Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:27:53 UTC

Tool: CHAINSHOT

Names	CHAINSHOT
Category	Malware
Type	Downloader
Description	(Palo Alto) We uncovered part of a new toolkit which was used as a downloader alongside Adobe Flash exploit CVE-2018-5002 to target victims in the Middle East. This was possible because the attacker made a mistake in using insecure 512-bit RSA encryption. The malware sends user information encrypted to the attacker server and attempts to download a final stage implant. It was allegedly developed with the help of an unknown framework and makes extensive use of custom error handling. Because the attacker made another mistake in using the same SSL certificate for similar attacks, we were able to uncover additional infrastructure indicating a larger campaign.
Information	<https://unit42.paloaltonetworks.com/unit42-slicing-dicing-cve-2018-5002-payloads-new-chainshot-malware/> <https://atr-blog.gigamon.com/2018/06/07/adobe-flash-zero-day-leveraged-for-targeted-attack-in-middle-east/> <https://www.icebrg.io/blog/adobe-flash-zero-day-targeted-attack>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.chainshot>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:chainshot>

Last change to this tool card: 13 May 2020

Download this tool card in JSON format

All groups using tool CHAINSHOT

Changed	Name	Country	Observed
APT groups			

	SandCat		2018	

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