# Ancient ICEFOG APT malware spotted again in new wave of attacks

By Catalin Cimpanu

Published: 2019-06-07 · Archived: 2026-04-05 21:13:53 UTC

Malware developed by Chinese state-sponsored hackers that was once thought to have disappeared has been recently spotted in new attacks, in an updated and more dangerous form.

Spotted by FireEye senior researcher Chi-en (Ashley) Shen, the malware is named ICEFOG (also known as Fucobha).

It was initially used by a Chinese APT (advanced persistent threat, a technical term for state-sponsored hacking units), also named ICEFOG, whose operations were first detailed in a Kaspersky report in September 2013.

Following the publication of that report, the ICEFOG group's activities stopped, and so have sightings of its eponymously named malware.

## New ICEFOG versions discovered

But in a presentation at a cyber-security conference in Poland this week, Shen said she discovered new and upgraded versions of the presumed-to-be-dead ICEFOG malware.

The two most important strains were ICEFOG-P and ICEFOG-M, spotted being used in attacks starting with 2014 and 2018, respectively.


ICEFOG new malware variants
Image: Shen, FireEye


ICEFOG-P new
Image: Shen, FireEye


ICEFOG-M new
Image: Shen, FireEye


ICEFOG malware timeline
Image: Shen, FireEye

Both ICEFOG strains were superior to the original ICEFOG malware sighted back in hacking campaigns in the early 2010s, suggesting that additional development has been done to bolster their capabilities.

Furthermore, Shen also found a Mac version of the ICEFOG malware, previously unseen.


ICEFOG for Mac

Image: Shen, FireEye

## ICEFOG now shared by multiple Chinese APTs

But these new ICEFOG malware variants were not being used in campaigns that could be associated with the original ICEFOG group. Instead, they were spotted across a large number of hacking campaigns orchestrated by different groups.

"The operations between 2011 and 2013 were pretty consistent, suggesting one group and an exclusive use of the malware," Shen told ZDNet in an email this week.

"The new variant was seemingly used by multiple groups after the 2013 campaign.

"I pivoted between the infrastructure from the campaign in 2013 and the new campaigns after 2014 and can't suggest a strong connection between them," she added.

It appears that ICEFOG evolved from a malware sample that was exclusively in the use of one Chinese hacking group into a tool now shared among many different APTs, each with its own agenda -- similar to how the Winnti group disolved and its Winnti malware was shared among different Chinese APTs in the past. Of course, this isn't a new theory, as cyber-security experts have previously pondered that many Chinese APTs may have a shared supply chain.

"It is unclear how the ICEFOG samples were shared, but we have seen tools shared among other China-nexus APT groups before," Shen said.

"An exploit document template has also been shared between several groups," the researcher added. "Also, other malware like SOGU is a commonly shared tool."

Shen said she spotted variants of the ICEFOG malware in attacks targeting:

- an unnamed agriculture company in Europe in 2015
- government, media, and finance organizations in Russia and Mongolia in 2015 (TOPNEWS campaign)
- the government of multiple former Soviet states in 2015 (Roaming Tiger)
- Kazach officials in 2016 (APPER campaign)
- water source provider, banks, and government entities in Turkey, India, Kazakhstan, Uzbekistan, and Tajikistan in 2018 (WATERFIGHT campaign)
- an unknown entity in the Philippines in 2018 (PHKIGHT campaign)
- organizations in Turkey and Kazakhstan in 2018 and 2019 (SKYLINE campaign)

ICEFOG attacks
Image: Shen, FireEye

ICEFOG actors
Image: Shen, FireEye

## ICEFOG used for cyber-espionage predominantly

"From my observation, most samples were [used] for political espionage and intelligence gathering," Shen told ZDNet.

"Some campaigns also targeted telecommunication, energy, media, transportation, and suspected financial sectors, presumably targeting intellectual property as well. However, we believe these are the minority of cases."

As to why new ICEFOG sightings haven't been reported, Shen also has a theory, suggesting that the malware wasn't detected because it very rarely used.

"The ICEFOG-P variant used between 2014 and 2018 is not particularly advanced," Shen told us. "The code is fairly simple and most samples were not even packed.

"The reason why the campaigns were not observed is probably because of the lower sample numbers between 2013 Q4 and 2017, especially compared to the campaign before 2013.

"In a case we observed in 2015, the actor seemed to leverage ICEFOG as a post-exploitation tool, which was deployed after the victim was compromised. As a result, a researcher would have to dig into the specific incident to find the ICEFOG connection.

"The variant ICEFOG-M, which appeared in 2019, used a file-less payload, making the campaign harder to track," Shen said.

The conclusion here is that the ICEFOG malware is now here to stay. After receiving so many updates over the past few years, and after proving successful in flying under the radar, Chinese cyber-espionage groups are most likely to continue using it for the foreseeable future.

Shen presented her findings at the CONFidence security conference that was held in Krakow, Poland, earlier this week. A copy of her presentation slides is available on SpeakerDeck. Indicators of compromise (IOCs) are also available.

### Related malware and cybercrime coverage:

- Hollywood lie: Bank hacks take months, not seconds
- 440 million Android users installed apps with an aggressive advertising plugin
- Germany: Backdoor found in four smartphone models; 20,000 users infected
- GandCrab ransomware operation says it's shutting down
- I2P network proposed as the next hiding spot for criminal operations
- A botnet is brute-forcing over 1.5 million RDP servers all over the world
- The dark web is smaller, and may be less dangerous, than we think **TechRepublic**
- Game of Thrones has the most malware of any pirated TV show **CNET**

---