China's Leading Cyber Security Firms Reveal Advanced Foreign Threat Groups; Identify Little Known Actors

Fusion (FS) | Cyber Espionage (CE)

October 25, 2022 10:34:00 AM, 22-00023954, Version: 1

Executive Summary

- Two China-based prominent cyber security firms recently revealed 60 foreign threat actors in public reporting.
- A combination of the two reports identified 18 advanced persistent threat (APT) groups that are either unknown or have limited coverage in Western reporting.
- Mandiant researched indicators of compromise (IOCs) associated with the groups (when available) to provide a partial Rosetta Stone between Qihoo 360 and Qi-ANXIN's naming conventions and Mandiant's tracked threat groups.

Threat Detail

Mandiant is providing a Rosetta Stone mapping internal, tracked espionage threat groups to open source reported advanced persistent threats (APTs) publicized by two China-based anti-virus and cyber security companies, Qihoo 360 and Qi-ANXI. These companies maintain threat intelligence divisions through the integration of security and incident response data to track global cyber threats primarily targeting China and their geographic locations. Of the total amount of threat actors revealed in public reporting, we identified 18 that are either unknown or have limited coverage in Western reporting.

Summary of Qihoo 360 and Qi-ANXIN Reports

In an online report for the first half of 2021, Qihoo 360 describes the foreign APT landscape as follows (summary):

- Overseas APT organizations continued to be active against China, increasing significantly compared with the same period last year. Qihoo 360 discovered 46 APT organizations from other countries and monitored more than 3,600 national-level cyberattacks against China.
- Twelve organizations were identified as being involved in attacks on China, two of which were discovered for the first time: APT-C-59 (Wuqiong Cave) and APT-C-60 (Pseudo Hunter).
- China's government, scientific research, and defense and military industries were the top-targeted industries. Among the most active against China are APT organizations from East Asia, South Asia, and Southeast Asia.
- Analysis of attacks on colleges and universities demonstrates that overseas APT groups are using the educational targets as a peripheral means to infiltrate China's defense industrial base and scientific and technology research institutes.

- During the rebound of the COVID-19 epidemic in South Asia and Southeast Asia, attacks on the medical, healthcare, and media industries became prominent.
- The attack surface of smart cities continues to expand, and the threat of APTs intensifies under the digital transformation of cities. The threat of ICT supply-chain attacks has further escalated.

Qihoo 360 identifies the top 10 cyber espionage threats to China, ranked by frequency of intrusions, the number of organizations and devices affected, as well as the sophistication of the intrusion group. One surprising revelation was North Korean "Kimsuky" appearing in the number seven position. The possibility exists that this is a Fallout Team.

Ranking	360 Named APT	Country of origin	Mandiant Name	Industries Targeted in China
1	APT-C-01 Poison Ivy □□□	Taiwan	Unknown	Government, Education, Scientific Research
2	APT-C-08 Creeping Vine Flower □□□	India	Hangover	Education, Military Industrial Base, Scientific Research
3	APT-C-00 Ocean Lotus □□□	Vietnam	APT32	Information and Communications Supplier, Government, Education
4	APT-C-06 Dark Hotel	South Korea	Fallout	Trade, Scientific Research, Media
5	APT-C-59 Wuqiong Cave □□□	Unknown	Unknown	Media, Scientific Research, Healthcare
6	APT-C-48 CNC	India	Unknown	Education, Scientific Research
7	APT-C-55 Kimsuky	North Korea	Kimsuky	Government
8	APT-C-60 Pseudo Hunters □□□	Unknown	Unknown	Trade, Government
9	APT-C-24 Sidewinder □□□	India	UNC1687	Government, Healthcare,
10	APT-C-47 Wang Thorn □□	Korean Peninsula	Unknown	Trade, Manufacturing, Construction

Table 1: Top 10 threats targeting China

Figure 1: Qihoo 360's geographic distribution of nation-state threat groups

The following is a partial Rosetta Stone that matches Qihoo 360 and Qi-ANXIN's IOCs to Mandiant tracked threat groups when the information was available. It should be noted that Mandiant does not track the IOCs attributed to these groups as a one-for-one match.

