APT32: APT32, active since 2014, is a Vietnam-based threat group targeting private industries, foreign governments, dissidents, and journalists, particularly in Southeast Asia (e.g., Vietnam, the Philippines, Laos, and Cambodia). They commonly use strategic web compromises to breach victims.

Associated Group Descriptions:

Name	Description
SeaLotus	[4]
OceanLotus	[1][2][4][5][6]
APT-C-00	[3][4][5][6]
Canvas Cyclone	[7]
BISMUTH	[7]

Techniques Used:

Domain	ID		Name	Use
Enterprise	T1087	.001	Account Discovery: Local Account	APT32 enumerated administrative users using the commands `net localgroup administrators`.[8]
Enterprise	T1583	.001	Acquire Infrastructure: Domains	APT32 has set up and operated websites to gather information and deliver malware.[9]

		.006	Acquire Infrastructure: Web Services	APT32 has set up Dropbox, Amazon S3, and Google Drive to host malicious downloads.[9]
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	APT32 has used JavaScript that communicates over HTTP or HTTPS to attacker controlled domains to download additional frameworks. The group has also used downloaded encrypted payloads over HTTP.[2][8]
		.003	Application Layer Protocol: Mail Protocols	APT32 has used email for C2 via an Office macro.[4][8]
Enterprise	T1560		Archive Collected Data	APT32's backdoor has used LZMA compression and RC4 encryption before exfiltration.[5]
Enterprise	T1547	.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	APT32 established persistence using Registry Run keys, both to execute PowerShell and VBS scripts as well as to execute their backdoor directly.[4][8][5]
Enterprise	T1059		Command and Scripting Interpreter	APT32 has used COM scriptlets to download Cobalt Strike beacons.[8]
		.001	PowerShell	APT32 has used PowerShell-based tools, PowerShell one-liners, and shellcode loaders for execution.[1][4][8]
		.003	Windows Command Shell	APT32 has used cmd.exe for execution.[8]

		.005	Visual Basic	APT32 has used macros, COM scriptlets, and VBS scripts.[4][8]
		.007	JavaScript	APT32 has used JavaScript for drive-by downloads and C2 communications.[8][9]
Enterprise	T1543	.003	Create or Modify System Process: Windows Service	APT32 modified Windows Services to ensure PowerShell scripts were loaded on the system. APT32 also creates a Windows service to establish persistence.[3][8][5]
Enterprise	T1189		Drive-by Compromise	APT32 has infected victims by tricking them into visiting compromised watering hole websites.[3][9]
Enterprise	T1585	.001	Establish Accounts: Social Media Accounts	APT32 has set up Facebook pages in tandem with fake websites.[9]
Enterprise	T1048	.003	Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted Non-C2 Protocol	APT32's backdoor can exfiltrate data by encoding it in the subdomain field of DNS packets.[5]
Enterprise	T1041		Exfiltration Over C2 Channel	APT32's backdoor has exfiltrated data using the already opened channel with its C&C server.[5]
Enterprise	T1203		Exploitation for Client Execution	APT32 has used RTF document that includes an exploit to execute malicious code. (CVE-2017-11882)[5]

Enterprise	T1068		Exploitation for Privilege Escalation	APT32 has used CVE-2016-7255 to escalate privileges.[1]
Enterprise	T1083		File and Directory Discovery	APT32's backdoor possesses the capability to list files and directories on a machine. [5]
Enterprise	T1222	.002	File and Directory Permissions Modification: Linux and Mac File and Directory Permissions Modification	APT32's macOS backdoor changes the permission of the file it wants to execute to 755.[10]
Enterprise	T1589		Gather Victim Identity Information	APT32 has conducted targeted surveillance against activists and bloggers.[6]
		.002	Email Addresses	APT32 has collected e-mail addresses for activists and bloggers in order to target them with spyware.[6]
Enterprise	T1564	.001	Hide Artifacts: Hidden Files and Directories	APT32's macOS backdoor hides the clientID file via a chflags function.[10]
		.003	Hide Artifacts: Hidden Window	APT32 has used the WindowStyle parameter to conceal PowerShellwindows. [1] [8]
		.004	Hide Artifacts: NTFS File Attributes	APT32 used NTFS alternate data streams to hide their payloads.[8]

