Pulsedive + BAYSIDE SOLUTIONS = Enriched, real-time phishing management

Bayside Solutions, Inc.

Founded 2001

US cybersecurity firm serving clients in energy, finance, defense, high-technology, and other sectors

Solution Spotlight

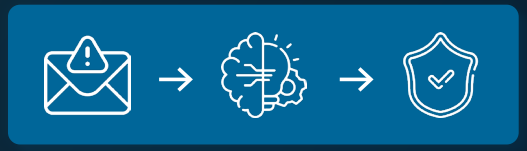
BSI's PhishQueue is a phishing management service that allows users to report suspicious messages, get expert analysis, and detect threats.

BSI leverages Pulsedive Enterprise for intelligence processing and management.

Pulsedive® Enterprise

A Fight Against Phishing

Phishing attacks remain one of the most common forms of cybercrime that can have severe consequences for organizations. To help clients defend their networks, BSI sought to enable users to proactively identify and report suspicious emails while freeing up precious in-house resources.



Clients were eager to implement such a service, but BSI first needed a way to collect and organize the intelligence generated by automated and human research. This led to the design of "PhishQueue," the phishing management service offering expert examination and threat detection.

Bolstered by Intelligence

Developed around proprietary systems, PhishQueue would:

1. Ingest emails reported by users
2. Analyze content: inspecting headers and attachments, verifying sender authenticity, detecting spoofing or malicious activity
3. Develop insight cards with tagging for long-term tracking and analysis
4. Return timely responses and reporting to end users
5. Return actionable IOCs and Purge requests to customer IT / security teams

Insight Cards

Summary of collected threat information for each reported email

- email directionality and timeline
- parsed and enriched IOCs (URLs, IPs)
- SMTP gateways
- DMARC records
- SPF records
- safe sender verification

“Pulsedive Enterprise offers seamless integration and powerful threat enrichment... The collection of correlated research and threat feeds makes sharing and collaboration easy to implement.”

Anthony Arrington, Director of Cyber Threat Intelligence

Threat Intel Requirements

The ideal threat intelligence partner had two core features: critical, on-demand enrichment data and a centralized database to efficiently manage PhishQueue’s unique IOCs. As a bonus for situations requiring deeper investigations, BSI sought a cyber threat intelligence (CTI) tool with robust user interfaces for human analysis and pivoting.

Unfortunately, many available threat intelligence platforms had irrelevant features, overly complex licensing and pricing, limitations on data ingestion, enrichment, and export, or needed more of the in-depth correlation, pivoting, and collaboration functionality that BSI required.

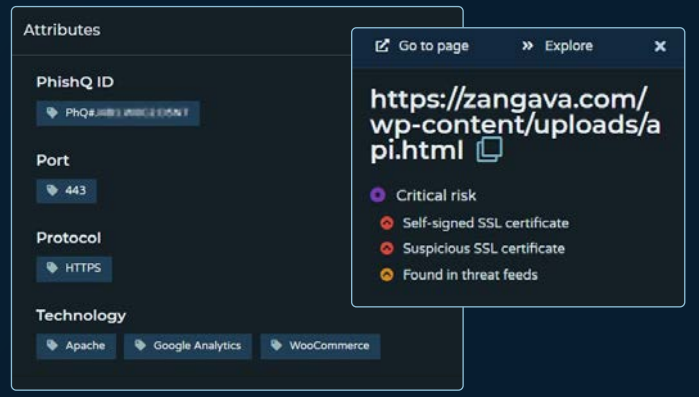
Three capabilities set Pulsedive apart as the winning choice:

- Flexibility in processing, editing, and exporting data
- Transparent risk factors behind each risk score, which supported analysis and accurate verdicts
- Preconfigured feeds with the ability to add, parse, and ingest new sources code-free

Hitting the Ground Running

Collaborating over three months, BSI & Pulsedive transitioned from a Pulsedive POC with the PhishQueue MVP to full commercial implementation and solution launch. Together, the team:

