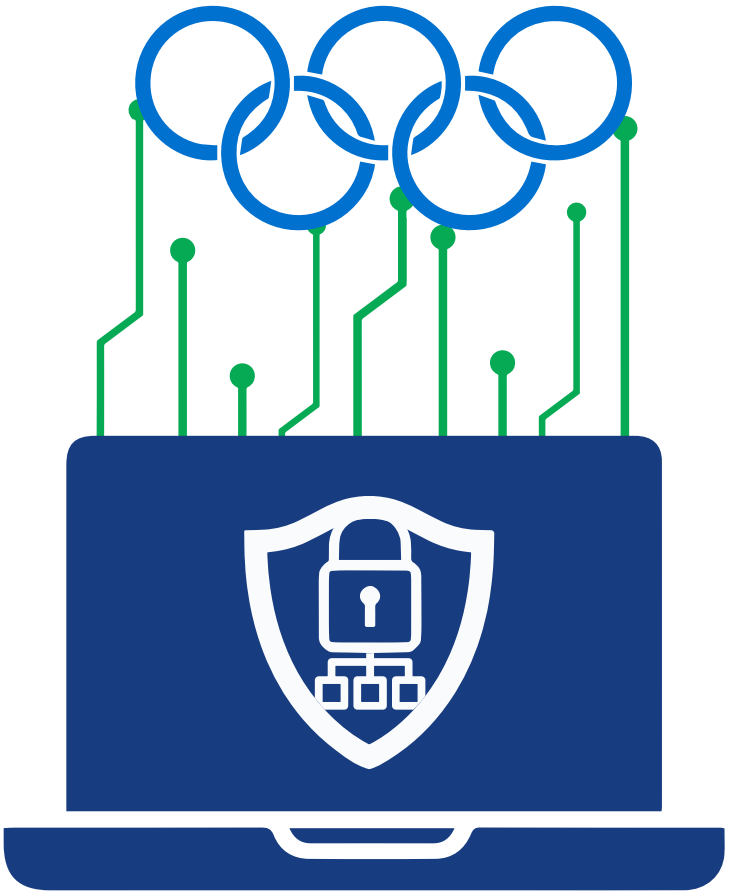
Recorded Future

FLASH REPORT

Targeting of Olympic Games IT Infrastructure Remains Unattributed

By Juan Andres Guerrero-Saade,
Priscilla Moriuchi, Greg Lesnewich
Recorded Future



FR-2018-0214

Executive Summary

A major telecommunications and IT provider was targeted by an unknown threat actor as part of an operation directed at disrupting the Olympic Games in PyeongChang. Recorded Future identified hardcoded credentials for the IT provider embedded in the Olympic Destroyer malware used in this campaign. Small amounts of code overlap connect the malware to numerous, disparate threat groups, which ultimately does not help to identify the threat actor responsible for developing the Olympic Destroyer malware.

Key Judgments

- Olympic Destroyer should be treated with a high level of concern, due to the destructive nature of the malware and its potent mechanisms to spread laterally.
- Commentary and analysis surrounding malware code similarities of Olympic Destroyer have yielded many leads but no conclusive attribution.
- The co-occurrence of disparate code overlaps in the malware may be indicative of a false flag operation, attempting to dilute evidence and confuse researchers.

Background

A major telecommunications and IT provider was targeted by an unknown threat actor as part of targeting the Olympic Games in PyeongChang prior to December 2017.

The malware, commonly referred to as Olympic Destroyer, was initially identified by Talos researchers. Researchers have theorized that Olympic Destroyer was used to disrupt the Olympic Games opening ceremony on February 9. The destructive malware moves laterally within a network via Psexec and WMI, to infect hosts and render their data useless. Psexec and WMI are built-in Windows internal tools; Psexec is used to execute processes on other systems in a shared network, and WMI is used to automate tasks on remote systems. The malware also uses Mimikatz, a password-stealing tool, to extract credentials from a compromised machine, also allowing it to move across the target network. Microsoft researchers stated that there is also evidence of use of EternalRomance, a leaked exploit recently abused by ransomware as a propagation method, but we were unable to verify this claim.

Threat Analysis: A Two-Pronged Campaign

Recorded Future found an extended set of malware targeting the PyeongChang Games using an additional set of Active Directory credentials. The diversity of credentials and presence of a software key suggest that an early reconnaissance phase would likely involve an initial malware infection and not just simple credential phishing.

All samples of the Olympic Destroyer malware variant targeting the IT provider were timestamped five minutes prior to the compilation of the samples identified by Talos researchers as targeting the PyeongChang 2018 network. This suggests a parallel, two-pronged attempt to target the Olympics event, aimed at both organizers and infrastructure providers.

Additional unreported malware hashes are contained in the appendix below.

Upon discovery of the hardcoded credentials, Recorded Future adhered to responsible disclosure practices, notified the relevant IT provider, and provided details of the campaign. An independent forensic investigation is underway and no damage is reported at this time.

