SOLUTION BRIEF

Account Takeover Attack Prevention

Protect Your Employees From Becoming Victims of Account Takeover-Based Attacks

Organizations are more likely to be breached today than ever before, as cybercriminals shift tactics once again, using account takeovers (ATOs) to launch targeted email attacks. In fact, a recent Osterman Research survey showed that 33% of organizations were victims of an ATO-based email attack. Attackers know that trusted email is the most effective way of breaching an enterprise, as existing security controls cannot detect these attacks since they come from previously-established credible senders. Meanwhile, employees have a hard time spotting these attacks because they appear to come from trusted colleagues. As such, organizations must place a higher priority in protecting against account takeovers—or risk becoming the next victim.

Anatomy of an Account Takeover-Based Email Attack

X-OriginatorOrg: zyx.com
X-Original-Sender: tkoslowsky@zyx.com
X-Original-Authentication-Results: mx.firstbanking.com;
dkim=pass header.i=@outlook.com header.s=selector1 header.b=Wexxd0VU;
spf=pass (zyx.com: domain of tkoslowsky@zyx.com designates 40.92.254.24 as permitted sender) smtp.mailfrom=tkoslowsky@zyx.com;
dmarc=pass (p=NONE sp=QUARANTINE dis=NONE) header.from=zyx.com
MIME-Version: 1.0

1 **Incoming ATO-based attacks pass DMARC authentication. DMARC does not apply to insider impersonation-based attacks.**

From: Todd Koslowsky <tkoslowsky@zyx.com>
Date: Fri, 28 Jun 2019 8:22:30 -0700
Subject: RE: EOQ Contracts Approval
To: Steve Bowman <sbowman@firstbanking.com>

2 **The attacker need not use impersonation and risk detection.**

Hi Steve,

Sorry, I just saw a critical error, can you review the changes in the attachment?

Thanks,
Todd

3 **The attacker hijacks the conversation and exploits previously-established trust to convince the victim to take action.**

From: Todd Koslowsky <tkoslowsky@zyx.com>
Date: Fri, 28 Jun 2019 at 11:02 AM
Subject: RE: EOQ Contracts Approval
To: Steve Bowman <sbowman@firstbanking.com>

Hi Steve,

Bill and I will finalize our review by tomorrow and provide feedback then.

Regards,
Todd

Introducing ATO-Based Email Attack Prevention

Agari Phishing Defense™ prevents account takeover-based attacks from reaching employee inboxes. It also inspects email flowing within the organization for indicators that an internal email account has been compromised for unauthorized use. Once an account takeover is suspected, Agari Phishing Defense prevents the spread of malicious emails from affected accounts laterally within and external to the organization.

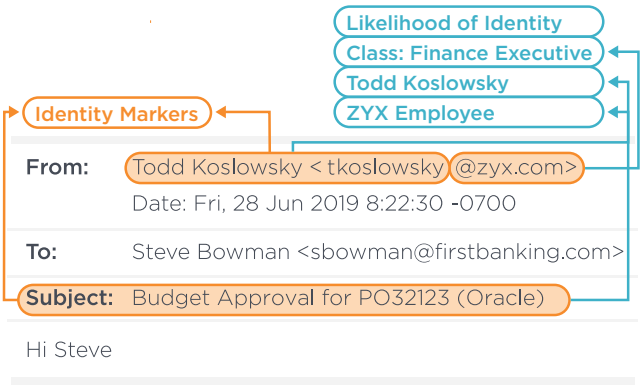
> "In the past year, we have seen a 300% increase in the number of compromised accounts sending advanced email attacks into the organization and we see stopping this threat as a critical security control."

CSO, Large Healthcare Organization

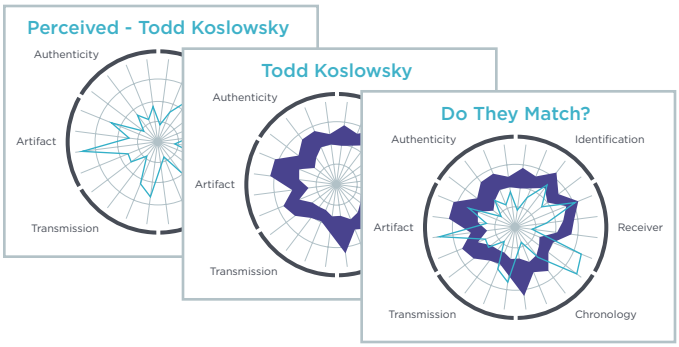
How Agari Phishing Defense Works

Agari has configured the Agari Identity Graph™ to model external ATO-based behavior to prevent account takeovers originating outside the organization. The Agari Identity Graph also scans internal employee-to-employee messages to detect malicious attachments and URLs sent from compromised internal accounts.

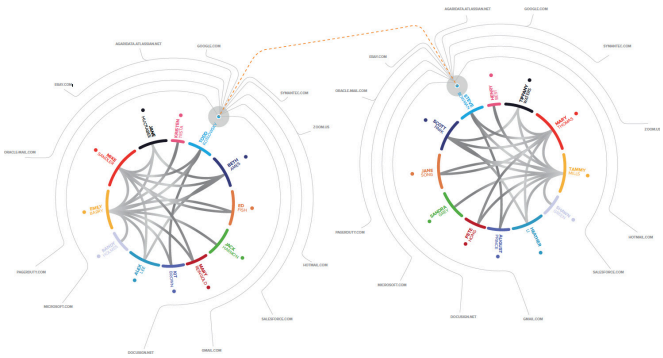
Identity Mapping: Determines the perceived identity of the sender, mapping the sender to a previously-established sender/organization or a broader classification.



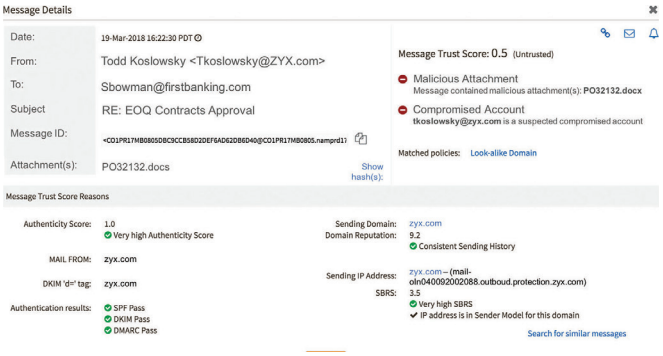
Behavioral Analytics: Given the derived identity, the message is evaluated for anomalies relative to the expected sender behavior, such as whether the sender has ever interacted with the recipient or whether the content of the message sent by the sender is expected.



Trust Modeling: The final phase determines if communication from the sender is expected by the recipient. Ultimately the system models interaction—how often the sender/recipient interact and if the responsiveness between the two is normal.



Identity Graph Scoring: The final Identity Graph Score of a message is a combination of the features and indicators of the three phases that determines whether the attack is indeed originating from a compromised account.



Benefits of Implementing Agari

With the increased effectiveness of exploiting account takeovers over existing techniques, rising financial gains, and lack of organizational protections, attackers are highly motivated to increase their attack rate in the coming year. With Agari Phishing Defense, organizations will have the prevention capabilities needed to stop these attacks—ensuring critical business communication continues to flow securely and uninterrupted.

The Company We Keep

Top 3 Social Networks | 6 of the Top 10 Banks | Top Cloud Providers

Microsoft HSBC aetna facebook citi CHASE Google

Learn More: www.agari.com/products