Anxun and Chinese APT Activity

By ReliaQuest Threat Research Team 5 March 2024

Published: 2024-03-05 · Archived: 2026-04-05 17:19:08 UTC

Key Points

- The compromise of a key Chinese information security (InfoSec) vendor, Shanghai Anxun Information Technology (Anxun; aka iSOON), led to a rare leak of information. The publicized documents revealed the company's collaborations with the Chinese government and advanced persistent threat (APT) groups in offensive cyber operations.
- Anxun is engaged in Chinese hacker-for-hire activity: facilitating surveillance operations of dissidents, cooperating in espionage campaigns against foreign governments, and training cybersecurity students, among other activities.
- The company is also involved with the modular backdoor malware "ShadowPad," and the 2022 attack against Canadian software company Comm100; this intelligence confirms that Anxun develops or promotes tools that Chinese APT groups often use.
- An Anxun insider is likely responsible for the breach, based on the nature of the information and how it was publicized—Anxun was portrayed as a bad employer whose poor business practices jeopardize China's national security.
- Customers operating in sectors frequently targeted by state-sponsored activity (e.g., manufacturing, public administration) will benefit from the recommendations in this report concerning insider threats and APT activity; steps include blocking suspicious web proxy categories and simulating phishing to increase employee awareness.

Documents recently leaked from Anxun, a key private security contractor of the Chinese Ministry of Public Security (MPS), provide rare insight into Chinese state-sponsored cyber-threat activity, especially the domestic hacker-for-hire ecosystem. The documents revealed that the Chinese government uses Anxun as hackers-for-hire to facilitate cyber-threat operations against foreign governments and dissidents, as well as other entities. Defenders can use the insights and recommendations described in this report to better guard against similar APT activity and insider threats—particularly in frequently targeted sectors: manufacturing; professional, scientific, and technical services; public administration; wholesale trade; information; and construction.

Anxun Surveillance and Aid to Chinese Government

On February 16, 2024, the stolen Anxun data became available on GitHub, and was subsequently removed. The documents included staff information, communication among employees and with customers, details of

surveillance tools that Anxun developed for the Chinese government, and more. They revealed dissident surveillance, espionage against foreign governments, and the dissemination of pro-Beijing content on social media:

- Anxun developed or advertised cyber-surveillance tools for the Chinese government, to target, for example: ethnic minority groups and pro-democracy individuals in Hong Kong and Xinjiang in west China, overseas telecommunications firms, and online-gambling companies in China.
- Anxun hacked into networks in Central and South-East Asia and Taiwan; valuable data stolen from these networks was allegedly sold to Chinese law-enforcement authorities.
- The company advertised “anti-terror” technical support to Xinjiang authorities to monitor native Uyghurs via hacked airline, telecommunications, and government entities from Afghanistan, Malaysia, Mongolia, and Thailand.
- In 2021, the public security bureau of Taizhou, China, paid Anxun RMB 2.6 million (approximately $361,000) to develop tools to track Telegram and X users.
- The Hubei government paid Anxun approximately RMB 1 million ($139,000) for tools to remotely attack iOS systems. The tools can extract the target’s email, phone number, and private messages; monitor them in real time; and publish tweets under their name.
- Anxun extensively promoted to its customers systems that it claimed could be used to generate phishing links. The links, Anxun claimed, would allegedly begin email extraction and activate several other capabilities, such as password changes and setting emails extraction timeframes.
- To its customers, Anxun advertised for sale remote-access trojans (RATs) that target Windows, iOS, and Android systems, and can harvest messages from popular Chinese messaging apps.
- Anxun’s customers expressed interest in data stolen from Australia, Cambodia, Congo, Guinea, Kazakhstan, India, Indonesia, Kyrgyzstan, Malaysia, Mongolia, Myanmar, Nigeria, North Macedonia, Rwanda, South Korea, Taiwan, Thailand, Timor Leste, the UK, and Vietnam, requesting proof of legitimacy in the form of recent samples.
- Anxun targeted the Taiwanese health ministry during the COVID-19 pandemic to find out about Taiwan’s caseload and hospital capacity.
- The company charged $55,000 for an operation to hack a Vietnamese government ministry
- Anxun provided hardware surveillance kits (basic or mini) that resemble a power strip or Xiaomi power bank, to be installed in a target’s home/office and used to infiltrate local Wi-Fi networks. The built-in battery can allegedly last 8 to 20 hours. No setup is required; after the user turns on the power, the device can be remotely controlled to penetrate the network.

