KCS Group Europe

The growing cyber threat: *Inter arma…*

July 2022

The Russian invasion of Ukraine brought the reality of war back to Europe in a manner not seen since the Bosnian civil conflict of the 1990s, and reawakened fears of a continental war thought dormant since the collapse of the Soviet Union. But, perhaps, it is more precise to say that these concerns apply only to physical manifestations of conflict. Just as there is a school of thought suggesting that the Cold War never truly ended, it just went into deep-freeze, there is an equally compelling argument to be made that Russia and China have long been waging a cyber-war against the Western world; and that for all the horror of the devastation of Ukraine, and the fear of this spreading across Eastern Europe, it is from the cyber-realm that the greatest existential threat to security comes.

Since the invasion of Ukraine began on 24 February 2022, Russian cyber-attacks against the country have included targeting the *Kyiv Post*, the satellite network, government departments, major banks, and telecoms & utility infrastructure: in other words, designed to cause societal and economic damage to Ukraine, regardless of the victim, while the military assaults were ongoing. But nations both European and worldwide have also seen an upswing in attacks: the ransomware groups Conti, BlackCat, Lockbit and REvil, have all surged in activity since the start of the war, all are closely tied to the Russian state, and not all are based within Russia's borders (for instance, REvil has a substantial dark web presence in Sweden). Partially, this is a consequence of the professionalisation of cyber-crime by organised criminal groups and state actors alike, utilising cyber capabilities on a more considered basis to target information and/or finances and seeing 'cyber' as effectively, an arm of state policy. But it is also part of the fallout of the war happening at all: with hackers taking advantage of desires to learn more, or make charitable donations, in pushing victims to fraudulent webpages and the like, or through bad actors looking to get 'in the middle of' new deals, and suppliers being thrown together at short notice after the expulsion of Russia from the Western world's contact book. Either way, corporates are at risk – no matter the sector, no matter the location.

Nations are equal-opportunity targets

The latest significant breach, at the time of writing, occurred at Albania's National Agency for Information Security (AKSHI) which was subjected to a Distributed Denial of Service attack that limited access to government-driven internet- and public-services. Romania was previously attacked via the same methodology, this time targeting the Ministry of Defence, the railway infrastructure, and the OTP Bank, with Russian hacker group, Killnet, claiming responsibility and asserting that 'any countries supporting Ukraine will be a target'. Estonia has seen an upswing in Russian-speaking bank frauds. Italy has seen multiple ransomware attacks on government, infrastructure, and corporate targets, and serves as uncomfortable proof of the reality of the situation: the University of Pisa refused to pay a ransom and now the personal data of staff and students is being sold on the Russian black market for one million Euros, with the group responsible stating that they wanted to target NATO countries (but crucially were easy on which bodies should suffer within those NATO countries, unless the University of Pisa is a cover for hosting black-ops training for Ukrainians). And even nations further afield have been struck, with Costa Rica stating itself to be 'at war' with Russian cyber-attackers, particularly over multiple compromises by the Conti ransomware group, which has put the hackers in profit to the tune of $2.7bn USD, in just two years.

Meanwhile, recent breaches in the UK have been focused on the corporate sector, with the ferry operator Wightlink being attacked by unknown bad actors, and the Scottish Association of Mental Health suffering a shutdown of all systems and technical-based services, with data then appearing on the dark web. While it has not been proven that Russian actors were behind either breach, in some respects, it hardly matters: the Ukrainian conflict has set the tone for a 'free for all' approach to cyber breaches, in the knowledge that it provides both the cover and the motivation for all manner of attacks, whether these originate from Russia or not.

The legal sector

It can be argued that the legal sector is in the first rank of tempting targets for any hacker, anywhere. They are in that 'sweet spot' of having important clients who tend to have a lot they would like to keep secret (the information imperative), and a lot of partners who charge very high fees (the financial imperative). Within the USA, there is a growing trend of legal firms being breached by ransomware and then blackmailed for the return of their sensitive data, precisely because they have such large quantities of both. At least one major legal breach per month has been reported between April and July of this year: at Richardson & Pullen, Horwitz Law, Nelsons Law and Podhurst Orseck. All these were the work of just one Russian hacking group, BlackCat.

As far as the UK goes, there remains the culture of *omerta* of talking openly about compromises in the legal sector. However, a rare investigation into the matter, in the form of a Solicitors Regulation Authority report, revealed that out of an investigation of 40 firms, 30 had suffered a cyber-attack and fully 23 had been purposefully and directly targeted either for their client secrets, or their finances, with a collective £4m GBP being lost. The report concluded by acknowledging that 'security is not often at the top of the priority list for legal practices'. This was two years ago. Nothing suggests that the situation has improved in the intervening years.

The biggest touchstone in recent years is the 2017 attack on DLA Piper using the EternalBlue ransomware; and the continuing assertions from that firm that no sensitive data was stolen, does not diminish the severity of the attack, and neither does the fact that nothing has been reported on the same scale since. Hackers do not necessarily need to go for the 'big beasts' to be successful, and once it has been proven that a system can be penetrated, they will simply bide their time or evolve their strategy until they get what they want. Plenty of comparatively 'smaller' incidents can still have a major impact.

