Threat Assessment: Hangover Threat Group

By Doel Santos, Alex Hinchliffe

Published: 2020-06-04 · Archived: 2026-04-02 10:47:20 UTC

Unit 42 researchers recently published on activity by the Hangover threat group (aka Neon, Viceroy Tiger, MONSOON) carrying out targeted cyberattacks deploying BackConfig malware attacks against government and military organizations in South Asia. As a result, we've created this threat assessment report for the Hangover Group's activities. The techniques and campaigns can be visualized using the Unit 42 Playbook Viewer.

Hangover Group is a cyberespionage group that was first observed in December 2013 carrying on a cyberattack against a telecom corporation in Norway. Cybersecurity firm Norman reported that the cyberattacks were emerging from India and the group sought and carried on attacks against targets of national interest, such as Pakistan and China. However, there have been indicators of Hangover activity in the U.S. and Europe. Mainly focusing on government, military, and civilian organizations. The Hangover Group's initial vector of compromise is to carry out spear-phishing campaigns. The group uses local and topical news lures from the South Asia region to make their victims more prone to falling into their social engineering techniques, making them download and execute a weaponized Microsoft Office document. After the user executes the weaponized document, backdoor communication is established between BackConfig and the threat actors, allowing attackers to carry on espionage activity, potentially exfiltrating sensitive data from compromised systems.

Palo Alto Networks Threat Prevention platform with WildFire, DNS Security and Cortex XDR detects activity associated with this threat group. Customers can also review activity associated with this Threat Assessment using AutoFocus with the following tags: Hangover and BackConfig.

Several adversarial techniques were observed in this activity and the following measures are suggested within Palo Alto Networks' products and services to ensure mitigation of threats related with the Hangover Group, as well as other groups using the same techniques:

Tactic	**Technique** **(Mitre ATT&CK ID)**	**Product / Service**	**Course of Action**
Initial Access	Spearphishing Link (T1192)	NGFW	Ensure application security policies exist when allowing traffic from an untrusted zone to a more trusted zone
			Ensure 'Service setting of ANY' in a security policy allowing traffic does not exist
			Ensure 'Security Policy' denying any/all traffic to/from IP addresses on Trusted Threat

			Intelligence Sources Exists
		Threat Prevention†	Ensure that antivirus profiles are set to block on all decoders except 'imap' and 'pop3'
			Ensure a secure antivirus profile is applied to all relevant security policies
			Ensure that User Credential Submission uses the action of 'block' or 'continue' on the URL categories
		DNS Security	Enable DNS Security in Anti-Spyware profile
		URL Filtering	Ensure that PAN-DB URL Filtering is used
			Ensure that URL Filtering uses the action of 'block' or 'override' on the <enterprise approved value> URL categories
			Ensure that access to every URL is logged
			Ensure all HTTP Header Logging options are enabled
			Ensure secure URL filtering is enabled for all security policies allowing traffic to the Internet
		WildFire	Ensure that WildFire file size upload limits are maximized
			Ensure forwarding of decrypted content to WildFire is enabled
			Ensure all WildFire session information settings are enabled
			Ensure alerts are enabled for malicious files detected by WildFire
			Ensure 'WildFire Update Schedule' is set to download and install updates every minute

Execution	Exploitation for Client Execution (T1203)	Threat Prevention†	Ensure a Vulnerability Protection Profile is set to block attacks against critical and high vulnerabilities, and set to default on medium, low, and informational vulnerabilities
			Ensure a secure Vulnerability Protection Profile is applied to all security rules allowing traffic
		Cortex XDR	Enable Anti-Exploit and Anti-Malware Protection
	User Execution (T1204)	NGFW	Ensure that User-ID is only enabled for internal trusted interfaces
			Ensure that 'Include/Exclude Networks' is used if User-ID is enabled
			Ensure that the User-ID Agent has minimal permissions if User-ID is enabled
			Ensure that the User-ID service account does not have interactive logon rights
			Ensure remote access capabilities for the User-ID service account are forbidden.
			Ensure that security policies restrict User-ID Agent traffic from crossing into untrusted zones
		Threat Prevention†	Ensure that antivirus profiles are set to block on all decoders except 'imap' and 'pop3'
			Ensure a secure antivirus profile is applied to all relevant security policies
			Ensure an anti-spyware profile is configured to block on all spyware severity levels, categories, and threats
			Ensure DNS sinkholing is configured on all anti-spyware profiles in use
			Ensure passive DNS monitoring is set to enabled on all anti-spyware profiles in use

