AREA 1

Microsoft Partner

Microsoft

Partner of the Year

Google Cloud

ACTIVE FRAUD PREVENTION

Comprehensive Protection Against Phishing-related Financial Cybercrimes

PROBLEM

- Fraud and phishing attacks, the cause of over 95% of breaches, increasingly rely on social engineering, making them difficult for traditional security tools to detect
- Legacy security solutions routinely miss over 30% of attack campaigns, creating more work for SOC teams

SOLUTION

- Area 1 Security is the only solution that preemptively stops phish across email, social, web and network attack vectors
- Area 1 extends protection to supply chain partners to comprehensively stop active fraud in progress

As cybercrime evolves, fraud — in particular phishing and business email compromise (BEC) — has risen to the top both in terms of prevalence and financial damage caused. The FBI recorded $3.5 billion in reported losses due to cybercrime in 2019. Much of this was due to financial fraud like BEC, rogue wire transfers, ransomware and spoofing. In fact, the most costly cybercrime in the U.S. was BEC, costing over $1.7 billion and making up over 40% of all internet crime related losses in 2019.

The latest forms of cyber fraud present a particular challenge to legacy email security systems. Traditional secure email gateways (SEGs) were built to handle commodity spam instead of today's targeted attacks, phish and BEC, resulting in missed detections. In fact, legacy solutions miss over 30% of attack campaigns. With 95% of breaches caused by phish, this creates a huge security gap and adds exponentially to security operation workloads.

To combat modern cybercrime, organizations need to adopt solutions with Active Fraud Prevention capabilities to comprehensively detect and stop attacks missed by SEGs.

[1] Federal Bureau of Investigation's Internet Crime Complaint Center (IC3). "2019 Internet Crime Report," Feb. 11, 2020. https://pdf.ic3.gov/2019_IC3Report.pdf

AREA 1

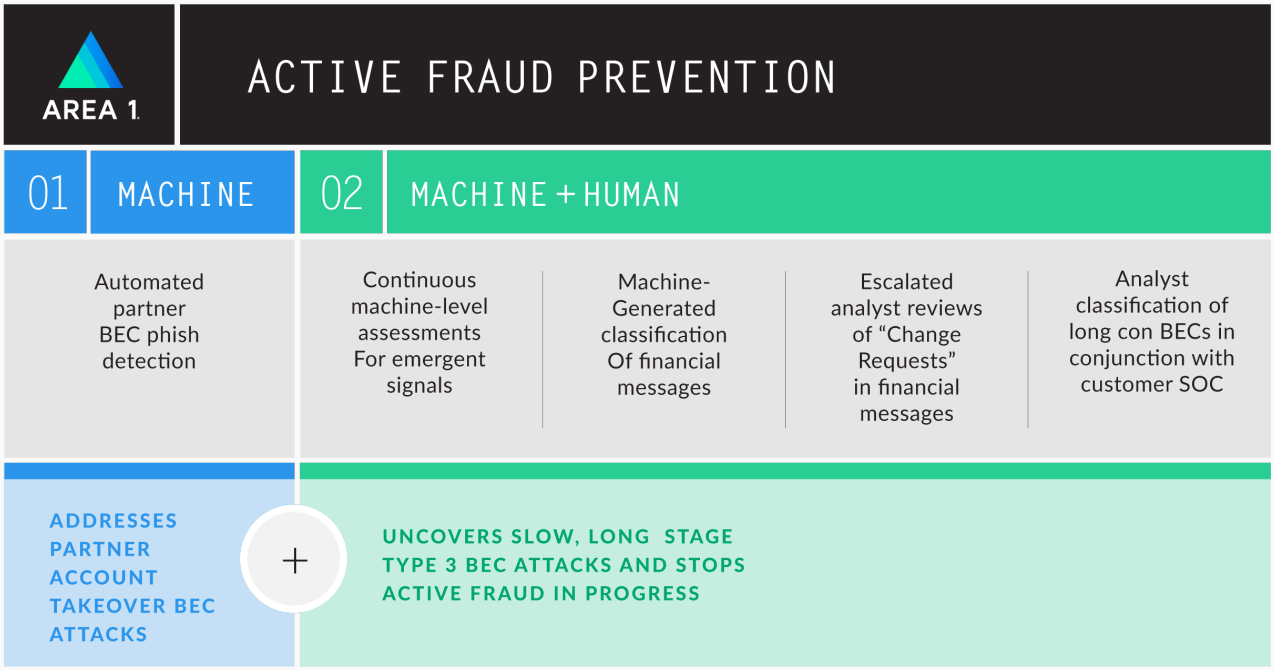
ACTIVE FRAUD PREVENTION

Stopping modern fraud attacks requires the ability to detect low-volume, targeted phish and BEC. As attackers increasingly use social engineering over malware for many of these attacks, detecting malicious intentions, even if there is no malware present, is key. Discovering fraud attempts, often conducted over a span of multiple conversations, over weeks and months, also calls for advanced machine learning algorithms.

