VULNERABILITIES AND FAILURES OF ARTIFICIAL INTELLIGENCE IN CYBER SECURITY DEFENSES

Effectively upholding cyber security is undeniably the major challenge of every organization and country. According to Ponemon Institute, endpoint security risks are the hottest issues for organizations to handle. With damage costs of successful cyber-attack exceeding $9 million in 2019, vendors must strive to deliver new complex defense mechanisms that help organizations counter the increasing trend of differentiated attacks.

As cyber threats keep evolving by the minute, numerous vendors have turned to Artificial Intelligence (A.I.) to fortify the building blocks of their cyber security solutions. Hailed as the future of cyber defenses, A.I. has been incorporated into a range of cyber security products with the hope of providing the ultimate protection against all cyber-attacks – a universal vaccine against all maladies. By analyzing historic threat activity using algorithms powered by neural networks, researchers state A.I. can be left to train itself and thus improve malware detection.

While A.I. protection has its fair share of strengths, A.I. driven cyber protection may not be as effective as portrayed. Experts in fact are highly concerned about numerous shortcomings that instill a false sense of security in organizations. This is a question of limits, and these limitations include:

- **Limited protection against zero-day exploits and new advanced threats** (e.g. morphing malware): The base principle of A.I. is the ability to learn from past data and activity patterns, which presumes pervasive monitoring sufficient to be sure the needles *are* in the haystack. A.I. driven cyber defenses follow those same

principles; they need to be trained to learn what malware looks like and how it behaves. The dependency on historic, viz., known and identifiable, malware activity makes A.I. based protection potentially less effective in detecting zero-day exploits and new variants of malware that do not match past malware patterns on which the A.I. was trained.

- **Higher rate of false positives:** Like other cyber methods, A.I. protection mechanisms are classifiers; they classify ongoing activity by estimating how similar such patterns are to malware behavior. Classification is inherently prone to both false positives and false negatives, and a potentially high degree of fine-tuning on a company by company basis is required. Caution also needs to be practiced to avoid false positives; one might unwittingly slack heavily in the configuration, which may lead to further vulnerabilities and a false sense of security. As a result, balancing and properly setting these up may become a time-consuming, daunting and frustrating endeavor. If the A.I. is completely hands off, then it is all but certain you cannot ask why it does what it does and get an intelligible answer; it is uninterrogatable.
- **Be outsmarted by A.I. based attacks:** A.I. is inherently dual use. In a 2018 study, "The Malicious Use of Artificial Intelligence: Forecasting, Prevention and Mitigation", concern was raised about the increased use of A.I. in malware. The 26 researchers and industry experts involved in this study jointly asserted that A.I. is becoming an integral building block of sophisticated malware. This is primarily attributed to the increased automation A.I. brings and its ability to learn the behavior of A.I. defense systems. Experts predict that A.I. may eventually help attackers to more easily dupe A.I. security products by:
    - **Adaptively changing malicious activity behavior on the fly so as to go by undetected**; e.g., by displaying activity patterns not known to the A.I. or slow down its reaction
    - **Disguise as a different malware to confuse the A.I.** or trigger actions that are not effective on the real attack.
    - **Generate decoys and disseminate false behavioral patterns,** making the A.I. defense mechanisms react ineffectively to the threats. This may also generate huge volumes of false positives that hog the bandwidth with notifications. This may eventually:
        - Cripple the network and slow operations causing chaos. Chaos typically leads to misunderstandings, mistakes and rushed actions that may result in disasters.
        - Overload the IT team with alerts to analyze and process. The more alarms that flash at once, the higher the probability operators will panic and freeze. This generally leads to mistakes or slower reaction thus enabling the attack to intensify or penetrate deeper causing more damage.
        - Lead organizations to switch off or restart their A.I. defenses in an attempt to restore control, free bandwidth and stop notification

alert overload. This would make organizations more vulnerable, opening a way for attackers to deliver their payload and additional waves of malicious attacks.

