Lazarus Group rises again from the digital grave with Hoplight malware for all

By Shaun Nichols

Published: 2019-04-10 · Archived: 2026-04-05 18:59:14 UTC

The Lazarus Group hacking operation, thought to be controlled by the North Korean government, has a new malware toy to pitch at potential targets and the US is getting worried about it.

This according to a report from US-Cert, which say that the group (also known as "Hidden Cobra") has a new piece of spyware capable of securely connecting to a control server and uploading pilfered files from infected machine.

Known as "Hoplight," the malware is a collection of nine files, though most of those are designed to work as obfuscation layers to keep admins and security software from spotting the attack.

"Seven of these files are proxy applications that mask traffic between the malware and the remote operators," US-Cert said in its write-up of the new Nork nasty.

"The proxies have the ability to generate fake TLS handshake sessions using valid public SSL certificates, disguising network connections with remote malicious actors."

Below those seven proxy layers, Hoplight uses its valid SSL certificate to create the secure connection, then a final, ninth file looks to create an outbound connection to the control server in order to transmit pilfered information. The certificate looks to be a public SSL cert from Naver, a Korean search engine and service provider.

Within the bundle of files, US-Cert says, the malware package is able to perform a number of remote control and spyware activities. This includes the ability to read and write local files, create, terminate, or modify running processes and registry settings, and connect to a remote host to upload and download files.

The Lazarus Group is something of an oddity in the world of government-backed hacking groups. Unlike other state-sponsored operations, the primary focus of the group has not been espionage or intellectual property theft, but rather financial crime aimed at helping the isolated nation get cash into its coffers.

Lazarus/Hidden Cobra was also famously credited with pulling off the high-profile 2014 attack on Sony Pictures.

The group has typically used spear-phishing techniques to get its malware onto foreign foreign targets, and US-Cert recommends admins and users take basic security measures (such as patching systems regularly and maintaining up-to-date malware protections) in order to safeguard from attacks. ®