# RUSSIAN CYBER SHRAPNEL?

BEYOND blue
NEWSLETTER
April 2022

In this month's newsletter, we look back over the cyber activity we've seen in the first month of the invasion of Ukraine. In particular, we reflect on Russia's extensive use of wiper malware and what all of this means for organisations in the West. We also look at Samsung's recent cyber woes, consider the unique challenges posed by ransomware attacks, and reflect on best practice for board-level engagement for Operational Resilience programmes.

**David Ferbrache, OBE**
Managing Director

Expectedly, the invasion of Ukraine by Russia on the 24th of February has been accompanied by a burst of related cyber activity. Beginning in mid-January, the Russians launched their first of many three-pronged assaults on Ukraine from the cyber domain. This approach involved utilising a combination of the following:

- large **DDoS attacks** against key Ukrainian civilian and military websites and networked services,
- **wiper malware** (disguised as ransomware) designed to overwrite the Master Boot Record (MBR) on the systems of key government entities and financial institutions to render them inoperable,
- the **dissemination of disinformation** often through the **defacement of government websites**.

All three techniques are familiar parts of the Russian cyber playbook. However, the widespread use of wiper malware and pseudoransomware is notable. Open-source threat intelligence has thus far registered the existence and deployment of five distinct Russian wiper malwares since January: WhisperGate, HermeticWiper, FoxBlade, IsaacWiper, and CaddyWiper. When considered alongside the scale of their deployment, this variety of different wipers suggests that Russian actors intended these tools to do a lot of heavy lifting.

As the crisis in Ukraine develops, we now see growing evidence of the attempted deployment of such malware as part of more targeted campaigns to paralyse operators of Ukrainian critical infrastructure. Such targeted cyber campaigns are far from simple, requiring advanced capabilities, and necessitating years of reconnaissance and planning. It is difficult to lift the veil on Russian activity to discern the scale and extent of preparation, although the Ukraine has attracted high levels of attention from threat groups alleged to be linked to Russian intelligence, most notably the GRU.

The attack on the Ukrainian power grid in December 2015 was highly disruptive leaving more than 230,000 residents of Ivano-Frankivsk in the dark, but was itself eclipsed in sophistication by the malware deployed in an attack against the Pivnichna substation outside Kiev in December 2016. We have also seen cyber espionage campaigns using malware such as VPNfilter since 2018, aimed at establishing access to communications infrastructure serving a range of purposes.

Nevertheless, we have yet to see large scale disruption of Ukrainian digital infrastructure, in the context of the current crisis, posing the question why not?

There are a few plausible explanations. One is that Russian cyber troops were caught off-guard for the Kremlin's escalation from brinkmanship at the border to all-out war. This could have meant that any nascent cyber battle plans for targeting infrastructure targets were not ready for deployment.

This could also explain the heavy deployment of wiper malware. Wipers taken by themselves are blunt instruments, but also highly destructive. Finding themselves short of any battle-ready tactics for targeting infrastructure sites, Russian cyber troops may have chosen to adopt a scorched earth approach.

A second, and perhaps more intriguing, answer comes in the snippets emerging around US action to bolster Ukrainian cyber defences in the run up to invasion. The April 5th testimony to the Senate Armed Services Committee by General Paul Nakasone hints at the scale of such activity with US Cyber Command providing hunt teams, intelligence and analysis capability.

A final explanation is simpler, when it comes to targeted strikes against critical infrastructure in conflict zones, traditional munitions remain a far simpler and more effective means of achieving one's objectives. It is notable that Russian forces chose to neutralise a major television tower in Kyiv via airstrike rather than via cyber-attack. For those sceptical of the very idea of cyber war, this explanation will no doubt seem compelling.

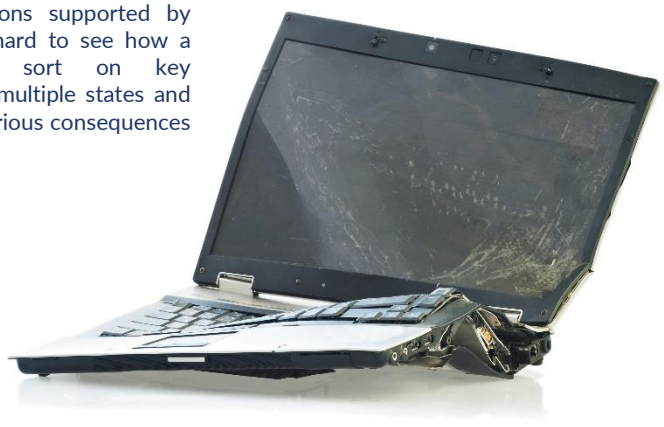
Whatever explanation we settle upon, some might be tempted to breathe a sigh of relief, and assume that Russian cyber power seem much lower than initially predicted. This would be a mistake. Western organisations cannot afford to be complacent.

The main source of elevated cyber risks from this conflict has always been the potential that there will be spill over effects, i.e., that western firms will be hit by "cyber shrapnel". This holds now more than ever. The spread of NotPetya pseudoransomware in 2017 beyond the borders of its target was an unintended consequence of supply chain dependencies of western firms on Ukrainian subsidiaries.

Moreover, there are other risks of spill over effects aside from those associated with wipers. In the early morning of February 24th, just as the first missiles began to hit the cities Kyiv, Kharkiv, and Odessa, tens of thousands of satellite modems across Europe ceased to function. The modems which were part of Viasat's KA-SAT network are widely suspected to have been taken offline by a targeted Russian cyber-attack. The strategic significance of this outage lies in the fact that Ukrainian military forces depend on the use of satellite communications supported by these modems. It's not hard to see how a cyber-attack of this sort on key infrastructure shared by multiple states and enterprises could have serious consequences beyond the battlefield.

