Shadow Brokers - Threat Group Cards: A Threat Actor Encyclopedia

Other threat group: Shadow Brokers

Names	Shadow Brokers *(self given)*	
Country	USA	
Motivation	Financial gain	
First seen	2016	
Description	Breached a server where zero-days accumulated by Equation Group were held, leaked a large section on the internet and tried to sell the rest afterward. Most of the published vulnerabilities have since been fixed by the respective vendors, but many have been used by other threat actors. Most notably among the dumps were zero-days such as ETERNALBLUE that were used for the creation of infamous ransomware explosions such as WannaCry and NotPetya. Shadow Brokers turned out to be an ex-NSA contractor.	
Observed		
Tools used		
Operations performed	Aug 2016	Initial public dump <https://musalbas.com/blog/2016/08/16/equation-group-firewall-operations-catalogue.html>
	Oct 2016	'Shadow Brokers' Whine That Nobody Is Buying Their Hacked NSA Files <https://www.vice.com/en_us/article/53djj3/shadow-brokers-whine-that-nobody-is-buying-their-hacked-nsa-files>
	Oct 2016	Second Shadow Brokers dump released <https://www.scmagazineuk.com/second-shadow-brokers-dump-released/article/1476023>

	Mar 2017	In March 2017, the ShadowBrokers published a chunk of stolen data that included two frameworks: DanderSpritz and FuzzBunch. <https://securelist.com/darkpulsar/88199/>
	Apr 2017	Shadow Brokers leaks show U.S. spies successfully hacked Russian, Iranian targets <https://www.cyberscoop.com/nsa-shadow-brokers-leaks-iran-russia-optimusprime-stoicsurgeon/>
	Apr 2017	New NSA leak may expose its bank spying, Windows exploits <https://www.csoonline.com/article/3190055/new-nsa-leak-may-expose-its-bank-spying-windows-exploits.html>
	Apr 2017	ShadowBrokers Dump More Equation Group Hacks, Auction File Password <https://threatpost.com/shadowbrokers-dump-more-equation-group-hacks-auction-file-password/124882/>
	Sep 2017	ShadowBrokers are back demanding nearly $4m and offering 2 dumps per month <http://securityaffairs.co/wordpress/62770/hacking/shadowbrokers-return.html>
	Sep 2017	ShadowBrokers Release UNITEDRAKE Malware <https://www.hackread.com/nsa-data-dump-shadowbrokers-expose-unitedrake-malware/>
Counter operations	Nov 2017	Who Was the NSA Contractor Arrested for Leaking the ‘Shadow Brokers’ Hacking Tools? <https://blacklakesecurity.com/who-was-the-nsa-contractor-arrested-for-leaking-the-shadow-brokers-hacking-tools/>
Information	<https://www.dropbox.com/s/buxkfotx1kei0ce/Whitepaper%20Shadow%20Broker%20-%20Equation%20Group%20Hack.pdf?dl=0>	

Last change to this card: 21 May 2020

Download this actor card in PDF or JSON format
