Ocean Lotus APT Group (APT32)

brandefense.io/blog/apt-groups/ocean-lotus-apt-group/

BRANDEFENSE August 22, 2022

Threat Actor ID

Country	Vietnam
Sponsor	State-sponsored[1]
First Seen	2014
Motivation	Information theft and espionage
Methods	Watering Hole, Malware, Spearphishing
Other Names	APT32 (Mandiant)Ocean Lotus (SkyEye Labs) Ocean Buffalo (Crowd Strike) Tin Woodlawn (SecureWorks)

Group's Mission and Vision

The Ocean Lotus APT group is a hacker group operating against both private and government organizations and their opponents since 2014. The primary motivation behind the attacks carried out by the Ocean Lotus group is information theft and espionage – given the private information sought to be obtained in the attacks and the high-profile individuals targeted.

The targets of the Ocean Lotus group are generally foreign companies with sure success and interests in Vietnam's hospitality, manufacturing, and consumer goods sectors. As well as the private sector, the Ocean Lotus group targets politicians and journalists opposed to the Vietnamese government.

Targeted Countries & Industries

The cyberespionage group Ocean Lotus, active since 2014, targets organizations in various industries in Vietnam and other Southeast Asian countries.

- Indonesia,
- Iran,
- Japan,
- Laos,

- Malaysia,
- Myanmar,
- Nepal,
- Netherlands,
- Philippines,
- Singapore,
- South Korea,
- Thailand,
- UK,
- USA,
- Vietnam,
- ASEAN,
- Australia,
- Bangladesh,
- Brunei,
- Cambodia,
- China,
- Denmark,
- Germany,
- India.

