APT 41 - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:23:39 UTC

APT group: APT 41

Names	APT 41 *(FireEye)* Double Dragon *(FireEye)* TG-2633 *(SecureWorks)* Bronze Atlas *(SecureWorks)* Red Kelpie *(PWC)* Blackfly *(Symantec)* Earth Baku *(Trend Micro)* SparklingGoblin *(ESET)* Grayfly *(Symantec)* TA415 *(Proofpoint)* BrazenBamboo *(Volexity)* G0096 *(MITRE)*
Country	China
Sponsor	State-sponsored
Motivation	Financial crime, Information theft and espionage
First seen	2012
Description	(FireEye) FireEye Threat Intelligence assesses with high confidence that APT41 is a prolific cyber threat group that carries out Chinese state-sponsored espionage activity in addition to financially motivated activity potentially outside of state control. Activity traces back to 2012 when individual members of APT41 conducted primarily financially motivated operations focused on the video game industry before expanding into likely state-sponsored activity. This is remarkable because explicit financially motivated targeting is unusual among Chinese state-sponsored threat groups, and evidence suggests these two motivations were balanced concurrently from 2014 onward. • APT41 overlaps at least partically with public reporting on group including Barium and Winnti Group, Wicked Panda. In some cases the primary observed similarity in the publicly reported Winnti activity was the use of the same malware – including HIGHNOON – across otherwise separate clusters of activity. • Previous FireEye Threat Intelligence reporting on the use of HIGHNOON and related activity was grouped together under both Ke3chang, Vixen Panda, APT 15,

	GREF, Playful Dragon and Mana, although we now understand this to be the work of several Chinese cyber espionage groups that share tools and digital certificates. • APT41 reflects our current understanding of what was previously reported as GREF, as well as additional indicators and activity gathered during our extensive review of our intelligence holdings. APT 41 has 2 subgroups: 1. Subgroup: Earth Longzhi 2. Subgroup: Earth Freybug Also see Earth Lusca and RedGolf.	
Observed	Sectors: Construction, Defense, Education, Energy, Financial, Government, Healthcare, High-Tech, Hospitality, Manufacturing, Media, Oil and gas, Petrochemical, Pharmaceutical, Retail, Shipping and Logistics, Telecommunications, Transportation, Online video game companies. Countries: Australia, Bahrain, Brazil, Canada, Chile, Denmark, Finland, France, Georgia, Hong Kong, India, Indonesia, Italy, Japan, Malaysia, Mexico, Myanmar, Netherlands, Pakistan, Philippines, Poland, Qatar, Saudi Arabia, Singapore, South Korea, South Africa, Spain, Sri Lanka, Sweden, Switzerland, Taiwan, Thailand, Turkey, UAE, UK, USA, Vietnam.	
Tools used	9002 RAT, AceHash, ADORE.XSEC, AntSword, ASPXSpy, Barlaiy, BEACON, BlackCoffee, BLUEBEAM, certutil, China Chopper, Cobalt Strike, COLDJAVA, Crackshot, CrossWalk, DBoxAgent, DEADEYE, DEPLOYLOG, Derusbi, DIRTCLEANER, DragonEgg, DUSTPAN, DUSTTRAP, EasyNight, FunnySwitch, GearShift, Gh0st RAT, HDRoot, HighNoon, HighNote, HKDOOR, HUI Loader, Jumpall, KEYPLUG, LATELUNCH, LIFEBOAT, Lowkey, MessageTap, Meterpreter, Mimikatz, MoonBounce, MoonWalk, njRAT, NTDSDump, PACMAN, PINEGROVE, PipeMon, PlugX, POTROAST, PRIVATELOG, pwdump, RedXOR, ROCKBOOT, SAGEHIRE, SerialVlogger, ShadowHammer, ShadowPad Winnti, SideWalk, Skip-2.0, SPARKLOG, Speculoos, Spyder, SQLULDR2, STASHLOG, SWEETCANDLE, TERA, TIDYELF, Voldemort, WIDETONE, WINNKIT, Winnti, WINTERLOVE, WyrmSpy, xDll, XDOOR, XMRig, ZXShell, Living off the Land.	
Operations performed	Autumn 2016	Breach of TeamViewer <https://www.bleepingcomputer.com/news/security/teamviewer-confirms-undisclosed-breach-from-2016/>
	Jul 2017	ShadowPad is one of the largest known supply-chain attacks. Had it not been detected and patched so quickly, it could potentially have targeted hundreds of organizations worldwide. <https://www.kaspersky.com/about/press-