Qihoo 360 APT Designation	Qi-ANXIN	APT Country of Origin	APT English and Chinese Name	Mandiant APT Designator
APT-C-00	APT-Q-31	Vietnam	Ocean Lotus □□□	APT32
APT-C-01	APT-C-20	Taiwan	Poison Cloud Ivy □□□	Unknown
APT-C-03	None	North Korea	Onion Dog □□□	South Korean
APT-C-06	APT-Q-10	South Korea	Dark Hotel	Fallout UNC1136
APT-C-07	APT-Q-61	Middle East	Mermaid □□□	UNC722 TEMP[.]Lice
APT-C-08	APT-Q-37	India	Creeping Vine Flower □□□	Hangover
APT-C-09	APT-Q-36	India	□□□ Moha Grass	Hangover
APT-C-11	Fin-7	Russia	Carbanak	Fin-7
APT-C-12	APT-Q-21	Taiwan	Blue Mushroom □□□	Unknown
APT-C-13	APT-Q-79	Russia	Worm □□	Sandworm
APT-C-15	APT-Q-62	Middle East	Sphinx □□□	Unknown, deploying NJRAT
APT-C-16	APT-Q-93	U.S.	Sauron's Eye/Equation	

		NSA	Group □□□□	
APT-C-17	Unknown	India	Flying Shark □□	UNC2464 UNC2155 UNC1586
APT-C-20	APT-Q-76	Russia	Fancy Bear □□□	APT28
APT-C-23	Unknown	Middle East	Double Tailed Scorpion □□□	Molerats Hamas
APT-C-24	APT-Q-39	India	Sidewinder □□□	UNC1687
APT-C-25	APT29	Russia	APT29	APT29
APT-C-26	APT-Q-1 APT38	North Korea	Lazarus	APT38
APT-C-27	APT-Q-64	Middle East	Golden Rat □□□	UNC1124
APT-C-28	APT-Q-3	Korean Peninsula	Scarcruft Group123	APT37
APT-C-29	APT-Q-78	Russia	Turla	Turla
APT-C-30	APT -Q-32	Southeast Asia	Stalker □□□	Unknown
APT-C-31		Kazakhstan	Poison Needle □□	UNC1298
APT-C-32	Sandcat	Israel	Sandcat Qi-ANXIN attributes this activity to Uzbekistan	Unknown
APT-C-33	Unknown	Middle East	ArmaRat	Unknown
APT-C-34	APT-Q-90	Kazakhstan	Golden Flacon □□□	Unknown
APT-C-35	APT-Q-38	India	Stomach Worm □□□	Hangover
APT-C-36	APT-Q-98	South America	Blind Eagle □□□	UNC1080
APT-C-37	APT-Q-67	Middle East	Papa Bear □□□	Likely Syrian Electronic Army (mobile operation)
APT-C-38	APT-Q-66	Middle East	Saber Lion (Mobile malware)	Unknown
APT-C-39	Unknown	U.S. CIA	Vault7/Lamberts	
APT-C-40	APT-Q-91	U.S.	Equation □□□	

