# Stone Panda, APT 10, menuPass





## APT group: Stone Panda, APT 10, menuPass

| | |
|---|---|
| Names | Stone Panda *(CrowdStrike)*<br>APT 10 *(Mandiant)*<br>menuPass Team *(Symantec)*<br>menuPass *(Palo Alto)*<br>Red Apollo *(PWC)*<br>CVNX *(BAE Systems)*<br>Potassium *(Microsoft)*<br>Hogfish *(iDefense)*<br>Happyyongzi *(FireEye)*<br>Cicada *(Symantec)*<br>Bronze Riverside *(SecureWorks)*<br>CTG-5938 *(SecureWorks)*<br>ATK 41 *(Thales)*<br>TA429 *(Proofpoint)*<br>ITG01 *(IBM)*<br>Granite Taurus *(Palo Alto)*<br>Earth Kasha *(Trend Micro)*<br>Cuckoo Spear *(Cybereason)*<br>Purple Typhoon *(Microsoft)*<br>G0045 *(MITRE)*<br>G0093 *(MITRE)* |
| Country | China |
| Sponsor | State-sponsored, Tianjin bureau of the Chinese Ministry of State Security, Huaying Haitai |
| Motivation | Information theft and espionage |
| First seen | 2006 |
| Description | menuPass is a threat group that appears to originate from China and has been active since approximately 2009. The group has targeted healthcare, defense, aerospace, and government sectors, and has targeted Japanese victims since at least 2014. In 2016 |

| | | |
|---|---|---|
| | and 2017, the group targeted managed IT service providers, manufacturing and mining companies, and a university.<br><br>Also see Operation LiberalFace, MirrorFace and Twisted Panda. | |
| Observed | Sectors: Aerospace, Defense, Energy, Financial, Government, Healthcare, High-Tech, IT, Media, NGOs, Pharmaceutical, Telecommunications and MSPs.<br>Countries: Australia, Belgium, Brazil, Canada, China, Finland, France, Germany, Hong Kong, India, Israel, Italy, Japan, Montenegro, Netherlands, Norway, Philippines, Singapore, South Africa, South Korea, Sweden, Switzerland, Taiwan, Thailand, Turkey, UAE, UK, USA, Vietnam. | |
| Tools used | Anel, BloodHound, certutil, ChChes, China Chopper, Cobalt Strike, Derusbi, DILLJUICE, DILLWEED, Ecipekac, Emdivi, EvilGrab RAT, Gh0st RAT, HTran, Impacket, Invoke the Hash, LODEINFO, Mimikatz, MiS-Type, nbtscan, NOOPDOOR, P8RAT, PlugX, Poison Ivy, Poldat, PowerSploit, PowerView, PsExec, PsList, pwdump, Quarks PwDump, QuasarRAT, RedLeaves, Rubeus, SharpSploit, SodaMaster, SNUGRIDE, Trochilus RAT, WinRAR, WmiExec, Living off the Land. | |
| Operations performed | Sep 2016 | Spear-phishing attack<br>Method: The attackers spoofed several sender email addresses to send spear-phishing emails, most notably public addresses associated with the Sasakawa Peace Foundation and The White House.<br>Target: Japanese academics working in several areas of science, along with Japanese pharmaceutical and a US-based subsidiary of a Japanese manufacturing organizations.<br><https://unit42.paloaltonetworks.com/unit42-menupass-returns-new-malware-new-attacks-japanese-academics-organizations/> |
| | 2016 | Operation “Cloud Hopper”<br>The campaign, which we refer to as Operation Cloud Hopper, has targeted managed IT service providers (MSPs), allowing APT10 unprecedented potential access to the intellectual property and sensitive data of those MSPs and their clients globally. A number of Japanese organizations have also been directly targeted in a separate, simultaneous campaign by the same actor<br><https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-report-final-v4.pdf><br><https://www.reuters.com/investigates/special-report/china-cyber-cloudhopper/><br><https://www.wsj.com/articles/ghosts-in-the-clouds-inside-chinas-major-corporate-hack-11577729061> |

| | |
|---|---|
| 2016/2017 | Leveraging its global footprint, FireEye has detected APT10 activity across six continents in 2016 and 2017. APT10 has targeted or compromised manufacturing companies in India, Japan and Northern Europe; a mining company in South America; and multiple IT service providers worldwide. We believe these companies are a mix of final targets and organizations that could provide a foothold in a final target. <https://www.fireeye.com/blog/threat-research/2017/04/apt10_menupass_grou.html> |
| Feb 2017 | Operation “TradeSecret”<br>The National Foreign Trade Council (NFTC) website was allegedly infiltrated by Chinese nation-state threat actors, according to a new report from Fidelis Cybersecurity. The attack against the NFTC site has been dubbed ‘Operation TradeSecret’ by Fidelis and is seen as an attempt to gain insight into individuals closely associated with U.S trade policy activities.<br><https://www.eweek.com/security/chinese-nation-state-hackers-target-u.s-in-operation-tradesecret> |
| 2017 | Operation “ChessMaster”<br>Take for instance the self-named ChessMaster, a campaign targeting Japanese academe, technology enterprises, media outfits, managed service providers, and government agencies. It employs various poisoned pawns in the form of malware-laden spear-phishing emails containing decoy documents.<br><https://blog.trendmicro.com/trendlabs-security-intelligence/chessmaster-cyber-espionage-campaign/> |
| 2017 | Operation “Soft Cell”<br>Earlier this year, Cybereason identified an advanced, persistent attack targeting telecommunications providers that has been underway for years, soon after deploying into the environment.<br>The threat actor was attempting to steal all data stored in the active directory, compromising every single username and password in the organization, along with other personally identifiable information, billing data, call detail records, credentials, email servers, geo-location of users, and more.<br><https://www.cybereason.com/blog/operation-soft-cell-a-worldwide-campaign-against-telecommunications-providers> |
| Nov 2017 | Targeted Norwegian MSP and US Companies in Sustained Campaign<br>A sustained cyberespionage campaign targeting at least three companies in the United States and Europe was uncovered by Recorded Future and Rapid7 between November 2017 and September |

