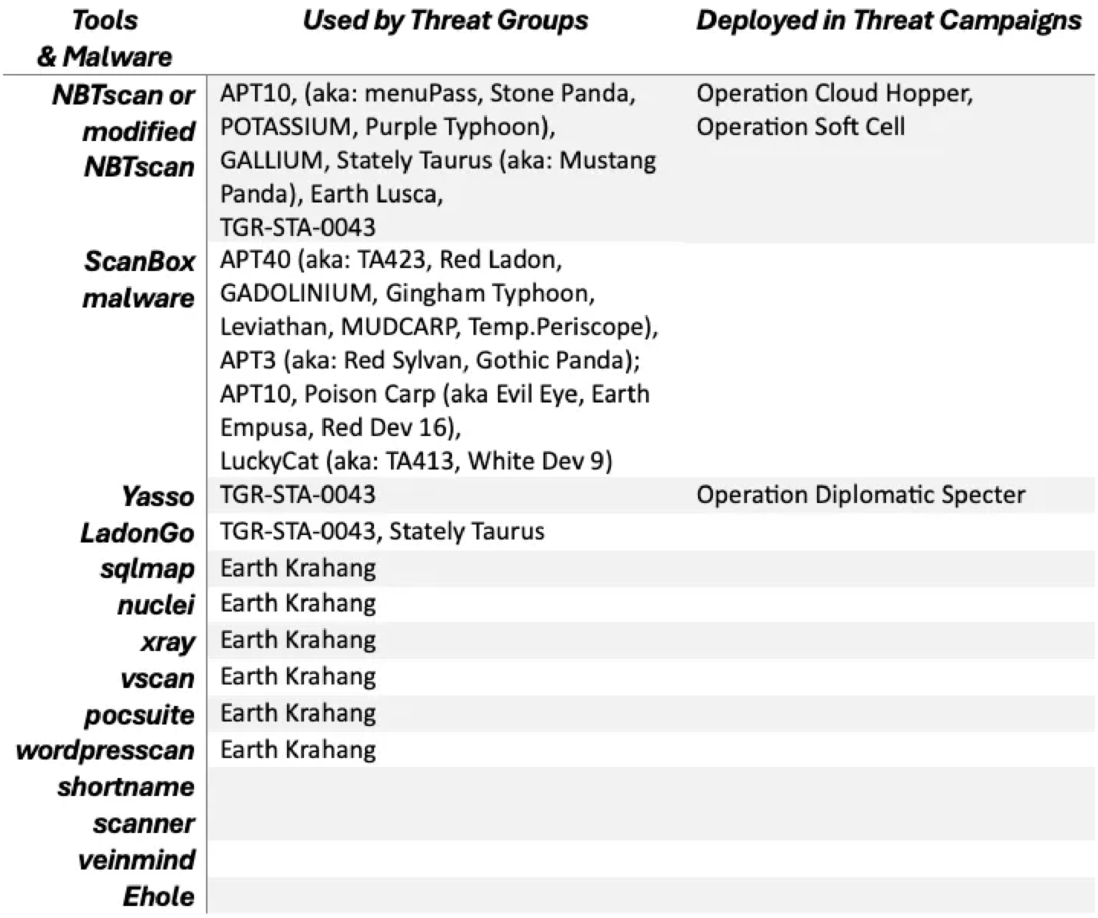
Reconnaissance Scanning Tools Used by Chinese Threat Actors and Those Available in Open Source

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

APT10, GALLIUM and Stately Taurus Use NBTscan or Modified NBTscan – a Tool That Has Appeared Repeatedly Over Ten Years

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 Taurus (a.k.a Mustang Panda) used NBTscan or modified NBTscan in their threat campaigns, according to various reports from firms in the cybersecurity industry.

NBTscan is a free and open-source tool that scans IP networks for NetBIOS (Network Basic Input/Output System) name information. NBTscan is useful for security check, network discovery and forensics investigations. It sends a

NetBIOS status query to each address in a supplied range and lists received information in human-readable form. For each responding host it lists IP address, NetBIOS computer name, logged-in username and MAC address.

APT10

APT10 is a threat group associated with the Chinese Ministry of State Security (MSS). The US Department of Justice (US DoJ) indicted two members of APT10, Zhu Hua (朱华) and Zhang Shilong (张士龙), in December 2018.

