
APT
32
AXIAL

A SURVEY ON OCEAN LOTUS: ABOUT, WEAPON OF CHOICE, TECHNIQUES & ENGAGEMENTS

-NERDS OF AX1AL

I. ABOUT

APT32 also known as OceanLotus, SeaLotus, APT-C-00, SectorF01, CyberOne Security/CyberOne Technologies, Hanh Tinh Company Limited, Planet, and Diacauso is a State-sponsored Threat Group from Vietnam. It has been active since 2013 and has been targeting foreign corporations with an interest in Vietnam's manufacturing, consumer products, and hospitality sectors. It has also targeted Foreign Governments besides the private sectors. It has targeted several countries in Asia as well as the EU.

II. TARGET SECTORS

APT32's primary targets are Defence, Financial, Government, High-Tech, Hospitality, Manufacturing, Media, Retail, Telecommunications, and dissidents. Secondary Targets are human rights organizations, research institutes, and maritime construction firms in China. They have been heavily targeting the automotive sector since 2018.

III. METHODS USED

APT32 leverages a unique suite of fully-featured malware, in conjunction with commercially-available tools, to conduct targeted operations.

IV. IOC

C2

1. udt.sophiahoule[.]com
2. summerevent.webhop[.]net
3. dance-til-dawn.podzone[.]net
4. andreagahuvrauvin[.]com
5. 43.254.132[.]212.
6. browsersyn[.]com
7. log.osloger[.]biz
8. file.log4jv[.]info
9. news.sqllitlever[.]info
10. us.jaxonsorensen[.]club
11. staff.kristianfiedler[.]club
12. bit.catalinabonami[.]com
13. hr.halettebiermann[.]com
14. cyn.ettebiermahalet[.]com

MD5

- 0dd468ee3a4ec0f6f84473bd8428a1e1
- b28c80ca9a3b7deb09b275af1076eb55
- 2e06bbc26611305b28b40349a600f95c
- b1990e19efaf88206f7bffe9df0d9419
- c630ab7b51f0c0fa38a4a0f45c793e24
- ce5bae8714ddfca9eb3bb24ee60f042d
- d61c18e577cfc046a6252775da12294f
- fe15c0eacdbf5a46bc9b2af9c551f86a
- 07e01c2fa020724887fc39e5c97eccee
- 79f06cb9281177a51278b2a33090c867
- b107c35b4ca3e549bdf102de918749ba
- 83cd59e3ed1ba15f7a8cadfe9183e156
- c399d93146f3d12feb32da23b75304ba
- 83c423c36ecda310375e8a1f4348a35e
- 94a3ca93f1500b5bd7fd020569e46589
- 54777021c34b0aed226145fde8424991
- 872a3dd2cd5e01633b57fa5b9ac4648d
- 243e2c6433815f2ecc204ada4821e7d6

AX1AL

V. ENGAGEMENTS

- In April 2014, A backdoor Trojan on Google Play was being used by APT32. It was a long-term campaign known as Operation PhantomLance.
- August 2015, RSA found a satellite array of VPN services targeted towards the community of the People's Republic of China.
- In March 2017, the ASEAN site was compromised over several high-profile summit meetings.
- In May 2017, APT32 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. Dubbed as Operation Cobalt Kitty, the attackers compromised more than 40 PCs and servers, including the domain controller, file servers, Web application server, and database server.
- In the same month, Volexity tracked 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.
- In October 2017, Cylance incident responders and threat researchers uncovered several backdoors deployed by APT32 as well as evidence of the threat actor using obfuscated CobaltStrike Beacon payloads to perform C2.
- In April 2018, Trend Micro identified a macOS backdoor (detected as OSX_OCEANLOTUS.D) that is the latest version of a threat used by APT32. In the same month, it was discovered that the OceanLotus APT is using two new loaders that use steganography to read their encrypted payloads.
- In May 2018, APT32 started a Watering Hole Attack using the Phnom Penh Post Website targeting Cambodia's Human Rights group.
- In 2018, OceanLotus exploited CVE-2017-11882 vulnerability using documents.
- In September 2018, ESET Researchers discovered a new watering hole campaign targeting several websites in the SEA region.
- In March 2019, Malicious macro armed documents targeted ASEAN affairs and meeting members. Telemetry and spreading statistics related to these decoy documents highlight their diffusion in the geographical area of Thailand. In the same month, Toyota's servers in Australia, Japan, Thailand, and Vietnam were hacked and stored sales information on up to 3.1 million customers was stolen.
- In January 2020, APT32 Targeted Wuhan Government and Chinese Ministry of Emergency Management in COVID-19 Related Espionage.

VI. REFERENCES

- https://securelist.com/apt-phantomlance/96772/
- https://krebsonsecurity.com/2015/08/chinese-vpn-service-as-attack-platform/
- https://blogs.blackberry.com/en/2019/07/threat-spotlight-ratsnif-new-network-vermin-from-oceanlotus
- https://www.trendmicro.com/en_us/research/18/d/new-macos-backdoor-linked-to-oceanlotus-found.html
- https://blogs.blackberry.com/en/2018/10/report-the-spyrats-of-oceanlotus
- https://www.abc.net.au/news/2018-05-15/hackers-trigger-software-trap-after-phnom-penh-post-sale/9763906
- https://www.fireeye.com/blog/threat-research/2020/04/apt32-targeting-chinese-government-in-covid-19-related-espionage.html