Tropic Trooper, Pirate Panda, APT 23, KeyBoy

Archived: 2026-04-02 11:36:17 UTC

NamesTropic Trooper *(Trend Micro)*
Pirate Panda *(CrowdStrike)*
APT 23 *(Mandiant)*
Iron *(Microsoft)*
KeyBoy *(Rapid7)*
Bronze Hobart *(SecureWorks)*
Earth Centaur *(Trend Micro)*
G0081 *(MITRE)* Country China SponsorState-sponsored MotivationInformation theft and espionage First seen2011 DescriptionTropic Trooper is an unaffiliated threat group that has led targeted campaigns against targets in Taiwan, the Philippines, and Hong Kong. Tropic Trooper focuses on targeting government, healthcare, transportation, and high-tech industries and has been active since 2011. ObservedSectors: Defense, Government, Healthcare, High-Tech, Transportation.
Countries: Hong Kong, India, Malaysia, Philippines, Taiwan, Tibet, Vietnam and Middle East. Tools used8.t Dropper, ByPassGodzilla, China Chopper, CREDRIVER, fscan, KeyBoy, Neo-reGeorg, PCShare, Poison Ivy, ShadowPad Winnti, Swor, Titan, USBferry, Yahoyah, Winsloader. Operations performed2012Operation “Tropic Trooper”
Taiwan and the Philippines have become the targets of an ongoing campaign called “Operation Tropic Trooper.” Active since 2012, the attackers behind the campaign have set their sights on the Taiwanese government as well as a number of companies in the heavy industry. The same campaign has also targeted key Philippine military agencies.
<https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-operation-tropic-trooper.pdf> Jun 2013KeyBoy, Targeted Attacks against Vietnam and India
<https://blog.rapid7.com/2013/06/07/keyboy-targeted-attacks-against-vietnam-and-india/> 2014New Strategy
Tropic Trooper (also known as KeyBoy) levels its campaigns against Taiwanese, Philippine, and Hong Kong targets, focusing on their government, healthcare, transportation, and high-tech industries.
<https://blog.trendmicro.com/trendlabs-security-intelligence/tropic-trooper-new-strategy/> Dec 2014We found that Tropic Trooper’s latest activities center on targeting Taiwanese and the Philippine military’s physically isolated networks through a USBferry attack (the name derived from a sample found in a related research). We also observed targets among military/navy agencies, government institutions, military hospitals, and even a national bank. The group employs USBferry, a USB malware that performs different commands on specific targets, maintains stealth in environments, and steals critical data through USB storage.
<https://blog.trendmicro.com/trendlabs-security-intelligence/tropic-troopers-back-usbferry-attack-targets-air-gapped-environments/> Mar 2015Throughout March to May 2015, our researchers noted that 62% of the Tropic Trooper-related malware infections targeted Taiwanese organizations while the remaining 38% zoned in on Philippine entities.
<https://blog.trendmicro.com/trendlabs-security-intelligence/operation-tropic-trooper-old-vulnerabilities-still-pack-a-punch/> Aug 2016In early August, Unit 42 identified two attacks using similar techniques. The more

interesting one was a targeted attack towards the Secretary General of Taiwan's Government office – Executive Yuan. The Executive Yuan has several individual boards which are formed to enforce different executing functions of the government. The Executive Yuan Council evaluates statutory and budgetary bills and bills concerning martial law, amnesty, declaration of war, conclusion of peace and treaties, and other important affairs. <https://unit42.paloaltonetworks.com/unit42-tropic-trooper-targets-taiwanese-government-and-fossil-fuel-provider-with-poison-ivy/> Aug 2016KeyBoy and the targeting of the Tibetan Community <https://citizenlab.ca/2016/11/parliament-keyboy/> Feb 2017The KeyBoys are back in town <https://www.pwc.co.uk/issues/cyber-security-data-privacy/research/the-keyboys-are-back-in-town.html> 2017Tropic Trooper goes mobile with Titan surveillanceware

The latest threat to follow this trend is Titan, a family of sophisticated Android surveillanceware apps surfaced by Lookout's automated analysis that, based on command and control infrastructure, is linked to the same actors behind Operation Tropic Trooper.

<https://blog.lookout.com/titan-mobile-threat> Early 2020Ongoing PIRATE PANDA Operations Using Current Event Themes to DeployPoison Ivy <https://www.scribd.com/document/451284814/CrowdStrike-Ongoing-Pirate-Panda-operations-using-current-event-themes> Apr 2020The Anomali Threat Research Team detected a spear phishing email targeting government employees in the Municipality of Da Nang, Vietnam. <https://www.anomali.com/blog/anomali-suspects-that-china-backed-apt-pirate-panda-may-be-seeking-access-to-vietnam-government-data-center#When:15:00:00Z> Jul 2020Collecting In the Dark: Tropic Trooper Targets Transportation and Government <https://www.trendmicro.com/en_us/research/21/l/collecting-in-the-dark-tropic-trooper-targets-transportation-and-government-organizations.html> Jun 2023Tropic Trooper spies on government entities in the Middle East <https://securelist.com/new-tropic-trooper-web-shell-infection/113737/> Information<https://blogs.cisco.com/security/scope-of-keyboy-targeted-malware-attacks> MITRE ATT&CK<https://attack.mitre.org/groups/G0081/>

Source: https://apt.etda.or.th/cgi-bin/showcard.cgi?u=dcba8f16-98e2-4d31-b7db-f4f1bdbfdb56