REPORT

Abnormal SECURITY

Quarterly Threat Report

High-Profile Socially-Engineered Email Attacks Drive Record-High Employee Engagement & Fraud

Executive Summary

On March 17, the FBI released its seminal annual Internet Crime Report. Once again, socially-engineered attacks (including business email compromise, spoofing and phishing) by far were the number one cybercrime by financial loss, accounting for $2.1 billion of the $4.2 billion in losses to U.S. businesses and consumers. These attacks utilize impersonations to get companies to transfer money to fraudulent accounts, and pose significantly more financial danger to an organization than well-known tactics such as malware and ransomware.

As the FBI noted in its report, "fraudsters have become more sophisticated by evolving their techniques to use social engineering to compromise vendor email accounts and use stolen identities to establish bank accounts to receive stolen funds through invoice fraud."

Attackers haven't let up in 2021. As the only source of industry data on the true volume of BEC attacks, we found that attacks across a variety of categories grew at significant rates. Quite simply, attackers are more successful by using socially-engineered attacks to bypass existing protections such as secure email gateways.

Key Research Takeaways:

- The rate of employee engagement **increased by 50%** for socially-engineered attacks that bypass secure email gateways or other existing protections.
- Employees are **four times more likely** to engage attackers through lateral phishing attacks from compromised internal accounts than with credential phishing from external accounts.
- There was a **250% increase** in the presence of malicious mail filters from Q4 2020 to Q1 2021.
- The percentage of companies across industries hit with VEC attacks **increased 119%** between July 2020 and April 2021.

It's clear traditional secure email gateway defenses were not designed to stop socially-engineered attacks. In order to stem the tide, organizations need to consider a new approach. Without one, high-profile attacks such as SolarWinds and USAID, which we can surmise started with socially-engineered campaigns, will continue to cause severe financial and reputational loss.

- The Abnormal Security Threat Research Team

Q1 2021 State of BEC

Attackers Leverage Socially-Engineered Attacks to Drive Significantly Higher Engagement and Account Takeover

For socially-engineered BEC attacks, there is a 50% increase in employee engagement when compared to traditional email attacks. Socially-engineered attacks are zero-day in nature, have never-seen-before and contain no malicious payloads. These techniques make them more successful at bypassing traditional defenses and eliciting engagement in order to lure targets into rerouting funds.

For less sophisticated traditional email attacks that contain malicious attachments or links there's relatively low engagement - approximately 3% overall - and hence do not pose as much of a financial risk as socially engineered attacks.

50% ⇧

Increase in employee engagement

for novel sophisticated attacks

The Impact of Socially-Engineered Attacks

According to the FBI, Socially-Engineered email attacks are responsible for more than $2.1B in lost revenue last year, by far the most of any security threat. They use impersonations to get companies to transfer money, and pose significantly more financial danger to an organization than well-known tactics such as malware and ransomware.

2020 FBI IC3
Jan 2021

$2.1B

Socially-Engineered Attacks:

- BEC/EAC
- Spoofing
- Phishing

$29.1M
Ransomware

$6.9M
Malware

The USAID Attack is the Latest in a Long Line of Credential Phishing Attacks

We can surmise that high-profile attacks such as SolarWinds and USAID started with a successful credential phishing attempt of a vendor or employee account.

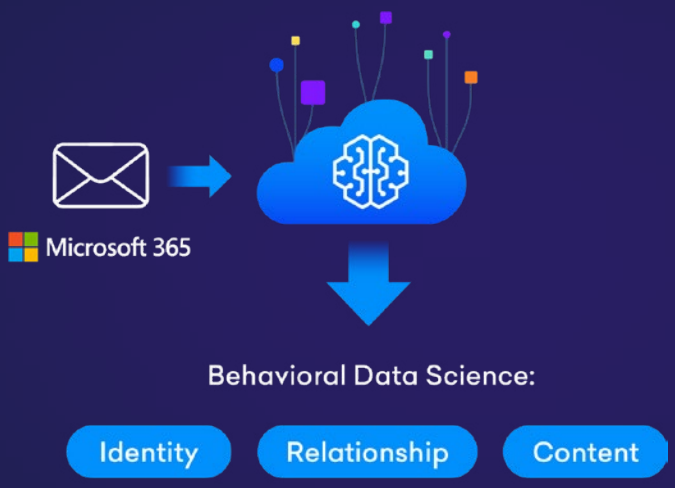
Once an employee's account credentials are phished, attackers can move laterally across the organization (known as east-west traffic), and send malware or ransomware attacks that are likely to be engaged with.

Lateral, east-west traffic often goes undetected by traditional defenses that miss out on device and sign-in location data signals.

In contrast, with an API architecture approach, organizations should be able to detect east-west traffic and catch internal account compromises.

