Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 03:18:07 UTC

Description(Qihoo 360) Starting in April this year, 360 Baize Lab intercepted a large number of attack samples from an unknown hacker organization. The hacker organization sent a phishing email to the victim by forging a police station investigation letter, COVID-19 detection notice, etc. Through the backdoor virus to control the victim’s machine, steal valuable sensitive data related to the target.

(Proofpoint) In late March 2020, Proofpoint researchers began tracking a new actor with a penchant for using NanoCore and later AsyncRAT, popular commodity remote access trojans (RATs). Dubbed TA2719 by Proofpoint, the actor uses localized lures with colorful images that impersonate local banks, law enforcement, and shipping services. To date, Proofpoint has observed this actor send low volume campaigns to recipients in Austria, Chile, Greece, Hungary, Italy, North Macedonia, Netherlands, Spain, Sweden, Taiwan, United States, and Uruguay.
