To fight email scammers, take a different view. Literally.

November 1 2018

The FBI's Internet Crime Complaint Center (IC3) last year received complaints from 300,00 victims scammed of $1.4 billion. NYU Tandon School of Engineering researchers have worked with Agari to develop visualization tools that let police quickly identify the likely culprits. Credit: US Federal Bureau of Investigation

A team of researchers is helping law enforcement crack down on email scammers, thanks to a new visual analytics tool that dramatically speeds up forensic email investigations and highlights critical links within email data. Email scams are among the most prevalent, insidious forms of cybercrime.

Rental scams, romance scams, and business e-mail compromise scams are rampant, and even the savviest computer users can be duped. Law enforcement has long struggled to prosecute these crimes due to the difficulty of identifying cybercriminals, but several agencies are already deploying the new software to trace the trail of email scammers.

The new tool is the work of a research team at the New York University Tandon School of Engineering, led by Assistant Professor of Computer Science and Engineering Enrico Bertini, in collaboration with Silicon Valley-based data security company Agari, which specializes in developing email security products for corporations. Bertini named the tool Beagle—a play on the sharp search skills of canines used to sniff out evidence in criminal investigations.

The research team has already begun sharing Beagle with law enforcement agencies at no cost to assist in their investigations, and will continue to refine its capabilities based on real-world feedback.

The pre-Beagle tools for current forensic email investigations are surprisingly primitive. Investigators often rely on the search functions of common email clients, which retrieve results based on specific queries and are most useful when investigators know what to search for—no small feat in cases that can involve many scammers and hundreds of thousands of emails.

"This is where our work starts," said Bertini. He explained that Beagle creates a visual analytical interface that can return queries as well as

summarize emails and highlight commonalities between them, even in fields investigators might otherwise overlook— such as the time an email is sent, the geographical location of victims, and key words and content patterns.

"Beagle builds pictures from the data, making it much easier to connect the dots and ultimately understand how scam networks operate, from first contact with a victim through what are often multiple rounds of extortion," Bertini said.

Beagle was developed in a two-year iterative process using a database of more than 100,000 emails intercepted from real-life scammers by Agari. A case study of its development and deployment process appears in the journal *IEEE Transactions on Visualization and Computer Graphics*. Co-authors of the study include NYU Tandon doctoral students Jay Koven, Cristian Felix, and Hossein Siadati, as well as contributors from Agari.

"Business email compromise and other forms of email fraud are being perpetuated by multinational criminal organizations on a global scale," said John Wilson, Field CTO, Agari. "Beagle has enhanced our ability to monitor and track these criminal organizations, painting a fuller picture of the individuals involved and their relationships between one another."

Beagle has already been used to illuminate an entire network of scammers and victims, starting with emails from a single known scammer and ultimately encompassing multiple scammers and a cohort of victims—information that was subsequently shared with law enforcement agencies.

"We were surprised to discover that Beagle can actually build evidence," Bertini said, noting that the tool can amplify the analytical process by surfacing connections that lead to additional queries and data enrichment.

Provided by NYU Tandon School of Engineering