1. Deployed a fully functional Pulsedive POC
2. Ingested reputable phishing feeds for real-time cross-referencing against known threats
3. Built custom automation connectors and workflows to process and enrich IOCs
4. Implemented BSI’s custom “PhishQueue ID” tagging system to track threat actors and campaigns



Faster Speed to Response

Complete analysis for every report, with >95% response within 2h during core hours

Increased Accuracy in Determinations

Correcting up to 25% false positives, false negatives, and mis-categorizations of other tools

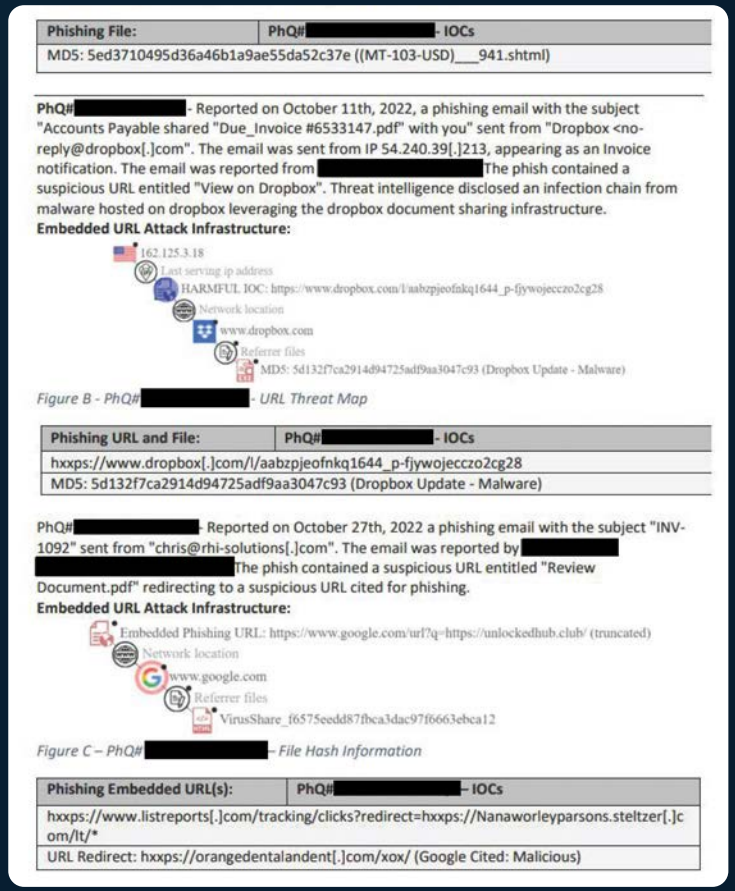
Intel-Informed Proactive Defense

Augmenting strategic defense with threat actor TTPs and campaigns reporting

Results

After deployment in client environments, PhishQueue successfully expanded in both processing volume and CTI maturity. Their dedicated Pulsedive Enterprise Threat Intelligence Platform processes millions of IOCs weekly, with the streamlined workflows making it possible for the team to address over 95% of all reported emails within 2 hours during core hours. Facilitated by Pulsedive's enrichment and custom curation capabilities, PhishQueue now also provides monthly reports with deep-dive threat activity and actor tracking.

Intelligence. Equipped with live and historical data from Pulsedive, PhishQueue creates detailed phishing attack timelines with initiation, malicious activity, and remediation timestamps. The team has detected numerous phishing kits and tracks specific threat actors, including the resurgence of Emotet's "Swiss army knife style" malware in early 2022. Beyond individual reports, PhishQueue's ability to analyze threat actor tactics, techniques, and procedures (TTPs), monitor evolving themes, and assess motivations informs proactive defense at a larger scale.



Phishing File:	PhQ#[redacted]- IOCs
MD5: 5ed3710495d36a46b1a9ae55da52c37e ((MT-103-USD)___941.shtml)	

PhQ#[redacted]- Reported on October 11th, 2022, a phishing email with the subject "Accounts Payable shared "Due_Invoice #6533147.pdf" with you" sent from "Dropbox <no-reply@dropbox[.]com". The email was sent from IP 54.240.39[.]213, appearing as an Invoice notification. The email was reported from [redacted] The phish contained a suspicious URL entitled "View on Dropbox". Threat intelligence disclosed an infection chain from malware hosted on dropbox leveraging the dropbox document sharing infrastructure.