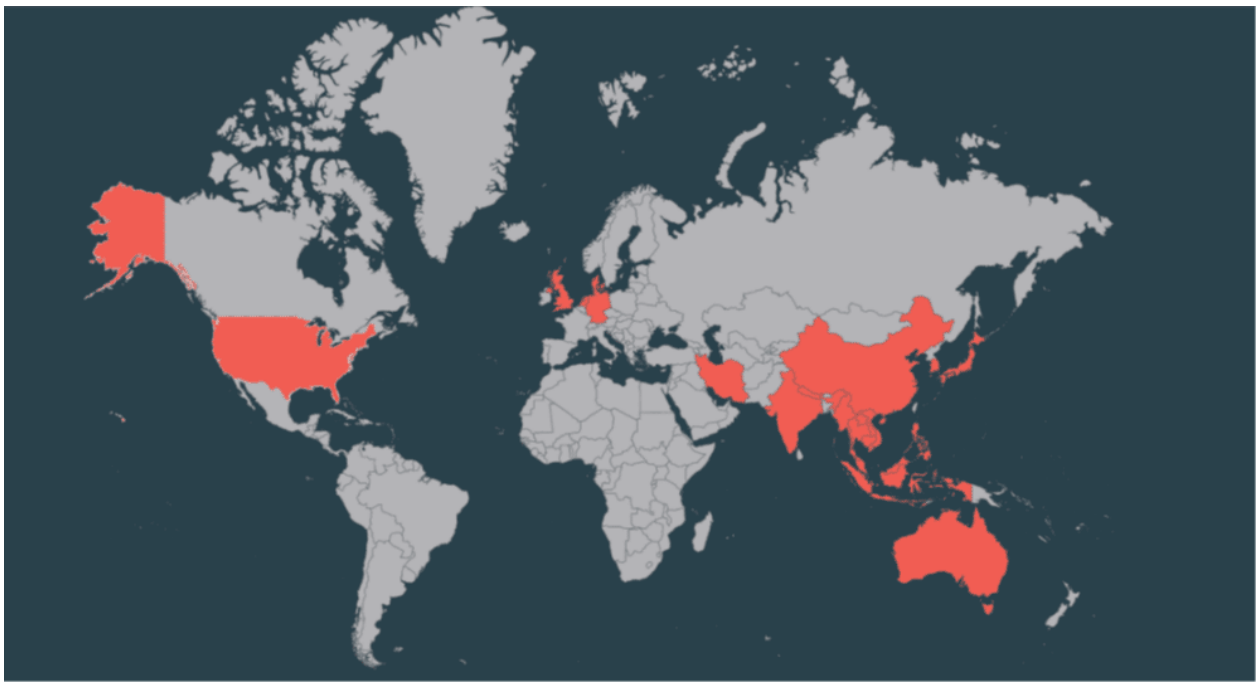

Figure 1: Targeted countries

- Ocean Lotus targeted dissidents and journalists operating against Vietnam.
- Ocean Lotus attempted to steal trade secrets by breaching the network security of automotive manufacturers BMW and Hyundai.

- Ocean Lotus targeted the Chinese Ministry of Emergency Management and the Wuhan Municipal Government to obtain information on the COVID-19 pandemic.
- Ocean Lotus compromised the mod.gov[.]kh domain of the Cambodia Ministry of Defense in its Watering Hole campaign.
- Ocean Lotus used mobile malware to attack mobile devices and steal confidential personal information such as SMS, call logs, connections, geolocation, and browser logs.

Various security vendors have reported that the Ocean Lotus group also has targeted finance, hospitality, and product sales sectors.

Operations Performed by APT32

In 2016, Ocean Lotus was observed targeting a number of Vietnamese organizations with a watering hole attack. The group used a website that masqueraded as a site for Vietnamese students studying abroad. When visitors to the site attempted to register for an account, they were redirected to a malicious website that served malware. This malware allowed Ocean Lotus to gain control of the victim's computer.

In 2017, Ocean Lotus carried out a campaign against Vietnam's National Assembly. The group sent spear phishing emails containing a link to a fake website that mimicked the National Assembly's intranet login page. Victims who attempted to log in had their credentials stolen by Ocean Lotus.

In 2018, Ocean Lotus launched a successful campaign against Vietnam's Ministry of Foreign Affairs. The group sent spear phishing emails containing a link to a fake website that mimicked the Ministry of Foreign Affairs intranet login page. Victims who attempted to log in had their credentials stolen by Ocean Lotus.

In 2019, Ocean Lotus was observed targeting a number of Vietnamese organizations with watering hole attacks. The group used websites that masqueraded as sites for Vietnamese students studying abroad. When visitors to the sites attempted to register for an account, they were redirected to malicious websites that served malware. This malware allowed Ocean Lotus to gain control of the victim's computer.

Ocean Lotus' operations have continued into 2020. **In February 2020,** the group was observed targeting Vietnamese organizations with a phishing campaign. The group sent emails containing a link to a fake website that mimicked the login page for Google's Gmail service. Victims who attempted to log in had their credentials stolen by Ocean Lotus.

Ocean Lotus has been active for over eight years and shows no signs of slowing down. The group is skilled in carrying out sophisticated attacks and is considered a serious threat to organizations in Vietnam and other Southeast Asian countries.

TTPs & Attack Lifecycle

The techniques, tactics, and procedures used by the Ocean Lotus group to violate the security of the target system in their attacks help define the threat group's characteristics and determine the countermeasures that can be taken. In addition, the information below will be helpful for an overview of how a typical attack lifecycle is performed with the software used by Ocean Lotus and for what purposes the tools are used.

Tactic	Tactic ID	Technique	Technique ID
Initial Access	TA0001	Drive-by CompromisePhishing •Spearphishing Attachment	T1189T1566 T1566.001
		•Spearphishing Link	T1566.002
		Valid Accounts	T1078
		•Local Accounts	T1078.003

Execution	TA0002	Command and Scripting Interpreter•JavaScript •PowerShell	T1059T1059.007 T1059.001
		•Visual Basic	T1059.005
		•Windows Command Shell	T1059.003
		Exploitation for Client Execution	T1203
		Scheduled Task/Job	T1053
		•Scheduled Task	T1053.005
		Software Deployment Tools	T1072
		System Services	T1569
		•Service Execution	T1569.002
		•Malicious File	T1204.002
		•Malicious Link	T1204.001
		Windows Management Instrumentation	T1047

