Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:52:40 UTC

Tool: WARP

Names	WARP
Category	Malware
Type	Reconnaissance, Backdoor
Description	The WARP malware family is an HTTP based backdoor written in C++, and the majority of its code base is borrowed from source code available in the public domain. Network communications are implemented using the same WWW client library (w3c.cpp) available from www.dankrusi.com/file_69653F3336383837.html. The malware has system survey functionality (collects hostname, current user, system uptime, CPU speed, etc.) taken directly from the BO2K backdoor available from www.bo2k.com. It also contains the hard disk identification code found at www.winsim.com/diskid32/diskid32.cpp. When the WARP executing remote commands, the malware creates a copy of the ? %SYSTEMROOT%\system32\cmd.exe? file as '%USERPROFILE%\Temp\~ISUN32.EXE'. The version signature information of the duplicate executable is zeroed out. Some WARP variants maintain persistence through the use of DLL search order hijacking.
Information	<http://contagiodump.blogspot.com/2013/03/mandiant-apt1-samples-categorized-by.html>

Last change to this tool card: 20 April 2020

Download this tool card in JSON format

All groups using tool WARP

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

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