APT 3, Gothic Panda, Buckeye

Archived: 2026-04-05 18:45:22 UTC

NamesAPT 3 *(Mandiant)*
Gothic Panda *(CrowdStrike)*
Buckeye *(Symantec)*
TG-0110 *(SecureWorks)*
Bronze Mayfair *(SecureWorks)*
UPS Team *(Symantec)*
Group 6 *(Talos)*
Red Sylvan *(PWC)*
Boron *(Microsoft)*
Brocade Typhoon *(Microsoft)*

G0022 *(MITRE)* Country China SponsorState-sponsored, Ministry of State Security and Internet security firm Guangzhou Bo Yu Information Technology Company Limited (“Boyusec”) MotivationInformation theft and espionage First seen2007 Description(Recorded Future) APT3 (also known as UPS, Gothic Panda, and TG-0110) is a sophisticated threat group that has been active since at least 2010. APT3 utilizes a broad range of tools and techniques including spear-phishing attacks, zero-day exploits, and numerous unique and publicly available remote access tools (RAT). Victims of APT3 intrusions include companies in the defense, telecommunications, transportation, and advanced technology sectors — as well as government departments and bureaus in Hong Kong, the U.S., and several other countries. ObservedSectors: Aerospace, Construction, Defense, High-Tech, Manufacturing, Technology, Telecommunications, Transportation.
Countries: Belgium, Hong Kong, Italy, Luxembourg, Philippines, Sweden, UK, USA, Vietnam. Tools usedAPT3 Keylogger, Bemstour, DoublePulsar, EternalBlue, HTran, Hupigon, LaZagne, OSInfo, Pirpi, PlugX, RemoteCMD, shareip, TTCalc, w32times and several 0-days for IE, Firefox and Flash. Operations performed2007Hupigon and Pirpi Backdoors
<https://www.fireeye.com/blog/threat-research/2010/11/ie-0-day-hupigon-joins-the-party.html> Apr 2014Operation “Clandestine Fox”
FireEye Research Labs identified a new Internet Explorer (IE) zero-day exploit used in targeted attacks. The vulnerability affects IE6 through IE11, but the attack is targeting IE9 through IE11. This zero-day bypasses both ASLR and DEP. Microsoft has assigned CVE-2014-1776 to the vulnerability and released security advisory to track this issue.
<https://www.fireeye.com/blog/threat-research/2014/04/new-zero-day-exploit-targeting-internet-explorer-versions-9-through-11-identified-in-targeted-attacks.html> Jun 2014Operation “Clandestine Fox”, Part Deux
While Microsoft quickly released a patch to help close the door on future compromises, we have now observed the threat actors behind “Operation Clandestine Fox” shifting their point of attack and using a new vector to target their victims: social networking.
<https://www.fireeye.com/blog/threat-research/2014/06/clandestine-fox-part-deux.html> Nov 2014Operation “Double Tap”
This actor initiated their most recent campaign on November 19, 2014 targeting multiple organizations. The

attacker leveraged multiple exploits, targeting both CVE-2014-6332 and CVE-2014-4113. <https://www.fireeye.com/blog/threat-research/2014/11/operation_doubletap.html> Jun 2015Operation "Clandestine Wolf"

In the last several weeks, APT3 actors launched a large-scale phishing campaign against organizations in the following industries: Aerospace and Defense, Construction and Engineering, High Tech, Telecommunications and Transportation.

<https://www.fireeye.com/blog/threat-research/2015/06/operation-clandestine-wolf-adobe-flash-zero-day.html> Mar 2016Variant of the DoublePulsar Backdoor

Beginning in March 2016, Buckeye began using a variant of DoublePulsar (Backdoor.Doublepulsar), a backdoor that was subsequently released by the Shadow Brokers in 2017. DoublePulsar was delivered to victims using a custom exploit tool (Trojan.Bemstour) that was specifically designed to install DoublePulsar.

<https://www.symantec.com/blogs/threat-intelligence/buckeye-windows-zero-day-exploit> <https://research.checkpoint.com/upsynergy/> Mar 2016Buckeye cyberespionage group shifts gaze from US to Hong Kong

<https://www.symantec.com/connect/blogs/buckeye-cyberespionage-group-shifts-gaze-us-hong-kong> Counter operationsNov 2017DOJ reveals indictment against Chinese cyber spies that stole U.S. business secrets

<https://www.cyberscoop.com/boyusec-china-doj-indictment/> Nov 2017U.S. Charges Three Chinese Hackers Who Work at Internet Security Firm for Hacking Three Corporations for Commercial Advantage

<https://www.justice.gov/opa/pr/us-charges-three-chinese-hackers-who-work-internet-security-firm-hacking-three-corporations> Information<https://intrusiontruth.wordpress.com/2017/05/09/apt3-is-boyusec-a-chinese-intelligence-contractor/>

<https://www.recordedfuture.com/chinese-mss-behind-apt3/> MITRE ATT&CK<https://attack.mitre.org/groups/G0022/>
