

## Emissary Panda, APT 27, LuckyMouse, Bronze Union

Archived: 2026-04-02 10:52:11 UTC

[Home](#) > [List all groups](#) > Emissary Panda, APT 27, LuckyMouse, Bronze Union

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

Names	Emissary Panda ( <i>CrowdStrike</i> ) APT 27 ( <i>Mandiant</i> ) LuckyMouse ( <i>Kaspersky</i> ) Bronze Union ( <i>Secureworks</i> ) TG-3390 ( <i>SecureWorks</i> ) TEMP.Hippo ( <i>Symantec</i> ) Budworm ( <i>Symantec</i> ) Group 35 ( <i>Talos</i> ) ATK 15 ( <i>Thales</i> ) Iron Tiger ( <i>Trend Micro</i> ) Earth Smilodon ( <i>Trend Micro</i> ) Red Phoenix ( <i>PWC</i> ) ZipToken (?) Iron Taurus ( <i>Palo Alto</i> ) Circle Typhoon ( <i>Microsoft</i> ) Linen Typhoon ( <i>Microsoft</i> ) G0027 ( <i>MITRE</i> )	
Country	 <a href="#">China</a>	
Motivation	<a href="#">Information theft and espionage</a>	
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 <a href="#">Turbine Panda</a> , <a href="#">APT 26</a> , <a href="#">Shell Crew</a> , <a href="#">WebMasters</a> , <a href="#">KungFu Kittens</a> and possibly <a href="#">UNC2</a> This actor worked together with <a href="#">TA428</a> in Operation StealthyTrident.	
Observed	Sectors: <a href="#">Aerospace</a> , <a href="#">Aviation</a> , <a href="#">Defense</a> , <a href="#">Education</a> , <a href="#">Embassies</a> , <a href="#">Government</a> , <a href="#">Manufacturing</a> , <a href="#">Technology</a> , <a href="#">Telecommunications</a> Countries: <a href="#">Australia</a> , <a href="#">Canada</a> , <a href="#">China</a> , <a href="#">Germany</a> , <a href="#">Hong Kong</a> , <a href="#">India</a> , <a href="#">Iran</a> , <a href="#">Israel</a> , <a href="#">Japan</a> , <a href="#">Mongolia</a> , <a href="#">Philippines</a> , <a href="#">Russia</a> , <a href="#">Spain</a> , <a href="#">St Thailand</a> , <a href="#">Tibet</a> , <a href="#">Turkey</a> , <a href="#">UK</a> , <a href="#">USA</a> and Middle East.	
Tools used	<a href="#">Antak</a> , <a href="#">ASPXSpY</a> , <a href="#">China Chopper</a> , <a href="#">Gh0st RAT</a> , <a href="#">gsecdump</a> , <a href="#">HTTPBrowser</a> , <a href="#">HTran</a> , <a href="#">Hunter</a> , <a href="#">HyperBro</a> , <a href="#">Mimikatz</a> , <a href="#">Nishang</a> , <a href="#">OwPsExec</a> , <a href="#">SysUpdate</a> , <a href="#">TwoFace</a> , <a href="#">Windows Credentials Editor</a> , <a href="#">ZXShell</a> , <a href="#">Living off the Land</a> .	
Operations performed	2010	Operation “Iron Tiger” Operation Iron Tiger is a targeted attack campaign discovered to have stolen trillions of data from defense cc including stolen emails, intellectual property, strategic planning documents – data and records that could be t organization. < <a href="https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/blob/master/2015/2015.09.operation-iron-tiger.pdf">https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/blob/master/2015/2015.09.operation-iron-tiger.pdf</a> >
	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. < <a href="https://arstechnica.com/information-technology/2015/08/newly-discovered-chinese-hacking-group-hacked-watering-holes/">https://arstechnica.com/information-technology/2015/08/newly-discovered-chinese-hacking-group-hacked-watering-holes/</a> >
	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

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

Last change to this card: 16 August 2025

Download this actor card in [PDF](#) or [JSON](#) format

---

Source: <https://apt.eta-da.or.th/cgi-bin/showcard.cgi?u=960355e3-27d8-4e62-a4cc-a807f031865f>