APT 12, Numbered Panda - Threat Group Cards: A Threat Actor Encyclopedia

APT group: APT 12, Numbered Panda

Names	APT 12 *(Mandiant)* Numbered Panda *(CrowdStrike)* CTG-8223 *(SecureWorks)* Bronze Globe *(SecureWorks)* BeeBus *(FireEye)* Calc Team *(Symantec)* DynCALC *(Symantec)* DNSCalc *(Symantec)* Group 22 *(Talos)* Crimson Iron *(ThreatConnect)* Hexagon Typhoon *(Microsoft)* G0005 *(MITRE)*
Country	China
Sponsor	State-sponsored
Motivation	Information theft and espionage
First seen	2009
Description	(CrowdStrike) Numbered Panda has a long list of high-profile victims and is known by a number of names including: DYNCALC, IXESHE, JOY RAT, APT-12, etc. Numbered Panda has targeted a variety of victims including but not limited to media outlets, high-tech companies, and multiple governments. Numbered Panda has targeted organizations in time-sensitive operations such as the Fukushima Reactor Incident of 2011, likely filling intelligence gaps in the ground cleanup/mitigation operations. Screen saver files, which are binary executables and PDF documents, are common Numbered Panda weaponization tactics. One of the most interesting techniques that Numbered Panda likes to use is to dynamically calculate the Command and Control (C2) port by resolving a DNS. This effectively helps Numbered Panda bypass egress filtering implemented to prevent unauthorized communications on some enterprises. The malware will typically use two DNS

	names for communication: one is used for command and control; the other is used with an algorithm to calculate the port to communicate to.	
Observed	Sectors: Defense, Government, High-Tech, Media, Telecommunications and Electronics and journalists. Countries: Germany, Japan, Taiwan, USA and East Asia.	
Tools used	AUMLIB, ETUMBOT, IHEATE, IXESHE, RapidStealer, THREEBYTE, WaterSpout.	
Operations performed	Jul 2009	"IXESHE" campaign Target: East Asian governments, Taiwanese electronics manufacturers and a telecommunications company. <http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_ixeshe.pdf>
	May 2011	"AUMLIB" campaign <https://www.fireeye.com/blog/threat-research/2013/08/survival-of-the-fittest-new-york-times-attackers-evolve-quickly.html>
	2011	"ETUMBOT" campaign Target: Taiwan Once the malicious file was downloaded and extracted by the victim, Etumbot uses a right-to-left override exploit to trick the victim to download the malware installer. According to Arbor Security, the "technique is a simple way for malware writers to disguise names of malicious files. A hidden Unicode character in the filename will reverse the order of the characters that follow it, so that a .scr binary file appears to be a .xls document, for example." <https://www.arbornetworks.com/blog/asert/wp-content/uploads/2014/06/ASERT-Threat-Intelligence-Brief-2014-07-Illuminating-Etumbot-APT.pdf>
	Oct 2012	Breach of The New York Times "For the last four months, Chinese hackers have persistently attacked The New York Times, infiltrating its computer systems and getting passwords for its reporters and other employees." The attack occurred after the New York Times published a story about how the relatives of Wen Jiabao, the sixth Premier of the State Council of the People's Republic of China, "accumulated a fortune worth several billion dollars through business dealings." The computers used to launch the attack are believed to be the same university computers used by the Chinese military to attack United States military contractors.

		<https://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html?pagewanted=all>
	Oct 2012	“RIPTIDE” campaign Spear-phishing on Taiwanese Government
	Aug 2014	“HIGHTIDE” campaign Spear-phishing on Taiwanese Government Uses an updated version of ETUMBOT.
	Aug 2014	“THREEBYTE” campaign Spear-phishing on Taiwanese Government
	Aug 2014	“WATERSPOUT” campaign Spear-phishing on Taiwanese Government
	Jan 2016	IXESHE Derivative IHEATE Targets Users in America <https://blog.trendmicro.com/trendlabs-security-intelligence/ixeshe-derivative-iheate-targets-users-america/>
	Nov 2016	“CNACOM” campaign On November 7, we spotted a malicious injection on the registration page of a major Taiwanese public service website. An iframe was injected into the footer of the page, which then loaded a unique landing page containing the CVE-2016-0189 exploit code. <https://www.zscaler.com/blogs/research/cnacom-open-source-exploitation-strategic-web-compromise>
Information	<https://www.crowdstrike.com/blog/whois-numbered-panda/> <https://www.fireeye.com/blog/threat-research/2014/09/darwins-favorite-apt-group-2.html> <https://en.wikipedia.org/wiki/Numbered_Panda>	
MITRE ATT&CK	<https://attack.mitre.org/groups/G0005/>	

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
