APT 32, OceanLotus, SeaLotus - Threat Group Cards: A Threat Actor Encyclopedia

APT group: APT 32, OceanLotus, SeaLotus

Names	APT 32 *(Mandiant)* OceanLotus *(SkyEye Labs)* SeaLotus *(?)* APT-C-00 *(Qihoo 360)* Ocean Buffalo *(CrowdStrike)* Tin Woodlawn *(SecureWorks)* ATK 17 *(Thales)* SectorF01 *(ThreatRecon)* Pond Loach *(Accenture)* APT-LY-100 *(?)* Lotus Bane *(Group-IB)* G0050 *(MITRE)*
Country	Vietnam
Sponsor	State-sponsored
Motivation	Information theft and espionage
First seen	2013
Description	(FireEye) Since at least 2014, FireEye has observed APT32 targeting foreign corporations with a vested interest in Vietnam's manufacturing, consumer products, and hospitality sectors. Furthermore, there are indications that APT32 actors are targeting peripheral network security and technology infrastructure corporations. In addition to focused targeting of the private sector with ties to Vietnam, APT32 has also targeted foreign governments, as well as Vietnamese dissidents and journalists since at least 2013.
Observed	Sectors: Defense, Financial, Government, High-Tech, Hospitality, Manufacturing, Media, Retail, Telecommunications and Uyghurs, dissidents and journalists. Countries: ASEAN, Australia, Bangladesh, Brunei, Cambodia, China, Denmark,

	Germany, India, Indonesia, Iran, Japan, Laos, Malaysia, Myanmar, Nepal, Netherlands, Philippines, Singapore, South Korea, Thailand, UK, USA, Vietnam.	
Tools used	AtNow, CACTUSTORCH, CamCapture Plugin, Cobalt Strike, Cuegoe, DKMC, fingerprintjs2, Goopy, HiddenLotus, KerrDown, KOMPROGO, METALJACK, Mimikatz, MSFvenom, Nishang, OceanLotus, Pagoda, PhantomLance, PHOREAL, PowerSploit, QuasarRAT, RatSnif, Remy, Roland, Salgorea, SOUNDBITE, Terracotta VPN, Veil and 0-day exploits in MS Office.	
Operations performed	Apr 2014	Operation “PhantomLance” In July 2019, Dr. Web reported about a backdoor trojan in Google Play, which appeared to be sophisticated and unlike common malware often uploaded for stealing victims’ money or displaying ads. So, we conducted an inquiry of our own, discovering a long-term campaign, which we dubbed “PhantomLance”, its earliest registered domain dating back to December 2015. <https://securelist.com/apt-phantomlance/96772/> <https://labs.bitdefender.com/2020/05/android-campaign-from-known-oceanlotus-apt-group-potentially-older-than-estimated-abused-legitimate-certificate/>
	Dec 2014	These applications disguise as a normal application, and their icons will hide automatically after they are running. They will release malicious sub-packages in the background, receive the remote control command, steal the privacy information of users such as SMS messages, contacts, call records, geographic locations, and browser records. They also download apks secretly and record audios and videos, then upload users’ privacy information to server, causing users’ privacy leakage. <https://www.antiy.net/p/analysis-of-the-attack-of-mobile-devices-by-oceanlotus/>
	Aug 2015	Terracotta VPN Dubbed by RSA as “Terracotta VPN” (a reference to the Chinese Terracotta Army), this satellite array of VPN services “may represent the first exposure of a PRC-based VPN operation that maliciously, efficiently and rapidly enlists vulnerable servers around the world,” the company said in a report released today. <https://krebsonsecurity.com/2015/08/chinese-vpn-service-as-attack-platform/>
	Sep 2016	Blackberry Cylance threat researchers have analyzed the Ratsnif rojans, which offer a veritable swiss-army knife of network attack techniques. The rojans, under active development since 2016,

