Reconnaissance Scanning Tools Used by Chinese Threat Actors and Those Available in Open Source

By Natto Team

Published: 2024-09-04 · Archived: 2026-04-05 15:18:01 UTC

At the end of May, the Natto Team looked into threat group APT41's reconnaissance techniques and toolkit. As we continue our ongoing research on Chinese threat groups, we discovered several other Chinese threat groups using similar reconnaissance techniques and tools to those APT41 used, such as Nmap, a free and open-source network scanner. We also came across reconnaissance techniques and scanning tools that were unique to some of the Chinese threat groups. In addition, like APT41, Chinese threat groups heavily use open-source and locally developed tools, whether well-known security tools or customized malware.

Tools & Malware	Used by Threat Groups	Deployed in Threat Campaigns
NBTscan or modified NBTscan	APT10, (aka: menuPass, Stone Panda, POTASSIUM, Purple Typhoon), GALLIUM, Stately Taurus (aka: Mustang Panda), Earth Lusca, TGR-STA-0043	Operation Cloud Hopper, Operation Soft Cell
ScanBox malware	APT40 (aka: TA423, Red Ladon, GADOLINIUM, Gingham Typhoon, Leviathan, MUDCARP, Temp.Periscope), APT3 (aka: Red Sylvan, Gothic Panda); APT10, Poison Carp (aka Evil Eye, Earth Empusa, Red Dev 16), LuckyCat (aka: TA413, White Dev 9)	
Yasso	TGR-STA-0043	Operation Diplomatic Specter
LadonGo	TGR-STA-0043, Stately Taurus	
sqlmap	Earth Krahang	
nuclei	Earth Krahang	
xray	Earth Krahang	
vscan	Earth Krahang	
pocsuite	Earth Krahang	
wordpresscan	Earth Krahang	
shortname scanner		
veinmind		
Ehole		

Tools, malware, threat groups and threat campaigns mentioned in this report. Source: Natto Thoughts

At least three Chinese state threat groups, including APT10 (a.k.a menuPass, Stone Panda, POTASSIUM (Purple Typhoon); GALLIUM (a.k.a Granite Typhoon), and Stately …

natto thoughts

Continue reading this post for free, courtesy of Natto Team.