Enterprise	T1574	.002	Hijack Execution Flow: DLL Side-Loading	APT32 ran legitimately-signed executables from Symantec and McAfee which load a malicious DLL. The group also side-loads its backdoor by dropping a library and a legitimate, signed executable (AcroTranscoder).[4][8][5]
Enterprise	T1070	.001	Indicator Removal: Clear Windows Event Logs	APT32 has cleared select event log entries.[1]
		.004	Indicator Removal: File Deletion	APT32's macOS backdoor can receive a "delete" command.[10]
		.006	Indicator Removal: Timestomp	APT32 has used scheduled task raw XML with a backdated timestamp of June 2, 2016. The group has also set the creation time of the files dropped by the second stage of the exploit to match the creation time of kernel32.dll. Additionally, APT32 has used a random value to modify the timestamp of the file storing the clientID.[1][5][10]
Enterprise	T1105		Ingress Tool Transfer	APT32 has added JavaScript to victim websites to download additional frameworks that profile and compromise website visitors.[2]
Enterprise	T1056	.001	Input Capture: Keylogging	APT32 has abused the PasswordChangeNotify to monitor for and capture account password changes.[8]
Enterprise	T1570		Lateral Tool Transfer	APT32 has deployed tools after moving laterally using administrative accounts.[8]

Enterprise	T1036		Masquerading	APT32 has disguised a Cobalt Strike beacon as a Flash Installer.[8]
		.003	Rename System Utilities	APT32 has moved and renamed pubprn.vbs to a .txt file to avoid detection.[11]
		.004	Masquerade Task or Service	APT32 has used hidden or non-printing characters to help masquerade service names, such as appending a Unicode no-break space character to a legitimate service name. APT32 has also impersonated the legitimate Flash installer file name "install_flashplayer.exe".[1]
		.005	Match Legitimate Name or Location	APT32 has renamed a NetCat binary to kb-10233.exe to masquerade as a Windows update. APT32 has also renamed a Cobalt Strike beacon payload to install_flashplayers.exe. [8][9]
Enterprise	T1112		Modify Registry	APT32's backdoor has modified the Windows Registry to store the backdoor's configuration. [5]
Enterprise	T1046		Network Service Discovery	APT32 performed network scanning on the network to search for open ports, services, OS finger-printing, and other vulnerabilities.[8]
Enterprise	T1135		Network Share Discovery	APT32 used the `net view` command to show all shares available, including the administrative shares such as `C$` and `ADMIN$`.[8]

Enterprise	T1571		Non-Standard Port	An APT32 backdoor can use HTTP over a non-standard TCP port (e.g 14146) which is specified in the backdoor configuration.[5]
Enterprise	T1027	.001	Obfuscated Files or Information: Binary Padding	APT32 includes garbage code to mislead anti-malware software and researchers.[3][5]
		.010	Obfuscated Files or Information: Command Obfuscation	APT32 has used the `Invoke-Obfuscation` framework to obfuscate their PowerShell.[1][12][8]
		.011	Obfuscated Files or Information: Fileless Storage	APT32's backdoor has stored its configuration in a registry key.[5]
		.013	Obfuscated Files or Information: Encrypted/Encoded File	APT32 has performed code obfuscation, including encoding payloads using Base64 and using a framework called "Dont-Kill-My-Cat (DKMC). APT32 also encrypts the library used for network exfiltration with AES-256 in CBC mode in their macOS backdoor.[1][12][3][4][8][5][10]
Enterprise	T1588	.002	Obtain Capabilities: Tool	APT32 has obtained and used tools such as Mimikatz and Cobalt Strike, and a variety of other open-source tools from GitHub.[1][4]
Enterprise	T1137		Office Application Startup	APT32 have replaced Microsoft Outlook's VbaProject.OTM file to install a backdoor macro for persistence.[4][8]
Enterprise	T1003		OS Credential Dumping	APT32 used GetPassword_x64 to harvest credentials.[4][8]

