


## Mphasis SOC – Information Security News

### Date & Time Issued: 28-JUN-2024, 21:30 IST

<b>Title</b>	<b>Attackers Exploit Cobalt Strike Profiles</b>	
<b>Summary</b>	<ul style="list-style-type: none"> <li>Palo Alto researchers have uncovered new malicious uses of Cobalt Strike, a tool design for cybersecurity testing but often misused by cybercriminals. There are some instances where attackers modify Malleable C2 profiles to conceal Cobalt Strike's traffic, making it difficult to detect.</li> <li>These profiles, originally shared on public repositories for legitimate purposes, are easily replicated and changed by attackers. Analyzing profiles and document alterations in HTTP paths and User-Agent details, show how attackers modify them to avoid being detected. The evolving tactics of attackers pose a challenge for traditional network security due to the variety of profile variations.</li> <li>Recent findings of malicious Cobalt Strike infrastructure. We also share examples of malicious Cobalt Strike samples that use Malleable C2 configuration profiles derived from the same profile hosted on a public code repository.</li> </ul>	
<b>Severity</b>	Medium 	
<b>Attack Vectors</b>	<ul style="list-style-type: none"> <li>Threat actors continue to leverage Cobalt Strike for malicious purposes. Due to its malleable and evasive nature, Cobalt Strike remains a significant security threat to organizations.</li> <li>Beacon Traffic: Cobalt Strike uses “beacons” to maintain communication with compromised systems. Look for unusual or unexpected network traffic patterns, especially if they involve encrypted or obfuscated data.</li> <li>Suspicious Processes: Monitor running processes for any unusual executables or services. Cobalt Strike often disguises itself as legitimate system processes or services.</li> <li>Process Injection: Cobalt Strike injects its code into other processes to evade detection. Keep an eye out for signs of process hollowing or reflective DLL injection.</li> <li>Network Scans: Attackers using Cobalt Strike may perform network scans to identify vulnerable systems. Look for unusual scanning activity originating from internal hosts.</li> <li>Lateral Movement: Cobalt Strike enables lateral movement within a network. Watch for unusual authentication attempts, lateral connections, or privilege escalation.</li> <li>Unusual DNS Requests: Cobalt Strike may use DNS tunneling for communication. Monitor DNS logs for suspicious domain requests.</li> <li>Encoded or Encrypted Traffic: Cobalt Strike can obfuscate its network traffic. Analyze network packets for signs of base64 encoding, XOR operations, or other encryption techniques.</li> </ul>	
<b>Indicator of Compromise</b>	INDICATOR TYPE	INDICATORS
	Domain	<ul style="list-style-type: none"> <li>msupdate.azurefd[.]net</li> <li>o365updater.azureedge[.]net</li> <li>gupdater.bbteco[.]com</li> <li>teamsupd.azurewebsites[.]net</li> <li>msdn1357.centralus.cloudapp.azure[.]com</li> <li>cupdater.bbteco[.]com</li> <li>msupdate.brazilsouth.cloudapp.azure[.]com</li> <li>msdn1357.centralus.cloudapp.azure[.]com</li> <li>update37.eastus.cloudapp.azure[.]com</li> <li>update.westus.cloudapp.azure[.]com</li> <li>www.consumershop.lenovo.com.cn.d4e97cc6.cdnhwggk22[.]com</li> </ul>
	IP	<ul style="list-style-type: none"> <li>146.235.52[.]69</li> <li>159.112.177[.]137</li> </ul>
	File Hash	<ul style="list-style-type: none"> <li>38eeb82dbb5285ff6a2122a065cd1f820438b88a02057f4e31a1e1e5339feb2b</li> </ul>
<b>Recommendations</b>	<p>Palo Alto Networks customers are better protected from Cobalt Strike through the following products:</p> <ul style="list-style-type: none"> <li>The Next-Generation Firewall (NGFW) with an Advanced Threat Prevention subscription can identify and block Cobalt Strike HTTP C2 requests generated by custom profiles and block Cobalt Strike HTTP C2 requests.</li> <li>Advanced WildFire, Cortex XDR and Prisma Cloud can identify and block Cobalt Strike Beacon binaries, and XDR will report related exploitation attempts.</li> <li>Cortex XSOAR response pack and playbook can automate the mitigation process.</li> <li>Malicious URLs and IPs have been added to Advanced URL Filtering.</li> </ul>	

- Endpoint Protection: Deploy advanced endpoint protection solutions that can identify and block malicious executables.
- Patch Management: Keep software and systems up to date to prevent exploitation of known vulnerabilities.
- User Training: Educate employees about phishing, social engineering, and safe browsing practices.

**NOTE: The recommended settings/controls should be implemented after due shall be tested on Pre -Prod or test environment before implementing. diligence and impact analysis.**

## References

- <https://unit42.paloaltonetworks.com/attackers-exploit-public-cobalt-strike-profiles/>

The information contained in this message is proprietary. It is for Mphasis and its customers only.  
Copyright © 2023. All rights reserved by Mphasis.