| | |
|---|---|
| | 2018.<br><https://go.recordedfuture.com/hubfs/reports/cta-2019-0206.pdf> |
| 2018 | Operation “New Battle”<br>This report provides a technical overview of the bespoke RedLeaves implants leveraged by the actor in their “new battle” campaign.<br><https://www.accenture.com/t20180423T055005Z_w_/se-en/_acnmedia/PDF-76/Accenture-Hogfish-Threat-Analysis.pdf><br><https://www.us-cert.gov/sites/default/files/publications/IR-ALERT-MED-17-093-01C-Intrusions_Affecting_Multiple_Victims_Across_Multiple_Sectors.pdf> |
| Jul 2018 | Attack on the Japanese media sector<br>In July 2018, FireEye devices detected and blocked what appears to be APT10 (menuPass) activity targeting the Japanese media sector.<br><https://www.fireeye.com/blog/threat-research/2018/09/apt10-targeting-japanese-corporations-using-updated-ttps.html> |
| Jan 2019 | Breach of Airbus<br><https://www.mirror.co.uk/travel/news/breaking-airbus-cyber-attack-believed-13955680> |
| Mar 2019 | Operation “A41APT”<br><https://securelist.com/apt10-sophisticated-multi-layered-loader-ecipekac-discovered-in-a41apt-campaign/101519/><br><https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/cicada-apt10-japan-espionage> |
| Apr 2019 | In April 2019, enSilo detected what it believes to be new activity by Chinese cyber espionage group APT10. The variants discovered by enSilo are previously unknown and deploy malware that is unique to the threat actor.<br><https://blog.ensilo.com/uncovering-new-activity-by-apt10> |
| Oct 2019 | Japan-Linked Organizations Targeted in Long-Running and Sophisticated Attack Campaign<br><https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/cicada-apt10-japan-espionage> |
| Feb 2021 | Chinese hackers target Indian vaccine makers SII, Bharat Biotech, says security firm<br><https://www.cnbctv18.com/healthcare/chinese-hackers-target-indian-vaccine-makers-sii-bharat-biotech-says-security-firm-8461981.htm> |
| Apr 2021 | Operation “Cuckoo Spear”<br>CUCKOO SPEAR Part 1: Analyzing NOOPDOOR from an IR |

| | | |
|---|---|---|
| | | Perspective <https://www.cybereason.com/blog/cuckoo-spear-analyzing-noopdoor> <https://www.cybereason.com/blog/cuckoo-spear-pt2-threat-actor-arsenal> |
| | Nov 2021 | Operation “Cache Panda” A hacking group affiliated with the Chinese government is believed to have carried out a months-long attack against Taiwan’s financial sector by leveraging a vulnerability in a security software solution used by roughly 80% of all local financial organizations. <https://therecord.media/chinese-hackers-linked-to-months-long-attack-on-taiwanese-financial-sector/> |
| | Feb 2022 | Cicada: Chinese APT Group Widens Targeting in Recent Espionage Activity <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/cicada-apt10-china-ngo-government-attacks> |
| | Early 2023 | Spot the Difference: Earth Kasha's New LODEINFO Campaign And The Correlation Analysis With The APT10 Umbrella <https://www.trendmicro.com/en_us/research/24/k/lodeinfo-campaign-of-earth-kasha.html> |
| | Jun 2024 | Guess Who’s Back - The Return of ANEL in the Recent Earth Kasha Spear-phishing Campaign in 2024 <https://www.trendmicro.com/en_us/research/24/k/return-of-anel-in-the-recent-earth-kasha-spearphishing-campaign.html> |
| | Mar 2025 | Earth Kasha Updates TTPs in Latest Campaign Targeting Taiwan and Japan <https://www.trendmicro.com/en_us/research/25/d/earth-kasha-updates-ttps.html> |
| Counter operations | Dec 2018 | Chinese Hackers Indicted <https://www.fbi.gov/news/stories/chinese-hackers-indicted-122018> <https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-announces-charges-against-chinese-hackers> |
| | Jul 2020 | EU imposes the first ever sanctions against cyber-attacks <https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/> |
| Information | <https://intrusiontruth.wordpress.com/2018/08/15/apt10-was-managed-by-the-tianjin-bureau-of-the-chinese-ministry-of-state-security/> | |

| | |
|---|---|
| | <https://www.carbonblack.com/2019/02/25/defeating-compiler-level-obfuscations-used-in-apt10-malware/><br><https://adeo.com.tr/wp-content/uploads/2020/02/APT10_v1.2_public.pdf><br><https://exchange.xforce.ibmcloud.com/threat-group/706490628c8aa20a8a3a6e5ec81ca49b><br><https://en.wikipedia.org/wiki/Red_Apollo> |
| MITRE ATT&CK | <https://attack.mitre.org/groups/G0045/><br><https://attack.mitre.org/groups/G0093/> |
| Playbook | <https://pan-unit42.github.io/playbook_viewer/?pb=granite-taurus> |

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format

---