4X

Employee engagement with attackers through lateral phishing attacks vs. external attacks



API Architecture Enables Compromise and Phishing Detection

The new API driven approach pioneered by Abnormal Security uniquely leverages behavioral data science to profile and baseline good behavior to detect account compromises and phishing attacks. We deliver this approach through a cloud-native email security platform that can be deployed instantly into Microsoft Office 365 via a 1-click API integration - and can be used to extend your existing Secure Email Gateways.

Substantial Increase in Malicious Mail Filters

The presence of malicious mail filters jumped considerably this past quarter. There was a 250% increase in malicious mail filters from 7% to 23% between Q4 2020 and Q1 2021.

Malicious mail filters indicate an attacker either currently has, or previously had, compromised the account and set up mail configurations to obfuscate their tracks. The mail filter can be used to redirect emails to an impersonated domain, or send replies to the junk folder or trash.

Overall, we see that at least 6% of the mail filters explicitly forward or redirect internal messages to an external domain, and another 8% hide invoice related messages.

The presence of malicious mail filters goes undetected by traditional email security defenses. In order to combat them, organizations need an API-architecture approach that can detect abnormal behavioral patterns to prevent these attacks.

250%

Increase in the presence of malicious mail filters

from Q4 2020 to Q1 2021

How Mail Filters are Maliciously Used

1. Redirects conversation to an impersonated domain
2. Sends replies meant for the real accounts to Junk folders or Trash

Percent of Customers with Malicious Mail Filters Found After Integration

Figure 1. Percent of Companies with Malicious Mail Filters Present in the Environments

Vendor Email Compromise (VEC) Attacks Accelerate At Fast Rate

The percentage of companies across industries getting hit with VEC attacks increased 119% from July 2020 to April 2021, as threat actors increasingly see communications between vendors and customers as the weakest link and focus their efforts on these types of supply chain attacks.

There have been a string of recent high-profile, socially-engineered phishing attacks this year, with SolarWinds and the USAID attack, which we can surmise all started with credential phishing attempts of a vendor or employee email account.

119%

Increase of VEC attacks

These attacks are hard-to-detect for organizations because they leverage trusted relationships. Forward thinking security professionals are increasingly coming to the conclusion their security is tied to their partner ecosystem, which in many cases spend less on security than they do.

To combat vendor compromise attacks, organizations need a solution (VendorBase) that can automate the process of knowing which vendors are compromised and removes the manual burden of remediating and investigating VEC attacks from compromised vendors.

