The Olympic False Flag: How infamous OlympicDestroyer malware was designed to confuse cybersecurity community

A new attribution method helped Kaspersky Lab to identify a very sophisticated false flag

Kaspersky Lab’s Global Research and Analysis Team has published the results of its own research into attacks by the OlympicDestroyer malware, providing technical evidence of a very sophisticated false flag placed inside the worm by the malware creator in order to knock threat hunters off the trail to its real origin.

The OlympicDestroyer worm made some headlines during the Winter Olympic Games. The Pyeongchang Olympics experienced a cyberattack that temporarily paralyzed IT systems ahead of the official opening ceremony, shutting down display monitors, killing Wi-Fi, and taking down the Olympics website so that visitors were unable to print tickets. Kaspersky Lab has also found that several ski resort facilities in South Korea suffered from this worm, which disabled the operation of ski gates and ski lifts at the resorts. Although the actual impact of attacks with this malware was limited, it clearly contained the capability to be devastating, which luckily didn’t happen.

Nevertheless, the real interest of the cybersecurity industry lay not in the potential or even actual damage caused by the Destroyer’s attacks, but in the origin of the malware. Perhaps no other sophisticated malware has had so many attribution hypotheses put forward as the OlympicDestroyer. Within days of its discovery, research teams from all over the world had between them managed to attribute this malware to Russia, China and North Korea, based on a number of features previously attributed to cyber-espionage and sabotage actors allegedly based in these countries or working for these countries’ governments.

Kaspersky Lab researchers were also trying to understand which hacking group was behind this malware. At some point during their research, they came across something that looked like 100% evidence connecting the malware to Lazarus – an infamous nation state backed group linked to North Korea.

This conclusion was based on a unique trace left by the attackers. A combination of certain features of the code development environment stored in the files can be used as a ‘fingerprint’, in some cases identifying the malware authors and their projects. In the sample analyzed by Kaspersky Lab, this fingerprint gave a 100% match with previously known Lazarus malware components and zero overlap with any other clean or malicious file known to date to Kaspersky Lab. Combined with other similarities in tactics, techniques and procedures (TTPs), it drew researchers to the preliminary conclusion that OlympicDestroyer was yet another Lazarus operation. However, the motives and other inconsistencies with Lazarus TTPs uncovered during the investigation by Kaspersky Lab onsite at the compromised facility in South Korea made researchers revisit the rare artefact.

Following another careful look at the evidence and manual verification of each feature, researchers discovered that the set of features didn’t match the code – it had been forged to perfectly match the fingerprint used by Lazarus.

As a result, the researchers concluded that the features’ ‘fingerprint’ is a very sophisticated false flag, intentionally placed inside the malware in order to give threat hunters the impression that they had found ‘smoking gun’ evidence, knocking them of the trail to more accurate attribution.

“To our knowledge, the evidence we were able to find was not previously used for attribution. Yet the attackers decided to use it, predicting that someone would find it. They counted on the fact that forgery of this artefact is very hard to prove. It’s as if a criminal had stolen someone else’ DNA and left it at a crime scene instead of their own. We discovered and proved that the DNA found on the crime scene was dropped there on purpose. All this demonstrates how much effort attackers are ready to spend in order to stay unidentified for as long as possible. We’ve always said that attribution in cyberspace is very hard as lots of things can be faked, and OlympicDestroyer is a pretty precise illustration of this,” – said Vitaly Kamluk, Head of APAC Research Team, Kaspersky Lab.

“Another takeaway from this story for us is that attribution is has to be taken extremely seriously. Given how politicized cyberspace has recently become, the wrong attribution could lead to severe consequences and actors may start trying to manipulate the opinion of the security community in order to influence the geopolitical agenda,” – he added.

The accurate attribution of OlympicDestroyer is still an open question – simply because it is a unique example of the implementation of very sophisticated false flags. However, Kaspersky Lab researchers found that the attackers used privacy-protecting service NordVPN and a hosting provider called MonoVM, which both accept Bitcoins. These and some other discovered TTPs were previously seen to be used by Sofacy – the Russian-speaking actor.

Kaspersky Lab products successfully detect and block the OlympicDestroyer malware.

Read more about how Kaspersky Lab researchers investigated the OlympicDestroyer attacks in South Korea and Europe in the blogpost on Securelist.com.

OlympicDestroyer is here to trick the industry