	releases/2017_shadowpad-how-attackers-hide-backdoor-in-software-used-by-hundreds-of-large-companies-around-the-world>
Jun 2018	Operation “ShadowHammer” A supply-chain attack dubbed “Operation ShadowHammer” has been uncovered, targeting users of the ASUS Live Update Utility with a backdoor injection. The China-backed BARIUM APT is suspected to be at the helm of the project. According to Kaspersky Lab, the campaign ran from June to at least November 2018 and may have impacted more than a million users worldwide – though the adversaries appear to have been after specific victims in Asia. <https://threatpost.com/asus-pc-backdoors-shadowhammer/143129/>
2019	Operation “CuckooBees” Cybereason Uncovers Massive Chinese Intellectual Property Theft Operation <https://www.cybereason.com/blog/operation-cuckoobees-cybereason-uncovers-massive-chinese-intellectual-property-theft-operation> <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/spyder-loader-cuckoobees-hong-kong>
Mar 2019	Although the malware uses different configurations in each case, the three affected software products included the same backdoor code and were launched using the same mechanism. While two of the compromised products no longer include the backdoor, one of the affected developers is still distributing the trojanized version: ironically, the game is named Infestation, and is produced by Thai developer Electronics Extreme. <https://www.welivesecurity.com/2019/03/11/gaming-industry-scope-attackers-asia/>
Apr 2019	In April 2019, FireEye’s Managed Defense team identified suspicious activity on a publicly-accessible web server at a U.S.-based research university. This activity, indicated that the attackers were exploiting CVE-2019-3396, a vulnerability in Atlassian Confluence Server that allowed for path traversal and remote code execution. <https://www.fireeye.com/blog/threat-research/2019/08/game-over-detecting-and-stopping-an-apt41-operation.html>

Aug 2019	APT41's newest espionage tool, MESSAGETAP, was discovered during a 2019 investigation at a telecommunications network provider within a cluster of Linux servers. Specifically, these Linux servers operated as Short Message Service Center (SMSC) servers. <https://www.fireeye.com/blog/threat-research/2019/10/messagetap-who-is-reading-your-text-messages.html>
Oct 2019	Winnti Group's skip-2.0: A Microsoft SQL Server backdoor <https://www.welivesecurity.com/2019/10/21/winnti-group-skip2-0-microsoft-sql-server-backdoor/>
Nov 2019	In November 2019, we discovered a new campaign run by the Winnti Group against two Hong Kong universities. We found a new variant of the ShadowPad backdoor, the group's flagship backdoor, deployed using a new launcher and embedding numerous modules. The Winnti malware was also found at these universities a few weeks prior to ShadowPad. <https://www.welivesecurity.com/2020/01/31/winnti-group-targeting-universities-hong-kong/>
Jan 2020	Between January 20 and March 11, FireEye observed APT41 attempt to exploit vulnerabilities in Citrix NetScaler/ADC, Cisco routers, and Zoho ManageEngine Desktop Central at over 75 FireEye customers. <https://www.fireeye.com/blog/threat-research/2020/03/apt41-initiates-global-intrusion-campaign-using-multiple-exploits.html> <https://unit42.paloaltonetworks.com/apt41-using-new-speculoos-backdoor-to-target-organizations-globally/>
Feb 2020	In February 2020, we discovered a new, modular backdoor, which we named PipeMon. Persisting as a Print Processor, it was used by the Winnti Group against several video gaming companies that are based in South Korea and Taiwan and develop MMO (Massively Multiplayer Online) games. Video games developed by these companies are available on popular gaming platforms and have thousands of simultaneous players. <https://www.welivesecurity.com/2020/05/21/no-game-over-winnti-group/>
2020	New Linux Backdoor RedXOR Likely Operated by Chinese Nation-State Actor

	<https://www.intezer.com/blog/malware-analysis/new-linux-backdoor-redxor-likely-operated-by-chinese-nation-state-actor/>
Mar 2020	During threat research in March 2020, PT Expert Security Center specialists found a previously unknown backdoor and named it xDll, based on the original name found in the code. As a result of a configuration flaw of the malware's command and control (C2) server, some server directories were externally accessible. <https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/shadowpad-new-activity-from-the-winnti-group/>
Apr 2020	Hackers linked to Chinese government stole millions in Covid benefits, Secret Service says <https://www.nbcnews.com/tech/security/chinese-hackers-covid-fraud-millions-rcna59636>
Jul 2020	APT41 Resurfaces as Earth Baku With New Cyberespionage Campaign <https://www.trendmicro.com/en_us/research/21/h/apt41-resurfaces-as-earth-baku-with-new-cyberespionage-campaign.html>
Oct 2020	Lookout Attributes Advanced Android Surveillanceware to Chinese Espionage Group APT41 <https://www.lookout.com/threat-intelligence/article/wyrmspy-dragonegg-surveillanceware-apt41>
2021	APT41 World Tour 2021 on a tight schedule <https://blog.group-ib.com/apt41-world-tour-2021>
Feb 2021	You never walk alone: The SideWalk backdoor gets a Linux variant <https://www.welivesecurity.com/2022/09/14/you-never-walk-alone-sidewalk-backdoor-linux-variant/>
Early 2021	New Wave of Espionage Activity Targets Asian Governments <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/espionage-asia-governments>
Mar 2021	Operation “ColunmTK” Big airline heist <https://blog.group-ib.com/colunmtk_apt41>
Spring 2021	MoonBounce: the dark side of UEFI firmware <https://securelist.com/moonbounce-the-dark-side-of-uefi-firmware/105468/>