Technical Analysis: Attribution Remains Elusive

One of the most innovative techniques currently employed by advanced research teams is hunting for code similarity at scale. Google researchers were the first to notably employ this technique to cluster previously unattributed campaigns like that of North Korean threat actor Scarcruft and WannaCry, ultimately tying both to the Lazarus Group . BAE researchers discovered the first overlaps in malware used by BlueNoroff employed in the Bangladesh SWIFT heist by noting use of a shared wiping function, once again pointing the finger at North Korea. Kaspersky researchers used this method to link the trojan targeting CCleaner to the Axiom group, and so on.

The trouble with this technique is that while code similarity can be stated with certainty, down to a percentage of bytes shared, the results are not straightforward and require expert interpretation. The Olympic Destroyer malware is a perfect example of how we can be led astray by this clustering technique when our standard for similarity is too low.

Olympic Destroyer remains unclustered and unattributed. Because this technique still requires expert interpretation, casual or incomplete analysis can yield seemingly cohesive narratives, for example, pointing in the direction of North Korea, China, or Russia. This occurs when the code is looked at with a low enough correlative threshold.

Below are some disparate observations derived from the Olympic Destroyer malware based on code similarity analysis:

China: Intezer researchers were the first to point to fragments of code similarity with diverse threat actors in the general Chinese cluster, including APT3 (UPS), APT10 (menuPass), and APT12 (IXESHE).

North Korea: Our own research turned up trivial but consistent code similarities between Olympic Destroyer modules and several malware families used by the Lazarus Group. These include standard but different functions within BlueNoroff Banswift malware, the LimaCharlie family of Lazarus malware from the Novetta Blockbuster report, and a module from the Lazarus SpaSpe malware meant to target domain controllers.

Before one concludes that these widely diverse threat actors have formed an axis of evil intent on disrupting the Olympics, we need to take a step back and look at our research techniques.

Code similarity historically yielded significant research findings in clustering new campaigns to known threat actors and continues to hold great promise for research and malware classification. However, it does require scrutiny and discernment when the similarity threshold is so low as to focus on a few functions, or less. As with previous attributory methods, researchers must remain vigilant to the ever-looming threat of adversary adaptability.

Israeli nation-state-sponsored threat actor Flame leveraged a previously theoretical cryptographic attack to spread laterally. Threat group Turla lead incident responders astray by placing unrelated malware on their victims' machines, and the Lamberts spliced random clean code to use as encryption keys in order to avoid accurate clustering. Our adversaries are resourceful. While fooling code similarity clustering takes significant effort and skill, we must consider it possible for determined, higher-tier attackers with the right motivations.

Outlook

The operation to disrupt the PyeongChang Winter Olympic Games was more extensive than originally reported, with both organizers and infrastructure targeted simultaneously. The wealth of spreading mechanisms embedded within the malware suggests an aggressive effort to spread within these networks and cause maximum damage. The co-occurrence of code overlap in the malware may be indicative of a false flag operation, attempting to dilute evidence and confuse researchers. For the time being, attribution remains inconclusive.

Targeting of Olympic Games IT Infrastructure Remains Unattributed

Appendix A: Indicators of Compromise

Hashes

SHA256	MD5
3e27b6b287f0b9f7e85bfe18901d961110ae969d58b44af15b1d75be749022c2	ca0eaca077aa67f2609f612cefe7f1f3
9ebb32fbc698819215f56a52c028b00ef107fbbecb186c9641f1f5ed1ebd6d53	dfedf303b4d9b77ce5e59407c9484c37
32efb1eb360cda726f0eb7647d1963adf37dada4b1a4b5ec486c88bfa1f21471	59c3f3f99f44029de81293b1e7c37ed2
28858cc6e05225f7d156d1c6a21ed11188777fa0a752cb7b56038d79a88627cc	ec724ef33521c4c2965de078e36c8277
d934cb8d0eadb93f8a57a9b8853c5db218d5db78c16a35f374e413884d915016	221c6db5b60049e3f1cdbb6212be7f41
9e0d68d3ea0db211bdcf3a6e64572ccbfef2dc901ce3def2898337319cc9744b	a8224a04579b7e9039f91ac9b76c19dc
60fae5d55dbce0dc78bcb384ccff6ac52e2889824cfc33a5534f7bad9d917875	c0876c9079234bfa816ed9bc6502a351
E8349cfcc422310c259688b0226cb14f5196a6daad77b622405282aeac89ab06	E5f9b1500510a540a532a2378dce3c6b
5e9a61086a03ce7854bb3dd44cf337d8d141ca9bc50250c1d33224fdd5da1e18	907c2c79ef21d84ff5ea6ed854f24f05

940e0c1cb1940e3af272f49246459bf0343f3371329b095bea5b6c09366f04d6	F37d710247e186d84a2a1a04cccfd9fe
Ae9db7cbbb1b36ac5e6e761ed4f7885074bdeffbe3aeca80312d04364e56cd00	Bf88eb2d4294554f73d39f54dc817dd5
08cc6b8c73cb94af33efbcb74a58d7d0fc08e4d4f799d9b2da82170b38cbb7a8	Da24c88fff360419801814d74c2ddae5
8d92931af98496c2281553325fb9baec822ab33620b2bb9f1745d42ec64722e0	5778d8ff5156de1f63361bd530e0404d