Data From Chinese Security Services Company i-Soon Linked to Previous Chinese APT Campaigns

Executive Summary

On Feb. 16, 2024, someone uploaded data to GitHub that included possible internal company communications, sales-related materials and product manuals belonging to the Chinese IT security services company i-Soon, also known as Anxun Information Technology. The leaked materials appear to show how a commercial entity developed and supported cyber espionage tools in support of Chinese-affiliated threat actors. As part of initial investigation into the leaked data, Unit 42 discovered links between information in the data leak and previous Chinese-affiliated advanced persistent threat (APT) campaigns. Unit 42 assesses with high confidence that the leaks are genuine.

For example, documents in the leak appear to show i-Soon was marketing the Treadstone malware controller software, which was attributed to Elemental Taurus (aka APT41) in the 2019 U.S. grand jury indictment against three Chengdu 404 employees [PDF].

Through analysis of the leaked data, Unit 42 has identified actor-owned infrastructure and potential malware related to historic reporting on Chinese threat actors. Given the scope of the data leak, this report will cover initial analysis and significant findings, with further reporting likely to come at a future time. (While the original GitHub repo where the leak was posted has now been taken down by GitHub staff, citing a violation of terms of service, researchers will continue to study what was initially shared.)

Based on our current understanding of the data leak, customers can be better protected through Palo Alto Networks security products against the tools and techniques used by the Chinese threat actors mentioned in this article.

Related Unit 42 Topics	GitHub, China

Technical Analysis

Text on the GitHub repository claims that i-Soon has targeted the governments of India, Thailand, Vietnam and South Korea, as well as the intergovernmental organization NATO. We continue to analyze the leaked data to verify these claims.

The GitHub repository contains a mixture of online chat conversations, screenshots and probable victim data, as well as sales- and support-related documents. The text conversations dated between November 2018 and January 2023, and they involve 37 unique usernames.

The conversations range from general conversation and workplace issues to talking about targets, software vulnerabilities and customers.

Figure 1 graphs the text communications observed between the members of i-Soon, showing relationships between employees and the volume of messages between them. (Specific user names and given names have been redacted.)

