Trend Micro Research Finds Growing Cyber Threats Targeting eSports Industry

New report predicts escalating attacks by cybercriminals and players

DALLAS--(BUSINESS WIRE)--Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global leader in cybersecurity solutions, today announced the findings of new research predicting multiple cyber threats to the fast-growing electronic sports (eSports) sector. Though cybercriminals have been targeting the gaming community since 2010, eSports players, gaming companies, sponsors and viewers will be more at risk over the coming years from data theft, ransomware, DDoS, hardware hacks and cybercrime-as-a-service.

The eSports industry has grown rapidly in popularity over recent years and is projected to reach $1.7B in revenue by 2021. It has also evolved to include a professional sporting league, with stadiums selling out to host competitions and top players earning millions. This growth is attractive for financially motivated criminals.

“If there’s one thing we know about malicious actors, it’s that they follow the money. Trend Micro has already observed financially motivated groups taking advantage of security gaps to target the gaming industry for financial gain, and we expect the same in eSports,” said Jon Clay, director of global threat communications for Trend Micro. “As eSports becomes a billion-dollar industry, it’s inevitable that attackers will look to capitalize over the coming years. We predict the sector will experience the same kind of attacks as the gaming industry, but on a much larger scale, with financially motivated actors getting involved for monetary and geopolitical reasons.”

Based on this research, Trend Micro predicts cybercriminals will ramp up their efforts to make money from ransomware aimed at sponsors and players, DDoS-for-hire services, breaches of personal information (PII), services to illegally boost gaming scores, and stolen gaming accounts. Weak password and authentication security, which is already enabling widespread account takeover, will continue to play a role in making these attacks possible.

The impacts from breaches, ransomware, DDoS and other attacks on gaming companies and sponsors can be severe, leading to damaged brand reputation and revenue loss. The servers used by companies to host valuable gaming assets are a prime target for exploitation by hackers.

To protect these valuable assets, the eSports industry should leverage a multi-layered defense system to protect servers and virtually patch known vulnerabilities.

To read the full report, *Cheats, Hacks, and Cyberattacks: Threats to the eSports Industry in 2019 and Beyond*, please visit: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/cheats-hacks-and-cyberattacks-threats-to-the-esports-industry-in-2019-and-beyond.

About Trend Micro

Trend Micro Incorporated, a global leader in cybersecurity solutions, helps to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses, and governments provide layered security for data centers, cloud environments, networks, and endpoints. All our products work together to seamlessly share threat intelligence and provide a connected threat defense with centralized visibility and control, enabling better, faster protection. With more than 6,000 employees in over 50 countries and the world’s most advanced global threat intelligence, Trend Micro secures your connected world. For more information, visit www.trendmicro.com.

Contact:

Erin Johnson
817-522-7911
media_relations@trendmicro.com

Public Company Information:

TOKYO:
4704
JP3637300009
OTC Pink:
TMICY

https://newsroom.trendmicro.com/2019-10-29-Trend-Micro-Research-Finds-Growing-Cyber-Threats-Targeting-eSports-Industry