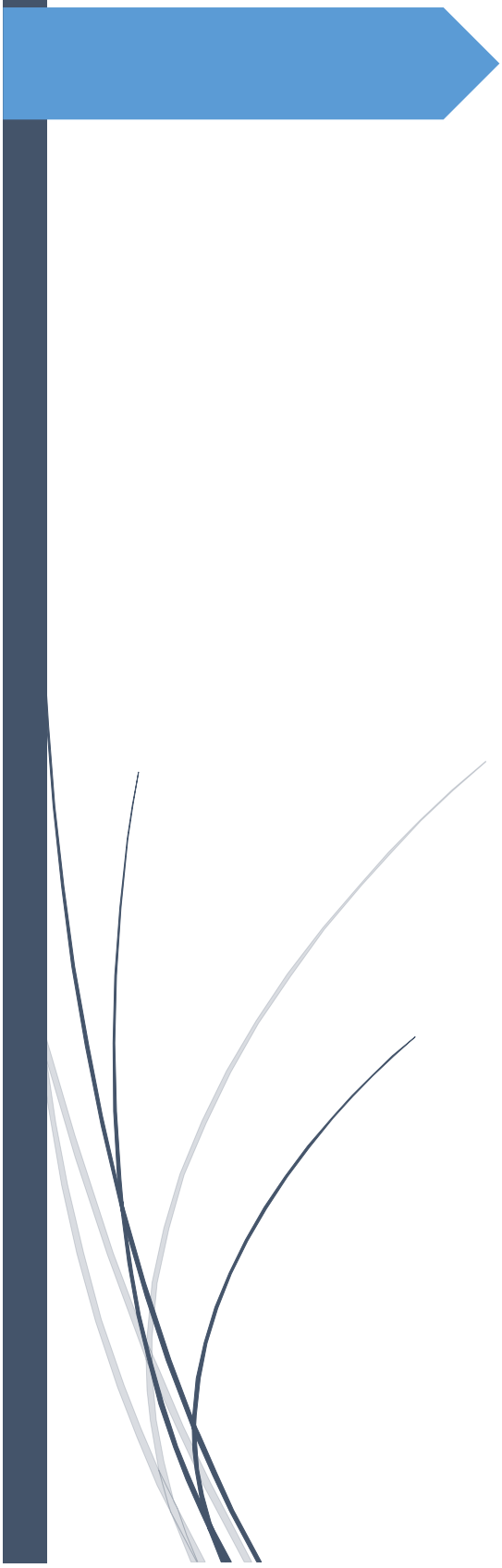
AM I OWNED

DEKENEAS NEXT-GEN TECHNOLOGIES SRL



www.dekeneas.com

AM I OWNED

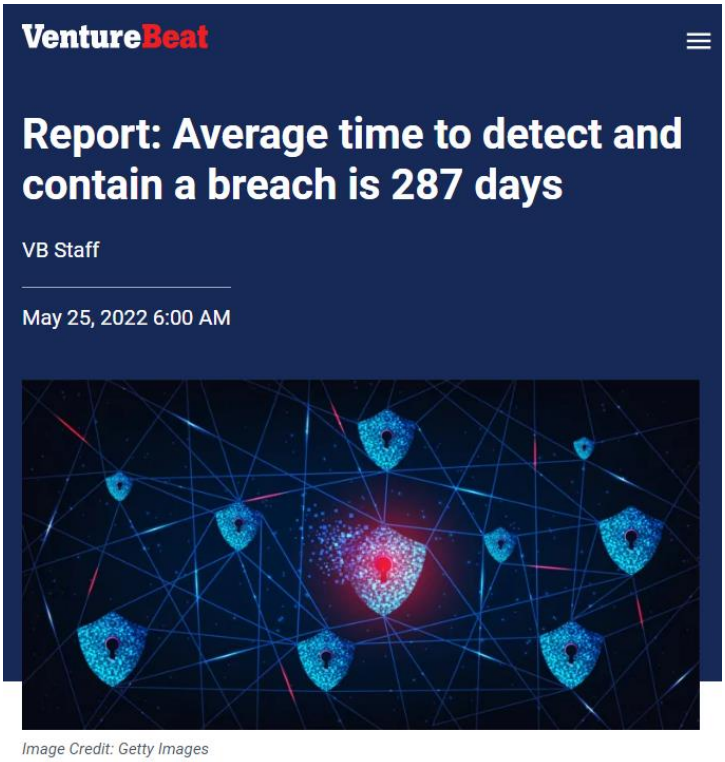


Image Credit: Getty Images

Safeguarding data is a continual process fraught with challenges and a breach in the protection of that data can have major repercussions. Detecting and reporting a breach in a timely manner is crucial to maintaining compliance standards and ensuring the integrity of an organization's data. Though many breaches are detected in a timely manner, it is an unfortunate reality that the majority of organizations take months or even years before detecting a breach. In 2019, security teams at Verizon released the Verizon Data Breach Investigations Report; an analysis of many of the year's big data breaches across organizations. A total of 41,686 security incidents were analyzed in the report, shining a light on a grim reality: While cybercriminals' first steps towards compromising customer information and data can happen in a span of minutes, the time taken to discover the breach by these malicious actors often takes months. Using the data from the analyzed incidents, Verizon's security teams determined that a total of 56 percent of breaches took months or even years to detect – a significant sample size given the enormity of cyberspace that the 41,686 analyzed sites represent. This revelation tells us of the growing level of impact a well-established system of governance can have for an organization – a system by which attacks can be properly mitigated and reported to save precious time in recovering from a breach. Blue teams regularly engage in the mission of preventing attacks from occurring but having the systems to detect a breach in progress – assuming preventative measures have failed – is just as critical to ensure the integrity of an organization's systems and the confidentiality of customer data.

Tracing the steps

Data breaches and cyber-attacks are not singular events. They are an ongoing process with multiple steps. The first step usually is infiltration, during which an attacker gains a foothold in the network. Infiltration can happen in many ways. It can come by way of targeted credential theft, exploiting vulnerable web applications, third party credential theft, malware, and more. The next step is usually reconnaissance. This