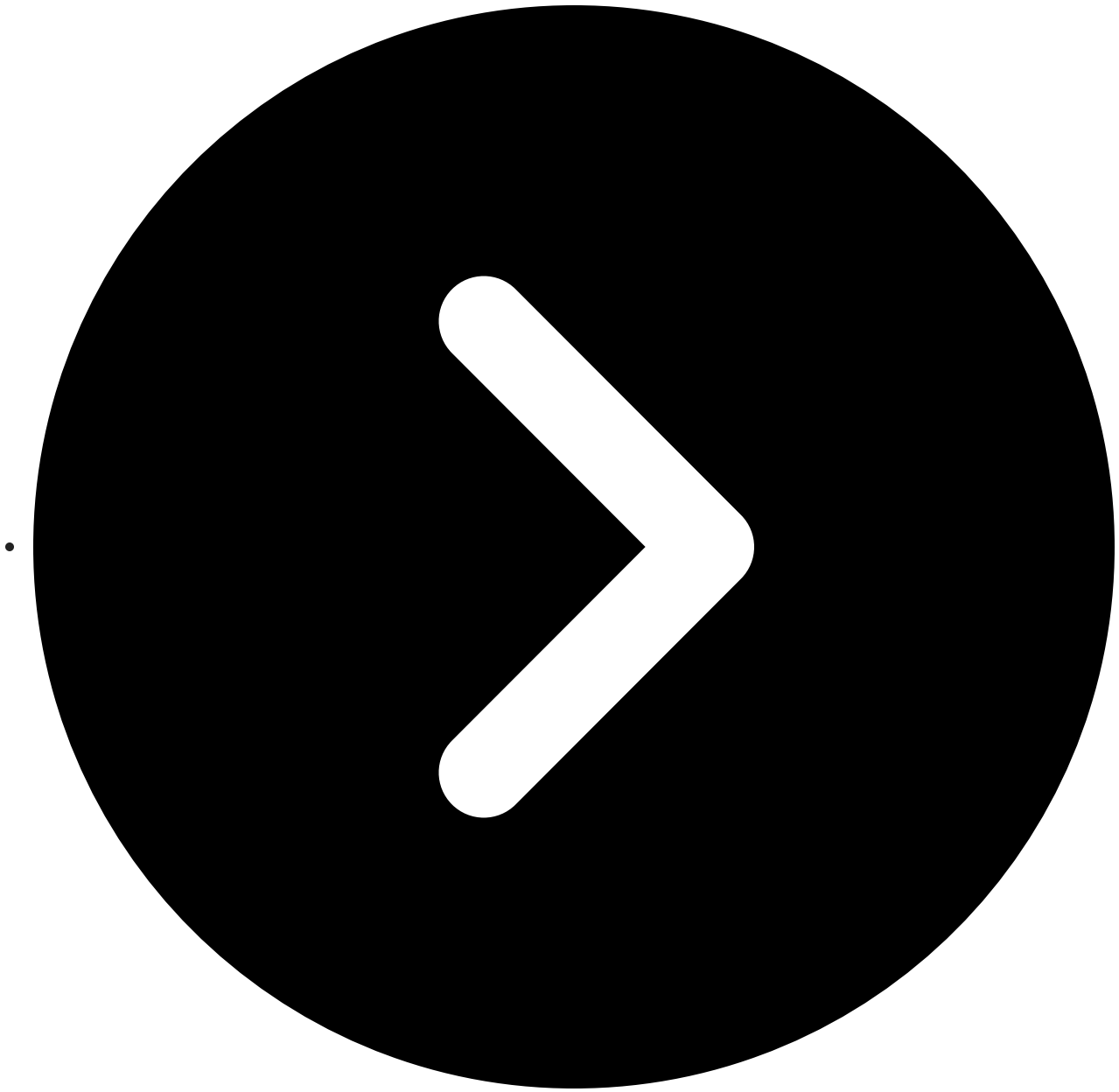
Data Leaks from the Chinese Hacking-for-Hire Industry

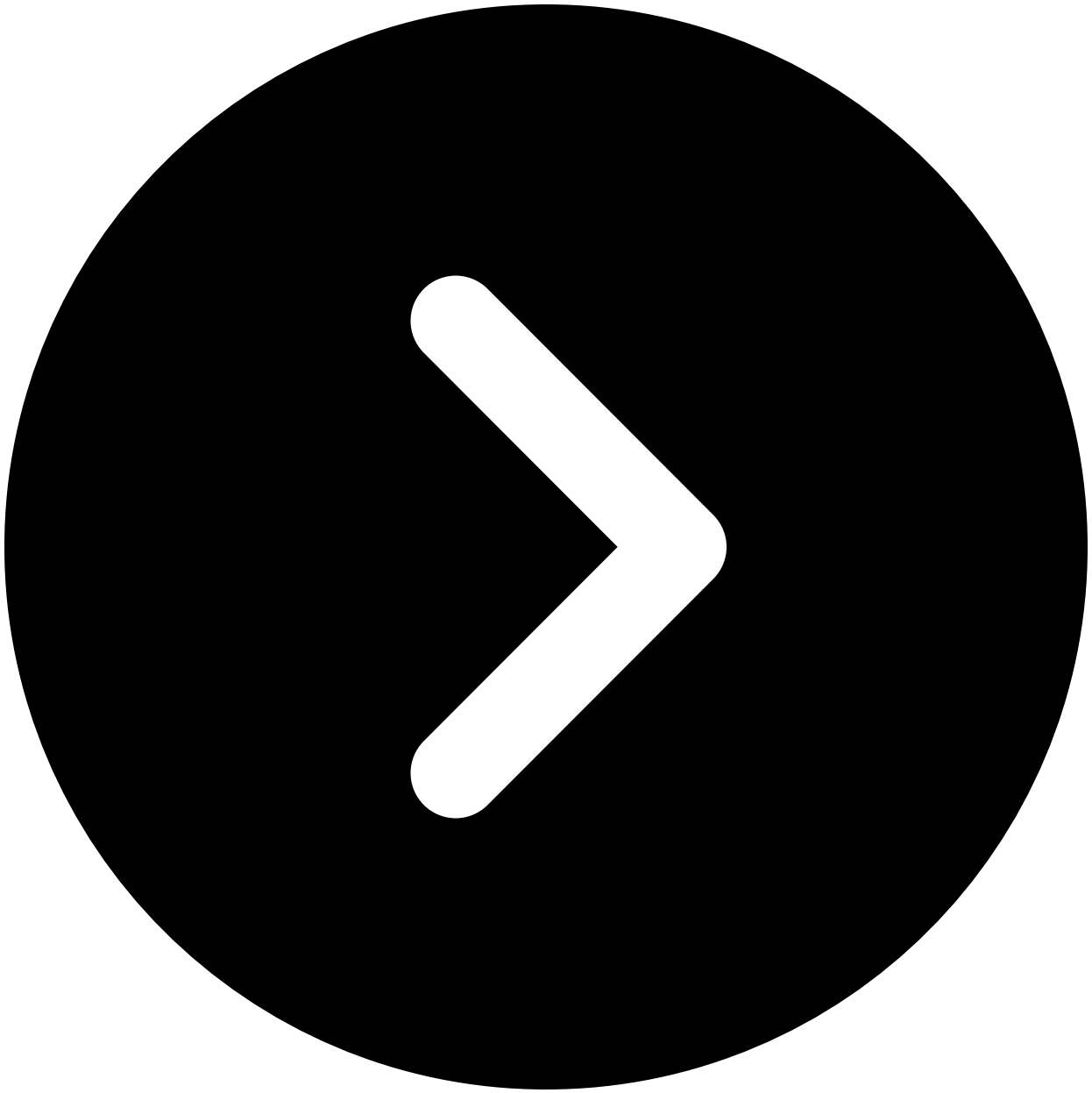
spycloud.com/blog/state-secrets-for-sale-chinese-hacking/

SpyCloud Labs Research Team July 1, 2025

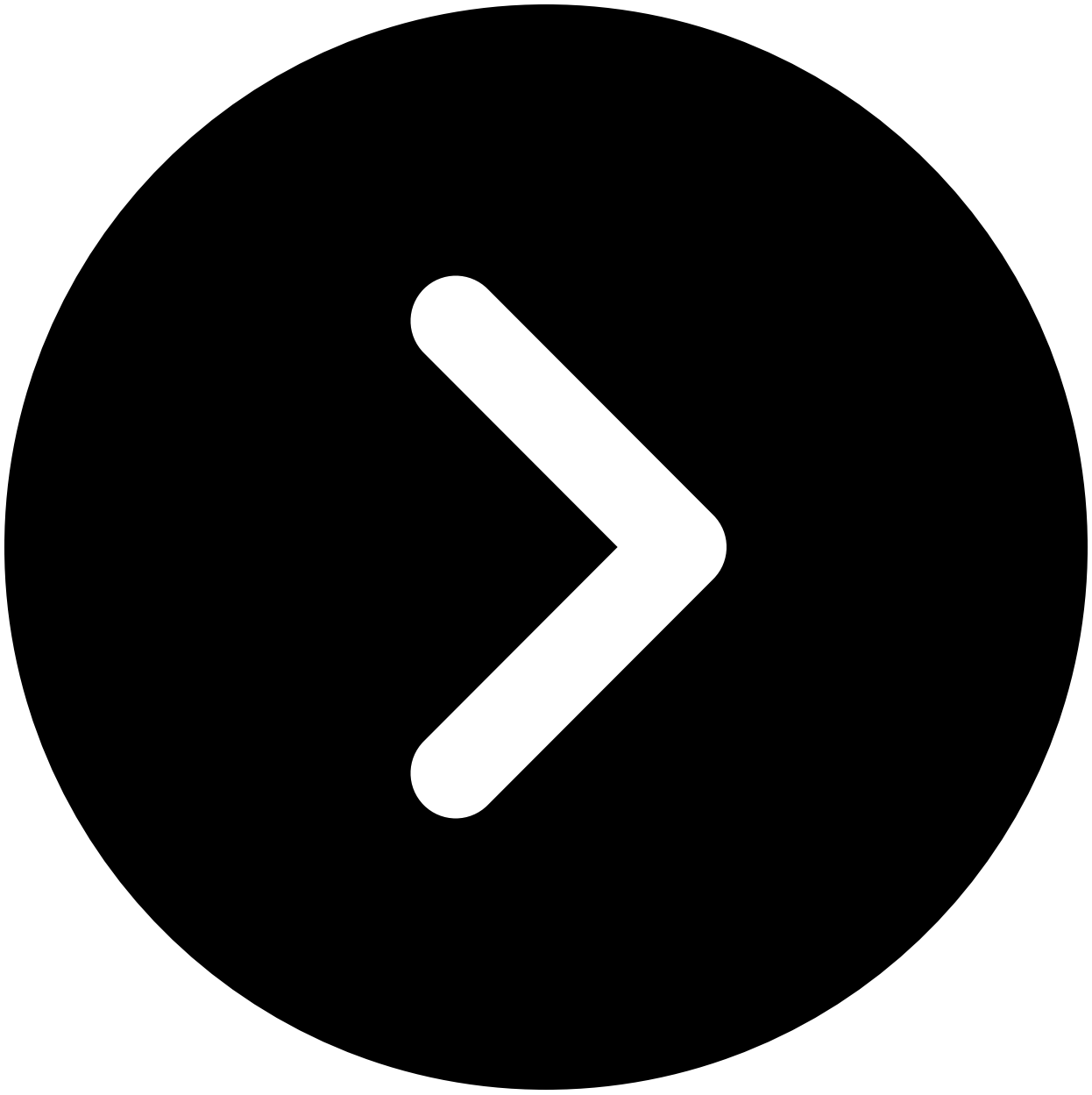
In late May, two particularly interesting Chinese datasets appeared for sale in posts on DarkForums, an English-language data breach and leak forum that has become popular since BreachForums went dark in mid-April. These two posts, which we're calling the **VenusTech Data Leak** and the **Salt Typhoon Data Leak**, had some interesting similarities. Both posts:



