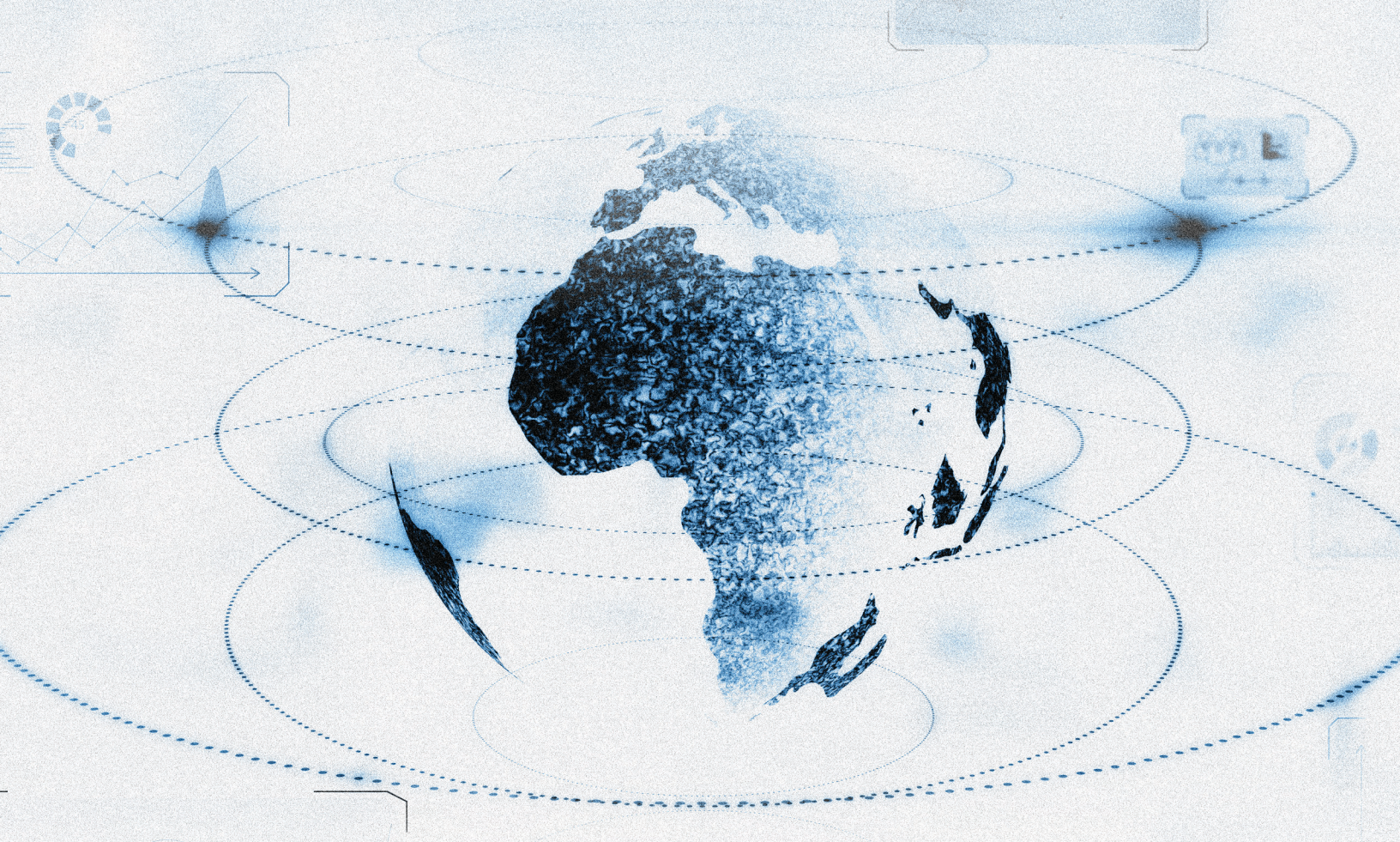
Recorded Future®

By Insikt Group®



Attributing i-SOON: Private Contractor Linked to Multiple Chinese State-sponsored Groups

Executive Summary

On February 18, 2024, an anonymous GitHub user posted a trove of leaked documents and material from Anxun Information Technology Co., Ltd. (安洵信息技术有限公司; also known as i-SOON), a China-based cybersecurity and information technology company that almost certainly conducts offensive cyber-espionage operations for Chinese government clients. The leak offers an unprecedented glimpse inside the inner workings of China's cyber-espionage ecosystem and represents the most significant leak of data linked to a company suspected of providing targeted intrusion services for Chinese security services.

By correlating historical tracking of Chinese state-sponsored threat activity groups and the leaked material, Insikt Group identified strong infrastructure, tooling, victimology, and personnel overlap between i-SOON and multiple tracked Chinese state-sponsored threat activity groups that likely operate as subgroups under i-SOON: RedAlpha[1], RedHotel[2], and POISON CARP. The leaked material corroborates our previous assessment that RedHotel is one of the most prominent, active, Chinese state-sponsored threat activity groups based on the group's consistently high operational tempo and global targeting remit. The leak also further supports hypotheses that Chinese state-sponsored groups are supported by "digital quartermasters" that enable the sharing of custom capabilities under commercial arrangements.

In addition to gaining an understanding of the inner workings of cyber-espionage operations, network defenders can apply victimology intelligence gained from the leak to improve internal threat models. This information, often obscured from public view, can allow for a more thorough understanding as to why specific commercial, communication, or other data may be targeted and how it can be used for intelligence purposes. One such example of this from the i-SOON leak is the apparent exfiltration of call data records (CDR) and other material from multiple telecommunications companies, likely to enable tracking of individuals' locations and communications within specific countries.

Despite i-SOON's global impact and extensive targeting, it is a relatively small company operating alongside numerous other similar entities within China's complex private contractor landscape, again underscoring the broad scope and scale of Chinese state-sponsored cyber operations. In the aftermath of substantial media attention following the leak, we anticipate i-SOON-linked threat activity groups will attempt to continue operations unabated beyond tactical operational security adjustments. We have already observed signs of renewed infrastructure developments attributed to RedAlpha and RedHotel. Future tracking of the company's targeting may provide insight as to whether they will continue to be favored for use by Chinese security services against specific targets or if they will be relegated to lower-priority tasking in the aftermath of the leak. In addition to potential internal changes, the leak is

[1] RedAlpha activity overlaps with public reporting under the aliases Deepcliff and Red Dev 3.
[2] RedHotel activity overlaps with public reporting under the aliases Aquatic Panda, Bronze University, Charcoal Typhoon, Earth Lusca, Fishmonger, and Red Scylla.

also likely to assist US law enforcement in providing supporting evidence for potential future indictments of i-SOON personnel.

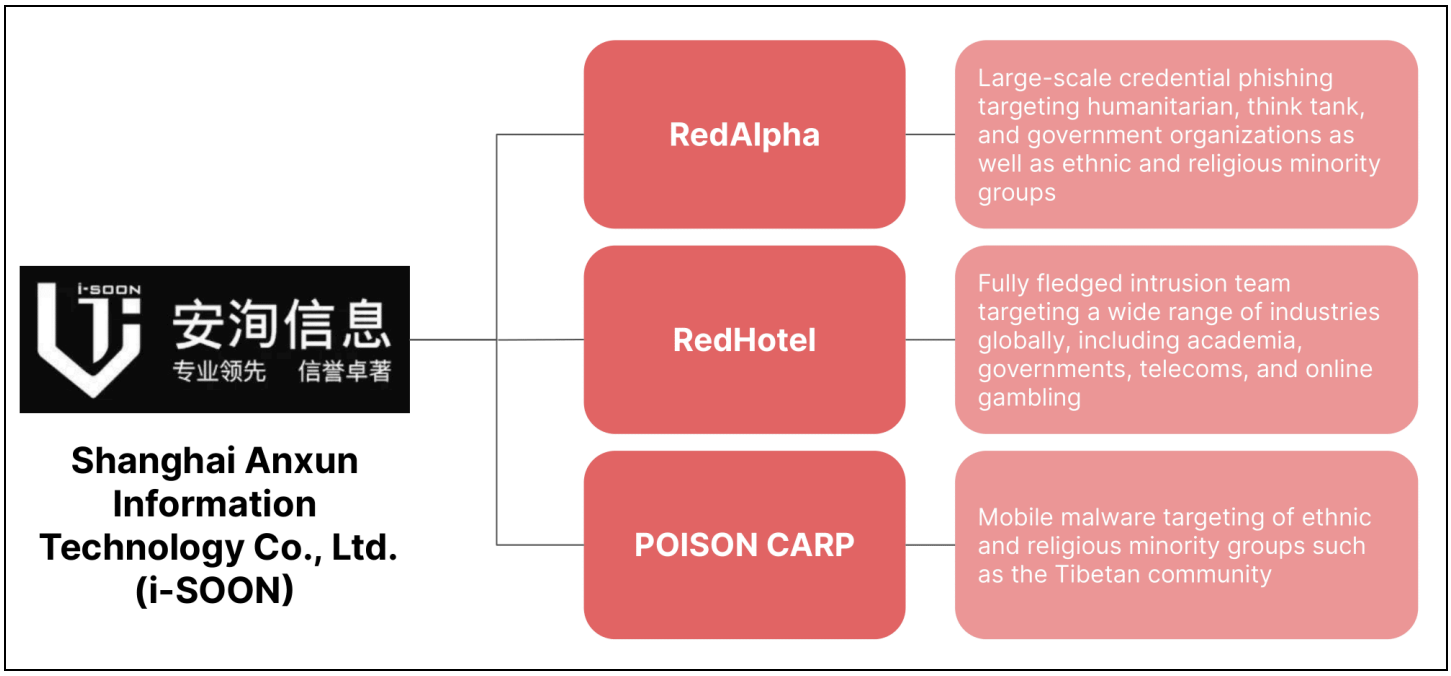


Figure 1: *Chinese threat activity groups linked to i-SOON (Source: Recorded Future)*