Persistence	TA0003	Boot or Logon Autostart Execution•Registry Run Keys / Startup Folder Create or Modify System Process	T1547T1547.001 T1543
		•Windows Service	T1543.003
		Hijack Execution Flow	T1574
		•DLL Side-Loading	T1574.002
		Office Application Startup	T1137
		Server Software Component	T1505
		•Web Shell	T1505.003
Privilege Escalation	TA0004	Exploitation for Privilege EscalationProcess Injection	T1068T1055

Defense Evasion	TA0005	Hide Artifacts•Hidden Files and Directories •Hidden Window	T1564T1564.001 T1564.003
		•NTFS File Attributes	T1564.004
		Indicator Removal on Host	T1070
		•Clear Windows Event Logs	T1070.001
		•File Deletion	T1070.004
		•Timestomp	T1070.006
		Masquerading	T1036
		•Masquerade Task or Service	T1036.004
		•Match Legitimate Name or Location	T1036.005
		•Rename System Utilities	T1036.003
		Modify Registry	T1112
		Obfuscated Files or Information	T1027
		•Binary Padding	T1027.001
		System Binary Proxy Execution	T1218
		•Mshta	T1218.005
		•Regsvr32	T1218.010
		•Rundll32	T1218.011
			T1216

		System Script Proxy Execution	T1216.001
		•PubPrn	T1550
		Use Alternate Authentication Material	T1550.002
		•Pass the Hash	T1550.003
		•Pass the Ticket	
Credential Access	TA0006	Input Capture•Keylogging OS Credential Dumping	T1056T1056.001 T1003
		•LSASS Memory	T1003.001
		Unsecured Credentials	T1552
		•Credentials in Registry	T1552.002

Discovery	TA0007	Account Discovery•Local Account File and Directory Discovery	T1087T1087.001 T1083
		Network Service Discovery	T1046
		Network Share Discovery	T1135
		Query Registry	T1012
		Remote System Discovery	T1018
		System Information Discovery	T1082
		System Network Configuration Discovery	T1016
		System Network Connections Discovery	T1049
		System Owner/User Discovery	T1033

Tactic	Tactic ID	Technique	Technique ID
Lateral Movement	TA0008	Lateral Tool TransferRemote Services •SMB/Windows Admin Shares	T1570T1021 T1021.002
		Software Deployment Tools	T1072
Collection	TA0009	Archive Collected Data	T1560
Command and Control	TA0011	Application Layer Protocol•Mail Protocols •Web Protocols	T1071T1071.003 T1071.001
		Ingress Tool Transfer	T1105
		Non-Standard Port	T1571
		Web Service	T1102
Exfiltration	TA0010	Exfiltration Over Alternative Protocol•Exfiltration Over Unencrypted Non-C2 Protocol Exfiltration Over C2 Channel	T1048T1048.003 T1041