- Were posted by new accounts that appear to have been created explicitly to sell a single dataset



Included data that allegedly came from companies in China's large hack-for-hire ecosystem



Included data samples that, while limited, give us some insight into the companies they came from

While the samples provided on DarkForums were relatively small in comparison to previous data leaks of a similar nature (including Chinese IT contractor leaks, such as TopSec and iSoon), the latest leaks provide critical pivot points for assessing the state and structure of the Chinese cybersecurity contractor ecosystem.

We wanted to take a moment to analyze these two recent posts, dive into the sample data, and make some connections between this activity and some overall trends we are observing in our research into the Chinese cybercriminal underground.

Analysis of the VenusTech Data Leak

VenusTech is a major IT security vendor in China with a focus on serving government clients. It was founded in 1996 and is traded on the Shenzhen Stock Exchange. They have previously documented ties to the hack-for-hire industry including procuring services from XFocus, who created the original Blaster worm in 2003, as well as providing startup funding to Integrity Tech, the company responsible for the offensive hacking activity associated with Flax Typhoon.

On May 17, a post relating to VenusTech was created by an account called “IronTooth” and titled “Chinese tech company venus leaked documents.” The IronTooth account appears to have been newly created and simply uses the default profile image for DarkForums. The full post text reads:

selling sourced leaked documents dump of chinese tech company. includes papers, products sold to government, accesses, clients and more random shit sold to highest bidder after 48h. crossposted.

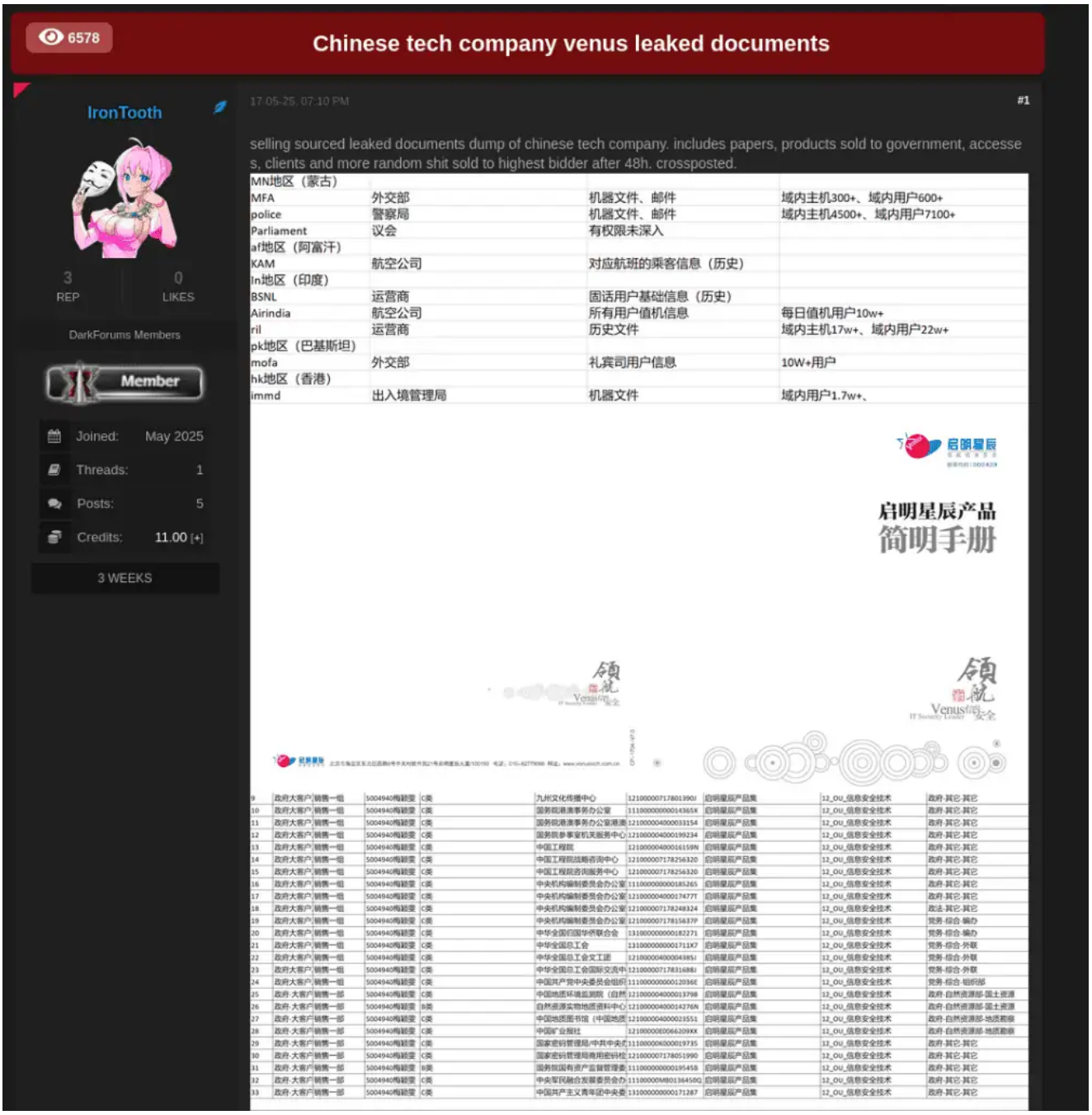


Image 1: Screenshot of IronTooth's post to DarkForums offering data from VenusTech for sale.

IronTooth then included 16 images which appear to be screenshots of various nonpublic VenusTech documents, presentations, spreadsheets, and contracts.

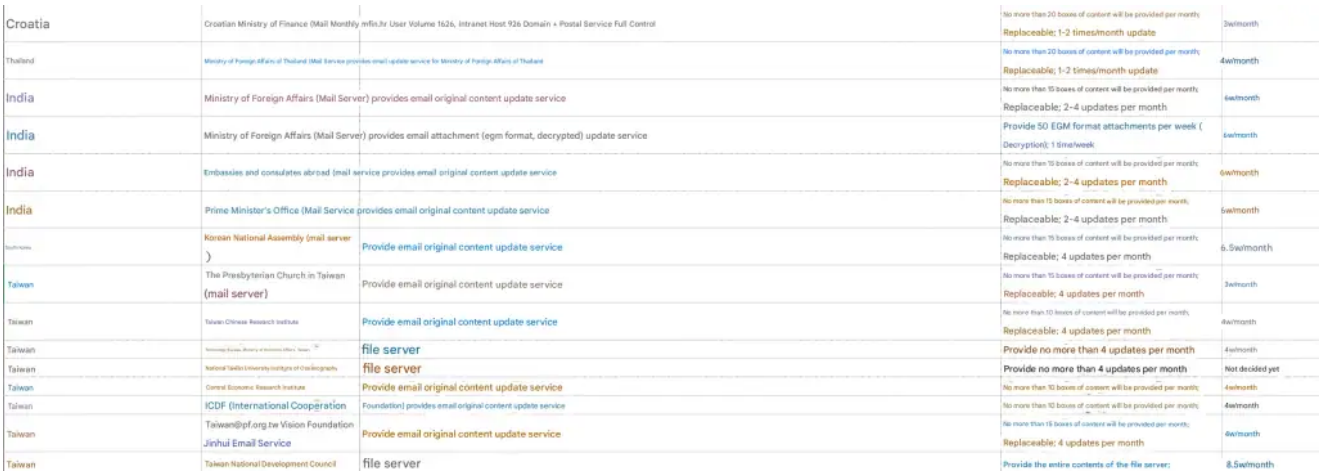
The documents that piqued our interest the most were the three spreadsheets towards the top of the post, which appear to contain details on Chinese government contracts and offensive services. The selected portions of the spreadsheets don't contain column headers, complicating interpretations of the data, but two of them (Image 2 and Image 3) appear to contain detailed line items of collections targets and already hacked organizations.

MN地区（蒙古）			
MFA	外交部	机器文件、邮件	域内主机300+、域内用户600+
police	警察局	机器文件、邮件	域内主机4500+、域内用户7100+
Parliament	议会	有权限未深入	
af地区（阿富汗）			
KAM	航空公司	对应航班的乘客信息（历史）	
In地区（印度）			
BSNL	运营商	固话用户基础信息（历史）	
Airindia	航空公司	所有用户值机信息	每日值机用户10w+
ril	运营商	历史文件	域内主机17w+、域内用户22w+
pk地区（巴基斯坦）			
mofa	外交部	礼宾司用户信息	10W+用户
hk地区（香港）			
immd	出入境管理局	机器文件	域内用户1.7w+、
MN region (Mongolia)			
MFA		Machine files, emails	300+ hosts and 600+ users in the domain
police	police station	Machine files, emails	4500+ hosts and 7100+ users in the domain
Parliament	parliament	Have permission but not go deep	
af region (Afghanistan)			
CAME	airline	Passenger information of the corresponding flight (history)	
In region (India)			
BSNL	Operator	Fixed-line user basic information (history)	
Airindia	airline	All user check-in information	Daily check-in users 10w+
ril	Operator	historical documents	170,000+ hosts and 220,000+ users in the domain
pk region (Pakistan)			
nold		Concierge user information	10W+ users
hk region (Hong Kong)			
immd	Immigration Bureau	machine files	17,000+ users in the domain,

Image 2: Screenshot showing a spreadsheet of entities that may correspond to either intelligence targets, access, or exfiltrated data. It appears to list organizations and regions, information about data types, and notes on amounts of hosts and daily active users. Below the original screenshot is an automated translation generated with Google Translate.