APT-C-41	Promethium	Turkey	Magic Blue Eye Evil Eye □□□□	Promethium, Strongpity Deploys RUDEBOY
APT-C-42	WellMess APT29	Russia	Wellmess Magic/Devil Mouse □□	APT29
APT-C-43	APT-Q-99	South America	Machete	UNC856 UNC3862
APT-C-44	North African Fox	Algeria	North African Fox □□□	Unknown Mobile Operation
APT-C-45	Unknown	India	Baby Elephant □□	UNC1502 UNC2800
APT-C-46	LPR	Ukraine	Luhansk □□□□	Unknown
APT-C-47	Wang Thorn	Korean Peninsula	Wang Thorn □□	Unknown
APT-C-48	Unknown	India	CNC	unknown
APT-C-50	Unknown	Iran	Domestic Kitten	UNC2104
APT-C-51	Unknown	Iran	APT35	APT35
	APT-Q-52	Iran	APT33	APT33
APT-C-53	InvisiMole APT-Q-82	Russia	Gamaredon	TEMP[.]Armageddon
APT-C-54	Unknown	Russia	UNC2452	APT29
APT-C-55	APT-Q-2	Korean Peninsula	Kimsuky	UNC1130
APT-C-56	Unknown	India	Transparent Tribe	APT36
APT-C-58	Unknown	Pakistan	Gorgon	Deploys FORMBOOK and NANOCORE
APT-C-59	Unknown	unknown	Wuqiong Cave □□□	Unknown
APT-C-60	Unknown	Unknown	Pseudo Hunters □□□	Unknown
APT-C-61	Unknown	Southeast Asia	Tengyun Snake □□□	Unknown
Unknown	APT-Q-54	Iran	Muddywater □□	TEMP[.]Zagros
Unknown	APT-Q-55	Iran	Charming Kitten	APT42
Unknown	Stealth Falcon	UAE	Stealth Falcon	Unknown
Unknown	APT-Q-57	Iran	Oilrig	APT34
Unknown	APT-Q-80	Russia	Energetic Bear	UNC2186/Koala
Unknown	GhostWriter	Russia	GhostWriter	UNC1151
Unknown	Triton	Russia	Triton	TEMP[.]Veles
Unknown	SlingShot	US	SlingShot	Unknown

Unknown	APT-Q-40 □□□ (MoLuoSuo) Aka Confucius	India	□□□ (MoLuoSuo) Aka Confucius	Unknown

Table 2: Partial Rosetta Stone

Reviewing the lists provided, there are 18 groups tracked under Qihoo 360 and Qi-ANXIN that are either unknown or have limited reporting in the Western press.

Qihoo 360 APT Groups	Qi-ANXIN APT Groups	Country/Region of Origin	Chinese Name
APT-C-01	APT-C-20	Taiwan	Poison Cloud Ivy □□□
APT-C-12	APT-Q-21	Taiwan	Blue Mushroom □□□
APT-C-15	APT-Q-62	Middle East	Sphinx □□□
APT-C-30	APT-Q-32	Southeast Asia	Stalker □□□
APT-C-32	Sandcat	Israel Qi-ANXIN attributes this activity to Uzbekistan	Sandcat
APT-C-33	Unknown	Middle East	ArmaRat
APT-C-34	APT-Q-90	Kazakhstan	Golden Flacon □□□
APT-C-38	APT-Q-66	Middle East	Saber Lion (Mobile malware)
APT-C-44	North African Fox	Algeria	North African Fox □□□
APT-C-46	LPR	Ukraine	Luhansk □□□□ Potentially related
APT-C-47	Wang Thorn	Korean Peninsula	Wang Thorn □□
APT-C-48	Unknown	India	CNC
APT-C-59	Unknown	unknown	Wuqiong Cave □□□
APT-C-60	Unknown	Unknown	Pseudo Hunters □□□

APT-C-61	Unknown	Southeast Asia	Tengyun Snake □□□
Unknown	SlingShot	US	SlingShot
Unknown	Stealth Falcon	UAE	Stealth Falcon
Unknown	APT-Q-40 □□□ (MoLuoSuo) Aka Confucius	India	□□□ (MoLuoSuo) Aka Confucius

Table 3: Unknown or limited Western reporting

Outlook and Implications

China's monitoring of foreign threat groups provides a broader view of the cyber espionage landscape and potentially new avenues for investigation. We also believe the Rosetta Stone will assist in follow-on analysis. In addition, it broadens the scope of targeting for groups that are currently tracked.

Please rate this product by taking a short four question survey

First Version Publish Date

October 25, 2022 10:34:00 AM

Version Information

Version:1.0, October 25, 2022 10:34:00 AM
China's Leading Cyber Security Firms Reveal Advanced Foreign Threat Groups; Identify Little Known Actors

5950 Berkshire Lane, Suite 1600 Dallas, TX

75225

For more information please visit: https://intelligence.fireeye.com/reports/22-00023954