Key Findings

- Lax operational security and leaked material link i-SOON corporate infrastructure and personnel to offensive cyber-espionage operations attributed to RedHotel, RedAlpha, and POISON CARP.
- While these threat activity groups have been considered operationally distinct based on significantly differing tactics, techniques, and procedures (TTPs), the identified links to i-SOON indicate that they are likely sub-teams focused on specific missions within the same company.
- Based on victim data, i-SOON's victims span at least 22 countries, with government, telecommunications, and education representing the most targeted sectors.
- i-SOON also supports domestic security priorities, including the targeting of ethnic and religious minorities (such as the Tibetan community) and the online gambling industry catering to the Chinese market.
- i-SOON very likely uses and sells access to custom malware families such as ShadowPad and Winnti. This corroborates long-held hypotheses regarding China's offensive cyber activity, where privately held malware families and exploits are often observed in use by multiple distinct threat activity groups under commercial arrangements or via the vulnerability research ecosystem.

Background

On February 18, 2024, an anonymous GitHub user posted a trove of leaked company documents and material related to i-SOON. The leak — which is no longer available via GitHub — includes over 500 files of promotional material, product and service "white papers", spreadsheets of contracts and targets, and employee chat logs that reveal the company's clients, potential victims, and claimed capabilities. Interviews by the Associated Press (AP) with two i-SOON employees have corroborated that the leak is almost certainly genuine.

As summarized within public reporting, i-SOON advertises a range of offensive, defensive, and training capabilities and platforms. The company offers capabilities designed to allow remote access to all major operating systems and mobile devices, as well as capabilities to monitor major social media sites and to analyze and query exfiltrated victim data.

i-SOON's clients range across three systems in China:

- The public security system, which generally refers to police forces under the Ministry of Public Security (MPS)
- The state security system, which generally refers to intelligence forces under the Ministry of State Security (MSS)
- The military system, primarily meaning the People's Liberation Army (PLA)

i-SOON's activities on behalf of public security clients included targeting foreign government and telecommunications organizations that analysts may have previously assumed were more likely to be associated with state security priorities, highlighting overlapping areas of responsibility between public and state security organizations, and broad use of offensive cyber operations across both systems.

Countries in which government and corporate entities have almost certainly been targeted by i-SOON include India, Pakistan, Kazakhstan, Kyrgyzstan, Thailand, Malaysia, Mongolia, Myanmar, Nepal, Rwanda, Vietnam, Indonesia, Cambodia, Nigeria, Egypt, South Korea, Türkiye, and others, as well as entities in Hong Kong and Taiwan.

We also note more ambiguous references to organizations within the leak, where it is unclear as to whether these organizations were victims, targets, or otherwise. Countries in which entities may have been targeted include the United Kingdom (UK) and the United States (US), as well as organizations such as the North Atlantic Treaty Organization (NATO).

Specific Tools Identified in i-SOON Leak Offer Attribution Clues

i-SOON Very Likely Uses and Distributes the Custom ShadowPad Backdoor

Malware controller and builder screenshots of a Windows malware family documented within a "user manual" indicate that i-SOON is very likely selling access to the custom modular backdoor ShadowPad. ShadowPad has been privately distributed across Chinese state-sponsored groups since at least 2015, with Insikt Group tracking over thirteen distinct Chinese groups using the custom backdoor. The link between the leaked i-SOON material and ShadowPad is based on the following evidence:

- A builder screenshot shown in **Figure 2** and **Figure 3** directly aligns with known ShadowPad configurations seen in the wild, specifically the use of `MyTest` and the install path `%ALLUSERPROFILE%\DRM\Test\Test.exe` (1, 2). More specifically, this configuration appears to align with the bespoke ShadowPad packer ScatterBee (also known as ShadowShredder and PoppingBee). This evidence, alongside identified links between i-SOON and the primary ScatterBee user RedHotel, indicates that i-SOON is likely an original developer of ScatterBee.
- Furthermore, one of the builder screenshots shown in **Figure 2** features the IP address *118.31.3[.]116*. This is a known ShadowPad C2 that was likely active in May 2019 based on the presence of unique HTTP headers associated with ShadowPad usage. This time frame aligns with additional timestamps visible within the product screenshots contained within the leaked material.