Image 3 also contains what look like cadences for data delivery. For example, one of the lines in Image 3 appears to suggest that VenusTech has access to the Korean National Assembly's email server and is contracted to deliver four updates of data per month from this access to an unnamed customer at the price of 65,000 yuan (equivalent to about $9,000 USD).

克罗地亚	克罗地亚财政部（邮件	mfin.hr用户量1626，内网主机926 域+邮服全控	每月提供不超过20个箱子内容；可更换；1-2次/月的更新	3w/月
泰国	泰国外交部（邮件服务	提供tai外交部电子邮箱更新服务	每月提供不超过20个箱子内容；可更换；1-2次/月的更新	4w/月
印度	外交部（邮件服务器）	提供电子邮箱原始内容更新服务	每月提供不超过15个箱子内容；可更换；2-4次/月的更新	6w/月
印度	外交部（邮件服务器）	提供邮件附件（egm格式，已解密）更新服务	每周提供egm格式附件50篇（已解密）;1次/周	6w/月
印度	驻外使领馆（邮件服务	提供电子邮箱原始内容更新服务	每月提供不超过15个箱子内容；可更换；2-4次/月的更新	6w/月
印度	总理办公室（邮件服务	提供电子邮箱原始内容更新服务	每月提供不超过15个箱子内容；可更换；2-4次/月的更新	6w/月
韩国	韩国国会（邮件服务器）	提供电子邮箱原始内容更新服务	每月提供不超过15个箱子内容；可更换；4次/月的更新	6.5w/月
台湾	台湾基督教长老会（邮件服务器）	提供电子邮箱原始内容更新服务	每月提供不超过15个箱子内容；可更换；4次/月的更新	3w/月
台湾	台湾中华研究院	提供电子邮箱原始内容更新服务	每月提供不超过10个箱子内容；可更换；4次/月的更新	4w/月
台湾	台湾经济部技术局	文件服务器	每月提供不超过4次/月的更新	4w/月
台湾	台湾大学海洋研究所	文件服务器	每月提供不超过4次/月的更新	暂时未定
台湾	中央经济研究院	提供电子邮箱原始内容更新服务	每月提供不超过10个箱子内容；	4w/月
台湾	ICDF（财团法人国际合	提供电子邮箱原始内容更新服务	每月提供不超过10个箱子内容；	4w/月
台湾	台湾@pf.org.tw远景基金会邮箱服务	提供电子邮箱原始内容更新服务	每月提供不超过15个箱子内容；可更换；4次/月的更新	4w/月
台湾	台湾国家发展委员会	文件服务器	提供文件服务器全部内容；	8.5w/月



Croatia	Croatian Ministry of Finance (Mail Monthly mfin.hr User Volume 1626, Intranet Host 926 Domain + Postal Service Full Control	No more than 20 boxes of content will be provided per month; Replaceable; 1-2 times/month update	2w/month
Thailand	Ministry of Foreign Affairs of Thailand (Mail Service provides email update service for Ministry of Foreign Affairs of Thailand	No more than 20 boxes of content will be provided per month; Replaceable; 1-2 times/month update	4w/month
India	Ministry of Foreign Affairs (Mail Server) provides email original content update service	No more than 15 boxes of content will be provided per month; Replaceable; 2-4 updates per month	6w/month
India	Ministry of Foreign Affairs (Mail Server) provides email attachment (egm format, decrypted) update service	Provide 50 EGM format attachments per week (Decryption); 1 time/week	6w/month
India	Embassies and consulates abroad (mail service provides email original content update service	No more than 15 boxes of content will be provided per month; Replaceable; 2-4 updates per month	6w/month
India	Prime Minister's Office (Mail Service provides email original content update service	No more than 15 boxes of content will be provided per month; Replaceable; 2-4 updates per month	6w/month
[redacted]	Korean National Assembly (mail server) Provide email original content update service	No more than 15 boxes of content will be provided per month; Replaceable; 4 updates per month	6.5w/month
Taiwan	The Presbyterian Church in Taiwan (mail server) Provide email original content update service	No more than 15 boxes of content will be provided per month; Replaceable; 4 updates per month	3w/month
Taiwan	Taiwan Chinese Research Institute Provide email original content update service	No more than 10 boxes of content will be provided per month; Replaceable; 4 updates per month	4w/month
Taiwan	[redacted] file server	Provide no more than 4 updates per month	4w/month
Taiwan	National Taiwan University Institute of Oral Biography file server	Provide no more than 4 updates per month	Not decided yet
Taiwan	Central Economic Research Institute Provide email original content update service	No more than 10 boxes of content will be provided per month;	4w/month
Taiwan	ICDF (International Cooperation Foundation) provides email original content update service	No more than 10 boxes of content will be provided per month;	4w/month
Taiwan	Taiwan@pf.org.tw Vision Foundation Jinhui Email Service Provide email original content update service	No more than 15 boxes of content will be provided per month; Replaceable; 4 updates per month	6w/month
Taiwan	Taiwan National Development Council file server	Provide the entire contents of the file server;	8.5w/month

Image 3: Screenshot showing what appears to correspond to intelligence targets, delivery schedules, and monthly prices. The first column contains country names, the second contains organization names, the third contains what appear to be service types, and the fourth appears to contain monthly data delivery quotas and additional stipulations. The final column appears to contain monthly prices ranging from 30,000 yuan per month to 85,000 yuan per month. Below the original screenshot is an automated translation generated with Google Translate.

Image 4 appears to contain contract information showing various Chinese government entities who are customers of VenusTech and additional information about their contracts.

9	政府大客户	销售一组	5004940梅颖雯	C类	九州文化传播中心	121000007178013901	启明星辰产品集	12_OU_信息安全技术	政府-其它-其它
10	政府大客户	销售一组	5004940梅颖雯	C类	国务院港澳事务办公室	11100000000014365X	启明星辰产品集	12_OU_信息安全技术	政府-其它-其它
11	政府大客户	销售一组	5004940梅颖雯	C类	国务院港澳事务办公室港澳	121000004000033154	启明星辰产品集	12_OU_信息安全技术	政府-其它-其它
12	政府大客户	销售一组	5004940梅颖雯	C类	国务院参事室机关服务中心	121000004000199234	启明星辰产品集	12_OU_信息安全技术	政府-其它-其它
13	政府大客户	销售一组	5004940梅颖雯	C类	中国工程院	12100000400016159N	启明星辰产品集	12_OU_信息安全技术	政府-其它-其它
14	政府大客户	销售一组	5004940梅颖雯	C类	中国工程院战略咨询中心	121000007178256320	启明星辰产品集	12_OU_信息安全技术	政府-其它-其它
15	政府大客户	销售一组	5004940梅颖雯	C类	中国工程院咨询服务中心	121000007178256320	启明星辰产品集	12_OU_信息安全技术	政府-其它-其它
16	政府大客户	销售一组	5004940梅颖雯	C类	中央机构编制委员会办公室	111000000000185265	启明星辰产品集	12_OU_信息安全技术	政府-其它-其它
17	政府大客户	销售一组	5004940梅颖雯	C类	中央机构编制委员会办公室	12100000400017477T	启明星辰产品集	12_OU_信息安全技术	政府-其它-其它
18	政府大客户	销售一组	5004940梅颖雯	C类	中央机构编制委员会办公室	121000007178248324	启明星辰产品集	12_OU_信息安全技术	政法-其它-其它
19	政府大客户	销售一组	5004940梅颖雯	C类	中央机构编制委员会办公室	12100000717815637P	启明星辰产品集	12_OU_信息安全技术	党务-综合-编办
20	政府大客户	销售一组	5004940梅颖雯	C类	中华全国归国华侨联合会	131000000000182271	启明星辰产品集	12_OU_信息安全技术	党务-综合-编办
21	政府大客户	销售一组	5004940梅颖雯	C类	中华全国总工会	13100000000171 1X7	启明星辰产品集	12_OU_信息安全技术	党务-综合-外联
22	政府大客户	销售一组	5004940梅颖雯	C类	中华全国总工会文工团	121000004000043851	启明星辰产品集	12_OU_信息安全技术	党务-综合-外联
23	政府大客户	销售一组	5004940梅颖雯	C类	中华全国总工会国际交流中	121000007178316881	启明星辰产品集	12_OU_信息安全技术	党务-综合-外联
24	政府大客户	销售一组	5004940梅颖雯	C类	中国共产党中央委员会组织	111000000000120 36E	启明星辰产品集	12_OU_信息安全技术	党务-综合-组织部
25	政府-大客户	销售一部	5004940梅颖雯	C类	中国地质环境监测院（自然	121000004000137 98	启明星辰产品集	12_OU_信息安全技术	政府-自然资源部-国土资源
26	政府-大客户	销售一部	5004940梅颖雯	B类	自然资源实物地质资料中心	12100000400014276N	启明星辰产品集	12_OU_信息安全技术	政府-自然资源部-国土资源
27	政府-大客户	销售一部	5004940梅颖雯	C类	中国地质图书馆（中国地质	121000004000023551	启明星辰产品集	12_OU_信息安全技术	政府-自然资源部-地质勘察
28	政府-大客户	销售一部	5004940梅颖雯	C类	中国矿业报社	12100000E0066209XX	启明星辰产品集	12_OU_信息安全技术	政府-自然资源部-地质勘察
29	政府-大客户	销售一部	5004940梅颖雯	C类	国家密码管理局/中共中央办	11100000K000019735	启明星辰产品集	12_OU_信息安全技术	政府-其它-其它
30	政府-大客户	销售一部	5004940梅颖雯	C类	国家密码管理局商用密码检	121000007178051990	启明星辰产品集	12_OU_信息安全技术	政府-其它-其它
31	政府-大客户	销售一部	5004940梅颖雯	B类	国务院国有资产监督管理委	11100000000019545B	启明星辰产品集	12_OU_信息安全技术	政府-其它-其它
32	政府-大客户	销售一部	5004940梅颖雯	C类	中央军民融合发展委员会办	11100000MB0136450Q	启明星辰产品集	12_OU_信息安全技术	政府-其它-其它
33	政府-大客户	销售一部	5004940梅颖雯	C类	中国共产主义青年团中央委	131000000000171287	启明星辰产品集	12_OU_信息安全技术	政府-其它-其它