Embedded URL Attack Infrastructure:

Figure B - PhQ#[redacted]- URL Threat Map

Phishing URL and File:	PhQ#[redacted]- IOCs
hxxps://www.dropbox[.]com/l/aabzpjeofnkq1644_p-fjywojecczo2cg28	
MD5: 5d132f7ca2914d94725adf9aa3047c93 (Dropbox Update - Malware)	

PhQ#[redacted]- Reported on October 27th, 2022 a phishing email with the subject "INV-1092" sent from "chris@rhi-solutions[.]com". The email was reported by [redacted] The phish contained a suspicious URL entitled "Review Document.pdf" redirecting to a suspicious URL cited for phishing.

Embedded URL Attack Infrastructure:

Figure C – PhQ#[redacted]– File Hash Information

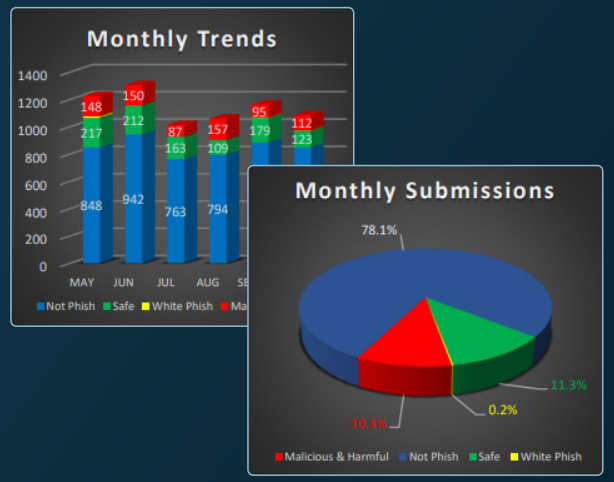
Phishing Embedded URL(s):	PhQ#[redacted]– IOCs
hxxps://www.listreports[.]com/tracking/clicks?redirect=hxxps://Nanaworleyparsons.steltzer[.]com/lt/*	
URL Redirect: hxxps://orangedentalandent[.]com/xox/ (Google Cited: Malicious)	

PhishQueue client report detailing phishing submission and attack infrastructure. IOCs are enriched and stored in Pulsedive Enterprise TIP.

“Pulsedive Enterprise’s threat insights and workflows take the TIP beyond simple enrichment.

“Our unique deployment of the Pulsedive Enterprise platform allows tactical threat intelligence to be accessed from one centralized application. The rich API provides access to granular meta-data and privately hosted analyst notes. Pulsedive’s insight into sophisticated threats places the threat data under the fingertips of analysts to deploy quick and systematic countermeasures.”

Anthony Arrington, Director of Cyber Threat Intelligence



Monthly PhishQueue reports summarizing client email reports, categorizations, and trends over time.

Closing the Gap. In comparative analyses with leading phishing protection tools, PhishQueue is closing the gap on erroneous determinations.

The team regularly detects and neutralizes false negatives, handles false positives, and addresses other mis-categorizations. In some cases, the inaccurate verdicts of widely used tools rose higher than 20%.

For example, PhishQueue was able to identify malicious emails with CAPTCHA, which other services failed to detect. This was a significant discovery as adding CAPTCHA increases the chance of a successful phishing attempt two-fold: creating a more realistic infection chain to trick users of legitimacy while slowing down defense operations.

Conclusion. Overall, PhishQueue has increased user engagement and awareness, while allowing client teams to redirect their security operations resources to more strategic measures.

Next, PhishQueue will leverage more of Pulsedive’s features by developing its own API framework. Doing so will allow the team to expand their insight cards, publish a unique threat feed, and create more customized tracking as BSI’s clients’ leading phishing email analysis service.