- **Higher demand on resources thus effecting performance:** To have some degree of effectiveness, A.I. requires extensive data analysis operations on system logs and malware data from prior attacks. Consequently, it comes as no surprise that the learning process is resource-intensive at runtime and may necessitate higher spec hardware and network bandwidth in support of this process and to mitigate performance issues.
- **Potentially slower to achieve high degree of protection:** The dependency of A.I. to learn from the past is similar to the dependency that legacy protection systems have on signatures - without this process, these systems would be heavily under performant much like legacy systems were with outdated signatures. In a sense, A.I. is once again signatures, only more sophisticated. A.I. defense systems also need to be tweaked to adapt to the activity patterns of the network where it is deployed (to also minimize false positives and enhance detection rate), as well as a A.I. learning process that varies in duration and effort from one organization to another. Consequently, until the A.I.s training and tweaking are done, organizations that fully and solely rely on such cyber security mechanisms may become highly vulnerable to attacks and risk being exploited due to the less effective cyber protection levels. Once again, interrogatability is the principle issue.

As malware evolves, so must our defenses… and in a timely fashion. With the increased presence of new malware variants, the best method of defense is one that is not solely dependent on learning from past attacks. The problem with A.I. is that yesterday's malware behavior may already be superseded by newer variants. This lag is inherent in machine learning systems.

In their 2018 State of Endpoint Security Risk Report, Ponemon Institute states that false positive rates for existing endpoint security solutions are up to 58%. The effectiveness of A.I. protection is highly pivotal on its training and configuration. A wrongly calibrated A.I. system may inundate the network with false positives and bury your IT team in alerts. This may further slow attack countermeasures leaving your network vulnerable. Ultimately, too many false positives will tarnish the trust in a defense mechanism, and we already have more alerts than we can reasonably act upon.

In the race for the best cyber protection, vendors must also keep in mind operational overheads. Defense systems using A.I. may require increased infrastructure resources due to the historic-patterns data crunching needed during the A.I. learning process. An additional downside is that protection is not at optimum levels on deployment. This increases exploit risks unless additional budgets are spent on supplementary defense mechanisms that will hold the fort while the A.I. is learning and can complement it thereafter. It is bringing in heavier armor, which naturally requires more logistical support.

Ultimately, the right solution is one that is:

- Can be understood and thus trusted to be effective from day-one of deployment
- Measurably comprehensive in security coverage and long-term protection
- Able to notify users about the real (immediate) priorities consistent with operational capacity, i.e., without inundating them with false alerts
- Scalable yet reasonably low in resource consumption.

Introducing Digital Immunity

Digital Immunity is a deterministic, preventive cyber security solution that guarantees the integrity of trusted code in memory at runtime based on advanced activity monitoring algorithms. It stops advanced threats including Advanced Persistent (and Volatile) Threats (APT/AVTs) and zero-day attacks from occurring at the most vulnerable parts of a network: the execution pipeline on the endpoint.

Applying a patented Digital DNA Mapping and in memory protection of all executable code, the Digital Immunity endpoint protection creates an alternate digital representation of all trusted executable code and compares that to actual code executing in memory at runtime, immediately prior to its execution on the endpoint to detect and thus prevent threats other traditional solutions cannot – all this without needing lengthy A.I. malware learning process or signature downloads.

Unlike conventional endpoint protection typically deployed in organizations, Digital Immunity is NOT dependent on signature databases, nor does it require training to learn malware behavior. As a result, it uses a fraction of the system resources required for conventional A.I. defense mechanisms and it is fully effective from day one of deployment.

Through its advanced algorithms, the Digital Immunity approach prevents virtually all foreign or malicious code, even zero-day and novel strains of malware, from executing and exploiting vulnerabilities on your network. Digital Immunity is highly scalable and can be deployed to effectively protect both SMB and Enterprise infrastructures with low maintenance overheads.

Some key aspects of Digital Immunity

- **Prevent and Detect** the Execution of Malware / Ransomware – File or File-less
- **Effective immediately on day 1 of deployment –** no dependency on historic malware-data analysis, no lengthy A.I. learning process needed.
- **Active in Memory at Runtime –** when Applications are most Vulnerable
- **No Pre-Existing Knowledge** of Exploits or Vulnerabilities Needed to deploy, configure and run
- **No Dependency on signatures databases**
- **Threat Intelligence directly at your endpoints –** Full capture of forensic artifacts at point of Attack
- **Deterministically remediate** at the Endpoint, i.e. right at the source of exploit
- **Lightweight on system resources - Sensor runs** at Kernel level with no resource-demanding historic data analysis needed
- **Intelligent alert management -** notifies you of the real immediate priorities; does not inundate you with false, superfluous or repeated alerts

Sounds too good to be true? Don't just take our word for it – we invite you to take our solution for a spin! Request a Digital Immunity demo now.

Have a query? Send us an email at Info@digitalimmunity.com
Want more info? Check our Datasheet or visit our website: www.digitalimmunity.com