May 2, 2024

2024 Eurovision Song Contest in Malmö

The Eurovision Song Contest is an internationally televised songwriting competition, organized by the European Broadcasting Union (EBU) and featuring participants chosen by EBU member broadcasters representing their countries from across Europe and beyond.

The Grand Final of the 2024 Eurovision Song Contest will take place in Sweden’s Malmö Arena on Saturday, May 11 with Semi-Finals on Tuesday, May 7 and Thursday, May 9.

Radware assesses with moderate confidence that the 2024 song content could experience attempts to disrupt the event given current geopolitical tensions.

Background

Previous song contests have experienced cyberattacks due to geo-political conflicts. The 2022 Eurovision Song Contest was held in Turin, Italy. Ukraine's Kalush Orchestra won the contest with their entry "Stefania" riding a wave of public support to claim an emotional victory that was welcomed by the country's president Volodymyr Zelenskyy.

During voting and the performances, the Italian police cybersecurity department blocked several cyberattacks on network infrastructure claimed by pro-Russian hacktivist group Killnet and its affiliate Legion.

Similar concerns were raised during the 2023 song contest. Ukraine was originally set to host that year’s Eurovision after winning in 2022, but it was unable due to instabilities in the region after the Russian invasion in February 2022. Therefore, Liverpool in the United Kingdom (UK) was selected as host city for the 2023 contest. Experts from the UK’s National Cyber Security Centre were brought in to protect the competition’s public vote from potential cyberattacks by pro-Russian hackers.

Potential Targets

BROADCASTING SYSTEM

The Eurovision Song Contest is broadcasted through multiple channels:

- TV Broadcast: All participating countries must use the local national broadcaster with an active EBU membership capable of receiving the contest via the Eurovision network and broadcasting it live nationwide.

- Digital: Viewers can watch the song contest via one of many music and streaming services, including Apple Music, Amazon Music, Spotify, YouTube Music, YouTube, Deezer, Tidal, Eurovision websites and Qobuz.

VOTING

Several changes have been made to the voting system in 2024. Viewers watching around the world, outside those in participating countries, can now vote for their favorite songs for 24 hours before each semi-final and the Grand Final.

Voting in the Grand Final will also open just before the first song is performed. It will remain open throughout the performances and for up to 40 minutes after the final song is performed.

All viewers in participating and non-participating countries alike can vote using the official Eurovision app or go directly to www.esc.vote. In addition, those watching in the participating countries can vote by telephone and/or SMS. Relevant, local, numbers will be displayed on screen by each participating broadcaster and on www.esc.vote.

With multiple streaming and voting channels, the threat surface expands to include web, API, TCP, UDP, DNS and telephony. Several attack methods can be leveraged by attackers.

Geo-political Tensions

Geo-political tensions drive hacktivists' motivation to target and attempt to disrupt the song contest, especially given the recent joining of Sweden in NATO. Sweden's relations with NATO date back to 1994, when Sweden joined the Partnership for Peace. Since then, Sweden's cooperation with NATO has gradually increased and on March 7, 2024, Sweden became a full member of NATO.

Additionally, calls have been made to exclude countries from the contest based on political conflicts. Beginning in 2022, Russia has been banned from participating in the Eurovision Song Contest because of its invasion of Ukraine. And since the outbreak of the Israel–Hamas war on October 7, 2023, calls have been made for Israel to be excluded from the contest on the grounds of the humanitarian crisis resulting from Israeli military operations in the Gaza Strip. Malmö police received multiple requests for protests during the Eurovision week. Some are against Israeli participation in the contest, against the war in Gaza or in favor of Palestine. Others are in support of the Israeli Eurovision delegation.

Reasons for Concern

The Eurovision Song Contest in Sweden will create a platform for cybercriminals to spread propaganda, create disruption and generate profits. With attackers leveraging new tools and generative artificial intelligence to automate attacks, it has become increasingly easier for cybercriminals and even average citizens to carry out disruptive attacks. Toolkits, attack services and initial access are widely available for download or purchase across the internet and—as a result of the growing cyber conflict between Russia and the rest of the world—attack techniques have improved.