1	府大客户二本	销售一组	5009461王硕	C类	人民共和国国家发展和改革委	111000000000139 39Y	启明星辰产品集	12_OU_信息安全技术	政府-电子政务-电子政务外网
2	府大客户二本	销售一组	5009461王硕	C类	发展和改革委员会宏观经济研	12100000400004 81X2	启明星辰产品集	12_OU_信息安全技术	政府-其它-其它
3	府大客户二本	销售一组	5009461王硕	C类	和改革委员会培训中心（宣	12100000400004369W	启明星辰产品集	12_OU_信息安全技术	政府-其它-其它
4	府大客户二本	销售一组	5009461王硕	C类	发展和改革委员会价格认证	121000004000076 58F	启明星辰产品集	12_OU_信息安全技术	政府-其它-其它
5	府大客户二本	销售一组	5009461王硕	C类	改革委员会经济与国防协调发	12100000400017004K	启明星辰产品集	12_OU_信息安全技术	政府-其它-其它
6	府大客户二本	销售一组	5009461王硕	C类	和改革委员会国家投资项目	121000007178016575	启明星辰产品集	12_OU_信息安全技术	政府-其它-其它
7	府大客户二本	销售一组	5009461王硕	C类	发展和改革委员会价格监测	12100000400003876R	启明星辰产品集	12_OU_信息安全技术	政府-其它-其它
8	府大客户二本	销售一组	5009461王硕	C类	发展和改革委员会国际合作	121000004000085 38Y	启明星辰产品集	12_OU_信息安全技术	政府-其它-其它
9	府大客户二本	销售一组	5009461王硕	A类	改革委员会城市和小城镇改	12100000400019499H	启明星辰产品集	12_OU_信息安全技术	政府-其它-其它
10	府大客户二本	销售一组	5009461王硕	C类	展和改革委员会价格成本调	12100000MB0442490C	启明星辰产品集	12_OU_信息安全技术	政府-其它-其它
11	府大客户二本	销售一组	5009461王硕	C类	发展和改革委员会国家节能中心		启明星辰产品集	12_OU_信息安全技术	政府-其它-其它
12	府大客户二本	销售一组	5009461王硕	C类	国家地理空间信息中心	12100000MB0452111X	启明星辰产品集	12_OU_信息安全技术	政府-其它-其它
13	府大客户二本	销售一组	5009461王硕	C类	国家公共信用信息中心	12100000MB0134850X	启明星辰产品集	12_OU_信息安全技术	政府-其它-其它
14	府大客户二本	销售一组	5009461王硕	C类	和改革委员会一带一路建设	121000007178135 00T	启明星辰产品集	12_OU_信息安全技术	政府-其它-其它
15	府大客户二本	销售一组	5009461王硕	C类	展和改革委员会创新驱动发	12100000MB15915781	启明星辰产品集	12_OU_信息安全技术	政府-其它-其它

请先阅读规则 | Named客户名单 | 行业

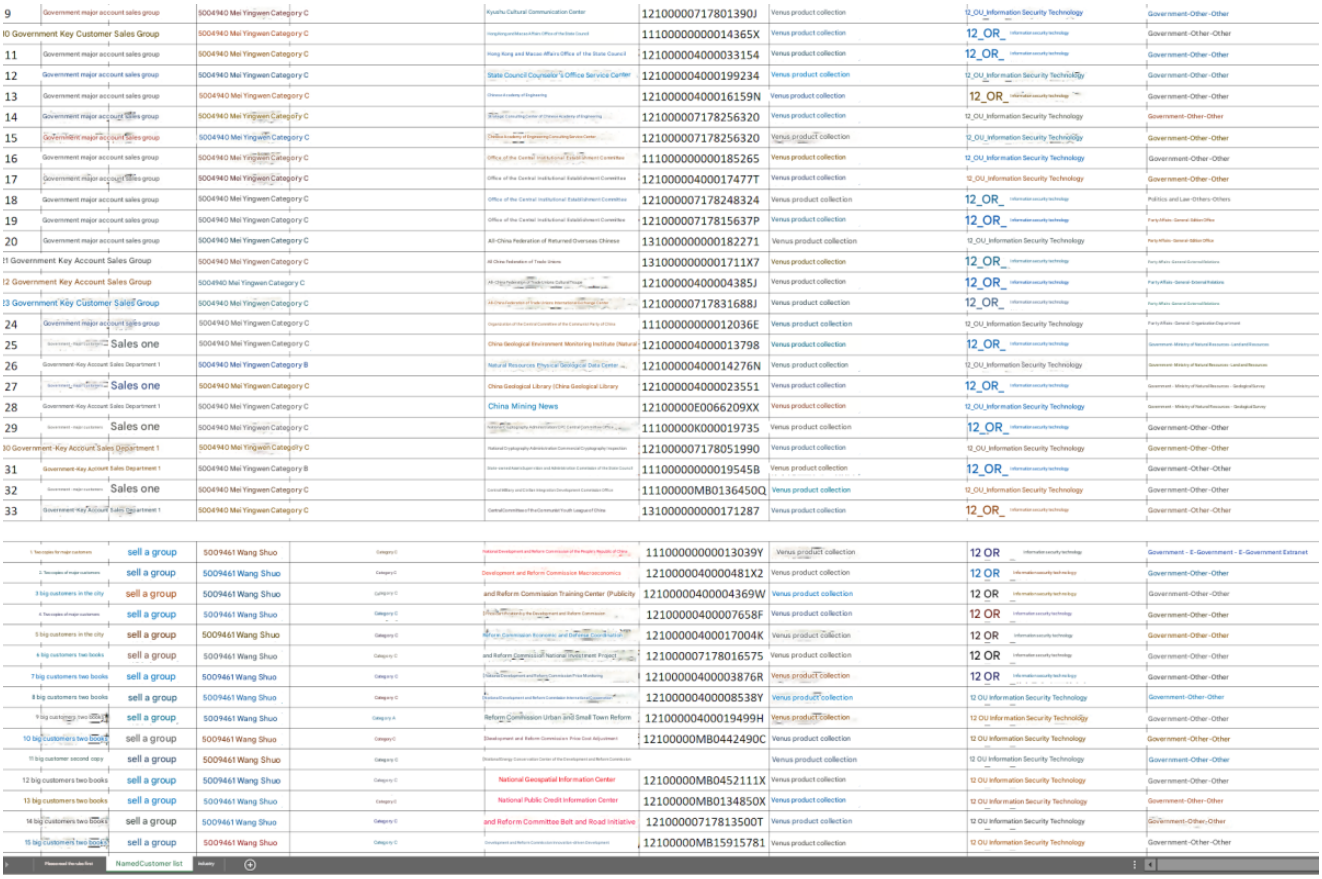


Image 4: Screenshot that appears to show Chinese government clients of VenusTech and additional information about their contracts. The column of alphanumeric strings in the center appear to be Unified Social Credit Codes. Below the original screenshot is an automated translation generated with Google Translate.

All together, these samples appear to provide evidence of specific offensive hacking services that VenusTech is providing to the Chinese government, as well as specific intelligence targets, including organizations in Hong Kong, India, Taiwan, South Korea, Croatia, and Thailand.

Analysis of the Salt Typhoon Data Leak

Salt Typhoon is a Chinese state-sponsored advanced persistent threat (APT) actor that is believed to be controlled by the Ministry of State Security (MSS). They are most notable for a series of intrusions into major US telecommunications companies and internet service providers that were discovered in late 2024. Since then, cybersecurity defenders have continued to discover additional intrusions into global telecommunications systems and universities attributed to Salt Typhoon, including, most recently, Viasat.

On May 18, a post relating to Salt Typhoon was created on DarkForums by user ‘ChinaBob’; their profile picture appears to be the titular character from an early-2000s era Chinese children’s cartoon called the Legend of Nezha. The username ChinaBob is reminiscent of the

username ChinaDan, which was used by the account that posted the Shanghai National Police (SHGA) database for sale on BreachForums in 2022. The post is titled “Chinese government hacking group [Salt Typhoon]: Banking Data + Internal Files.”

The body of the post begins:

selling first-hand data from hacking companies working for the central government. Data includes employee data, financial data of companies and banking data, router configurations of hacked routers with passwords and chats of employees and officials being investigated.

Data: CSV, XLSX, TXT, PDF

Region: China

News Article: t[.]me/xhqcankao/17466

Price: $$$$$U (contact for price)

The post goes on to include multiple data samples, both in the original post and in three separate follow-up posts over the course of the next couple of days.

