KPMG

Machine learning:

Why it should be used for early detection and prevention of ransomware

Malicious individuals exploit vulnerabilities, such as weaknesses in software from unpatched systems, to gain access to organisations and navigate through the network undetected in order to perform malicious attacks against organisations. Over the years businesses around the world have succumbed to a variety of ransomware attacks, causing the unavailability of critical business data through encryption. As a result, organisations are unable to provide their services or products which ultimately leads to the deterioration of the business. Last year, it was reported that South Africa had the third highest number of cybercrime victims of any country.[1] Worrisomely, adversaries are using ransomware to target South African national critical infrastructures and services which not only threatens public safety, but also the availability of essential services. The most recent high-profile ransomware attack paralysed the City of Johannesburg Metropolitan Municipality for almost two weeks leading to the disruption of regular operations. In this instance the ransom was not paid but Cyber professionals were hired to assist in the restoration of files and systems in order to resume business-as-usual operations, which cost the Municipality up to R50 million.[2]

With the rapid growth of new daily malware variations, traditional methods of detecting ransomware (using reactive tools such as Anti-Virus (AV) solutions) are slowly becoming obsolete and less efficient. Detecting ransomware now requires a prompt response, often faster than the capacity of the human brain, and so machine learning has become the rising star in detecting zero-day threats and combatting ransomware.[3] The power of machine learning is underpinned by security software systems that incorporate behavioural analytics and are trained to detect suspicious behaviour. Machine learning leverages off reference models that are created and tailored to each unique environment and are built by collecting a plethora of benign and malicious files (datasets), which are classified into pre-defined categories based on their features.[4] These files serve as reference points and patterns to train the model, resulting in the creation of an algorithm which accurately classifies the files and performs pre-defined actions such as deletion or sandboxing of malicious files, with minimal human intervention required. Predictive models are generated using this technique and this makes detecting both the behaviour of ransomware and its new variants possible.[5] These models are also fine-tuned frequently to stay abreast with the latest ransomware behavioural trends which will lead to greater chances of new malware being detected. By creating predictive models that will detect ransomware signatures based on heuristics and behaviour, machine learning surpasses the capabilities of its more traditional counterparts that rely on a pre-defined database.

[1] "https://www.businessinsider.co.za/sa-third-highest-number-of-cybercrime-victims-2020-6

[2] Your Money or Your Data – The Rise of Ransomware | Carte Blanche | M-Net - YouTube

[3] https://www.mimecast.com/de/blog/ai-vs.-ai-now-ai-is-required-for-your-business-cyber-resilience/

[4] A Study on the Evolution of Ransomware Detection Using Machine Learning and Deep Learning Techniques by Damien Warren Fernando, Nikos Komninos and Thomas Chen

[5] A Study on the Evolution of Ransomware Detection Using Machine Learning and Deep Learning Techniques by Damien Warren Fernando, Nikos Komninos and Thomas Chen

The rise of ransomware can have a devasting effect in South Africa's COVID-19 vaccine delivery system

In June 2020, the Life Healthcare Group hospital chain consisting of 66 hospitals in South Africa were the victims of a ransomware attack.[6] This is just one of the many examples that emphasise the attacks on healthcare providers, who are often targeted because of the Personally Identifiable Information (PII) they store and process in order to service the public. Today, this critical realisation has a huge impact on the role healthcare plays in the current COVID-19 pandemic. In the next few months it is expected that the vaccine programme will be expedited for South Africa to achieve herd immunity, just as the fourth wave descends on the country. It is therefore essential that the government proactively take steps to strengthen the security posture of the Electronic Vaccination Data System (EVDS) self-registration system which uses PII such as passport numbers, ID numbers, home addresses and medical aid information in order to register and book vaccination appointments. Without the consideration on the security of this key system, ransomware can weaken the integrity of the EVDS, cripple the vaccine rollout programme and ultimately endanger the lives of all citizens. With public trust at risk, government and local providers should take the necessary steps to gain 'cyber immunity'. Without the consideration on the security of this key system, ransomware can weaken the integrity of the EVDS, cripple the vaccine rollout programme and ultimately endanger the lives of all citizens. With public trust at risk, government and local providers should take the necessary steps to gain 'cyber immunity'.

Artificial Intelligence effectiveness in malware attack defences

While the use of Artificial Intelligence (AI) has empowered security teams with self-defending mechanisms for the early detection and prevention of malware, it may not be the silver bullet solution. AI detection solutions are relatively new and need to stand the test of time, however malware will continue to evolve and look to include its own AI element. It is inevitable that AI will disrupt the cyber threat landscape by equipping the attackers with weaponised ransomware to plot more efficient attacks whereby the speed of attacks will continue to increase to the advantage of the attacker. Fundamentally, as ransomware continues to evolve, it is crucial for organisations of all sizes to be proactive in adopting protective layers to detecting malware.

Definitions

Ransomware: A class of malware that encrypts sensitive data which is then held at ransom.

Artificial Intelligence (AI): Attempts to mimic human behaviour through analysing data and training models to think and behave in a human-like manner.

Anti-Virus tool: Anti-Virus (AV) solutions block malware signatures, rules and patterns based on past attacks or threats.

Sibahle Nhleko
Junior Analyst
KPMG South Africa

About Sibahle Nhleko:

Sibahle Nhleko is a Junior Analyst 2 in the Cyber Division based at the KPMG Durban Office. She joined KPMG in January 2020. Her role involves the assessment of technical cyber security controls across a myriad of industries which include Banking, Retail and Telecommunications as well as recommending security enhancements to clients. She has extensive experience in Penetration Testing, Vulnerability Assessment, Firewall Analysis, Industrial Control System Reviews, High Availability/Disaster Recovery Reviews, and more. She holds a Bachelor of Science (Magna cum Laude) in Computer Information Technology from Methodist University as well as a Master of Science degree (with Merit) in Cyber Security from the University of Birmingham.

[6] https://health-e.org.za/2021/01/09/cyberattackers-increasingly-target-healthcare-and-south-africa-is-not-immune/