China, North Korea pursue new targets while honing cyber capabilities

blogs.microsoft.com/on-the-issues/2023/09/07/digital-threats-cyberattacks-east-asia-china-north-korea/

September 7, 2023

In the past year, China has honed a new capability to automatically generate images it can use for influence operations meant to mimic U.S. voters across the political spectrum and create controversy along racial, economic, and ideological lines. This new capability is powered by artificial intelligence that attempts to create high-quality content that could go viral across social networks in the U.S. and other democracies. These images are most likely created by something called diffusion-powered image generators that use AI to not only create compelling images but also learn to improve them over time.

Today, the Microsoft Threat Analysis Center (MTAC) is issuing Sophistication, scope, and scale: Digital threats from East Asia increase in breadth and effectiveness, as part of an ongoing series of reports on the threat posed by influence operations and cyber activity, identifying specific sectors and regions at heightened risk.

We have observed China-affiliated actors leveraging AI-generated visual media in a broad campaign that largely focuses on politically divisive topics, such as gun violence, and denigrating U.S. political figures and symbols. This technology produces more eye-catching content than the awkward digital drawings and stock photo collages used in previous campaigns. We can expect China to continue to hone this technology over time, though it remains to be seen how and when it will deploy it at scale.

As Microsoft noted in our recent report Governing AI: A Blueprint for the Future, public- and private-sector institutions need to collectively address the weaponization of technology, including AI, by cyber and influence threat actors. We report on digital threats we detect – including the use of AI – to inform policymakers, security practitioners, and the public about any threats, current or emerging, that new technologies may pose to information integrity and democracy. We will continue to share our knowledge, and call on partners to do so as well, as part of our larger blueprint to promote transparency and guide the governance of AI.

In its cyber operations, multiple Chinese state-affiliated threat actors have focused cyberattacks in the South China Sea region, conducting intelligence collection and malware execution against regional governments and industries. Other actors have targeted the U.S. defense industry and U.S. infrastructure, looking for competitive advantages to bolster strategic military aims.

Beginning in May 2023, Storm-0558, a China-based threat actor, accessed Microsoft customer email accounts of approximately 25 organizations including U.S. and European government entities. Microsoft assesses this activity was likely conducted for espionage purposes and has successfully blocked this campaign.

The report also details how China has continued its global efforts to spread state-sponsored propaganda and soften the country's image abroad. The Chinese government is investing resources in messaging to audiences in more languages, on more platforms, while evolving its techniques. For example, we know China employs more than 230 state media employees and affiliates who masquerade as independent social media influencers across all major Western social media platforms.

These influencers, who are recruited, trained, promoted, and funded by China Radio International (CRI) and other Chinese state media outfits, expertly spread localized CCP propaganda that achieves meaningful engagement with audiences around the world, reaching a combined following of at least 103 million people across multiple platforms speaking at least 40 languages.

While China-based threat groups continue to develop and utilize impressive cyber capabilities and IO operations, we have not observed China to combine cyber and influence together – unlike Iran and Russia, which regularly engage in hack-and-leak campaigns.

In addition to what we've observed from China, North Korea is a capable cyber threat, focusing on intelligence gathering and the theft of cryptocurrency needed to generate revenue for the state. Several of North Korea's threat actors have targeted the maritime and shipbuilding sectors, suggesting this as a high-priority area for the North Korean government.

Additionally, multiple North Korean threat actors have recently targeted the Russian government and defense industry – likely for intelligence collection – while simultaneously providing material support for Russia in its war on Ukraine.

The report also looks toward anticipated future actions from China and North Korea in the months ahead, as increasing geopolitical tensions fuel new threat priorities and adversarial strategies. With upcoming elections in 2024, Taiwan and the United States are likely to remain top priorities for China.

No technology platform, including Microsoft's, is perfect. But as nation-state actors continue to target vulnerabilities and deploy malign narratives across the world, we believe it is vital to continue to share intelligence such as this report and to increase cross-industry collaboration on these important issues.

Editor's note: As a part of an ongoing series, today Microsoft published Sophistication, scope, and scale: Digital threats from East Asia increase in breadth and effectiveness. These semi-annual updates on nation-state actors serve to warn our customers and the global community of the threat posed by influence operations and cyber activity, identifying specific sectors and regions at heightened risk. See our previous reporting on Russia and Iran.

Tags: cyberattacks, cybersecurity, cyberwar, Digital Threat Analysis Center, MTAC, Ukraine