Operation BugDrop - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:50:22 UTC

APT group: Operation BugDrop

Names	Operation BugDrop *(CyberX)*
Country	Russia
Motivation	Information theft and espionage
First seen	2016
Description	(CyberX) CyberX has discovered a new, large-scale cyber-reconnaissance operation targeting a broad range of targets in the Ukraine. Because it eavesdrops on sensitive conversations by remotely controlling PC microphones – in order to surreptitiously “bug” its targets – and uses Dropbox to store exfiltrated data, CyberX has named it “Operation BugDrop.” CyberX has confirmed at least 70 victims successfully targeted by the operation in a range of sectors including critical infrastructure, media, and scientific research. The operation seeks to capture a range of sensitive information from its targets including audio recordings of conversations, screen shots, documents and passwords. Unlike video recordings, which are often blocked by users simply placing tape over the camera lens, it is virtually impossible to block your computer’s microphone without physically accessing and disabling the PC hardware.
Observed	Sectors: Engineering, Oil and gas, Media, Research. Countries: Austria, Saudi Arabia, Russia, Ukraine.
Tools used	Dropbox.
Information	<https://cyberx-labs.com/blog/operation-bugdrop-cyberx-discovers-large-scale-cyber-reconnaissance-operation/>

Last change to this card: 14 April 2020

Download this actor card in PDF or JSON format