SOLUTION BRIEF

Communications Service Providers
Network Security

Ammune* Defense Shield Server Utilizes AI for Cyberdefense

Ammune Defense Shield is an artificial intelligence (AI)-based self-learning cyberdefense system from L7 Defense* that reacts quickly to protect against next-generation scripted or artificial intelligence (AI)-based cyberattacks. These attacks can evolve faster than humans can respond, but Ammune starts quickly and changes its defenses to match changes in the attack.

AI Brings New Cybersecurity Challenges

Today's cyberattackers are becoming more sophisticated, using automated attacks and potentially artificial intelligence (AI), to give them greater ability to penetrate a network undetected, or to shut down a network with a massively distributed denial of service (DDoS) attack.

Many industry experts say it's hard to determine if scripted DDoS, ransomware, or criminal chatbots attacks use an AI algorithm, but most believe the use of this technology has already started.[1]

The use of AI for cyberattacks gives hackers powerful new ways to penetrate networks, including:

- Nearly infinite ways to attack a single web target: AI attacks can evolve, combining hundreds of request types with typically up to 10 request parameters to make infinite variations of attacks.
- Dynamic attacks on thousands of web system targets: AI adds instantaneous feedback loops combined with the ability to immediately improve attack tactics, allowing the attack to evolve against defenses.
- Control of IoT bots: For DDoS attacks, the more bots under control, the more damage can be caused. AI allows optimization of the dynamics of these attacks against one or multiple targets in parallel.

An AI-based cyberattack can produce complex and highly targeted scripts at a rate and level of sophistication far beyond any individual human hacker. When AI attacks become popular among hackers, then every computing system in a home or enterprise becomes a target for a focused attack—from IoT-enabled refrigerators to game consoles to servers in a data center or cloud.

The sheer volume of traffic coming from an AI-based attack combined with the evolution of the attack as the algorithm learns and adapts will make it hard for humans to manually combat the attack. The industry has experimented with automated defense systems, but early systems reported too many false positives. Without human intervention to provide context and interpretation, these systems classified a high number of innocent data flows as cyberattacks.

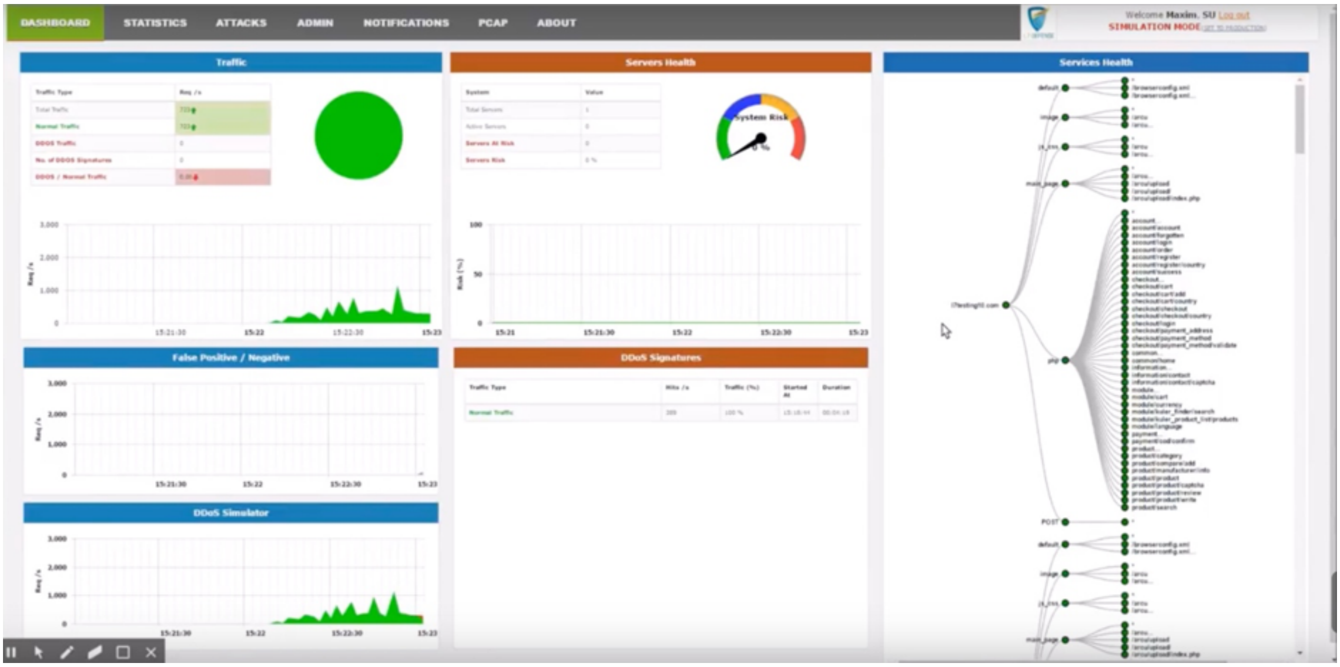
These issues should be addressed in emerging AI-based cybersecurity systems that can react much more quickly than a human initiated system. These systems also can learn during the attack in order to provide context and interpretation to better understand the right indicators of compromise, which, in turn, more correctly identify cyberattacks and cut down on false positives.

