an end. With a short audio sample, AI voice generators can impersonate anyone from celebrities to your actual boss. With 30 seconds or less of good quality audio samples, attackers can now generate an audio clip to impersonate a more influential voice in the hopes of getting the desired outcome of the attack. With an increase of 142% from Q3 to Q4 of last year, it is worth noting that these types of attacks are on the rise. For mitigation of these types of attacks, there are a few ways to go about that. First, by asking questions that are not expected, you can throw off the call. As of the writing of this article, the AI software is not at a place where attackers can listen in and make changes on the fly. An example of this would be things like "What do you think of the weather we have been having?". Another way to combat these types of attacks is dropping the call and calling directly from the number that you have. This is more possible when the call is coming from a "coworker" or "boss".

As always, remember that this is not everything and that only you can stay on top of what is going on. Learning of new attack types, ensuring that patches haven't been bypassed and knowing if you may be a target of a nation-backed attacker can make the difference between a minor annoyance to an all-out breach of the system.

Thank you,

Caleb Leggett