In March 2022, Tuckers Solicitors was fined £98,000 GBP after sensitive data was stolen and sold on the dark web, given that it failed to apply a security patch for five months and thus left the door open for hackers, and the Ince Group was forced to seek an injunction preventing disclosure of data after its sensitive information was ransomed. In April, cyber-criminals attempted to blackmail Ward Hadaway for $6m USD after stealing sensitive data. And the Bar Council itself was targeted, which – while it does not appear to have resulted in any data loss – meant that the Council had to turn off its entire IT system, thereby being forced to choose disruption regardless of whether they were actually compromised or not.

Such attacks may have nothing to do with the Russian situation but prove that the threat to legal firms is very real regardless. And now that the climate is conducive to both rising attacks and their severity, the threat is only going to rise.

Tactics and targets

Currently, three main groupings of cyber breaching can be identified. Denial of service attacks, whereby key websites of governments and firms are overloaded with Internet traffic to render them unusable (which typically act as distractions from other more insidious attacks), ransomware to steal and lock data for financial recompense or as theft for its own sake, and phishing to capitalise on information on, or appeals due to, the conflict.

It is debatable whether the concept of 'low-hanging fruit' – those firms (in whichever sectors) with comparatively less protection than others that are thus riper for targeting – still holds true. Russia has made it quite clear through its state-sponsored hackers that any business working in Ukraine, or even residing in a NATO country, is fair game, and it is not as if the Russian state needs to worry about temporal or monetary concerns in choosing who it goes after. There are three broad categories of hack, and the Russians enjoy all of them: targeting corporate institutions for money, government bodies for information or to prove a political point, or (to be fair) anyone at all simply to cause disruption for disruption's sake. Therefore, the old attitudes are falling. Think you have nothing of value? All information is of value to someone. Think you are well prepared? There is a big difference going up against lone-wolf hackers compared to the Russian state. Think it wouldn't happen to you? In a climate of war, anyone and everything is arguably fair game.

Why isn't action being taken?

We have written before about the arrogance, ignorance, and greed of corporates with regards to ignoring due diligence or other standard intelligence-based practices. While greed may be less of an issue here – unless it be the greed of an IT department to take all the credit for things that go right – arrogance and ignorance are certainly major factors. Arrogance in that some think they know best in their kingdom and object to any attempt to provide help or offer greater clarity; and ignorance in not bothering to remain aware of the full nature and extent of the evolving cyber-threat. Partially, the scale of the problem is not known as those that are affected are attempting to 'keep it quiet' as much as is practically and legally possible, for fear of reputational damage or even assorted criminal charges from customers/clients caught up in any breach. Therefore, it may seem on the surface as though the problem is not as bad as it actually is. While it is acknowledged that the public impact is lessened if firms do not have a clear picture of exactly who is being targeted, and in which ways, simply putting one's head in the sand and ignoring what you do know – or have the capacity to find out – is never the answer.

Certainly, IT departments do not often have the full range of tools, or knowledge, to properly tackle the threat. Partially this is not their fault. For instance, zero-day vulnerabilities – brand-new means of attack that are unknown to antivirus software or security signature tools – are extremely difficult to detect until they have already done their damage (and for what it is worth, China is currently the world-leader in deploying these through its state-sponsored actors). If you don't know the threat is out there, you can't adequately defend against it – but it then becomes more important to proactively monitor and audit to make sure that you can deal with everything else. Alternatively, with specific reference to the greater threat posed by Russia, matters are complicated by the opacity of cyber-attacks in that it is not always absolutely

clear where they come from (as opposed to an invasion, where it is typically obvious which country is invading you).

Russian state-sponsored groups are known to operate out of Moldova, Sweden, and Albania, to name but three, and Virtual Private Networks complicate things further. All because an attack does not undeniably originate from Russia, does not mean that Russia is not the ultimate arbiter of it. The state-sponsored threat has to be considered at the highest level as a matter of course.

But these are arguments for more help, not less. Certainly, internal IT security teams are becoming aware of the broader array of capabilities that can be employed to identify and mitigate the cyber-threat, ranging from monitoring programs and enrolment in SOCs, to regular external penetration testing and 'red teaming', aimed at gauging in blunt terms how successful an attack would be at any given time. The three problems are: firstly, one of attitude (as described above), secondly, whether any such measures will be enough to survive a 'war footing' - and lastly, whether these two can be reconciled. Vulnerabilities will only be exacerbated as the capabilities and intentions of hackers are increased; and while the current surge of malware is not being evidentially directed at legal firms over and above any other sector at present, the increased commercial activity in multiple competitive sectors, not to mention the ongoing difficulty of extricating clients from agreements with out-of-favour Russian partners (or making sure that any new deals do not include the same), means that the legal sector needs to adopt a footing of permanent pro-activity and scrutiny; and if that means accepting that there are some things better done by outside assistance, and acknowledging the current failings in reporting and discussing the issues within the sector, then that is what must be done. In times of war, the laws may fall silent, but there is no excuse for legal firms to do the same.