Winning the battle against blended threats

BLOG IN APPLICATION SECURITY
BY TOM HICKMAN

We're watching evolution in real-time. The bad guys have industrialized the attack toolbox. They're a step ahead of firewalls. They know where the tripwires and detection thresholds are for DDOS and Bot Detection solutions. Staying low and slow is cheap and productive. They're sappers and deftly understand how to stay below the threshold of detection.

From reconnaissance towards pwnage, attack methodologies shift, shimmer and shimmy through cracks in defense systems designed for a less clever attack. What was once a winning defense strategy tooling designed to block a single variant of an automated attack just doesn't cut it anymore.

For good reason, companies are calling ThreatX for help. Their allegedly best-of-breed point-solutions for DDOS mitigation and Bot detection are failing in the face of this evolution in attack sophistication. When we get the call, we start with forensic analysis to determine how and why things went wrong, and we deploy the full power of the ThreatX Platform to get them protected going forward.

Recently, several of these engagements have shared a common theme the damage was getting done because attackers used a blend of tools and techniques that didn't fit cleanly into any single layer of the client's defense perimeter. As we dug into these attacks, obvious questions emerged;

> *Was it a bot attack?*
>
> *Was it a large-scale Distributed Denial of Service (DDOS) attack?*
>
> *Was it an attempt to exploit a known vulnerability deep in some application's tech stack?*

Spoiler Alert: the answer to all three questions is "YES"!
Because attackers are under no obligation to conform to our defense toolchain's definitions or expectations.

Increasingly, our threat-hunters observe highly sophisticated, multi-faceted, mixed-mode attacks that penetrate defenses by staying just below detection thresholds. Then they morph. Then they move one more step. Then they

In the cat-and-mouse game of cyber defense, it's good sport!

In most cases, the problem isn't that attackers employed some novel new evasion technique or zero-day exploit. The problem usually centers around individual security tools that can only see a portion of the overall attack. Let's look at why this tends to happen and what we can do about it.

The defense toolchain is fractured and faceted.

Security tools are built and sold to solve problems with neat boundaries, because that's how security buyer's shop. But attackers don't care how you allocate your 2021 security budget. They monetize their work through ″ ahem ″ less traditional avenues. So, they're unconstrained as they develop new types of threats or techniques.

Over time, an organization's security stack becomes a patchwork of specialized uni-taskers. Each addressing a specific attack type. Each plugging a specific gap. Trouble creeps in when attackers cobble together a hundred one-trick ponies and tie them together in a purposeful array of multi-faceted, blended threats.

Maybe somewhere there's a hacker in a black hoodie clacking away on a mechanical keyboard like in those classic hacker movie montage cut-scenes. More likely, there's an attack orchestrator moving and modifying these attack probes, collecting data, observing, orienting, deciding, attacking. That attacker itself is also made of software. Attackers are using robots that are using robots to attack your sites.

Bots are used in all phases of an attack, not just the account takeover or credential stuffing use cases that drove last year's purchase of an anti-bot product.

Organizations usually call us in because they've ended up with a curated collection of specific detection strategies designed for specific issues–usually at scale. Often unclever, but massive in scale. Big things that are easy to see are often easy to stop. But small clever things can slip through the cracks. **The attack has evolved.**

Attackers use every-tool toolkits these days. They can easily design and build sophisticated, multi-faceted attacks. Each attack facet operates just below industrialization of the attack toolbox.

ThreatX was built to handle this new world. Our goal isn't to simply check all the individual AppSec feature boxes. Our goal is to bring all of the best detection strategies together into a single defense posture that notices these shifting attack modes, sees them for what they are, and stops attacks that pretty much everybody else in the industry is missing.

It's time for an attacker-centric security solution. How fortuitous!

We've been talking about our attacker-centric model for a long time. It was a founding idea for the company. But we're security guys, not advertising executives. It's been a hard concept to get across to a world flooded with messaging about NGWAF and WAAP and DDOS and all the other acronyms tied to all the other security budgets in the world.

But people are starting to get it, because they're under a new kind of attack. It's super cool when we're able to help.

Other solutions never accumulate enough signal to see the entire risk landscape and protect customer assets. ThreatX integrates that risk signal across multiple attack types, over multiple toolchain variants, over changing IPs, over long time scales. We notice everything the attacker does, even if it seems innocuous at the time. We do this while it's happening so we can do something about it for you. Contrast that with other solutions that do the same thing, weeks or months after a breach, so you know who to blame and who to buy. Skip the forensics. Give us a shout and let us show you what we can do in the face of this new challenge.

The defenses that worked last year or even last week no longer work. We need new countermeasures to protect applications from this reality. We need security tools that use all the industry's best analysis, detections, and protections together in one context. Only then can we be prepared for what the future holds. If you'd like to see what that looks like in practice, just reach out to us at sales@srccybersolutions.com,and we would be happy to show you. **Schedule a demo today**!

About the Author

Tom Hickman

Tom has a long track record of building and scaling product delivery capabilities at mid- and growth-stage startups. He served as the VP of Engineering at Edgewise Networks, where he led engineering through early releases of Edgewise's zero-trust micro-segmentation product. While at Veracode, a leader in AppSec, Hickman led engineering through an Agile transformation and helped the company become a true multi-faceted AppSec platform prior to its acquisition by CA Technologies in 2017. Tom holds a B.S. degree in mechanical engineering from the Georgia Institute of Technology.

SHARE

Subscribe for updates

Sign up for exclusive threat research, company and content updates, and the occasional fun contest.

JOIN OUR NEWSLETTER

Ready to get started?

REQUEST A DEMO