

# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 02:08:51 UTC

[Home](#) > [List all groups](#) > [List all tools](#) > List all groups using tool HOPLIGHT

## Tool: HOPLIGHT

Names	HOPLIGHT HANGMAN
Category	<a href="#">Malware</a>
Type	<a href="#">Tunneling</a>
Description	<a href="#">(US-CERT)</a> This report provides analysis of twenty malicious executable files. Sixteen of these files are proxy applications that mask traffic between the malware and the remote operators. The proxies have the ability to generate fake TLS handshake sessions using valid public SSL certificates, disguising network connections with remote malicious actors. One file contains a public SSL certificate and the payload of the file appears to be encoded with a password or key. The remaining file does not contain any of the public SSL certificates, but attempts outbound connections and drops four files. The dropped files primarily contain IP addresses and SSL certificates.
Information	< <a href="https://www.us-cert.gov/ncas/analysis-reports/ar20-045g">https://www.us-cert.gov/ncas/analysis-reports/ar20-045g</a> > < <a href="https://www.computing.co.uk/ctg/news/3074007/lazarus-rises-warning-over-new-hoplight-malware-linked-with-north-korea">https://www.computing.co.uk/ctg/news/3074007/lazarus-rises-warning-over-new-hoplight-malware-linked-with-north-korea</a> >
MITRE ATT&CK	< <a href="https://attack.mitre.org/software/S0376/">https://attack.mitre.org/software/S0376/</a> >
Malpedia	< <a href="https://malpedia.caad.fkie.fraunhofer.de/details/win.hopligh">https://malpedia.caad.fkie.fraunhofer.de/details/win.hopligh</a> >
AlienVault OTX	< <a href="https://otx.alienvault.com/browse/pulses?q=tag:HOPLIGHT">https://otx.alienvault.com/browse/pulses?q=tag:HOPLIGHT</a> >

Last change to this tool card: 13 May 2020

Download this tool card in [JSON](#) format

### All groups using tool HOPLIGHT

Changed	Name	Country	Observed
<b>APT groups</b>			

	<a href="#">Lazarus Group, Hidden Cobra, Labyrinth Chollima</a>		2007-May 2025	
--	---	--	---------------	---

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

---

Source: <https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=a2a00578-4e93-4833-acbc-25ace6e45504>