Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:33:58 UTC

Tool: Buhtrap

Names	Buhtrap Ratopak
Category	Malware
Type	Banking trojan, Backdoor, Keylogger, Credential stealer, Info stealer, Downloader, Exfiltration
Description	(ESET) The infection vector we have seen consists of Microsoft Word documents sent as email attachments that exploit CVE-2012-0158, a vulnerability in Microsoft Word that was patched three years ago. The images below show two of the decoy documents used in this campaign. The first document, titled “Счет № 522375-ФЛОРЛ-14-115.doc” mimics an invoice. The second, aptly titled “kontrakt87.doc”, copies a generic telecommunications service contract from MegaFon, a large Russian mobile phone operator. The tools deployed on the victim’s computer allow them to control it remotely and to record the user’s actions. The malware allows the criminals to install a backdoor, attempt to obtain the account password, and even create a new account. They also install a keylogger, a clipboard stealer, a smart card module, and have the capability to download and execute additional malware.
Information	<https://www.welivesecurity.com/2015/04/09/operation-buhtrap/> <https://malware-research.org/carbanak-source-code-leaked/> <https://www.group-ib.com/brochures/gib-buhtrap-report.pdf> <https://www.arbornetworks.com/blog/asert/diving-buhtrap-banking-trojan-activity/> <https://blog.dcso.de/pegasus-buhtrap-analysis-of-the-malware-stage-based-on-the-leaked-source-code/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.buhtrap>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:buhtrap>

Last change to this tool card: 13 May 2020

Download this tool card in JSON format

All groups using tool Buhtrap

Changed	Name	Country	Observed	
APT groups				
	Buhtrap, Ratopak Spider		2015-Jun 2019	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=7790d629-5724-4da6-8201-e2b031e8c487