| Overall Report Distribution is TLP: GREEN |
| --- |
| Overall Source/Information Reliability: B2 |

# Executive Summary

On May 12, the WannaCry ransomware began spreading across the globe, infecting computers in at least 150 countries. At least one security organization detected 200,000 detections as of this writing, with Russia, China, Taiwan, and Ukraine suffering the largest amount of infections. The malware, which was initially delivered via an unknown initial infection vector, utilizes leaked National Security Agency (NSA) exploits to propagate as a worm and deliver the ransomware payload. Some versions of the malware feature a "kill-switch," which temporarily stopped some infections globally.

The actual WannaCry payload does not stand out from other new strains of ransomware, but its delivery mechanism and propagation as a worm is what sets it apart. Threat sources anticipate a disturbing new trend of cyber criminals repurposing pieces of leaked nation state toolkits, as seen with WannaCry. This decreases development time, and maximizes impact and potential monetization, therefore increasing the overall effect. Currently, it is not known what individual or group is behind this aggressive campaign.

## Key Points

- On May 12, 2017, the WannaCry ransomware began aggressively spreading throughout the world, infecting computers in at least 150 countries with Russia, China, Taiwan, and Ukraine having the most infections.
- The initial infection vector is currently unknown – there is no evidence to support previously reported claims that it came from emails containing malicious attachments.
- The malware features NSA exploits to propagate as a worm via internal and external networks.
- There have been multiple versions of the malware released already, indicating active development and response to the security community's research and mitigation actions.
- As of this writing, there is no information as to the individual or group behind this campaign.

**This report is based on open source findings. Therefore, the report is open source intelligence and does not constitute definitive evidence. Information found in the open source cannot necessarily be verified and is presented as intelligence and as additional information to enhance or expand current investigations.*