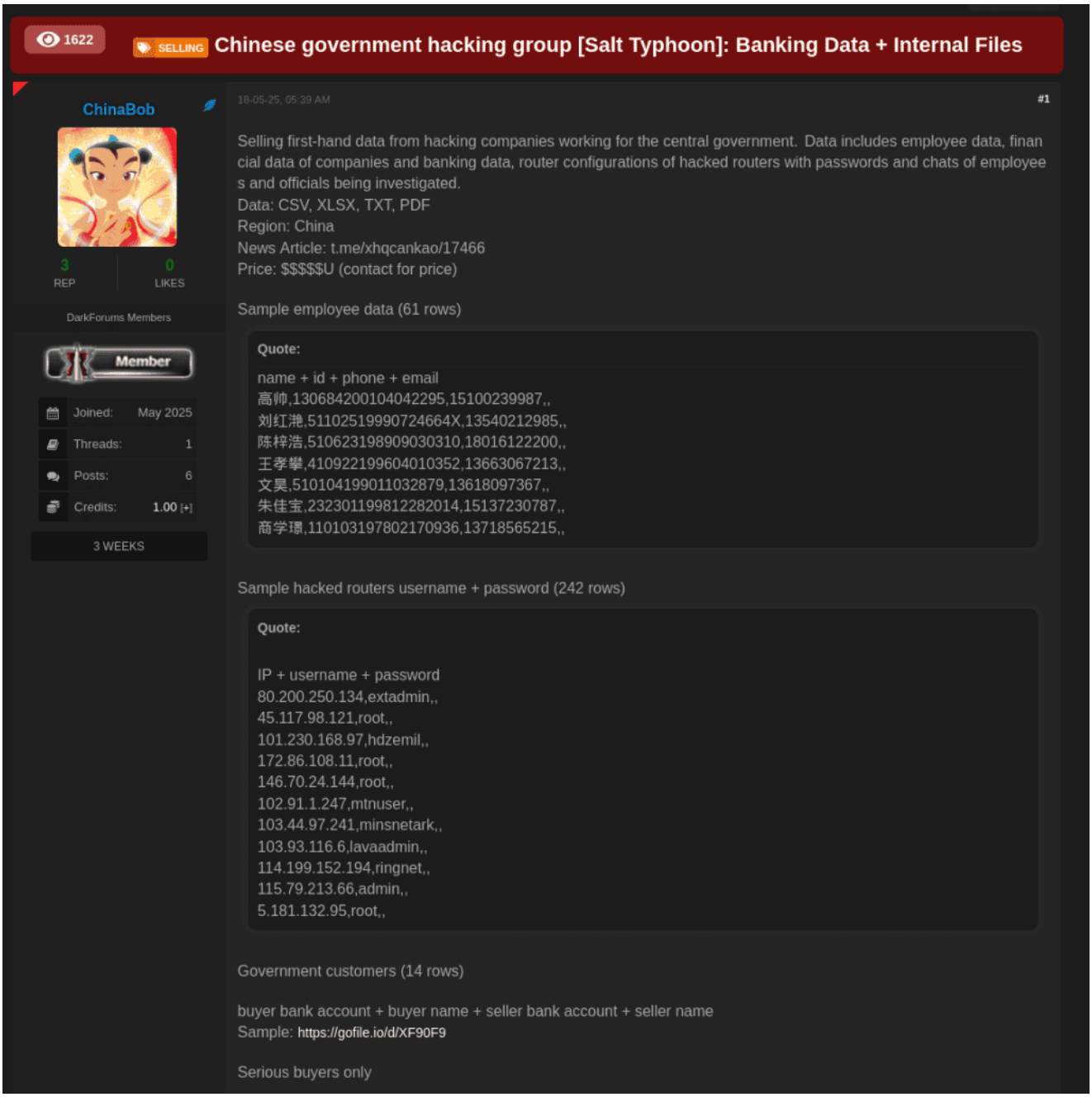


Image 5: Screenshot of ChinaBob's original post to DarkForums offering Salt Typhoon data for sale.

Salt Typhoon employee data samples

The first sample appears to include names, Chinese national ID numbers, and phone numbers for seven Salt Typhoon employees (see Image 5). ChinaBob also followed up, apparently in response to people asking for additional samples, with data for an additional eight employees (see Image 6).

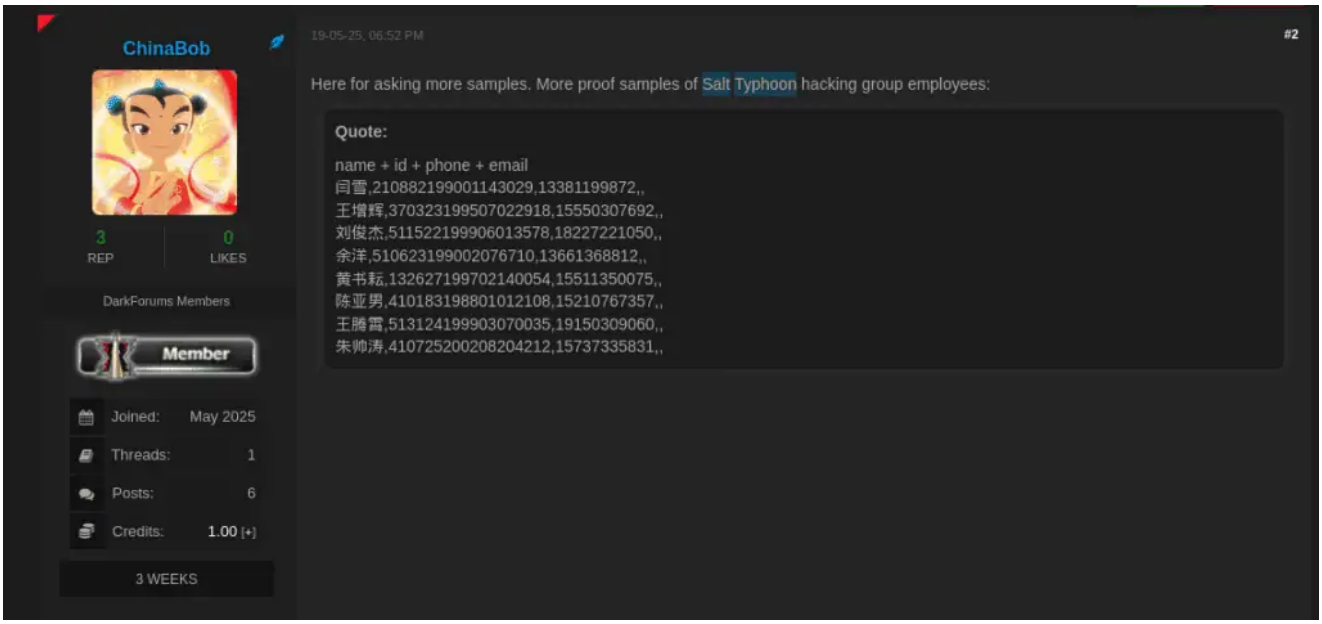


Image 6: Follow-up comment including additional employee data.

Our team searched for these identifiers in our extensive repository of breached and leaked data, as well as in a few SGKs (repositories of leaked and stolen PII, created by Chinese-language cybercriminal actors which allow for easy queryability of PII on Chinese citizens and users). Based on these searches, the data generally does appear to match with other sources of PII on Chinese individuals – additional sources confirm links between the listed names, national ID numbers, and phone numbers.

Compromised router samples

The next sample advertised by ChinaBob appears to show IP addresses of routers that were allegedly hacked by Salt Typhoon and associated usernames. The post indicates that the full dataset for sale will contain information on 242 hacked routers, including their passwords. ChinaBob also followed up with a fileshare link to a longer file including the full router configuration for one of the hacked routers (see Image 7).

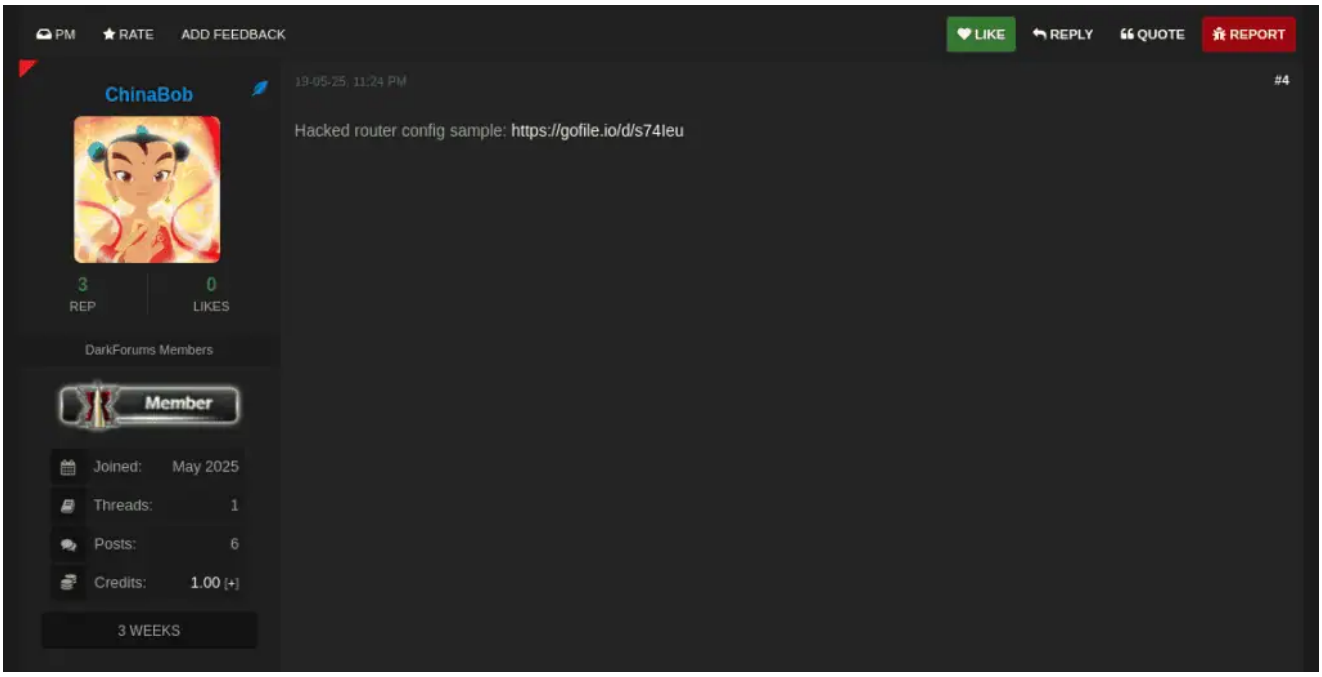


Image 7: Follow-up comment including a link to a file on a filesharing site containing a full hacked router config.

Of the twelve total IP addresses, six appear to have internet-facing Cisco devices behind them, which Salt Typhoon has been known to compromise. Three more appear to have some other high-likelihood indicator of compromise – either based on unusually high fraud scores or being known as tied to residential proxy services.

While these indicators don't necessarily equate to Salt Typhoon activity, they do indicate that there are unpatched and exploitable internet-facing devices behind these IPs that were very likely compromised by at least one cyber threat actor. Additionally, some of the listed router usernames do line up with some of the listed ISPs (for example, the IP address listed in ChinaBob's sample with username *lavaadmin* is administered by the Lava International Limited ISP), making the data appear more credible.

Salt Typhoon transaction activity

The next sample shows transactions between various customers and three "seller" companies, which we hypothesize are associated with the Salt Typhoon threat activity. The spreadsheet (see Image 8) includes transactions between these three companies, transactions in which the three companies appear to be selling services to large, established Chinese cybersecurity vendors such as Qi'anxin (QAX) Legendsec and VenusTech, and transactions in which the three companies appear to be selling services to Chinese government and military units.