		.001	LSASS Memory	APT32 used Mimikatz and customized versions of Windows Credential Dumper to harvest credentials.[4][8]
Enterprise	T1566	.001	Phishing: Spearphishing Attachment	APT32 has sent spearphishing emails with a malicious executable disguised as a document or spreadsheet.[3][4][8][5][13][6]
		.002	Phishing: Spearphishing Link	APT32 has sent spearphishing emails containing malicious links.[3][4][13][9][6]
Enterprise	T1598	.003	Phishing for Information: Spearphishing Link	APT32 has used malicious links to direct users to web pages designed to harvest credentials.[9]
Enterprise	T1055		Process Injection	APT32 malware has injected a Cobalt Strike beacon into Rundll32.exe.[8]
Enterprise	T1012		Query Registry	APT32's backdoor can query the Windows Registry to gather system information. [5]
Enterprise	T1021	.002	Remote Services: SMB/Windows Admin Shares	APT32 used Net to use Windows' hidden network shares to copy their tools to remote machines for execution.[8]
Enterprise	T1018		Remote System Discovery	APT32 has enumerated DC servers using the command `net group "Domain Controllers" /domain`. The group has also used the `ping`command.[8]

Enterprise	T1053	.005	Scheduled Task/Job: Scheduled Task	APT32 has used scheduled tasks to persist on victim systems.[1][4][8][5]
Enterprise	T1505	.003	Server Software Component: Web Shell	APT32 has used Web shells to maintain access to victim websites.[2]
Enterprise	T1072		Software Deployment Tools	APT32 compromised McAfee ePO to move laterally by distributing malware as a software deployment task.[1]
Enterprise	T1608	.001	Stage Capabilities: Upload Malware	APT32 has hosted malicious payloads in Dropbox, Amazon S3, and Google Drive for use during targeting.[9]
		.004	Stage Capabilities: Drive-by Target	APT32 has stood up websites containing numerous articles and content scraped from the Internet to make them appear legitimate, but some of these pages include malicious JavaScript to profile the potential victim or infect them via a fake software update.[9]
Enterprise	T1218	.005	System Binary Proxy Execution: Mshta	APT32 has used mshta.exe for code execution.[4][8]
		.010	System Binary Proxy Execution: Regsvr32	APT32 created a Scheduled Task/Job that used regsvr32.exe to execute a COM scriptlet that dynamically downloaded a backdoor and injected it into memory. The group has also used regsvr32 to run their backdoor.[5][1][8]

		.011	System Binary Proxy Execution: Rundll32	APT32 malware has used rundll32.exe to execute an initial infection process.[8]
Enterprise	T1082		System Information Discovery	APT32 has collected the OS version and computer name from victims. One of the group's backdoors can also query the Windows Registry to gather system information, and another macOS backdoor performs a fingerprint of the machine on its first connection to the C&C server. APT32 executed shellcode to identify the name of the infected host.[3][5][10][13]
Enterprise	T1016		System Network Configuration Discovery	APT32 used the `ipconfig /all` command to gather the IP address from the system.[8]
Enterprise	T1049		System Network Connections Discovery	APT32 used the `netstat -anpo tcp` command to display TCP connections on the victim's machine.[8]
Enterprise	T1033		System Owner/User Discovery	APT32 collected the victim's username and executed the `whoami`command on the victim's machine. APT32 executed shellcode to collect the username on the victim's machine. [13][3][8]
Enterprise	T1216	.001	System Script Proxy Execution: PubPrn	APT32 has used PubPrn.vbs within execution scripts to execute malware, possibly bypassing defenses.[14]
Enterprise	T1569	.002	System Services: Service Execution	APT32's backdoor has used Windows services as a way to execute its malicious payload. [5]

