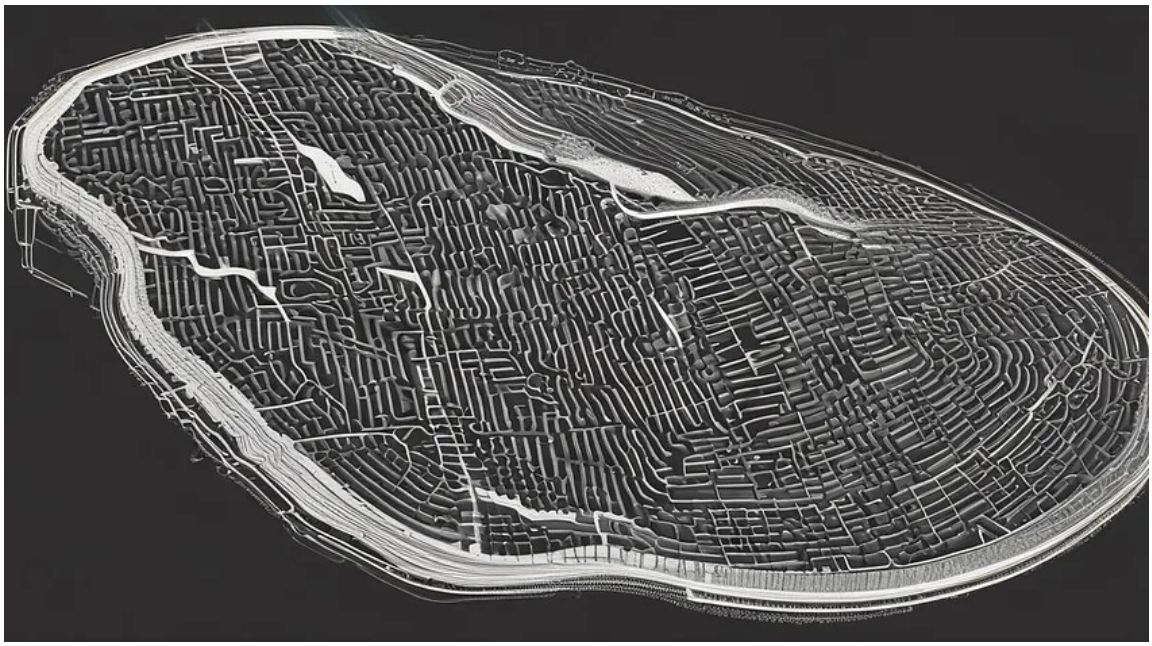
APT41's Reconnaissance Techniques and Toolkit: Nmap and What Else?

Natto Team ⋮⋮ 5/29/2024

APT41 and other Chinese malicious cyber actors can choose from numerous reconnaissance tools developed in China and abroad, including those developed for legitimate defensive purposes.

In the previous report "i-SOON Toolkit: What is 'TZ'?", the Natto Team discovered the importance of network reconnaissance work for the Chinese Public Security bureaus and companies in the information security industry that support the work. Reconnaissance – gathering information on a target – is the first step that cyber threat actors take in an operation, according to the so-called Cyber Kill Chain framework. Reconnaissance provides the threat actor with both non-technical information on the target, such as a target's organizational details and information on personnel, and technical information, including information about the network, hosts, applications, and users. Over the years, researchers have observed and studied various reconnaissance techniques and tools commonly used in targeted attack cases. In this report, the Natto Team looks into the reconnaissance techniques and toolkit of APT41, a Chinese state-sponsored hacking group, and explores popular network reconnaissance tools developed in China.



APT41's Reconnaissance Techniques

As the Natto Team previously pointed out, network reconnaissance can be used defensively by security researchers for security testing purposes, as in penetration testing, to identify the vulnerabilities of a system one is protecting. However, when adversaries perform reconnaissance as part of a malicious operation, their goal is to identify weak points of the targeted system and set up an effective attack plan.

APT41 infamously used well-known security tools while conducting technical information reconnaissance. The "China-based Threat Actor Profiles," published by the Health Sector Cybersecurity Coordination Center (HC3) of the US Department of Health and Human Services in August 2023, described APT41 as using "Acunetix, Nmap, JexBoss, Sqlmap, a customized version of Cobalt Strike, and fofa.so which is roughly a Chinese equivalent of the popular website Shodan." … "To conduct reconnaissance, they [APT41] are known to use the previously-mentioned Acunetix and Nmap, as well as Sqlmap, OneForAll, subdomain3, subDomainsBrute, and Sublist3r. They

frequently use spear phishing as an infection vector, but are also heavily reliant on SQL injections to initially penetrate a target organization." (See below for descriptions of these tools).

