THE EXPERTS BEHIND CAST

BY BARRETT DARNELL

Managing Senior Operator Barrett Darnell studied computer science in college, which led to him eventually joining the United States Air Force as a Communications Officer. “My interest in information security started from the perspective of a defender until I transitioned to offensive security around 2015,” stated Barrett. This blend of experiences has provided him with the ability to think like both a member of the red team and a member of the blue team. He would spend the last five years of his Air Force career at Fort Meade, MD working for the United States Cyber Command and their mission partner.

When it came time to part ways from the military, Barrett sought out a company that had “just the right culture and shared my same values.” A close friend of his, Caleb Gross, had separated from the Air Force a few months earlier. Searching together, Caleb and Barrett were introduced to Bishop Fox, and were hired as members of the Continuous Attack Surface Testing (CAST) team. Working as a CAST Operator has given Barrett the opportunity to apply the cybersecurity skills he honed in the military on a daily basis. “Our work is uniquely designed to always challenge us.” Barrett also appreciates that the CAST team can “walk away from engagements knowing that we have protected our clients to the best of our ability against potentially devastating security issues.”

As a CAST Operator, Barrett’s work includes weaponizing emerging threats and notifying clients on their potential risk before any exploits are made public for use by opportunistic adversaries. “Our exploit development capability is top-tier,” he said, bringing into focus a major differentiator for the CAST offering. As an example, he recalled the critical Citrix vulnerability disclosed in late 2019, which he said was a “race against time.” The Bishop Fox CAST team jumped on that threat quickly. “Lots of folks were digging in to see how they could leverage that vulnerability. We developed a proof of concept to test for the issue on our clients’ attack surfaces before any other such exploit was released.” More than simply alerting CAST clients to their potential risk, the team was able to demonstrate the possible impact if these systems were left unpatched or if mitigations were not quickly applied.

Compared to similar services, Barrett sees several key differences between them and the Bishop Fox CAST offering. One specifically stands out to him, though: the human element. “Clients can ask us questions and raise their concerns in real time on the CAST platform,” he said. “You can’t do that with an automated system. Plus, there is much more direct communication between technicians to get systems secured as effectively and as soon as possible.”

He added, “What we do is different – it’s better. There is no one doing what we’re doing right now. It’s not vulnerability scanning, it’s not pen testing, and it’s not red teaming. Instead, we’re

blending all of these together into this mix that is entirely in a league of its own."

ORI ZIGINDERE

Ori's interest in security has been nearly lifelong: "I've been interested in security since I jumped on the Internet. For me, the main attraction has been how things work and how systems come together." Even before he wrote a line of code, Ori had begun to adopt the hacker mindset. He would go on to teach himself HTML, JavaScript, and CSS. With his newly found interest in programming, he obtained a degree in computer science. At the start of the 2010s, while working as a software engineer, Ori's interest in infosec grew exponentially. His very first infosec conference, a BSides Boston event, proved to be the game-changer he needed to pursue security seriously. Inspired by the presentations he heard and the people he met, Ori began improving his pen testing skillset while picking up a handful of certifications along the way.

Ori would go on to apply at Bishop Fox, where he was hired as a member of our newly formed CAST team. As a CAST Operator, Ori finds himself confronted with dynamic situations daily: "No day is the same. And no customer's attack surface is the same, either. I'm constantly learning and experimenting with new technologies, which I can then apply to my testing with CAST clients."

The CAST Operators embrace an agile approach to their tasks. Ori is a scrum master for one of the delivery teams in CAST, helping others on his team be thorough, but efficient. "I guide my colleagues on what should float to the top in terms of priorities. I also remove blockers for others whenever possible and contribute improvements to our delivery process." Using the Agile methodology and a Kanban board, the Operators can direct their focus on high-priority items during two-week sprints. This allows them to be more effective in their day-to-day work and help address high-impact client concerns faster.

"We keep up with bleeding-edge stuff, tracking emerging threats. We stay informed – part of what we do is keeping up on CVEs as they are released and analyzing them to see if they affect any CAST clients. If a client is affected, we alert them before attackers have a chance to strike. And then we prioritize the issues for further analysis accordingly." In late 2019, Ori caught wind of CVE-2019-19871 – a critical-severity vulnerability affecting several Citrix products. Ori and the other Operators worked quickly to inform clients about their risk level. Then, the Operators were able to support clients in expediting change management tasks related to patching, based on substantiated evidence and based on a proof-of-concept exploit. As a result, CAST clients were able to remediate the issue a full month before Citrix even released a patch.

But for Ori, CAST goes beyond threats, technology, and advantageous attackers waiting for the right moment: "I work with a group of super talented people who I'm happy to be among. Everyone is easygoing and hyper-communicative. It helps us work around issues as they arise.

