Mustang Panda APT

Chinese advanced persistent threat (APT) actor, Mustang Panda (a.k.a. Earth Preta, RedDelta or BRONZE PRESIDENT) is delivering lure archives via spear-phishing emails and Google Drive links. Previously there were three arrival vectors used by Mustang Panda: dynamic link library (DLL) sideloading, shortcut links, and fake file extensions. In October 2022, researchers observed a shift in Mustang Panda's tactics to custom tools such as TONEINS (Trojan), TONESHELL (Backdoor), and PUBLOAD (Trojan). These tools infect a device when the victim clicks on a password protected Google Drive link embedded in the body of a phishing email. This phishing campaign successfully bypasses email scanning services.

A change in targets was also noted at the end of 2022. Historically, Mustang Panda targeted academic institutions, ore and material refineries, specialized fabrication plants, financial institutions, and energy production and distribution. New data revealed the APT group has shifted its focus to maritime, shipping, border control, and immigration agencies. This APT group operates worldwide and is largely motivated by cyberespionage operations. For further information on this threat actor, please visit https://www.criticalstart.com/mustang-panda-and-rise-of-custom-malware-usage/.

The Critical Start Cyber Threat Intelligence (CTI) team will continue to monitor the situation and work closely with the Threat Detection Engineering (TDE) team and the SOC to implement any relevant detections. For future updates, the CTI team will post via ZTAP® Bulletins and on the Critical Start Intelligence Hub.

References:

1. https://www.trendmicro.com/en_us/research/23/c/earth-preta-cyberespionage-campaign-hits-over-200.html?&web_view=true
2. https://www.trendmicro.com/en_us/research/23/c/earth-preta-updated-stealthy-strategies.html
3. https://www.criticalstart.com/mustang-panda-and-rise-of-custom-malware-usage/

2.