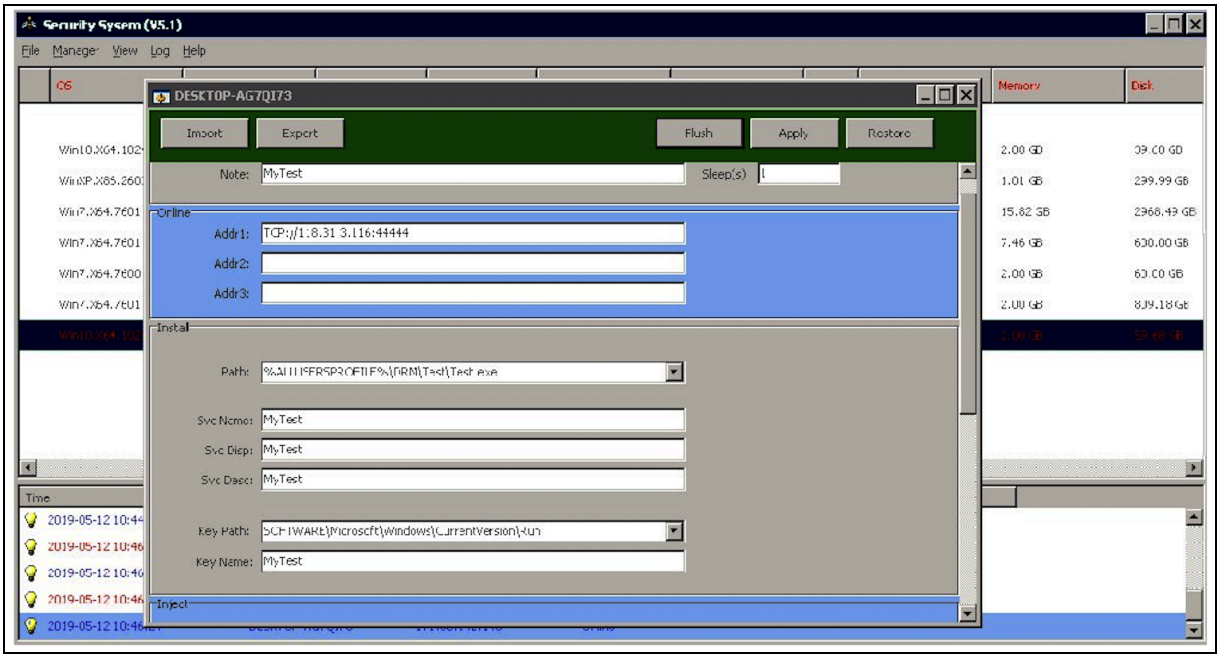


Figure 2: *Suspected ShadowPad configuration (Source: i-SOON leak)*

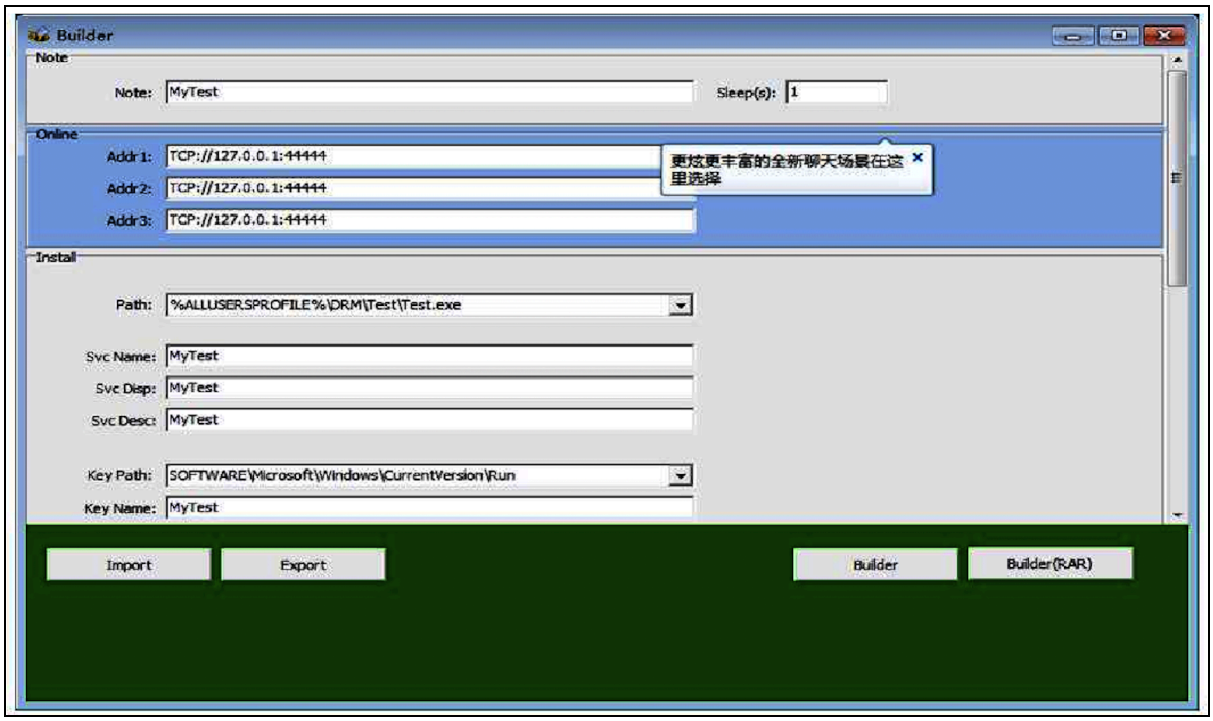
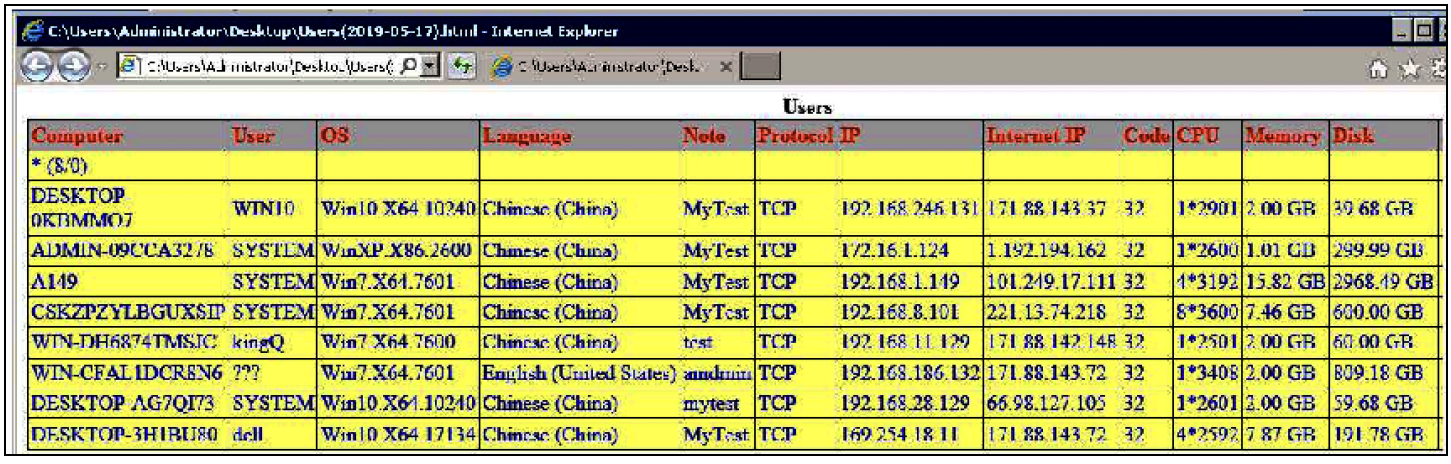


Figure 3: *Suspected ShadowPad builder (Source: i-SOON leak)*

An additional notable finding is the inclusion of a ShadowPad controller data export displaying a summary of multiple suspected test infections (**Figure 4**). One of the included IP addresses is the CHINANET Chengdu, Sichuan province network IP address *171.88.143[.]72*, which has historically hosted the dynamic DNS domain *lengmo.myds[.]me*. Based on the leaked material and additional corroborative evidence, "lengmo" is the handle of the Chengdu-based i-SOON co-founder Chen Cheng (陈诚).



Users

Computer	User	OS	Language	Note	Protocol	IP	Internet IP	Code	CPU	Memory	Disk
* (8/0)											
DESKTOP 0KBMMO7	WIN10	Win10 X64 10240	Chinese (China)	MyTest	TCP	192.168.246.131	171.88.143.37	32	1*2901	2.00 GB	39.68 GB
ADMIN-09CCA32J8	SYSTEM	WinXP X86 2600	Chinese (China)	MyTest	TCP	172.16.1.124	1.192.194.162	32	1*2600	1.01 GB	299.99 GB
A149	SYSTEM	Win7 X64 7601	Chinese (China)	MyTest	TCP	192.168.1.149	101.249.17.111	32	4*3192	15.82 GB	2968.49 GB
CSKZPZYLBGUXSIP	SYSTEM	Win7 X64 7601	Chinese (China)	MyTest	TCP	192.168.8.101	221.13.74.218	32	8*3600	7.46 GB	600.00 GB
WIN-DH6874TMSJC	kingQ	Win7 X64 7600	Chinese (China)	test	TCP	192.168.11.129	171.88.142.148	32	1*2501	2.00 GB	60.00 GB
WIN-CFALIDCREN6	???	Win7 X64 7601	English (United States)	andmin	TCP	192.168.186.132	171.88.143.72	32	1*3408	2.00 GB	809.18 GB
DESKTOP AG7QI73	SYSTEM	Win10 X64 10240	Chinese (China)	mytest	TCP	192.168.28.129	66.98.127.105	32	1*2601	2.00 GB	59.68 GB
DESKTOP-3H1BU80	dell	Win10 X64 17134	Chinese (China)	MyTest	TCP	169.254.18.11	171.88.143.72	32	4*2592	7.87 GB	191.78 GB

Figure 4: *Suspected test ShadowPad infection report (Source: i-SOON leak)*

i-SOON Very Likely Uses and Distributes Winnti Linux Variant

In addition to ShadowPad, the leaked material contains references to what is almost certainly the Linux variant of the custom Winnti backdoor, which is again sold as a commercial offering to i-SOON clients. The visible use of the internal name "TreadStone" (**Figure 5**) for the malware controller directly aligns with material referenced in US Department of Justice indictments against the Chinese information technology company Chengdu 404 Network Technology ("Chengdu 404"), specifically related to the custom malware family Winnti (**Figure 6**). Similar to ShadowPad, Winnti has been privately shared across a range of Chinese state-sponsored threat activity groups since early 2013. Incidentally, Chengdu 404, a private contractor attributed to the Chinese state-sponsored threat activity group RedGolf (APT41, Brass Typhoon, Wicked Panda), has been engaged in a legal case with i-SOON centered on a software development contract dispute. As referenced within public reporting, the leaked material also details a business relationship between these two organizations.

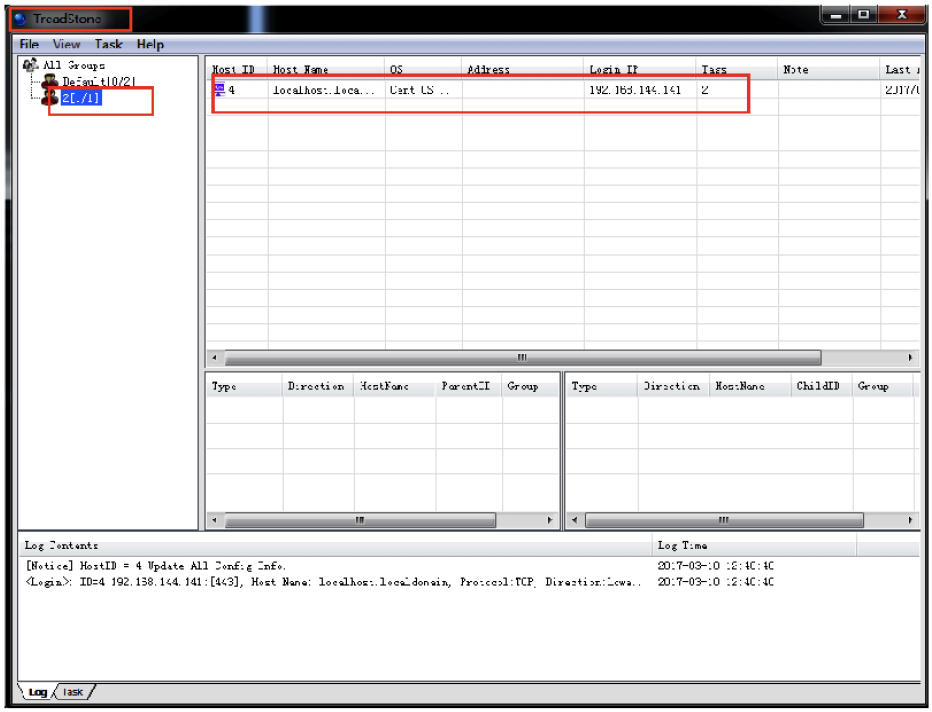
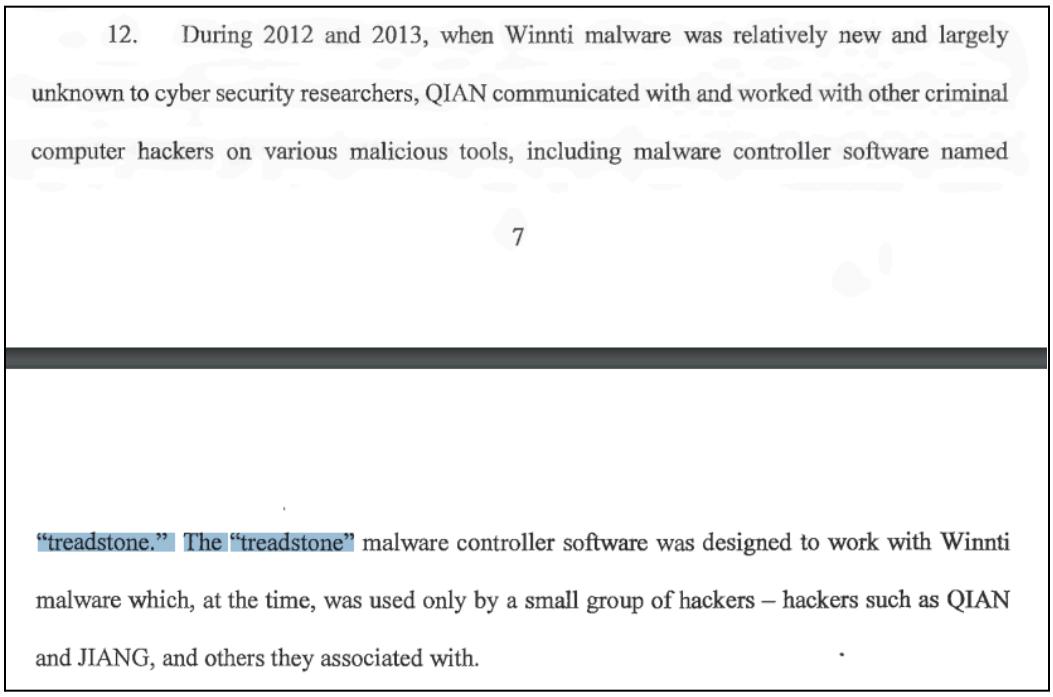


