Subgroup: BeagleBoyz - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:10:26 UTC

APT group: Subgroup: BeagleBoyz

Names	BeagleBoyz *(US Government)*
Country	North Korea
Motivation	Financial crime
First seen	2014
Description	(US CERT) The BeagleBoyz, an element of the North Korean government's Reconnaissance General Bureau, have likely been active since at least 2014. As opposed to typical cybercrime, the group likely conducts well-planned, disciplined, and methodical cyber operations more akin to careful espionage activities. Their malicious cyber operations have netted hundreds of millions of U.S. dollars and are likely a major source of funding for the North Korean regime. The group has always used a calculated approach, which allows them to sharpen their tactics, techniques, and procedures while evading detection. Over time, their operations have become increasingly complex and destructive. The tools and implants employed by this group are consistently complex and demonstrate a strong focus on effectiveness and operational security. North Korea's intelligence apparatus controls a hacking team dedicated to robbing banks through remote internet access. To differentiate methods from other North Korean malicious cyber activity, the U.S. Government refers to this team as BeagleBoyz, who represent a subset of HIDDEN COBRA activity. The BeagleBoyz overlap to varying degrees with groups tracked by the cybersecurity industry as Lazarus Group, Hidden Cobra, Labyrinth Chollima and Subgroup: Bluenoroff, APT 38, Stardust Chollima and are responsible for the FASTCash ATM cash outs reported in October 2018, fraudulent abuse of compromised bank-operated SWIFT system endpoints since at least 2015, and lucrative cryptocurrency thefts. This illicit behavior has been identified by the United Nations (UN) DPRK Panel of Experts as evasion of UN Security Council resolutions, as it generates substantial revenue for North Korea. North Korea can use these funds for its UN-prohibited nuclear weapons and ballistic missile programs. Additionally, this activity poses significant

	operational risk to the Financial Services sector and erodes the integrity of the financial system.	
Observed	Sectors: Financial. Countries: Argentina, Brazil, Bangladesh, Bosnia and Herzegovina, Bulgaria, Chile, Costa Rica, Ecuador, Ghana, India, Indonesia, Japan, Jordan, Kenya, Kuwait, Malaysia, Malta, Mexico, Mozambique, Nepal, Nicaragua, Nigeria, Pakistan, Panama, Peru, Philippines, Singapore, South Africa, South Korea, Spain, Taiwan, Tanzania, Togo, Turkey, Uganda, Uruguay, Vietnam, Zambia.	
Tools used	FASTCash, NachoCheese, PSLogger.	
Operations performed	2016/2018	Operation “FASTCash” On October 2, 2018, an alert was issued by US-CERT, the Department of Homeland Security, the Department of the Treasury, and the FBI. According to this new alert, Hidden Cobra (the U.S. government’s code name for Lazarus) has been conducting “FASTCash” attacks, stealing money from Automated Teller Machines (ATMs) from banks in Asia and Africa since at least 2016. <https://www.symantec.com/blogs/threat-intelligence/fastcash-lazarus-atm-malware>
	Feb 2016	Bangladeshi Bank Attack <https://blog.trendmicro.com/trendlabs-security-intelligence/what-we-can-learn-from-the-bangladesh-central-bank-cyber-heist/>
Information	<https://us-cert.cisa.gov/ncas/alerts/aa20-239a>	

Last change to this card: 29 December 2022

Download this actor card in PDF or JSON format