			Ensure a secure anti-spyware profile is applied to all security policies permitting traffic to the Internet
		DNS Security	Enable DNS Security in Anti-Spyware profile
		URL Filtering	Ensure that PAN-DB URL Filtering is used
			Ensure that URL Filtering uses the action of 'block' or 'override' on the <enterprise approved value> URL categories
			Ensure that access to every URL is logged
			Ensure all HTTP Header Logging options are enabled
			Ensure secure URL filtering is enabled for all security policies allowing traffic to the Internet
		WildFire	Ensure that WildFire file size upload limits are maximized
			Ensure forwarding of decrypted content to WildFire is enabled
			Ensure all WildFire session information settings are enabled
			Ensure alerts are enabled for malicious files detected by WildFire
			Ensure 'WildFire Update Schedule' is set to download and install updates every minute
		Cortex XDR	Enable Anti-Exploit and Anti-Malware Protection
	Scripting (T1064)	WildFire	Ensure that WildFire file size upload limits are maximized
			Ensure forwarding of decrypted content to WildFire is enabled
			Ensure all WildFire session information settings are enabled

			Ensure alerts are enabled for malicious files detected by WildFire
			Ensure 'WildFire Update Schedule' is set to download and install updates every minute
		Cortex XDR	Enable Anti-Exploit and Anti-Malware Protection
Defense Evasion	BITS Jobs (T1197)	NGFW	Ensure that User-ID is only enabled for internal trusted interfaces
			Ensure that 'Include/Exclude Networks' is used if User-ID is enabled
			Ensure that the User-ID Agent has minimal permissions if User-ID is enabled
			Ensure that the User-ID service account does not have interactive logon rights
			Ensure remote access capabilities for the User-ID service account are forbidden.
			Ensure that security policies restrict User-ID Agent traffic from crossing into untrusted zones
			Ensure application security policies exist when allowing traffic from an untrusted zone to a more trusted zone
			Ensure 'Service setting of ANY' in a security policy allowing traffic does not exist
			Ensure 'Security Policy' denying any/all traffic to/from IP addresses on Trusted Threat Intelligence Sources Exists
		Cortex XDR	Configure Host Firewall Profile
	Code Signing (T1116)	Cortex XDR	Enable Anti-Exploit and Anti-Malware Protection
	Hidden Files and Directories (T1158)	Cortex XDR	Configure Behavioral Threat Protection under the Malware Security Profile

	Deobfuscate/Decode Files or Information (T1140)	WildFire	Ensure that WildFire file size upload limits are maximized
			Ensure forwarding of decrypted content to WildFire is enabled
			Ensure all WildFire session information settings are enabled
			Ensure alerts are enabled for malicious files detected by WildFire
			Ensure 'WildFire Update Schedule' is set to download and install updates every minute
	Obfuscated Files or Information (T1027)	WildFire	Ensure that WildFire file size upload limits are maximized
			Ensure forwarding of decrypted content to WildFire is enabled
			Ensure all WildFire session information settings are enabled
			Ensure alerts are enabled for malicious files detected by WildFire
			Ensure 'WildFire Update Schedule' is set to download and install updates every minute
		Cortex XDR	Enable Anti-Exploit and Anti-Malware Protection
Command and Control	Commonly Used Port (T1043)	NGFW	Ensure application security policies exist when allowing traffic from an untrusted zone to a more trusted zone
			Ensure 'Service setting of ANY' in a security policy allowing traffic does not exist
			Ensure 'Security Policy' denying any/all traffic to/from IP addresses on Trusted Threat Intelligence Sources Exists
		URL Filtering	Ensure that PAN-DB URL Filtering is used
			Ensure that URL Filtering uses the action of 'block' or 'override' on the <enterprise

