


## Mphasis SOC – Information Security News

Date & Time Issued: 26-06-2024, 5:00 IST

Title	<b>New Cyberthreat 'Boolka' Deploying BMANAGER Trojan via SQLi Attacks</b>	
Summary	<ul style="list-style-type: none"> <li>Threat actor dubbed Boolka has been observed compromising websites with malicious scripts to deliver a modular trojan codenamed BMANAGER.</li> <li>The threat actor behind this campaign has been carrying out opportunistic SQL injection attacks against websites in various countries since at least 2022.</li> <li>Over the last three years, the threat actors have been infecting vulnerable websites with malicious JavaScript scripts capable of intercepting any data entered on an infected website.</li> <li>Boolka is the third actor after GambleForce and ResumeLooters to leverage SQL injection attacks to steal sensitive data in recent months.</li> </ul>	
Severity	Medium 	
Attack Vectors	<ul style="list-style-type: none"> <li>Boolka gets its name from the JavaScript code inserted into the website that beacons out to a command-and-control server named "boolka[.]tk" every time an unsuspecting visitor lands on the infected site.</li> <li>The JavaScript is also designed to collect and exfiltrate user inputs and interactions in a Base64-encoded format, indicating the use of the malware to grab sensitive details like credentials and other personal information.</li> <li>Furthermore, it redirects users to a bogus loading page that prompts victims to download and install a browser extension when, in reality, it drops a downloader for the BMANAGER trojan, which, in turn, attempts to fetch the malware from a hard-coded URL. The malware delivery framework is based on the BeEF framework.</li> <li>The trojan, for its part, serves as a conduit to deploy four additional modules, including BMBACKUP (harvest files from particular paths), BMHOOK (record which applications are running and have keyboard focus), BMLOG (log keystrokes), and BMREADER (export stolen data). It also sets up persistence on the host using scheduled tasks.</li> <li>The injection of malicious JavaScript snippets into vulnerable websites for data exfiltration, and then the use of the BeEF framework for malware delivery, reflects the step-by-step development of the attacker's competencies.</li> </ul>	
Indicator of Compromise	INDICATOR TYPE	INDICATORS
	File Hash	<ul style="list-style-type: none"> <li>2f10a81bc5a1aad7230cec197af987d00e5008edca205141ac74bc6219ea1802</li> <li>7266f20123edcb2e0b92ac0b63225b8db2c5ff349818b339ef1553bff06719e4</li> <li>9434e2f277f764bb75302cd5355ed45f7624f1d993a454a7dbaf68b7e9b4b3a2</li> <li>b2dbd3187c67883c0f77c17530f41e05950e9e38b2798773770fe37f5985e367</li> <li>94430690ac9516a25ca764bae8c4b5a88d6f0308f558aea43ca50b5f750685ee</li> <li>227b8233071da4d3015cb04b69285885100c9f2e5d98b803b37d23afb798375a</li> </ul>
	Domain	<ul style="list-style-type: none"> <li>Boolka[.]tk</li> <li>boolka24.tk</li> <li>beonlineboo.com</li> <li>mainnode.beonlineboo.com</li> <li>beef.beonlineboo.com</li> <li>node.beonlineboo.com</li> <li>updatebrower.com</li> </ul>
	IP	<ul style="list-style-type: none"> <li>194.165.16[.]68</li> <li>141.98.81[.]23</li> <li>179.60.150[.]123</li> <li>141.98.9[.]152</li> <li>92.51.2[.]78</li> <li>179.60.147[.]74</li> <li>45.182.189[.]109</li> </ul>

Recommendations	<ul style="list-style-type: none"><li>• Block all threat indicators at your respective controls.</li><li>• Search for indicators of compromise (IOCs) in your environment utilizing your respective security controls.</li><li>• Never trust or open links and attachments received from unknown sources/senders.</li><li>• Regularly monitor network activity for any unusual behavior, as this may indicate that a cyberattack is underway.</li></ul> <p><b>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.</b></p>
References	<ul style="list-style-type: none"><li>• <a href="https://thehackernews.com/2024/06/new-cyberthreat-boolka-deploying.html">https://thehackernews.com/2024/06/new-cyberthreat-boolka-deploying.html</a></li><li>• <a href="https://www.group-ib.com/blog/boolka/">https://www.group-ib.com/blog/boolka/</a></li></ul>
<p>The information contained in this message is proprietary. It is for Mphasis and its customers only. Copyright © 2023. All rights reserved by Mphasis.</p>	