Indication of Leak from Inside Anxun

There are several possibilities regarding who leaked the Anxun documents:

- Disgruntled Anxun employee
- Rival company
- Foreign government
- Anti-Chinese Communist Party hacktivists

ReliaQuest regards, with medium confidence, the perpetrator as being a disgruntled employee, mainly based on the leak contents found on GitHub. The files were organized into several sections whose headings accused Anxun of jeopardizing national security and being a bad company to work for. The documents also contained screenshots of conversations in which employees complained about low company morale, long hours, low salary, and the difficulty of tasks.

A rival hacker-for-hire company would have been unlikely to publicly leak the details of Anxun's operations with the Chinese government, for fear of incurring notoriously severe government punishment. And a foreign government would have more likely used the exfiltrated information to determine whether there are any APT groups present in their networks, rather than disclose it publicly and risk Beijing's retaliation. Moreover, hacktivists typically claim responsibility for their attacks to boost their reputation and promote their cause, which did not happen in Anxun's case; it is unlikely that the data leak was ideologically motivated.

Chinese Hacking Ecosystem Links and Threats

Incorporated in September 2010 in Shanghai, Anxun describes itself as a technology-based enterprise that provides InfoSec solutions for various industries. The company has branches and subsidiaries across China and an APT Defense and Research Laboratory in Shanghai. Its role as a hacker-for-hire company is described in the following revelations found in the leaked documents.

Chinese Government Customers

Anxun has advertised offensive and defensive APT capabilities, listing dozens of Chinese government security agencies as its customers. (Anxun's website and its Weibo and WeChat accounts have been taken offline since the leak and remain unavailable at the time of writing.)

Hacker CEO

Anxun's CEO and main investor, Wu Haibo (whose alias in the leaked chats is shutd0wn), is a prominent, pioneering Chinese hacker and an early member of China's first hacktivist group, the Green Army. Wu remains actively involved in Anxun's operations and cyber activity in China, giving talks and interviews with Chinese media and universities.

Link to Chengdu, APT Groups

Evidence points to a working relationship between Anxun and Chinese APT groups based in Chengdu, Sichuan, where Anxun has a branch. Chengdu is an established hub of Chinese APT activity—"RedHotel" and "APT41"

are among the state-sponsored hacking groups based there, and multiple APT groups have set up front companies in Chengdu to hide illicit cyber operations.

According to a 2020 US Department of Justice indictment, Chengdu Silingsi Network Technology Company (aka Chengdu 404) is a front company to hide APT41 cyber-threat activity, which has affected more than 100 US companies. In October 2023, Chengdu 404 sued Anxun in a software development partnership contract dispute. Details of the partnership are not publicly available but, based on Anxun's service offerings, Chengdu 404 probably engaged Anxun to develop a platform or tool to aid cyber-threat campaigns.

Anxun is highly active in developing cyber-operational capabilities in Chengdu. Since 2018, the company has sponsored and/or organized the annual Anxun Cup event (most recently in December 2023): a training "bootcamp" to cultivate network security talents. The event focuses on discovering new techniques, vulnerabilities, and in-depth knowledge about an application or a coding language (see Figure 1). Similarly, Chengdu 404 has displayed an interest in nurturing talent; that company maintains close relations with Sichuan University, likely for recruitment.

Figure 1: Anxun's Weibo post about the Anxun Cup

Chengdu 404 and Anxun encourage cyber-threat capabilities through hacking competitions and training programs, are based in Chengdu, and have known ties to the Chinese government or APT groups. Although we cannot ascertain whether Anxun is an APT group or a front company for an APT group, its many operational similarities to Chengdu 404 suggest either option is a realistic possibility.

Link to Threat Groups via ShadowPad

Anxun's white paper on remote-control management systems, leaked on GitHub, refers to an IP address that was used as a ShadowPad command-and-control (C2) server in August 2021. ShadowPad is a modular backdoor that multiple Chinese threat groups have used since at least 2017. The malware has been attributed to the "Winnti Group," a collective of several Chinese APT groups, including APT41, whose activities occasionally overlap.

