HUNTRESS

Requesting Backup: The Almost-Invasion of Cobalt Strike

How Huntress caught an elusive threat actor's bid to gain control where SentinelOne missed

You have to pick your partner carefully.

In work—as in life—it's about finding someone who can fill in the gaps. One's weakness should be another's strength.

As a managed service provider, you may be an expert in your field but you're not invincible. Cybercrime is incessant and unmerciful, with attackers operating from all corners of the globe, at all hours.

Beat the Clock

It was the stroke of midnight. Magna5, a managed service provider (MSP) with a client base of over 700 small and midsize organizations, was setting up a new customer when Huntress sent an alert for Cobalt Strike, a powerful remote access tool commonly used by threat actors.

Huntress swiftly isolated the machine for Magna5's client. As it turned out, they had a SonicWall VPN appliance with an unpatched vulnerability. It allowed the attacker to gain remote access to a non-domain Windows 10 machine—a dangerous prospect.

magna5

Location

Offices in Boston, Charlotte, New York, Philladelphia, and Pittsburgh

Threat encountered

Cobalt Strike

About

Magna5 serves over 700 clients with the most demanding managed IT and cybersecurity needs by delivering comprehensive protection and unrelenting support. That's why leaders in education, healthcare, government, financial services, manufacturing, and other uptime-dependent industries turn to Magna5 for their crucial IT operations.

"As we were still in the process of onboarding, our security operations center (SOC) was not yet live for this customer," recalls Matt Kimpel, Director of Cybersecurity at Magna5. "The threat actor worked hard to bypass SentinelOne. But Huntress caught it. It's a great example of how many endpoint detection and response (EDR) solutions miss the origin and context around attacks. That context is critical to preventing issues."

Two's Company

For Kimpel and the Magna5 team, more is, in fact, more. At least it is when it comes to protecting their clients' business assets.

"No one solution alone can catch 100% of all attacks," Kimpel recognizes. "Bundling SentinelOne with the Huntress Managed EDR solution ensures we are able to catch more threat actors quickly to keep our business and our clients safe."

Magna5 set up SentinelOne with their own SOC but soon noticed potential issues being overlooked or surfacing without the context needed to isolate and resolve problems.

After reading peer feedback on Reddit and other forums about Huntress, Magna5 decided to give the solution a try. "The setup took minutes and immediately Huntress started finding issues missed by other endpoint solutions that our clients were using," says Kimpel.

Double Take

Magna5 started offering multiple bundles, including patching services combining SentinelOne with Huntress. "SentinelOne has ransomware prevention capabilities while Huntress adds a detection layer with Ransomware Canaries," Kimpel notes. "Pairing these together provides end-to-end layered ransomware protection. Now, it is extremely difficult for threat actors to go undetected."

Take BlackBasta for example. BlackBasta is a ransomware-as-a-service (RaaS) criminal enterprise that first emerged in early 2022 and quickly became one of the most active RaaS threat actors in the world.

When the Magna5 team spotted BlackBasta malware execute on their client's system, they rapidly rolled out their Huntress and SentinelOne solution and got instant feedback on the

> **"The threat actor worked hard to bypass SentinelOne. But Huntress caught it. It's a great example of how many endpoint detection and response (EDR) solutions miss the origin and context around attacks. That context is critical to preventing issues."**

incident, meaning they could remediate it at pace.

"Right away I knew what I was dealing with and was able to mitigate the situation without any impact on our client's business," says Kimpel.

Without this combination of solutions working together, they may have missed their window for damage control.

In addition to the SentinelOne and Huntress bundled patch solution, the team at Magna5 layers their internal SOC with the Huntress SOC, a 24/7 team who are continuously searching for compromises and minimizing false positive alerts.

"Humans are imperfect," Kimpel shrugs. "We make mistakes. Having a second set of eyes gives us a comprehensive view of what's happening to our systems so we can take action quickly and prevent real issues for our clients and our own business."

And therein lies the main advantage: Huntress doesn't just help the team at Magna5 to protect their clients, it safeguards their business too, providing education and guidance every step of the way.

"Huntress finds what other vendors miss," says Kimpel. "Period. And you just can't put a price on that."

"Humans are imperfect. We make mistakes. Having a second set of eyes gives us a comprehensive view of what's happening to our systems so we can take action quickly and prevent real issues for our clients and our own business."

About Huntress

Huntress is the leading cybersecurity partner for small- and mid-sized businesses (SMBs) and the managed service providers that support them. Combining the power of the Huntress Managed Security Platform with a fully staffed, 24/7 Security Operations Center (SOC), Huntress provides the technology, services, education, and expertise needed to help SMBs overcome their cybersecurity challenges and protect critical business assets. By delivering a suite of purpose-built solutions that meet budget, security, and peace-of-mind requirements, Huntress is how SMBs defend against cybersecurity attacks.

To learn more, visit huntress.com or follow Huntress (@HuntressLabs) on social media.

HUNTRESS.COM