			approved value> URL categories
			Ensure that access to every URL is logged
			Ensure all HTTP Header Logging options are enabled
			Ensure secure URL filtering is enabled for all security policies allowing traffic to the Internet
	Standard Cryptographic Protocol (T1032)	NGFW	Ensure 'SSL Forward Proxy Policy' for traffic destined to the Internet is configured
			Ensure 'SSL Inbound Inspection' is required for all untrusted traffic destined for servers using SSL or TLS
			Ensure that the Certificate used for Decryption is Trusted
			Ensure application security policies exist when allowing traffic from an untrusted zone to a more trusted zone
			Ensure 'Service setting of ANY' in a security policy allowing traffic does not exist
			Ensure 'Security Policy' denying any/all traffic to/from IP addresses on Trusted Threat Intelligence Sources Exists
		Threat Prevention†	Ensure that antivirus profiles are set to block on all decoders except 'imap' and 'pop3'
			Ensure a secure antivirus profile is applied to all relevant security policies
			Ensure an anti-spyware profile is configured to block on all spyware severity levels, categories, and threats
			Ensure DNS sinkholing is configured on all anti-spyware profiles in use
			Ensure passive DNS monitoring is set to enabled on all anti-spyware profiles in use

			Ensure a secure anti-spyware profile is applied to all security policies permitting traffic to the Internet
		DNS Security	Enable DNS Security in Anti-Spyware profile
		URL Filtering	Ensure that PAN-DB URL Filtering is used
			Ensure that URL Filtering uses the action of 'block' or 'override' on the <enterprise approved value> URL categories
			Ensure that access to every URL is logged
			Ensure all HTTP Header Logging options are enabled
			Ensure secure URL filtering is enabled for all security policies allowing traffic to the Internet
		WildFire	Ensure that WildFire file size upload limits are maximized
			Ensure forwarding of decrypted content to WildFire is enabled
			Ensure all WildFire session information settings are enabled
			Ensure alerts are enabled for malicious files detected by WildFire
			Ensure 'WildFire Update Schedule' is set to download and install updates every minute
	Remote File Copy (T1105)	NGFW	Ensure application security policies exist when allowing traffic from an untrusted zone to a more trusted zone
			Ensure 'Service setting of ANY' in a security policy allowing traffic does not exist
			Ensure 'Security Policy' denying any/all traffic to/from IP addresses on Trusted Threat Intelligence Sources Exists

		WildFire	Ensure that WildFire file size upload limits are maximized
			Ensure forwarding of decrypted content to WildFire is enabled
			Ensure all WildFire session information settings are enabled
			Ensure alerts are enabled for malicious files detected by WildFire
			Ensure 'WildFire Update Schedule' is set to download and install updates every minute
	Standard Application Layer Protocol (T1071)	NGFW	Ensure application security policies exist when allowing traffic from an untrusted zone to a more trusted zone
			Ensure 'Service setting of ANY' in a security policy allowing traffic does not exist
			Ensure 'Security Policy' denying any/all traffic to/from IP addresses on Trusted Threat Intelligence Sources Exists
		Threat Prevention†	Ensure that antivirus profiles are set to block on all decoders except 'imap' and 'pop3'
			Ensure a secure antivirus profile is applied to all relevant security policies
			Ensure an anti-spyware profile is configured to block on all spyware severity levels, categories, and threats
			Ensure DNS sinkholing is configured on all anti-spyware profiles in use
			Ensure passive DNS monitoring is set to enabled on all anti-spyware profiles in use
			Ensure a secure anti-spyware profile is applied to all security policies permitting traffic to the Internet
		DNS Security	Enable DNS Security in Anti-Spyware profile

		URL Filtering	Ensure that PAN-DB URL Filtering is used
			Ensure that URL Filtering uses the action of 'block' or 'override' on the <enterprise approved value> URL categories
			Ensure that access to every URL is logged
			Ensure all HTTP Header Logging options are enabled
			Ensure secure URL filtering is enabled for all security policies allowing traffic to the Internet

Table 1. Courses of Action for Hangover Group
†These capabilities are part of the NGFW security subscriptions service

---