# Reliance acsn – Ukraine Crisis Update

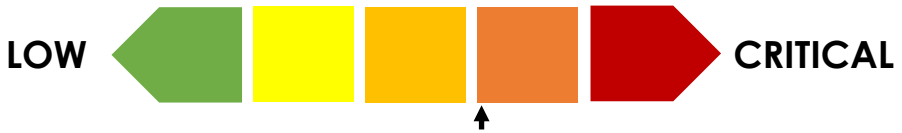
**Strategic Assessment**

*Forced into another reappraisal of its objectives following its forces' retreat from Kharkiv, the Kremlin has focused its military resources on the Donbas. The battles for Severodonetsk and Lyushansk are key. Severodonetsk, as the largest city in Luhansk Oblast still under Ukrainian control and crucially east of the Siverskiy Donets river, is of increasing strategic importance. In order to claim success in the Donbas, Putin needs his forces to capture both cities. Both sides recognise the importance of the outcome of the battle of Severodonetsk, with the Ukrainian government admitting it will have significant implications for the future of the country. The sheer ferocity and intensity of the conflict has surprised Western observers, including US DoD, particularly the scale of causalities on both sides and the extraordinary expenditure of munitions which has not been seen in a conflict since the Korean War. It has initiated a rethink about the West's capacity to replenish weapons stocks, much of which have been depleted to support Ukraine.*

*Russia's blockade of Ukraine's coast has brought home the global impact of the war. The Kremlin has not just weaponised food supplies but a far wider supply chain impacting on the plastics industry and microprocessor production to name two. The Kremlin will continue to exploit this to undermine the West's unity and pressure concessions over sanctions.*

*Evidence continues to emerge of an extensive Russian cyber campaign against Ukraine in the months running up to as well as during the invasion, with wiper malware, defacements and DDOS attacks prominent. Recorded Future (our TI partner) observed that of the nine wiperware attacks so far identified only two masqueraded as ransomware. The Russian special services have targeted Ukrainian organisations primarily through phishing campaigns rather than software vulnerabilities in order to maintain control and avoid 'spill-over' which could impact on the West. There remains no information to suggest that the Russian services are targeting UK organisations for an attack. Ransomware remains the main threat to British businesses.*

Threat to UK business:




**Tactical Updates**

Various reports indicate continued Phishing operations via reconnaissance campaigns of the Russian nation state-sponsored "Turla Group", that targeted the NATO platform Austrian Economic Chamber, as well as the Baltic Defence College.

**Sekoia** provided follow-up information published by Google on May 3rd, after Google observed two Turla domains observed in campaigns. Sekoia reports the destination IP addresses do not permit further investigation, however the IP addresses can be linked through Shodan services to new domains, which are of a Typosquatting nature. These domains host a malicious word document titled "War Bulletin April 27, 19:00 CET". This document pulls a .PNG file when obtained and contains no macros, indicating the intention is to track downloads of the PNG. Users should be wary of unsolicited emails and refrain from downloading files from unknown sources.

## Recommendations Guide

| NCSC Recommendation | Corresponding Reliance acsn Service |
|---|---|
| Check your system patching | *Internal and External Penetration Testing* |
| Verify access controls | *Internal Penetration Testing/ PAM* |
| Ensure defences are working | *Internal Penetration Testing/ PAM* |
| Logging and monitoring | *Managed Detection and Response* |
| Review your backups | *Assurance Services* |
| Incident plan | *Assurance & Incident Response* |
| Check your internet footprint | *Penetration Testing* |
| Phishing response | *Penetration Testing* |
| Third party access | *Penetration Testing/ Assurance/ PAM* |
| Brief your wider organisation | *Assurance & vCISO* |

Relianceacsn
Your Cyber Security Partner