Operation Blockbuster Coalition Ties Destructive Attacks to Lazarus Group

By Michael Mimoso

Published: 2016-02-24 · Archived: 2026-04-05 14:16:03 UTC

A group of security companies today published evidence linking the Sony hack, Dark Seoul and Operation Troy to the Lazarus Group.

The nation-state sponsored hacker group allegedly behind the 2014 attack against Sony Pictures Entertainment has been linked to similar intrusions against a number of companies in South Korea including the Dark Seoul and Operation Troy attacks.

A coalition of security companies called Operation Blockbuster, including Kaspersky Lab, Novetta, AlienVault, Invincea, ThreatConnect, Volexity, Symantec, and PunchCyber today published reports chronicling the activities of the Lazarus Group and also simultaneously a week ago published detection signatures to their respective software in the hopes of disrupting the APT group's activities.

The Lazarus Group's array of malware, including destructive wiper malware known as Destover, shares common characteristics among tens of attacks, Kaspersky Lab said, including Sony Pictures Entertainment. Two years ago, the Hollywood giant suffered an embarrassing, damaging attack that spilled not only confidential emails onto the Internet, but also intellectual property such as scripts, film ideas and new movies.

The group, said Kaspersky Lab researcher Brian Bartholomew, was active going back to at least 2010 and remains active.

"We hope this throws a wrench into their operations, causes them to retool and slows them down," Bartholomew said. "This will have an impact, but we don't think this will make them go away."

A similar 2014 initiative between security companies called Operation SMN led by Novetta published extensive details on the activities of the Axiom APT gang of China.

"What we learned from the last operation is that the group we targeted was back at it a handful of months later, retooled and ready to go. We were able to slow them down," Bartholomew said. "But the bigger thing as far as putting a dent in their operations is that we were exposing something that a lot of people know is going on, but nothing was officially outed until then. That's a bigger thing."

The Lazarus Group is a sizeable operation that has been connected to North Korea, according to the U.S. government in the wake of the Sony hack. The FBI officially blamed North Korea for the attacks on Sony in mid-December 2014, it said, after an analysis of the malware used in the attacks and hard-coded IP addresses in those samples. The FBI also noted similarities between the Sony hack and attacks in 2013 against South Korean media companies and a number of critical industries.

In January 2015, the U.S. levied sanctions against North Korea defense agencies, two other government agencies and 10 individuals. The Executive Order explaining the sanctions came two weeks after North Korea suffered a DDoS attack that disconnected much of the country from the Internet.

In a report published today, Kaspersky Lab researchers said that the Lazarus Group's malware is mostly custom-built, though not overly sophisticated. The use of Destover is significant because it was used against Sony, in the Dark Seoul attacks and against Aramco of Saudi Arabia. An unknown number of Sony workstations were left unusable by the Destover malware, which overwrites the master boot record of a computer after the attackers pick it clean of files.

"Espionage is a gentlemen's game of sorts with certain rules that most government agencies tend to follow," Bartholomew said. "Certain groups or countries don't tend to follow those rules. … These guys have no problem doing that. The malware is not super sophisticated, but its impact is large. If it works, it works. The payoff is huge for them compared to the resources needed to develop it."

The Lazarus Group's activity spiked in 2014 and 2015 and researchers involved in Operation Blockbuster saw a number of shared characteristics between the malware families used across all these attacks, which also includes Wild Positron and Hangman from last year.

Specifically, the researchers found a number of similarities in the networking functionality of the malware, including six user-agents reused over and over that included the same misspelling of “Mozillar.”

They also saw the use of BAT files to delete malware components after infections.

“These BAT files are generated on the fly and, while they serve their purpose of eliminating initial infection traces, they ironically double as a great way to identify the malware itself by honing in on the path-placeholder strings that generate the randomly-named BAT files on the infected systems,” Kaspersky Lab said in its report.

The group also shares passwords in its malware droppers, keeping the droppers in a password-protected zip archive called MYRES, which is unlocked with the same hardcoded password: !1234567890 dghtdhtrhgfjnui$%^^&fdr.

As to the Lazarus Group’s working habits, samples found and attributed to the group in 2015 doubled year-over-year from 2014, and most of those samples were compiled in the GMT+8 and GMT+9 time zones, which is North Korea’s time zone along a good chunk of Eastern Asia. Novetta, meanwhile, said that 62 percent of the samples it collected have resources set to Korean language sets.

“They are writing their own stuff, but their opsec [operational security] is not the best,” Bartholomew said. “That’s what allowed us to latch on to them. They tend to reuse the same techniques over and over again.”