Figure 5: *TreadStone/Winnti malware controller screenshot (Source: i-SOON leak)*



12. During 2012 and 2013, when Winnti malware was relatively new and largely unknown to cyber security researchers, QIAN communicated with and worked with other criminal computer hackers on various malicious tools, including malware controller software named

7

"treadstone." 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 – hackers such as QIAN and JIANG, and others they associated with.

Figure 6: *Reference to TreadStone/Winnti in Chengdu 404 DoJ indictments (Source: US Department of Justice)*

Additional Unknown Linux Malware Family "Hector"

A third malware family specifically referenced in an i-SOON instruction manual uses the internal name "Hector". Based on the leaked documents, Hector is a modular Linux backdoor that uses the WebSocket over TLS protocol (WSS) for C2 communications. The product manual references additional modules/plug-ins with the following names:

- `libCmdMgr.so`
- `libFileManagerRemote.so`
- `libFileTransferRemote.so`

The use of WSS for C2 communications is reminiscent of another modular custom malware family, KEYPLUG, which has a Linux variant and is shared across multiple Chinese state-sponsored groups. However, there is insufficient evidence to link Hector to a known malware family at this time.

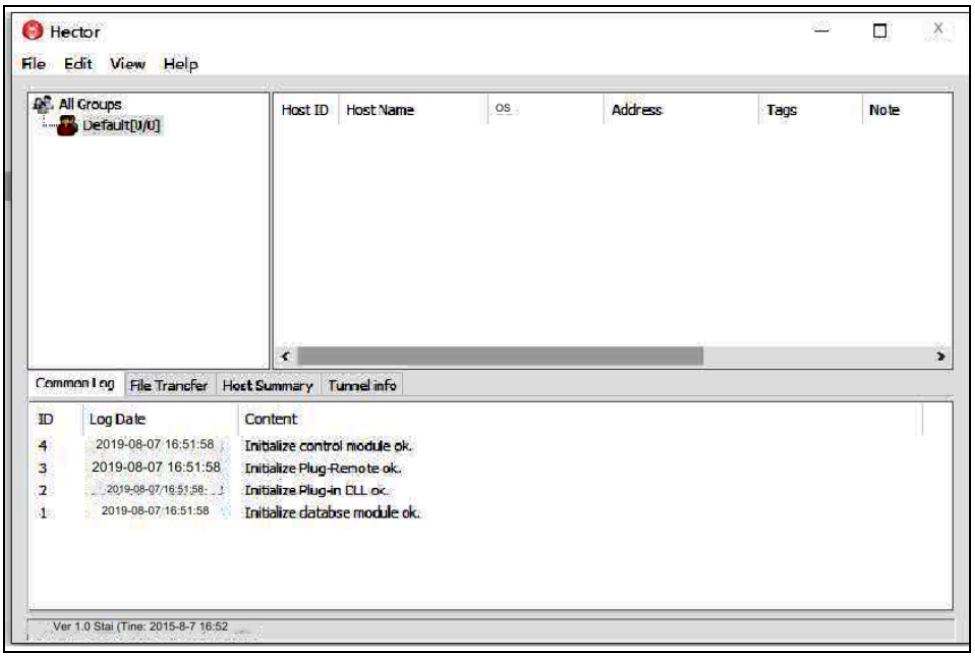


Figure 7: *"Hector" Linux malware controller (Source: i-SOON leak)*

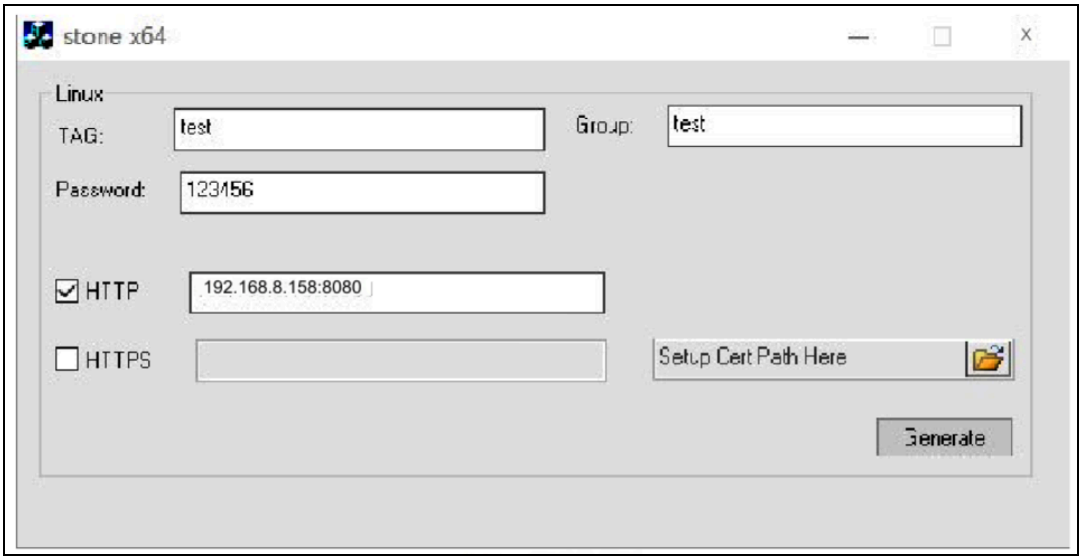


Figure 8: *"Hector" Linux malware builder named stone x64 (Source: i-SOON leak)*

The POISON CARP Connection — Mobile Device Targeting Subgroup

Public reporting identified clear infrastructure overlaps between i-SOON and activity attributed to POISON CARP, a suspected Chinese state-sponsored threat activity group that has been observed targeting mobile devices within the Tibetan community[3]. Insikt Group has corroborated these links and identified additional overlaps between POISON CARP-linked infrastructure and i-SOON.

The IT7NET IP address *74.120.172[.]10* is directly referenced in leaked i-SOON employee chat logs (see **Figure 10**). This *74.120.172[.]10* IP address has historically hosted the domain *mailnotes[.]online*, which is listed in POISON CARP reporting by the Citizen Lab. This IP address currently continues to host the similarly named *mailteso[.]online*. These employees also reference an Android remote access trojan (RAT), which is consistent with POISON CARP mobile device targeting.

In 2019, *mailnotes[.]online* resolved to the Vultr IP address *207.246.101[.]169* concurrently with a subdomain of *gmailapp[.]me*, another domain referenced in the Citizen Lab report. This *207.246.101[.]169* IP address concurrently hosted the subdomain *gmail.isooncloud[.]com*. Along with directly referencing i-SOON, WHOIS data for this domain indicates it is registered by an individual named Zheng Huadong (郑华东). Material from the i-SOON leak repeatedly references an i-SOON senior executive named Zheng Huadong in chat logs and within a company roster. The subdomain *gmail.isooncloud[.]com* also has a further historical hosting overlap with *www.gmailapp[.]me* on *107.150.102[.]143* dating back to 2018.