	combine capabilities like packet sniffing, gateway/device ARP poisoning, DNS poisoning, HTTP injection, and MAC spoofing. <https://threatvector.cylance.com/en_us/home/threat-spotlight-ratsnif-new-network-vermin-from-oceanlotus.html>
Mar 2017	Breach of the ASEAN website Steven Adair, founder and CEO, said the hacking group was still active, and had compromised the website of the Association of South East Asian Nations (ASEAN) over several high-profile summit meetings. ASEAN is holding another summit of regional leaders in the Philippines capital Manila this week. <https://www.reuters.com/article/us-cyber-attack-vietnam/vietnams-neighbors-asean-targeted-by-hackers-report-idUSKBN1D70VU>
May 2017	Operation “Cobalt Kitty” Dubbed Operation Cobalt Kitty, the APT targeted a global corporation based in Asia with the goal of stealing proprietary business information. The threat actor targeted the company’s top-level management by using spear-phishing attacks as the initial penetration vector, ultimately compromising the computers of vice presidents, senior directors and other key personnel in the operational departments. During Operation Cobalt Kitty, the attackers compromised more than 40 PCs and servers, including the domain controller, file servers, Web application server and database server. <https://www.cybereason.com/blog/operation-cobalt-kitty-apt>
May 2017	Mass Digital Surveillance and Attacks Targeting ASEAN, Asian Nations, the Media, Human Rights Groups, and Civil Society In May 2017, Volexity identified and started tracking a very sophisticated and extremely widespread mass digital surveillance and attack campaign targeting several Asian nations, the ASEAN organization, and hundreds of individuals and organizations tied to media, human rights and civil society causes. These attacks are being conducted through numerous strategically compromised websites and have occurred over several high-profile ASEAN summits. <https://www.volexity.com/blog/2017/11/06/oceanlotus-blossoms-mass-digital-surveillance-and-exploitation-of-asean-nations-the-media-human-rights-and-civil-society/>
Oct 2017	During an incident response investigation in the final quarter of 2017, Cylance incident responders and threat researchers uncovered several bespoke backdoors deployed by OceanLotus Group (a.k.a. APT32, Cobalt Kitty), as well as evidence of the threat actor using obfuscated CobaltStrike Beacon payloads to perform C2.

	<https://threatvector.cylance.com/en_us/home/report-the-spyrats-of-oceanlotus.html>
Early 2018	KerrDown downloader We identified two methods to deliver the KerrDown downloader to targets. One is using the Microsoft Office Document with a malicious macro and the other is RAR archive which contains a legitimate program with DLL side-loading. For RAR archive files, the file names used to trick targets are all in Vietnamese as shown in Figure 11. Our analysis shows that the primary targets of the ongoing campaign discussed in this blog are either in Vietnam or Vietnamese speaking individuals. <https://unit42.paloaltonetworks.com/tracking-oceanlotus-new-downloader-kerrdown/>
Mar 2018	OceanLotus ships new backdoor using old tricks <https://www.welivesecurity.com/2018/03/13/oceanlotus-ships-new-backdoor/>
Apr 2018	New MacOS Backdoor The MacOS backdoor was found in a malicious Word document presumably distributed via email. The document bears the filename "2018-PHIẾU GHI DANH THAM DỰ TĨNH HỘI HMDC 2018.doc," which translates to "2018-REGISTRATION FORM OF HMDC ASSEMBLY 2018.doc." The document claims to be a registration form for an event with HDMC, an organization in Vietnam that advertises national independence and democracy. <https://blog.trendmicro.com/trendlabs-security-intelligence/new-macos-backdoor-linked-to-oceanlotus-found/>
Apr 2018	Steganography to Shroud Payloads The OceanLotus APT is using two new loaders which use steganography to read their encrypted payloads. <https://threatpost.com/oceanlotus-apt-uses-steganography-to-shroud-payloads/143373/>
May 2018	Watering Hole Attack using the Phnom Penh Post website The attack started just days after Australian mining magnate Bill Clough sold the newspaper to Malaysian spin doctor Sivakumar Ganapathy, who specializes in "covert PR". "Since last Tuesday [May 8], computers in our office were targeted by a malicious piece of code when we visited the Phnom Penh Post website," said Naly Pilorge, director of Licadho — one of Cambodia's leading human rights groups.

