Bronze Butler, Tick, RedBaldNight, Stalker Panda

Archived: 2026-04-05 15:24:52 UTC

APT group: Bronze Butler, Tick, RedBaldNight, Stalker Panda

Names	Bronze Butler *(SecureWorks)* CTG-2006 *(SecureWorks)* Tick *(Symantec)* TEMP.Tick *(FireEye)* RedBaldNight *(Trend Micro)* Stalker Panda *(Crowdstrike)* Stalker Taurus *(Palo Alto)* Swirl Typhoon *(Microsoft)* G0060 *(MITRE)*
Country	China
Sponsor	State-sponsored, National University of Defense and Technology
Motivation	Information theft and espionage
First seen	2006
Description	(SecureWorks) CTU analysis indicates that Bronze Butler primarily targets organizations located in Japan. The threat group has sought unauthorized access to networks of organizations associated with critical infrastructure, heavy industry, manufacturing, and international relations. Secureworks analysts have observed Bronze Bulter exfiltrating the following categories of data: • Intellectual property related to technology and development • Product specification • Sensitive business and sales-related information • Network and system configuration files • Email messages and meeting minutes The focus on intellectual property, product details, and corporate information suggests that the group seeks information that they believe might be of value to competing organizations. The diverse targeting suggests that Bronze Bulter may be tasked by multiple teams or organizations with varying priorities.

Observed	Sectors: Critical infrastructure, Defense, Engineering, Government, High-Tech, Industrial, Manufacturing, Media, Technology and International relations. Countries: China, Hong Kong, Japan, Russia, Singapore, South Korea, Taiwan, USA.	
Tools used	9002 RAT, 8.t Dropper, Blogspot, Daserf, Datper, Elirks, Gh0st RAT, gsecdump, HomamDownloader, Lilith RAT, Mimikatz, Minzen, rarstar, ShadowPad Winnti, SymonLoader, Windows Credentials Editor.	
Operations performed	Jul 2015	Symantec discovered the most recent wave of Tick attacks in July 2015, when the group compromised three different Japanese websites with a Flash (.swf) exploit to mount watering hole attacks. Visitors to these websites were infected with a downloader known as Gofarer (Downloader.Gofarer). Gofarer collects information about the compromised computer and then downloads and installs Daserf. <https://www.symantec.com/connect/blogs/tick-cyberespionage-group-zeros-japan>
	Apr 2017	Wali is a backdoor used for targeted attacks. It gathers information about the compromised machines and their networks, in addition to stealing sensitive information and credentials. Wali's operators use this information to move laterally in an organization and compromise more machines. <https://www.cybereason.com/blog/labs-shadowwali-new-variant-of-the-xxmm-family-of-backdoors>
	Nov 2017	Daserf's infection chain accordingly evolved, as shown below. It has several methods for infecting its targets of interest: spear phishing emails, watering hole attacks, and exploiting a remote code execution vulnerability (CVE-2016-7836, patched last March 2017) in SKYSEA Client View, an IT asset management software widely used in Japan. <https://blog.trendmicro.com/trendlabs-security-intelligence/redbaldknight-bronze-butler-daserf-backdoor-now-using-steganography/>
	Jun 2018	Tick Group Weaponized Secure USB Drives to Target Air-Gapped Critical Systems <https://unit42.paloaltonetworks.com/unit42-tick-group-weaponized-secure-usb-drives-target-air-gapped-critical-systems/>
	2019	Operation "ENDTRADE" By the first half of 2019, we found that the group was able to zero in on specific industries in Japan from which it could steal proprietary information and classified data. We named this campaign "Operation

		ENDTRADE," based on its targets. <https://documents.trendmicro.com/assets/pdf/Operation-ENDTRADE-TICK-s-Multi-Stage-Backdoors-for-Attacking-Industries-and-Stealing-Classified-Data.pdf>
	Jun 2019	Breach of Mitsubishi Electric <https://www.zdnet.com/article/mitsubishi-electric-discloses-security-breach-china-is-main-suspect/>
	Feb 2021	Exchange servers under siege from at least 10 APT groups <https://www.welivesecurity.com/2021/03/10/exchange-servers-under-siege-10-apt-groups/>
	Mar 2021	The slow Tick-ing time bomb: Tick APT group compromise of a DLP software developer in East Asia <https://www.welivesecurity.com/2023/03/14/slow-ticking-time-bomb-tick-apt-group-dlp-software-developer-east-asia/> <https://asec.ahnlab.com/en/51340/>
Counter operations	Apr 2021	Tokyo police referred a Chinese man, who is a member of the Chinese Communist Party, to prosecutors Tuesday over his alleged involvement in the cyberattacks, they said. <https://www.japantimes.co.jp/news/2021/04/20/national/chinese-military-japan-cyberattacks/>
Information	<https://www.secureworks.com/research/bronze-butler-targets-japanese-businesses> <https://blog.trendmicro.com/trendlabs-security-intelligence/redbaldknight-bronze-butler-daserf-backdoor-now-using-steganography/> <https://unit42.paloaltonetworks.com/unit42-tick-group-continues-attacks/> <https://blog.talosintelligence.com/2018/10/tracking-tick-through-recent-campaigns.html> <https://wikileaks.org/vault7/document/2015-08-20150814-256-CSIR-15005-Stalker-Panda/2015-08-20150814-256-CSIR-15005-Stalker-Panda.pdf>	
MITRE ATT&CK	<https://attack.mitre.org/groups/G0060/>	
Playbook	<https://pan-unit42.github.io/playbook_viewer/?pb=stalkertaurus>	

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format

Source: https://apt.etda.or.th/cgi-bin/showcard.cgi?u=334d9e0e-dab2-4bc5-8db2-5ab016f36947