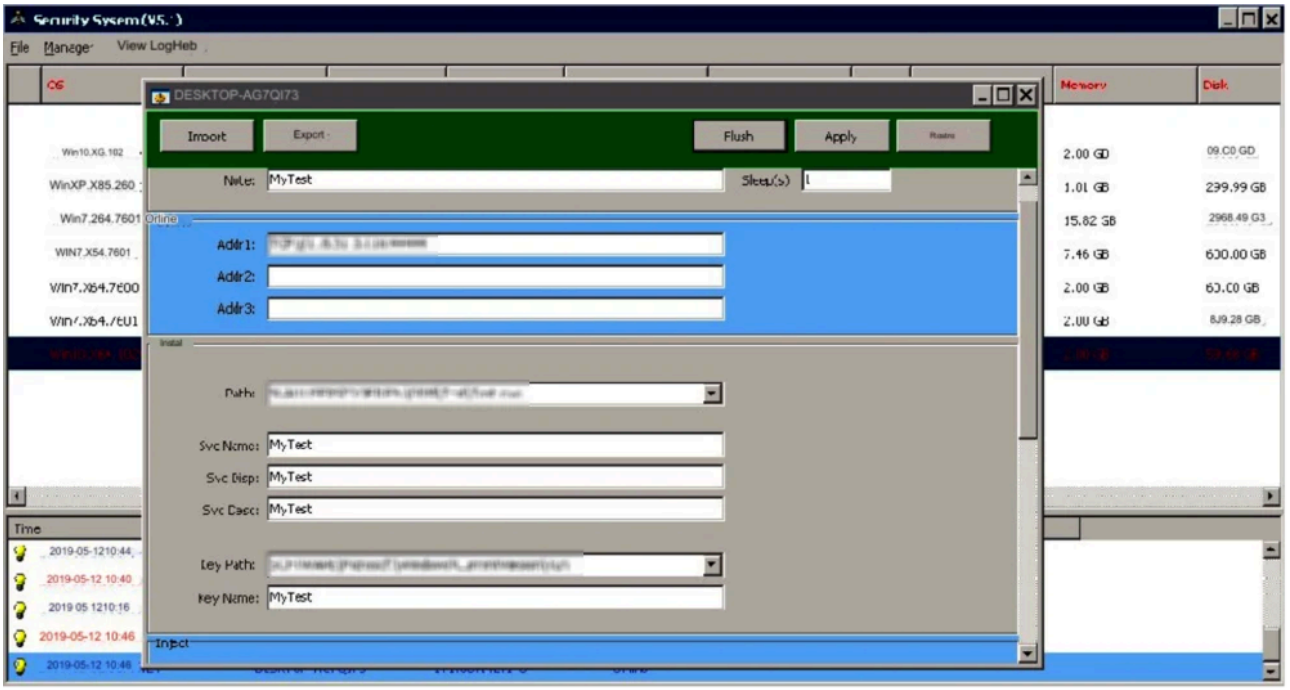

Figure 2: Screenshot of leaked Anxun white paper, showing the redacted IP address used as a ShadowPad C2 server (Source: GitHub)

Link to Attack via Comm100

In September 2022, threat actors used a trojanized installer of Comm100, a chat-based customer engagement application, for a supply-chain attack campaign. A leaked transcript of a conversation between Anxun employees (see Figure 3) confirmed an IP address that is one of the campaign's indicators of compromise (IoCs)—is an Anxun server, cementing the company's involvement. Since August 2022, Comm100 had been unknowingly loading backdoor scripts from the threat actors' infrastructure. In some of the attacks, advanced malware was delivered to the employees of several online gambling platforms; the employees had administrative privileges for their employers' websites, indicating a likely campaign goal of securing administrative access.

2022-06-13 07:40:26	wxid_zb45i0rc71yk21	wxid_c9yv0nsla3yn22	【TCP隧道】 【账号】 admin 【密码】	TCP Tunnel [Account] admin [Password]:
2022-06-13 07:40:34	wxid_c9yv0nsla3yn22	wxid_zb45i0rc71yk21	嗯嗯	Yes, yes
2022-06-13 07:40:37	wxid_c9yv0nsla3yn22	wxid_zb45i0rc71yk21	我日	[swear word]
2022-06-13 07:40:44	wxid_c9yv0nsla3yn22	wxid_zb45i0rc71yk21		
2022-06-13 07:40:54	wxid_c9yv0nsla3yn22	wxid_zb45i0rc71yk21	这个服务器在香港的	This server is in Hong Kong
2022-06-13 07:41:06	wxid_zb45i0rc71yk21	wxid_c9yv0nsla3yn22	你不管	You don't have to care
2022-06-13 07:41:07	wxid_c9yv0nsla3yn22	wxid_zb45i0rc71yk21	domain_access_result(1).csv	
2022-06-13 07:41:11	wxid_c9yv0nsla3yn22	wxid_zb45i0rc71yk21	嗯	Ok
2022-06-13	wxid_zb45i0rc71yk21	wxid_c9yv0nsla3yn22	这个服务器是我们的	This server belongs to us

Figure 3: Screenshot of conversation between Anxun employees, with translation shown to right of original text

Motive and Targets

As the leaked documents indicate, Anxun's cyber-threat activity seems politically oriented, focusing on espionage and surveillance across Asia, followed by Europe, then the US. The company seems to dedicate many of its resources to targeting foreign governments to gain valuable information, which aligns with the general direction and goals of Chinese APT groups and of Chengdu 404.