Enterprise	T1552	.002	Unsecured Credentials: Credentials in Registry	APT32 used Outlook Credential Dumper to harvest credentials stored in Windows registry.[4][8]
Enterprise	T1550	.002	Use Alternate Authentication Material: Pass the Hash	APT32 has used pass the hash for lateral movement.[8]
		.003	Use Alternate Authentication Material: Pass the Ticket	APT32 successfully gained remote access by using pass the ticket.[8]
Enterprise	T1204	.001	User Execution: Malicious Link	APT32 has lured targets to download a Cobalt Strike beacon by including a malicious link within spearphishing emails.[8][9][6]
		.002	User Execution: Malicious File	APT32 has attempted to lure users to execute a malicious dropper delivered via a spearphishing attachment.[3][4][5][13][6]
Enterprise	T1078	.003	Valid Accounts: Local Accounts	APT32 has used legitimate local admin account credentials.[1]
Enterprise	T1102		Web Service	APT32 has used Dropbox, Amazon S3, and Google Drive to host malicious downloads.[9]
Enterprise	T1047		Windows Management Instrumentation	APT32 used WMI to deploy their tools on remote machines and to gather information about the Outlook process.[8]

Software

ID	Name	References	Techniques
S0099	Arp	[8]	Remote System Discovery, System Network Configuration Discovery

S0154	Cobalt Strike	[1][2][4][8][9][6][15]	Abuse Elevation Control Mechanism: Sudo and Sudo Caching, Abuse Elevation Control Mechanism: Bypass User Account Control, Access Token Manipulation: Parent PID Spoofing, Access Token Manipulation: Token Impersonation/Theft, Access Token Manipulation: Make and Impersonate Token, Account Discovery: Domain Account, Application Layer Protocol: DNS, Application Layer Protocol: Web Protocols, Application Layer Protocol: File Transfer Protocols, BITS Jobs, Browser Session Hijacking, Command and Scripting Interpreter: JavaScript, Command and Scripting Interpreter: Visual Basic, Command and Scripting Interpreter: PowerShell, Command and Scripting Interpreter: Python, Command and Scripting Interpreter: Windows Command Shell, Create or Modify System Process: Windows Service, Data Encoding: Standard Encoding, Data from Local System, Data Obfuscation: Protocol or Service Impersonation, Data Transfer Size Limits, Deobfuscate/Decode Files or Information, Encrypted Channel: Asymmetric Cryptography, Encrypted Channel: Symmetric Cryptography, Exploitation for Client Execution, Exploitation for Privilege Escalation, File and Directory Discovery, Hide Artifacts: Process Argument Spoofing, Impair Defenses: Disable or Modify Tools, Indicator Removal: Timestomp, Ingress Tool Transfer, Input Capture: Keylogging, Modify Registry, Native API, Network Service Discovery, Network Share Discovery, Non-Application Layer Protocol, Obfuscated Files or Information: Indicator Removal from Tools, Obfuscated Files or Information, Office Application Startup: Office Template Macros, OS Credential Dumping: LSASS Memory, OS Credential Dumping: Security Account Manager, Permission Groups Discovery: Domain Groups, Permission Groups Discovery: Local Groups,

			Process Discovery, Process Injection: Dynamic-link Library Injection, Process Injection: Process Hollowing, Process Injection, Protocol Tunneling, Proxy: Domain Fronting, Proxy: Internal Proxy, Query Registry, Reflective Code Loading, Remote Services: Remote Desktop Protocol, Remote Services: SSH, Remote Services: Windows Remote Management, Remote Services: SMB/Windows Admin Shares, Remote Services: Distributed Component Object Model, Remote System Discovery, Scheduled Transfer, Screen Capture, Software Discovery, Subvert Trust Controls: Code Signing, System Binary Proxy Execution: Rundll32, System Network Configuration Discovery, System Network Connections Discovery, System Service Discovery, System Services: Service Execution, Use Alternate Authentication Material: Pass the Hash, Valid Accounts: Domain Accounts, Valid Accounts: Local Accounts, Windows Management Instrumentation
S0354	Denis	[4][8]	Application Layer Protocol: DNS, Archive Collected Data: Archive via Library, Command and Scripting Interpreter: PowerShell, Command and Scripting Interpreter: Windows Command Shell, Data Encoding: Standard Encoding, Deobfuscate/Decode Files or Information, File and Directory Discovery, Hijack Execution Flow, Hijack Execution Flow: DLL Side-Loading, Indicator Removal: File Deletion, Ingress Tool Transfer, Native API, Obfuscated Files or Information: Command Obfuscation, Obfuscated Files or Information, Process Injection: Process Hollowing, Query Registry, System Information Discovery, System Network Configuration Discovery, System Owner/User Discovery, Virtualization/Sandbox Evasion: System Checks

