Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 03:23:13 UTC

Tool: Tarsip

Names	Tarsip
Category	Malware
Type	Backdoor, Exfiltration
Description	The TARSIP malware family is a backdoor which communicates over encoded information in HTTPS headers. Typical TARSIP malware samples will only beacon out to their C2 servers if the C2 DNS address resolves to a specific address. The capability of TARSIP backdoors includes file uploading, file downloading, interactive command shells, process enumeration, process creation, process termination. The TARSIP-ECLIPSE family is distinguished by the presence of 'eclipse' in .pdb debug strings present in the malware samples. It does not provide a built in mechanism to maintain persistence. The TARSIP-MOON family is distinguished by the presence of 'moon' in .pdb debug strings present in the malware samples. It does not provide a built in mechanism to maintain persistence.
Information	<http://contagiodump.blogspot.com/2013/03/mandiant-apt1-samples-categorized-by.html>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.tarsip>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool Tarsip

Changed	Name	Country	Observed	
APT groups				
	Comment Crew, APT 1		2006-May 2018	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=97384be1-282a-41cb-8c15-2fbe9a882b3c