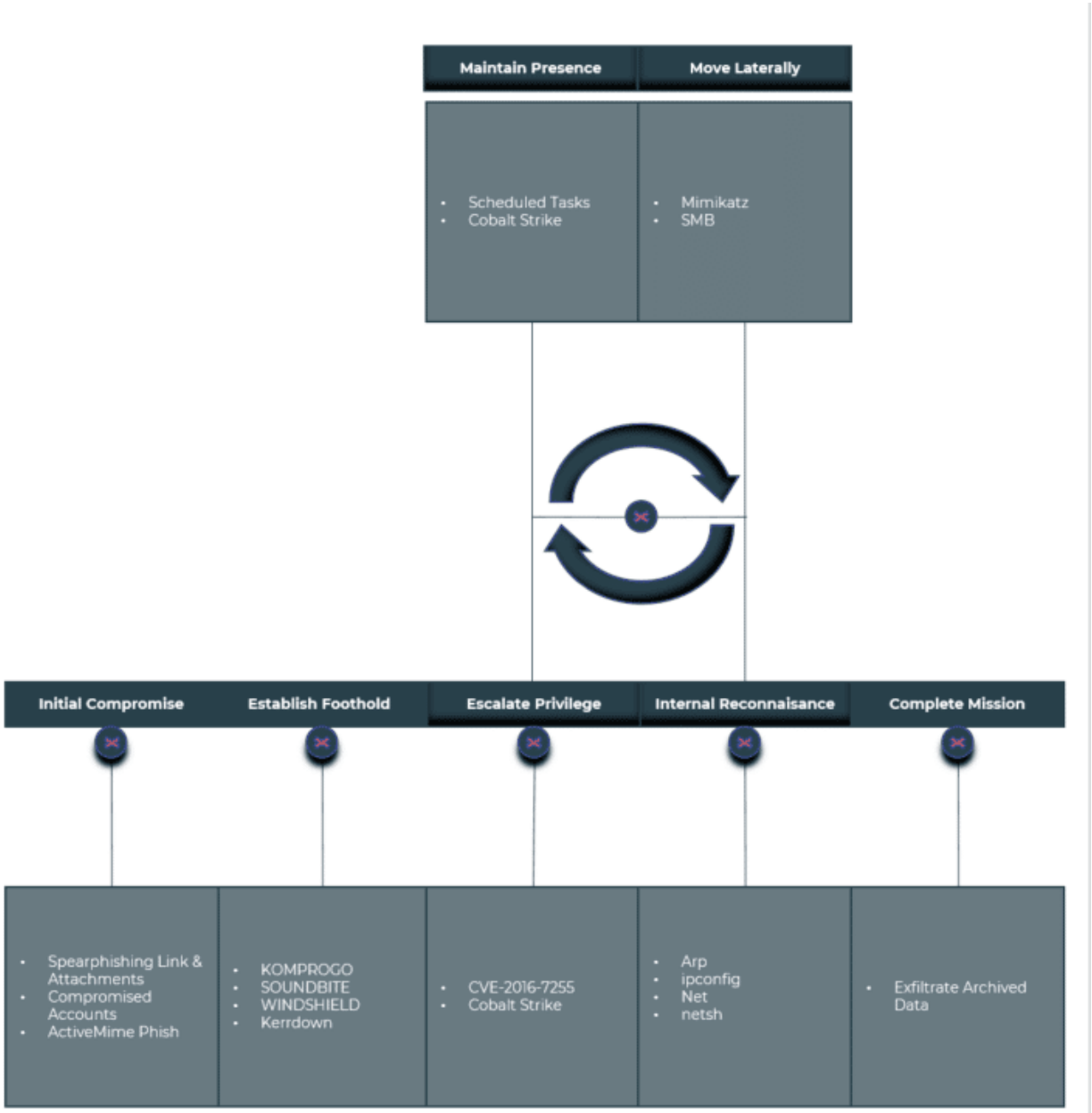

Figure 2: Attack Lifecycle Ocean Lotus / APT32

Recommendations & Mitigations

We have listed the steps to be taken in order to be protected from the threat and/or to minimize the possible damage according to the identified techniques, tactics, and procedures of the Ocean Lotus APT group.

- **Use strong passwords and multi-factor authentication:** This will help to protect your accounts from being compromised by password guessing or brute force attacks. Multi-factor authentication adds an extra layer of security by requiring another form of verification, such as a code sent to your mobile phone, in addition to your password.

- **Keep your software up to date:** Outdated software can contain security vulnerabilities that can be exploited by attackers. By ensuring that your software is up to date, you can help to close these potential entry points.
- **Install a reputable security suite:** A good security suite can provide protection against a wide range of threats, including viruses, malware, and phishing attacks.
- **Be cautious when opening email attachments:** Email attachments may contain malicious code that can infect your computer. Before opening an attachment, make sure that you trust the sender and that you have scanned the attachment for viruses using reliable antivirus software.
- **Don’t click on links in emails from unknown senders:** Emails from unknown or untrustworthy sources may contain malicious code/attachments.

Conclusion

Ocean Lotus is well-resourced and executes its attacks with precision and care. The group uses a variety of custom tools, which suggests a high level of technical capability. Additionally, the group appears to have significant financial resources, as evidenced by its use of 0-day exploits and ability to mount long-term operations.

> **Download IoCs**