Securities Industry Risk Group (SIRG)

Global Cybersecurity Brief – May 2022

New Russian Sponsored Threat Actor

Many wonder if the conflict with Russia and Ukraine would initiate a '**cyberwar**' by the Russian government. **Researchers** have identified a Russian state sponsored threat actor named 'Ember Bear', also believed to be known as UAC-0056, Lorec53, Lorec Bear, Bleeding Bear, and Saint Bear, and is likely an intelligence gathering adversary group that has operated against government and military organizations in Eastern Europe. The group seems to weaponize its data obtained during intrusions to support information operations aiming at creating public mistrust in targeted institutions and degrading a government's ability to counter. Ember Bear is responsible for using the WhisperGate wiper malware against Ukraine networks in January before Russia invaded the country.

Despite Ember Bear being a state sponsored. threat actor, it is different because it cannot be tied to a specific Russian organization. Its target profile assessed intent. Its tactics, techniques, and procedures (TTPs) are consistent with other Russian GRU cyber operations.

An Authenticated Zero-Trust Approach in Four Steps

Many organizations are relying more on a **zero-trust policy** when users access their systems. While authenticating a user is a critical step, evaluating the authorization of a user is equally important. Authorization is not new but moving to an orchestrated approach to authorization provides a centralized, overarching view of policies. There are four integral steps within the policy modeling process: identifying applications, determining requirements, considering attributes, and authoring policies. As with any zero-trust policy, an organization should never trust and always verify to ultimately provide a reasonable access decision.

Are Cyber-Defense Strategies Secure in the Public-Cloud?

The great migration to **utilize the public-cloud** took a fast track within the last two years, with many organizations scrambling to secure their remote workforce. While moving to the cloud provided the preferred security method for employees working remotely, misconfigurations and a lack of visibility into cloud assets and inventory were a major concern. According to a report from Cloud Security Alliance (CSA), respondents showed there is still a lack of alignment between an organization's cloud security, IT operations, and developer teams on not only security policies but the enforcement of strategies leaving gaps in communications of these critical areas.

CISA Adds Flaws to It's Actively Exploited Bugs List

The **Cybersecurity and Infrastructure Security Agency** (CISA) added the following security flaws: (**CVE-2022-22960**), a VMware vulnerability, was patched on 6 April that "allows attackers to escalate privileges to root vulnerable servers due to improper permissions in support scripts" and (**CVE-2022-01364**), allowing remote code execution due to a V8 type confusion weakness.