TECH HIVE ADVISORY

Cybersecurity, News, Events and Threat Advisories

Security Advisory

Volume 1 / Issue 2

Vulnerability Research Community Now Target of Attackers

What is the issue

The threat actors' posts on social media such as Twitter, LinkedIn, and Telegram usually contain links to their research blogs which contain vulnerability disclosures that are already publicly disclosed. The blogs also contain research works of unsuspecting legitimate security researchers. All of these make them appear credible. They then approach targeted security and vulnerability researchers with whom they establish initial communication. One of the reported tactics is to propose a collaboration to the targets to whom they send a Visual Studio Project. Unknown to the targets, the Visual Studio Project would contain a source code for exploiting vulnerabilities in their systems and malware that would communicate with the threat actors.

Another tactic used is to send a link that leads to their research blogs to the target where a malicious code would be installed on the latter's system and communicated to the threat actors. Noteworthy is the fact that when these attacks happened, the victims were reported to have fully patched up and up-to-date Windows 10 and Chrome browser. Also, the attacks have only been seen to be targeted at Windows systems.

Google TAG has made a list of the blogs, social media accounts, and some links for security researchers to view. Some vulnerability researchers have come out to disclose their encounter or communication with these threat actors.

The attacks are aimed at accessing data on the vulnerability that their victims had discovered so that the threat actors may use it for their own exploits.

What should you do?

- Security and vulnerability researchers are advised to check their browsing history to confirm if they had interacted with any of the social media profiles, links, or blogs. If yes, the researcher's system may have been compromised.
- A separate system or device should be used for actual security research work and for interaction with the vulnerability and security research community and general browsing.

TLDR

Security and vulnerability researchers of different organisations are now targets of an ongoing campaign attributed to threat actors believed to be sponsored by the North Korean government. The threat actors are reported to create blogs and multiple social media accounts to look credible when they interact with their targets. They also post on their blogs, social media, and share contents that may catch the attention of their targets and thereafter establish communication with them. These attacks were discovered by Google Threat Analysis Group (TAG). See detailed information here

Severity: high

Contact Us

@techhiveadvisory
contact@techhiveadvisory.org.mg
www.techhiveadvisory.org.ng