Area 1 Security takes a machine + human approach for comprehensive Active Fraud Prevention across all threat vectors for fraud: email, social, web and network. Our approach allows us to stop all the threats anti-spam, anti-virus and advanced threat protection systems typically catch, but we also go above and beyond to preempt attacks and stop active fraud campaigns before they do harm.

In the first 12 weeks of service, Area 1 intercepted $233 million in Type 3 BEC fraud campaigns

Area 1 takes a machine + human approach to preemptively prevent phishing attacks as well as stop active fraud in progress:



AREA 1

Preempting attacks starts with Area 1's ActiveSensors™ for massive-scale web crawling and small pattern analytics engine (SPARSE™), which allow us to proactively discover and track attacker infrastructure. With these technologies, Area 1 is able to detect emerging attack infrastructure an average of 24 days before phishing campaigns go live.

Through our extensive research and detection of phishing campaigns, we've tracked and divided BEC evolution into three types. **Type 1 BEC** uses CXOs and display names as a lure through inter-organization impersonation. **Type 2 BEC** uses hijacked employee accounts as a lure in intra-organization impersonation. **Type 3 BEC**, the most difficult to detect and most financially damaging, relies on account takeovers of trusted supply chain partners and vendors to appear authentic. Area 1 excels at detecting all three types of BEC, but we're particularly good at catching the sophisticated, long-con Type 3 BEC fraud commonly missed by legacy email security systems.

Our Active Fraud Prevention starts with Area 1's automated supply chain BEC phish detection, which addresses the vast majority of these partner account takeover-based BECs. We also take a combined machine/human approach designed to uncover the slow, drawn-out development of Type 3 BEC phish.

Area 1 conducts continuous machine level assessments of all messages for emergent signals of fraud. Messages are also auto-classified, surfacing categories of interest like financial messages. After multiple levels of machine-driven detection, we employ escalated analyst reviews of change requests in the small amount of financial messages with undetermined verdicts. Final joint confirmation with Area 1 security analysts and customer SOC teams results in precise verdicts with low false-positive rates. This process allows for scalable and accurate detections that stop active fraud campaigns in their tracks.

The methodologies and technologies we employ for preemptive and active fraud prevention can be summarized in the chart below.

1 CAMPAIGN SOURCE ANALYSIS

Preemptive crawling to discover and track attacker infrastructure

2 MESSAGE SENTIMENT ANALYSIS

Understanding what's being expressed within the message

3 PARTNER SOCIAL GRAPHING

Assessing supply chain partner reputation and vendor account takeover

4 CONVERSATIONAL CONTEXT ANALYSIS

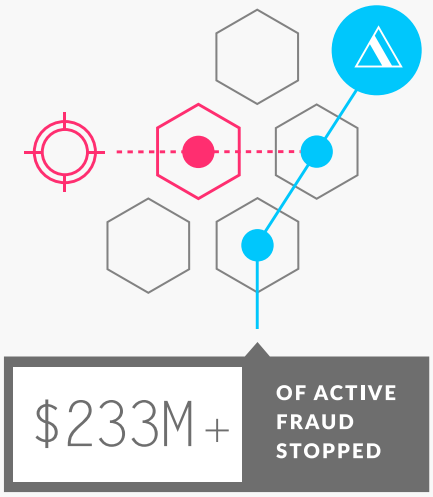
Analyzing variations within an entire message thread for suspected fraud

5 UNIVERSAL MESSAGE CLASSIFICATION

Surfacing Categories of Interest (COIs) for secondary assessments

6 VERDICT ESCALATIONS

Rapid escalations for analyst review and customer SOC confirmation



THROUGH THIS ADVANCED METHOD, AREA 1 HAS INTERCEPTED MORE THAN $233 MILLION IN TYPE 3 BEC FRAUD CAMPAIGNS TARGETING FORTUNE 500 COMPANIES IN JUST THE FIRST 12 WEEKS.

Since 2019, we have also caught more than 100 million phish missed by SEGs.

Area 1 Security is the only cybersecurity company able to comprehensively block phishing and fraud attacks before they do harm. To protect your organization from modern cybercrimes, try us out at ***www.area1security.com/try-area1***

About Area 1 Security

Area 1 Security offers the only pay-for-performance solution in the cybersecurity industry - and the only technology that comprehensively blocks phishing attacks before they damage your business. Phishing is the root cause of 95 percent of security breaches.

Area 1 Security works with some of the most sophisticated organizations in the world, including Fortune 500 banks, insurance companies, and healthcare providers to preempt and stop targeted phishing attacks at the outset, improve their cybersecurity posture and change outcomes.

Learn more at www.area1security.com, join the conversation at @area1security or subscribe to the Phish of the Week for the latest industry news and insights on how to deal with phishing.