In **Operation Cloud Hopper,** reported by PwC (PricewaterhouseCoopers) UK and BAE Systems in 2017, APT10 targeted managed IT service providers. APT10 used **NBTscan** to "search for services of interest across the IT estate and footprint of endpoints of interest," as US-based cybersecurity firm Cybereason summarized it, and to identify system information.

In **Operation Soft Cell,** reported by Cyberreason in 2018, APT10 targeted telecommunications providers worldwide. Researchers discovered one of the reconnaissance commands was to run a **modified NBTscan** tool to identify available NetBIOS name servers locally or over the network.

GALLIUM

GALLIUM is a Chinese state or state-affiliated threat group first named by Microsoft.

Microsoft Threat Intelligence reported that GALLIUM targeted global telecommunication providers in 2019. GALLIUM used a variety of tools, mainly off-the-shelf tools or modified versions of known security tools, to perform reconnaissance and move laterally within a target network. Microsoft researchers observed that GALLIUM used NBTscan to scan for open NetBIOS nameservers on a local or remote TCP/IP network.

Stately Taurus, a.k.a. Mustang Panda

Stately Taurus, a.k.a. Mustang Panda, is a China-based cyber espionage threat actor first named by CrowdStrike.

Unit42 of Palo Alto Networks identified Stately Taurus targeting Southeast Asian governments with cyberespionage attacks in 2023. In a cluster of activity named CL-STA-0044, Stately Taurus scanned infected environments to find live hosts and open ports, as well as existing domain users and domain groups to better understand the breached networks. One of the scanning tools the threat actor used was NBTscan.

Other than the above-mentioned three Chinese threat groups, the Natto Team also discovered reports of Chinese threat groups such as Earth Lusca and TGR-STA-0043 (discussed further below) using NBTscan.

Overall, from observed threat targeting activities spanning the past ten years, Chinese threat groups have repeatedly used NBTscan or modified versions of it. NBTscan is definitely a popular tool among threat groups from China.

Share

APT40 Utilizes ScanBox Malware – a Reconnaissance Tool with a History

APT40 (a.k.a. TA423, Red Ladon, BRONZE MOHAWK, Gadolinium, Gingham Typhoon, Kryptonite Panda, Leviathan, MUDCARP, Periscope, Temp.Periscope, and Temp.Jumper), associated with China's MSS Hainan State Security Department, has been active since at least 2009. Three years ago, in July 2021, The US DoJ indicted four Chinese nationals who were affiliated with APT40's activities.

In July 2024 the Australian Cyber Security Centre (ACSC) – together with the cybersecurity agencies of the countries of the so-called Five Eyes intelligence partnership, plus Germany, Japan and South Korea – jointly issued an urgent "APT40 Advisory" to alert organizations about the group's recent tactics. The 2024 Advisory detailed two significant case studies of APT40 malicious activities against Australian networks. As to the group's reconnaissance techniques and tools, the Advisory highlighted that in one of the case studies APT40 used the Nmap network scanning tool on the compromised appliance to scan other appliances in the same network segment. “This was likely used by the actor to discover other reachable network services which might present opportunities for lateral movement,” according to the Advisory. In addition, “APT40 regularly conducts reconnaissance against networks of interest, including networks in the authoring agencies’ countries, looking for opportunities to compromise its targets. This regular reconnaissance postures the group to identify vulnerable, end-of-life or no longer maintained devices on networks of interest, and to rapidly deploy exploits. APT40 continues to find success exploiting vulnerabilities from as early as 2017.”

Other than the most recent APT40 Advisory, the Natto Team examined reports about APT40’s threat activity published in 2022 and discovered APT40’s use of ScanBox malware is particularly interesting.

In August 2022, researchers from PwC and US cybersecurity company Proofpoint jointly published an analysis of APT40 (a.k.a. TA423 / Red Ladon)’s cyber espionage campaign targeting local and federal Australian governmental agencies, Australian news media companies, and global heavy industry manufacturers that maintain fleets of wind turbines in the South China Sea. In its targeted phishing campaigns, APT40 used malicious websites, with URLs impersonating those of Australian media entities, to serve the Scanbox reconnaissance framework to anyone visiting those sites.