is where attackers try to understand what the network architecture is, what access they have via stolen credentials, and where sensitive data is stored. Compare this to thieves breaking into a house in the middle of the night. The first thing they do is check the house's layout and determine where the valuables are being kept. Once attackers are done with basic reconnaissance, usually they will attempt lateral expansion in the network. They move within the network into a higher tier with better access, perform privilege escalation to gain permissions with wider access, acquire sensitive data, and finally exfiltrate it outside the network. These steps take weeks and months to progress,

performed via a painstaking trial-and-error process by attackers, as they strive to identify sensitive resources and expand within the network. Usually, in the case of a cyber-attack, we hear only of the first and last steps – infiltration into the network and data exfiltration. But during the steps in between, there is a whole world of activity that often goes unnoticed.

DEKENEAS NEXT-GEN TECHNOLOGIES S.R.L.
Bd. Libertatii, 20
Bucuresti, Romania

https://www.dekeneas.com
dekeneas@dekeneas.com

SCAN ME

What we do

We do not provide another network monitoring tool. These tools are known to have problems in detecting complex attacks and sometimes they even unwillingly help the attackers through security holes in their own code. While we acknowledge the importance of intrusion detection sensors and traffic monitoring instruments, we also found that most of the times, in practice this is not enough as even the best ones give a lot of false positives and "noise" traffic, making it difficult to pinpoint the malicious activities.

What we do instead is giving the attackers what they are looking for: juicy documents, user accounts and credentials, database access, etc. But with a twist.. All these resources are decoys, being specifically crafted to "call home" when accessed, just like a tripwire alarm, forcing the attacker to reveal himself before being able to mount further more dangerous attacks against the network and devices he finds, and giving the beneficiary actionable intelligence needed to counter the threat.

DEKENEAS NEXT-GEN TECHNOLOGIES S.R.L.
Bd. Libertatii, 20
Bucuresti, Romania

https://www.dekeneas.com
dekeneas@dekeneas.com

SCAN ME