Because many of our Operators have military backgrounds and an inclination toward discipline and rigor, our team has taken on those traits. That discipline is what helps us work quickly to analyze risks in a sustainable way that scales for our clients and lets us stay ahead of attackers."

JON WILLIAMS

Jon Williams' professional career started off in international development, but he eventually would end up "working in computers." Jon commented on those early days, "I realized this is never going to get old."

Jon would go on to work at a startup for a decade, where he owned the entire network. While working in IT, Jon also dove "headfirst" into cybersecurity. "I grew into a security role," he said. "I taught myself how to architect a security system. From there, I got into red teaming and began doing my own pen tests." He then started a new job at a mid-sized regional bank as a member of its blue team, and learned the incident response side of the house. "But my heart was always with the red team," he remembered. While working at the bank, Jon found himself in charge of overhauling their penetration testing program. He was evaluating security consultants for the company and ended up choosing Bishop Fox. While partnering on the project, he was drawn to how the consultants worked creatively and in a supportive, Agile culture. "It was exactly the type of environment I was seeking." Jon eventually joined the company as a CAST Operator.

"CAST is always innovating. We're applying things in novel ways. There's so much experimentation and free reign. I love that we have this creativity and license to innovate, which in turn benefits our clients." Jon's eclectic mix of skills puts him in a unique position as a member of CAST – in fact, it informs how he thinks when working on engagements. "I can easily step into a client's shoes, since I've been there myself." Jon also finds the automation aspect of the CAST platform an invaluable asset. "Our goal is to automate to the fullest extent possible. CAST brings together the best of both worlds: automation and skilled professionals."

In one instance, Jon was brought on during an engagement with a client to test the security of a smaller company they had recently acquired. "I was able to achieve full stack compromise, and get into an encrypted database. I found decrypted tax records for millions of people upon doing this, and helped the client save themselves from a disaster."

For potential clients, Jon understands that they might see a parallel between CAST and bug bounty programs. "But with bug bounties, you don't really get to know the people. There's no relationship," he said. "When you know the people you're working alongside and who are finding weaknesses in your perimeter, the quality of your results is better. We are looking for what will produce the most impact for the client, which is a stark contrast to financially driven bug bounty hunters."

NATE ROB

When he was in sixth grade, Nate Robb took it upon himself to build a computer – starting down the path that eventually would take him to Bishop Fox's CAST team. Later in life, Nate would earn a CIS degree and go into a career of IT auditing. "Security was always a fascination for me," he said. I fell in love with penetration testing; I wanted to do it full time."

He earned his Offensive Security Certified Professional (OSCP) certification and began working at a smaller consulting firm where his clients consisted of private companies and federal agencies. His responsibilities ran the gamut from penetration testing to social engineering, but most of his time was spent web application testing. After leaving that position, Nate became a full-time bug bounty hunter for several months, where he got a taste of the "race to find as many bugs as you can, no matter the severity" mission of crowdsourced bug bounty programs. But this experience proved pivotal to Nate's development as a penetration tester – and influenced his future work with CAST clients. "Since bug bounty is heavily incentivized, the community comes up with some creative ways of finding vulnerabilities." However, he acknowledges the split between the world of bug bounty and professional penetration testing. "There's much less of a focus on interaction with customers or thorough reporting in bug bounty. Pen testing is similar in that you are using creative ways to find vulnerabilities, but you generally want to push impact as far as possible. There's also plenty of client interaction and an emphasis on robust, well-written reports with actionable findings and recommendations."

It was during this time as a bug bounty hunter that Nate came across the CAST Operator job posting. Nate wanted to switch from a "find all the things for profit" mindset to more of a partnership with a client to find the real risks in their business and from their specific attackers, and saw the role as a potential fit. "It completely aligned with my skillset," he said. "Every Operator has their specialties and we complement each other well. One Operator might gain a foothold via a critical security issue, then ping the group for assistance with post-exploitation to ensure we identify the highest-impact findings for the client. We build and improve for clients together."

Nate specifically finds tracking emerging threats to be an impactful part of his work. "A new vulnerability drops, and we have these talented exploit developers on our team. So we build an exploit and begin hunting for the vulnerability across our clients' perimeters – before the script kiddies can begin scanning the Internet for it." He also enjoys working with the CAST clients, who are receptive and curious about the team's findings – truly seeing the CAST Operators as an extension of their security teams. "They're interested in the technical details of the vulnerabilities we find, and they're quick to fix things."

One of his foremost achievements as a CAST Operator came when evaluating Gravana, a fairly popular off-the-shelf software. "We had early access to a proof-of-concept exploit for an N-day

server-side request forgery vulnerability in the software that we could use to hunt for affected instances. We then used our findings to point our clients to where they were exposed and what the impact would be if left unfixed," he remembered. "This was just as news of this vulnerability had leaked, and no real exploit had been made public yet. So we were able to alert our clients and help them protect themselves right away – before any attackers could get access to an exploit." (To see how CAST Operators track and respond to emerging threats, go here.)

