Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:20:20 UTC

Tool: Gh0stnet

Names	Gh0stnet Ghostnet Remosh
Category	Malware
Type	Backdoor, Info stealer, Exfiltration
Description	(UCAM) Our next observation concerns the malware payloads used. These were packaged as either .doc or .pdf files that installed rootkits on the machines of monks who clicked on them. During our initial network monitoring exercise, we observed sensitive files being transferred out of the Office of His Holiness the Dalai Lama (OHHDL) using a modified HTTP protocol: the malware picked up files from local disks and sent them to three servers which, according to APNIC, were in China's Sichuan province, using a custom protocol based on HTTP. The malware uses HTTP GET and HTTP POST messages to transfer files out and also appears to verify successful transmission. Sichuan, by the way, is the location of the Chinese intelligence unit specifically tasked with monitoring the OHHDL.
Information	<https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-746.pdf> <https://securitynews.sonicwall.com/xmlpost/gh0stnet-now-spreads-as-a-fileless-malware-nov-022017/> <https://www.nartv.org/2019/03/28/10-years-since-ghostnet/> <http://contagiodump.blogspot.com/2011/07/jul-25-mac-olyx-gh0st-backdoor-in-rar.html>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.ghostnet>

Last change to this tool card: 13 May 2020

Download this tool card in JSON format

All groups using tool Gh0stnet

Changed	Name	Country	Observed

APT groups

	GhostNet, Snooping Dragon		2009-2010	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=1ab15fc8-f2d0-4796-b342-2eb5f4527f86