HUNTRESS

Cloak and Dagger: Unmasking a Cyber Villain

How a criminal's convincing camouflage couldn't fool Huntress

Just when you think you've seen it all, cybercriminals always have the capacity to surprise.

For small- to medium-sized businesses (SMBs), these kinds of surprises are never welcome. And as attackers grow more creative by the day, SMBs might not be ready for their next sleight of hand.

The Heat of the Moment

"My heart sank. We had been down this road before. They couldn't afford another breach."

It was the final days of summer and Cramer Snuggs, founder of Cascade Technologies, was heading out of the office when his phone buzzed. It was Huntress.

The team had emailed to report that a remote access trojan (RAT) had been used on one of his longest-standing clients, a stalwart restaurant serving the Grand Strand for over 40 years. The malware threat had been detected by Huntress' Managed Endpoint Detection Response (EDR) solution as the result of a phishing email, containing a not-so-innocent hyperlink that diverted the user to a malicious website. The criminal's aim? To gain complete control of one of the computers.

"We had deployed both SentinelOne and Huntress, and the machine in question was running Acronis Cyber Protect for its backups," says Snuggs. "We had already bolstered our security stack to prevent such an attack. I was nervous."

CASCADE TECHNOLOGIES

Location

Myrtle Beach, SC

Threat encountered

Remote access trojan (RAT)

About

Clients choose Cascade Technologies for its proactive approach and innovative solutions, enabling them to navigate and thrive in the ever-evolving world of information technology. The mission is clear: to bring enterprise-level IT services, including cybersecurity, disaster recovery, VOIP, and more, within reach of small to medium-sized businesses.

The chilling consequences, were the attack to succeed, raced through his mind: this couldn't be allowed to unfold. Not again.

"The stakes were sky-high—especially seeing as a former incident with this client had led to us working with the Secret Service to mitigate and triage what had taken place," divulges Snuggs.

Lightning Strikes Twice

Given Cascade's history with the client, this latest attack was completely unexpected.

"I was shocked," admits Snuggs. "Considering all that we had been through, I honestly didn't think that this would happen again. We had worked with all the users and made it very clear about the dangers of clicking random links and opening unknown emails."

Nonetheless, Snuggs' team understood that there would always be room for human error. They were thorough. They doubled down on the protection and scrutinized vendor activity within the network ever more closely.

"It was actually the catalyst for us to engage Huntress," explains Snuggs. "We were trying to implement zero trust, without necessarily having a zero-trust solution. It was the reason we essentially mandated that the rest of our clients adopt our full set of security products, rather than picking and choosing à la carte."

It turned out to be a very wise decision.

The Devil in Disguise

The attack rapidly set a sequence of events in motion.

"Before I could so much as log into the dashboard to take a look at what was going on, I'd been sent an email from our account manager at Huntress, letting us know that the machine had been isolated and asking if there was anything else they could do," he recalls.

"At the same time, I had jumped onto Huntress' messenger service on their website and ended up connected with a SOC analyst. So, there I was: I had an expert chatting to me live, answering questions and giving me reassurance, plus a dedicated account manager on the phone, guiding me through it all."

But it wasn't over yet. Another machine was in trouble.

"It was one that wasn't under management, and we already had a lot of concerns with," says

"Before I could so much as log into the dashboard to take a look at what was going on, I'd been sent an email from our account manager at Huntress, letting us know that the machine had been isolated and asking if there was anything else they could do."

Snuggs. "We were worried it could have been affected as well. Within half an hour, we had boots on the ground, additional agents deployed, and Huntress support working with me directly. Scans were completed on the additional machine and soon it too was isolated.

"While all this was going on behind the scenes, it was business as usual for the client. That was key. We were able to do what we needed to do, while they continued making revenue.

"It left me feeling like we had some true subject matter experts on our side, who really respected the urgency of the situation. We weren't alone."

When the dust had settled, one question remained: how could this have happened? Although the client had taken responsibility for clicking the link, it still didn't explain how the attacker had broken through such a substantial security stack in the first place. How did they manage it?

"Huntress' alert revealed that the RAT was in fact masquerading as Acronis Cyber Protect," answers Snuggs. "A generic alert would have had us believe that it was simply updating or something legitimate was going on with that piece of software. But no. It was a RAT! Had we not had Huntress in place, this might have flown catastrophically under the radar."

Straight to the Point

Rather than inundating the team with data, Huntress provided a clear path forward.

"It was very clear what we had to do," he remembers. "Instead of spending hours sifting through data, trying to fit the pieces together, we were given actionable information and steps to take. Huntress devised an entire remediation plan to resolve the issue."

As a result, other than one machine being offline for a few business hours, the attempted breach didn't affect the client's bottom line.

"The biggest thing for the client is the trust between us," reflects Snuggs. "We've always had a strong relationship, but now it's stronger. Comparing our response to this incident to the last, they feel like they're in safe hands. With other solutions, we'd have to be more proactive, to log a ticket or make a call. There would be a delay. Because of its continuous monitoring, Huntress is on it immediately, and we have access to its resources instantly."

"Partnering with Huntress is like having a full security operations team on my payroll," says Snuggs. "It's such a small price to have Huntress protection on that endpoint, yet in return, I get a fully staffed team that I wouldn't be able to afford otherwise. It's priceless."

"With this experience, I realized just how far we had come as an MSP since the last incident we'd dealt with, and the biggest difference was Huntress."

"Partnering with Huntress is like having a full security operations team on my payroll. It's such a small price to have Huntress protection on that endpoint, yet in return, I get a fully staffed team that I wouldn't be able to afford otherwise. It's priceless."

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.

Founded in 2015 by a group of former National Security Administration (NSA) operators, Huntress has more than doubled over the past couple of years to support 4,300 partners and more than 105,000 organizations, now protecting more than two million endpoints. The company recently closed a $60M series C led by Sapphire Ventures.

For more information about Huntress, visit huntress.com or follow us on social media.

HUNTRESS.COM