Finally, there can be little doubt that the risks of a targeted attack by Russian cyber operatives on some non-Ukrainian western targets is grow-ing ever more likely. In the wake of imposing broad, swingeing sanctions on Russia along with its allies, the White House issued a sombre warning to private sector companies operating critical infrastructure on March 21st. In it, they cite 'evolving intelligence that the Russian Government is exploring options for potential cyberattacks'. As sanctions against Russia ensure its effective removal from the global financial system, Russia perhaps has less to lose by attacking the vital digital infrastructure supporting that system than it has ever before. Equally, the alignment of activist and organized crime interests (such as Conti) with the Russian state further increases the risk of escalation and complexities of managing de-escalation in this messy and ill-defined cyber battle.

Western organisations cannot hope to get a complete overview of this complex and increasingly volatile risk landscape. Supply chain dependencies are increasingly convoluted and global as are the digital networks on which they depend. Geopolitical events such as the war in Ukraine highlight just how important it is to shore up organisational resilience.



# SECURITY SPOTLIGHT

***Samsung has had a bad few weeks***. First, it was revealed in late February that they supplied and shipped an estimated 100 million smartphones with flawed encryption, spanning from the Galaxy S8 in 2017 to the Galaxy S21 in 2021. Researchers from Tel Aviv University found the weakness, which is linked to how certain Galaxy smartphones store cryptographic keys in the ARM TrustZone system. Attackers were able to steal the devices' hardware-based cryptographic keys and access to security-critical data. Cyber attackers could even downgrade a device's security protocols. These flaws have subsequently been addressed in various CVEs (CVE-2021-25490). The flaw has far-reaching ramifications for users. An attacker might use the issue to get access to sensitive data that would typically be encrypted, such as passwords and other credentials stored on a device. Researchers from Tel Aviv University used the flaw to get around hardware-based two-factor authentication. Android users who own one of the impacted devices have been warned to update their devices immediately.

To make matters worse, Samsung also acknowledged at the beginning of March that a group known as Lapsus$ had successfully obtained sensitive business information and source code for Galaxy smartphones. Lapsus$, which previously attacked Nvidia, posted a torrent file to its Telegram account, claiming it held the stolen data. According to cyber-security news website Security Affairs, which also released a snapshot of the data, the files contained information from both Samsung and one of its suppliers, Qualcomm. Samsung has insisted that it does not see any significant impacts as of yet but there is no official response outlining the impacts on the company and customers. If the breach is severe, Samsung may be compelled to rework its source code, impacting millions of Samsung products on the market.

## JODIE NEVIN ON RANSOMWARE PAYMENTS

***82% of UK firms paid a ransomware demand in 2021 according to security researchers Proofpoint, with 58% being the global average.*** I have first-hand experience of supporting victims of ransomware in my previous job in the police Cyber Crime unit. I've seen the chaos and destruction that these attacks have on their victims. Whether I agree with making the payments is another thing, but an organisation's first priority is to halt the attack and get back on their feet to continue operating as soon as possible.

Law enforcement strongly advise not to pay the ransom that the cyber criminals are demanding. There is no guarantee you will regain access to systems. Moreover, the data and payments will likely fund the actors to commit further attacks. Several do decide to pay due to potential impacts to business operations, finances, and reputation. Most notably, JBS Foods and Colonial Pipeline paid up in order to get their systems working again. In this case, it is vital to ask for proof of life from the actors to prove they can decrypt the data and systems. Without this guarantee, you could end up both out of pocket and without your business-critical data.

Ransomware attacks and their significant financial threat to organisations have contributed to a growing investment in cyber insurance policies. This can help offset the financial risk and manage the incident. But this alone is not enough. Actors are increasingly adopting double and triple extortion methods, stealing business critical or sensitive data and even contacting customers to make them aware of the attack. Whatever approach you adopt, it is vital you ensure that there is an established policy in place in advance of any attacks. In the face of this continuing ransomware threat, organisations must be proactive and adopt a multi-layered approach.

I'm often asked "What's the point in reporting a cyber crime?" The simple answer is that the information you provide will be vital in helping law enforcement to tackle crimes under the Computer Misuse Act. The intelligence and analysis of the attack shared may be the last piece in the puzzle to identify a threat actor and is the crucial tool in combatting cyber crime. In supporting this public good, you are helping to ensure that we are all safer and more resilient.

**JODIE NEVIN**
**SENIOR CONSULTANT**

*Jodie is a driven cyber security professional with extensive experience in the public and private sector. Before joining Beyond Blue, Jodie worked as Information Security Training Consultant for BUPA and spent several years working on cyber crime law enforcement.*

# OPERATIONAL RESILIENCE


## BOARD LEVEL ENGAGEMENT

The first cycle of self-assessment under the UK financial sector's operational resilience regulations has now come to a close. Boards have been asked to **take ownership** of their submissions to the regulators and have found themselves having to engage on the topic of resilience as they contemplate important business services, impact tolerances and scenario testing outputs offering a holistic view of their firm's resilience for the first time.

Concerns over highly disruptive cyber attacks, including of course ransomware, have re-emerged. Supply chain issues are once again on the radar with concerns over systemically important third parties, and discussions have turned to community wide resilience measures which might allow a crippled financial institution to restore service. The regulations have forced discussions on reducing harm to customers, and reinforced the need for preparedness to deal with major disruptive events. **An outcome I am sure they intended.**

Questions are being raised over the scale of investment needed to meet impact tolerances, and whether this can actually be achieved in the case of legacy systems or whether success depends on new and more resilient architectures – **but will they be in place by 2025?**