Article

Oct 2024

Russian military cyber actors target U.S. and global critical infrastructure

The UK, alongside nine international allies, has publicly attributed a campaign of malicious cyber activity to Russia's GRU Unit 29155.

Alex McIntosh
Information Security Consultant
Email alex.mcintosh@waterstons.com

These operations were conducted for the purpose of espionage, sabotage and reputational harm, and have believed to have been ongoing since 2020. Paul Chichester the director of operations at the NCSC said: "The UK, alongside our partners, is committed to calling out Russian malicious cyber activity." The intervention comes as governments in Europe have reportedly witnessed a rise in Russian Espionage in the wake of the Ukrainian war.

Within the arsenal of Unit 29155 is a type of destructive malware called Whispergate, which has two stage to corrupt a system's master boot record: displaying a fake ransomware note, and encrypting files based on certain file extensions. Although a ransomware message is displayed during the attack, Microsoft highlighted that the targeted data is destroyed and is not recoverable even if a ransom is paid.

As a result of these malicious activities, a new joint advisory has been created by the National Cyber Security Centre (NSCS) and other similar agencies from around the world to help organisations bolster their defences.

Wider context

GRU Unit 29155 operates distinctively from other Russian cyber units like Fancy Bear (Unit 26165) and Sandworm (Unit 74455), leveraging junior GRU officers and cybercriminal collaborations for espionage and sabotage. The exposure of Unit 29155 highlights a trend of Russian cyber operations targeting entities aligned with aid efforts to Ukraine, reflecting broader geopolitical conflicts. WhisperGate is part of Russia's ongoing cyber warfare tactics, which include leveraging destructive malware to destabilise victim organisations and sow confusion. It is believed that the same unit has been carrying out cyber operations since 2020.

Recommendations

NCSC strongly advises the use of the mitigation advice and guidance in the advisory.

According to the advisory there are three main actions that organisations should take today to mitigate malicious cyber activity:

- Prioritise routine system updates and remediate known exploited vulnerabilities
- Segment networks to prevent the spread of malicious activity
- Enable phishing-resistant multifactor authentication (MFA) for all externally-facing account services, especially for webmail, virtual private networks (VPNs), and accounts that access critical systems.

This article and other fantastic insights are shared in our monthly cyber threat report. You can join the mailing list to receive it here.

Waterstons has 25+ years' experience across the UK and Australia preparing and protection organisations from cyber threats. We are committed to assisting all organisations to stay agile and prepared in today's cyber conscious economy.

Empower your organisation today, get in touch with one of our team members.

info@waterstons.com.au | 02 9160 8430