The Big Bang - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:36:44 UTC

APT group: The Big Bang

Names	The Big Bang *(Check Point)*
Country	[Unknown]
Motivation	Information theft and espionage
First seen	2017
Description	(Talos) Talos continuously monitors malicious emails campaigns. We identified one specific spear phishing campaign launched against targets within Palestine, and specifically against Palestinian law enforcement agencies. This campaign started in April 2017, using a spear phishing campaign to deliver the MICROPSIA payload in order to remotely control infected systems. Although this technique is not new, it remains an effective technique for attackers. The malware itself was developed in Delphi; in this article, we describe the features and the network communication to the command and control server used by the attackers. The threat actor has chosen to reference TV show characters and include German language words within the attack. Most significantly, the attacker has appeared to have used genuine documents stolen from Palestinian sources as well as a controversial music video as part of the attack. (Check Point) While the APT has gone through significant upgrades over the past year, the conductors of these campaigns maintained evident fingerprints, both in the delivery methods and malware development conventions. These unique traces assisted us in correlating the current wave to past attacks, and may also have some resemblance to attacks related to the Molerats, Extreme Jackal, Gaza Cybergang APT group.
Observed	Sectors: Law enforcement and others. Countries: Palestine and Middle East.
Tools used	Micropsia.
Information	<https://blog.talosintelligence.com/2017/06/palestine-delphi.html> <https://research.checkpoint.com/2018/apt-attack-middle-east-big-bang/>

Last change to this card: 15 April 2020

Download this actor card in PDF or JSON format