	<https://www.abc.net.au/news/2018-05-15/hackers-trigger-software-trap-after-phnom-penh-post-sale/9763906>
Mid-2018	Equation Editor exploit In mid-2018, OceanLotus carried out a campaign using documents abusing the weakness exposed by the CVE-2017-11882 vulnerability. Indeed, several Proofs-of-Concept were made available. The vulnerability resides in the component responsible for rendering and editing mathematical equations. <https://www.welivesecurity.com/2019/03/20/fake-or-fake-keeping-up-with-oceanlotus-decoys/>
Sep 2018	Watering Hole Attack in Southeast Asia ESET researchers have discovered a new watering hole campaign targeting several websites in Southeast Asia, and that is believed to have been active since September 2018. This campaign stands out because of its large scale, as we were able to identify 21 compromised websites, some of which are particularly notable. Among the compromised websites were the Ministry of Defense of Cambodia, the Ministry of Foreign Affairs and International Cooperation of Cambodia and several Vietnamese newspaper or blog websites. <https://www.welivesecurity.com/2018/11/20/oceanlotus-new-watering-hole-attack-southeast-asia/>
Jan 2019	Self-Extracting archives After using RTF files, the group started using self-extracting (SFX) archives that use common document icons in an attempt to further mislead their victims. It was briefly documented by Threatbook (in Chinese). When run, these self-extracting RAR files drop and execute DLL files (with a .ocx extension) with the final payload being the previously documented {A96B020F-0000-466F-A96D-A91BBF8EAC96}.dll. Since the middle of January 2019, OceanLotus began reusing the technique but changed some configuration over time.
Mar 2019	macOS malware update Early in March 2019, a new macOS malware sample from the OceanLotus group was uploaded to VirusTotal, a popular online multi-scanner service. This backdoor executable bears the same features as the previous macOS variant we looked at, but its structure has changed and its detection was made harder. Unfortunately, we couldn’t find the dropper associated with this sample so we do not know the initial compromise vector.

	<https://www.welivesecurity.com/2019/04/09/oceanlotus-macos-malware-update/>
Mar 2019	Malicious macro armed documents likely targeting ASEAN affairs and meeting members. Telemetry and spreading statistics related to these decoy documents highlight their diffusion in the geographical area of Thailand. <https://brica.de/alerts/alert/public/1258637/oceanlotus-on-asean-affairs/>
Mar 2019	Breach of Toyota in Australia, Japan, Thailand and Vietnam Toyota said the servers that hackers accessed stored sales information on up to 3.1 million customers. The carmaker said there's an ongoing investigation to find out if hackers exfiltrated any of the data they had access to. <https://www.zdnet.com/article/toyota-announces-second-security-breach-in-the-last-five-weeks/>
May 2019	Attacks to Indochinese Peninsula In this report, we share our summary of the latest attack techniques, attack payloads and related attacks of the OceanLotus, hoping that we can jointly improve understanding of OceanLotus group, an extremely active APT group. <https://ti.qianxin.com/blog/articles/oceanlotus-attacks-to-indochinese-peninsula-evolution-of-targets-techniques-and-procedure/>
Dec 2019	Breach of BMW and Hyundai <https://www.zdnet.com/article/bmw-and-hyundai-hacked-by-vietnamese-hackers-report-claims/>
Jan 2020	Vietnamese Threat Actors APT32 Targeting Wuhan Government and Chinese Ministry of Emergency Management in Latest Example of COVID-19 Related Espionage <https://www.fireeye.com/blog/threat-research/2020/04/apt32-targeting-chinese-government-in-covid-19-related-espionage.html>
2020	Throughout the year, Volexity identified multiple Vietnamese-language news websites that appeared to be compromised, as they were being used to load an OceanLotus web profiling framework. <https://www.volexity.com/blog/2020/11/06/oceanlotus-extending-cyber-espionage-operations-through-fake-websites/>
Jul 2020	New APT32 Malware Campaign Targets Cambodian Government <https://www.recordedfuture.com/apt32-malware-campaign/>

	Nov 2020	New MacOS Backdoor Connected to OceanLotus Surfaces <https://www.trendmicro.com/en_us/research/20/k/new-macos-backdoor-connected-to-oceanlotus-surfaces.html>
	Aug 2024	Advanced Persistent Threat Targeting Vietnamese Human Rights Defenders <https://www.huntress.com/blog/advanced-persistent-threat-targeting-vietnamese-human-rights-defenders>
Counter operations	Dec 2020	Taking Action Against Hackers in Bangladesh and Vietnam <https://about.fb.com/news/2020/12/taking-action-against-hackers-in-bangladesh-and-vietnam/>
Information	<https://www.fireeye.com/blog/threat-research/2017/05/cyber-espionage-apt32.html> <https://www.welivesecurity.com/wp-content/uploads/2018/03/ESET_OceanLotus.pdf> <https://www.cylance.com/content/dam/cylance-web/en-us/resources/knowledge-center/resource-library/reports/SpyRATsofOceanLotusMalwareWhitePaper.pdf> <https://www.riskiq.com/blog/analyst/oceanlotus/> <https://github.com/eset/malware-research/tree/master/oceanlotus>	
MITRE ATT&CK	<https://attack.mitre.org/groups/G0050/>	

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