[3] While POISON CARP is often equated to the EvilEye/Earth Empusa cluster, industry reporting notes that these are likely distinct groups with access to the same vendor-developed tooling.

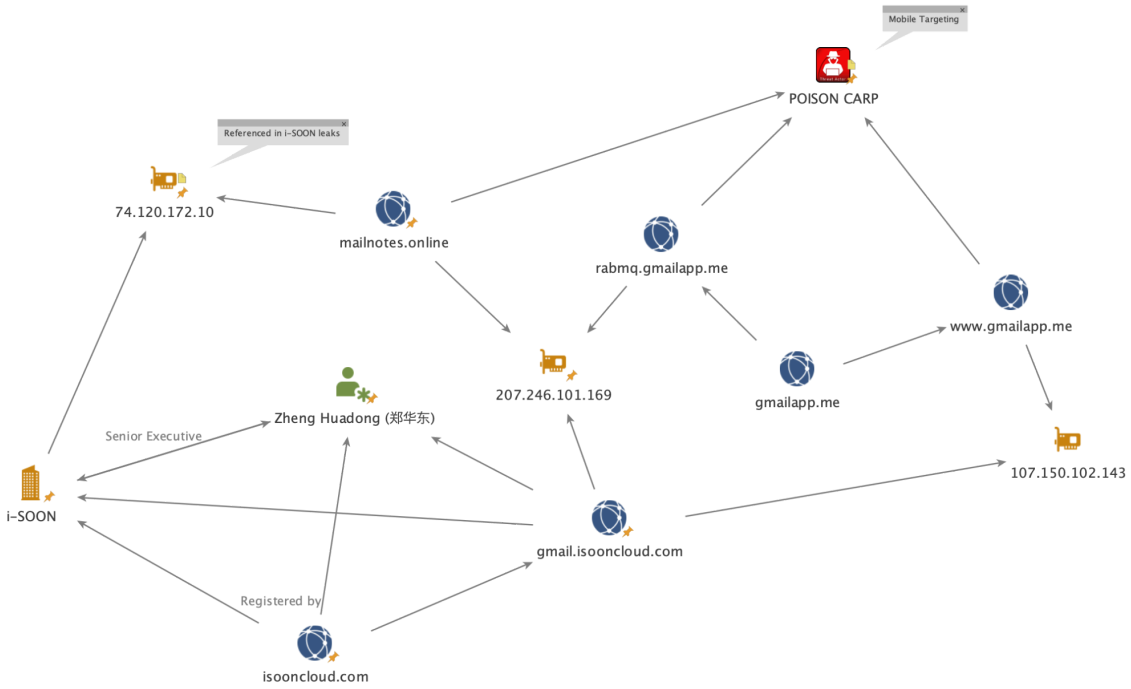


Figure 9: *Links between i-SOON and the "POISON CARP" threat activity group (Source: Recorded Future)*

Date	*Message*	*Translated*
2023-01-09 02:28:14	*等一下 平台有点问题*	*Wait, there are some issues with the platform*
2023-01-09 02:28:18	*好的*	*OK*
2023-01-09 02:36:19		*hxxps[://]74.120.172[.]10:10092/home*
2023-01-09 02:36:25		*access OrFRXV LZtestUser lzqzmp@123*
2023-01-09 02:43:51	*演示视屏发一个*	*Send over a demo video*
2023-01-09 02:44:06	*这个资料都不用给了*	*No need to give this information*
2023-01-09 02:44:09	*[呲牙]*	*[Grinning emoji]*
2023-01-09 02:44:20	*这是微软的试用版*	*This is the trial version of the Microsoft [tool]*
2023-01-09 02:44:33	*恩，我看到了*	*I saw it*
2023-01-09 02:44:51	*微软的演示视频有吗*	*Do you have a demo video [for Microsoft Windows tool]?*
2023-01-09 02:44:58	*我问下*	*Let me ask*
2023-01-09 02:52:01	*是不是你们视频错了啊*	*Is your video wrong?*
2023-01-09 02:52:03	*我打不开*	*I can not open it*
2023-01-09 02:55:53	*嗯？*	*Huh?*
2023-01-09 02:55:56	*解压就行了呀*	*Just decompress it*
2023-01-09 02:56:36	*估计是我没看视屏的*	*I guess I didn't watch the video*
2023-01-09 03:01:26	*还有安卓的远控*	*Also the Android RAT*
2023-01-09 03:02:07	*安卓稍等一下 有点问题*	*Wait, there's some issues with the Android one*
2023-01-09 03:02:26	*好*	*ok*

Figure 10: *Links between i-SOON and the "POISON CARP" threat activity group based on chat logs between "wxid_hlmnhsq64tt722" and "wxid_12n748um1thl21" (Source: i-SOON Leak)*

The RedAlpha Connection — Large-Scale Credential Phishing Subgroup

Insikt Group has also identified multiple overlaps between i-SOON and a prolific credential phishing threat activity group we track under the alias RedAlpha (Deepcliff, Red Dev 3). We have historically reported on RedAlpha activity conducting credential phishing activity targeting humanitarian, think tank, and government organizations globally, as well as specific ethnic and religious minority groups such as the Tibetan and Uyghur communities (1, 2). This targeting aligns with material within the i-SOON leak and the documented intelligence requirements of i-SOON's local and regional customers within China's public security and state security apparatus. Elements of the highlighted RedAlpha and RedHotel connections were also noted in a 2023 PWC presentation at the LABScon conference.

RedAlpha's Infrastructure Connection to i-SOON

Insikt Group identified an overlap between i-SOON-linked infrastructure and RedAlpha credential phishing infrastructure. Specifically, continuing on from findings noted in the POISON CARP section above, the previously referenced i-SOON-linked domain *gmail.isooncloud[.]com* resolved to the dedicated UCLOUD INFORMATION TECHNOLOGY HK LIMITED IP address *107.150.102[.]143* in 2018. This IP address concurrently hosted two additional domains, *www.sw-hk[.]services* and *antspam-mail[.]services*. These two domains in turn directly correlate with a large number of RedAlpha credential phishing domains via concurrent hosting overlaps on the dedicated RedAlpha INVESTCLOUD IP address *23.249.165[.]150* in 2018 (see **Figure 11**).

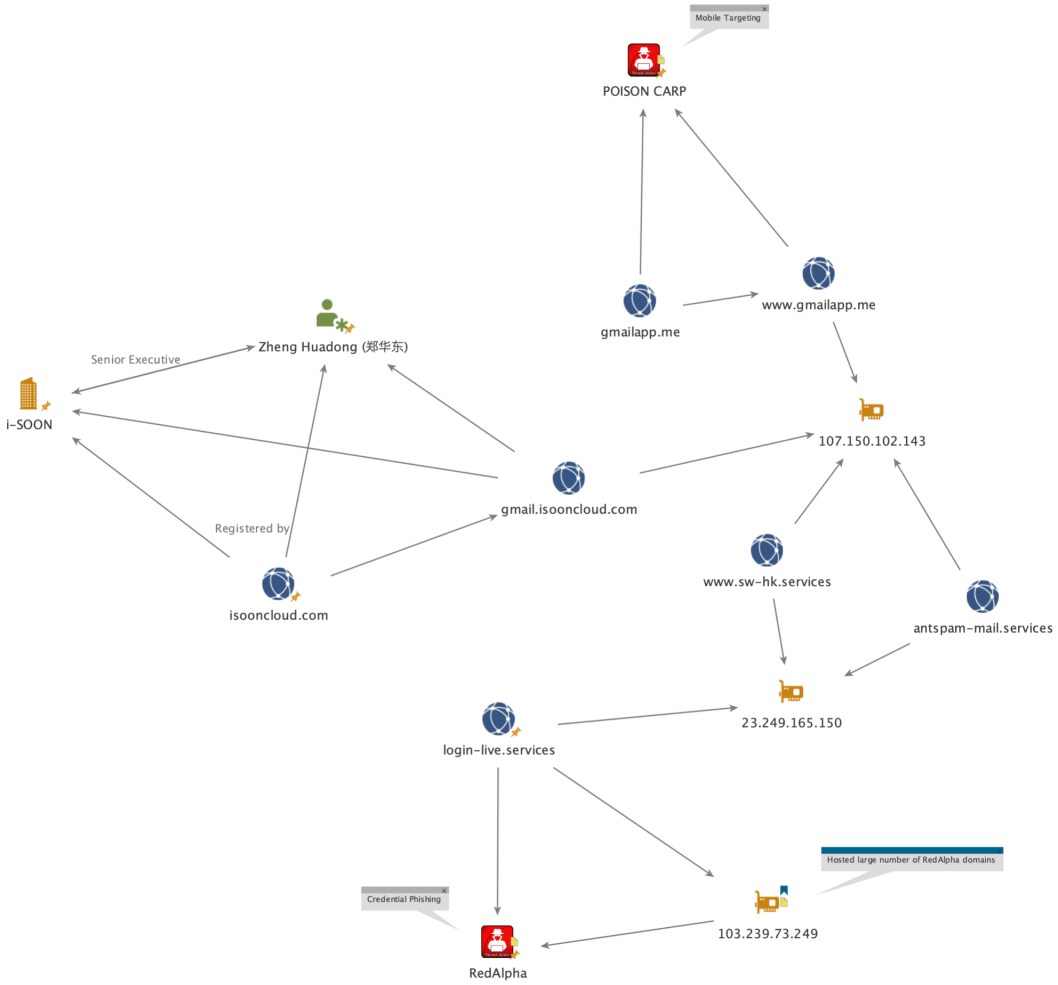


Figure 11: *Infrastructure links noted in 2018 between i-SOON and the RedAlpha threat activity group (Source: Recorded Future)*

