Operation Domino, Operation Kremlin - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:13:21 UTC

APT group: Operation Domino, Operation Kremlin

Names	Operation Domino *(Hunting Shadow Lab)* Operation Kremlin *(ClearSky)*	
Country	Russia	
Motivation	Information theft and espionage	
First seen	2019	
Description	(Clearsky) ClearSky researchers identified a malicious ".docx" file that was uploaded to VirusTotal from Russia in mid-December. The file contains an obfuscated URL to a remote template which contains malicious VBA, eventually leading to the execution of VBS on the infected machine. The attack's purpose is to stealthily exfiltrate information without running any external executables on the system. Notably, the process is escalated on a certain day of the week, suggesting a possible familiarity with the intended victim or victims. We estimate with medium confidence that the same threat actor responsible for the attacks described in this paper also conducted an attack named "Operation Domino" that occurred earlier in 2020. We decided to name the operation "Kremlin" due to the use of a parameter named "kreml" in the "poslai" (meaning send in Russian) function that exfiltrates the data.	
Observed	Countries: Belarus.	
Tools used		
Operations performed	Sep 2020	Operation "Domino" <https://ti.dbappsecurity.com.cn/blog/index.php/2020/09/18/operation-domino/>

	Dec 2020	Operation “Kremlin” <https://www.clearskysec.com/operation-kremlin/>
Information	<https://www.clearskysec.com/operation-kremlin/>	

Last change to this card: 29 December 2024

Download this actor card in PDF or JSON format
