ORNA™

Cybersecurity Advisory

Dear ORNA Customer,

We are sending you this advisory to provide situational awareness about a cybersecurity attack against the british company Newsquest Media Group and its many subsidiary newspapers and magazines.

Summary

On the 18th of May, a group only known by their self-identifying moniker "first-class Russian hackers" defaced numerous local and regional British newspaper websites, all owned by Newsquest Media Group. The hackers posted a breaking news story titled "***PERVOKLASSNIY RUSSIAN HACKERS ATTACK***", which lacked any actual content except for the group's name, a logo, and a Cyrillic byline. Although several Newsquest titles were affected, it remains unclear if the hackers were genuinely Russian.

Threat Intelligence researchers have highlighted that this attack with similar cyber incidents has links to Russian and Belarusian threat actors like the **Ghostwriter** group, known for spreading false stories to create discord. Ghostwriter typically targets journalists through spear-phishing to access their content management systems. Earlier this year, a Czech news service was hacked to publish a false assassination story about the Slovak president, likely an information operation. This recent attack on Newsquest raises concerns about the resilience of local media against such cyber threats, underscoring the need for robust cybersecurity measures in the media sector.

Recommendations

Recommendation #1: Stay up do date

Monitor official channels to stay informed and updated on the situation involving these cybersecurity attacks.

Recommendation #2: Vigilance and monitoring

Maintain heightened vigilance and monitor network activity for suspicious behavior or indicators of compromise.

Recommendation #3: Prepare for the Worst

ORNA **strongly recommends** that organizations ensure that all critical systems are backed up appropriately and that incident response plans are rehearsed regularly so that all participants understand their role.

References

1. https://therecord.media/newsquest-media-group-british-newspaper-websites-defaced
2. https://malpedia.caad.fkie.fraunhofer.de/actor/ghostwriter

If you have any additional questions, please reach out to your ORNA representative at sme@orna.app.

Sincerely,
ORNA Team