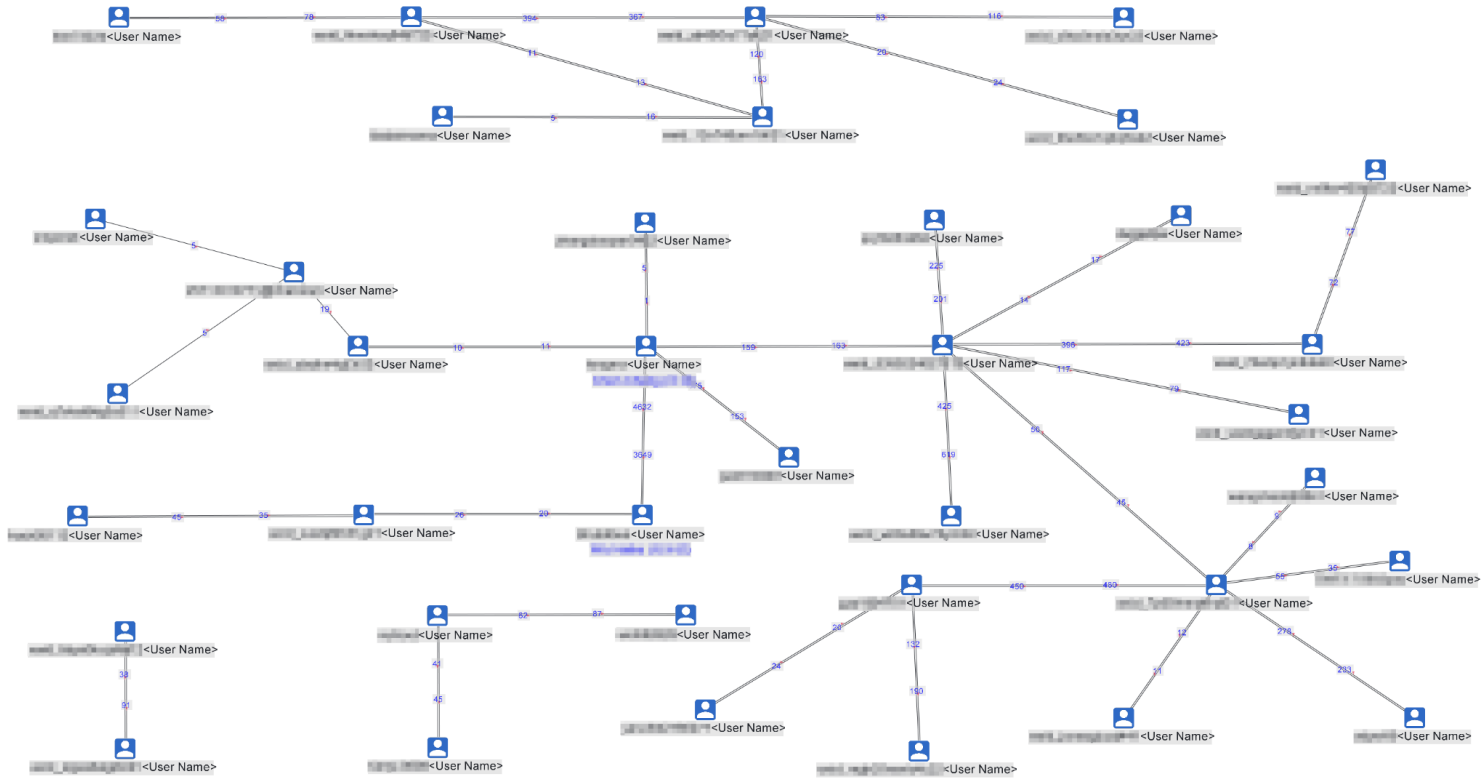

Figure 1. Visualization of i-Soon's leaked online chats (specific user names redacted).

Links to Previous Threat Intelligence Reporting

Unit 42 has found links in the leaked i-Soon text message conversations to two previously reported campaigns attributed to Chinese advanced persistent threat (APT) groups.

Campaign 1: 2022 Supply Chain Attack

In September 2022, Trend Micro reported about a supply chain attack on the Canadian software company Comm100. The attackers trojanized the installer for Comm100's chat-based customer engagement application hosted on their official website. When we looked through the i-Soon data leak, we found indications that i-Soon was involved in that attack.

Table 1 includes an excerpt taken from a conversation between two members of i-Soon where they claim IP address `8.218.67[.]52` is their server.

Date	From	To	Message	Translated
2022-06-13 7:39:19	wxid_c9xxxxxxxxx	wxid_zbxxxxxxxxxx	pc	[A person or organization from Yangzhou] wants to ask for or request access to a PC channel that belongs to a specific individual.
2022-06-13 7:39:21	wxid_c9xxxxxxxxx	wxid_zbxxxxxxxxxx	[]	[emoji suggesting embarrassment or sorry to bother you]
2022-06-13 7:39:23	wxid_c9xxxxxxxxx	wxid_zbxxxxxxxxxx		Can you give it now?

2022-06-13 7:40:26	wxid_zbxxxxxxxxx	wxid_c9xxxxxxxxxx	8.218.67[.]52:27011 TCP 8.218.67[.]52:17011 admin 88888888	Gambling or lottery site Proxy 8.218.67[.]52:27011 TCP Tunnel 8.218.67[.]52:17011 account admin password 88888888
2022-06-13 7:40:34	wxid_c9xxxxxxxxx	wxid_zbxxxxxxxxx		Uh-huh
2022-06-13 7:40:37	wxid_c9xxxxxxxxx	wxid_zbxxxxxxxxx		[Expletive]

