AN INTELLIGENCE-DRIVEN APPROACH TO SPEARPHISH ANALYSIS

Spearphishing is undoubtedly one of the most prolific and successful attack vectors currently employed to compromise targets. Unlike classic technical attacks, it exploits one of the hardest vulnerabilities to patch or mitigate: the human characteristics of curiosity and trust.

ThreatQ™ is a Threat Intelligence Platform designed to enable true threat operations and management. It allows analysts and responders to analyze, investigate and respond to cyber events with an intelligence-driven approach. Due to the popularity and impact of Spearphishing campaigns, ThreatQ provides special parsing of email content to accelerate the analysis and response process to spearphish events.

IT ALL STARTS WITH ONE INNOCENT-LOOKING EMAIL

Spearphish messages commonly arrive as part of a wider campaign that spans multiple targets and emails, and therefore tracking the larger campaign is critical to understand the full scope of the attack. ThreatQ allows all intelligence objects and events to be linked to enable just that, a full view of the broader picture and techniques that span multiple emails and targets.

AT A GLANCE

- Automatically create Spearphish events driven by email content
- Parse the raw message body to identify mail contents
- Extract, save and link attachments to the original message and event
- Extract and relate indicators found within the message body
- Relate messages and indicators to adversaries and campaigns
- Outlook MSG, EML, EMLX, TXT

INVESTIGATE & RESPOND

- Use ThreatQ Operations to enrich extracted data
- Automatically deploy indicators to defence and response tools
- Investigate attachments and indicators
APPLICATION NOTE

IMPORTING SPEARPHISH EVENTS

STEP 1
Add new event and upload the spearphish email. Supports EML, EMIX and MSG file formats, or just paste the raw text.

STEP 2
Details about the event are automatically parsed from the email. Additional context can be added including links to known adversaries or other objects.

STEP 3
Review all the indicators and additional context that was identified in the mail sample before adding to the Threat Library™

THE THREATQ ADVANTAGE

Compare the Spearphish sample with intelligence stored in the Threat Library

Use an Adaptive Workbench™ to enrich and investigate the indicators and attachments found within the message

Use the ThreatQ Open Exchange™ to integrate with the sensor grid, feeding it with the latest details of active spearphish infrastructure to block and hunt

Add your own local context and information to support your event investigation

THREATQ ANSWERS HARD QUESTIONS

Is this email really malicious?

Is it associated with an advanced adversary?

Does it have malware attached?

What is the staging infrastructure used, and has anyone else communicated with it?

Who is targeted, and did they click a link?

ABOUT THREATQUOTIENT™

ThreatQuotient understands that the foundation of intelligence-driven security is people. The company's open and extensible threat intelligence platform, ThreatQ, empowers defenders to ensure the right threat intelligence is utilized within the right tools, at the right time. Leading global companies are using ThreatQ as the cornerstone of their threat intelligence operations and management system, increasing security effectiveness and efficiency.

For additional information, please visit threatq.com.

Copyright © 2017, ThreatQuotient, Inc. All Rights Reserved.

11400 Commerce Park Drive, Suite 200, Reston, VA 20191 • ThreatQ.com
Sales@ThreatQ.com • Sales and General Inquiries: +1 703 574-9885