What is Scanbox? According to the Infosec Institute,

> ScanBox is a JavaScript-based web reconnaissance and exploitation framework. The function of ScanBox is to collect information about the visitor's system without infecting the system. Examples of collected information includes:
>
> - the last page the user was on before visiting the compromised website,
> - the OS (operating system) of the system and the language settings of the system,
> - the screen width and height,
> - the web browsers used by the victim,
> - the geographical location,
> - security softwares used
> - and programs like Java, Acrobat Reader, Microsoft Office and Adobe Flash versions used.
>
> ScanBox also can log the keystrokes the victim is typing inside the website under the control of the attacker, which could include the passwords and other sensitive information of the users. All this information is then sent to a remote C&C [command and control] server controlled by the attackers.
>
> ScanBox's goal is to collect information that will later be misused to compromise specific targets. ScanBox is particularly dangerous, as it doesn't require malware to be successfully deployed to [the victim’s] disk in order to steal information. Instead, the key logging functionality would do the same work by simply requiring the JavaScript code to be executed by the web browser. The framework also facilitates surveillance, enabling attackers to exploit vulnerabilities in visitors' systems by pushing & executing malware.

AlienVault, (now LevelBlue, a joint venture with AT&T), first described ScanBox as early as 2014. Over the past ten years, cyber security firms have reported ScanBox being deployed in various threat campaigns, mostly conducted by Chinese threat groups, such as the following:

- Red Sylvan (a.k.a. APT3, Gothic Panda);
- Red Apollo (a.k.a. APT10, Stone Panda);
- Red Phoenix (a.k.a. APT27, Emissary Panda);
- TA423 / Red Ladon (a.k.a. APT40, Leviathan, GADOLINIUM, TEMP.Periscope);

- Red Dev 16 (a.k.a. Evil Eye, Earth Empusa, Poison Carp); and,
- TA413 / White Dev 9 (a.k.a. LuckyCat).

PwC Threat Intelligence assessed it is highly likely that ScanBox was shared privately amongst multiple China-based threat actors. Leaked internal documents of Chinese information security company i-SOON provided ample evidence that China's hacker-for-hire groups share tools and services for a price.

In the 2022 APT40 threat activity reported by Proofpoint and PwC, APT40 customized ScanBox script and related modules for its campaign. Before 2022, the last time that APT40 used ScanBox was observed in 2018. Proofpoint and PwC Researchers have observed that APT40, both in 2018 and 2022, conducted campaigns using an upcoming national election as a lure, wherein the threat actor built local news-themed malicious websites to draw targets.

Although Chinese threat actors have been using web reconnaissance tools like Scanbox for over a decade, it seems they have no reason to stop using them. This is likely because Scanbox is effective and available.

Operation Diplomatic Specter and Yasso, a New Penetration Testing Tool Set, Point to Evolving Reconnaissance Techniques and Tools

In May 2024, Unit 42 of Palo Alto Networks reported Operation Diplomatic Specter, an ongoing cyber espionage campaign since at least late 2022, conducted by a Chinese APT group named TGR-STA-0043, and targeting governmental entities in the Middle East, Africa and Asia. As to the reconnaissance techniques and tools, Unit 42 researchers observed tools often used by other Chinese groups, such as LadonGo, a web scanning tool, and the NBTscan tool discussed above. However, the threat actor also used a relatively new penetration testing tool set named **Yasso**, which "marked a shift in the tactics" employed by TGR-STA-0043. Unit 42 researchers assessed Yasso's unique features, such as "incorporating powerful SQL penetration functions and database capabilities," set Yasso apart from other tools. Yasso tool set comes with "a range of functionalities, including…scanning, brute forcing, remote interactive shell capabilities and arbitrary command execution."

Interestingly, the developer of Yasso is a Chinese speaking penetration tester nicknamed SaiRson. In the "about me" section of his Github repository, SaiRson claims to be "the code people who make weapons for the Red team," and "a college student."

Unit42 assessed with "high confidence that a single threat actor orchestrates Operation Diplomatic Specter, operating on behalf of Chinese state-aligned interests." The TGR-STA-0043 actor focused on current geopolitical affairs and attempted to obtain sensitive and classified information about entities, such as diplomatic and economic missions, embassies, military operations, political meetings, ministries of the targeted countries and high-ranking officials.

Unlike Scanbox, Yasso is a new tool that was first released in January 2022 with a range of functionalities. The campaigns that used Yasso looked like high-level cyber espionage campaigns. Does it mean TGR-STA-0043 actor is more like a uniformed state actor rather than just a state-aligned hacker-for-hire? Probably Yes.

