Threat Group Cards: A Threat Actor Encyclopedia

Tool: Inception

Names	Inception
Category	Malware
Type	Backdoor
Description	(Symantec) Word documents attached to Inception's spear-phishing emails leveraged two Microsoft Office vulnerabilities (CVE-2014-1761 and CVE-2012-0158) to install malware on the recipient's computer. The malware had a multi-staged structure that began with a malicious RTF document and ended with an in-memory DLL payload that communicated, via the WebDAV protocol, with a command and control (C&C) address from a legitimate cloud service provider (CloudMe.com). The name "Inception" comes from the group's many levels of obfuscation and indirection it employed in delivering this payload.
Information	<https://symantec-blogs.broadcom.com/blogs/threat-intelligence/inception-framework-hiding-behind-proxies>

Last change to this tool card: 20 April 2020

Download this tool card in JSON format

All groups using tool Inception

Changed	Name	Country	Observed	
APT groups				
	Inception Framework, Cloud Atlas		2012-2024	

1 group listed (1 APT, 0 other, 0 unknown)