

# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:14:02 UTC

[Home](#) > [List all groups](#) > [List all tools](#) > List all groups using tool WebC2

## Tool: WebC2

Names	<p>WebC2</p> <p>WebC2-AdSpace</p> <p>WebC2-Ausov</p> <p>WebC2-Bolid</p> <p>WebC2-Cson</p> <p>WebC2-DIV</p> <p>WebC2-GreenCat</p> <p>WebC2-Head</p> <p>WebC2-Kt3</p> <p>WebC2-Qbp</p> <p>WebC2-Rave</p> <p>WebC2-Table</p> <p>WebC2-UGX</p> <p>WebC2-Yahoo</p>
Category	<a href="#">Malware</a>
Type	<a href="#">Backdoor</a> , <a href="#">Downloader</a>
Description	<p>A WEBC2 backdoor is designed to retrieve a Web page from a pre-determined C2 server. It expects the Web page to contain special HTML tags; the backdoor will attempt to interpret the data between the tags as commands. This family of malware is capable of downloading and executing a file. All variants represented here are the same file with different MD5 signatures. This malware attempts to contact its C2 once a week (Thursday at 10:00 AM). It looks for commands inside a set of HTML tags, part of which are in the File Strings indicator term below.</p>
Information	< <a href="http://contagiodump.blogspot.com/2013/03/mandiant-apt1-samples-categorized-by.html">http://contagiodump.blogspot.com/2013/03/mandiant-apt1-samples-categorized-by.html</a> >
MITRE ATT&CK	< <a href="https://attack.mitre.org/software/S0109/">https://attack.mitre.org/software/S0109/</a> >
Malpedia	<p>&lt;<a href="https://malpedia.caad.fkie.fraunhofer.de/details/win.webc2_adspace">https://malpedia.caad.fkie.fraunhofer.de/details/win.webc2_adspace</a>&gt;</p> <p>&lt;<a href="https://malpedia.caad.fkie.fraunhofer.de/details/win.webc2_ausov">https://malpedia.caad.fkie.fraunhofer.de/details/win.webc2_ausov</a>&gt;</p> <p>&lt;<a href="https://malpedia.caad.fkie.fraunhofer.de/details/win.webc2_bolid">https://malpedia.caad.fkie.fraunhofer.de/details/win.webc2_bolid</a>&gt;</p>

<[https://malpedia.caad.fkie.fraunhofer.de/details/win.webc2\\_cson](https://malpedia.caad.fkie.fraunhofer.de/details/win.webc2_cson)>  
<[https://malpedia.caad.fkie.fraunhofer.de/details/win.webc2\\_div](https://malpedia.caad.fkie.fraunhofer.de/details/win.webc2_div)>  
<[https://malpedia.caad.fkie.fraunhofer.de/details/win.webc2\\_greencat](https://malpedia.caad.fkie.fraunhofer.de/details/win.webc2_greencat)>  
<[https://malpedia.caad.fkie.fraunhofer.de/details/win.webc2\\_head](https://malpedia.caad.fkie.fraunhofer.de/details/win.webc2_head)>  
<[https://malpedia.caad.fkie.fraunhofer.de/details/win.webc2\\_kt3](https://malpedia.caad.fkie.fraunhofer.de/details/win.webc2_kt3)>  
<[https://malpedia.caad.fkie.fraunhofer.de/details/win.webc2\\_qbp](https://malpedia.caad.fkie.fraunhofer.de/details/win.webc2_qbp)>  
<[https://malpedia.caad.fkie.fraunhofer.de/details/win.webc2\\_rave](https://malpedia.caad.fkie.fraunhofer.de/details/win.webc2_rave)>  
<[https://malpedia.caad.fkie.fraunhofer.de/details/win.webc2\\_table](https://malpedia.caad.fkie.fraunhofer.de/details/win.webc2_table)>  
<[https://malpedia.caad.fkie.fraunhofer.de/details/win.webc2\\_ugx](https://malpedia.caad.fkie.fraunhofer.de/details/win.webc2_ugx)>  
<[https://malpedia.caad.fkie.fraunhofer.de/details/win.webc2\\_yahoo](https://malpedia.caad.fkie.fraunhofer.de/details/win.webc2_yahoo)>

Last change to this tool card: 23 April 2020

Download this tool card in [JSON](#) format

### All groups using tool WebC2

Changed	Name	Country	Observed	
<b>APT groups</b>				
	<a href="#">Comment Crew, APT 1</a>		2006-May 2018	

1 group listed (1 APT, 0 other, 0 unknown)

---

Source: <https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=a1e54b72-3eed-49ae-852c-9621bdde6be3>