HUNTRESS

One Suspicious Login. One Client in Jeopardy. One Expert Team on the Hunt.

How Huntress' Managed Detection and Response cracked the case for a New Zealand IT service provider.

Cybercriminals are getting sharper. Slicker. Smarter.

Whatever stereotypical image you have in your mind of the culprits, banish it: hacking has become a highly sophisticated sport, exploiting weaknesses you never knew existed and unleashing advanced attacks designed to inflict maximum, devastating damage at pace.

They're also targeting smaller, less protected businesses just as often as global corporations. Why? Because these companies are vulnerable by nature and ripe for ransomware, malware, and other threats. It's not just the 1% who need watertight cybersecurity: it's the 99%.

Knowledge is Power

When Andrew Fergus, managing director of New Zealand-based IT managed service provider **Ultra IT**, noticed a server login from Indonesia, he didn't think much of it. The client in question was a global food company, with a team spread across New Zealand, Africa, and several European countries, so the login location wasn't entirely unusual. Or so it seemed.

It was at that moment he received an alert from the Huntress Managed Detection Response (MDR) for Microsoft 365 solution, noting that the activity was suspicious, coming from a command line from Azure—uncommon end-user behavior.

ULTRA
PROACTIVE IT SOLUTIONS

Location
New Zealand

Threat encountered
Business email compromise

About
Ultra IT are specialists in IT solutions for businesses across a variety of sectors. They provide reliable and stress-free services that go above and beyond the call of duty. No tricky jargon or complicated pitches—just good, honest IT support that you can trust.

The Ultra IT team has a strong background in IT and are experts in delivering services from email hosting, to anti-virus and firewall, to backups and file security.

In New Zealand, business email compromise (BEC), known commonly as 'email hacking', is a growing concern. In fact, a recent **study** revealed that when asked to determine whether example emails were real or fake, only 5% of Kiwi IT decision-makers were able to correctly identify them all.

"We're hearing a lot about email hackers going in to set up fake email accounts and stealing proceeds from real estate transactions between agents and lawyers," cautions Fergus. "Having an always-on email protection system is critical."

Considering this, another current email phishing campaign affecting many small- to medium-sized businesses (SMBs) in New Zealand is of particular concern. Its target? Finance teams.

Its mission is to hack into invoices, using Microsoft 365 login credentials: users receive an email with an attached invoice and when this fake invoice is opened, it calls for the recipient to log in to M365 to view it. Once the credentials have been swiped, the attacker then has full access to the account if multi-factor authentication isn't enabled.

A Fighting Chance

In the face of such security challenges, Fergus and the Ultra IT team had been waiting for a suitable solution to become available, at a price point that worked for a small- to medium-sized business like theirs. The firm needed the best protection possible, combining cutting-edge technology, innovation, and round-the-clock support with actual human beings on standby to quite literally 'hunt down' compromises.

"When we heard Huntress was looking for alpha testers for their new MDR for Microsoft 365 solution we signed right up," enthuses Fergus. "Alternative BEC solutions out there are really geared towards protecting large enterprises and require security analysts on staff."

With Huntress MDR for Microsoft 365 doing the detective work, monitoring for suspicious login events and other signs of BEC attacks, the Ultra IT team could see clients being able to breathe a little easier, knowing sensitive data was secured and access guarded.

"We liked that Huntress MDR for Microsoft 365 is purpose-built to meet the needs of smaller service providers like us," says Fergus. "Huntress understands that today, most small businesses are run from the Cloud, so, for our clients, email protection is absolutely critical."

"Huntress MDR for Microsoft 365 is purpose-built to meet the needs of smaller service providers like us. Huntress understands that today, most small businesses are run from the Cloud, so, for our clients, email protection is absolutely critical."

Den of Thieves

Before Fergus could even register his suspicious login incident as a threat, Huntress was already on the case.

The investigation showed emails being intercepted and forwarded to fake folders after marking them as read, then sending out spoof invoices and routing replies to that same folder. The next step would have been money collection. "And there would have been no way for my client to catch this until the true invoicing process caught up," says Fergus.

Huntress had other plans. By blocking all access to the email account and resetting the password, the team stopped the fake emails in their tracks and protected customer data and revenue.

"With 230 tenants under management, it's impossible for us to stay on top of every login and monitor all activity," Fergus explains. "Having the Huntress solution working for me in the background prevented what could have been a hugely costly and dangerous compromise for my client."

The rising BEC threat has also spurred the Ultra IT team to double down on other defensive measures, starting with the first line of defense: employees.

"To help our clients quickly identify email attacks, we're also rolling out the Huntress Security Awareness Training (SAT) solution, which delivers a powerful and fun combination of episodes, assessments, simulations, and reports to help employees become more cyber-savvy in the fight against bad actors," adds Fergus.

Peace of Mind

Fergus was so impressed with the power and efficiency of the solution, the firm bought it as soon as it was released and even added on Huntress' flagship Managed Endpoint Detection and Response (EDR) product.

This allows Fergus and the Ultra IT team to carry out continuous monitoring of process executions and associated metadata in near real-time at the source, i.e. protected endpoints, increasing visibility and making it much harder for attackers to disguise their exploits.

"Protecting endpoints and mailboxes helps us keep our clients safe from growing threats," he

> **"With 230 tenants under management, it's impossible for us to stay on top of every login and monitor all activity. Having the Huntress solution working for me in the background prevented what could have been a hugely costly and dangerous compromise for my client."**

stresses. "Having both MDR and EDR working for us covers us fully from even the most creative of criminal activity, constantly capturing process execution data as well as user actions and making highly educated calls on whether anything is suspicious. It's completely comprehensive and thorough, but without the noise and false alarms."

So, what's next for the team at Ultra IT?

"Right now, we are working with a large number of indigenous tribes here in New Zealand, helping them protect their heritage data for future generations," Fergus explains.

"We hope to expand coverage to all Far North tribes and the Huntress suite of solutions will secure the genealogical data for these under-served tribes, protecting their history and culture—and ours."

Case closed.

Key features of Huntress MDR for Microsoft 365 include:

Active monitoring of Microsoft 365 Active Directory logins, configuration, and email rules

Detection of indicators that identities have been compromised to provide security teams with immediate, actionable steps to close doors and stop potential attacks

24/7 SOC analysis and remediation powered by expert threat analysts who investigate threat activity and provide remediation guidance

Instant lockdown capabilities to ensure any suspicious activity that could result in a damaging attack is shut down quickly

Learn More

> **"Having both MDR and EDR working for us covers us fully from even the most creative of criminal activity, constantly capturing process execution data as well as user actions and making highly educated calls on whether anything is suspicious. It's completely comprehensive and thorough, but without the noise and false alarms."**

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 protect more than two million endpoints, supporting 4,300 partners and more than 115,000 organizations. 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.

HUNTRESS.COM