# Lotus Blossom, Spring Dragon, Thrip





## APT group: Lotus Blossom, Spring Dragon, Thrip

| | |
|---|---|
| Names | Lotus Blossom *(Palo Alto)*<br>Spring Dragon *(Kaspersky)*<br>Dragonfish *(iDefense)*<br>Billbug *(Symantec)*<br>Thrip *(Symantec)*<br>Bronze Elgin *(SecureWorks)*<br>CTG-8171 *(SecureWorks)*<br>ATK 1 *(Thales)*<br>ATK 78 *(Thales)*<br>Red Salamander *(PWC)*<br>G0030 *(MITRE)*<br>G0076 *(MITRE)* |
| Country | China |
| Sponsor | State-sponsored |
| Motivation | Information theft and espionage |
| First seen | 2012 |
| Description | (Kaspersky) Spring Dragon is a long running APT actor that operates on a massive scale. The group has been running campaigns, mostly in countries and territories around the South China Sea, since as early as 2012. The main targets of Spring Dragon attacks are high profile governmental organizations and political parties, education institutions such as universities, as well as companies from the telecommunications sector.<br><br>Spring Dragon is known for spear phishing and watering hole techniques and some of its tools have previously been analyzed and reported on by security researchers, including Kaspersky Lab.<br><br>Operation Poisoned News, TwoSail Junk may be one of their campaigns. |
| Observed | Sectors: Aerospace, Defense, Education, Government, High-Tech, Satellites, Telecommunications.<br>Countries: ASEAN, Brunei, Cambodia, Hong Kong, Indonesia, Japan, Laos, Macao, Malaysia, Myanmar, Philippines, Singapore, Taiwan, Thailand, USA, Vietnam. |
| Tools used | Catchamas, Elise, Emissary, gpresult, Hannotog, Mimikatz, PsExec, Rikamanu, Sagerunex, Spedear, WMI Ghost, Living off the Land. |

| | | |
|---|---|---|
| Operations performed | Jun 2015 | Operation “Lotus Blossom”<br>Today Unit 42 published new research identifying a persistent cyber espionage campaign targeting government and military organizations in Southeast Asia. The adversary group responsible for the campaign, which we named “Lotus Blossom,” is well organized and likely state-sponsored, with support from a country that has interests in Southeast Asia. The campaign has been in operation for some time; we have identified over 50 different attacks taking place over the past three years.<br><https://unit42.paloaltonetworks.com/operation-lotus-blossom/> |
| | Nov 2015 | Attack on French Diplomat<br>We observed a targeted attack in November directed at an individual working for the French Ministry of Foreign Affairs. The attack involved a spear-phishing email sent to a single French diplomat based in Taipei, Taiwan and contained an invitation to a Science and Technology support group event.<br><https://unit42.paloaltonetworks.com/attack-on-french-diplomat-linked-to-operation-lotus-blossom/> |
| | Early 2017 | In the beginning of 2017, Kaspersky Lab became aware of new activities by an APT actor we have been tracking for several years called Spring Dragon (also known as LotusBlossom).<br>Information about the new attacks arrived from a research partner in Taiwan and we decided to review the actor’s tools, techniques and activities.<br>Using Kaspersky Lab telemetry data we detected the malware in attacks against some high-profile organizations around the South China Sea.<br><https://securelist.com/spring-dragon-updated-activity/79067/> |
| | Jan 2018 | Attacks on Association of South East Asian Nations (ASEAN) countries<br>During the last weeks of January (2018), nation state actors from Lotus Blossom conducted a targeted malware spam campaign against the Association of South East Asian Nations (ASEAN) countries.<br><https://community.rsa.com/community/products/netwitness/blog/2018/02/13/lotus-blossom-continues-asean-targeting><br><https://www.accenture.com/t20180127T003755Z_w_/us-en/_acnmedia/PDF-46/Accenture-Security-Dragonfish-Threat-Analysis.pdf> |
| | Jan 2018 | Back in January 2018, TAA triggered an alert at a large telecoms operator in Southeast Asia.<br><https://www.symantec.com/blogs/threat-intelligence/thrip-hits-satellite-telecoms-defense-targets> |
| | Jun 2018 | Since Symantec first exposed the Thrip group in 2018, the stealthy China-based espionage group has continued to mount attacks in South East Asia, hitting military organizations, satellite communications operators, and a diverse range of other targets in the region.<br><https://www.symantec.com/blogs/threat-intelligence/thrip-apt-south-east-asia> |
| | Mar 2022 | Billbug: State-sponsored Actor Targets Cert Authority, Government Agencies in Multiple Asian Countries |

| | | |
|---|---|---|
| | | <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/espionage-asia-governments-cert-authority> |
| | Aug 2024 | Billbug: Intrusion Campaign Against Southeast Asia Continues <https://www.security.com/threat-intelligence/billbug-china-espionage> |
| Information | <https://blog.talosintelligence.com/lotus-blossom-espionage-group/> | |
| MITRE ATT&CK | <https://attack.mitre.org/groups/G0030/><br><https://attack.mitre.org/groups/G0076/> | |

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format

---