Operation Poison Needles - Threat Group Cards: A Threat Actor Encyclopedia

APT group: Operation Poison Needles

Names	Operation Poison Needles *(Qihoo 360)*
Country	Ukraine
Motivation	Information theft and espionage
First seen	2018
Description	(Qihoo 360) On the evening of November 29, 2018, shortly after the break-out of the Kerch Strait Incident, 360 Advanced Threat Response Team was the first security team to discover the APT attack against the FSBI “Polyclinic No.2” affiliated to the Presidential Administration of Russia. The lure document used to initiate the attack was a carefully forged employee questionnaire, which exploited the latest Flash 0day vulnerability CVE-2018-15982 and a customized Trojan with self-destruction function. All the technical details indicate that the APT group is determined to compromise the target at any price, but at the same time, it is also very cautious.
Observed	Sectors: Healthcare. Countries: Russia.
Tools used	0-day Flash exploit.
Information	<http://blogs.360.cn/post/PoisonNeedles_CVE-2018-15982_EN>

Last change to this card: 14 April 2020

Download this actor card in PDF or JSON format