Brasfield & Gorrie Finds and Destroys Phishing Campaigns in Seconds

1 user email
enables rapid searching to protect all users

3 clicks
to search and quarantine even advanced threats

In seconds
stops entire phishing campaigns

CHALLENGE

"Our solution was slow. It sometimes took an hour to search and destroy phish."

Patrick Burch and his team at Brasfield & Gorrie needed help.

As IT Security Manager for the large general contractor, with operations in eight states and three billion dollars in annual revenues, Burch needed a faster solution for email search-and-destroy—that is, searching all inboxes for phishing campaigns and quarantining threats. Brasfield & Gorrie has approximately 2,400 users, each a potential target.

"Like everyone else, we get hit by phishing a lot," said Burch. "It's probably our number one cyber-attack vector. We see everything from sextortion scams to basic attachment phish, the whole gamut."

To find and remove phish reported by end users, the IT Security team created a solution in PowerShell. It worked to a point, but the homemade solution involved too many steps and refining it proved difficult—a problem when you consider that on average global users start clicking on a phishing campaign within 82 seconds.[1]

When Covid-19 appeared and more people worked from home, phishing attacks intensified. "We needed to respond faster and remove emails in fewer steps," Burch said. Indeed, research by TAG Cyber and NYU has shown that phishing attacks rose as much as eight percent during the pandemic's first few months.

SOLUTION

"Cofense Vision® is faster because it's much simpler."

Brasfield & Gorrie had been using Cofense Triage™ for a couple of years, relying on it to analyze user-reported emails and separate real threats from noise. Adding Cofense Vision was a no-brainer. The two solutions work on a single dashboard, eliminating steps to speed response and remediation. Moreover, Vision users don't need privileged access to the mail environment. They can run searches themselves to identify even the most elusive threats.

"Now when we remove offending emails, it's three mouse clicks," said Burch. "That's all it takes to search and destroy. We can access Vision in Triage, and everything is right there. You can just keep your hand on the mouse and hardly ever touch the keyboard."

The efficiencies add up when you consider the volume of email reports. For many organizations, including the Cofense Phishing Defense Center, non-malicious reports account for close to 90% of report volume. "We probably get 50 email reports a day," Burch said. "Not all of them are malicious, of course, and that's where Triage helps, enabling us to focus on real threats. Now with Vision, we can remove them rapidly. We use it throughout the day."

Phishing campaigns don't strike all at once. Research shows the average campaign lasts 21 hours.[2] Thanks to the new Auto Quarantine function, Brasfield & Gorrie can start quarantining phish as soon as users report them, with no manual effort. "From time to time, phishing emails will trickle in," said Burch. "So you might get into Triage and see that three people have reported something, and when you come back from lunch another two people have reported. Auto Quarantine saves us time by making the process seamless."

Burch noted that the addition of wildcards, which enable faster detection of phishing links, has made Vision even better. "We can respond to threats a lot easier, especially as attackers change things up to make detection harder," he said.

RESULTS

"Now we search and destroy in seconds."

With so many employees and sub-contractors using Brasfield & Gorrie email, the clock is ticking whenever the company finds a phishing threat. Said Burch, "Thanks to Vision, all we need is for one employee to report a bad email. That one report can protect all 2,400 users after we search our inboxes to see who else received it. Then we just click 'quarantine' and the email disappears. The whole process takes just seconds."

"With our old solution, as more people received an email it took longer to remove it," he added. "If a thousand users got an email, we'd be busy for an hour. Vision frees up a full-time employee to focus on other things."

It also gives corporate leadership a little peace of mind. "Because the Cofense solutions work so well," Burch said, "our leadership doesn't even have to think about phishing attacks."

W: cofense.com/contact **T:** 703.652.0717
A: 1602 Village Market Blvd, SE #400
Leesburg, VA 20175