Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-02 12:38:21 UTC

APT group: Nazar

Names	Nazar *(Epic Turla)* SIG37 *(NSA)*
Country	Iran
Motivation	Information theft and espionage
First seen	2008
Description	(Epic Turla) It's hard to understand the scope of this operation without access to victimology (e.g.: endpoint visibility or command-and-control sinkholing). Additionally, some possible timestomping muddies the water between this operation possible originating in 2008-2009 or actually coming into full force in 2010-2013 (the latter dates being corroborated by VT firstseen submission times and second-stage drop timestamps). There's a level of variable developmental capability visible throughout the stages. Multiple components are abused commonly-available resources, while the orchestrator and two of the DLL drops actually display some developmental ingenuity (in the form of seemingly novel COM techniques). Far from the most advanced coding practices but definitely better than the sort of .NET garbage other 'Farsi-speaking' APTs have gotten away with in the past. Somehow, this operation found its way onto the NSA's radar pre-2013. As far as I can tell, it's eluded specific coverage from the security industry. A possible scenario to account for the disparate visibility between the NSA and Western researchers when it comes to this cluster of activity is that these samples were exclusively encountered on Iranian boxes overlapping with EQGRP implants. Submissions of Nazar subcomponents from Iran (as well as privately shared visibility into historical and ongoing victimology clustered entirely on Iranian machines) could support that theory. Perhaps this is an internal monitoring framework (a la Attor) but given the sparse availability of historical data, I wouldn't push that beyond a low-confidence assessment, at this time.
Observed	
Tools used	Distribute.exe, EYService, GpUpdates.exe, Microolap Packet Sniffer.
Information	<https://www.epicturla.com/blog/the-lost-nazar> <https://research.checkpoint.com/2020/nazar-spirits-of-the-past/>

Last change to this card: 13 March 2024

Download this actor card in PDF or JSON format