To help fight next-generation AI-driven cyberattacks, Intel® Network Builders ecosystem partner L7 Defense* has introduced its Ammune* Defense Shield Server AI cyberdefense platform that leverages the technology to embed DDoS defense capabilities in a wide range of cloud or on-premises applications.

The Solution

Ammune Defense Shield (ADS) is a virtual cybersecurity platform that helps protect web systems and servers from network (layers 3/4) and application (layer 7) DDoS attacks, as a standalone server or embedded within other systems and devices. It is based on an algorithm that can provide unsupervised learning technology so that the system is continuously scanning for DDoS attacks, and then mitigates both known and unknown attacks.

The "deploy-and-run" design of the platform means it automatically discovers the characteristics of the web system(s) it is deployed on to go into protect mode very quickly with no pre-training or rules to maintain. It then continuously monitors for changes to the web system(s) with no human intervention needed. In customer applications today, the AI technology at the heart of the solution has shown a close-to-zero rate of reported false positive mistakes as well as false negative mistakes—both during normal and attack conditions. This is due to the algorithmic core that is designed to manage these numbers as part of its operation cycle.



Traffic Type	Req /s
Total Traffic	723
Normal Traffic	723
DDOS Traffic	0
No. of DDOS Signatures	0
DDOS / Normal Traffic	0.00

System	Value
Total Servers	1
Active Servers	0
Servers At Risk	0
Servers Risk	0 %

Traffic Type	Hits /s	Traffic (%)	Started At	Duration
Normal Traffic	289	100 %	15:18:44	00:04:15

Figure 1. Ammune Defense Shield Dashboard[2]

The Ammune Defense Shield (ADS) Server virtual network function (VNF) runs on cloud- or data center-based web servers. It also is available in an embedded version that runs on a system on chip (SoC) located on a network interface controller. In this mode, the software can detect a DDoS attack just as the packets are entering the enterprise network and servers, which can mean a very fast response time, thus mitigating significant damage.

ADS can plug into a firewall and web application firewall (WAF) as well to help protect against http-based application attacks as well as layer 3/4 attacks ranging from botnet volumetric attacks to a brute force password guessing attack type. In this mode, it becomes a software blade in the firewall that manages DDoS attacks.

Ammune Is Always On

The ADS Server operates in "always on" mode while its "discovery-analysis-mitigate" process reacts as the attack initiation is recognized. As a virtual system, the ADS Server is portable and can be remotely and rapidly deployed on cloud or on-premises servers. When needed to guard against high-data-volume attacks, the software can automatically scale up by instantiating a new VNF to add more capacity as well as a load balancing function that can divide the data flows among the different VNFs.

