KCS Group Europe

No Mr Bond, I Expect You to Pay!

17 June 2021

In Ian Fleming's *Goldfinger*, the titular villain bemoans that his chosen area of art has been overlooked. *"Man has achieved miracles in every human endeavour… except crime!"*. In order to rectify this, and prove himself an artist, he plans to rob Fort Knox (spoiler alert: it does not work). But in the film version, Goldfinger's plan had an added edge: he would irradiate Fort Knox's gold supply on behalf of the Chinese government, thus essentially carrying out an economic 'hit' against the US. Were Goldfinger around today, there would be no need to bother with the messy business of a dirty bomb – he would simply ransomware the Federal Reserve to its knees. Such a measure would be entirely unremarkable: the artistry of crime remains a fallacy, but its professionalisation cannot be in doubt.

A leading speech by GCHQ's head of cyber-crime, Lindy Cameron, has reiterated that ransomware remains the biggest single cyber threat to the UK. Private individuals, corporations, and government bodies alike are all at risk from this particularly malicious, and pernicious, cyber-threat. Ransomware ticks a number of boxes for the bad actors: it is relatively low-cost (as the code can cost a few hundred dollars at most), is not resource-intensive (one computer and a few cryptocurrency lockers are all you need) and performs such a specific task that the victims are often faced with having to comply (businesses and governments in particular often cannot function without their data). Moreover, it offers a laundry list to criminals of exactly which bodies are willing to pay the ransom, and which are not – crucial when deciding where to make their next move. If you already know which firm is happy to pay the millions, and which was weak enough to be compromised the first time around, pulling the same trick twice is an obvious move.

The above reasons indicate how ransomware can be so devastatingly effective for those that use it. In terms of why it has become the predominant form of cyber-threat, there are a few contextual factors in the wider world. First (as with everything) the coronavirus pandemic: with moves to mass remote-working, reliance on technology and disassociation from a central group, there are both more opportunities to enact ransomware attacks, and a greater chance that they will be successful, as remote workers may not have the immediate 'network' around them to verify the veracity of a potentially compromising email and so on.

But second are the motivations of the bad actors themselves, who are broadly split into Organised Criminal Gangs and government-sponsored perpetrators – albeit that there is a significant degree of crossover between the two. For the organised gangs, ransomware attacks do become a truly 'professionalised' service, scouting their targets and operating a minimum-risk, maximum-reward policy. Given that it is extremely difficult to find the ultimate authors of the ransomware frauds, the OCGs have an insurance policy of practical anonymity, and in any case can operate virtually round-the-clock in an intensive program of compromise. Meanwhile, states can give bad actors free reign to operate, if they do nothing against their domestic government – and indeed can even be used to target sensitive corporations or institutions (utility companies, banks and so on) that have an underlying political or soft power edge, but which gives the host government plausible deniability. The recent G7 summit singled out Russia as a particular plague upon this house, indicating that in certain quarters, ransomware might not just be professionalised, but policy.

Cameron has called for the UK government to enact a raft of tougher measures, not least illegalising the payment of ransoms (still permitted) which only serves to encourage the bad actors and implementing further cyber resilience measures against the professionalised threat. But as always, the last line of defence, and the first line of response, needs to come from companies themselves, to take a pro-active and educational approach to identifying ransomware threats, and preventing them taking effect. Losing thousands of pounds or sensitive data is, after all, liable to leave you shaken and stirred.