Earth Krahang Employs Open-Source Scanning Tools to Get the Job Done

Researchers from Trend Micro, an American-Japanese cyber security company, assessed that Earth Krahang is a "China-nexus threat actor." Earth Krahang and Earth Lusca, a threat group with potential links to the Chinese information technology company i-Soon, targeted a similar range of victims and became "more intertwined as they approach their goal." Although Earth Krahang uses different infrastructure and different initial stage backdoors than Earth Lusca did in 2021, the two groups are possibly "managed by the same threat group," according to Trend Micro.

In a report titled "Earth Krahang Exploits Intergovernmental Trust to Launch Cross-Government Attacks" published in March 2024, Trend Micro researchers detailed reconnaissance techniques and tools Earth Krahang used. Earth Krahang scanned public-facing servers as one of the infection vectors. According to the report:

> “Earth Krahang heavily employs open-source scanning tools that perform recursive searches of folders such as .git or .idea. The threat actor also resorts to simply brute-forcing directories to help identify files that may contain sensitive information such as file paths or passwords on the victim’s servers. They also tend to examine the subdomains of their targets to find interesting and possible unmaintained servers. Earth Krahang also conducts vulnerability scanning with tools like **sqlmap**, **nuclei**, **xray**, **vscan**, **pocsuite**, and **wordpressscan** to find web server vulnerabilities that allow them to access the server, drop web shells, and install backdoors.”

The Natto Team discovered that at least two of the six vulnerability scanning tools mentioned above were created by Chinese-speaking developers. See the following details:

- sqlmap: rated as the best specialty scanner for databases by eSecurity Planet, a resource of cybersecurity vendors and trends.
- nuclei: described as “a fast and customizable vulnerability scanner powered by simple YAML-based templates.”
- xray: a security assessment tool that is not open source, although it can be found in a repository that “mainly contains community-contributed POCs (proof-of-concepts),” according to its Github repository introduction. The tool is coded in both English and Chinese description. It is likely developed by a Chinese developer.
- pocsuite (updated version pocsuite3): an open-sourced remote vulnerability testing framework developed by the Chinese information security company Knownsec’s 404 team. (The Natto Team discusses KnownSec in the report “Who Has the Best Scanning Tools in China?)
- **Wordpressscan** (likely WPScan): a vulnerability database for WordPress, a web content management system often used for blogs and other do-it-yourself websites. The tool runs a Wordpress vulnerability scan to find Wordpress exploits, outdated plugins, and more.

Countless Open-Source Scanning Tools Available

While the Natto Team was digging into the world of reconnaissance and scanning tools, we ran into a GitHub repository called “We5ter/Scanners-Box” with a logo displayed as “Hacker Toolkit SCANBOX”. The repository is in both English and Chinese languages and described as follows: “Scanners Box also known as scanbox, is a powerful hacker toolkit.” It claims it “has collected more than 10 categories of open-source scanners from Github, including subdomain, database, middleware and other modular design scanner etc.” The collection excluded well-known scanning tools, such as Nmap, Metasploit and brakeman. The author of the Github repository is “Wester” or “We5ter.” Wester’s Github page lists his Paypal address, giving the name Zhiyang Zeng . It also lists his personal webpage. In his personal webpage, Wester displayed the Scanners Box project and two conference slides which he presented. One is POC 2019 in South Korea and the other is Black Hat Asia 2021. The Black Hat speaker biography identified Wester as Zhiyang Zeng, “a senior security researcher at OPPO ZIWU Security Lab, he specializes in penetration testing, browser security and android security.” OPPO is a Chinese consumer electronics manufacturer. OPPO’s smartphone was the top smartphone brand in China in 2019 and was ranked fourth in market share worldwide in 2023.

The Scanners Box collection included hundreds of scanning tools. Unsurprisingly, many of them are Chinese developers’ tools. Some examples include the following:

- shortname scanner, developed by Li Jiejie. The Natto Team discussed Li’s tools in the APT41 scanning tool report;
- veinmind, a container security toolset developed by Chinese information security company CHAITIN, one of the Chinese companies with the top scanning products.
- **Ehole**: a core system fingerprint detection tool for Red team developed by Edge Security Team (hxxps://forum.ywhack[.]com/index.php), a Chinese security hacking forum.

Chinese developers’ enthusiasm for scanning tools likely reflects the popularity, importance and demand for better tools. No matter whether it is for white-hat security testing purposes or for malicious threat campaigns, using scanning tools to find access points or security weaknesses is always the first step.

Thanks for reading Natto Thoughts! Subscribe for free to receive new posts and support the Natto Team’s work.