APT32

attack.mitre.org/groups/G0050/

APT32 is a suspected Vietnam-based threat group that has been active since at least 2014. The group has targeted multiple private sector industries as well as foreign governments, dissidents, and journalists with a strong focus on Southeast Asian countries like Vietnam, the Philippines, Laos, and Cambodia. They have extensively used strategic web compromises to compromise victims.[1][2][3]

ID: G0050

ⓘ

Associated Groups: SeaLotus, OceanLotus, APT-C-00

Contributors: Romain Dumont, ESET

Version: 2.5

Created: 14 December 2017

Last Modified: 14 October 2021

Version Permalink
Live Version

Domain	ID		Name	Use
Enterprise	T1087	.001	Account Discovery: Local Account	APT32 enumerated administrative users using the commands `net localgroup administrators`.[7]

Domain	ID	Name	Use	
Enterprise	T1583	.001	Acquire Infrastructure: Domains	APT32 has set up and operated websites to gather information and deliver malware.[8]
		.006	Acquire Infrastructure: Web Services	APT32 has set up Dropbox, Amazon S3, and Google Drive to host malicious downloads.[8]
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][7]
		.003	Application Layer Protocol: Mail Protocols	APT32 has used email for C2 via an Office macro.[4][7]
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][7][5]
Enterprise	T1059	Command and Scripting Interpreter	APT32 has used COM scriptlets to download Cobalt Strike beacons.[7]	

Domain	ID	Name	Use	
		.001	PowerShell	APT32 has used PowerShell-based tools, PowerShell one-liners, and shellcode loaders for execution.[1][4][7]
		.003	Windows Command Shell	APT32 has used cmd.exe for execution.[7]
		.005	Visual Basic	APT32 has used macros, COM scriptlets, and VBS scripts.[4][7]
		.007	JavaScript	APT32 has used JavaScript for drive-by downloads and C2 communications.[7][8]
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][7][5]
Enterprise	T1189	Drive-by Compromise	APT32 has infected victims by tricking them into visiting compromised watering hole websites.[3][8]	
Enterprise	T1585	.001	Establish Accounts: Social Media Accounts	APT32 has set up Facebook pages in tandem with fake websites.[8]
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]

Domain	ID	Name	Use	
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.[9]
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]

Domain	ID	Name	Use	
Enterprise	T1564	.001	Hide Artifacts: Hidden Files and Directories	APT32's macOS backdoor hides the clientID file via a chflags function.[9]
		.003	Hide Artifacts: Hidden Window	APT32 has used the WindowStyle parameter to conceal PowerShell windows. [1] [7]
		.004	Hide Artifacts: NTFS File Attributes	APT32 used NTFS alternate data streams to hide their payloads.[7]
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][7][5]
Enterprise	T1070	.001	Indicator Removal on Host: Clear Windows Event Logs	APT32 has cleared select event log entries.[1]
		.004	Indicator Removal on Host: File Deletion	APT32's macOS backdoor can receive a "delete" command.[9]

Domain	ID	Name	Use	
		.006	Indicator Removal on Host: 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][9]
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.[7]
Enterprise	T1570	Lateral Tool Transfer	APT32 has deployed tools after moving laterally using administrative accounts.[7]	
Enterprise	T1036	Masquerading	APT32 has disguised a Cobalt Strike beacon as a Flash Installer.[7]	
		.003	Rename System Utilities	APT32 has moved and renamed pubprn.vbs to a .txt file to avoid detection.[16]

Domain	ID	Name	Use	
		.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.[7][8]
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.[7]	
Enterprise	T1135	Network Share Discovery	APT32 used the `net view` command to show all shares available, including the administrative shares such as `C$` and `ADMIN$`.[7]	

Domain	ID	Name	Use	
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	Obfuscated Files or Information	APT32 uses the Invoke-Obfuscation framework to obfuscate their PowerShell and also performs other code obfuscation. APT32 has also encoded payloads using Base64 and 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][11][3][4][7][5][9]	
		.001	Binary Padding	APT32 includes garbage code to mislead anti-malware software and researchers.[3][5]
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][7]	

Domain	ID	Name	Use	
Enterprise	T1003	OS Credential Dumping	APT32 used GetPassword_x64 to harvest credentials.[4][7]	
		.001	LSASS Memory	APT32 used Mimikatz and customized versions of Windows Credential Dumper to harvest credentials.[4][7]
Enterprise	T1566	.001	Phishing: Spearphishing Attachment	APT32 has sent spearphishing emails with a malicious executable disguised as a document or spreadsheet.[3][4][7][5][12][6]
		.002	Phishing: Spearphishing Link	APT32 has sent spearphishing emails containing malicious links.[3][4][12][8][9]
Enterprise	T1598	.003	Phishing for Information: Spearphishing Link	APT32 has used malicious links to direct users to web pages designed to harvest credentials.[8]
Enterprise	T1055	Process Injection	APT32 malware has injected a Cobalt Strike beacon into Rundll32.exe.[7]	
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.[7]

Domain	ID	Name	Use	
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.[7]	
Enterprise	T1053	.005	Scheduled Task/Job: Scheduled Task	APT32 has used scheduled tasks to persist on victim systems.[1][4][7][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.[8]
		.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.[8]

Domain	ID	Name	Use	
Enterprise	T1218	.005	System Binary Proxy Execution: Mshta	APT32 has used mshta.exe for code execution.[4][7]
		.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][7]
		.011	System Binary Proxy Execution: Rundll32	APT32 malware has used rundll32.exe to execute an initial infection process.[7]
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][9][12]	
Enterprise	T1016	System Network Configuration Discovery	APT32 used the `ipconfig /all` command to gather the IP address from the system.[7]	

Domain	ID	Name	Use	
Enterprise	T1049	System Network Connections Discovery	APT32 used the `netstat -anpo tcp` command to display TCP connections on the victim's machine.[7]	
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. [12][3][7]	
Enterprise	T1216	.001	System Script Proxy Execution: PubPrn	APT32 has used PubPrn.vbs within execution scripts to execute malware, possibly bypassing defenses.[13]
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][7]
Enterprise	T1550	.002	Use Alternate Authentication Material: Pass the Hash	APT32 has used pass the hash for lateral movement.[7]
		.003	Use Alternate Authentication Material: Pass the Ticket	APT32 successfully gained remote access by using pass the ticket.[7]

Domain	ID	Name	Use	
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.[7][8][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][12][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.[8]	
Enterprise	T1047	Windows Management Instrumentation	APT32 used WMI to deploy their tools on remote machines and to gather information about the Outlook process.[7]	