Tomorrow's Affairs
Analysis of today
Assessment of tomorrow

By: Tomorrow's Affairs Staff

A specialised group within the Russian GRU is behind the cyberattack on Western critical infrastructure

Western governments published a joint cybersecurity advisory after the discovery that the Russian military intelligence service GRU is directly behind a series of global cyberattacks, particularly on infrastructure in NATO member states.

The security services of the US, UK, Germany, Canada, and Western European governments determined that their cyber infrastructure was exposed to attacks by a specialised group within the GRU—Unit 29155.

The attacks were long-running and systematic, and their goal was unauthorised data collection, espionage, sabotage, and publication of stolen data.

According to the German domestic intelligence agency BfV, a specialised cyber-warfare group within the GRU was tasked with undertaking malicious activities against critical infrastructure globally, including the US.

New Russian player

This is the first time that Unit 29155 has been identified as responsible for attacks on Western targets, so government intelligence agencies specifically warn that its actions and methods should be distinguished from some previously identified Russian groups.

This is the same department of the Russian intelligence service (GRU) that was involved in the poisoning of former Russian agent Sergei Skripal and his daughter in Salisbury in 2018.

Western services point out that this group has already been involved in attempted coups around the world, sabotage, and assassinations, and that since 2020, if not earlier, it has focused on cyberattacks.

Unit 29155 specifically targeted the computer systems and databases of state agencies, as well as companies from NATO member states

Unit 29155 specifically targeted the computer systems and databases of state agencies, as well as companies from NATO member states dealing with finance, energy, and the health sector.

The primary objective of these attacks is believed to have been to disrupt the delivery of Western aid to Ukraine's defence against Russian aggression.

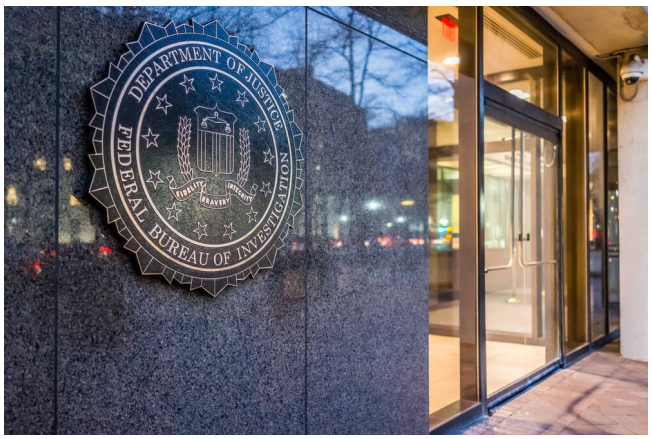
“The exposure of Unit 29155 as a capable cyber actor illustrates the importance that Russian military intelligence places on using cyberspace to pursue its illegal war in Ukraine and other state priorities,” said Paul Chichester, director of operations at the UK's National Cyber Security Centre (NCSC).

Recommendations for defence

Western intelligence has thoroughly analysed the methods and techniques used by a group within the Russian GRU during the attacks. Based on this analysis, Western intelligence has issued several recommendations to all organisations potentially threatened by 29155, requiring their implementation immediately.

According to the US Cybersecurity and Infrastructure Security Agency (CISA), organisations should immediately prioritise routine system updates and remediate known exploited vulnerabilities, as well as segment networks to prevent the spread of malicious activity.

They also recommended enabling phishing-resistant multifactor authentication (MFA) for all externally facing account services, especially for webmail, virtual private networks (VPNs), and accounts that access critical systems.



GRU junior active-duty officers, under the supervision of more experienced members of this service, carried out the attacks with support from known cybercriminals outside the GRU - FBI

Several US government agencies, including the Department of the Treasury and the Department of State, as well as related agencies from the UK, Canada, the Netherlands, the Czech Republic, Germany, Estonia, Latvia, Ukraine, and Australia, jointly analysed Russian cyberattacks to produce these recommendations.

"Unit 29155 cyber actors' objectives appear to include the collection of information for espionage purposes, reputational harm caused by the theft and leakage of sensitive information, and systematic sabotage caused by the destruction of data," stated the joint cybersecurity advisory.

The FBI estimated that GRU junior active-duty officers, under the supervision of more experienced members of this service, carried out the attacks with support from known cybercriminals outside the GRU.

Focus shifted to Ukraine

Since 2020 (or earlier), this group's activities have primarily focused on website defacements, infrastructure scanning, data exfiltration, and data leak operations. They sold or published the data they collected in this way.

However, in the run-up to and following Russia's attack on Ukraine in February 2022, its focus has shifted to disrupting Ukrainian defence aid coming from NATO member states and their partners.

> Attackers scouted targets in government organisations and infrastructure systems, using publicly available tools

Attackers scouted targets in government organisations and infrastructure systems, using publicly available tools to scan and assess the vulnerabilities of the objects of their attacks.

The Russian military intelligence service is believed to have a broader victim base for its cyberattacks than previously identified. In particular, Western agencies warn all potential targets not to use previous experience with Russian attackers linked to the GRU to protect against the actions of this group, as 29155 uses authentic tactics for attacks on Western critical infrastructure.