Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 23:13:23 UTC

Tool: XSLCmd

Names	XSLCmd
Category	Malware
Type	Backdoor, Keylogger, Info stealer
Description	(FireEye) The backdoor code was ported to OS X from a Windows backdoor that has been used extensively in targeted attacks over the past several years, having been updated many times in the process. Its capabilities include a reverse shell, file listings and transfers, installation of additional executables, and an updatable configuration. The OS X version of XSLCmd includes two additional features not found in the Windows variants we have studied in depth: key logging and screen capturing.
Information	<https://www.fireeye.com/blog/threat-research/2014/09/forced-to-adapt-xslcmd-backdoor-now-on-os-x.html> <https://objective-see.com/blog/blog_0x16.html>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/osx.xslcmd>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:xslcmd>

Last change to this tool card: 02 July 2020

Download this tool card in JSON format

All groups using tool XSLCmd

Changed	Name	Country	Observed	
APT groups				
	Ke3chang, Vixen Panda, APT 15, GREF, Playful Dragon		2010-Oct 2024	

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