The ADS Server can operate as a standalone system, or as part of a hybrid model utilizing the Ammune scrubbing center. The scrubbing center is a virtual system that scales elastically to absorb terabytes of attacking traffic. It will analyze the incoming traffic and match that automatically with the best company locations to absorb the data flows based on the customer. The traffic redirection and filtering process occurs automatically only while an attack is active.

Ammune Defense Shield Server Mitigation Cycle

- Sniffing: Ammune is always on, so it is always sniffing inbound and outbound traffic. Outbound sniffing is a unique feature that offers a unique way to detect DDoS attacks.
- Smart sampling: The Ammune algorithm samples less than 5 percent of the traffic that is precisely selected by the algorithm.
- Full analysis: As for layer 7 attack monitoring, the header and body of the sampled traffic is analyzed through a unique, application-aware process. Layer 3/4 attack monitoring demands no traffic decryption.
- Attack alerting: These alerts are triggered as consensus is generated between SLA disruption and traffic pattern changes—resulting in automatically generated attack signatures.
- Mitigation: Signatures are fed to a reverse proxy or to transparent inspection systems in real time and used to mitigate bad requests.

Performance of Intel® Xeon® Processors

The ADS is optimized for servers that are based on the Intel® Xeon® processor family, such as the Intel Xeon processor E5-2686 v4. The Intel Xeon processor E5 family is built on 14 nm processor technology with CPU models that feature up to 22 cores and 44 threads per socket and 55 megabytes of last-level cache (LLC) per socket for outstanding performance, as well as Intel® Transactional Synchronization Extensions (Intel® TSX) for excellent parallel workload performance.

The CPUs are optimized for next-generation software defined infrastructure (SDI) because they support efficient virtualization, smart resource allocation, and enhanced protection of systems and data.

For enhanced encryption/decryption processing, L7 Defense specifies Intel® QuickAssist Technology (Intel® QAT), which delivers hardware acceleration to assist with the performance demands of compute-intensive security and compression operations. This capability, built into the Intel® C620 series chipsets, accelerates this processing, thereby reserving processor cycles for application control processing.

Conclusion

As hackers utilize AI to ratchet up the intensity and complexity of their attacks, enterprises need to be able to respond to attacks at a speed that can only come from an automated system. The Ammune Defense Shield from L7 Defense provides these enterprises with AI-based cyber protection that can match the speed of incoming attacks, protecting their information assets against these next-generation attacks with a very high reliability and accuracy.

About L7 Defense

L7 Defense is a cybersecurity company, located in the cybersecurity area, Beer Sheva, Israel. It was founded in 2015 by an experienced team of entrepreneurs with deep knowledge and experience in marketing and sales, in enterprise architecture and the cybersecurity domain, as well as solid scientific background. L7 Defense DDoS mitigation Ammune platform is recognized among the most promising DDoS mitigation platforms 2016 by the *CIOReview** magazine. The company was also recognized as a key innovator company by MarketsandMarkets.*

About Intel® Network Builders

Intel Network Builders is an ecosystem of infrastructure, software, and technology vendors coming together with communications service providers and end users to accelerate the adoption of solutions based on network functions virtualization (NFV) and software defined networking (SDN) in telecommunications and data center networks. The program offers technical support, matchmaking, and co-marketing opportunities to help facilitate joint collaboration through to the trial and deployment of NFV and SDN solutions. Learn more at http://networkbuilders.intel.com.

[1] https://threatmatrix.cylance.com/en_us/home/black-hat-attendees-see-ai-as-double-edged-sword.html

[2] Figure provided courtesy of L7 Defense.

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No computer system can be absolutely secure. Check with your system manufacturer or retailer or learn more at intel.com.

0518/DO/H09/PDF ♻ Please Recycle 337635-001US