Ke3chang, Vixen Panda, APT 15, GREF, Playful Dragon

APT group: Ke3chang, Vixen Panda, APT 15, GREF, Playful Dragon

Names	Ke3chang *(FireEye)* Vixen Panda *(CrowdStrike)* APT 15 *(Mandiant)* GREF *(SecureWorks)* Bronze Palace *(SecureWorks)* Bronze Davenport *(SecureWorks)* Bronze Idlewood *(SecureWorks)* CTG-9246 *(SecureWorks)* Playful Dragon *(FireEye)* Royal APT *(NCC Group)* Nickel *(Microsoft)* BackdoorDiplomacy *(ESET)* Playful Taurus *(Palo Alto)* Metushy *(?)* Social Network Team *(?)* Nylon Typhoon *(Microsoft)* Flea *(Symantec)* Red Vulture *(PWC)* PurpleHaze *(SentinelOne)* G0004 *(MITRE)* G0135 *(MITRE)*
Country	China
Sponsor	State-sponsored
Motivation	Information theft and espionage
First seen	2010
Description	Ke3chang is a threat group attributed to actors operating out of China. Ke3chang has targeted several industries, including oil, government, military, and more.
Observed	Sectors: Aerospace, Aviation, Chemical, Defense, Embassies, Energy, Government, High-Tech, Industrial, Manufacturing, Mining, Oil and gas, Telecommunications,

	Utilities and Uyghur communities. Countries: Afghanistan, Albania, Argentina, Barbados, Belgium, Bhutan, Bosnia and Herzegovina, Brazil, Bulgaria, Chile, China, Colombia, Croatia, Czech, Dominican Republic, Ecuador, Egypt, El Salvador, France, Georgia, Germany, Ghana, Guatemala, Honduras, Hungary, India, Indonesia, Iran, Italy, Jamaica, Kazakhstan, Kuwait, Libya, Malaysia, Mali, Mexico, Montenegro, Namibia, Nigeria, Pakistan, Panama, Peru, Poland, Portugal, Saudi Arabia, Slovakia, South Africa, Sri Lanka, Switzerland, Syria, Trinidad and Tobago, Turkey, UAE, UK, USA, Uzbekistan, Venezuela.	
Tools used	BS2005, CarbonSteal, Cobalt Strike, DarthPusher, EarthWorm, EternalBlue, DoubleAgent, GoldenEagle, Graphican, HenBox, HighNoon, IRAFAU, Ketrican, Ketrum, Mimikatz, MirageFox, MS Exchange Tool, nbtscan, netcat, Okrum, PluginPhantom, PortQry, ProcDump, PsList, RoyalCli, RoyalDNS, SilkBean, Sinowal, SMBTouch, spwebmember, SpyWaller, TidePool, Turian, Winnti, XSLCmd, Living off the Land and EternalRocks and EternalSynergy.	
Operations performed	2010	Operation “Ke3chang” As the crisis in Syria escalates, FireEye research-ers have discovered a cyber espionage campaign, which we call “Ke3chang,” that falsely advertises information updates about the ongoing crisis to compromise MFA networks in Europe. We believe that the Ke3chang attackers are operating out of China and have been active since at least 2010. However, we believe specific Syria-themed attacks against MFAs (codenamed by Ke3chang as “moviestar”) began only in August 2013. The timing of the attacks precedes a G20 meeting held in Russia that focused on the crisis in Syria. <https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/wp-operation-ke3chang.pdf>
	Aug 2014	Forced to Adapt: XSLCmd Backdoor Now on OS X <https://www.fireeye.com/blog/threat-research/2014/09/forced-to-adapt-xslcmd-backdoor-now-on-os-x.html>
	2015	The Lookout Threat Intelligence team has discovered four Android surveillanceware tools, which are used to target the Uyghur ethnic minority group. Our research indicates that these four interconnected malware tools are elements of much larger mAPT (mobile advanced persistent threat) campaigns that have been active for years. Although there is evidence that the campaigns have been active since at least 2013, Lookout researchers have been monitoring the surveillanceware families — SilkBean, DoubleAgent, CarbonSteal and GoldenEagle — as far back as 2015.

	<https://www.lookout.com/documents/threat-reports/us/lookout-uyghur-malware-tr-us.pdf>
May 2016	Little has been published on the threat actors responsible for Operation Ke3chang since the report was released more than two years ago. However, Unit 42 has recently discovered the actors have continued to evolve their custom malware arsenal. We've discovered a new malware family we've named TidePool. It has strong behavioral ties to Ke3chang and is being used in an ongoing attack campaign against Indian embassy personnel worldwide. This targeting is also consistent with previous attacker TTPs; Ke3chang historically targeted the Ministry of Affairs, and also conducted several prior campaigns against India. <https://unit42.paloaltonetworks.com/operation-ke3chang-resurfaces-with-new-tidepool-malware/>
May 2017	Attack on a company that provides a range of services to UK Government A number of sensitive documents were stolen by the attackers during the incident and we believe APT15 was targeting information related to UK government departments and military technology. During our analysis of the compromise, we identified new backdoors that now appear to be part of APT15's toolset. The backdoor BS2005 – which has traditionally been used by the group – now appears alongside the additional backdoors RoyalCli and RoyalDNS. <https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2018/march/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/>
2017	BackdoorDiplomacy: Upgrading from Quarian to Turian <https://www.welivesecurity.com/2021/06/10/backdoordiplomacy-upgrading-quarian-turian/>
Jun 2018	Operation "MirageFox" The malware involved in this recent campaign, MirageFox, looks to be an upgraded version of a tool, a RAT believed to originate in 2012, known as Mirage. <https://www.intezer.com/miragefox-apt15-resurfaces-with-new-tools-based-on-old-ones/>
Mar 2019	The group continues to be active in 2019 – in March 2019, we detected a new Ketrican sample that has evolved from the 2018 Ketrican backdoor. It attacked the same targets as the backdoor from 2018.

		<https://www.welivesecurity.com/2019/07/18/okrum-ke3chang-targets-diplomatic-missions/>
	Sep 2019	NICKEL targeting government organizations across Latin America and Europe <https://www.microsoft.com/security/blog/2021/12/06/nickel-targeting-government-organizations-across-latin-america-and-europe/>
	May 2020	In mid May, we identified three recently uploaded samples from VirusTotal that share code with older APT15 implants. We named this new family of samples, “Ketrum”, due to the merger of features in the documented backdoor families “Ketrican” and “Okrum”. <https://www.intezer.com/blog/research/the-evolution-of-apt15s-codebase-2020/>
	Aug 2021	BackdoorDiplomacy Wields New Tools in Fresh Middle East Campaign <https://www.bitdefender.com/blog/labs/backdoor-diplomacy-wields-new-tools-in-fresh-middle-east-campaign/>
	Apr 2022	Chinese Playful Taurus Activity in Iran <https://unit42.paloaltonetworks.com/playful-taurus/>
	Late 2022	Graphican: Flea Uses New Backdoor in Attacks Targeting Foreign Ministries <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/flea-backdoor-microsoft-graph-apt15>
	Oct 2024	Follow the Smoke | China-nexus Threat Actors Hammer At the Doors of Top Tier Targets <https://www.sentinelone.com/labs/follow-the-smoke-china-nexus-threat-actors-hammer-at-the-doors-of-top-tier-targets/>
Information	<https://github.com/nccgroup/Royal_APT>	
MITRE ATT&CK	<https://attack.mitre.org/groups/G0004/> <https://attack.mitre.org/groups/G0135/>	
Playbook	<https://pan-unit42.github.io/playbook_viewer/?pb=playful-taurus>	

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format