

Cofense Case Study

Cofense Intelligence Helps
Massive Global Retailer Fight
Growing Security Threats





Cofense Case Study

COFENSE AND MASSIVE GLOBAL RETAILER



Background

Trying to keep up with a barrage of spam and potential phishing threats, one of the world's largest retailers realized its incident response (IR) team had little time for anything else. Phishing campaigns were becoming more frequent and dangerous, and if any of them succeeded in penetrating the company's defenses, the results could be devastating.

"Our email spam filters were not keeping up with the malicious spam intake. And our IR team spent way too much time cleaning up spam campaigns," according to the retailer's cyber intelligence researcher. "We have seen the increase over the past few years steadily going through the roof. When the spam campaigns started turning truly malicious, we knew we had to do something."

So the team started looking for a threat intelligence feed that provides real-time, contextual information on phishing threats to more effectively block them. In evaluating several threat intelligence solutions, the team concluded only one delivers the type of reliable, actionable information the company needed – Cofense Intelligence.

Detailed Threat Information

Most threat intelligence sources are generalist in nature, providing a little information about everything, while others dive deeply into specific threat actor groups. But Cofense Intelligence addresses the biggest threat currently faced by the enterprise – malware delivered through phishing. Cofense employs a unique combination of technology that identifies criminal infrastructure threats and trained analysts who investigate and confirm indicators of compromise. The Cofense approach accurately confirms threats, puts them in context, and reports them to companies so they can address them.

By identifying relevant threats, Cofense Intelligence was precisely what this global retailer needed. The company wanted insight into specific phishing campaigns and their delivery infrastructures. The retailer wanted access to every indicator and malware attribute possible, including IP addresses, URLs and domain names, in order to make smart decisions to defend itself. When analyzing malware, the company wanted to know if it is part of a generalized campaign or an attack targeted specifically at the company or its users. This way, the retailer avoids setting blockers that might adversely impact the business.

Most threat intelligence providers don't provide enough context, the cyber intelligence researcher says. "They'll say, 'Hey go block this,' but we won't know why the malware was trying to hit us or what it was. The intelligence from Cofense gives us the context. Context is crucial. We can see from the network traffic what type of malware it is." So if a user's machine gets infected, "we can see what the malware is and clean it up based on the reports and analysis Cofense sends us." In addition, he says, Cofense identifies threats before others do.

Added Security Layer

Once the retailer opted to implement Cofense Intelligence, it only took a couple of weeks before it was fully up and running. Cofense sent over the solution's APIs and scripts, which were "very easy to follow," the cybersecurity researcher says. "It was a very easy implementation."

Cofense Intelligence, he says, added a much-needed layer to the company's security defenses. "We had insight into all other kinds of threats, but we really needed insight into phishing campaigns specifically," he says.

Now, the company routinely uses Cofense Intelligence to identify and block phishing threats. When the company receives the information, it already has undergone enrichment by Cofense analysts, which means they have analyzed it to add context and meta information. For instance, when a previously unknown domain name is used by malware, the analysts investigate how it is being used to support the malware and whether it's always bad or also contains legitimate content. This is crucial information because blocking the wrong thing can hinder businesses processes and inundate the help desk with calls.

Once the retailer receives this information, its team adds further context relevant to its own environment. Information such as infected IP addresses and URLs is then automatically fed to the company's security proxy servers to block the malware from penetrating the network.



"We go straight to the Cofense report. We want to see how that malware was getting in, what kind of spam campaign was it, what were the subject lines, and then we clean it up,"

Cyber Intelligence Researcher, Global Retailer

Cofense Intelligence is a highly vetted and trusted intelligence stream used by the retailers, also consumed directly by the company's SIEM (Security Information and Event Management). When a malware indicator is spotted already inside the network – possibly as a result of a user clicking on an infected URL or attachment – the team receives an alert and springs into action. Its first step is to check if the indicator matches anything reported by Cofense Intelligence.

"We go straight to the Cofense report. We want to see how that malware was getting in, what kind of spam campaign was it, what were the subject lines, and then we clean it up," the researcher says. Then the team conducts an analysis to determine what impact the malware would have on the network if allowed to spread.

"When we deal with a piece of malware, we'll end up dealing with it across 20 or 40 different machines, or something to that effect. Very rarely it's an isolated incident."

Actionable Outcomes

Aside from better contextual information, the retailer also has found that Cofense Intelligence picks up on network traffic that other intelligence feeds miss. Out of forty active intelligence feeds consumed by the retailer, Cofense Intelligence often catches what many other premium intelligence feeds miss. That's important because those anomalies are malware indicators that if left unaddressed can disrupt business operations.

In addition, says the researcher, Cofense Intelligence delivers no false positives, something the other feeds' vendors cannot claim. "I have not seen any false positives," he says. "Every time we've spotted an indicator, absolutely there has been something on the box that needs to be investigated."

Thanks to Cofense Intelligence, the IR team hardly spends any time on cleanup anymore. This allows them to better focus on targeted threats, which are increasingly common. Cybercriminals have been refining their methods to zero in on specific individuals and groups within an organization.

And while it's difficult to ascertain an unknown – how much potential damage Cofense Intelligence has helped the company avert – the researcher says that without Cofense, malware would have gotten through in some cases and caused damage. "We are getting indicators for things that would absolutely impact our business," he says.

As a result, the researcher says his team would have no trouble defending the budget for Cofense Intelligence if ever management asked them to make cuts. The company already has seen ROI just from reducing the amount of malware cleanup time to a fraction of what it used to be.

"With the amount of phishing going on currently, especially in retail, we cannot afford to let any of that get through. Cofense Intelligence is absolutely worth it."