银行账号 （Bank Account）	买方（Buyer）	Buyer	银行账号 （Bank Account）	售方（Seller）	Seller
3807010104005554	中国人民解放军61419部队	People's Liberation Army of China 61419 Unit	510501446436000019	四川醋信锐捷网络科技有限公司	Sichuan Zhixin Ruijie Network Technology Company Limited
134000424983	一五二单位	152 Unit	510501446436000019	四川醋信锐捷网络科技有限公司	Sichuan Zhixin Ruijie Network Technology Company Limited
291220010400378	０７１８单位	0718 Unit	510501446436000019	四川醋信锐捷网络科技有限公司	Sichuan Zhixin Ruijie Network Technology Company Limited
020008050600014	北京市对外服务办公室第三室	Beijing Foreign Service Office Room 3	510501446436000019	四川醋信锐捷网络科技有限公司	Sichuan Zhixin Ruijie Network Technology Company Limited
105003634701	青海九七一一所	Qinghai 9711 Institute	510501446436000019	四川醋信锐捷网络科技有限公司	Sichuan Zhixin Ruijie Network Technology Company Limited
12937228936	成都市经济和信息化局	Chengdu Bureau of Economy and Information Technology	510501446436000019	四川醋信锐捷网络科技有限公司	Sichuan Zhixin Ruijie Network Technology Company Limited
110902261210404	奇安信网神信息技术（北京）股份有限公司	Qi'anxin Legendsec Information Technology （Beijing） Company Limited	510501446436000019	四川醋信锐捷网络科技有限公司	Sichuan Zhixin Ruijie Network Technology Company Limited
112012830005657	永信至诚科技集团股份有限公司	Beijing Integrity Technology Group Company Limited	510501446436000019	四川醋信锐捷网络科技有限公司	Sichuan Zhixin Ruijie Network Technology Company Limited
020000290620032727	北京京堪至达信息技术有限公司	Beijing Jingyuan Shengda Information Technology Company Limited	510501446436000019	四川醋信锐捷网络科技有限公司	Sichuan Zhixin Ruijie Network Technology Company Limited
861583890110001	北京启明星辰信息安全技术有限公司	Beijing VenusTech Information Security Technology Company Limited	510501446436000019	四川醋信锐捷网络科技有限公司	Sichuan Zhixin Ruijie Network Technology Company Limited
200049628217001003	中国科学院信息工程研究所	Institute of Information Engineering of the Chinese Academy of Sciences	110501112830000023	北京寰宇天穹信息技术有限公司	Beijing Huanyu Tianqiong Information Technology Company Limited
010903346001201053918	北京国博科技有限公司	Granpect Company Limited	110501112830000023	北京寰宇天穹信息技术有限公司	Beijing Huanyu Tianqiong Information Technology Company Limited
621691010644344	余洋	Yu Yang	510501647227000025	四川醋信和网络科技有限公司	Sichuan Juxinhe Network Technology Company Limited
110501112830000023	北京寰宇天穹信息技术有限公司	Beijing Huanyu Tianqiong Information Technology Company Limited	510501647227000025	四川醋信和网络科技有限公司	Sichuan Juxinhe Network Technology Company Limited

Image 8: Spreadsheet containing transaction data between the organizations allegedly behind the Salt Typhoon threat activity and their "government customers."

The first transaction in this sample lists PLA Unit 61419 as the buyer, which has been affiliated with the 'Tick' threat activity group and was discovered in 2021 purchasing foreign antivirus products with the suspected goal of developing exploits for them. Another familiar listed buyer is the Institute of Information Engineering of the Chinese Academy of Sciences, a publicly owned academic institute which established China's first cyber range, owns a small stake in iSoon, and has significant known ties to the Chinese hack-for-hire industry.

The three listed "seller" organizations in this sample include one which had already been named and sanctioned by the US Government for threat activity associated with Salt Typhoon – *Sichuan Juxinhe Network Technology Company* – as well as two additional business entities, *Beijing Huanyu Tiangiong Information Technology Company Limited* and *Sichuan Zhixin Ruijie Network Technology Company Limited.*

The cybersecurity analysis team Natto Thoughts published a deep-dive into Sichuan Juxinhe Network Technology Companyearlier this year, concluding that they had characteristics resembling a front company of the MSS. Based on our initial searches, the two other companies listed as sellers in this spreadsheet also share some of the key characteristics of a front company including a limited digital footprint (including no public-facing website) and having a very small number of listed employees according to business intelligence databases.

Additionally, we see three of the individuals from ChinaBob's sample employee lists reflected in public business registration records for Sichuan Zhixin Ruijie Network Technology Company Limited: Yu Yang (余洋), Yan Xue (闫雪), and Chen Zihao (陈梓浩). Based just on these three individuals, we can also find connections to public business registration records for four additional small companies not otherwise listed in this breach. Each of these additional four businesses also appear to have very limited digital footprints and few employees.

Using information derived from SpyCloud's data holdings as well as business registration, we compiled basic business and identity details for each of the three individuals.

Chen Zihao (陈梓浩)

Male | 36 years old | Sichuan Province
National ID Number: 510623198909030310 | DOB: September 3, 1989
Phone Numbers: 18016122200, 15882059538

QQ: 523386132 | Weibo ID: 2608965270

Associated Business Registration Records:

Sichuan Zhixin Ruijie Network Technology Co., Ltd.

- Sichuan Mubin Information Consulting & Edit Co., Ltd.
- Mubin (Deyang) Business Information & Edit Consulting Services Co., Ltd.

Yan Xue (闫雪)

Female | 35 years old | Liaoning Province
National ID number: 210882199001143029 | DOB: January 14, 1990
Phone Numbers: 13381199872, 17739345534

Weibo ID: 5746370894

Associated Business Registration Records:

Sichuan Zhixin Ruijie Network Technology Co., Ltd.

- Shanghai Meicheng Network Technology Service Center
- Beijing Bole Human Resources Co., Ltd.

Yu Yang (余洋)

Male | 35 years old | Sichuan Province
National ID Number: 510623199002076710 | DOB: February 7, 1990
Phone Number: 13661368812

QQ: 517011513 | Weibo ID: 2759346040 | Email: lanyi__158@163.com

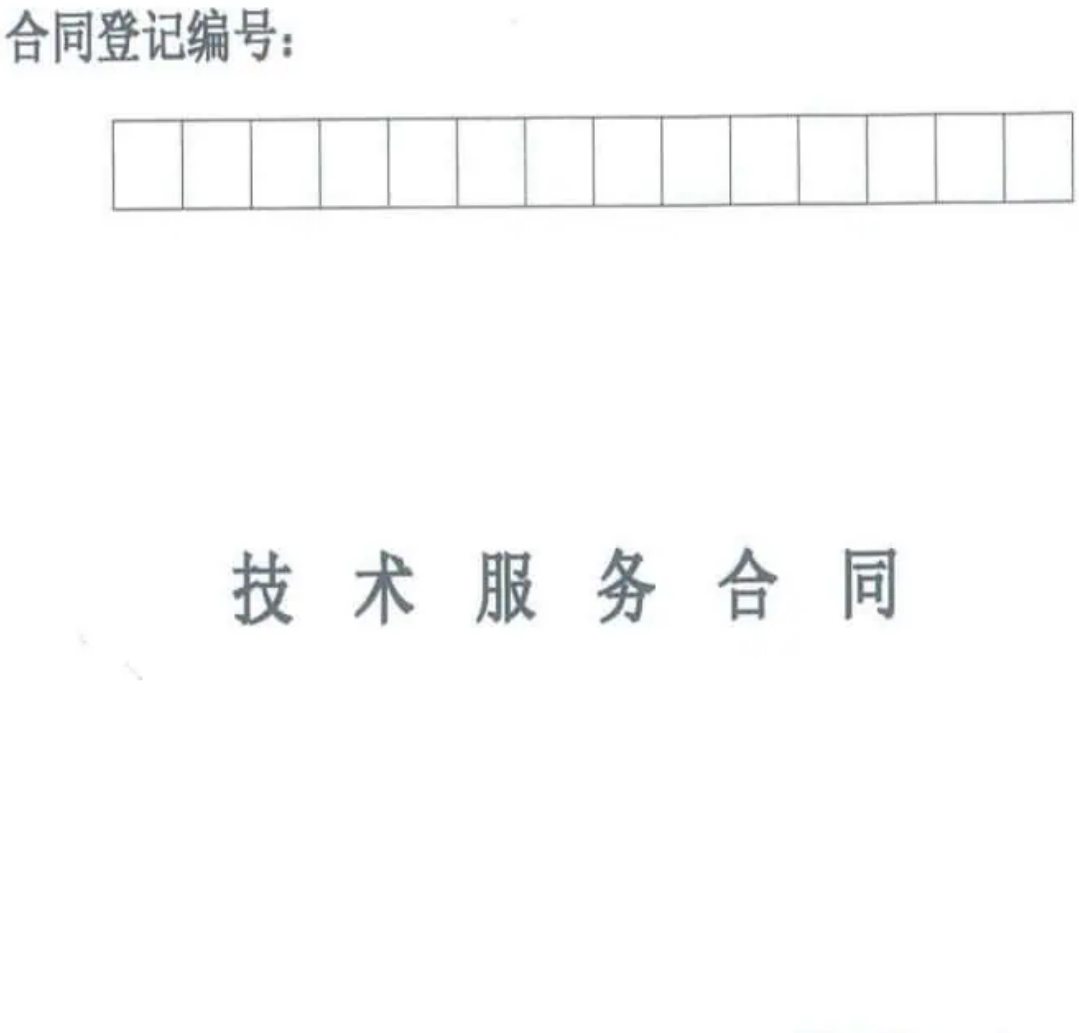
Associated Business Registration Records:

Sichuan Zhixin Ruijie Network Technology Co., Ltd.

Salt Typhoon contract data

ChinaBob also made a follow-up post including a technical service contract between Beijing Huanyu Tiangiong Information Technology Company Limited and Tongfang Co, a publicly traded state-owned enterprise based in Beijing. Tongfang Co, (Tsinghua Tongfang Co. Ltd.) is a high-tech information technology company that is closely associated with Tsinghua

University and supplies military equipment to the PLA. In 2019, the China National Nuclear Corporation (CNNC), which oversees both China's military and civilian nuclear programs, became a controlling stockholder of Tongfang Co.