Nate believes that a significant driving force of CAST is that it can respond to the fluid nature of a client's attack surface. "Continuous monitoring means you're constantly aware of your vulnerabilities – because we're always out there looking for them."

TRAVIS MILLER

"Security is always evolving, and that's something I find interesting," said Travis Miller, a CAST Operator. Earlier in his career, he was working as a QA developer/manual tester on a software development team. Eventually though, Travis decided he wanted something more. "I was looking to branch out and find that next step in my career." A friend had introduced Travis to penetration testing, something he had never heard of before. He was quickly hooked.

The thirst to learn new skills was what drove Travis to CAST. After receiving his OSCP, Travis applied to Bishop Fox. Once Travis was hired as a CAST Operator, he became impressed with what he saw as the "ethos of the team – it's an extremely supportive environment."

Travis derives a sense of purpose from his work as a CAST Operator. "We protect our clients' information, and we protect their clients' information, too. That makes what I'm doing extremely meaningful. It's more than likely a breach will occur at some point, and when it does, it will be through a client's public attack surface. We provide our clients with real-world attack methods, real engagement that thoroughly tests their security infrastructure."

A highlight from Travis's work came when he completely took over a client's cloud infrastructure. "It wasn't due to vulnerable software; it was the result of a misconfiguration," he said. "We found a reference to a site in a GitHub repository. There wasn't anything exactly sensitive in the repo, but it did contain a reference to an internal Jenkins deployment server. It turns out the server was misconfigured and completely exposed to the Internet. From there, I was able to download the source code of all the hosted projects. I then extracted credentials, API keys, and other sensitive information."

In a separate instance, Travis identified exposed UI documentation belonging to a technology client. "I went to GitHub and found some credentials that allowed me to create a token," he explained.

Travis then hit numerous other endpoints on the UI page that were behind an authentication wall. “Eventually, my attack chain led to the client’s Amazon Web Services (AWS) infrastructure. Through enumerating their S3 buckets, I discovered additional sensitive information which allowed me to escalate privileges and take over their entire AWS infrastructure.”

Travis and the other Operators are constantly looking at CVEs and procuring proof of concepts before anything is otherwise available. Whenever a new CVE is disclosed, the CAST Operators are leveraging the platform to identify it in clients’ attack surfaces. “We care about doing a good job and protecting our clients’ data. We strive for a true continuous effort, which is what makes CAST stand apart from similar services.”

ZACH ZEITLIN

“I always liked tinkering. As a kid, I would take apart my parents’ VCR player just to see what was inside – and then I’d put it back together,” Operator Zach Zeitlin recalled. He credits this early fascination with finding out the why behind a thing – a staple of the hacker mindset – for propelling him into cybersecurity. “That curiosity combined with the childhood thrill of testing boundaries led me into security.”

As an adult, this curiosity has served Zach well. He has held several roles in cybersecurity – most of those while serving in the United States Air Force. Working in the Cyber Mission Team and National Mission Team gave him a one-of-a-kind security foundation. Training, planning, and testing network defenses were among his chief responsibilities, which gave him the well-refined perspective of a red teamer. Prior to joining Bishop Fox, Zach also managed capability acquisition, where he inspected new tools for integration into existing operational procedures. This process involved organizing the development pipeline for several cyber offense and defense tools.

It was while in the Air Force that Zach heard about Bishop Fox. “I found out that immense opportunities for growth were available at the firm,” he said, which led to him applying as a CAST Operator.

A moment that sticks out to Zach about his tenure as a CAST team member involves a time when he saw his direct impact on a client. “A customer had a question about remediating a vulnerability identified by our team. The question shined a light on a confusing portion of a vulnerability report, and prompted a further team discussion, a quick process change, and then some code debugging. Then, we split the original report into two sub-reports, delivered it, and notified the client all in one evening.” Responding to change quickly – and making necessary adjustments for the sake of the customer – is just one example of the CAST team’s remarkable agility. “It felt great to be involved in that process,” Zach said. “CAST is multi-functional and comprised of people who respond well to input. A client can interact and shape the service to benefit both themselves and CAST as a whole.”

A key reason that the CAST team is able to stay so flexible and pivot as needed is because of their use of the Agile methodology. Zach recently became a scrum master for the CAST team, which means he works to ensure proper priorities and allocation of resources. “If there is a lot of work in the queue, we must determine how to best prioritize that queue and work together so we can provide the best service for CAST customers. I also relay updates to and from the leadership team to enable a feedback loop that allows for continuous improvement and scalability.”