KCS Group Europe

Desert RATS: cybercrime in the Middle East

02/11/2017

As the Middle East becomes the world's pre-eminent business destination and a financial powerhouse, bad actors are equally shifting their attention to exploiting the region and taking advantage of lapses in security. Any effort to preserve the security of the region must be met with as much inward defence as outward planning.

Much of the Gulf Cooperation Council's blueprint for the future is built upon digital transformation – utilising the growing capabilities and spread of the Internet and wider technology to effect positive changes in society. 76% of the combined population is online, but concerted efforts are underway to move the GCC from an overall *'consumer'* to *'creator'.*

This domestic upsurge in the use and application of technology is matched by the adoption of the Middle East as a new major business and financial destination for companies worldwide, with the Emirates in particular being singled out. It is estimated that by 2025, the Middle Eastern *'online market'* will see 160 million unique users and contribute $95 billion to the combined economies. The marriage of digitisation and internationalism is thus set to pay dividends but given the degree to which this relies on technology, could see dire consequences if things go wrong.

Governments must do more – and share more

One would expect such a venture to be met by equal *'preparedness'* for the dark side of cyber, but curiously this is somewhat lacking. For instance, coordination is next to impossible as not only do neighbouring states have differing definitions of terms such as *'cybercrime'*, there is no region-wide approach that sees states working in concert rather than all just playing at the same time, and implementation of standards across all countries has been patchy at best.

Nobody can accuse the GCC states of not investing in cyber-security but, at a time when levels of cyber-threat are the biggest they have ever been, the current state of affairs is insufficient.

Desert RATS: cybercrime in the Middle East

Clearly a stronger governmental framework is needed, one that pushes co-operation to the fore, and a more formalised and stronger (in terms of both wording and consequence) delineation of what constitutes various types of cyber-crime and how this is to be tackled.

Most users in the region remain unaware they have been targeted with malware or that their computers have been hit with remote access Trojans – and cybercrime is rising year on year. According to a PWC report of last year, 30% of Middle Eastern companies have been hit but only 33% have a cyber response plan – and less than half of boards are involved in setting cyber-readiness. Words are not quite being backed up by action.

Cyber technology easily exploited as a geopolitical weapon

The 2012 Saudi Aramco incident hangs heavy over any discussion of Middle Eastern cyber-crime. In the space of less than six hours, the biggest and most valuable company on Earth was electronically crippled, unable to operate and reduced to using typewriters. What started with the clicking of a bad link ended five months later with Aramco's reputation damaged, three-quarters of data lost, large quantities of oil being given away for free simply to keep flows going, and the fear that – given responsibility and motive were never 100% established, although most fingers pointed towards Iran – this could easily happen again. (Indeed, the particular virus behind this, named Shamoon, was used in another attack in January 2017).

This demonstrates at a stroke the degree to which critical infrastructure can be harmed by even the simplest mistake and an example of how consequences of said mistake can spiral out of control. Moreover, in a region already riven by political and military struggle, it represented a genuine turning point: of escalation and evolution in a new form of warfare. Even though Iran's centrifuges had been almost wiped out by Stuxnet back in 2010 that was strictly political. The taking down of Aramco is something more: certainly a political act in terms of Iran vs. Saudi Arabia, but something else: proof positive that a company, no matter how big or bulletproof, is not untouchable.

Varying attack vectors mean that *'hacking'* is sometimes a misnomer

The traditional image of computer compromise is one of a *'basement hacker'* forcibly gaining entry to a system and manually having to place viruses and issue commands. This is not true and focus on such a criminal alone can be damaging. Much more common these days (as seen with Shamoon) is for an insider to accidentally (or otherwise) trigger a virus through their own actions. Firewalls and other security measures can be passed very easily in this way – there is no actual *'hacking'* involved. Bad actors are also becoming far more discriminatory in who they target, and how – no more emails from Nigerian princes

on the run with $200m, more likely a faked email from your *'boss'* regarding an urgent transfer of money that is at once more plausible and compelling.

Identity theft across the Middle East is on the rise. Although precise and recent figures are not always available, there was a noticeable 200% rise between 2011 and 2013 in the number of reported cases in Dubai alone, and nothing suggests the number has not risen since then. Again, identity theft can be conducted online with little to no actual *'hacking'* – thorough review of social media, online *'honey traps'* (to which Middle Easterners may be more at risk from, given the social sensibilities of the region) and so on.

In such cases the victim may not be aware that their identity or security has been compromised until it is too late, and insurance companies have to date shown themselves highly unwilling to pay out on issues of *'fakery'.*

An enabling and enticing environment

The Middle East represents the perfect environment for cyber-crime for multiple reasons. First among them is the region's proven willingness to adapt and adopt to new cyber and digital technologies as part of the transformation program – the level of opportunity, both good and bad, is significant. Secondly, the traditional dependencies on oil and gas make large numbers therefore reliant on the systems that oil and gas industries require (as was the case with Shamoon).

Thirdly, the ever-increasing complexity and range of attack vectors means that people are not aware of, or cannot keep up with, what is going on. Fourth, ever since the Arab Spring was *'promoted'* so successfully on Twitter and through social media, the Middle East has become the hotbed of *'hacktivism'* aimed at toppling various regimes. Fifth, the rebirth of the Emirates and Qatar (in particular) as international business hubs has meant that the eyes of bad actors are automatically drawn to where the money is – and to the best method of getting some.

Again, figures bear out this position of the Middle East as a weighted heavy-hitter in the cyber-crime market. Not only are the raw numbers of attacks rising year-on-year, but they are also doing so in greater range and depth: 85% of business are targeted regionally compared to the 79% elsewhere in the world, and the number of companies that reported suffering over 5,000 is double: 18% to 9%.

Perhaps the biggest danger is in the targeting of Middle Eastern-critical industry, whether by state actors or private criminals – with remote access Trojans (RATS), which permit the bad actor to steal data, key log actions and externally trigger programs within a system. Such malware has been in use in the Middle

KCS Group Europe

Desert RATS: cybercrime in the Middle East

East since 2013 through the *njrat* variant, targeting the critical government, communications and energy sectors. Again, the most common vector of delivery was unintentional user error. The damage done by RATS was highly significant – file deletion, registry manipulation, remote viewing of extremely sensitive material. In a better-connected, more open and more target-rich environment as the Middle East is now becoming, RATS may very well become the norm rather than the exception.

So what to do…

Keeping up to date with the latest developments is crucial, but so too is knowing how to use them – the human edge, if you will. Better technology must combine with stronger framework and greater will to act. As the age of oil slowly comes to an end, the GCC appears to have found its future *'niche'* in offering a destination for international financial business and the *'digital economy'*. This transformation is well underway, but the true potential will not be met unless an overarching framework can be established that regulates the sector, and both public and private enterprises co-operate and take a pro-active stance in ensuring that Middle Eastern cyber-defence is of the highest standard.