Buhtrap, Ratopak Spider - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:10:00 UTC

APT group: Buhtrap, Ratopak Spider

Names	Buhtrap *(Group-IB)* Ratopak Spider *(CrowdStrike)* UAC-0008 *(CERT-UA)*
Country	Russia
Motivation	Financial crime
First seen	2015
Description	(Group-IB) Buhtrap has been active since 2014, however their first attacks against financial institutions were only detected in August 2015. Earlier, the group had only focused on targeting banking clients. At the moment, the group is known to target Russian and Ukrainian banks. From August 2015 to February 2016 Buhtrap managed to conduct 13 successful attacks against Russian banks for a total amount of 1.8 billion rubles ($25.7 mln). The number of successful attacks against Ukrainian banks has not been identified. Buhtrap is the first hacker group using a network worm to infect the overall bank infrastructure that significantly increases the difficulty of removing all malicious functions from the network. As a result, banks have to shut down the whole infrastructure which provokes delay in servicing customers and additional losses. Malicious programs intentionally scan for machines with an automated Bank-Customer system of the Central Bank of Russia (further referred to as BCS CBR). We have not identified incidents of attacks involving online money transfer systems, ATM machines or payment gates which are known to be of interest for other criminal groups. Buhtrap has some infrastructure overlap with TA505, Graceful Spider, Gold Evergreen.

Observed	Sectors: Financial, Government. Countries: Russia, Ukraine.	
Tools used	Buhtrap, FlawedAmmyy, Niteris EK, NSIS.	
Operations performed	2014	On October 20, 2014 we notified Group-IB Bot-Trek Intelligence subscribers about phishing emails which were sent from the info@beeline-mail.ru address with the subject “Invoice No 522375-ФЛОРЛ-14-115” (pic. 1). The beeline-mail.ru domain name was also registered on October 20, 2014. <https://www.group-ib.com/brochures/gib-buhtrap-report.pdf>
	Oct 2015	We noticed in late October that users visiting the Ammyy website to download the free version of its remote administrator software were being served a bundle containing not only the legitimate Remote Desktop Software Ammyy Admin, but also an NSIS (Nullsoft Scriptable Installation Software) installer ultimately intended to install the tools used by the Buhtrap gang to spy on and control their victims’ computers. <https://www.welivesecurity.com/2015/11/11/operation-buhtrap-malware-distributed-via-ammyy-com/>
	Dec 2015	In December 2015, employees from several Russian banks were targeted with spoofed emails, a common technique in attack campaigns. The emails were made to look like they were from the Central Bank of Russia and offered employment to their recipients. Instead of being an actual employment offer, the emails were an attempt to deliver Trojan.Ratopak onto the target’s computer. <https://www.symantec.com/connect/blogs/russian-bank-employees-received-fake-job-offers-targeted-email-attack>
	Sep 2016	Breach of the Russian boxing site allboxing[.].ru <https://www.forcepoint.com/blog/security-labs/highly-evasive-code-injection-awaits-user-interaction-delivering-malware>
	2017	Operation “TwoBee” Buhtrap resurfaced in the beginning of 2017 in the TwoBee campaign, where it served primarily as means of malware delivery. In March of last year, it hit the news (literally), spreading through several compromised major news outlets in whose main pages malicious actors implanted scripts. This scripts executed an exploit for Internet Explorer in visitor’s browsers. <https://www.kaspersky.com/blog/financial-trojans-2019/25690/>

	Jun 2019	Throughout our tracking, we've seen this group deploy its main backdoor as well as other tools against various victims, but June 2019 was the first time we saw the Buhtrap group use a zero-day exploit as part of a campaign. In that case, we observed Buhtrap using a local privilege escalation exploit, CVE-2019-1132, against one of its victims. <https://www.welivesecurity.com/2019/07/11/buhtrap-zero-day-espionage-campaigns/>
Information	<https://www.group-ib.com/brochures/gib-buhtrap-report.pdf> <https://www.welivesecurity.com/2015/04/09/operation-buhtrap/>	

Last change to this card: 08 April 2022

Download this actor card in PDF or JSON format