Once gaining access to targeted systems, APT41 performed internal reconnaissance in its threat campaigns which played a significant role contributing to a successful attack.

Throughout the attack process, reconnaissance can be seen in two phases: external reconnaissance and internal reconnaissance, according to a study of "Survey and Taxonomy of Adversarial Reconnaissance Techniques" published on ACM Computer Surveys in December 2022. The study explained,

> "External reconnaissance is performed to collect technical or non-technical information before gaining access to an internal asset, and internal reconnaissance is performed to obtain system information from the internal network. The adversary can perform internal reconnaissance utilizing various scanning, such as active host or port scan, and local host discovery techniques. Sometimes, adversaries wait and utilize passive scanning techniques such as sniffing packets to obtain a network view and discover system architectures, protocol mappings, and exploitable vulnerabilities. Passive scanning helps adversaries to remain undetected for extended periods of time. Adversaries can exploit vulnerabilities using the collected information to compromise other hosts to get closer to the target resources."

When conducting internal reconnaissance, APT41 used a technique called Execution Guardrails. Execution Guardrails techniques utilize information collected from a host (operating system version, Internet Protocol [IP] address, Active Directory name, shared network name, etc.) to limit the activation of malware. Threat actors use execution guardrails to avoid detection and exposure of their malware in parts of victim systems that they do not intend to compromise. They check for an expected target-specific value and only continue execution of the malware if there is such a match. Security researchers who closely follow APT41's tactics, techniques and procedures (TTPs) informally awarded APT41 "the lifetime achievement in guardrailing." APT41 applied the techniques in its supply chain compromises from 2014 to 2018. In an APT41 activity analysis published by Mandiant, now a Google company, researchers discovered that the initial stages of APT41 supply chain compromises affected very large numbers of victims. However, the actors limited follow-on activity to a very select list of victims, most likely to reduce detection and ensure any additional malware is delivered only to intended victims. In one case, the malware payloads were restricted by MAC (media access control) address — the unique identifier of each device within a network.

In the process of internal reconnaissance, APT41 leveraged built-in Windows commands, such as "netstat" and "net share," in addition to the custom and non-public malware families SOGU, HIGHNOON, and WIDETONE to collect host information and network connections and conduct port scans. For example, WIDETONE is capable of conducting port scans and password brute-force attacks and collecting network information.

APT41's Reconnaissance Tools

Examining well-known security tools used by APT41, the Natto Team discovered APT41 has taken advantage of reputable tools developed overseas, such as Nmap, as well as tools developed in China. Some examples below:

- **Nmap (Network Mapper)**, is a free and open-source network scanner for network discovery, administration, and security auditing. Nmap has been widely studied and used in China. A search for nmap on Sogou (see sceenshot below), a popular Chinese search engine, yielded websites providing Nmap downloads and installs, Nmap Wikipedia, and Nmap instruction and training videos. One Nmap instruction video was part of the "Hacker Toolkits" training series from the 51CTO institute (edu.51cto[.]com), a well-known IT training platform based in Beijing China with 20 million registered users.

Search results for "Nmap": downloads, articles, tutorials and videos related to the tool. Source: Sogou

- **OneForAll** is a reconnaissance tool for subdomain enumeration. It is developed by Jing Ling (@shmilylty) who is likely based in China. The developer Jing Ling and online reviews called OneForAll "a powerful Chinese subdomain enumeration tool" with "powerful collection capability and processing feature." It supports "subdomain blasting, verification and takeover." The developer of OneForAll claimed to pull data from "a multitude of exotic Chinese data sources that other tools typically do not query," such as Baidu Cloud Observation, Gitee (the Chinese equivalent of GitHub), and ChinaZ Alexa. It is worth noting Jing Ling has not

been active on Twitter (now called X), a platform officially banned in China, since May 2020. Jing Ling's last contribution activity on his GitHub account was in December 2022. Jing Ling's website Hackfun is still active.

- **Subdomain3**, is a tool to be used to discover subdomains. GitHub account "yanxiu0614" hosts Subdomain3. A Chinese language website search suggested yanxiu0614 is a Chinese developer located in China. A review and instruction manual for Subdomain3 – "Hacking with Subdomain3" described how to install and use Subdomain3.

