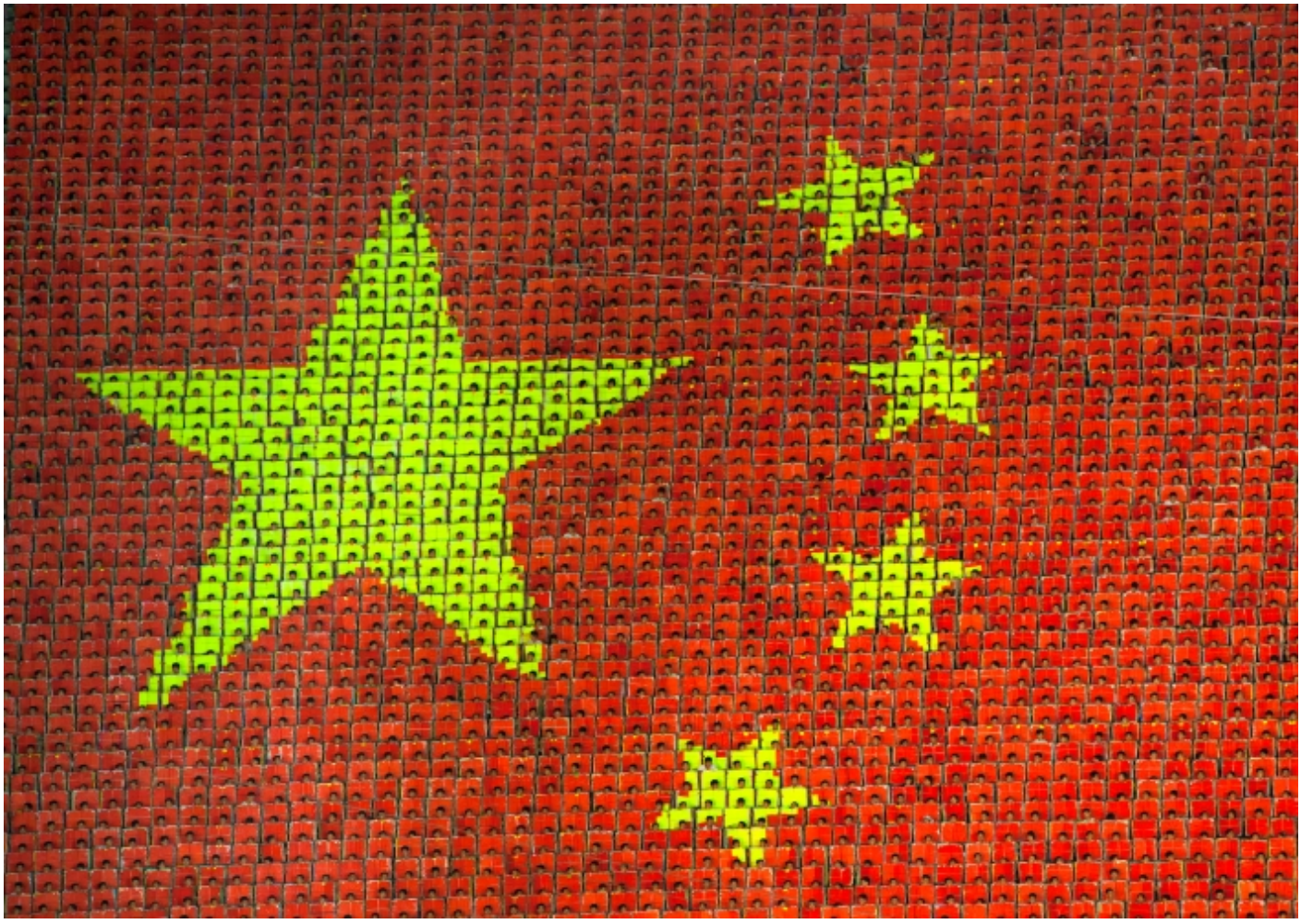
www.cyberscoop.com /china-hacking-budworm-apt27-nsa-threat/

Chinese-linked hackers targeted U.S. state legislature, researchers say

By AJ Vicens ⋮⋮ 10/13/2022



Chinese flag made by children holding up colored boards in North Korea on Sept. 6, 2012. (Photo by Eric Lafforgue/Art In All Of Us/Corbis via Getty Images)

A long-running Chinese-linked cyberespionage group targeted a U.S. state legislature's network in July, marking the outfit's first confirmed attack against the U.S. in years, according to analysis published Thursday.

The findings from the Symantec Threat Hunter Team point to a group the company refers to as Budworm. Other researchers call the group Bronze Union, APT27, Emissary Panda, Lucky Mouse and Temp.Hippo. The group has operated since at least 2013 and is known for targeting a wide range of industries "in support of its political and military intelligence-collection objectives."

The outfit has attacked "a number of strategically significant targets" over the last six months, Symantec said, including the government of a Middle Eastern country, a multinational electronics manufacturer as

well as the unnamed U.S. state legislature.

Dick O'Brien, principal intelligence analyst for the Symantec Threat Hunter Team, declined to share additional details related to the attack, other than to say that it was an attack on its network, "which presumably both legislators and employees had access to."

It's unclear if the operation against the legislature resulted in data theft or other lasting effects.

The findings come as U.S. officials warn that Chinese hacking activity represents a growing and troubling threat. National Security Agency cyber chief Rob Joyce told reporters last week that China has become "really brazen, doubling down on their activities to steal intellectual property and compromise sensitive networks."

The comments came after the NSA, FBI and the Cybersecurity Infrastructure and Security Agency published the top vulnerabilities that Chinese-linked cyber operators use to target U.S. and allied networks. The notice reported that the agencies assess that these efforts represent "one of the largest and most dynamic threats to U.S. government and civilian networks," particularly with respect to telecoms, defense industrial base organizations and other critical infrastructure entities.

Chinese-aligned hacking groups represent a sprawling and active adversary to government and private institutions around the world. Activities ranging from espionage to disinformation to ransomware (potentially as a cover for other activity and sometimes perhaps as a money-making effort on the side) have been well documented in recent years, attributable to a range of overlapping and fluid Chinese-linked groups.

In November 2021, researchers with Palo Alto Networks said tools and tactics similar to those used by APT27 were involved in cyberespionage efforts against U.S. targets in September of last year, but no definitive links were established at the time.

O'Brien told CyberScoop that his team agreed with Palo Alto's assessment of that situation, but added that "in this case, we're confident that what we're seeing is Budworm."

The recent attacks Symantec attributes to Budworm took advantage of two Log4j vulnerabilities to compromise Apache Tomcat service on servers and install web shells. From there, the group installed malware from the HyperBro malware family, as well as the PlugX/Korplug remote access trojan, the researchers said.

"Budworm is known for mounting ambitious attacks against high-value targets," the researchers said. "While there were frequent reports of Budworm targeting U.S. organizations six to eight years ago, in more recent years the group's activity appears to have been largely focused on Asia, the Middle East, and Europe … A resumption of attacks against U.S.-based targets could signal a change in focus for the group."