The Advanced Persistent Threat files: Lazarus Group | Malwarebytes Labs

By William Tsing

Published: 2019-03-11 · Archived: 2026-04-02 12:21:47 UTC

We've heard a lot about Advanced Persistent Threats (APTs) over the past few years. As a refresher, APTs are prolonged, aimed attacks on specific targets with the intention to compromise their systems and gain information from or about that target.

While the targets may be anyone or anything—a person, business, or other organization—APTs are often associated with government or military operations, as they tend to be the organizations with the resources necessary to conduct such an attack. Starting with Mandiant's APT1 report in 2013, there's been a continuous stream of exposure of nation-state hacking at scale.

Cybersecurity companies have gotten relatively good at observing and analyzing the tools and tactics of nation-state threat actors; they're less good at placing these actions in context sufficient enough for defenders to make solid risk assessments. So we're going to take a look at a few APT groups from a broader perspective and see how they fit into the larger threat landscape.

Today, we're going to review the activities of Lazarus group, alternatively named Hidden Cobra and Guardians of Peace.

Who is Lazarus Group?

Lazarus Group is commonly believed to be run by the North Korean government, motivated primarily by financial gain as a method of circumventing long-standing sanctions against the regime. They first came to substantial media notice in 2013 with a series of coordinated attacks against an assortment of South Korean broadcasters and financial institutions using DarkSeoul, a wiper program that overwrites sections of the victims' Master Boot Record.

In November 2014, a large scale breach of Sony Pictures was attributed to Lazarus. The attack was notable due to its substantial penetration across Sony networks, the extensive amount of data exfiltrated and leaked, as well of use of a wiper in a possible attempt to erase forensic evidence. Attribution on the attacks was largely hazy, but the FBI released a statement tying the Sony breach to the earlier DarkSeoul attack, and officially attributed both incidents to North Korea.

Fast forward to May 2017 with the widespread outbreak of WannaCry, a piece of ransomware that used an SMB exploit as an attack vector. Attribution to North Korea rested largely on code reuse between WannaCry and previous North Korean attacks, but this was considered to be thin grounds given the common practice of tool sharing between regional threat groups. Western intelligence agencies released official statements to the public

reaffirming the attribution, and on September 6, 2018, the US Department of Justice charged a North Korean national with involvement in both WannaCry and the Sony breach.

More recently, the financially-motivated arm of Lazarus Group has been garnering attention for attacks against financial institutions, as well as cryptocurrency exchanges. The latter is notable for involving Trojanized trading apps for both Windows and MacOS.

Malware commonly deployed

- DarkSeoul
- Fallchill
- Trojan.Fastcash
- Bitsran
- Assorted backdoors for persistence

Should you be worried?

Yes, but not to the degree you might think. Lazarus Group activities center on financial gain, as well as achieving the political goals of the North Korean regime. Given that North Korea's stated political objectives tend to hyper focus on regional conflicts with South Korea and Japan, businesses outside of that sphere probably are at a low risk of politically-motivated attacks.

Financial motivations, however, do pose a significant risk to almost all organizations. Fortunately, defense against these types of attacks is largely the same whether they are state sponsored or not. Defenders should have robust log-monitoring capability, a patch management program, anti-phishing protection, and flags to distinguish legitimate communications from leadership from imposters.

What might they do next?

Attribution for Lazarus attacks is softer than with many other threat groups, and divining political motivations for North Korea has proven difficult for decades. As a result, it's tough to project what their next targets might be. It's a reasonable assumption, however, that while sanctions remain on North Korean leadership, the financial motivations of Lazarus will also remain. Organizations at particular risk of financially-motivated attacks should include Lazarus while considering security mitigations.

Additional resources

Comprehensive review of TTPs by Kaspersky

Extensive review of the Sony attack

April 10th US-CERT report on North Korean trojan HOPLIGHT

About the author

Breaking things and wrecking up the place since 2005.
