Cybereason exposes Winnti campaign and achieves industry recognition

Cybereason, a leading endpoint protection platform, has revealed new insights into a cyber espionage campaig that has been targeting technology and manufacturing companies in Asia, Europe and North America since at least 2019.

Source: Cottonbro studio/Pexels

The campaign, attributed to the notorious Winnti group, involves the use of novel and stealthy malware, such as digitally signed kernel-level rootkits and a complex multi-stage infection chain. Cybereason's researchers have uncovered the Win group's tactics and techniques, which include exploiting legitimate software, abusing code signing certificates, and evadin detection by antivirus and network security tools.

AUTOMOTIVE

Top Gear is over

21 Nov 2023

The goal behind these intrusions was to steal sensitive intellectual property for cyber espionage purposes. They have also discovered a new malware strain called DEPLOYLOG used by the Winnti APT group and highlighted new versions of kno Winnti malware, including Spyder Loader, PRIVATELOG, and WINNKIT3.

New industry standard

Cybereason's findings come after the company achieved an exceptional performance score in the MITRE ATT&CK evaluation, a rigorous and independent assessment of endpoint security solutions. The evaluation measured Cybereason's ability to detect and respond to real-world attack scenarios based on the MITRE ATT&CK framework, a globally recognise knowledge base of adversary behaviours.

This year, Cybereason set a new benchmark with perfect results in nearly every aspect of the evaluations, including:

- 100% Protection: uncovered and prevented 100% of the 13 attack sequences evaluated
- 100% Detection: detected 100% of all 19 attack steps executed by the Turla threat actor
- 100% Visibility: exposed 100% of the 143 attack behaviours evaluated for both Windows and Linux

- 97% Technique Coverage: nearly every detection mapped back to the key ATT&CK techniques being evaluated
- 100% Real Time Protection: zero delayed detections
- 100% Out of the Box: delivered complete out-of-the-box performance with no configuration changes required

Gartner recognition

Greg Day, VP and global field CISO

The company demonstrated its MalOp detection and response capabilities, which provide a holistic and contextual view of malicious operations across the entire attack lifecycle.

Exceptional performance in the MITRE ATT&CK evaluation also contributed to its recognition as a leader in the Gartner Magic Quadrant for Endpoint Protection Platforms, a prestigious report that evaluates vendors based on their vision and ability to execute.

Cybereason was positioned highest for its ability to execute and furthest for its completeness of vision in the leader's quadrant, reflecting its innovation and customer satisfaction.