The data leak has provided rare insight into how the Chinese government outsources parts of its cyber operations to private third-party companies, and how these companies work with one another to fulfill these demands. Screenshots of employee conversations hint at infighting among these third-party contractors despite their collaborations, but the maturity of the Chinese hacker-for-hire industry is evident: Numerous companies like Anxun and Chengdu 404 offer a broad range of hacking services to the Chinese government and APT groups. Anxun will very likely continue to operate without major disruptions.

APT41: A Real and Active Threat

The APT41 group primarily wages financially and politically motivated attacks against the following sectors in North America, Europe, and Asia: public administration; professional, scientific, and technical services; and arts, entertainment, and recreation. However, APT41 attacks have spanned more than 20 countries, and also compromised entities in the information; health care and social assistance; finance and insurance; manufacturing; and utilities sectors. The group remains active, despite the US indictment of several of its members; we most recently reported on APT41's activity in December and September 2023.

Recommendations and Best Practices

We offer the following resources and recommendations to mitigate the risks associated with general APT activity and insider threats.

APT Threats

GreyMatter includes an intelligence content library of threat profiles and intelligence updates to keep our customers abreast of the latest APT activity. Topics include threat-actor tactics, techniques, and procedures; IoCs; tools; and attacks/campaign details. In addition, consider the following practices to guard against common APT activity.

- Routinely review application, security, and system event logs. Look for events outside the normal user baseline that could indicate potentially malicious activity.
- Limit port proxy use within environments and only enable it for the period in which it is required.
- Look for abnormal account activity, such as logons outside normal working hours and impossible time-and-distance logons (e.g., a user logging on from two discrete locations at the same time, or a user who is based in the US logging on repeatedly during typical Chinese working hours).
- Review standard directories for unexpected or unusual files. Monitor these temporary file storage directories for files typically located in standard system paths.
- Forward log files to a hardened centralized logging server, preferably on a segmented network, to ensure log integrity and availability; APT groups typically try to hide their tracks by clearing logs. This recommended action will make it harder for threat actors to cover their tracks as their actions will be captured in multiple locations.
- Patch edge network devices:
    - Ensure that all edge network devices (routers, switches, firewalls, etc.) are regularly updated with the latest security patches. These updates often fix known vulnerabilities that could be exploited by attackers.
    - Use network segmentation to limit the reach of potential attackers. If an edge device is compromise, segmentation can help contain the threat.
    - Ensure that devices are configured properly, according to industry best practices. Misconfiguration can lead to vulnerabilities.
    - Enforce best-practice multi-factor authentication (MFA) and conditional access policies:
        - Require MFA for access to all systems and data. MFA adds an additional layer of security by requiring multiple forms of verification.
        - Regularly review and update MFA and conditional access to adapt to new threats and changes in the organization.

        - Educate users on the importance of MFA and how to use it properly to prevent accidental lockouts or misuse.
        - Implement conditional access policies that take into account user context, device health, location, and risk when granting access to resources.
    - Use strong email security solutions to prevent phishing:
        - Choose email security solutions that offer advanced protection capabilities, such as scanning email attachments and links in real time.
        - Deploy robust anti-spam filters that can detect and block spam and phishing emails before they reach end users.
        - Implement email authentication methods, like Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting & Conformance (DMARC), to prevent spoofing and ensure that emails are verified as coming from legitimate sources.
        - Simulate phishing campaigns to increase employee awareness and help them recognize phishing attempts.
        - Complement technology solutions with user education, as even the best systems can be bypassed by sophisticated social-engineering techniques.

Insider Threats

Although we cannot confirm that an insider was responsible for the leak of Anxun's data, it is the most likely option, based on our analysis.

Customers specifically concerned about insider threats should:

- Employ application controls (e.g., AppLocker) to restrict the execution of unsigned files.
- Implement role-based access control (RBAC) to protect sensitive data, reduce the risk of insider threats, and simplify compliance with regulations. It's important to continuously manage and update RBAC settings as your organization evolves and as employees move to new roles.
- Blocking suspicious web proxy categories, such as "Online Storage and Backup," is a critical step in preventing data exfiltration, as these services can be used to upload and store sensitive information outside the organization's control.
