Ovum

Cymulate expands BAS functionality and its market reach

Publication Date: 12 Nov 2019 | Product code: INT005-000054

Rik Turner

Ovum view

Summary

Breach and attack simulation (BAS) vendor Cymulate has been expanding the scope of its platform, both in terms of the functionality offered by similar vendors and its addressable market. Halfway through this year it added the ability to simulate advanced persistent threats (APTs), shortly after it introduced the industry's first agentless APT simulation, then unveiled bundles of its technology designed for easy consumption by small and midsize businesses (SMBs) directly and/or through MSSPs and MDRs, where previously BAS had primarily targeted the large enterprise segment.

BAS is an emerging market category

BAS is a technology category that has arisen over the last half decade or so. It remains an emerging sector, with all the dozen or so vendors in the space being startups, or recently acquired startups and still privately held.

Cymulate was founded in 2016 and has so far raised a total of $26m in venture funding, most recently (November 2019) announcing a $15m Series B round led by Vertex Growth Fund. The round also sees participation from existing investing partners, including the investment arm of Vertex Ventures Israel, Dell Technologies Capital, and Susquehanna Growth Equity (SGE). Seed investment was provided by serial entrepreneur Eyal Gruner.

The company has customers in various parts of the world across all verticals and has doubled its revenue over the last 12 months.

Beyond pen testing and red teaming

BAS can be considered an evolution of the manual pen testing and red teaming services provided either by in-house teams or external security consultancies, because like these activities, it tests for misconfigurations, insecure settings, and so on, but is automated without vector-specific limitations.

Even when pen testers use automated tools, these are specific to a given attack vector, such as testing a web gateway or a web application firewall (WAF), which means they don't cover the full kill chain and usually require some scripting on the part of the user. These tools cannot therefore help to prioritize remediation, because they don't test a company's entire set of controls.

Enhancing vulnerability scanners

BAS can therefore serve as an overlay enhancement to vulnerability scanners, as well as a complement to the kind of pen testing or red teaming exercises many enterprises carry out periodically. While it does not look for vulnerabilities in the sense of CVEs, Cymulate's BAS platform integrates with vulnerability management technology to identify them, taking remediation a step further by identifying what else needs to be mitigated to reduce the attack surface. This might involve changing configurations, modifying privileges and policies, or changing settings, such as disabling macros, inspecting nested files, implementing least privilege, closing unnecessary ports, removing unused software components that can be exploited, and fine-tuning control settings relevant to each attack vector.

Simplicity of use is a differentiator

One of the main attractions of Cymulate's technology is its ease of use. Its BAS platform is cloud-based and delivered in software-as-a-service mode, with customers needing only to deploy an agent downloaded to a single, dedicated machine holding a golden image of what the customer wants to test, such as a laptop, workstation, server, or virtual machine. The image can be that of a standard employee's machine, or that of a privileged user such as a sysadmin. With its UI, Cymulate promotes ease of use and creates no business interference. Customers configure the type and frequency of the attack to be simulated, then hit a button to launch it against an entire network domain. The business model is flexible, so that customers can choose to purchase any or all of the attack vectors and modules Cymulate offers, including

- email gateway
- web gateway
- web application firewall
- phishing awareness
- endpoint security
- lateral movement
- data exfiltration
- immediate threats
- full kill-chain APT.

Email attack simulation

Attack simulation differs by vector. In the case of email gateways, for instance, the Cymulate agent is allocated a unique email address to which the cloud-based platform will send emails with malware and malicious links, testing the efficacy of security infrastructure, such as secure email gateways and sandboxes, along with checking whether controls can identify attachments' true file type, forged email senders, and other malicious features. When the agent receives an email, it performs a comparison of the email content to validate that the file that was sent from Cymulate's server is the file that arrived in the test machine's mailbox, then deletes it. It also attributes a risk score to it that is calibrated to reflect how many clicks were required to release malware, for instance, with scores aggregated into an overall total for the customer's email security.