S0477	Goopy	[8]	Application Layer Protocol: DNS, Application Layer Protocol: Web Protocols, Application Layer Protocol: Mail Protocols, Command and Scripting Interpreter: Visual Basic, Command and Scripting Interpreter: Windows Command Shell, Data from Local System, Deobfuscate/Decode Files or Information, Exfiltration Over C2 Channel, Hijack Execution Flow: DLL Side-Loading, Impair Defenses: Disable or Modify Tools, Indicator Removal: Clear Mailbox Data, Masquerading: Match Legitimate Name or Location, Native API, Obfuscated Files or Information, Obfuscated Files or Information: Binary Padding, Process Discovery, Scheduled Task/Job: Scheduled Task, System Owner/User Discovery
S0100	ipconfig	[8]	System Network Configuration Discovery
S0585	Kerrdown	[6][15]	Command and Scripting Interpreter: Visual Basic, Deobfuscate/Decode Files or Information, Hijack Execution Flow: DLL Side-Loading, Ingress Tool Transfer, Obfuscated Files or Information, Phishing: Spearphishing Link, Phishing: Spearphishing Attachment, System Information Discovery, User Execution: Malicious File, User Execution: Malicious Link
S0156	KOMPROGO	[1]	Command and Scripting Interpreter: Windows Command Shell, System Information Discovery, Windows Management Instrumentation

S0002	Mimikatz	[1][4][8]	Access Token Manipulation: SID-History Injection, Account Manipulation, Boot or Logon Autostart Execution: Security Support Provider, Credentials from Password Stores, Credentials from Password Stores: Credentials from Web Browsers, Credentials from Password Stores: Windows Credential Manager, OS Credential Dumping: DCSync, OS Credential Dumping: Security Account Manager, OS Credential Dumping: LSASS Memory, OS Credential Dumping: LSA Secrets, Rogue Domain Controller, Steal or Forge Authentication Certificates, Steal or Forge Kerberos Tickets: Golden Ticket, Steal or Forge Kerberos Tickets: Silver Ticket, Unsecured Credentials: Private Keys, Use Alternate Authentication Material: Pass the Hash, Use Alternate Authentication Material: Pass the Ticket
S0039	Net	[8]	Account Discovery: Domain Account, Account Discovery: Local Account, Account Manipulation: Additional Local or Domain Groups, Create Account: Local Account, Create Account: Domain Account, Indicator Removal: Network Share Connection Removal, Network Share Discovery, Password Policy Discovery, Permission Groups Discovery: Domain Groups, Permission Groups Discovery: Local Groups, Remote Services: SMB/Windows Admin Shares, Remote System Discovery, System Network Connections Discovery, System Service Discovery, System Services: Service Execution, System Time Discovery
S0108	netsh	[8]	Event Triggered Execution: Netsh Helper DLL, Impair Defenses: Disable or Modify System Firewall, Proxy, Software Discovery: Security Software Discovery

S0352	OSX_OCEANLOTUS.D	[16][6]	Application Layer Protocol: Web Protocols, Archive Collected Data: Archive via Library, Archive Collected Data: Archive via Custom Method, Command and Scripting Interpreter: Unix Shell, Command and Scripting Interpreter: Visual Basic, Command and Scripting Interpreter: PowerShell, Create or Modify System Process: Launch Agent, Create or Modify System Process: Launch Daemon, Data Encoding: Standard Encoding, Data from Local System, Deobfuscate/Decode Files or Information, Encrypted Channel: Symmetric Cryptography, File and Directory Permissions Modification: Linux and Mac File and Directory Permissions Modification, Hide Artifacts: Hidden Files and Directories, Indicator Removal: File Deletion, Indicator Removal: Timestomp, Ingress Tool Transfer, Masquerading: Masquerade Task or Service, Masquerading: Masquerade File Type, Non-Application Layer Protocol, Non-Standard Port, Obfuscated Files or Information: Encrypted/Encoded File, Obfuscated Files or Information: Software Packing, Shared Modules, Subvert Trust Controls: Gatekeeper Bypass, System Information Discovery, System Network Configuration Discovery, Virtualization/Sandbox Evasion: System Checks
S0158	PHOREAL	[1]	Command and Scripting Interpreter: Windows Command Shell, Modify Registry, Non-Application Layer Protocol

