New Cyber Security Threats that are Expected to Emerge this Year

February 21, 2019

Right Size Solutions is definitely no stranger to the most recent attacks on apps, software, operating systems, websites, smartphones, and everything else that hackers can use to steal data and/or demand ransoms. This is important because the most recent, scalable, and highly profitable cyber attacks are most likely to be the ones we'll see again in 2019.

For instance, one of the current biggest potential threats to watch out for are banking Trojans. Following the drop in cryptocurrency's market value, cryptojacking became less of a threat at the end of 2018 – only to make room for banking Trojans. As fiat currencies get a foothold against the looming threat of cryptocurrency, the world's banks have once again become the main targets for hackers. Banking Trojans, such as last year's Trickbot and Emotet, are viruses that hide within seemingly safe programs and applications, and once activated they allow hackers to steal banking credentials. Individuals have become targets in the past, but corporations worth billions of dollars are at even more risk. If cryptocurrency continues in the same downward direction while fiat currency maintains its somewhat stable market value, we are definitely going to see an increasing number of banking Trojans target corporations this year.

Another huge threat is the combination of malware with artificial intelligence (AI). A company called Darktrace uses AI to identify and defend against cyber attacks, and their director of threat hunting Max Heinemeyer believes that it's only a matter of time before attackers use AI to supercharge their malware and launch cyber attacks. *"What if ransomware worms or other attacks can intelligently choose, tailored to the environment, which way to move around is best?"* This is a particularly dangerous scenario because technically speaking, specialized AI algorithms can be used to supercharge Trojans, viruses, and even phishing schemes. Instead of the typical phishing emails that are now recognizable to cyber professionals and the public, AI could analyze email data to enable the creation of *smart* phishing emails that can organically insert themselves into email conversations, making them virtually indistinguishable from genuine emails.

One of the biggest digital trends of 2019 will be the increasing connectivity of smart devices and IoT technology. The supply chain in particular will become more digital dependent. While this means that more services will be streamlined, it also opens the global supply chain up to more cyber attacks. DZone listed three separate attacks in 2018 on different supply chains in order to access downstream companies. If the hackers get entry to one port, they can then

easily take data from any organization or individual connected to that supply chain. The article also notes that hackers are deliberately “planting vulnerabilities directly into the global supply of open source components.” This allows future attacks to happen much faster and be much harder to detect and avoid.

All of these threats have led to one very fine silver lining – a consistent increase in the demand for cyber security experts across all industries. Michael Brown, the CEO of Symantec (the world’s largest security software vendor) is quoted on Maryville University, saying that even in 2016 there was already an estimated shortfall of 1.5 million jobs in the industry. And unfortunately, even in the moneyed world of corporate organizations, this problematic shortage of cyber professionals continues today – with no end in sight. This was revealed in the annual industry surveys by the Enterprise Strategy Group (ESG): From 2018 to 2019, 53% of organizations surveyed reported a lack of cyber security experts. Considering the amount, variety, and the magnitude of cyber attacks happening today and in recent history, this is a definite cause for concern.

The good news is that many organizations seem to be taking these threats seriously. According to a Depository Trust and Clearing Corp. survey of 145 industry experts, 37% said that cyber security is their company’s top risk while 69% said that it was in their top five. In short, the world’s most significant industries know that they’re at risk – we can only hope that they can also do what’s necessary to mitigate the risk to themselves as well as their customers.

Article composed by **Bea Jarvis** for the exclusive use of **Rightsize-Solutions.com**