RedAlpha's Personnel Connection to i-SOON

Insikt Group also identified multiple overlaps between i-SOON and a previously identified RedAlpha-linked persona, "Liang Guodong" (梁国栋, also known under the monikers "girder" and "liner"), whom we previously referenced in 2022 reporting. These overlaps are summarized as follows:

- A 2011 iteration of the i-SOON corporate website *i-soon[.]net* linked to just two external websites, both of which were personal blogs: *lengmo[.]net* and *linercn[.]org*. The *lengmo[.]net* domain was registered and operated by i-SOON co-founder Chen Cheng (陈诚), aka lengmo.
- Insikt Group previously tied *linercn[.]org* to the Liang Guodong persona within customer-facing reporting based on matching WHOIS registrant information and historical archives of the site, which lists a specific personal QQ account as a contact point: *6060841@qq[.]com*. This QQ account has numerous links to the Liang Guodong persona and was historically used to register multiple RedAlpha credential phishing domains (1, 2). A summary of the connections between

the Liang Guodong persona's email addresses and personal blog sites and RedAlpha infrastructure is shown in **Figure 13**.

- According to sources held by Recorded Future, prior to March 2022, an individual called Liang Guodong was a partner and investor in a company called Chengdu Xingcan Information Technology Cooperative Enterprise (Limited Partnership) 成都星璨信息技术合伙企业. This company was founded by i-SOON CEO Wu Haibo, is located at the same address as the i-SOON's Chengdu office, and was listed alongside a contact email address of *tao_tingting@i-soon[.]net*, an email address belonging to i-SOON's finance manager Tao Tingting (陶婷婷).
- Sources held by Recorded Future also indicate that Chengdu Xingcan holds a 6.45% stake in Anxun Information Technology Co., Ltd. (i-SOON), with some sources stating they are part of the same "group" (集团/族群).
- Notably, both the Liang Guodong persona and the founder of i-SOON (Wu Haibo, aka "Shutd0wn") are self-proclaimed ex-members of the prominent Chinese underground hacking group Green Corps (绿色兵团) (1, 2).

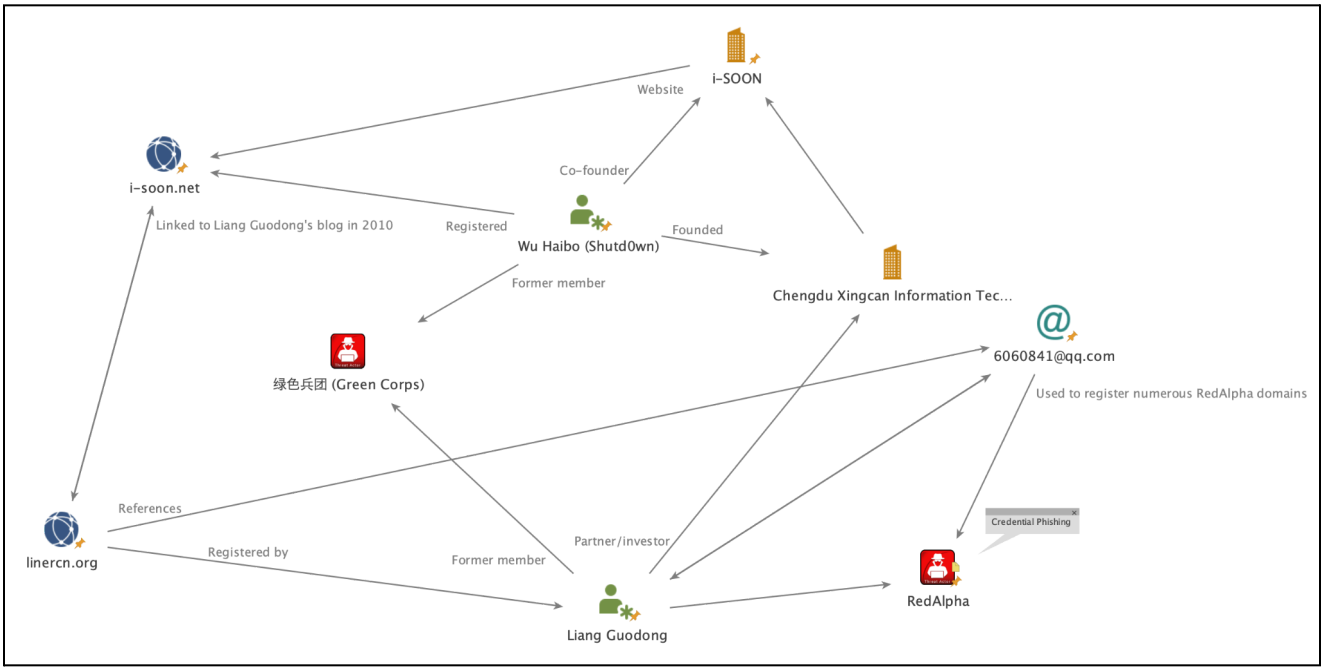


Figure 12: *Personnel links between i-SOON and the RedAlpha threat activity group (Source: Recorded Future)*

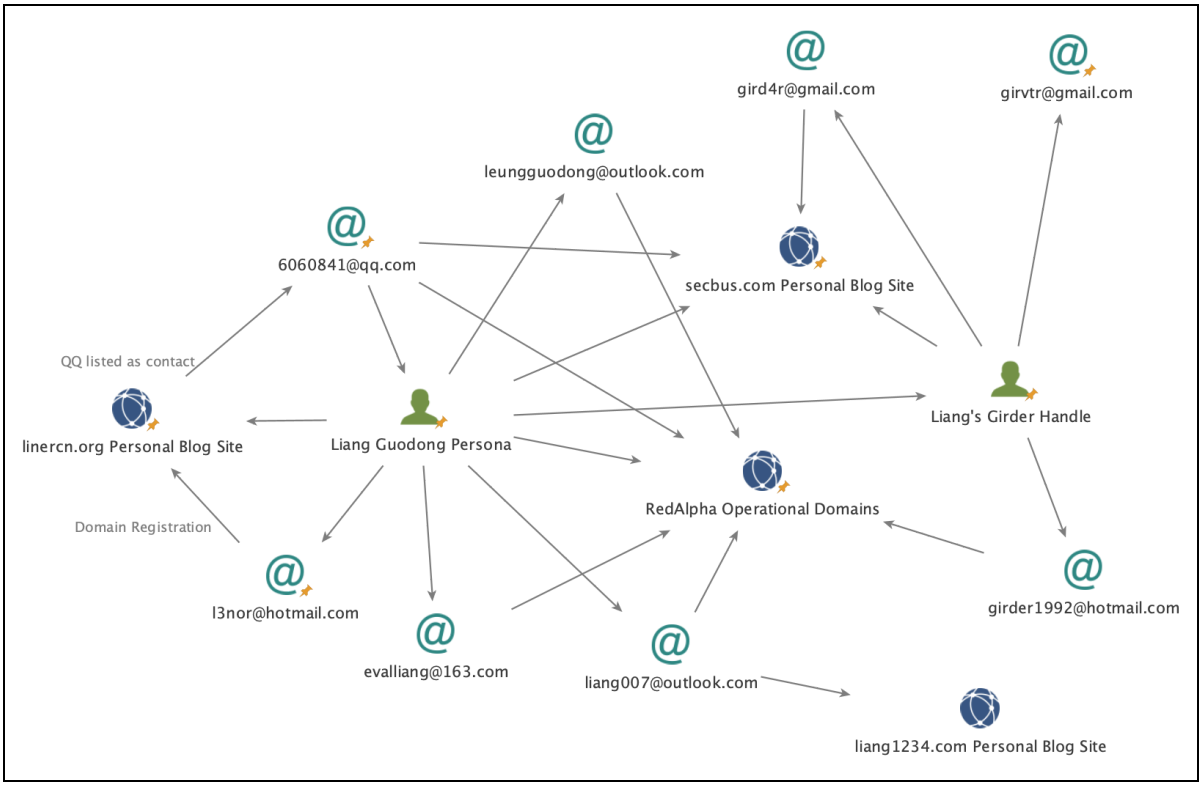


Figure 13: *Links between Liang Guodong and RedAlpha (Source: Recorded Future)*

The RedHotel Connection — Fully Fledged Network Intrusion Subgroup

Finally, Insikt Group identified tooling, infrastructure, location, and victimology overlap with the Chinese state-sponsored threat activity group we track as RedHotel (Aquatic Panda, Bronze University, CHROMIUM, Charcoal Typhoon, ControlX, Earth Lusca, Fishmonger, Red Dev 10, Red Scylla, TAG-22). The connection between RedHotel and i-SOON has also been noted by multiple other organizations (1, 2, 3).

i-SOON and RedHotel Are Both Based in Chengdu

Insikt Group has previously assessed that RedHotel likely operates out of Chengdu, Sichuan province. This aligns with the operation location of i-SOON's "penetration" team, per material within the i-SOON leak. The leaked material also reveals that 122 of i-SOON's 159 employees are based in Chengdu, incorporating all of the company's technical personnel.