S1078	RotaJakiro	[17]	Automated Collection, Boot or Logon Autostart Execution: XDG Autostart Entries, Boot or Logon Initialization Scripts, Create or Modify System Process: Systemd Service, Data Encoding: Standard Encoding, Deobfuscate/Decode Files or Information, Encrypted Channel: Symmetric Cryptography, Event Triggered Execution: Unix Shell Configuration Modification, Exfiltration Over C2 Channel, Inter-Process Communication, Masquerading: Match Legitimate Name or Location, Native API, Non-Application Layer Protocol, Non-Standard Port, Process Discovery, Shared Modules, System Information Discovery
S0157	SOUNDBITE	[1]	Application Layer Protocol: DNS, Application Window Discovery, File and Directory Discovery, Modify Registry, System Information Discovery
S0155	WINDSHIELD	[1]	Indicator Removal: File Deletion, Non-Application Layer Protocol, Query Registry, System Information Discovery, System Owner/User Discovery

References

1. Carr, N.. (2017, May 14). Cyber Espionage is Alive and Well: APT32 and the Threat to Global Corporations. Retrieved June 18, 2017.
2. Lassalle, D., et al. (2017, November 6). OceanLotus Blossoms: Mass Digital Surveillance and Attacks Targeting ASEAN, Asian Nations, the Media, Human Rights Groups, and Civil Society. Retrieved November 6, 2017.
3. Foltýn, T. (2018, March 13). OceanLotus ships new backdoor using old tricks. Retrieved May 22, 2018.
4. Dahan, A. (2017, May 24). OPERATION COBALT KITTY: A LARGE-SCALE APT IN ASIA CARRIED OUT BY THE OCEANLOTUS GROUP. Retrieved November 5, 2018.
5. Dumont, R. (2019, March 20). Fake or Fake: Keeping up with OceanLotus decoys. Retrieved April 1, 2019.
6. Amnesty International. (2021, February 24). Vietnamese activists targeted by notorious hacking group. Retrieved March 1, 2021.
7. Microsoft . (2023, July 12). How Microsoft names threat actors. Retrieved November 17, 2023.

8. Dahan, A. (2017). Operation Cobalt Kitty. Retrieved December 27, 2018.
9. Adair, S. and Lancaster, T. (2020, November 6). OceanLotus: Extending Cyber Espionage Operations Through Fake Websites. Retrieved November 20, 2020.
1. Dumont, R.. (2019, April 9). OceanLotus: macOS malware update. Retrieved April 15, 2019.
2. Carr, N.. (2017, December 26). Nick Carr Status Update APT32 pubprn. Retrieved September 12, 2024.
3. Bohannon, D.. (2017, March 13). Invoke-Obfuscation - PowerShell Obfuscator. Retrieved June 18, 2017.
4. Henderson, S., et al. (2020, April 22). Vietnamese Threat Actors APT32 Targeting Wuhan Government and Chinese Ministry of Emergency Management in Latest Example of COVID-19 Related Espionage. Retrieved April 28, 2020.
5. Carr, N. (2017, December 22). ItsReallyNick Status Update. Retrieved September 12, 2024.
6. Ray, V. and Hayashi, K. (2019, February 1). Tracking OceanLotus’ new Downloader, KerrDown. Retrieved October 1, 2021.
7. Horejsi, J. (2018, April 04). New MacOS Backdoor Linked to OceanLotus Found. Retrieved November 13, 2018.
8. Alex Turing. (2021, May 6). RotaJakiro, the Linux version of the OceanLotus. Retrieved June 14, 2023.