2022-06-13 7:40:54	wxid_c9xxxxxxxxx	wxid_zbxxxxxxxxxx		This server is in Hong Kong
2022-06-13 7:41:06	wxid_zbxxxxxxxxx	wxid_c9xxxxxxxxxx		You don't need to worry about it
2022-06-13 7:41:07	wxid_c9xxxxxxxxx	wxid_zbxxxxxxxxxx	domain_access_result(1).csv	
2022-06-13 7:41:11	wxid_c9xxxxxxxxx	wxid_zbxxxxxxxxxx		Um
2022-06-13 7:41:14	wxid_zbxxxxxxxxx	wxid_c9xxxxxxxxxx		This server is ours

Table 1. Transcript of conversation between i-Soon members about IP address `8.218.67[.]52`.

On June 17, 2022, days after the above conversation occurred, the IP address `8.218.67[.]52` served a Linux ELF file with the SHA256 of `db4497090a94d0189aa3c3f4fcee30d5381453ec5aa38962e2ca971074b74e8b`. The file was served from the URL `hxxp[://]8.218.67[.]52/js/xxx.jpg`. When executed, the file attempts to contact the domain `unix.s3amazonbucket[.]com` (which is not a legitimate Amazon domain).

The Trend Micro report also mentioned that another subdomain of `s3amazonbucket[.]com` (`analyaze.s3amazonbucket[.]com`) was used as a command and control (C2) server for the trojanized installers.

Given the domain `s3amazonbucket[.]com` was likely under the control of i-Soon, Unit 42 assesses with moderate confidence that a group of hackers within i-Soon was involved in the supply chain attack on Comm100.

Campaign 2: 2019 Poison Carp Attack

In September 2019, Citizen Lab reported on attackers targeting Tibetan groups via multiple iOS and Android exploits. Citizen Lab attributed the attack to the Chinese threat group they track as POISON CARP. The report references domains that were tied to an IP address that we found references to in this data leak.

The IP address `74.120.172[.]10` was associated with the domain `mailteso[.]online` between Sept. 22, 2020, and Feb. 20, 2024, and `mailnotes[.]online` between Aug. 7, 2021, and July 12, 2022.

Table 2 outlines the conversation between i-Soon employees about IP address `74.120.172[.]10`.

Date	From	To	Message	Translated

2023-01-09 02:28:14	wxid_hlxxxxxxxx	wxid_12xxxxxxxx		Wait, there are some issues with the platform
2023-01-09 02:28:18	wxid_12xxxxxxxx	wxid_hlxxxxxxxx		OK
2023-01-09 02:36:19	wxid_hlxxxxxxxx	wxid_12xxxxxxxx	hxxps[://]74.120.172[.]10:10092/home	
2023-01-09 02:36:25	wxid_hlxxxxxxxx	wxid_12xxxxxxxx	access OrFRXV LZtestUser lzqzmp@123	
2023-01-09 02:43:51	wxid_12xxxxxxxx	wxid_hlxxxxxxxx		Send over a demo video

2023-01-09 02:44:06	wxid_12xxxxxxxx	wxid_hlxxxxxxxx		No need to give this information
2023-01-09 02:44:09	wxid_12xxxxxxxx	wxid_hlxxxxxxxx	[]	[Grinning emoji]
2023-01-09 02:44:20	wxid_hlxxxxxxxx	wxid_12xxxxxxxx		This is the trial version of the Microsoft [tool]
2023-01-09 02:44:33	wxid_12xxxxxxxx	wxid_hlxxxxxxxx		I saw it
2023-01-09 02:44:51	wxid_12xxxxxxxx	wxid_hlxxxxxxxx		Do you have a demo video [for Microsoft Windows tool]?

