HUNTRESS

# You've Not Got Mail: The Strange Case of Missing Letters and Multi-Factor Authentication

## How Huntress MDR for Microsoft 365 helped uncover an attempt at business email compromise for a Milwaukee-based IT firm

"We had no concept of how deep this went. How could we? We were just talking about mailbox rules! But it wasn't a simple case of an account being infiltrated and spam being sent, it was far more coordinated than that. It could have done serious damage."

The digital world doesn't exist in a vacuum. It's not like Vegas: what happens online most certainly won't stay online. And while most of us grasp this fact, the extent to which it makes the leap from digital to physical reality depends on the success – and sophistication – of the attack.

But what if it could work the other way around? What if a cyber threat alert could uncover, rather than lead to, a bigger crime, one that was very much already in the physical realm?

When – and how – does cybersecurity translate into physical security?

stammtech

**Company Name**
Stamm Tech

**Location**
Milwaukee, WI

**Threats encountered**
Business Email Compromise, Malicious inbox rules

**Take It From the Top**

"Our first clue was a notification from Huntress," says Bryan Heindel, director of IT at Stamm Tech in Milwaukee. "It was only our first week of rolling out its Managed Detection Response (MDR) for Microsoft 365 solution when it flagged a client account for a battery backup seller."

It wasn't just anyone's account, either.

"It belonged to the CEO of that company," Heindel elaborates. "There had been some suspicious activity: namely, some inbox rules had been created, redirecting senders to the RSS feeds folder and specifically to two bank domains."

The direction of travel was evident – and frightening. Heindel knew they had to act fast.

"One of our team members quickly reached out to let them know and discuss next steps," he says. "They were advised to go through their logins, check their access points, and reset their passwords. Thankfully, Huntress was able to clean up the rules automatically. All in all, the downtime only amounted to about an hour at most, as we worked to reestablish multi-factor authentication (MFA) and clean up any additional MFA devices that weren't recognized."

The coast was clear, right? Not quite. As the pair continued talking, a curious picture was starting to emerge.

"The more the CEO thought on it, the less isolated the incident seemed," says Heindel. "They mentioned that physical mail had also coincidentally been going missing. It was then that they had a scary realization: they hadn't received any mail from their bank for weeks."

**On the Money**

The client immediately got in touch with their bank. Sure enough, a storm was brewing.

"They discovered that there had been attempts to add an authorized user to their bank account," Heindel says. "From there, wire transfers could have been made. Even obtaining a login to the banking site would have allowed the attacker to zero in on other aspects of the business, or access other tools and services. Had we not contacted the client, they wouldn't have made the connection. Things likely would have got much, much worse."

Did Huntress' initial detection just foil a wider extortion plot? Heindel certainly believes so.

"We had no concept of how deep this went," he says. "How could we? We were just talking about mailbox rules! But it wasn't a simple case of an account being infiltrated and spam being sent, it was far more coordinated than that. It could have done serious damage. Who knew what else they could have gained access to?"

"They were advised to go through their logins, check their access points, and reset their passwords. Thankfully, Huntress was able to clean up the rules automatically. All in all, the downtime only amounted to about an hour at most, as we worked to reestablish multi-factor authentication (MFA) and clean up any additional MFA devices that weren't recognized."

Even more alarming was the precision of the attack. Though Huntress had caught the attackers in the act before they were able to redirect via email, they had already managed that via physical mail.

"The criminals were concentrating on banks that the client used," says Heindel. "It wasn't just typical, generic bank addresses or email accounts. That information was known.

"Without Huntress, we wouldn't have picked up on anything until the client was having far more issues," he continues. "Its Security Operations Center (SOC) works around the clock, meaning even the smallest change or potential threat is detected. When we first spoke, they were experiencing some difficulties trying to sign in, thanks to Huntress' early remediation efforts, but nothing else. They were surprised to hear from us at all. It was so subtle."

Huntress' MDR for Microsoft 365 solution is specifically designed to identify behavioral signs, like creating suspicious inbox rules, helping detect malicious activity early. And with the full backing of the Huntress SOC, identities can be isolated as soon as suspicious activity is detected, so the attackers can't do more damage. Plus, you can be notified of threats in a variety of ways – via ticketing system, email, automated call, or even a text message – to ensure you never miss anything critical.

"When someone calls and says they're not getting any emails, then you know there's a problem," states Heindel. "But to be able to narrow it down to not receiving emails from two banking sites in particular? It could have been weeks before anyone was aware. Ours would have been a more reactive approach, as opposed to the proactive approach we were able to take."

**Target Acquired**

What does Heindel take away from this close call?

"MFA isn't bulletproof," he offers. "It can be very beneficial, but it's not the be-all and end-all in cybersecurity. It can be susceptible to attack. Just because MFA is enabled, it doesn't mean that you can ease up on your protection. I've received tickets after the fact where Huntress had double checked something that had previously been resolved and reported that an additional iPhone was added on the same day for MFA detection."

Huntress' meticulous, 24/7 monitoring by dedicated experts, Managed Detection and Response for Microsoft 365, and a razor-sharp-focused remediation plan were key to fending off financial ruin for the client. This robust suite of capabilities strengthened Stamm's overall

> **"Without Huntress, we wouldn't have picked up on anything until the client was having far more issues. Its Security Operations Center (SOC) works around the clock, meaning even the smallest change or potential threat is detected."**

security stack, integrated well with the company's existing tools and, most crucially, didn't call for labor-intensive attention from the team. There wasn't time to analyze complex data.

"We were on SentinelOne for about four years before it became a challenge to sort through all the data," explains Heindel, of the firm's decision to adopt Huntress. "We were getting a lot of false positives, or worse, what seemed like false positives turning out to be very real positives requiring urgent attention.

"We began looking at alternatives. I'd been hearing about Huntress for a long time and when it came to deciding whether to add more features to SentinelOne or to switch products altogether, it just made more sense to switch, especially with the significant price difference."

"Huntress flips the script on how we manage threats," he summarizes. "You don't need to be specialized in how the product works – any technician can take a look at what's going on and it all makes sense. It really accelerates the resolution process: in this instance, the client was contacted in just five minutes, and back up and running in an hour.

"To have that kind of instant intel from a partner like Huntress, with very little doubt in its accuracy, is invaluable."

**“Huntress flips the script on how we manage threats. You don't need to be specialized in how the product works – any technician can take a look at what's going on and it all makes sense. It really accelerates the resolution process: in this instance, the client was contacted in just five minutes, and back up and running in an hour.”**

# About Stamm Tech

Stamm Tech, a Milwaukee-based IT service organization, embodies its own philosophy of 'whatever IT takes'.

Committed to providing cutting-edge IT services, its mission is to deeply understand an organization's goals and deliver tailored solutions that align seamlessly with its business objectives. Passionate and warm in its approach, Stamm Tech aims to be a go-to advisor, leveraging technology to help fulfill any company's mission.

The exceptional team, ever inspired by the commitment to do 'whatever IT takes', ensures that each individual's efforts make a significant contribution. Stamm Tech prioritizes relationship continuity, assigning each client a dedicated technical account manager and IT manager, who genuinely engages with the team and business. Valuing reputation over profits, Stamm Tech focuses on earning clients for life, through stellar customer service and regular business reviews.

At Stamm Tech, it's not just about technology, it's about making a positive impact on an organization's business journey.

# 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 Huntress on social media.

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

**HUNTRESS.COM**