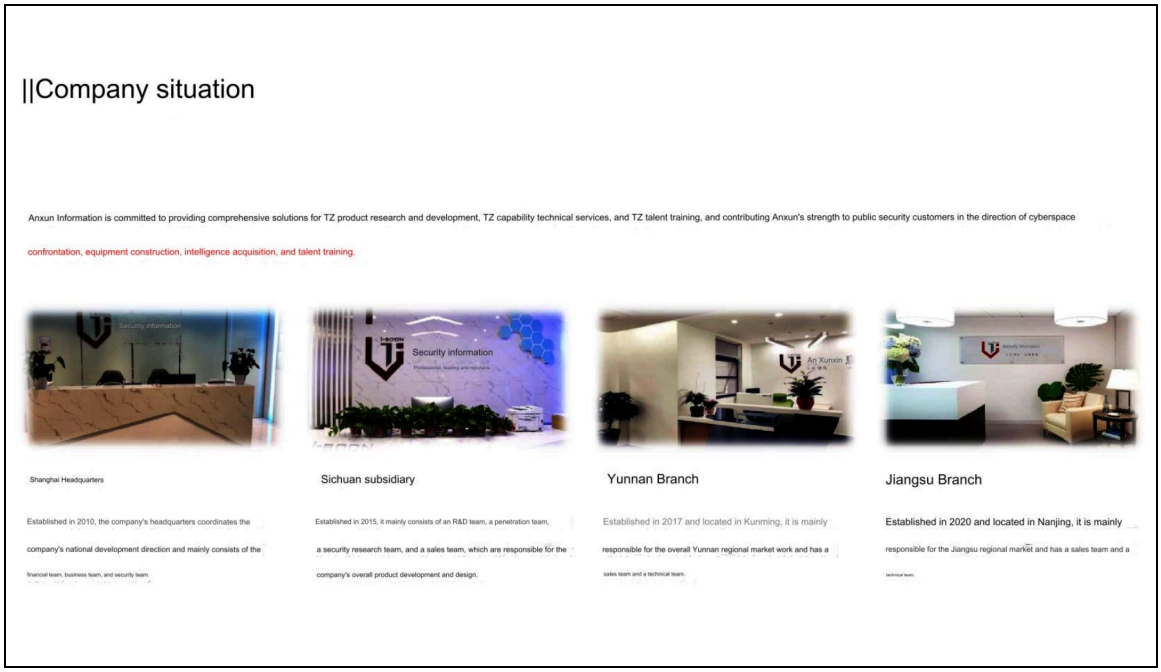


Figure 14: *i-SOON operating locations (Source: optical character recognition [OCR] machine-translated from i-SOON leak)*

i-SOON and RedHotel Infrastructure Overlaps

Similar to POISON CARP and RedAlpha, we observed an infrastructure correlation between known RedHotel infrastructure and i-SOON. Building on the Liang Guodong connection highlighted earlier in this report, Insikt Group observed that three domains registered by one of Liang's previously identified

email addresses, *girder1992@hotmail[.]com*, resolved to the IPTELECOM ASIA IP address *43.239.156[.]63* throughout 2017 and 2018. This IP address also concurrently hosted one additional domain, *news.1ds[.]me*. Notably, other subdomains of *1ds[.]me* have direct links to RedHotel activity:

- The subdomain *docx.1ds[.]me* has concurrent hosting overlaps on dedicated infrastructure with multiple previously identified RedHotel domains such as *web.goog1eweb[.]com*, as shown in **Figure 15**.
- The subdomain *ip.1ds[.]me* was a C2 domain for multiple identified Winnti (Linux) samples shown in **Table 1**.

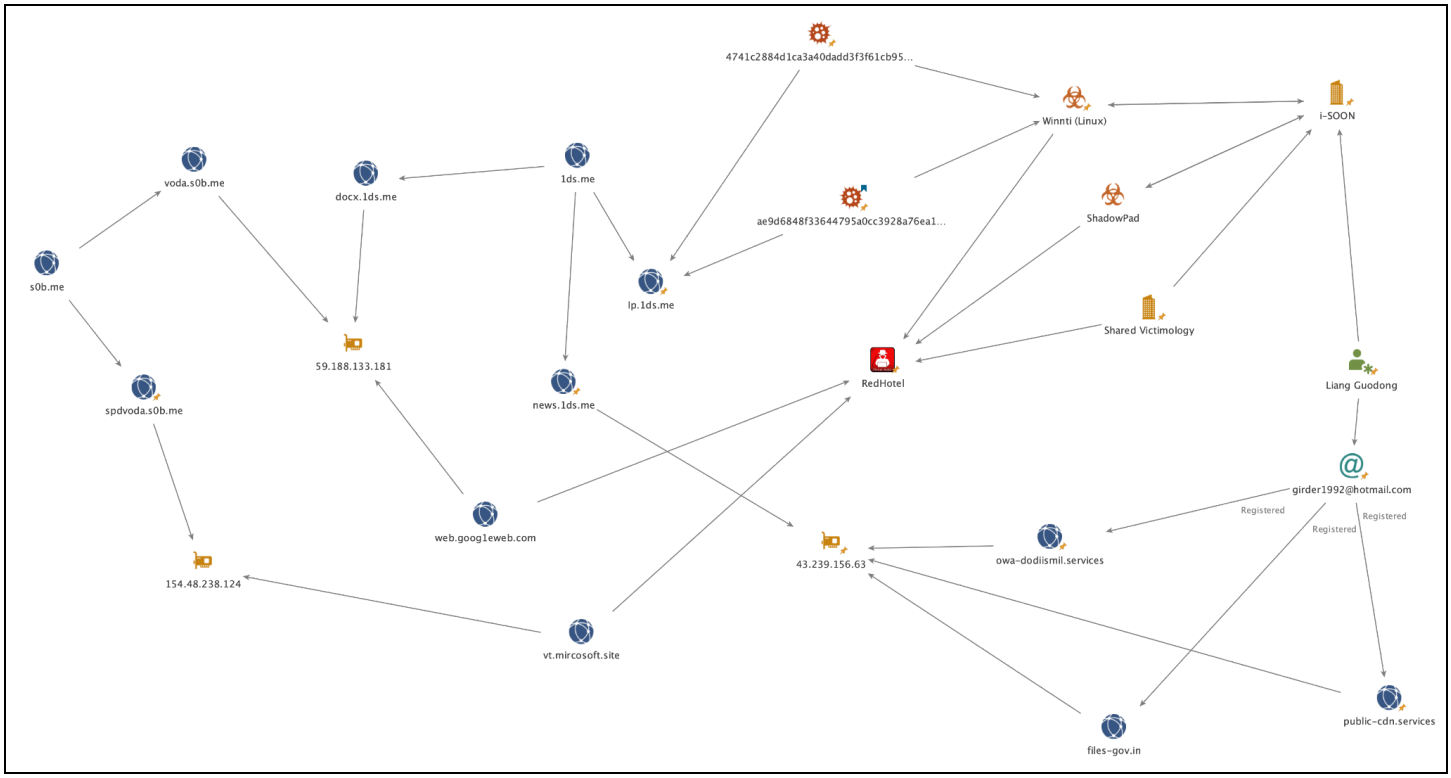


Figure 15: *Links between i-SOON and the RedHotel threat activity group (Source: Recorded Future)*

SHA256	C2 Domain
ae9d6848f33644795a0cc3928a76ea194b99da3c10f802db22034d9f695a0c23	ip.1ds[.]me
4741c2884d1ca3a40dadd3f3f61cb95a59b11f99a0f980dbadc663b85eb77a2a	ip.1ds[.]me

Table 1: *Associated RedHotel Winnti Linux samples (Source: Recorded Future)*

RedHotel Is a Prolific ShadowPad and Winnti (Linux) User

The previously established use of ShadowPad and Winnti (Linux) by i-SOON, both privately held custom malware families, aligns with tracked RedHotel activity as one of the most prolific users of both of these

malware families in recent years. Furthermore, as previously noted, i-SOON appears to be selling a ShadowPad variant obfuscated using the bespoke packing mechanism known as ScatterBee. RedHotel has been the primary user of the ShadowPad ScatterBee variant historically, supporting the hypothesis that i-SOON is the original developer and user of this variant.