May 2021	Does This Look Infected? A Summary of APT41 Targeting U.S. State Governments <https://www.mandiant.com/resources/apt41-us-state-governments>
Jul 2021	BIOPASS RAT: New Malware Sniffs Victims via Live Streaming <https://www.trendmicro.com/en_us/research/21/g/biopass-rat-new-malware-sniffs-victims-via-live-streaming.html>
Aug 2021	The SideWalk may be as dangerous as the CROSSWALK <https://www.welivesecurity.com/2021/08/24/sidewalk-may-be-as-dangerous-as-crosswalk/>
Aug 2022	Winnti APT group docks in Sri Lanka for new campaign <https://www.malwarebytes.com/blog/threat-intelligence/2022/winnti-apt-group-docks-in-sri-lanka-for-new-campaign-final.pdf>
Late 2022	Blackfly: Espionage Group Targets Materials Technology <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/blackfly-espionage-materials>
Late 2022	A Dive into Earth Baku's Latest Campaign <https://www.trendmicro.com/en_us/research/24/h/earth-baku-latest-campaign.html>
2023	APT41 Has Arisen From the DUST <https://cloud.google.com/blog/topics/threat-intelligence/apt41-arisen-from-dust>
Jul 2023	APT41 likely compromised Taiwanese government-affiliated research institute with ShadowPad and Cobalt Strike <https://blog.talosintelligence.com/chinese-hacking-group-apt41-compromised-taiwanese-government-affiliated-research-institute-with-shadowpad-and-cobaltstrike-2/>
2024	Chinese APT Uses VPN Bug to Exploit Worldwide OT Orgs <https://www.darkreading.com/ics-ot-security/chinese-apt-vpn-bug-worldwide-ot-orgs>
Mar 2024	Winnti APT41 Targets Japanese Firms in RevivalStone Cyber Espionage Campaign <https://thehackernews.com/2025/02/winnti-apt41-targets-japanese-firms-in.html>

	Apr 2024	DodgeBox: A deep dive into the updated arsenal of APT41 | Part 1 MoonWalk: A deep dive into the updated arsenal of APT41 | Part 2 <https://www.zscaler.com/blogs/security-research/dodgebox-deep-dive-updated-arsenal-apt41-part-1> <https://www.zscaler.com/blogs/security-research/moonwalk-deep-dive-updated-arsenal-apt41-part-2>
	Apr 2024	LightSpy: APT41 Deploys Advanced DeepData Framework In Targeted Southern Asia Espionage Campaign <https://blogs.blackberry.com/en/2024/11/lightspy-apt41-deploys-advanced-deepdata-framework-in-targeted-southern-asia-espionage-campaign>
	Jul 2024	BrazenBamboo Weaponizes FortiClient Vulnerability to Steal VPN Credentials via DEEPDATA <https://www.volexity.com/blog/2024/11/15/brazenbamboo-weaponizes-forticlient-vulnerability-to-steal-vpn-credentials-via-deepdata/>
	Aug 2024	The Malware That Must Not Be Named: Suspected Espionage Campaign Delivers “Voldemort” <https://www.proofpoint.com/us/blog/threat-insight/malware-must-not-be-named-suspected-espionage-campaign-delivers-voldemort>
	Oct 2024	Mark Your Calendar: APT41 Innovative Tactics <https://cloud.google.com/blog/topics/threat-intelligence/apt41-innovative-tactics>
	Jul 2025	The SOC files: Rumble in the jungle or APT41’s new target in Africa <https://securelist.com/apt41-in-africa/116986/>
Counter operations	Aug 2020	Seven International Cyber Defendants, Including “Apt41” Actors, Charged In Connection With Computer Intrusion Campaigns Against More Than 100 Victims Globally <https://www.justice.gov/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer>
Information	<http://content.fireeye.com/apt41/rpt-apt41> <https://arstechnica.com/information-technology/2018/05/researchers-link-a-decade-of-potent-hacks-to-chinese-intelligence-group/> <https://www.kaspersky.com/about/press-releases/2019_operation-shadowhammer-new-supply-chain-attack> <https://www.welivesecurity.com/wp-content/uploads/2019/10/ESET_Winnti.pdf>	

	<https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/higaisa-or-winnti-apt-41-backdoors-old-and-new/> <https://blogs.blackberry.com/en/2021/10/drawing-a-dragon-connecting-the-dots-to-find-apt41> <https://www.infosecurity-magazine.com/news/chinas-apt41-manages-library/> <https://www.hhs.gov/sites/default/files/apt41-recent-activity.pdf> <https://www.cyfirma.com/outofband/the-origins-of-apt-41-and-shadowpad-lineage/>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0096/>

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