合同登记编号：

技 术 服 务 合 同

项目名称：同方股份综合应用平台等保测评项目

（甲方）同方股份有限公司

（乙方）北京寰宇天穹信息技术有限公司

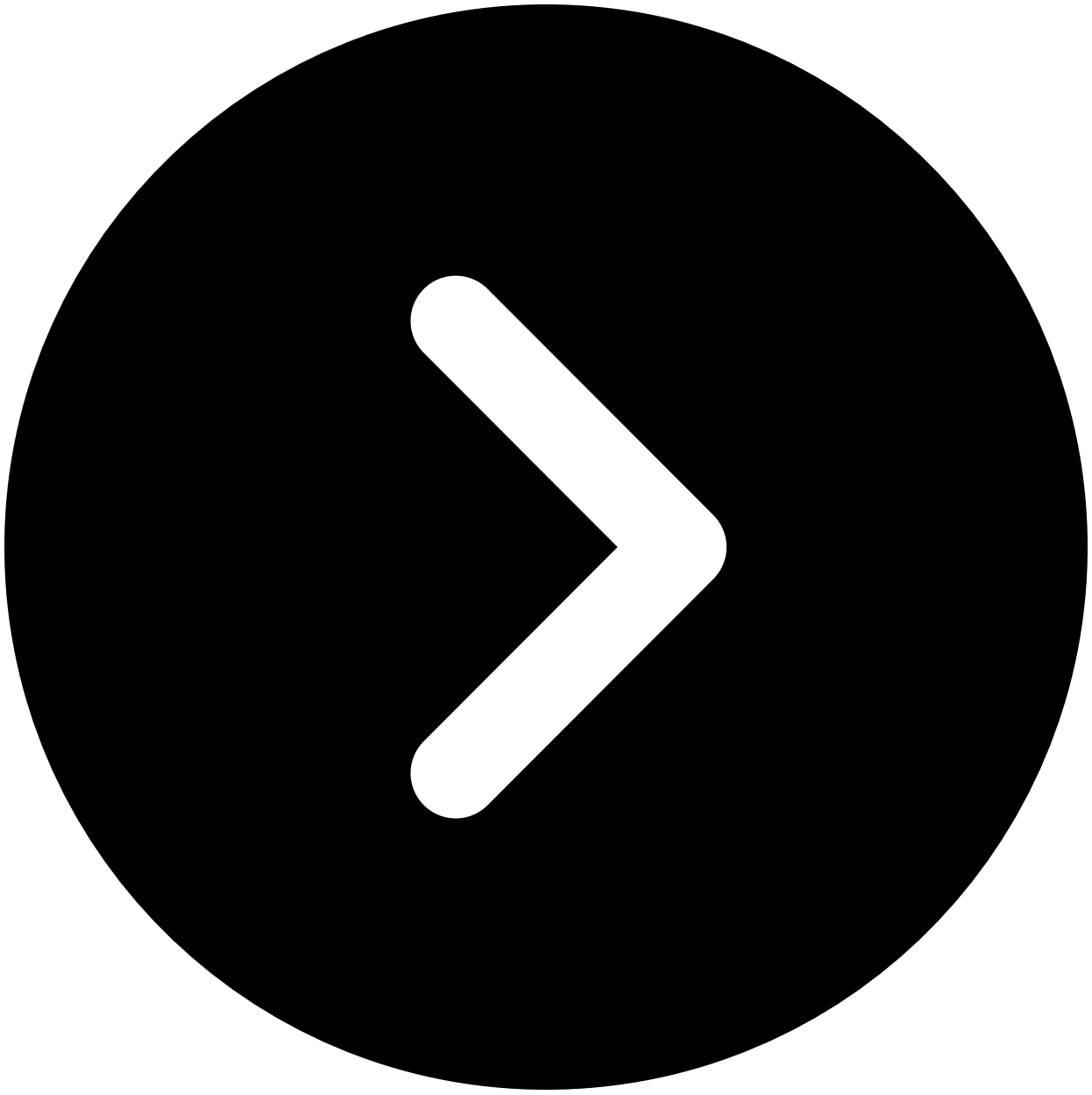
Image 9: Page one of the final Salt Typhoon sample, of a service contract with a buyer.

Analysis and key takeaways from the latest Chinese data leaks

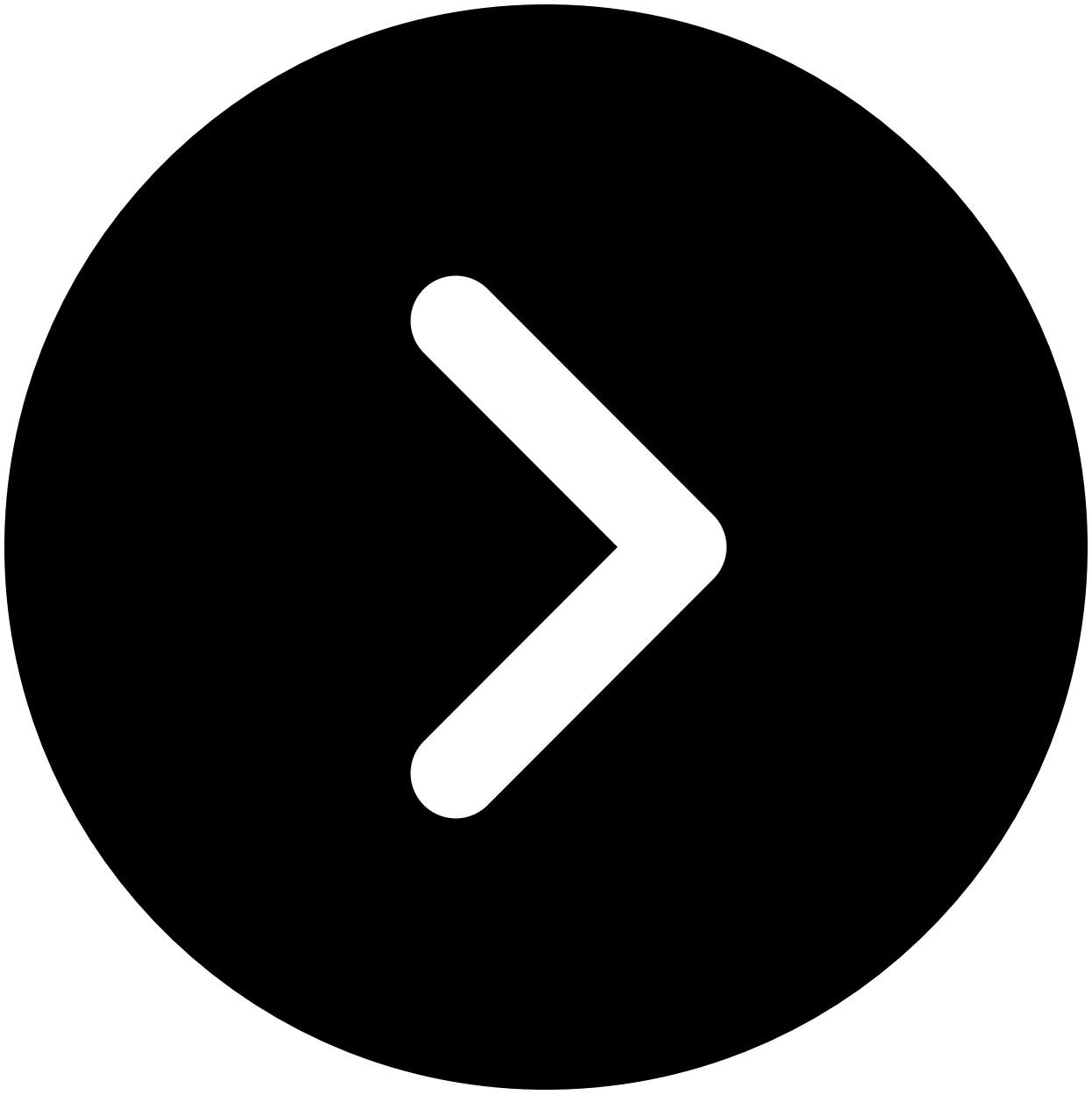
These two recent posts on DarkForums appear to contain nonpublic data sourced from tech companies within China's robust hack-for-hire industry. While the public samples associated with these posts are nowhere near as large as the iSoon or TopSec leaks, they can still shed some additional light on the Chinese offensive cybersecurity contractor industry.

The "Salt Typhoon Data Leak" in particular appears to name two additional business entities as part of the threat activity cluster that have not yet been indicted or sanctioned by US authorities: *Beijing Huanyu Tiangiong Information Technology Company Limited* and *Sichuan Zhixin Ruijie Network Technology Company Limited*, in addition to the company that had already been named*, Sichuan Juxinhe Network Technology Company*.

While the origin of these leaks is uncertain, this data appearing for sale on a Western hacking forum fits into a few overarching trends that we have observed from monitoring Chinese cybercriminal communities:



China’s state-sanctioned data collection and intelligence apparatus is leaky. We have observed a vast ecosystem of corrupt insiders siphoning data from China’s state-sponsored data collections apparatus and selling it on the black market. This threat activity most acutely affects Chinese citizens, whose personal data is readily available to any paying customer.



Cybercriminals from the Sinosphere appear to be increasingly present in Western digital crime spaces. This trend seems to be somewhat driven by Chinese scam and smishing actors aggressively and successfully targeting overseas victims. We frequently observe Chinese-language actors re-sharing (or sometimes taking and attempting to re-sell) data breaches from English-language forums in Chinese-speaking communities.