Inbound and outbound web traffic

In the case of simulated attacks on employees' browsing activities, Cymulate tests controls for detection capabilities specific to malicious inbound traffic and those relevant for detecting malicious outbound traffic.

- For inbound traffic, Cymulate has a website specifically to deliver simulated malware to the tested system, enabling the platform to test the strength of its customers' defenses against exploits and malicious files downloaded from the web (in this case, its attack simulation servers).
- For outbound traffic, Cymulate attempts to establish a connection with malicious sites that are collected and updated from security feeds on a daily basis. In the outbound test, the agent attempts to connect to live malicious sites, serving as a proxy to prevent infection.)

Lateral movement

The lateral movement vector (the "hopper") is scenario-dependent, using numerous techniques to compromise a network. For example, if a user wants to learn (by simulation) what might happen to the organization's internal network if the CFO is compromised, a Cymulate agent should be installed on the CFO's workstation.

When launching the assessment, the following activities will be performed on a workstation:

- Discovery: At first, the hopper will try to gain knowledge about the system and internal network by scanning it for potentially reachable systems' other pertinent data.
- Credential access: The credential dumping process will then start, collected from the workstation based on common credential-dumping techniques. Credentials are saved for spreading later in the network.
- Lateral movement: Based on results from previous stages, the hopper will try to spread laterally by using techniques, such as pass the hash, kerberoasting, LLMNR/NB-NS poisoning, and others.

This enables Cymulate to test systems such as endpoint detection and response (EDR), deception honeypots, and heuristics behavior that can also be tested with other vectors, including the endpoint security vector.

For lateral movement simulation results, customers can choose to save test results locally or in the cloud. All reports on assessment results, be they executive or technical, can be automatically delivered to designated recipients on the simulation's completion.

APTs are low and slow and can be lethal

APTs fit into the "low and slow" variety of cyberattacks, in that they employ stealth to avoid detection and enable the threat actor to move laterally in the network without getting caught. This is in contrast to simpler opportunistic malware attacks that exploit the first system they land on without seeking to move laterally deeper into the network in search of high-value targets, such as critical servers, databases, or operational systems. The stealth techniques used by APTs enable threat actors to lie in wait for an opportune moment to spread in the network (for example, a suddenly opened port, a late-night hour), with the ultimate objective to move laterally until targets of interest are located.

APTs work by gaining unauthorized access to a network and remaining undetected for an extended period to achieve their nefarious goals. The average dwell time on a victim's network in 2018 ranged from 71 days in North America to 204 in Asia-Pacific. One of the most frequent goals is the theft of sensitive data such as intellectual property or lists of customers, contacts, or financial information in the business world, or state secrets in the political sphere. High-value transactions have also been perpetrated by APT groups, some with purported ties to nation states. Disruption of a victim's systems might also be on the agenda, by deleting files or planting bogus data.

Cymulate refers to its recently added capability as "Full Kill-Chain APT simulation" in that it enables customers to test their cyber-readiness across the entire Cyber Kill Chain (as originally defined by Lockheed Martin), from pre-exploitation (reconnaissance, weaponization, and delivery) to exploitation, and on into post-exploitation activities, such as command and control communication and data exfiltration. It believes this is a significant differentiator vis-à-vis its competitors in the BAS market.

Appendix

Further reading

On the Radar: Cymulate provides breach and attack simulation from a single agent, INT003-000008 (January 2018)

Author

Rik Turner, Principal Analyst, Infrastructure Solutions

rik.turner@ovum.com

Ovum Consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Ovum's consulting team may be able to help you. For more information about Ovum's consulting capabilities, please contact us directly at consulting@ovum.com.

Copyright notice and disclaimer

CONTACT US

ovum.informa.com
askananalyst@ovum.com

INTERNATIONAL OFFICES

Beijing
Boston
Chicago
Dubai
Hong Kong
Hyderabad
Johannesburg
London
Melbourne
New York
Paris
San Francisco
Sao Paulo
Shanghai
Singapore
Sydney
Tokyo