Reliance acsn – Ukraine Crisis Update

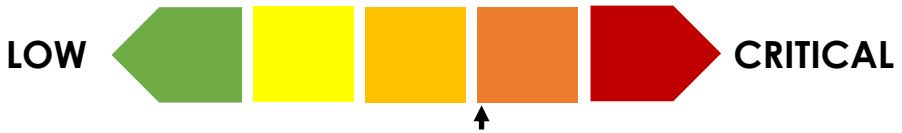
Strategic Assessment

The battles for Severodonetsk continues, inflicting significant losses on both sides. The Russian military's concentration of forces makes the city's capture an imperative. However, since our last sitrep, Ukrainian forces have managed to push back their opponents whose offensive may be running out of steam. Russian artillery heavily outnumbers the Ukrainian military and continues to pummel Ukrainian positions but it remains to be seen whether it has sufficient numbers in terms of infantry to take and hold territory.

The disruption of food supplies continues to present a real challenge to the international community. The impact of Western embargoes is being felt in Russia and is also impacting on supply chains globally. This is likely to impact companies beyond the specific theatre of war, particularly but not exclusively in Europe.

Russian and Ukrainian cyber forces continue to mount attacks against each other's infrastructure as part of the overall campaign. The actions of autonomous hackers, particularly acting against Russia, remains a concern for Western governments, as these actions risk being misinterpreted as carried out by a state. In the information war, the Russian special services are continuing to carry out a sophisticated campaign targeted at audiences in Africa, Asia and Latin America. There remains no information however to suggest that the Russian special services are targeting UK businesses directly. Online fraud and ransomware continue to pose the major threat to most organisations in the UK.

Threat to UK business:



Tactical Updates

Malspam Warning of "Chemical Attack" Spreading Infostealer in Ukraine

On May 7, 2022, the Computer Emergency Response Team of Ukraine (CERT-UA) warned of a mass distribution of emails in Ukraine with the theme "chemical attack", which are spreading Jester Stealer, an infostealer malware capable of large amounts of data theft. The emails do not contain requests for passwords or logins but contain a link to an Excel document with malicious macros. Jester Stealer exfiltrates the data from various applications such as browsers, VPN clients, passwords managers, chat messengers, email clients, crypto wallets, and gaming software. The exfiltrated data will be then uploaded to the Tor servers or Telegram bots, but if the upload fails it will then go to the anonymous file sharing platform (AnonFiles). In addition, the malware can also take screenshots and steal system information. The stealer also has the capability of deleting itself from the victim's machine to minimize the chances of detection after the exfiltration of data.

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