While a less strong correlation, the use of open-source offensive security tools such as Acunetix and multiple open-source webshells referenced in the i-SOON leak also aligns with historical RedHotel activity.

i-SOON Victim Data Overlaps Temporally With RedHotel Intrusion Activity

Finally, Insikt Group observed multiple overlaps between specific victim organizations referenced in the i-SOON leak and historically identified RedHotel victims. A selection of identified examples of these overlaps are provided below:

Organization	Overlap Between i-SOON and RedHotel Victims
Nepal Telecom	The leaked i-SOON material references data exfiltrated from Nepal Telecom from May 2021 (see **Figure 16***).* Insikt Group observed likely data exfiltration from Nepal Telecom corporate infrastructure to a RedHotel Spyder C2 IP address this same month, as previously reported.
Ministry of Economy and Finance (MEF) of Cambodia	The leaked material references exfiltrated data from *fmis.mef[.]gov[.]kh*, the Financial Management Information System (FMIS) of the Ministry of Economy and Finance of Cambodia. Insikt Group previously observed and reported on an FMIS mail server communicating to RedHotel ShadowPad C2 infrastructure in June 2022.
Thai Government Departments	The leaked i-SOON material also references multiple Thai government departments as victims with no time frames provided. Many of these overlap with known RedHotel victims historically reported by Insikt Group.
Scientific and Technological Research Council of Türkiye	Using Recorded Future Network Intelligence, Insikt Group observed Scientific and Technological Research Council of Türkiye (Tübitak) SSL VPN and mail server infrastructure regularly communicating to a RedHotel actor-controlled server. This organization is also referenced in the i-SOON leak as being compromised in 2020.
Various Telecommunications Organizations	The i-SOON leak refers to the compromise of multiple Asian telecommunications firms including Myanmar Posts and Telecommunications (Myanmar), Digi (Malaysia), and Bayan Telecommunications (Philippines). While we have not observed RedHotel compromising these organizations directly, we have observed historical typosquat domains spoofing these organizations, which we attribute to RedHotel. For example:

	• Myanmar Posts and Telecommunications (MPT): *mpt[.]buzz* and *mptcdn[.]com* • Bayan Telecommunications: *bayantele[.]xyz* • Digi: *mydigi[.]site*
Hong Kong Universities	The leaked i-SOON documents reference multiple compromised Hong Kong universities from 2019 to 2021 (see **Figure 17**). This directly aligns with RedHotel activity reported publicly by ESET during this time frame. Notably, the ESET report references the use of subdomains containing specific victim identities within subdomains as follows: • *b[org_name].dnslookup[.]services:443* • *w[org_name].livehost[.]live:443* • *w[org_name].dnslookup[.]services:443* Based on passive DNS data, we observed that two of these overlapped with Hong Kong universities identified as victims of the i-SOON leak during this time period: • Hong Kong University of Education: *whkedu.dnslookup[.]services* • Chinese University of Hong Kong: *wcuhk.livehost[.]live*

Table 2: *Overlaps between RedHotel and i-SOON victimology (Source: Recorded Future)*

尼泊尔	运营商	尼泊尔电信	ntc.net.np	2.26GB	数据表	2021.05

Figure 16: *Reference to Nepal Telecom data exfiltration in May 2021 (Source: i-SOON leak)*

香港	教育	香港东华学院	twc.edu.hk				主站权限，办公网权限，邮服权限
香港	教育	香港教育大学	eduhk.hk	3.23GB	数据表		主站权限，办公网权限，邮服权限
香港	教育	香港科技大学	ust.hk	2.48GB	文件、邮件	2021	部分院系PC权限
香港	教育	香港树仁大学	hksyu.edu	643MB	数据表、邮件	2019.10 - 2021.03	主站权限，办公网权限，邮服权限
香港	教育	香港中文大学	cuhk.edu.hk	2.95MB	数据表	2019.12	部分院系PC权限

Figure 17: *Reference to data exfiltration from multiple Hong Kong universities from 2019 to 2021 (Source: i-SOON leak)*

The Comm100 Supply-Chain Compromise Connection

Finally, we also note an overlap between the IP address *8.218.67[.]52* referenced in the i-SOON leak and a supply-chain compromise targeting a chat-based customer engagement application developed by the Canadian software firm Comm100, as explored in Palo Alto Unit42 research. CrowdStrike previously assessed this intrusion was likely conducted by a China-nexus actor in support of wider targeting of the online gambling sector. This directly aligns with i-SOON's documented support of China's public security service documented within the leaked material, which specifically refers to capabilities surrounding the monitoring of online gambling platforms catering to the Chinese market, including via an intelligence platform named "Falcon Anti-Gambling Platform".

Date	*Message*	*Translated*
2022-06-13 7:39:23	现在能给不	Can you give it now?
2022-06-13 7:40:26	(彩宝贝)	(Gambling or lottery site)
	(代理)	*(Proxy)*
	8.218.67[.]52:27011	
	(TCP隧道)	*(TCP Tunnel)*
	8.218.67[.]52:17011	
	(账号)	*(account)*
	admin	
	(密码)	*(password)*
	88888888	
2022-06-13 7:40:34	*嗯嗯*	*Uh-huh*
2022-06-13 7:40:37	*我日*	*[Expletive]*
2022-06-13 7:40:54	*这个服务器在香港的*	*This server is in Hong Kong*
2022-06-13 7:41:06	*你不管*	*You don't need to worry about it*
2022-06-13 7:41:07	*<ahref='068f70a1-1ff9-451 b-999e-2569860fd348.md'>domain_access_result(1).csv*	
2022-06-13 7:41:11	*嗯*	*Um*
2022-06-13 7:41:14	*这个服务器是我们的*	*This server is ours*

Figure 18: *i-SOON leaked chats between "wxid_zb45i0rc71yk21" and "wxid_c9yv0nsla3yn22" referencing the 8.218.67[.]52 IP address (Source: i-SOON leak)*

Outlook

The i-SOON leak offers an unprecedented look inside China's cyber-espionage ecosystem and specifically the role that a large complex web of private contractors plays in gathering intelligence on behalf of China's public security, state security, and military intelligence apparatus. It provides supporting evidence regarding the long-suspected presence of "digital quartermasters" that provide capabilities to multiple Chinese state-sponsored groups. Despite i-SOON's global impact and extensive targeting, it is a relatively small company operating alongside numerous other entities within China's private contractor landscape that operate under a similar model (1, 2, 3), again underscoring the broad scope and scale of Chinese cyber operations supporting security services and military intelligence efforts.

In the future, Insikt Group anticipates that i-SOON-linked threat activity groups will continue to remain active and largely operate unabated. Notably, since the material was leaked, Insikt Group has already identified newly observed domain and infrastructure developments from i-SOON-linked groups RedAlpha and RedHotel, including the following examples:

- On February 27, 2024, RedAlpha registered the credential phishing domain *fwl[.]homes*, which resolved to the dedicated server *45.146.234[.]159*. This domain has been observed spoofing an email login site for Microsoft Outlook. The group also registered a further domain, *msew[.]homes*, on March 1, 2024, which resolved to the dedicated VirMach IP address *85.209.17[.]107*.
- On March 2, 2024, multiple subdomains of the known RedHotel domain *ekaldhfl[.]club* began resolving to the UFO Network IP address *45.195.198[.]103*. At this time, we also observed this IP address communicate with a known upstream RedHotel server in a manner consistent with previously highlighted activity.

Appendix A — Indicators of Compromise

Note: *These indicators are historical and often date back several years. They are included solely as a collation of the referenced infrastructure used in this report to identify connections between i-SOON and tracked Chinese state-sponsored threat activity and should not be used as indications of current activity.*

Domains:

1ds[.]me
antspam-mail[.]services
bayantele[.]xyz
dnslookup[.]services
docx[.]1ds[.]me
gmail[.]isooncloud[.]com
gmailapp[.]me
i-soon[.]net
ip[.]1ds[.]me
lengmo[.]myds[.]me
lengmo[.]net
linercn[.]org
livehost[.]live
mailnotes[.]online
mailteso[.]online
mpt[.]buzz
mptcdn[.]com
mydigi[.]site
news[.]1ds[.]me
wcuhk[.]livehost[.]live
web[.]goog1eweb[.]com
whkedu[.]dnslookup[.]services
www[.]gmailapp[.]me
www[.]sw-hk[.]services

IP Addresses:

1.192.194[.]162
66.98.127[.]105
101.219.17[.]111
118.31.3[.]116
171.88.142[.]148
171.88.143[.]37
171.88.143[.]72
221.13.74[.]218

Email Addresses:

Chen Cheng aka lengmo:

l3n6m0@gmail[.]com

Wu Haibo aka Shutd0wn:

shutdown@139[.]com

Zheng Huadong:

yetiddbb@qq[.]com

Liang Guodong aka liner aka girder:

girvtr@gmail[.]com
liang007@outlook[.]com
gird4r@gmail[.]com
girder1992@hotmail[.]com
evalliang@163[.]com
6060841@qq[.]com
leungguodong@outlook[.]com
l3nor@hotmail[.]com

Recorded Future®

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for clients, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest threat intelligence company. Recorded Future's Intelligence Cloud provides end-to-end intelligence across adversaries, infrastructure, and targets. Indexing the internet across the open web, dark web, and technical sources, Recorded Future provides real-time visibility into an expanding attack surface and threat landscape, empowering clients to act with speed and confidence to reduce risk and securely drive business forward. Headquartered in Boston with offices and employees around the world, Recorded Future works with over 1,700 businesses and government organizations across more than 75 countries to provide real-time, unbiased, and actionable intelligence. Learn more at recordedfuture.com