Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 23:17:32 UTC

APT group: LookBack, TA410

Names	LookBack *(Proofpoint)* TA410 *(Proofpoint)* Witchetty *(Symantec)* LookingFrog *(ESET)* FlowingFrog *(ESET)*
Country	[Unknown]
Motivation	Information theft and espionage
First seen	2019
Description	(Proofpoint) Between July 19 and July 25, 2019, several spear phishing emails were identified targeting three US companies in the utilities sector. The phishing emails appeared to impersonate a US-based engineering licensing board with emails originating from what appears to be an actor-controlled domain, nceess[.]com. Nceess[.]com is believed to be an impersonation of a domain owned by the US National Council of Examiners for Engineering and Surveying. The emails contain a malicious Microsoft Word attachment that uses macros to install and run malware that Proofpoint researchers have dubbed “LookBack.” This malware consists of a remote access Trojan (RAT) module and a proxy mechanism used for command and control (C&C) communication. We believe this may be the work of a state-sponsored APT actor based on overlaps with historical campaigns and macros utilized. The utilization of this distinct delivery methodology coupled with unique LookBack malware highlights the continuing threats posed by sophisticated adversaries to utilities systems and critical infrastructure providers. Proofpoint found similarities in malware delivery with Stone Panda, APT 10, menuPass, but those may have been false flags.
Observed	Sectors: Energy, Utilities. Countries: USA and Middle East and Africa.
Tools used	FlowCloud, GUP Proxy Tool, SodomMain, SodomNormal.

Operations performed	Jul 2019	At the same time as the LookBack campaigns, Proofpoint researchers identified a new, additional malware family named FlowCloud that was also being delivered to U.S. utilities providers. <https://www.proofpoint.com/us/blog/threat-insight/ta410-group-behind-lookback-attacks-against-us-utilities-sector-returns-new>
	Aug 2019	LookBack Forges Ahead: Continued Targeting of the United States' Utilities Sector Reveals Additional Adversary TTPs <https://www.proofpoint.com/us/threat-insight/post/lookback-forges-ahead-continued-targeting-united-states-utilities-sector-reveals>
	Feb 2022	Witchetty: Group Uses Updated Toolset in Attacks on Governments in Middle East <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/witchetty-steganography-espionage>
Information	<https://www.proofpoint.com/us/threat-insight/post/lookback-malware-targets-united-states-utilities-sector-phishing-attacks> <https://www.welivesecurity.com/2022/04/27/lookback-ta410-umbrella-cyberespionage-ttps-activity/>	

Last change to this card: 29 November 2023

Download this actor card in PDF or JSON format