2023-01-09 02:44:58	wxid_hlxxxxxxxx	wxid_12xxxxxxxx		Let me ask
2023-01-09 02:48:54	wxid_hlxxxxxxxx	wxid_12xxxxxxxx	.7z	Microsoft Mail Secret Platform .7z
2023-01-09 02:52:01	wxid_12xxxxxxxx	wxid_hlxxxxxxxx		Is your video wrong?
2023-01-09 02:52:03	wxid_12xxxxxxxx	wxid_hlxxxxxxxx		I can not open it

2023-01-09 02:55:53	wxid_hlxxxxxxxx	wxid_12xxxxxxxx		Huh?
2023-01-09 02:55:56	wxid_hlxxxxxxxx	wxid_12xxxxxxxx		Just decompress it
2023-01-09 02:56:36	wxid_12xxxxxxxx	wxid_hlxxxxxxxx		I guess I didn't watch the video
2023-01-09 03:01:26	wxid_12xxxxxxxx	wxid_hlxxxxxxxx		Also the Android RAT
2023-01-09 03:02:07	wxid_hlxxxxxxxx	wxid_12xxxxxxxx		Wait, there’s some issues with the Android one

2023-01-09 03:02:26	wxid_12xxxxxxxx	wxid_hlxxxxxxxx		ok

Table 2. Transcript of conversation between i-Soon employees about IP address 74.120.172[.]10.

At the time of Citizen Lab publication, `mailnotes[.]online` was associated with IP address `207.246.101[.]169`, which was concurrently associated with the domain `gmail.isooncloud[.]com`.

Links to Known Chinese Intrusion Sets

The data leaks include manuals and whitepapers for various software tools. Of particular importance, these tools include software previously attributed to Chinese APT groups.

We do not currently know whether i-Soon were developers, resellers or even simply end users of these tools. However, the leaked documents help confirm previous reporting that multiple China-attributed threat actor groups often use the same, likely commercialized, malware tool sets.

One document contains a footer that translates to “Anxun Information Technology Co., Ltd.” and appears to be a product manual for a range of software tools sold by i-Soon. These tools include remote control management systems for Windows, Mac, iOS, Android and Linux.

The Linux remote control management software shown in Figure 2 is notable because the screenshot provided in the document to help explain the tool’s functionality shows the malware control panel is named “Treadstone.” The 2019 U.S. grand jury indictment of three Chengdu 404 employees directly references Treadstone.