- SubDomainsBrute, is a subdomain brute forcing tool. Subdomain brute forcing uses "a list of common subdomain names and attempts to connect to them by appending them to a target domain." GitHub account "lijiejie" hosts SubDomainBrute. The account also has other tools such as "BBScan – a fast vulnerability scanner", "EasyPen – a GUI program helps pentesters do target discovery, vulnerability scan and exploitation," and "GitHack – a '.git' folder disclosure exploit." "lijiejie"'s blog – "李劼杰的博客" (hxxps://www.lijiejie[.]com/) uses "lijiejie" in three Chinese characters which likely is the blogger's name.

- FOFA, is an internet asset scanner developed by Chinese Company "Beijing Huashun Xin'an Technology Co., Ltd(北京华顺信安科技公司). FOFA claims to have accumulated "4 billion internet assets and more than 350,000 fingerprint rules and identified most software and hardware network assets." APT41 used FOFA to searched open technical databases for passive scanning of victims.

Other Popular Chinese Scanning Tools

APT41's heavy use of locally developed tools, either well-known security tools or customized malware such as WIDETONE, suggests that one of the group's operational tactics is to have tools that they could easily access and control. Since improving network reconnaissance capability has been a focus for the Chinese government, black hat or white hat hackers and commercial businesses in China have been keen on developing products and providing services in reconnaissance tools. X-scan and ZoomEye are two examples. It is not known whether APT41 has used these particular tools, but they too would be at its disposal.

X-scan – a Hacker-Developed Nmap-like Tool

X-scan is the most well-known network vulnerability scanner in China that operates both at the command line and GUI (graphical user interface) front-end. (hxxp://www.vulnerabilityassessment.co[.]uk/xscan.htm) X-scan was developed by China's famous hacker group Xfocus in 2000. Xfocus was founded in 1998 in China as a "non-profit and free technology organization" and "devoted to research and demonstration of weaknesses (vulnerabilities) related to network services and communication security." The group's slogan was "From the Internet. For the Internet." Its website currently is unavailable, and its last post was uploaded in September 2010.

Xfocus has been hosting a closed-door conference called XCon since 2002. (hxxp://xcon.xfocus[.]net/). In the early years of Xcon, many individual hackers or wanna-be hacker participated in the conference. In the past 10 years or so, Xcon has been commercialized and become an open conference with many industry representatives participating, looking for business opportunities.

The most recent version of X-scan is X-scan3.3. It is available for download in various Chinese software download websites. Many still rave about X-scan as "the brainchild of many hackers in China." (https://baike.sogou[.]com/v126682.htm?ch=frombaikevr&fromTitle=X-scan)

ZoomEye, a Search Engine that can Search Industrial Control Systems

ZoomEye is developed by Knownsec Hong Kong. KnownSec (知道创宇) is an information security company headquartered in Beijing China. Welivesecurity, an internet security news outlet of ESET, a malware detection and analysis company headquartered in Bratislava, Slovakia, listed ZoomEye as one of the top 5 search engines for Internet-connected devices and services along with Shodan, Censys, FOFA, and BinaryEdge. These search engines offer detailed information on internet-connected devices and services, including their IP address, operating system, software and open ports. As noted previously, FOFA is also owned by Chinese company Huashun Xin'an. Therefore, two of the five top cyberspace search engines are owned by Chinese companies.

ZoomEye is also listed as one of the top industrial control security tools. A Chinese tech blog on network reconnaissance and scanning demonstrated using ZoomEye to discover an IP (Internet Protocol Address) of a Siemens industrial control system (ICS).

Is the Offensive Use of Reconnaissance Tools a Trend?

Many reconnaissance tools are originally designed and developed for security testing purposes. However, in the APT41 case, the actors have used locally sourced well-known security tools for malicious threat campaigns. As we know previously, several APT41 actors operated the Chengdu 404 company. Chengdu 404 had developed software products and provided services for its ongoing business operations. For example, in August 2019, Chengdu 404 provided penetration test services for i-SOON, a company linked to multiple Chinese state-sponsored groups and which the Natto Team has discussed previously. i-SOON also signed a technical service contract with Chengdu 404 to use its "Sonar-X Big Data Analysis Platform," which was "an easily searchable repository for social media data that previously had been obtained by Chengdu 404." These companies may have developed these products and services as part of legitimate business. However, Chengdu 404 and i-SOON are part of China's commercial hacking industry, and they apply these products or tools applied both offensively and defensively depending on the "clients." Therefore, reconnaissance tools, particularly locally sourced (farm-to-table as well?), for offensive use in the Chinese context seem to be ubiquitous and convenient.