Weekly Percent of Companies Hit with VEC Campaigns

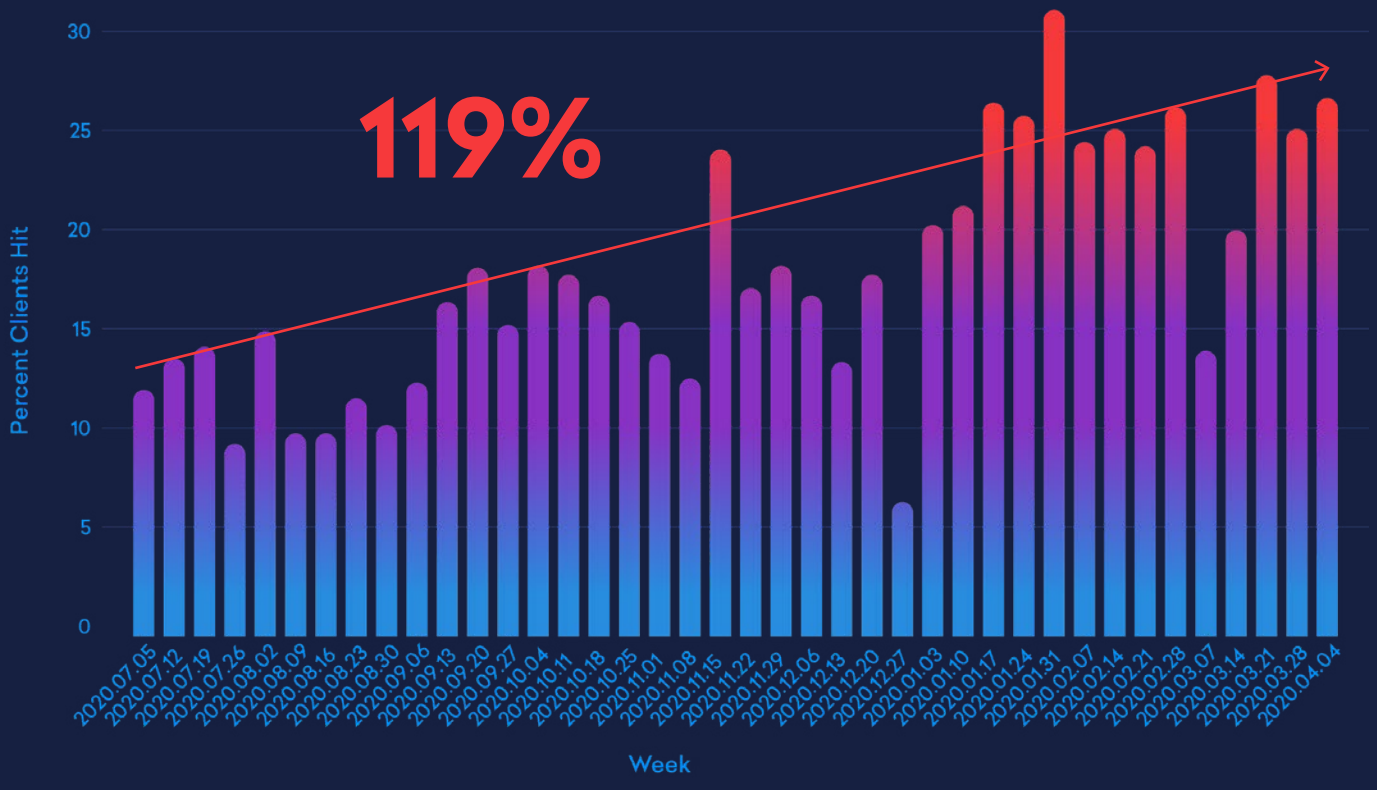


Figure 2. Percentage of companies hit with VEC attack each week

Figure 3: Percentage of companies getting hit with a VEC attack at least once a quarter.

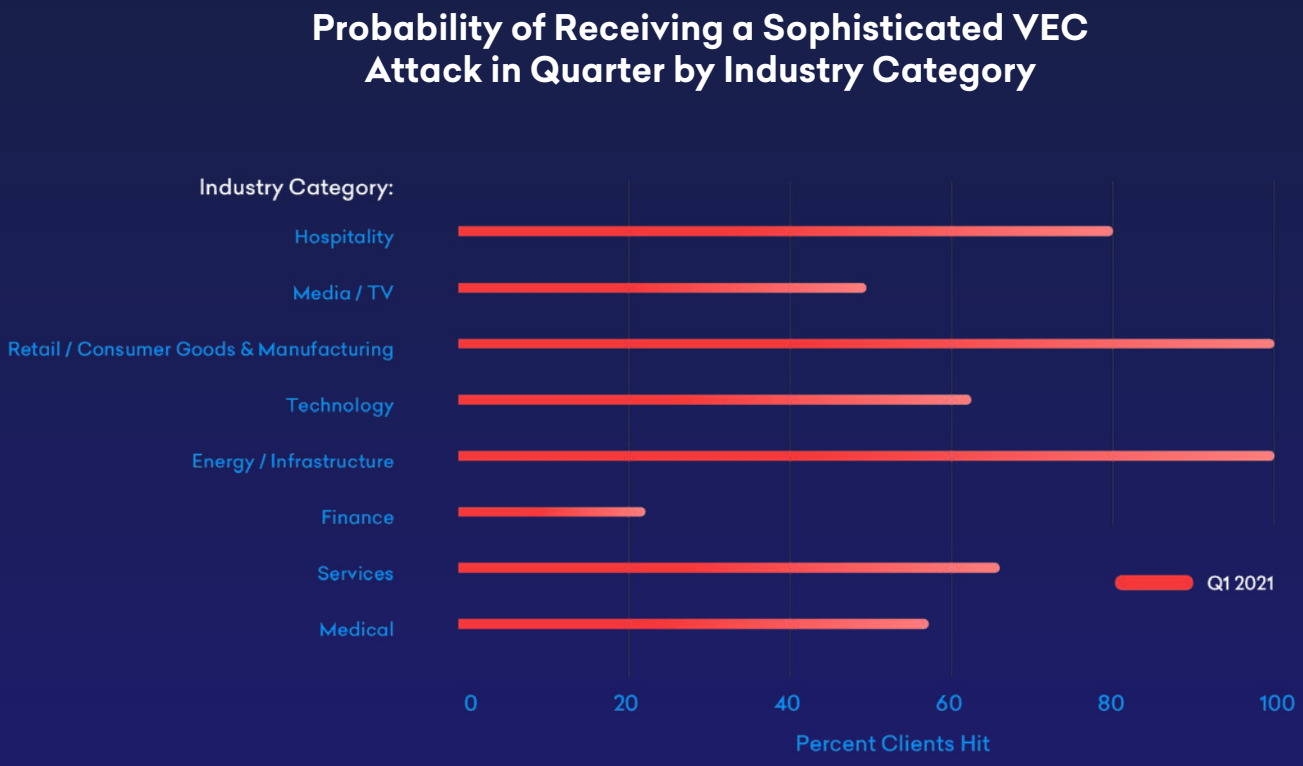


Figure 4. Chance of companies getting hit with a VEC attack at least once per quarter, by industry

Abnormal Security provides the leading cloud-native email security platform that leverages behavioral data science to stop modern email attacks.

Unlike legacy email security solutions, the Abnormal Security platform uses an innovative AI-based approach that deeply understands the people, relationships and business processes to stop the most sophisticated cyber-attacks.

Abnormal Security is based in San Francisco, CA.

More information is available at:

abnormalsecurity.com

Follow us on Twitter:

@AbnormalSec