Stay in the loop

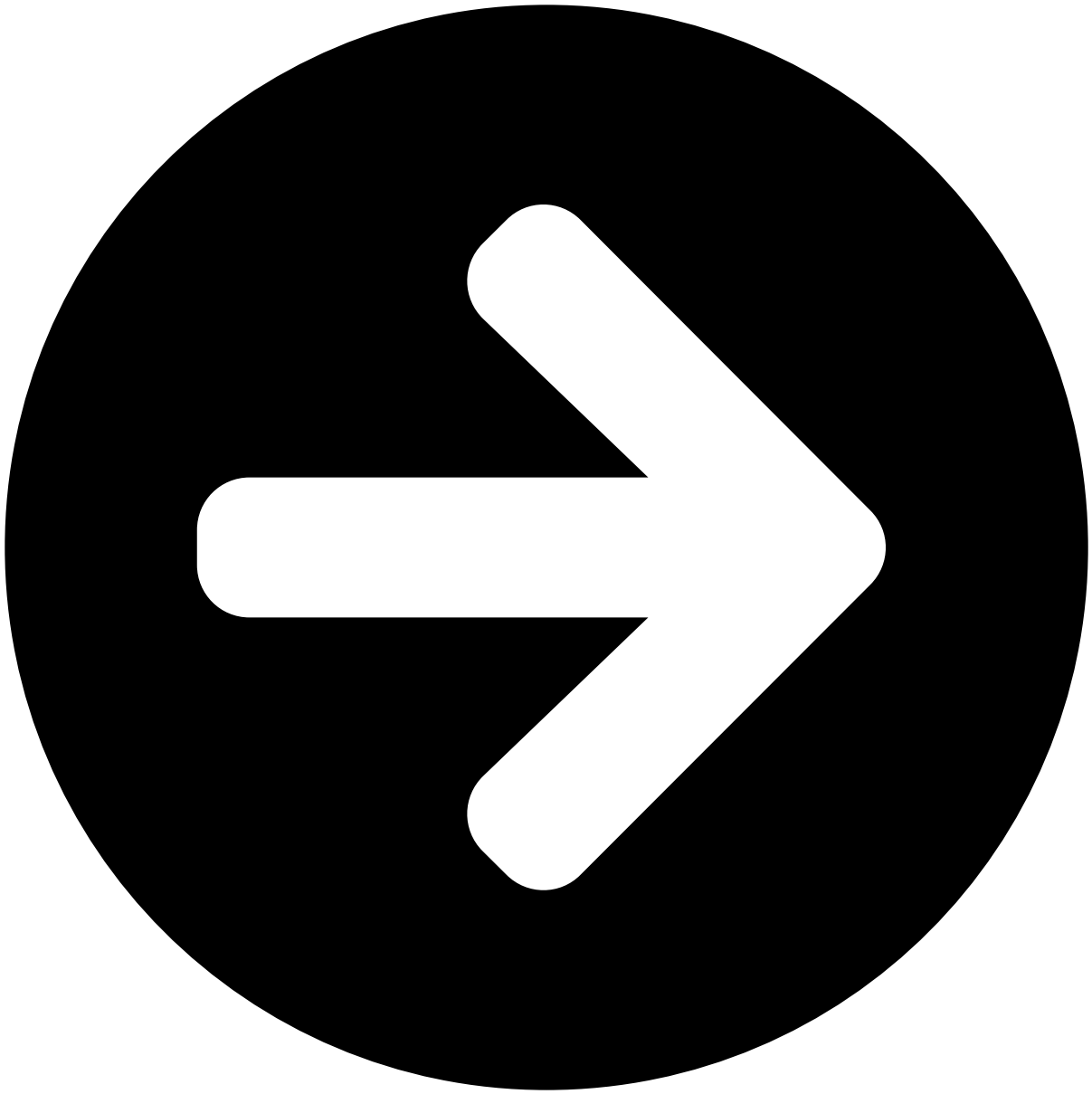
Our team at SpyCloud Labs keeps close tabs on the Chinese cybercrime ecosystem. Sign up to stay in the loop with our latest research.

Keep reading

Summer Cybercrime Trends, Recycled Leaks & Nefarious Nation-State Activity

July 7, 2025

From the “16 billion passwords” leak to trends in the Chinese criminal underground, our June cybercrime update breaks down the biggest cyber threats and news.

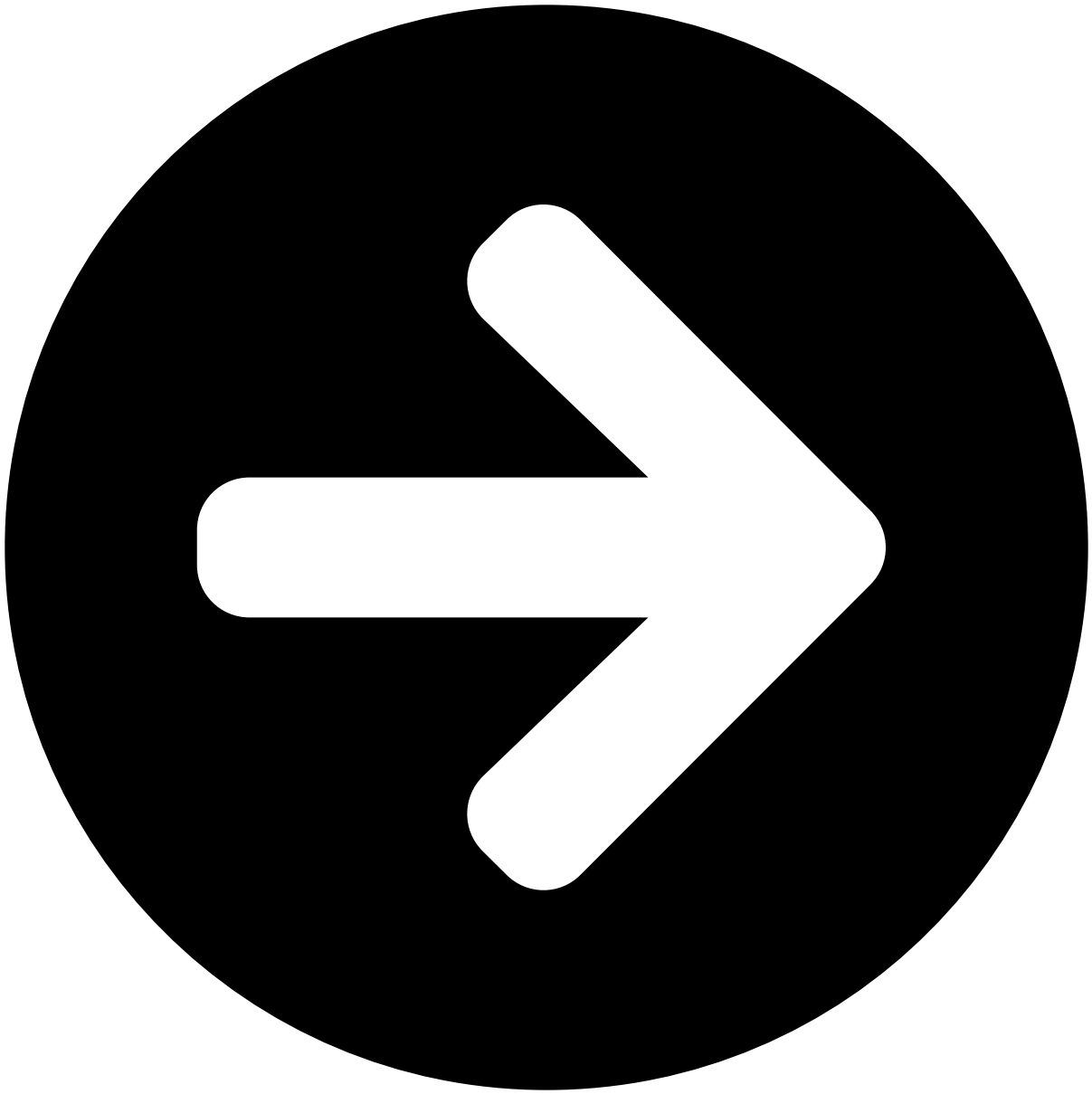


SpyCloud Labs

[What's Inside the Massive Chinese Data Leak]

June 18, 2025

With over 4 billion records, it's being dubbed the biggest leak of Chinese personal data ever. Here's what to know.

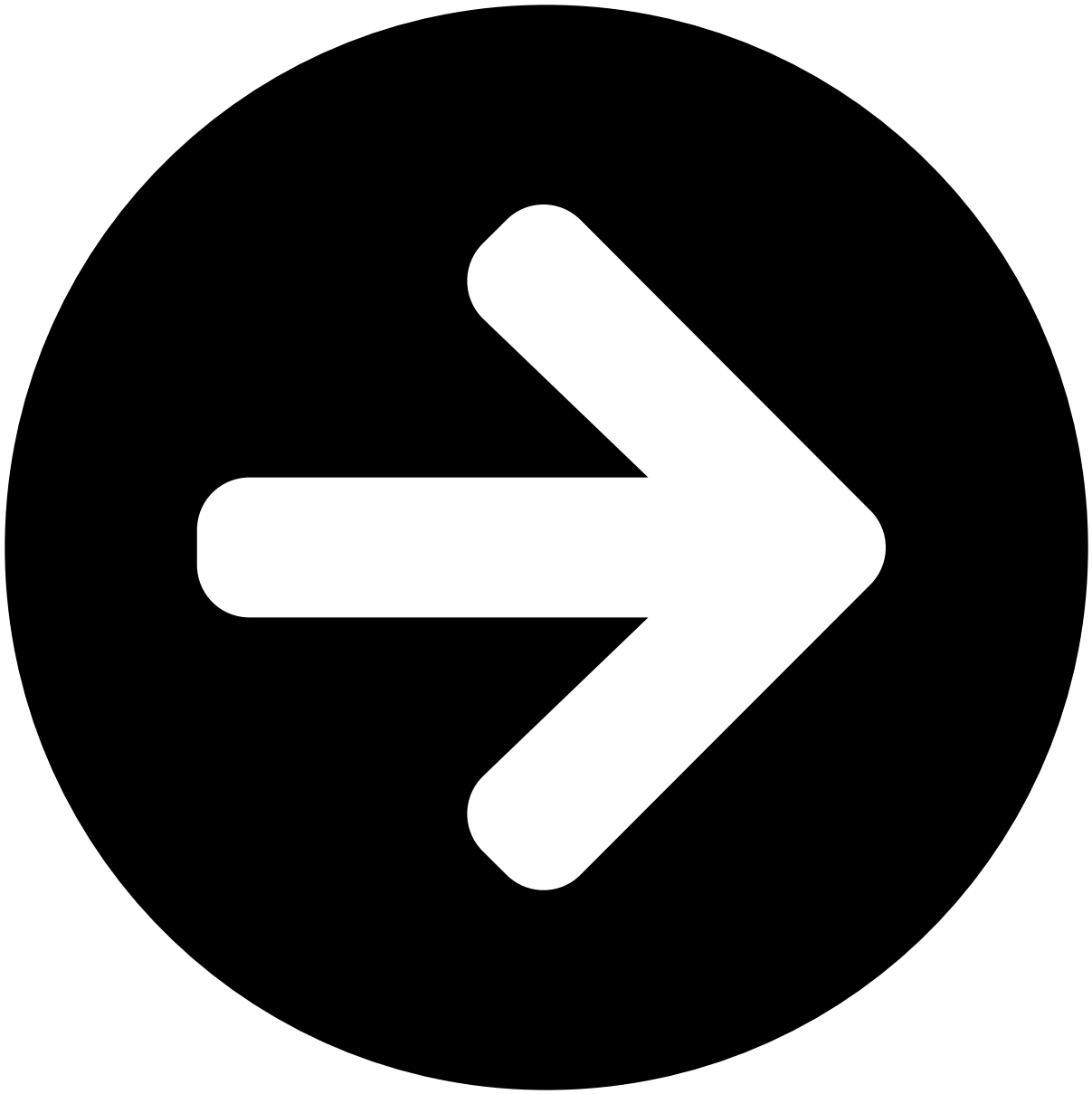


SpyCloud Labs

The LummaC2 Takedown, Attack Trends & Forum War Fighting

June 3, 2025

From the LummaC2 takedown to the BreachForums void, our May cybercrime update breaks down the biggest cyber threats & news.



SpyCloud Labs