One of the biggest concerns for network operators surrounding large-scale events such as the Eurovision Song Contest is protecting networks and applications that support multiple operations. Broadcast networks, streaming, voting, control, operational networks and other related systems are all considered at risk because of geo-political conflicts.

Using DDoS attack techniques, hacktivist groups may attempt to:

- Interrupt live video or audio streams during specific songs according to the countries they represent
- Interrupt voting channels or the complete voting system during specific songs
- Interrupt contest operations to cause chaos or harm the reputation of the games
- Interrupt the ticket validation infrastructure during the semi-final or final events. There's nothing worse than having a long queue of people and not being able to validate tickets

The above threats may result in partial event disruption, reputation loss and promoting political propaganda in an event created to unite people around music and art.

EFFECTIVE DDOS PROTECTION ESSENTIALS

Hybrid DDoS Protection – Use on-premises and **cloud DDoS protection** for real-time **DDoS attack prevention** that also addresses high-volume attacks and protects from pipe saturation

Behavioral-Based Detection – Quickly and accurately identify and block anomalies while allowing legitimate traffic through

Real-Time Signature Creation – Promptly protect against unknown threats and zero-day attacks

Web DDOS Tsunami Protection – Automated immediate detection and mitigation of Web DDOS encrypted high RPS and morphing attacks

A Cybersecurity Emergency Response Plan – Turn to a dedicated emergency team of experts who have experience with Internet of Things security and handling IoT outbreaks

Intelligence on Active Threat Actors – High fidelity, correlated and analyzed data for preemptive protection against currently active known attackers

For further **network and application protection** measures, Radware urges companies to inspect and patch their network to defend against risks and threats.

EFFECTIVE WEB APPLICATION SECURITY ESSENTIALS

Full OWASP Top-10 coverage against defacements, injections, etc.

Low false positive rate using negative and positive security models for maximum accuracy

Auto-policy generation capabilities for the widest coverage with the lowest operational effort

Bot protection and device fingerprinting capabilities to overcome dynamic IP attacks and achieve improved bot detection and blocking

Securing APIs by filtering paths, understanding XML and JSON schemas for enforcement, and using activity tracking mechanisms to trace bots and guard internal resources

Flexible deployment options including on-premises, out-of-path, virtual or cloud-based

LEARN MORE AT RADWARE'S SECURITY RESEARCH CENTER

To know more about today's attack vector landscape, understand the business impact of cyberattacks, or learn more about emerging attack types and tools, visit Radware's **Security Research Center**. Additionally, visit Radware's **Quarterly DDoS & Application Threat Analysis Center** for quarter-over-quarter analysis of DDoS and application attack activity based on data from Radware's cloud security services and threat intelligence.

THIS REPORT CONTAINS ONLY PUBLICLY AVAILABLE INFORMATION, WHICH IS PROVIDED FOR GENERAL INFORMATION PURPOSES ONLY. ALL INFORMATION IS PROVIDED “AS IS” WITHOUT ANY REPRESENATION OR WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES THAT THIS REPORT IS ERROR-FREE OR ANY IMPLIED WARRANTIES REGARDING THE ACCURACY, VALIDITY, ADEQUACY, RELIABILITY, AVAILBILITY, COMPLETENESS, FITNESS FOR ANY PARTICULAR PURPOSE OR NON-INFRINGEMENT. USE OF THIS REPORT, IN WHOLE OR IN PART, IS AT USER’S SOLE RISK. RADWARE AND/OR ANYONE ON ITS BEHALF SPECIFICALLY DISCLAIMS ANY LIABILITY IN RELATION TO THIS REPORT, INCLUDING WITHOUT LIMITATION, FOR ANY DIRECT, SPECIAL, INDIREC, INCIDENTAL, CONSEQUENTIAL, OR EXAMPLARY DAMAGES, LOSSES AND EXPENSES ARISING FROM OR IN ANY WAY REALTED TO THIS REPORT, HOWEVER CAUSED, AND WHETHER BASED ON CONTRACT, TORT (INCLUDING NEGLIGENCE) OR OTHER THEORY OF LIABILITY, EVEN IF IT WAS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, LOSSES OR EXPENSES. **CHARTS USED OR REPRODUCED SHOULD BE CREDITED TO RADWARE.**