Emissary Panda, APT 27, LuckyMouse, Bronze Union

Archived: 2026-04-05 23:17:53 UTC

APT group: Emissary Panda, APT 27, LuckyMouse, Bronze Union

Names	Emissary Panda *(CrowdStrike)* APT 27 *(Mandiant)* LuckyMouse *(Kaspersky)* Bronze Union *(Secureworks)* TG-3390 *(SecureWorks)* TEMP.Hippo *(Symantec)* Budworm *(Symantec)* Group 35 *(Talos)* ATK 15 *(Thales)* Iron Tiger *(Trend Micro)* Earth Smilodon *(Trend Micro)* Red Phoenix *(PWC)* ZipToken *(?)* Iron Taurus *(Palo Alto)* Circle Typhoon *(Microsoft)* Linen Typhoon *(Microsoft)* G0027 *(MITRE)*	
Country	China	
Motivation	Information theft and espionage	
First seen	2010	
Description	Threat Group-3390 is a Chinese threat group that has extensively used strategic Web compromises to target victims. The group least 2010 and has targeted organizations in the aerospace, government, defense, technology, energy, and manufacturing sector Emissary Panda has some overlap with Turbine Panda, APT 26, Shell Crew, WebMasters, KungFu Kittens and possibly UNC2 This actor worked together with TA428 in Operation StealthyTrident.	
Observed	Sectors: Aerospace, Aviation, Defense, Education, Embassies, Government, Manufacturing, Technology, Telecommunications, Countries: Australia, Canada, China, Germany, Hong Kong, India, Iran, Israel, Japan, Mongolia, Philippines, Russia, Spain, Sc Thailand, Tibet, Turkey, UK, USA and Middle East.	
Tools used	Antak, ASPXSpy, China Chopper, Gh0st RAT, gsecdump, HTTPBrowser, HTran, Hunter, HyperBro, Mimikatz, Nishang, Owa PsExec, SysUpdate, TwoFace, Windows Credentials Editor, ZXShell, Living off the Land.	
Operations performed	2010	Operation “Iron Tiger” Operation Iron Tiger is a targeted attack campaign discovered to have stolen trillions of data from defense co including stolen emails, intellectual property, strategic planning documents – data and records that could be u organization. <https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/blob/master/2015/2015.09.operation-iron-tiger.pdf>
	2015	Penetration of networks for industrial espionage Designated as Threat Group 3390 and nicknamed “Emissary Panda” by researchers, the hacking group has c networks largely through “watering hole” attacks launched from over 100 compromised legitimate websites, were known to be frequented by those targeted in the attack. <https://arstechnica.com/information-technology/2015/08/newly-discovered-chinese-hacking-group-hacked-watering-holes/>
	Jul 2017	Operation “PZChao” The past few years have seen high-profile cyber-attacks shift to damaging the targets’ digital infrastructures t data, silently monitoring the victim and constantly laying the ground for a new wave of attacks. This is also the case of a custom-built piece of malware that we have been monitoring for several months as Our threat intelligence systems picked up the first indicators of compromise in July last year, and we have ke

		since. <https://labs.bitdefender.com/2018/02/operation-pzchao-a-possible-return-of-the-iron-tiger-apt/>
	Mar 2018	Campaign targeting a national data center in the Central Asia The choice of target made this campaign especially significant – it meant the attackers gained access to a wic resources at one fell swoop. We believe this access was abused, for example, by inserting malicious scripts ir websites in order to conduct watering hole attacks. <https://securelist.com/luckymouse-hits-national-data-center/86083/>
	Apr 2018	Operation “SpoiledLegacy” We have been monitoring a campaign targeting Vietnamese government and diplomatic entities abroad since <https://securelist.com/apt-trends-report-q1-2019/90643/>
	Apr 2019	In April 2019, Unit 42 observed the Emissary Panda (AKA APT27, TG-3390, Bronze Union, Lucky Mouse) webshells on Sharepoint servers to compromise Government Organizations of two different countries in the <https://unit42.paloaltonetworks.com/emissary-panda-attacks-middle-east-government-sharepoint-servers/>
	Summer 2019	Operation “DRBControl” <https://documents.trendmicro.com/assets/white_papers/wp-uncovering-DRBcontrol.pdf>
	2020	APT27 Turns to Ransomware <https://shared-public-reports.s3-eu-west-1.amazonaws.com/APT27+turns+to+ransomware.pdf>
	2020	Iron Tiger APT Updates Toolkit With Evolved SysUpdate Malware <https://www.trendmicro.com/en_us/research/21/d/iron-tiger-apt-updates-toolkit-with-evolved-sysupdate-ma
	Mar 2020	Is APT27 Abusing COVID-19 To Attack People ?! <https://marcoramilli.com/2020/03/19/is-apt27-abusing-covid-19-to-attack-people/>
	Apr 2020	Investigation with a twist: an accidental APT attack and averted data destruction <https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/incident-response-polar-ransomware
	Jun 2020	Operation “StealthyTrident” ESET researchers discovered that chat software called Able Desktop, part of a business management suite pc by 430 government agencies in Mongolia. <https://www.welivesecurity.com/2020/12/10/luckymouse-ta428-compromise-able-desktop/> <https://decoded.avast.io/luigicamastra/apt-group-targeting-governmental-agencies-in-east-asia/>
	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/>
	Mar 2021	German government warns of APT27 activity targeting local companies <https://therecord.media/german-government-warns-of-apt27-activity-targeting-local-companies/>
	Apr 2022	Budworm: Espionage Group Returns to Targeting U.S. Organizations <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/budworm-espionage-us-state>
	May 2022	LuckyMouse uses a backdoored Electron app to target MacOS <https://blog.sekoia.io/luckymouse-uses-a-backdoored-electron-app-to-target-macos/>
	Jul 2022	Iron Tiger’s SysUpdate Reappears, Adds Linux Targeting <https://www.trendmicro.com/en_us/research/23/c/iron-tiger-sysupdate-adds-linux-targeting.html>
	Aug 2022	Iron Tiger Compromises Chat Application Mimi, Targets Windows, Mac, and Linux Users <https://www.trendmicro.com/en_us/research/22/h/irontiger-compromises-chat-app-Mimi-targets-windows-
	Aug 2023	Budworm: APT Group Uses Updated Custom Tool in Attacks on Government and Telecoms Org <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/budworm-tool-update-telecoms-go
Information		<https://www.secureworks.com/research/threat-group-3390-targets-organizations-for-cyberespionage> <https://www.secureworks.com/research/a-peek-into-bronze-unions-toolbox> <https://www.secureworks.com/research/bronze-union>
MITRE ATT&CK		<https://attack.mitre.org/groups/G0027/>
Playbook		<https://pan-unit42.github.io/playbook_viewer/?pb=iron-taurus>

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format