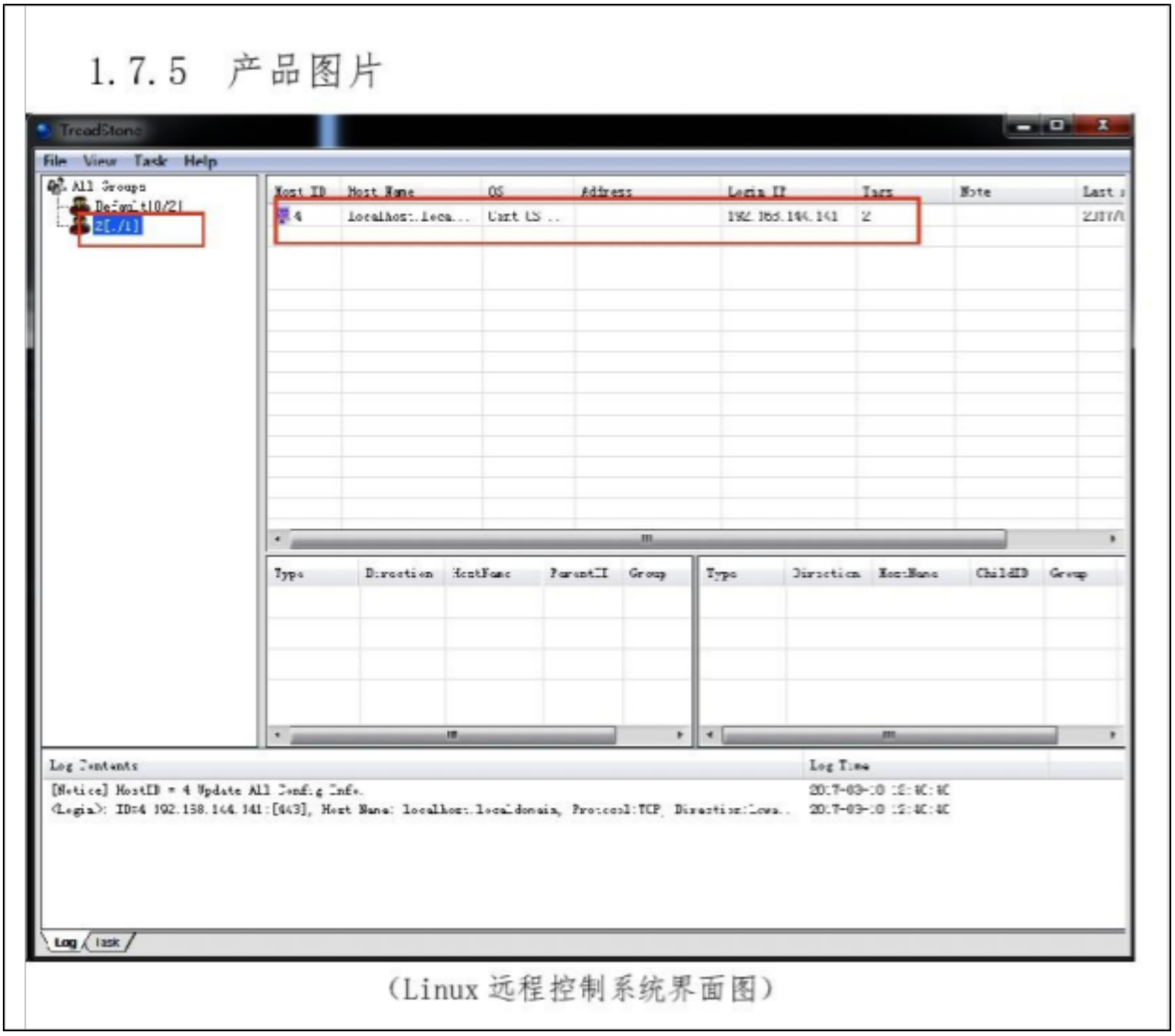

Figure 2. Screenshot of the Treadstone Linux malware control panel from a leaked product manual.

The indictment claims the Treadstone malware controller software “was designed to work with Winnti malware which, at the time, was used only by a small group of hackers.” Given reporting from October 2023 of Chengdu 404 taking i-Soon to court for a software development contract dispute, i-Soon might have developed the Treadstone panel.

Another document relating to known Chinese APT tools is a whitepaper for a Windows remote control management system. This document covers the system and network architecture and the product’s features. On one of the pages explaining management of the tool is a screenshot of what is likely the administrator panel, shown in Figure 3.

