Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 23:10:30 UTC

Tool: BS2005

Names	BS2005
Category	Malware
Type	Backdoor, Info stealer, Exfiltration
Description	(FireEye) Over the years, the Ke3chang attackers have used three types of malware that we call: “BS2005”, “BMW”, and “MyWeb”. We believe these three types of malware are an evolution of a single project from a single developer or small team of developers sharing code. Functionally, it is a typical first stage backdoor commonly found in APT attacks. It has the ability to upload and download files, run shell commands, and sleep for a configurable length of time. All of the CnC communications are performed over the HTTP protocol.
Information	<https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/wp-operation-ke3chang.pdf> <https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2018/march/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0014/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.bs2005>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:bs2005>

Last change to this tool card: 13 May 2020

Download this tool card in JSON format

All groups using tool BS2005

Changed	Name	Country	Observed
APT groups			

	Ke3chang, Vixen Panda, APT 15, GREF, Playful Dragon		2010-Oct 2024	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=34bcb564-8614-460b-9937-3a01f8d95637