CASE STUDY

Phishing & Business Email Compromise

Use Magnet AXIOM Cyber to Investigate Fraudulent Email

Fortune 500 Department Store Chain

500+ full line stores plus Online store | 100,000+ employees | Annual revenue $20+ billion

FORTUNE 500

Retailers are prime targets for cybercrime because they possess valuable customer payment information. According to Trustware's 2019 Global Security Report, the retail sector accounts for 18% of all cyber attacks. It is particularly vulnerable because retailers routinely transfer vast amounts of money and sensitive data, including bank and payment card information.

The Challenge

Organizations of all sizes are the targets of cyber attacks every day. Cybercrime is increasing in frequency, size, complexity, and cost to the victim organization. Two of the most common fraudulent email cases that organizations fall victim to are phishing attacks and business email compromise (BEC) fraud.

According to Cisco, in 2021, 86% of organizations had at least one user try to connect to a phishing site. Their popularity—and also effectiveness—relies social engineering that tricks unwitting employees, who are the most vulnerable point of access, into divulging sensitive information.

BEC fraud is a more complex, targeted, and methodical type of email attack. An employee's email account—usually the CEO or CFO—is spoofed or has actually been compromised and is then used to get others within the organization, usually Finance, to divulge confidential information or transfer money.

The FBI's Internet Crime Complaint Center (IC3) estimates global 'exposed dollar losses' to business email compromise fraud has exceeded $26 billion in the past three years.

> "Connections is my favorite tool for investigating Incident Response cases. I worked a BEC case where I had to examine OST and PST files. Using Connections I was able to quickly find where a zero-day phishing campaign originated. Without Magnet, I would have had to manually go through every email inbox."
>
> **– Cyber Fraud Analyst II, Threat Operations**

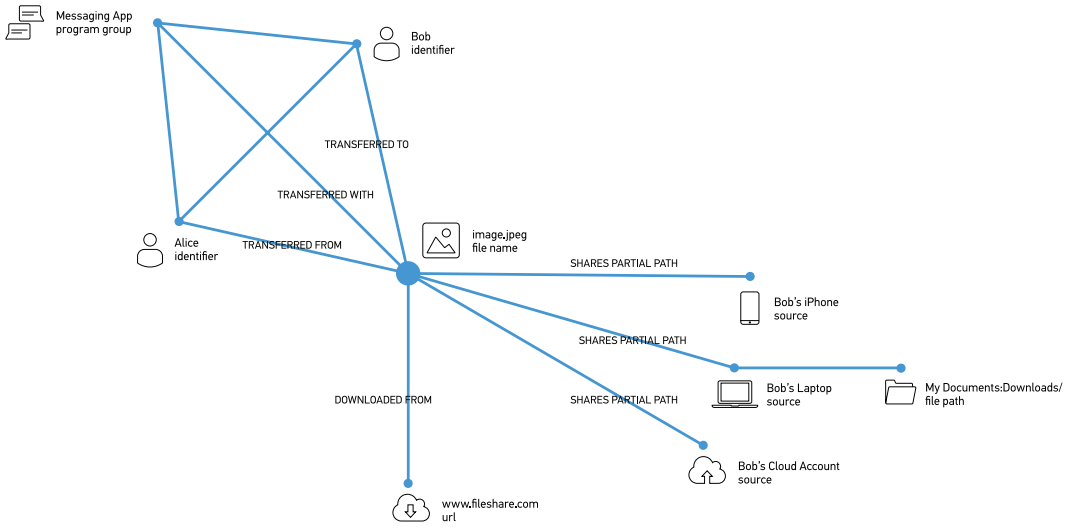
[1] https://www.trustwave.com/en-us/resources/library/documents/2019-trustwave-global-security-report/
[2] https://learn-umbrella.cisco.com/ebook-library/2021-cyber-security-threat-trends-phishing-crypto-top-the-list
[3] https://www.csoonline.com/article/3504649/fbi-bec-now-a-26-billion-fraud-as-hr-payroll-diversion-attacks-linked-to-same-scammers.html

HOW AXIOM CYBER HELPS

Visualize Connections

Connections is a powerful tool in AXIOM Cyber that quickly visualizes the relationships and correlations—or connections—between evidence items in your case. Use Connections in Fraud cases to quickly uncover things like:

- The point-of-origin of a malicious file, and how it infected other devices or compromised employee accounts.
- How and when sensitive data like customer payment information was accessed, by who, and also where it went. Armed with this knowledge, you can expedite the recovery of data and money.
- See how files move from cloud storage services like AWS or SharePoint to disk storage, and know what apps were used to access it, to paint a picture of how that file may have been fraudulently altered or shared.



See AXIOM Cyber in Action for Yourself

If you'd like to learn more about Magnet AXIOM Cyber and how it can help you simplify your remote forensic investigations, visit **magnetaxiomcyber.com**. While you're there, you can learn more about the product, request an in-depth personal demo from an AXIOM Cyber expert, and request a free trial version.

Learn more at magnetforensics.com

Book a demo today, call us at 1-844-638-7884 or email sales@magnetforensics.com

MAGNET FORENSICS®