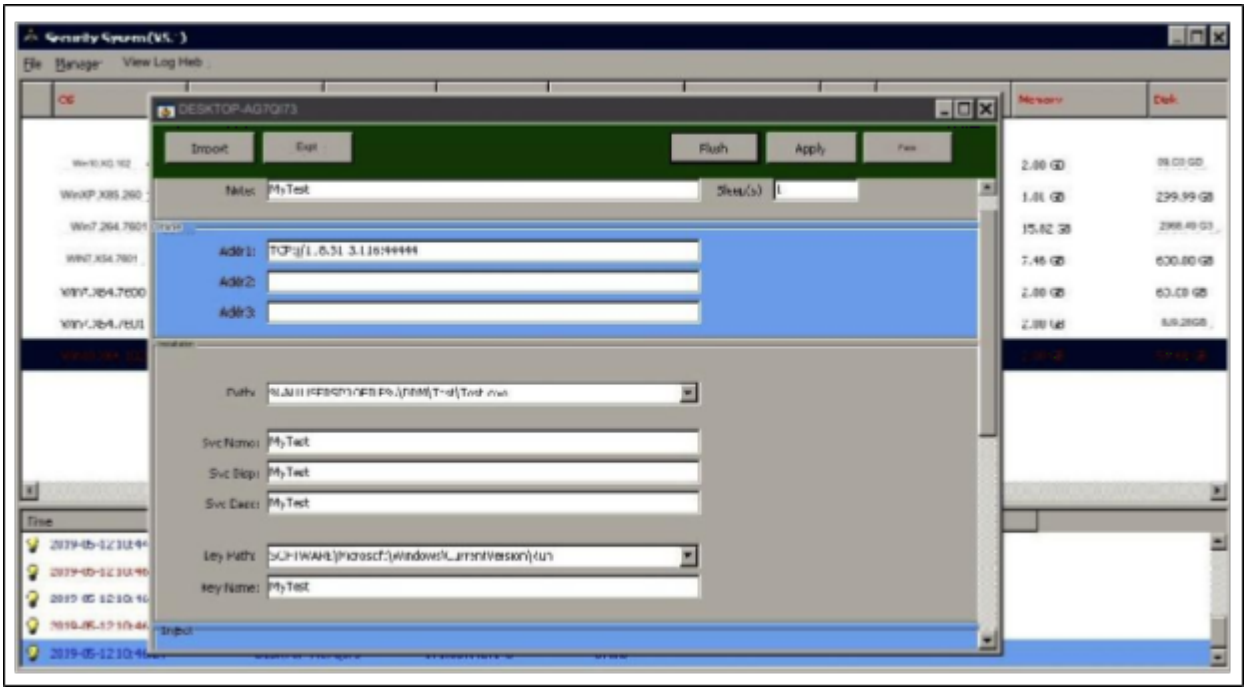

Figure 3. Administrator panel from Windows remote control management system related to known Chinese APT tool.

The screenshot shows the configured public IP address and port as `TCP[://]118.31.3[.]116:44444`. SentinelLabs reported this IP address was used as a ShadowPad C2 server in August 2021 and attributed to the Winnti group. This second link to the Winnti group adds further evidence that i-Soon was involved in the development of known Winnti tool sets.

Conclusion

This data leak provides unique insight into the Chinese private-sector hacking industry, which had previously only been seen through U.S. government indictments and reports. It also gives us a better understanding of the capabilities of Chinese threat actors, including how these groups are likely sharing or reselling the same tool sets. This dissemination of tools makes attribution more difficult for defenders and threat intelligence analysts.

Unit 42 will continue to analyze the leaked data, and we will update this post periodically, as we have more information to share.

Based on our understanding of the data leak, customers should be better protected through Palo Alto Networks security products against the tools and techniques used by the Chinese threat actors mentioned in this article. Malicious IPs related to the campaigns discussed have been blocked by Advanced URL Filtering.

If you think you might have been compromised or have an urgent matter, get in touch with the Unit 42 Incident Response team or call:

- North America Toll-Free: 866.486.4842 (866.4.UNIT42)
- EMEA: +31.20.299.3130
- APAC: +65.6983.8730
- Japan: +81.50.1790.0200

Palo Alto Networks has shared these findings with our fellow Cyber Threat Alliance (CTA) members. CTA members use this intelligence to rapidly deploy protections to their customers and to systematically disrupt malicious cyber actors. Learn more about the Cyber Threat Alliance.

Additional Resources

- Probing Weaponized Chat Applications Abused in Supply-Chain Attacks – Trend Micro
- Missing Link: Tibetan Groups Targeted with 1-Click Mobile Exploits – The Citizen Lab, Munk School of Global Affairs and Policy, University of Toronto
- ShadowPad | A Masterpiece of Privately Sold Malware in Chinese Espionage – SentinelLabs, SentinelOne

Updated Feb. 27, 2024, at 8:03 a.m. PT to switch the images for figures 2 and 3.