

RUSSIA - UKRAINE DIPLOMATIC TENSION AFTER CYBER ATTACKS

WHAT HAPPENED?

On 14 Jan, Ukraine reported a targeted hacking of at least seven ministries of the country's cabinet – including the **Treasury, the National Emergency Service and the state services website** – where Ukrainians' electrical passports and vaccination certificates are stored.

“Ukrainian! All your personal data was uploaded to the public network. All data on the computer is destroyed, it is impossible to restore it,”

“All information about you has become public, be afraid and expect the worst. This is for your past, present and future”

said the message visible on hacked government websites, written in Ukrainian, Russian and Polish.

Upon investigation by Ukraine's state security service, SBU it was revealed that more than 70 internet sites of government bodies had been hit by the cyberattack – including the security and defense council.

The Ukrainian government in a statement said that “almost all” websites were back up and running by 1400 Hrs. on 17 Jan, and that it had engaged experts from Microsoft to identify the origin of the attack,

BACKGROUND

Three Things To Note



Timing of the attacks

The attacks came only a day after the conclusion - with failure - of the latest round of diplomatic efforts in Europe aimed at deterring Russia's military build-up near Ukraine. The efforts ended with Russia standing rigidly on its demands, including



Involvement of Belarusian Group

Serhiy Demedyuk, The Deputy Secretary of the national security and defence council attributed the attacks to UNC1151, a Russian-backed cyber-espionage group linked to Belarus, a close ally of Russia. Demedyuk also marked that the attacks were cover for more destructive actions behind the scenes.



Arrest of Russian Hacker Group

Russia arrested the members of "REvil ransomware gang", announcing that it had done so at the request of Washington. The Russia-based "REvil" have carried out major cyber-attacks - including the Jul 2021 attack on software provider Kaseya, May 2021 attack on the JBS, the largest meat producer and involved in the cyberattack on the Colonial pipeline.

What was the nature of the Cyber-Attack?

- In a blog post published by Microsoft following the cyber-attacks, Microsoft Threat Intelligence Center (MSITC) identified evidence of a malware in multiple systems across Ukraine, originally designed to look like a ransomware but lacking a ransom recovery mechanism.
- As per MSTIC, the malware was intended to be destructive and designed to render targeted devices inoperable. The attacks were initiated by hacking the infrastructure of a commercial company that had access, with administrative privileges, to websites affected by the attack.

ASSESSMENT

Considering the timing of the cyber-attacks, and its attribution to Russian-backed groups; experts have pointed that the attacks could be a pretext to a further invasion of Ukraine. Although Russia denied any involvement, US, European Union and NATO released statements signaling solidarity with Kyiv and promised support to Ukraine in light of the cyberattacks.


WHAT IMPACT COULD THE CYBER ATTACKS HAVE ON THE RUSSIAN-UKRAINIAN CRISIS?

Preparation For War	Alternative To War	Risk of Misperceptions
<p>Russia's past behavior – during annexation of Crimea in 2014, and during invasion of Georgia in 2009 – suggests that the cyberattacks could be a pretext to launch a full-scale invasion.</p> <p>Such cyber-attacks may allow Moscow to enhance its military strategy, create uncertainty in Ukraine and deplete the trust in the government among the public.</p>	<p>The cyber-attacks could also be an alternative to invasion, since its low-cost, high impact nature may allow Moscow to raise tensions in non-military domain, while keeping other options on the table during a possible negotiation.</p> <p>It may also allow Kremlin to signal a continuance of its strident-stance vis-à-vis Ukraine, without risking physical violence.</p>	<p>The current situation in Ukraine also allows numerous geostrategic miscalculations on either sides.</p> <p>Russia could be using cyber-attacks to test the resolve of US and its allies in the region; whereby, any provocation could provide Moscow with a justification to further escalate the ongoing conflict.</p> <p>If the attack originated independently, threatening Russia make only make a conflict more likely.</p>




ABOUT THE AUTHOR


Piyush Singh is part of the Risk Intelligence Team at WoRisGo and a final-year student pursuing M.A in Diplomacy, Law and Business from Jindal School of International Affairs. He is passionate about security studies and intelligence studies. His areas of interest include contemporary geopolitics, cross-straits relations, and Chinese politics.




WORLD
RISK &
GOVERNANCE



www.worisgo.com



risk.services@worisgo.com




1800-572-8600

Prepared at the Risk Assessment and Analysis Centre, Bangalore

©COPYRIGHT-WoRisGo

Terms of Use - The business continuity, compliance and security risk advisory contained above is based on analysis of information in public domain and our expertise in the domains. For certain verifications, we have also depended on due diligence with officials wherever necessary or feasible. The analysis and information are provided on as-is basis with no liability. Various organizations may arrive at different outcomes, business continuity plans and other decisions based off on these inputs. Our analysis is just one of the several data points towards enabling such decisions. This analysis should be consumed in the context of your organization's risk appetite, business practices, governance policies and bearing other situational and relevant factors in mind.



**Your GRC Partner:
our assurance during
uncertainties**