Tonto Team, HartBeat, Karma Panda

APT group: Tonto Team, HartBeat, Karma Panda

Names	Tonto Team *(FireEye)* HeartBeat *(Trend Micro)* Karma Panda *(CrowdStrike)* CactusPete *(Kaspersky)* Bronze Huntley *(SecureWorks)* Earth Akhlut *(Trend Micro)* LoneRanger *(?)* TAG-74 *(Recorded Future)* G0131 *(MITRE)*
Country	China
Sponsor	State-sponsored, Shenyang Military Region Technical Reconnaissance Bureau, possibly Unit 65017
Motivation	Information theft and espionage
First seen	2009
Description	(Trend Micro) The first HeartBeat campaign remote access tool (RAT) component was discovered in June 2012 in a Korean newspaper company network. Further investigation revealed that the campaign has been actively distributing their RAT component to their targets in 2011 and the first half of 2012. Furthermore, we uncovered one malware component that dates back to November 2009. This indicates that the campaign started during that time or earlier. The HeartBeat campaign appears to target government organizations and institutions or communities that are in some way related to the South Korean government. Specifically, we were able to identify the following targets: • Political parties • Media outfits • A national policy research institute • A military branch of South Korean armed forces

	• A small business sector organization • Branches of South Korean government The profile of their targets suggests that the motive behind the campaign may be politically motivated. (Kaspersky) The actor has quite likely relied on much the same codebase and implant variants for the past six years. However these have broadened substantially since 2018. The group spear-phishes its targets, deploys Word and Equation Editor exploits and an appropriated/repackaged DarkHotel VBScript zero-day, delivers modified and compiled unique Mimikatz variants, GSEC and WCE credential stealers, a keylogger, various Escalation of Privilege exploits, various older utilities and an updated set of backdoors, and what appear to be new variants of custom downloader and backdoor modules.	
Observed	Sectors: Defense, Financial, Government, IT, Media. Countries: India, Japan, Mongolia, Russia, South Korea, Taiwan, USA and Eastern Europe.	
Tools used	8.t Dropper, Bioazih, Bisonal, Dexbia, DoubleT, Flapjack, Mimikatz, ShadowPad Winnti, Living off the Land.	
Operations performed	Nov 2009	Operation “Bitter Biscuit” <https://asec.ahnlab.com/1078>
	Feb 2017	FireEye's director of cyber-espionage analysis John Hultquist told the Wall Street Journal that FireEye had detected a surge in attacks against South Korean targets from China since February, when South Korea announced it would deploy THAAD in response to North Korean missile tests. <https://arstechnica.com/information-technology/2017/04/researchers-claim-china-trying-to-hack-south-korea-missile-defense-efforts/>
	Mar 2019	CactusPete APT group’s updated Bisonal backdoor The backdoor was used to target financial and military organizations in Eastern Europe <https://securelist.com/cactuspete-apt-groups-updated-bisonal-backdoor/97962/>
	Late 2019	At the end of 2019 the group seemed to shift towards a heavier focus on Mongolian and Russian organizations. <https://securelist.com/apt-trends-report-q1-2020/96826/>
	Dec 2019	In this campaign, the CactusPete threat actor used a new method to drop an updated version of the DoubleT backdoor onto the computers.

		<https://securelist.com/apt-trends-report-q2-2020/97937/>
	2020	Multi-year Chinese APT Campaign Targets South Korean Academic, Government, and Political Entities <https://go.recordedfuture.com/hubfs/reports/cta-2023-0919.pdf>
	Mar 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/>
	Jun 2022	Nice Try Tonto Team <https://www.group-ib.com/blog/tonto-team/>
	Apr 2023	Tonto Team Using Anti-Malware Related Files for DLL Side-Loading <https://asec.ahnlab.com/en/51746/>
Information	<https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp_the-heartbeat-apt-campaign.pdf> <https://securelist.com/apt-trends-report-q1-2019/90643/> <https://www.fireeye.com/content/dam/fireeye-www/summit/cds-2019/presentations/cds19-executive-s08-achievement-unlocked.pdf> <https://blog.talosintelligence.com/2020/03/bisonal-10-years-of-play.html>	
MITRE ATT&CK	<https://attack.mitre.org/groups/G0131/>	

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
