> **We position Huntress as an underlying layer or last line of defense," says Otis. "We've got our firewall, our antivirus, and then Huntress which monitors for persistence.**

Binatech Uses Huntress to Protect SMBs & Stop a Banking Trojan in its Tracks

Binatech has been in the IT space for more than 30 years—and for the past six, VP of Technical Services James Otis has been working to protect the company's small business clients. His team uses Huntress to detect hidden threats that slip past preventive security tools, and to respond to incidents as quickly as possible.

We position Huntress as an underlying layer or last line of defense," says Otis. "We've got our firewall, our antivirus, and then Huntress which monitors for persistence.

That "last line of defense" was put to the test when one of Binatech's clients was hit with a banking trojan.

From Hacking Demo to Real-Life Scenario

The situation was eerily similar to a Huntress workshop James had previously attended; a session that was designed to highlight these exact types of threats.

An end user received a somewhat-suspicious attachment and attempted to open it, but stopped short of enabling macros. They forwarded the doc to a second user, who did open it and unknowingly unleashed Qakbot—a banking trojan capable of logging keystrokes, harvesting browser credentials and self-propagating throughout a network.

One of the challenges with Qakbot is that it's designed specifically to bypass preventive security tools like antivirus and DNS filtering.

That's when the Huntress platform jumped into action. By identifying and analyzing newly created Windows auto-starting code, Huntress determined Qakbot was in play—and a ThreatOps engineer generated an incident report which explained what had happened and how to fix it.

Binatech System Solutions

LOCATION

Hamilton, Ontario

AVERAGE CLIENT SIZE

15-50 Users

SECURITY STACK

Antivirus, Firewall, Unified Threat Management, Multi-Factor, Spam Filtering, Backup, DNS, Huntress

THREAT ENCOUNTERED

Qakbot

The alert from Huntress gave us a clear understanding of what we were dealing with and which user was affected, which made it easy for us to respond right away. The platform truly delivered in this scenario—we were able to disconnect the machine and reset every password the user was tied to—all within twenty minutes of receiving the initial alert.

Moments later, the end user realized their mistake and sent an email to Binatech—where James and his team were already working to resolve the issue.

"We were taking remediation steps before that user's email hit our inbox," he said. "The alert from Huntress gave us a clear understanding of what we were dealing with and which user was affected, which made it easy for us to respond right away. The platform truly delivered in this scenario—we were able to disconnect the machine and reset every password the user was tied to—all within twenty minutes of receiving the initial alert."

"In addition to stopping the threat, Huntress really helped us demonstrate our value to the client," he added. "It ultimately even helped us upsell some additional services."

Without Huntress enabled, the attack could've played out quite differently. "Who knows how long it would've taken to remediate, assuming we'd found the banking Trojan," Otis explained. "The real question is how much money would have been lost had the Trojan successfully extracted bank account info—that's the part we're grateful to not have to deal with."

Finding Huntress

While Binatech had done some early testing with Huntress, the company was initially using an endpoint detection and response (EDR) tool and decided they didn't need to include Huntress as part of their security stack. That changed when the EDR's alerts started piling up.

"We were experiencing some growing pains for a few months and issues with false positives, so I was questioning what I was paying for," Otis recalled. "We took a second look at Huntress, and with some of its newer services like Assisted Remediation the decision to switch back was an easy one."

Assisted Remediation offers one-click execution of corrective actions when malicious footholds are detected. It's one of several ways Huntress enables its partners to respond quickly—and accurately—to discovered threats.

James R. Otis
VP TECHNICAL SERVICES
BINATECH SYSTEM SOLUTIONS

• • •

James has been with Binatech System Solutions for 6 years and has transitioned from working in the trenches as a tech, to client consultations, to participating as an active member of the management team. His focus now is primarily on keeping service operations secure while training and educating the Tier I & II techs.

Learn more at
huntress.com

Follow us on social
@HuntressLabs

Empowering Binatech's Staff

Thanks to the way Huntress' handles detection and response, Otis says the platform has helped his tech team stay sharp and agile when responding to alerts.

"Staffing for security is always challenging," he said. "We've got talented techs on our team, but having a platform like Huntress makes it easier for us to respond to incidents—including things we haven't seen before. We can follow the remediation steps and instructions we get via alerts, and our senior team can focus their time on forensics and investigative work."

About Binatech

For over 30 years, Binatech has been serving our customers with their best interest in mind, because we believe when our customers succeed, we succeed.

We've been providing custom IT solutions to solve the frustrations of our customers in the manufacturing, healthcare, law, and constructions industries with prices that are affordable and results that make a real difference.

Our aim is to solve problems before they happen and eliminate IT issues before they create costly damages and downtime for your business. Don't give IT problems control of your company. Let us take the frustration out of your technology solutions and give you and your employees the time and resources to grow your business and serve your customers with the excellence you aim for.

About Huntress

Hackers are constantly evolving, exploiting new vulnerabilities and dwelling in small business environments—until they meet Huntress.

Huntress enables IT providers to find and stop hidden threats that sneak past preventive security tools. Founded by former NSA Cyber Operators—and backed by a team of ThreatOps researchers—we help our partners protect their SMB clients and take the fight directly to hackers.